

SAP® ERP, 4th Edition Audit Programs/ICQs

ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP® ERP, 4th Edition Audit Programs/ICQs* (the “Work”) primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP’s kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: www.isaca.org/sap-erp-4th-edition

Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOOfficial>

Like ISACA on Facebook: www.facebook.com/ISACAHQ

SAP® ERP, 4th Edition Audit Programs/ICQs

Table of Contents

Security, Audit and Control Features SAP® ERP, 4th Edition provides practical guidance for all stakeholders involved in the SAP enterprise resource planning (ERP) audit/assurance process. The objective of the publication is to enable audit, assurance, risk and security professionals (information technology [IT] and non-IT) to evaluate risk and controls in existing ERP implementations and to facilitate the design and building of better practice controls into system upgrades and enhancements. The publication was designed to be a practical how-to guide based on SAP ECC versions 5.0 and 6.0. However, most of the features and testing techniques described are also applicable to the earlier versions of SAP® R/3, namely 4.6c and 4.7.

This tool kit provides appendices D and E in MS Word format to allow the user to customize the audit programs and internal control questionnaires (ICQs) to fit the organization under review.

1. SAP ERP Revenue Business Cycle Audit/Assurance Program and ICQ
2. SAP ERP Expenditure Business Cycle Audit/Assurance Program and ICQ
3. SAP ERP Inventory Business Cycle Audit/Assurance Program and ICQ
4. SAP ERP Financial Accounting (FI) Audit/Assurance Program and ICQ
5. SAP ERP Managerial Accounting (CO) Audit/Assurance Program and ICQ
6. SAP ERP Human Capital Management Cycle Audit/Assurance Program and ICQ
7. SAP ERP BASIS Administration and Security Audit/Assurance Program and ICQ
8. SAP ERP Control Environment ICQ
9. Blank Audit/Assurance Program Template

How to Use the Audit/Assurance Programs

Overview

ISACA developed the IT Assurance Framework (ITAF) as a comprehensive and good-practice-setting model. ITAF provides standards that are designed to be mandatory and that are the guiding principles under which the IS audit and assurance profession operates. The guidelines provide information and direction for the practice of IS audit and assurance.

Purpose

The audit/assurance program is a tool and template to be used as a road map for the completion of a specific assurance process. ISACA has commissioned assurance programs to be developed for use by IS audit and assurance practitioners. This assurance program is intended to be used by IS audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF standard 2006 Proficiency.

Control Framework

The audit/assurance programs have been developed in alignment with the ISACA COBIT 5 framework, using generally applicable and accepted good practices. The generic assurance program is presented in *COBIT 5 for Assurance* and ensures integration of all seven enablers in the assurance approach.

Governance, Risk and Control of IT

Governance, risk and control of IT are critical in the performance of any assurance management process. Governance of the process under review is evaluated as part of the policies and management oversight controls. Risk plays an important role in evaluating what to audit and how management approaches and manages risk. Both issues are evaluated in the assurance program. Enablers are the primary evaluation point in the process. The assurance program identifies the enablers and the steps to determine their design and operating effectiveness.

Responsibilities of IS Audit and Assurance Professionals

Assurance professionals are expected to customize the *SAP ERP Audit/Assurance Programs* for the environment in which they are performing the assurance engagement. This document is to be used as a review tool and starting point and may be modified by the IS audit and assurance professional; it is not intended to be a checklist or questionnaire. It is assumed that the IS audit and assurance professional has the necessary subject matter expertise that is required to conduct the work (see following paragraph) and is supervised by a professional with the Certified Information Systems Auditor (CISA) designation and/or necessary subject matter expertise to adequately review the work performed.

Minimum Audit Skills

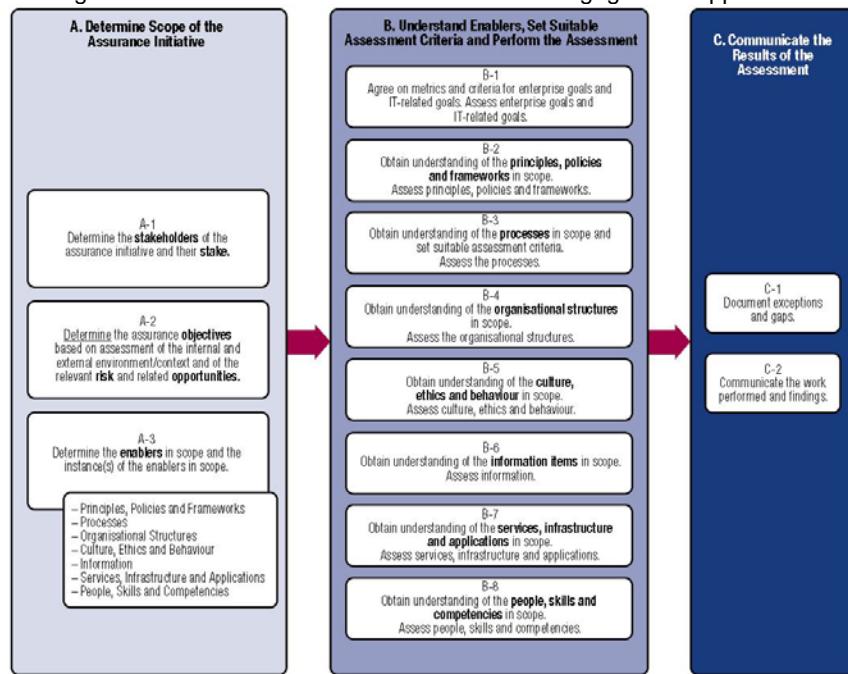
This review is considered highly technical. The IS audit and assurance professional must have an understanding of SAP best practice processes and requirements and be highly conversant in SAP tools, exposures and functionality. It should not be assumed that an audit and assurance professional holding the CISA designation has the requisite skills to perform this review.

Audit/Assurance Program Template

The assurance program table is a template for a detailed assurance work program, which is based on COBIT 5.

The assurance work program structures an assurance engagement into three major phases, as depicted in **figure 1**.

Figure 1—Generic COBIT 5-based Assurance Engagement Approach ¹



Assurance Engagement Approach Based on COBIT 5

As shown in **figure 1**, the proposed audit/assurance engagement approach refers explicitly to all COBIT 5 enabler categories. The COBIT 5 framework explains that the enablers are interconnected, e.g., Processes use Organisational Structures as well as Information items (inputs [I] and outputs [O]). When developing the audit/assurance program, it will become clear that when all possible entities of all enablers are included in the scope and reviewed in detail, there is potential for duplication.

In the development of this audit/assurance program, care has been taken to avoid or minimize duplication, meaning that:

- Some aspects of a process also relate to another enabler and are classified there, e.g., inputs and outputs can also be classified under the Information enabler heading and treated in detail there.
- Some aspects relating to Skills and Competencies are to a large extent covered by process APO07 *Manage human resources*.

In practice, assurance professionals will have to use their own professional judgment when developing their own customized audit/assurance programs, to avoid duplication of work.

In addition, while audit/assurance programs will be available for each process, in practice, a group of processes are often selected for audit. Therefore, a relevant set of audit/assurance programs of the applicable processes will need to be selected for conducting assurance.

¹ See www.isaca.org/COBIT/Pages/Assurance-product-page.aspx for more information on COBIT 5 for Assurance.

Generic Audit/Accurance Program

The assurance approach depicted in **figure 1** is described in more detail and developed into a **generic audit/assurance program**—including guidance on how to proceed during each step—in section 2B of *COBIT 5 for Assurance*. These *Audit/Assurance Programs* are:

- Fully aligned with COBIT 5:
 - It explicitly references all seven enablers. In other words, it is no longer exclusively process-focused; it also uses the different dimensions of the enabler model to cover all aspects contributing to the performance of the enablers.
 - It references the COBIT 5 goals cascade to ensure that detailed objectives of the assurance engagement can be put into the enterprise and IT context, and concurrently it enables linkage of the assurance objectives to enterprise and IT risk and benefits.
- Comprehensive yet flexible:
 - The generic program is comprehensive because it contains assurance steps covering all enablers in quite some detail, yet it is also flexible because this detailed structure allows clear and well-understood scoping decisions to be made. That is, the assurance professional can decide to not cover a set of enablers or some enabler instances and, while the decision will reduce the scope and related assurance engagement effort, the issue of what is or is not covered will be quite transparent to the assurance engagement user.
- Easy to understand, follow and apply because of its clear structure:
 - The table follows the flow described in the **figure 1**, but splits each phase into different steps and substeps.
 - For each step, a short description is included, as is guidance for the assurance professional on how to proceed with the step (text in italics).

Additional guidance on how to use other IT assurance-related standards for performing assurance can be found in section 3 of *COBIT 5 for Assurance*.

Customization of the Audit/Accurance Program

Customization and completion of the *SAP ERP Audit/Accurance Programs* will still be required, and consists of refining the scope by selecting goals and enabler instances—the lists included in the example are comprehensive, yet still are examples (i.e., different strategic priorities of the enterprise may dictate a different scope). The lists can also be considered prohibitive by some, as they can lead to a very broad scope, and therefore a very expensive assurance engagement; selection and prioritization will be required. The assurance professional will need to consider the following steps:

- Determine the stakeholders of the assurance initiative and their stake.
- Determine the assurance objectives based on assessment of the internal and external environment/context, including the strategic objectives, goals (figures 40 and 41 of *COBIT 5 for Assurance*) and priorities of the enterprise.
- Determine the **enablers** in scope and the instance(s) of the enablers in scope.

In each phase, one or two enabler examples are fully elaborated, to illustrate and demonstrate the suggested approach. The audit/assurance program phases for the other processes and other enablers in scope need to be detailed to the required level of detail.

Using the Assurance Program

The SAP ERP assurance topics are based on the generic audit/assurance program, and contain the following additional information:

- In the Guidance column, the shaded text is specific to the example and provides practical guidance, e.g., examples on which processes to include in scope, on which organizational structures to include in scope, on how to set assessment criteria for the different enablers, on how to actually assess the different enablers.
- Two additional columns, allowing the audit and assurance professional to identify and cross-reference issues and to record comments:
 - **Issue Cross-reference**—This column can be used to flag a finding/issue that the IT assurance professional wants to further investigate or establish as a potential finding. The potential findings should be documented in a work paper that indicates the disposition of the findings (formally reported, reported as a memo or verbal finding, or waived).
 - **Comment**—This column can be used to document any further notes.

For most of the enablers, there are several instances in scope. However, the assurance professional must complete the list to meet the environment in scope. The remaining instances can be deduced very similarly to those described in this program, using the COBIT 5 framework and the *COBIT 5: Enabling Processes* guides.

SAP ERP

Revenue Business Cycle
Audit/Assurance Program



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP ERP Revenue Business Cycle Audit/Assurance Program* (the ‘Work’) primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP’s kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: <http://www.isaca.org/sap-erp-4th-edition>

Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOfficial>

Like ISACA on Facebook: www.facebook.com/ISACAHQ

Acknowledgements

ISACA wishes to recognize

Project Leaders

Benjamin Fitts, CPA, Deloitte & Touche LLP, USA
Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA
Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA
Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Eva Sweet, CISA, CISM, ISACA, USA

Researchers

Syed Aamir Aarfi, Deloitte & Touche LLP, USA
Carlos Amaya, CISA, Deloitte & Touche LLP, USA
Dan Argynov, PMP, Deloitte & Touche LLP, USA
Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA
David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA
Ramamallikarjunaraao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA
Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA
Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA
Sagnik Mukherjee, Deloitte & Touche LLP, USA
Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA
Sonik Shah, Deloitte & Touche LLP, USA
Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA
Shweta Srivastava, Deloitte & Touche LLP, USA
Anurag Tewary, Deloitte & Touche LLP, USA
Percy Tsai, CPA, Deloitte & Touche LLP, USA
Ravi Maddela Veeriah, Deloitte & Touche LLP, USA
Sravan Vemana, Deloitte & Touche LLP, USA
Anukool Vyas, Deloitte & Touche LLP, USA

Expert Reviewers

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA
Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada
Mayank Garg, CISA, NetApp, USA
Ricci Leong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Jim Koveos, CISA, MBA, AmerisourceBergen, USA
Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia
Samuel Lim S.C., CISA, Auditor General's Office, Singapore
Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia
Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General's Office, Singapore
Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia
Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia
Paul O'Donnell, Ernst & Young, Canada
Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico
John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US
Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico
Naved Rehman, CISA, CRISC, MS-IS, SAPAuditCoach, US
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US
Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico
Jovari St. Victor, CISA, CPA, Sunera, LLC, US
Surapong Surabotsopon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,
KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico
Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand
David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President
Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cythus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK
Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil
Jotham Nyamari, CISA, Deloitte, USA
James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK
Gurvinder Singh, CISA, CISM, CRISC, Australia
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore
Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

SAP ERP Revenue Business Cycle Audit/Assurance Program

Introduction

This document contains an example audit/assurance program, **based on** the generic structure developed in section 2B of *COBIT 5 for Assurance*¹.

The engagement approach is based on, but **differs slightly** from the generic approach described in *COBIT 5 for Assurance*:

- The engagement approach described in this audit/assurance program is **focused on a business process** consequently no group of COBIT 5 processes dominates as primary processes and the lower-level processes are widespread, for evaluation purposes, the high-level COBIT 5 processes will be used as references.
- The assurance steps in this audit/assurance program are specific to the subject matter under review; therefore most of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources availableprocess audit/assurance program.

Assurance Engagement: SAP ERP Revenue Business Cycle

Assurance Topic

The topic covered by this assurance engagement is the SAP ERP Revenue Business Cycle.

Business Impact and Risk

SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical processes.

Risk resulting from ineffective or incorrect configurations or use of SAP could result in some of the following:

- Disclosure of privileged information
- Single points of failure
- Low data quality
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements

Goal of the Review

The objective of the SAP ERP audit/assurance review is to provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise's SAP ERP architecture.

Scoping

The review will focus on configuration of the relevant SAP ERP components and modules within the enterprise. The selection of the specific components and modules will be based upon the risk introduced to the enterprise by these components and modules.

From a process reference model (PRM) perspective, the following processes apply to this audit and assurance program:

- BAI02 *Manage requirements definition*
- BAI03 *Manage solution identification and build*
- DSS01 *Manage operations*
- DSS05 *Manage security services*
- DSS06 *Manage business process controls*

¹ See www.isaca.org/COBIT/Pages/Assurance-product-page.aspx for more information on *COBIT 5 for Assurance*.

Minimum Audit Skills

This review is considered highly technical. The IS audit and assurance professional must have an understanding of SAP best practice processes and requirements and be highly conversant in SAP tools, exposures and functionality. It should not be assumed that an audit and assurance professional holding the CISA designation has the requisite skills to perform this review.

Testing SAP Security

To determine which users have access to the relevant authorizations used in this audit program, use one of the following methods:

1. Use transaction code SUIM → Users → Users by Complex Selection Criteria
2. Use transaction code S_BCE_68001417
3. Use transaction code SA38 and the program RSUSR002. This method allows the user to specify a transaction code, a "valid to" date for users, and up to three other authorization objects (which also may be the authorization object for transaction code S_TCODE) with associated values (two values under an AND relationship and three values under an OR relationship).
This method is generally sufficient for testing logical access security in relation to SAP ERP application infrastructure areas, but it is less suitable when large numbers of authorizations must be reviewed, such as in segregation of duties analysis and in some of the more complex areas of business cycle controls.
4. Use transaction code SUIM → Users → Users with Critical Authorizations (also accessible with program RSUSR008_009_NEW, which replaces programs RSUSR008 and RSUSR009 and transaction codes SU98 and/or SU99, for SAP Web AS 6.20 and later). This method offers improvements such as allowing differentiation between SAP defaults for critical data for different business areas, extended combination options for critical authorization data, improved performance, display of user filters and more analysis options for users in the result list.

Audit/Accurance Program for SAP ERP Revenue Business Cycle						
Phase A—Determine Scope of the Assurance Initiative						
Ref.	Assurance Step	Guidance			Issue Cross-reference	Comment
A-1	Determine the stakeholders of the assurance initiative and their stakes .					
A-1.1	<u>Identify</u> the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	Intended user(s) of the assurance report	Board/audit committee: Needs assurance over the effectiveness and efficiency of SAP ERP processes within the enterprise. Chief financial officer (CFO): Needs assurance that internal controls for financial applications work as intended. Risk managers: Need assurance that controls intended to address previously identified risk are working as intended. The results from the audit should be used to update the risk registry as needed. Security managers: Need to identify gaps in the security plans for SAP applications. Owners / shareholders: Part or all of the SAP ERP assurance report may be included in statutory reporting. Regulators: Part or all of SAP ERP reporting may need to be disclosed to respective authorities			
A-1.2	<u>Identify</u> the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	Accountable and responsible parties for the subject matter	Business executives: The individuals responsible for identifying requirements, approving design and managing performance. These people are, together with IT management, responsible for managing the correct and controlled use of SAP ERP services—in line with good practices. Business process owners: Responsible for defining application and technical requirements. Responsible for data classification. IT management: Responsible for managing the correct and controlled use of SAP ERP services—together with the business executives.			
A-2	<u>Determine</u> the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities (i.e., not achieving the enterprise goals).		Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement. Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically. Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals. Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.			
A-2.1	<u>Understand</u> the enterprise strategy and priorities.	<i>Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.</i>				

Audit/Assurance Program for SAP ERP Revenue Business Cycle				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
A-2.2	<u>Understand</u> the internal context of the enterprise.	<p><i>Identify all internal environmental factors that could influence the performance and contents of the SAP ERP Revenue Business Cycle.</i></p> <ul style="list-style-type: none"> • Review prior report, if one exists, verify completion of any agreed-on corrections, and note remaining deficiencies. Determine whether: <ul style="list-style-type: none"> – Senior management has assigned responsibilities for information, its processing and its use – User management is responsible for providing information that supports the entity's objectives and policies – Information systems management is responsible for providing the capabilities necessary for the achievement of the defined information systems objectives and the policies of the entity – Senior management approves plans for development and acquisition of information systems – There are procedures to ensure that the information system being developed or acquired meets user requirements – There are procedures to ensure that information systems, programs and configuration changes are tested adequately prior to implementation – All personnel involved in the system acquisition and configuration activities receive adequate training and supervision – There are procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards – User management participates in the conversion of data from the existing system to the new system – Final approval is obtained from user management prior to going live with a new information/upgraded system – There are procedures to document and schedule all changes to information systems (including key ABAP programs) – There are procedures to ensure that only authorized changes are initiated – There are procedures to ensure that only authorized, tested and documented changes to information systems are accepted into the production client – There are procedures to allow for and control emergency changes – There are procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software – There is a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated – The organizational structure, established by senior management, provides for an appropriate segregation of incompatible functions – The database, application and presentation servers are located in a physically separate and protected environment (i.e., a data center) – Emergency, backup and recovery plans are documented and tested on a regular basis to ensure that they remain current and operational – Backup and recovery plans allow users of information systems to resume operations in the event of an interruption – Application controls are designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system – Access to the Implementation Guide (IMG) during production has been restricted – The production client settings have been flagged to not allow changes to programs and 		

Audit/Accurance Program for SAP ERP Revenue Business Cycle										
Phase A—Determine Scope of the Assurance Initiative										
Ref.	Assurance Step	Guidance			Issue Cross-reference	Comment				
		<p>configuration</p> <ul style="list-style-type: none"> • Identify the significant risk and determine the key controls <ul style="list-style-type: none"> - Develop a high-level process flow diagram and overall understanding of the Revenue Module, including the following subprocesses: <ul style="list-style-type: none"> a. Master data maintenance b. Sales order processing c. Invoice processing d. Collecting and processing cash receipts - Assess the key risk, determine key controls or control weaknesses, and test controls (refer to the sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> a. The controls culture of the organization (e.g., a just-enough-control philosophy). b. The need to exercise judgment to determine the key controls in the process and whether the controls structure is adequate. (Any weaknesses in the control structure should be reported to executive management and resolved.) • Gain an understanding of the SAP ERP environment (The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles) <p>In particular, the following information is important:</p> <ul style="list-style-type: none"> - Version and release of SAP ERP implemented - Total number of named users (for comparison with logical access security testing results) - Number of SAP instances and clients - Accounting period, company codes and chart of accounts - Identification of the components being used (Human Capital Management, Financials, Operations, Corporate Services) - Whether the organization has created any locally developed ABAP programs or reports - Details of the risk assessment approach taken in the organization to identify and prioritize risk - Copies of the organization's key security policies and standards <p>Obtain details of the following:</p> <ul style="list-style-type: none"> - Organizational Management Model as it relates to sales/revenue activity, i.e., sales organizational unit structure in SAP ERP and company sales organizational chart (required when evaluating the results of access security control testing) - An interview of the systems implementation team, if possible, and process design documentation for sales and distribution 								
A-2.3	<u>Understand the external context of the enterprise.</u>	<i>Identify all external environmental factors that could influence the performance and contents of the SAP ERP Revenue Business Cycle.</i>								
A-2.4	<u>Given the overall assurance objective, translate the identified strategic priorities into concrete objectives for the assurance engagement.</u>	<p>The following goals are retained as key goals to be supported, in reflection of enterprise strategy and priorities:</p> <table border="1"> <tr> <td>Key goals</td> <td>Enterprise goals:</td> </tr> <tr> <td></td> <td> <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability </td> </tr> </table>			Key goals	Enterprise goals:		<ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability 		
Key goals	Enterprise goals:									
	<ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability 									

Audit/Accurance Program for SAP ERP Revenue Business Cycle					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step		Guidance	Issue Cross-reference	Comment
			<ul style="list-style-type: none"> • EG11 Optimisation of business process functionality • EG15 Compliance with internal policies <p>IT-related goals:</p> <ul style="list-style-type: none"> • ITG01 Alignment of IT and business strategy • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG09 IT Agility • ITG10 Security of information, processing infrastructure and applications • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG15 IT compliance with internal policies • ITG16 Competent and motivated business and IT personnel 		
			Additional goals		
A-2.5	Define the organizational boundaries of the assurance initiative.		<p>The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment.</p> <ul style="list-style-type: none"> • Obtain information and form an understanding of the business reasons underlying the audit. • Identify the senior business resources responsible for the review. • Identify the senior IT audit/assurance resource responsible for the review. • Establish the process for suggesting and implementing changes to the audit/assurance program, and list the authorizations required. • Identify any limitations and/or constraints affecting the audit of specific systems and subsystems. • Identify any third-party services, applications, platforms and infrastructure elements that may not be or only partially be accessible. • Identify any legal, regulatory or contractual constraints on audit. • Identify any industrial relations-based or end user-based audit constraints. 		

Audit/Accurance Program for SAP ERP Revenue Business Cycle							
Phase A—Determine Scope of the Assurance Initiative							
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment		
A-3	Determine the enablers in scope and the instance(s) of the enablers in scope.	COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.					
A-3.1	Define the Principles, Policies and Frameworks in scope.	<p>Guiding principles and policies include:</p> <ul style="list-style-type: none"> • Policy for Master Data Maintenance • Information security management system (ISMS) policy • Legal and regulatory compliance requirements 					
A-3.2	Define which Processes are in scope of the review. Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of process goals • Application of process good practices • Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments) 	<i>COBIT 5: Enabling Processes</i> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed.					
		<table border="1"> <tr> <td>Key processes</td><td> <ul style="list-style-type: none"> • Master data maintenance • Sales order processing • Invoice processing • Collecting and processing cash receipts </td></tr> <tr> <td>Additional processes</td><td> <ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance </td></tr> </table>	Key processes	<ul style="list-style-type: none"> • Master data maintenance • Sales order processing • Invoice processing • Collecting and processing cash receipts 	Additional processes	<ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance 	
Key processes	<ul style="list-style-type: none"> • Master data maintenance • Sales order processing • Invoice processing • Collecting and processing cash receipts 						
Additional processes	<ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance 						
A-3.3	Define which Organisational Structures will be in scope. Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of Organisational Structure goals, i.e., decisions • Application of Organisational Structures good practices 	Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail.					
		<table border="1"> <tr> <td>Key Organisational Structures</td><td> <ul style="list-style-type: none"> • Sales and Use Tax department • Sales department • Accounts receivable • Credit • Warehouse • Shipping • Marketing and Pricing </td></tr> <tr> <td>Additional Organisational Structures</td><td> <ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office </td></tr> </table>	Key Organisational Structures	<ul style="list-style-type: none"> • Sales and Use Tax department • Sales department • Accounts receivable • Credit • Warehouse • Shipping • Marketing and Pricing 	Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office 	
Key Organisational Structures	<ul style="list-style-type: none"> • Sales and Use Tax department • Sales department • Accounts receivable • Credit • Warehouse • Shipping • Marketing and Pricing 						
Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office 						

Audit/Accurance Program for SAP ERP Revenue Business Cycle								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
A-3.4	<u>Define the Culture, Ethics and Behaviour aspects in scope.</u>	<p>In the context of this engagement, the following enterprise-wide culture and behaviours are in scope:</p> <ul style="list-style-type: none"> • Risk- and compliance-aware culture • Enabling of continuous improvement • Accountability • Discipline to follow instructions 						
A-3.5	<u>Define the Information items in scope.</u> Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of Information goals, i.e., quality criteria of the information items • Application of Information good practices (Information attributes) 	<p>Based on the subject matter of this audit/assurance program, the following Information items have been identified as key items.</p> <table border="1"> <tr> <td>Key Information Items</td> <td> <ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids </td> </tr> <tr> <td>Additional Information Items</td> <td> <ul style="list-style-type: none"> • Organizational charts </td> </tr> </table>	Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 	Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 		
Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 							
Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 							
A-3.6	<u>Define the Services, Infrastructure and Applications in scope.</u>	<p>Based on the subject matter of this audit/assurance program, the following services and related applications or infrastructure could be considered in scope of the review:</p> <ul style="list-style-type: none"> • Master data maintenance group • SAP ERP System • Change management • SAP training 						
A-3.7	<u>Define the People, Skills and Competencies in scope.</u> Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of skills set goals • Application of skills set and competencies good practices 	<p>In the context of this engagement, taking into account key processes and key roles, the following skill sets are included in scope:</p> <ul style="list-style-type: none"> • Proficiency using SAP Sales and Distribution, Treasury (Cash Applications), Accounts Receivable, and Credit Modules • Master data management skills • Order to Cash process skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 						

Audit/Accuracy Program for SAP ERP Revenue Business Cycle																											
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment																						
B-1	Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.																										
B-1.1	<p><u>Obtain</u> (and <u>agree on</u>) metrics for enterprise goals and expected values of the metrics. <u>Assess</u> whether enterprise goals in scope are achieved.</p> <p>Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.</p> <p>Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</p> <p>The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>Enterprise Goal</th><th>Metric</th><th>Expected Outcome (Ex)</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>EG03 Managed business risk (safeguarding of assets)</td><td> <ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG04 Compliance with externals laws and regulations</td><td> <ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG07 Business service continuity and availability</td><td> <ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG11 Optimisation of business process functionality</td><td> <ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG15 Compliance with internal policies</td><td> <ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>	Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step	EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG04 Compliance with externals laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG04 Compliance with externals laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
B-1.2	<p><u>Obtain</u> (and <u>agree on</u>) metrics for IT-related goals and expected values of the metrics and <u>assess</u> whether IT-related goals in scope are achieved.</p> <p>The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>IT-related Goal</th><th>Metric</th><th>Expected Outcome (Ex)</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>ITG01 Alignment of IT and business strategy</td><td> <ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services </td><td>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>	IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step	ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																		
IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								

Audit/Accurance Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> Percent of IT value drivers mapped to business value drivers 		criteria are achieved.	
	ITG02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment Number of non-compliance issues relating to contractual agreements with IT service providers Coverage of compliance assessments 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG04 Managed IT-related business risk	<ul style="list-style-type: none"> Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent of enterprise risk assessments including IT-related risk Frequency of update of risk profile 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG08 Adequate use of applications, information and technology solutions	<ul style="list-style-type: none"> Percent of business process owners satisfied with supporting IT products and services Level of business user understanding of how technology solutions support their processes Satisfaction level of business users with training and user manuals Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG09 IT Agility	<ul style="list-style-type: none"> Level of satisfaction of business executives with IT's responsiveness to new requirements Number of critical business processes supported by up-to-date infrastructure and applications Average time to turn strategic IT objectives into an agreed-on and approved initiative 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG10 Security of information, processing infrastructure and applications	<ul style="list-style-type: none"> Number of security incidents causing financial loss, business disruption or public embarrassment Number of IT services with outstanding security requirements Time to grant, change and remove access privileges, compared to agreed-on service levels 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	

Audit/Accurance Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	ITG12 Enablement and support of business processes by integrating applications and technology into business processes	<ul style="list-style-type: none"> Frequency of security assessment against latest standards and guidelines Number of business processing incidents caused by technology integration errors Number of business process changes that need to be delayed or reworked because of technology integration issues Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues Number of applications or critical infrastructures operating in silos and not integrated 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG14 Availability of reliable and useful information for decision making	<ul style="list-style-type: none"> Level of business user satisfaction with quality and timeliness (or availability) of management information Number of business process incidents caused by non-availability of information Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG15 IT compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices Frequency of policies review and update 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG16 Competent and motivated business and IT personnel	<ul style="list-style-type: none"> Percent of staff whose IT-related skills are sufficient for the competency required for their role Percent of staff satisfied with their IT-related roles Number of learning/training hours per staff member 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	

Audit/Accuracy Program for SAP ERP Revenue Business Cycle																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks																	
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment														
B-2	Obtain an understanding of the Principles, Policies and Frameworks in scope and set suitable assessment criteria. Assess Principles, Policies and Frameworks.																
Principles, policies and frameworks: Policy for Master Data Maintenance																	
B-2.1a	Understand the Principles, Policies and Frameworks context. <i>Obtain and understand of the overall system of internal control and the associated Principles, Policies and Frameworks.</i>																
B-2.2a	Understand the stakeholders of the Principles, Policies and Frameworks . <i>Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.</i>																
B-2.3a	<p>Understand the goals for the Principles, Policies and Frameworks, and the related metrics and agree on expected values. Assess whether the Principles, Policies and Frameworks goals (outcomes) are achieved, i.e., assess the effectiveness of the Principles, Policies and Frameworks.</p> <table border="1"> <thead> <tr> <th>Goal</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Comprehensiveness</td> <td>The set of policies is comprehensive in its coverage.</td> <td>Verify that the set of policies is comprehensive in its coverage.</td> </tr> <tr> <td>Currency</td> <td>The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update </td> <td>Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update </td> </tr> <tr> <td>Flexibility</td> <td>The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.</td> <td>Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.</td> </tr> <tr> <td>Availability</td> <td> <ul style="list-style-type: none"> Policies are available to all stakeholders. Policies are easy to navigate and have a logical and hierarchical structure. </td> <td> <ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. </td> </tr> </tbody> </table>	Goal	Criteria	Assessment Step	Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.	Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 	Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 	Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.	Availability	<ul style="list-style-type: none"> Policies are available to all stakeholders. Policies are easy to navigate and have a logical and hierarchical structure. 	<ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. 	
Goal	Criteria	Assessment Step															
Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.															
Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 	Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 															
Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.															
Availability	<ul style="list-style-type: none"> Policies are available to all stakeholders. Policies are easy to navigate and have a logical and hierarchical structure. 	<ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. 															
B-2.4a	<p>Understand the life cycle stages of the Principles, Policies and Frameworks, and agree on the relevant criteria. Assess to what extent the Principles, Policies and Frameworks life cycle is managed. <i>The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01 Manage the IT management framework.</i></p>																
B-2.5a	<p>Understand good practices related to the Principles, Policies and Frameworks and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. <i>The assurance professional will, by using appropriate auditing techniques assess the following aspects.</i></p> <table border="1"> <thead> <tr> <th>Good Practice</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Scope and validity</td> <td>The scope is described and the validity date is indicated.</td> <td>Verify that the scope of the framework is described and the validity date is indicated.</td> </tr> <tr> <td>Exception and escalation</td> <td> <ul style="list-style-type: none"> The exception and escalation procedure is explained and commonly known. The exception and escalation procedure has not become the de facto standard procedure. </td> <td> <ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. Through observation of a representative sample, verify that the exception and escalation procedure has not become de facto standard procedure. </td> </tr> <tr> <td>Compliance</td> <td>The compliance checking mechanism and non-</td> <td>Verify that the compliance checking mechanism and non-compliance</td> </tr> </tbody> </table>	Good Practice	Criteria	Assessment Step	Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.	Exception and escalation	<ul style="list-style-type: none"> The exception and escalation procedure is explained and commonly known. The exception and escalation procedure has not become the de facto standard procedure. 	<ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. Through observation of a representative sample, verify that the exception and escalation procedure has not become de facto standard procedure. 	Compliance	The compliance checking mechanism and non-	Verify that the compliance checking mechanism and non-compliance				
Good Practice	Criteria	Assessment Step															
Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.															
Exception and escalation	<ul style="list-style-type: none"> The exception and escalation procedure is explained and commonly known. The exception and escalation procedure has not become the de facto standard procedure. 	<ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. Through observation of a representative sample, verify that the exception and escalation procedure has not become de facto standard procedure. 															
Compliance	The compliance checking mechanism and non-	Verify that the compliance checking mechanism and non-compliance															

Audit/Assurance Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		compliance consequences are clearly described and enforced.	consequences are clearly described and enforced.		
B-2.1 to B-2.5	Repeat steps B-2.1 through B-2.5 for all remaining Principles, Policies and Frameworks in scope. Repeat the steps described above for the remaining Principles, Policies and Frameworks: • ISMS policy • Legal and regulatory compliance requirements				

Audit/Accurance Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3	Obtain understanding of the Processes in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes.				
SAP ERP Revenue process²: Master data maintenance					
B-3.1a	<u>Understand the Process context.</u>				
B-3.2a	<u>Understand the Process purpose.</u>				
B-3.3a	<u>Understand all process stakeholders</u> and their roles. This is equivalent to understanding the real RACI chart of the process. <i>Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.</i>				
	The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement:				
Master data maintenance stakeholders					
B-3.4a	<u>Understand the Process goals</u> and related <u>metrics³</u> and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.				
The Process Master data maintenance has four defined process goal.				The following activities can be performed to assess whether the goals are achieved.	
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	Issue Cross-reference	Comment
Master data records are valid, complete, accurate and timely.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
Master data remains current and pertinent.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
Access to master data changes is properly maintained.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
Changes to master data are properly authorized.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
B-3.5a	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement: <u>Define</u> and <u>agree</u> on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.) <u>Agree</u> on the process practices that should be in place (process design). <u>Assess</u> the process design , i.e., assess to what extent:				

² Because this is a business process audit/assurance program, several of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources available.

³ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

Audit/Accrual Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
<ul style="list-style-type: none"> • Expected process practices are applied. • Accountability and responsibility are assigned and assumed. COBIT 5 Processes ⁴ are described in <i>COBIT 5: Enabling Processes</i> . Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are: <ul style="list-style-type: none"> • A sound process design • The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented. 		Each practice is typically implemented through a number of activities, and a well-designed process will implement all these practices and activities.			
Reference Process	Master data maintenance	Criteria: 1.1 Changes made to master data are valid, complete, accurate and timely. 1.2 Master data remain current and pertinent. 1.3 Access to master data changes is properly maintained. 1.4 Changes to master data are properly authorized.			
Reference Process Practices ⁵	Good Practice	Assessment Step	Issue Cross-reference	Comment	
DSS01 DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.1 Use standard reports and transactions to assess the accuracy and completeness of changes applied to master data records against authorized source documents on a sample basis. Request evidence that management compares periodically reports detailing changes to master data to authorized source documents to assess accuracy, validity and completeness.			
DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.2 Determine whether the configurable control settings address the risk pertaining to the validity, completeness and accuracy of master data, and whether they have been set in accordance with management's intentions. View the settings online using the implementation guide (IMG) as follows: <ul style="list-style-type: none"> • Customer account groups—Use transaction code SPRO to display the IMG menu and follow path: Financial Accounting → Accounts Receivable and Accounts Payable → Customer Accounts → Master Data → Preparation for Creating Customer Master Data → Define Account Groups With Screen Layout (Customers) • Material types— Use transaction code SPRO to display the IMG menu and follow path: Logistics - General → Material Master → Basic Settings → Material Types → Define Attributes of Material Types • Industry sector— Use transaction code SPRO to display the IMG menu and follow path: Logistics - General → Material Master → Field Selection → Define Industry Sectors and Industry Sector-specific Field Selection (transaction code OMS3—Configure Industry Sectors) • Pricing—When reviewing pricing, be aware of three main configuration scenarios: 			

⁴ For this audit/accrual program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the SAP ERP Revenue Business Cycle processes in scope.

⁵ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Revenue Business Cycle audit/accrual program.

Audit/Accuracy Program for SAP ERP Revenue Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes				
Ref.	Assurance Steps and Guidance		Issue Cross-reference	Comment
		<ul style="list-style-type: none"> – Pricing may be coded into condition records in the system, and manual override may not be possible. – Pricing may be coded into the system; however, the system may be configured to allow the user to override the price at the time of order entry. – The system may be configured to allow the user to enter the price at the time of order entry, with price listings or schedules manually maintained. <p>Review of pricing condition types and records against the organization's pricing policy using the following menu path and transaction codes:</p> <ul style="list-style-type: none"> • Use transaction code SPRO to display the IMG menu and follow path: Sales and Distribution → Basic Functions →Pricing • V-44 (Display Material Price) for material price condition records • V-48 (Display Price List) for price list type condition records • V-52 (Display Customer Price) for customer-specific condition type <p>Review of manual (e.g., spot-checking, review of customer pricing complaints) or automated (e.g., release approval) supervisor controls over user price overrides. However, due to the complexity of pricing configuration, it is often most effective to take a sample of sales orders (e.g., using transaction code VA05—List of Sales Orders and reperform the pricing calculations outside the system using the organization's pricing policy as the basis for the calculations). Any anomalies can then be followed up with the users in the case of manual overrides or against the pricing configuration. To review a highly complex pricing scenario, you can use the pricing determination analysis on the Conditions tab of sales order line items to review what pricing is effective for a given line item.</p>		
DSS01 DSS06	Master data remains current and pertinent.	<p>1.2.1 Use standard reports and transactions on a sample basis to assess the timeliness of changes applied to master data records against authorized source documents.</p> <p>Determine whether master data maintenance reports are prepared and reviewed periodically by management for completeness and accuracy (Note: SAP does not provide a standard report to list all Customer Master Records. The enterprise should configure a report for audit purposes. Customer Master Data can be viewed using transaction Code SE16—Data Browser to view tables KNA1, KNB1, KNVV; however, this may be time consuming and yield inaccurate results).</p> <p>Master data types that should be part of this review are:</p> <ul style="list-style-type: none"> • Customer master list—Run transaction code F.20—A/R: Account List. • Material master list—Run transaction code MM03—Display Material & • Pricing master list by condition type—Run transaction code VK13—Display Condition. <p>Request a sample of master data create/change request forms and validate completeness and accuracy using transactions VD03—Display Customer or VD04—Customer Changes (transactions FD03, FD04 can be used to display the finance view and transactions XD03 and XD04 can be used to display the central view).</p> <p>Test master data as follows:</p> <p>Customer Use transaction code OV51 Display of Changes for Customer (also accessible using</p>		

Audit/Accuracy Program for SAP ERP Revenue Business Cycle																																																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																
Ref.	Assurance Steps and Guidance			Issue Cross-reference																																												
				Comment																																												
		<p>transaction code SA38 and program RFDABL00) to generate a list denoting the date and time of change, old and new values for fields and details of the user who input the change for comparison to authorized source documents.</p> <p>Use transaction code S_ALR_87009993 Display Changes to Credit Management (also accessible using transaction code SA38 and program RFDKLIAB) to display changes to credit management and credit information change details for comparison to authorized source documents.</p> <p>Material</p> <p>Use transaction code MM04 Display Material Change Documents to display changes for individual material records for comparison to authorized source documents.</p> <p>Pricing</p> <p>Generate a list of pricing changes using transaction code VK12 Change Condition and subsequently selecting the following path from menu options: Environment → Changes→ Change Report. Check the accuracy of changes made to the pricing master data records and also the time at which these changes have been applied (which is essential to the effective processing of pricing changes) for comparison to authorized source documents.</p>																																														
DSS05 DSS06	Access to master data changes is properly maintained.	<p>1.3.1 Review organizational policy and process design specifications regarding access to maintain master data.</p> <p>Use transaction code SUIM—User Information System to test user access to create and maintain customer, material and pricing master data as follows:</p> <p>Customer Master Data</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>(Finance view) FD01—Create customer</td> <td>B_BUPA_RLT</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>F_KNA1_APP</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>F_KNA1_BED</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>F_KNA1_BUK</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>F_KNA1_GEN</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>F_KNA1_GRP</td> <td>ACTVT</td> <td>01</td> </tr> </tbody> </table> <p>Also test user access to transaction codes FD02 Change Customer, FD05 Block Customer and FD06 Mark Customer for Deletion with the authorization objects used for FD01 above, but with ACTVT field values of 02, 05, and 06.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>(Sales view) VD01—Create customer</td> <td>B_BUPA_RLT</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>B_BUPR_BZT</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>F_KNA1_APP</td> <td>ACTVT</td> <td>01</td> </tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	(Finance view) FD01—Create customer	B_BUPA_RLT	ACTVT	01		F_KNA1_APP	ACTVT	01		F_KNA1_BED	ACTVT	01		F_KNA1_BUK	ACTVT	01		F_KNA1_GEN	ACTVT	01		F_KNA1_GRP	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values	(Sales view) VD01—Create customer	B_BUPA_RLT	ACTVT	01		B_BUPR_BZT	ACTVT	01		F_KNA1_APP	ACTVT	01		
Transaction(s)	Authorization Objects	Fields	Values																																													
(Finance view) FD01—Create customer	B_BUPA_RLT	ACTVT	01																																													
	F_KNA1_APP	ACTVT	01																																													
	F_KNA1_BED	ACTVT	01																																													
	F_KNA1_BUK	ACTVT	01																																													
	F_KNA1_GEN	ACTVT	01																																													
	F_KNA1_GRP	ACTVT	01																																													
Transaction(s)	Authorization Objects	Fields	Values																																													
(Sales view) VD01—Create customer	B_BUPA_RLT	ACTVT	01																																													
	B_BUPR_BZT	ACTVT	01																																													
	F_KNA1_APP	ACTVT	01																																													

Audit/Accuracy Program for SAP ERP Revenue Business Cycle																																																																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																																	
Ref.	Assurance Steps and Guidance					Issue Cross-reference																																																											
						Comment																																																											
				<table border="1"> <tr><td>F_KNA1_BED</td><td>ACTVT</td><td>01</td></tr> <tr><td>F_KNA1_GEN</td><td>ACTVT</td><td>01</td></tr> <tr><td>F_KNA1_GRP</td><td>ACTVT</td><td>01</td></tr> <tr><td>V_KNA1_BRG</td><td>ACTVT</td><td>01</td></tr> <tr><td>V_KNA1_VKO</td><td>ACTVT</td><td>01</td></tr> </table> <p>Also test user access to transaction codes VD02 Change Customer, VD05 Block customer and VD06 Mark customer for deletion with the authorization objects used for XD01 above, but with ACTVT field values of 02, 05 and 06, respectively.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr><td>(Central view) XD01—Create customer</td><td>B_BUPA_RLT</td><td>ACTVT</td><td>01</td></tr> <tr><td></td><td>B_BUPR_BZT</td><td>ACTVT</td><td>01</td></tr> <tr><td></td><td>F_KNA1_APP</td><td>ACTVT</td><td>01</td></tr> <tr><td></td><td>F_KNA1_BED</td><td>ACTVT</td><td>01</td></tr> <tr><td></td><td>F_KNA1_BUK</td><td>ACTVT</td><td>01</td></tr> <tr><td></td><td>F_KNA1_GEN</td><td>ACTVT</td><td>01</td></tr> <tr><td></td><td>F_KNA1_GRP</td><td>ACTVT</td><td>01</td></tr> <tr><td></td><td>V_KNA1_BRG</td><td>ACTVT</td><td>01</td></tr> <tr><td></td><td>V_KNA1_VKO</td><td>ACTVT</td><td>01</td></tr> </tbody> </table> <p>Also test user access to transaction codes XD02 Change Customer, XD05 Block customer, XD06 Mark customer for deletion and XD07 Change Customer Account Group with the authorization objects used for XD01 above, but with ACTVT field values of 02, 05, 06 and 07 respectively.</p> <p>Use transaction code SUIM—User Information System to test user access to transaction code XD99—Customer Master Mass Maintenance by evaluating access to the transaction code (there are no required authorization objects for this transaction code).</p> <p>Test for access to create or amend customer master data by company code by including the following authorization object/value combination in the search criteria.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> </table>	F_KNA1_BED	ACTVT	01	F_KNA1_GEN	ACTVT	01	F_KNA1_GRP	ACTVT	01	V_KNA1_BRG	ACTVT	01	V_KNA1_VKO	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values	(Central view) XD01—Create customer	B_BUPA_RLT	ACTVT	01		B_BUPR_BZT	ACTVT	01		F_KNA1_APP	ACTVT	01		F_KNA1_BED	ACTVT	01		F_KNA1_BUK	ACTVT	01		F_KNA1_GEN	ACTVT	01		F_KNA1_GRP	ACTVT	01		V_KNA1_BRG	ACTVT	01		V_KNA1_VKO	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values		
F_KNA1_BED	ACTVT	01																																																															
F_KNA1_GEN	ACTVT	01																																																															
F_KNA1_GRP	ACTVT	01																																																															
V_KNA1_BRG	ACTVT	01																																																															
V_KNA1_VKO	ACTVT	01																																																															
Transaction(s)	Authorization Objects	Fields	Values																																																														
(Central view) XD01—Create customer	B_BUPA_RLT	ACTVT	01																																																														
	B_BUPR_BZT	ACTVT	01																																																														
	F_KNA1_APP	ACTVT	01																																																														
	F_KNA1_BED	ACTVT	01																																																														
	F_KNA1_BUK	ACTVT	01																																																														
	F_KNA1_GEN	ACTVT	01																																																														
	F_KNA1_GRP	ACTVT	01																																																														
	V_KNA1_BRG	ACTVT	01																																																														
	V_KNA1_VKO	ACTVT	01																																																														
Transaction(s)	Authorization Objects	Fields	Values																																																														

Audit/Accuracy Program for SAP ERP Revenue Business Cycle																																																									
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																									
Ref.	Assurance Steps and Guidance					Issue Cross-reference	Comment																																																		
		<p>FD01—Create Customer (FI) VD01—Create Customer (SD) XD01—Create Customer (Central) XD99—Customer Master Mass Maintenance</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="4">FD32—Change Customer Credit Management</td><td>F_BKPF_BUK</td><td>ACTVT</td><td>02</td></tr> <tr> <td>F_KNA1_BUK</td><td>ACTVT</td><td>02</td></tr> <tr> <td>F_KNA1_KKB</td><td>ACTVT</td><td>02</td></tr> <tr> <td>F_KNA1_MAN</td><td>ACTVT</td><td>02</td></tr> </tbody> </table> <p>Use transaction code SUIM—User Information System to test user access to transaction code FD32—Change Customer Credit Management as follows.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="2">MM01—Create Material Master</td><td>M_MATE_MAR</td><td>ACTVT</td><td>01</td></tr> <tr> <td>M_MATE_STA</td><td>ACTVT</td><td>01</td></tr> </tbody> </table> <p>Also test user access to transaction codes MM02 Change Material and MM06 Flag Material for Deletion with the same authorization objects as above, but with ACTVT field values of 02 and 06, respectively.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="2">VK11—Create Condition</td><td>V_KONH_VKS</td><td>ACTVT</td><td>01</td></tr> <tr> <td>V_KONH_VKO</td><td>ACTVT</td><td>01</td></tr> </tbody> </table> <p>Also test user access to transaction code VK12 Change Condition with the authorization objects used for VK11 above, but with ACTVT field value of 02.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="2">BP—Create Business Partner</td><td>B_BUPA_ATT</td><td>ACTVT</td><td>01, 02, 03</td></tr> <tr> <td>B_BUPA_FDG</td><td>ACTVT</td><td>02, 03</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	FD32—Change Customer Credit Management	F_BKPF_BUK	ACTVT	02	F_KNA1_BUK	ACTVT	02	F_KNA1_KKB	ACTVT	02	F_KNA1_MAN	ACTVT	02	Transaction(s)	Authorization Objects	Fields	Values	MM01—Create Material Master	M_MATE_MAR	ACTVT	01	M_MATE_STA	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values	VK11—Create Condition	V_KONH_VKS	ACTVT	01	V_KONH_VKO	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values	BP—Create Business Partner	B_BUPA_ATT	ACTVT	01, 02, 03	B_BUPA_FDG	ACTVT	02, 03					
Transaction(s)	Authorization Objects	Fields	Values																																																						
FD32—Change Customer Credit Management	F_BKPF_BUK	ACTVT	02																																																						
	F_KNA1_BUK	ACTVT	02																																																						
	F_KNA1_KKB	ACTVT	02																																																						
	F_KNA1_MAN	ACTVT	02																																																						
Transaction(s)	Authorization Objects	Fields	Values																																																						
MM01—Create Material Master	M_MATE_MAR	ACTVT	01																																																						
	M_MATE_STA	ACTVT	01																																																						
Transaction(s)	Authorization Objects	Fields	Values																																																						
VK11—Create Condition	V_KONH_VKS	ACTVT	01																																																						
	V_KONH_VKO	ACTVT	01																																																						
Transaction(s)	Authorization Objects	Fields	Values																																																						
BP—Create Business Partner	B_BUPA_ATT	ACTVT	01, 02, 03																																																						
	B_BUPA_FDG	ACTVT	02, 03																																																						

Audit/Accurance Program for SAP ERP Revenue Business Cycle												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes												
Ref.	Assurance Steps and Guidance							Issue Cross-reference	Comment			
					B_BUPA_GRP	ACTVT	01, 02, 03					
					B_BUPA_RLT	ACTVT	01, 02, 03					
					B_BUPR_BZT	ACTVT	01, 02, 05					
					B_BUPR_FDG	ACTVT	01, 02, 03, 06					
					B_CCARD	ACTVT	01, 02, 03					
					B_USERSTAT	ACTVT	01, 06					
BAI06	Changes to master data are properly authorized.	1.4.1 The auditor should verify the validity of customers shipping addresses to determine whether: (a) The same shipping address is used by different customers, and (b) There is a match between the shipping address and employee address to detect fraud activities.										
DSS01 DSS06	Changes to master data are properly authorized.	1.4.2 Request evidence that management compares periodically reports detailing changes to master data to authorized source documents to assess accuracy, validity and completeness. Take a sample of source documents for evidence of comparison to inventory file updates. Confirm that management executes transaction code MM04—Display Material Change Documents and compares against source documents for a sample of changes that have been performed. Determine whether management regularly reviews master data for duplicate customers or materials via manual or automated methods. Consider obtaining an extract of key customer or materials master data tables (KNA1, MARA), and search for duplicates based on likely unique fields (postal or ZIP code, material name, weight or dimensions, etc.). Use transaction code F.32—Credit Management—Missing Data to provide an overview of customers for whom no credit information has been entered. Understand the number ranges used for customers and which customers should have a credit limit assigned. Check the output from transaction code F.32 to confirm that a credit limit has been set for customers in the range requiring a limit. Obtain the credit change report and verify that the changes have been approved by authorized personnel.										
DSS06	Changes to master data are properly authorized.	1.4.3 Review organizational policy and process design specifications regarding access to unlock customer master records.										
B-3.6a	Agree on the process work products ⁶ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.											
	Process Master data maintenance inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.				Criteria: All listed work products should demonstrably exist and be used.							
	Process Practice	Work Products			Assessment Step							
	Master data maintenance	• Master data add/change/delete request forms			Apply appropriate audit techniques to determine the							

⁶ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	<ul style="list-style-type: none"> • Master data maintenance procedures • Master data maintenance reports • List of SAP users with master data access 		existence and appropriate use of each work product.		
B-3.7a	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				
SAP ERP Revenue process: Sales order processing					
B-3.1b	Understand the Process context .				
B-3.2b	Understand the Process purpose .				
B-3.3b	Understand all process stakeholders and their roles.				
B-3.4b	Sales order processing stakeholders: Understand the Process goals and related metrics ⁷ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.				
	The Process Sales order processing has three defined process goals.		The following activities can be performed to assess whether the goals are achieved.		
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	
	Sales orders are processed with valid prices and terms, and processing is complete, accurate and timely.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Sales orders are processed within approved customer credit limits.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
B-3.5b	Order entry data is completely and accurately transferred to the shipping and invoicing activities.				
	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement				
	Reference Process	Sales order processing	Criteria: 2.1 Sales orders are processed with valid prices and terms, and processing is complete, accurate and timely. 2.2 Sales orders are processed within approved customer credit limits. 2.3 Order entry data is completely and accurately transferred to the shipping and invoicing activities.		
	Reference Process Practices ⁸	Good Practice	Assessment Step		Issue Cross-reference
	DSS05 DSS06	Sales orders are processed with valid prices and terms, and	2.1.1 Gain an understanding of the organization's policies, procedures, standards and guidance related to the ability to create, change, delete, block and unblock sales orders, contracts		

⁷ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

⁸ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Revenue Business Cycle audit/assurance program.

Audit/Accrual Program for SAP ERP Revenue Business Cycle																																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																	
Ref.	Assurance Steps and Guidance			Issue Cross-reference																													
				Comment																													
	processing is complete, accurate and timely.	<p>and delivery schedules.</p> <p>Use transaction code SUIM—User Information System to test user access to create, maintain, block and unblock sales orders, contracts and delivery schedules, and compare the results against the understanding of the business process and controls obtained earlier. The following are some examples of transactions to include in the testing (note that data can be maintained through finance or sales views):</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="2">(Sales view) VA01—Create Sales Orders</td><td>V_VBAK_AAT</td><td>ACTVT</td><td>01, 02, 05, 06, 43 (Release)</td></tr> <tr> <td>V_VBAK_VKO</td><td>ACTVT</td><td>01, 02, 05, 06, 43 (Release)</td></tr> <tr> <td colspan="4">Also test user access to transaction code VA02 Change Sales Order with the same authorization objects and field values 02, 05, 06 and 43. Value 01 is not valid for this transaction.</td><td></td></tr> <tr> <td rowspan="4">(Finance view) FB75—Enter Outgoing Credit Memos</td><td>F_BKPF_BLA</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td>F_BKPF_BUK</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td>F_BKPF_GSB</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td>F_BKPF_KOA</td><td>ACTVT</td><td>01, 02</td></tr> </tbody> </table> <p>Depending on the volume of sales input manually, it may also be necessary to verify a sample of sales input for accuracy.</p>	Transaction(s)	Authorization Objects	Fields	Values	(Sales view) VA01—Create Sales Orders	V_VBAK_AAT	ACTVT	01, 02, 05, 06, 43 (Release)	V_VBAK_VKO	ACTVT	01, 02, 05, 06, 43 (Release)	Also test user access to transaction code VA02 Change Sales Order with the same authorization objects and field values 02, 05, 06 and 43. Value 01 is not valid for this transaction.					(Finance view) FB75—Enter Outgoing Credit Memos	F_BKPF_BLA	ACTVT	01, 02	F_BKPF_BUK	ACTVT	01, 02	F_BKPF_GSB	ACTVT	01, 02	F_BKPF_KOA	ACTVT	01, 02		
Transaction(s)	Authorization Objects	Fields	Values																														
(Sales view) VA01—Create Sales Orders	V_VBAK_AAT	ACTVT	01, 02, 05, 06, 43 (Release)																														
	V_VBAK_VKO	ACTVT	01, 02, 05, 06, 43 (Release)																														
Also test user access to transaction code VA02 Change Sales Order with the same authorization objects and field values 02, 05, 06 and 43. Value 01 is not valid for this transaction.																																	
(Finance view) FB75—Enter Outgoing Credit Memos	F_BKPF_BLA	ACTVT	01, 02																														
	F_BKPF_BUK	ACTVT	01, 02																														
	F_BKPF_GSB	ACTVT	01, 02																														
	F_BKPF_KOA	ACTVT	01, 02																														
DSS05 DSS06	Sales orders are processed with valid prices and terms, and processing is complete, accurate and timely.	2.1.2 Use transaction code SUIM—User Information System to test user access to create and maintain sales pricing information and credit limits. Refer to testing technique 1.1.3. Obtain the credit change report and verify that the changes have been approved by authorized personnel.																															
DSS06	Sales orders are processed with valid prices and terms, and processing is complete, accurate and timely.	2.1.3 Review configuration options for pricing in the IMG according to testing technique 1.1.2 for master data maintenance.																															
DSS01 DSS06	Sales orders are processed with valid prices and terms, and processing is complete, accurate and timely.	2.1.4 Gain an understanding of the policies and procedures regarding reconciliation of sales orders. Review operations activity at selected times and check for evidence that reconciliations are being performed.																															
DSS06	Sales orders are processed within approved customer credit limits.	2.2.1 Determine whether the configurable control settings address the risk pertaining to the processing of orders outside customer credit limits and whether they have been set in accordance with management intentions. View the settings online using the IMG as follows: <ul style="list-style-type: none">• Use transaction code SPRO to display the IMG menu and follow path: Financial																															

Audit/Accrual Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.6a		Accounting → Accounts Receivable and Accounts Payable → Credit Management → Credit Control Account. <ul style="list-style-type: none"> • Execute transaction code OVAK—Sales Order Type Assignment to show the type of credit check performed for the corresponding transaction types in order processing. • Execute transaction code OVA7—Credit Relevancy of Items Category to determine whether a credit check is performed for appropriate document types being used. • Execute transaction code OVAD—Delivery Type Assignment to show the credit groups that have been assigned to the delivery types being used. • Execute transaction code OVA8—Automatic Credit Check to show an overview of defined credit checks for CCAs. 			
	DSS01 MEA01	Order entry data is completely and accurately transferred to the shipping and invoicing activities.	2.3.1 Obtain a full list of incomplete sales documents from the system using transaction code V.00—List of Incomplete Documents (also accessible using transaction code SA38—ABAP Reporting and program RVAUFERR). Review items on the list with the appropriate operational management and ascertain whether there are legitimate reasons for the sales documents to remain incomplete.		
	DSS01 MEA01	Order entry data is completely and accurately transferred to the shipping and invoicing activities.	2.3.2 Obtain a full list of sales orders with delivery blocks from the system using transaction code V.14—Sales Orders Blocked for Delivery (also accessible using transaction code SA38—ABAP Reports and program RVSPERAU). Review items on the list with the appropriate operational management and ascertain whether there are legitimate reasons for the sales documents to remain blocked.		
B-3.6b	<u>Agree on the process work products</u> ⁹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design).				
	<u>Assess</u> to what extent the process work products are available.				
	Process Sales order processing inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.	
B-3.7b	Process Practice		Work Products	Assessment Step	
	Sales order processing	<ul style="list-style-type: none"> • Incomplete Sales Order list • Delivery Due List (Sales Orders ready to be shipped) • Sales Orders on Credit Hold • Sales Order Pricing Variance List 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		
B-3.7b	<u>Agree on the process capability level</u> to be achieved by the process.				
	<i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				
SAP ERP Revenue process: Invoice processing					
B-3.1c	<u>Understand the Process context.</u>				
B-3.2c	<u>Understand the Process purpose.</u>				
B-3.3c	<u>Understand all process stakeholders</u> and their roles.				
	Invoice processing stakeholders:				

⁹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Revenue Business Cycle						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment
B-3.4c	<u>Understand the Process goals</u> and related metrics ¹⁰ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., <u>assess the effectiveness</u> of the process.					
	The Process Invoice processing has five defined process goal.		The following activities can be performed to assess whether the goals are achieved.			
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step		
	Controls are in place to prevent duplicate shipments or delay in the shipping of goods to customers.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
	Invoices are generated using authorized terms and prices and are accurately calculated and recorded.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
	All goods shipped are invoiced in a timely manner.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
B-3.5c	Credit notes and adjustments to accounts receivable are accurately calculated and recorded.					
	Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with the enterprise's policy and in a timely manner.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:					
	Reference Process	Invoice processing	Criteria: 3.1 Controls are in place to prevent duplicate shipments or delay in the shipping of goods to customers. 3.2 Invoices are generated using authorized terms and prices and are accurately calculated and recorded. 3.3 All goods shipped are invoiced in a timely manner. 3.4 Credit notes and adjustments to accounts receivable are accurately calculated and recorded. 3.5 Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with the enterprise's policy and in a timely manner.			
	Reference Process Practices ¹¹	Good Practice	Assessment Step		Issue Cross-reference	Comment
	APO06 DSS01	Controls are in place to prevent duplicate shipments or delay in the shipping of goods to customers.	3.1.1 Generate the list of current system configuration settings relating to copy control between sales and shipping documents using transaction code VTIA—Order to Delivery Copying Control. Select each combination of delivery type and sales document type, and click the Item			

¹⁰ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

¹¹ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Revenue Business Cycle audit/assurance program.

Audit/Accuracy Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
			<p>button. Double-click each item category, and verify that the entry for the Pos./neg. quantity field has been set to + (automatic update occurs between documents as deliveries are made for line items specified in the sales document). Depending on the volume of shipping and sales input manually, it may also be necessary to verify a sample of shipping and sales input for accuracy.</p>		
	APO06 DSS01	Controls are in place to prevent duplicate shipments or delay in the shipping of goods to customers.	<p>3.1.2 Interview management and determine whether any of the following reports are used to check the complete and timely shipment of goods to customers:</p> <ul style="list-style-type: none"> • Backorders Reports—V.15 • Sales Orders/Purchase Orders Worklist—VL04 • Outbound Deliveries for Picking—VL06 • Outbound Deliveries for Confirmation—VL06C • Outbound Deliveries for Loading—VL06L • Outbound Deliveries for Transportation Planning—VL06T • Outbound Deliveries for Goods Issue—VL06G <p>Review a sample of hard copy reports used for evidence of action taken and a sample of the reports online, and check the aging of items to determine whether entries have been cleared in a timely manner.</p>		
	DSS06	Invoices are generated using authorized terms and prices and are accurately calculated and recorded.	<p>3.2.1 Display current system settings relating to invoice preparation online using transaction code SPRO to display the IMG menu and follow path: Sales and Distribution → Billing → Billing Documents → Maintain Copy Controls for Billing Documents. Determine whether the connection between source and target documents supports the accurate flow of billing details through the sales process and supports the accurate calculation and posting of invoice data.</p>		
	APO13 DSS06	All goods shipped are invoiced in a timely manner.	<p>3.3.1 Execute transaction code VF04—Maintain Billing Due List. All documents that have not been invoiced, or that have been only partially invoiced, will appear on the list, sorted by invoice due date. Review the aging of items on the list. For items outstanding for more than one billing period, seek an explanation from management as to why the items have not been billed. Documents may not be invoiced fully for reasons that include:</p> <ul style="list-style-type: none"> • An invoice block set in either the document or the customer master record • Incomplete delivery <p>Although both of these reasons are valid, documents that have not been invoiced fully should be investigated promptly to ensure that revenue is matched with costs and the delay is resolved.</p>		
	DSS05	All goods shipped are invoiced in a timely manner.	<p>3.3.2 Assess user access to picking lists, delivery notes and goods issued. Deliveries can be created in the SAP ERP system using two different transactions. Use transaction SUIM—User Information System to test user access to:</p> <ul style="list-style-type: none"> • VL01—Create Delivery for a single delivery • VL04—Process Delivery Due List for multiple deliveries 		

Transaction(s)	Authorization Objects	Fields	Values
----------------	-----------------------	--------	--------

Audit/Assurance Program for SAP ERP Revenue Business Cycle								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes								
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment
			VL01—Create Delivery	V_LIKP_VST	ACTVT	01, 04		
			VL04—Process Delivery Due List	V_LIKP_VST	ACTVT	03, 18		
			<p>Deliveries can be changed using transaction code VL02. The authorization object for the general handling of the delivery is V_LIKP_VST. Any individual who is authorized to post the goods issued for a delivery must also be authorized to change a delivery. Movement types 601 and 651 are required to post goods issued for outgoing sales orders and incoming returns. Movement types 621 through 624 are required to handle deliveries for returnable packaging. Movement types 631 through 634 are required to handle deliveries for customer consignment. The typical values used in carrying out this test are as follows:</p> <ul style="list-style-type: none"> • Create—01 • Change—02 • Display—03 • Print, edit message—04 • Deliveries from collective processing—18 					

Audit/Accuracy Program for SAP ERP Revenue Business Cycle																																													
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																													
Ref.	Assurance Steps and Guidance			Issue Cross-reference																																									
				Comment																																									
	APO13 DSS06	All goods shipped are invoiced in a timely manner.	<p>3.3.3 Invoices in the SAP ERP system can be entered via the SD module or the FI module. When invoices are posted via the SD module, these invoices are transferred to the FI module where they become open items. During the transfer of invoices from SD to FI, errors can occur or invoices may be deliberately blocked for approval. Execute transaction code VF03—Display Billing Document, click on the expansion button next to the billing document field and select Billing Documents Still to Be Passed Onto Accounting. Obtain an explanation for any invoices that appear on this list.</p> <p>Use transaction code SUIM—User Information System to test access to enter invoices, and confirm that access is consistent with staff job roles and management's intentions. Test user access to create and maintain invoices as follows:</p> <p>AR entry Sales view:</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>VF01—Create Billing Document</td><td>V_VBRK_FKA</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td>VF04—Maintain Billing Due List</td><td>V_VBRK_VKO</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td></td><td>V_KONH_VKO</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td></td><td>V_KONH_VKS</td><td>ACTVT</td><td>01, 02</td></tr> </tbody> </table> <p>AR entry Finance view:</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>FB70—Enter Outgoing Invoices</td><td>F_BKPF_BLA</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td></td><td>F_BKPF_BUK</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td></td><td>F_BKPF_GSB</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td></td><td>F_BKPF_KOA</td><td>ACTVT</td><td>01, 02</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	VF01—Create Billing Document	V_VBRK_FKA	ACTVT	01, 02	VF04—Maintain Billing Due List	V_VBRK_VKO	ACTVT	01, 02		V_KONH_VKO	ACTVT	01, 02		V_KONH_VKS	ACTVT	01, 02	Transaction(s)	Authorization Objects	Fields	Values	FB70—Enter Outgoing Invoices	F_BKPF_BLA	ACTVT	01, 02		F_BKPF_BUK	ACTVT	01, 02		F_BKPF_GSB	ACTVT	01, 02		F_BKPF_KOA	ACTVT	01, 02		
Transaction(s)	Authorization Objects	Fields	Values																																										
VF01—Create Billing Document	V_VBRK_FKA	ACTVT	01, 02																																										
VF04—Maintain Billing Due List	V_VBRK_VKO	ACTVT	01, 02																																										
	V_KONH_VKO	ACTVT	01, 02																																										
	V_KONH_VKS	ACTVT	01, 02																																										
Transaction(s)	Authorization Objects	Fields	Values																																										
FB70—Enter Outgoing Invoices	F_BKPF_BLA	ACTVT	01, 02																																										
	F_BKPF_BUK	ACTVT	01, 02																																										
	F_BKPF_GSB	ACTVT	01, 02																																										
	F_BKPF_KOA	ACTVT	01, 02																																										
	DSS05	Credit notes and adjustments to accounts receivable are accurately calculated and recorded.	<p>3.4.1 Use transaction code SUIM—User Information System to test user access to sales order returns and credit notes. Typical transactions and authorization objects involved in this test include the following:</p> <p>Order entry Sales view:</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>VA01—Create Sales Order</td><td>V_VBAK_AAT</td><td>ACTVT</td><td>01, 02, 05, 06, 43 (Release)</td></tr> <tr> <td>VA02—Change Sales</td><td></td><td></td><td></td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	VA01—Create Sales Order	V_VBAK_AAT	ACTVT	01, 02, 05, 06, 43 (Release)	VA02—Change Sales																																	
Transaction(s)	Authorization Objects	Fields	Values																																										
VA01—Create Sales Order	V_VBAK_AAT	ACTVT	01, 02, 05, 06, 43 (Release)																																										
VA02—Change Sales																																													

Audit/Accuracy Program for SAP ERP Revenue Business Cycle																									
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																									
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment																	
			Order	V_VBAK_VKO	ACTVT	01, 02, 05, 06, 43 (Release)																			
			ACTVT 01 is not applicable for transaction code VA02.																						
			Order entry Finance view: <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td rowspan="4">FB75—Enter Outgoing Credit Memos</td><td>F_BKPF_BLA</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td>F_BKPF_BUK</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td>F_BKPF_GSB</td><td>ACTVT</td><td>01, 02</td></tr> <tr> <td>F_BKPF_KOA</td><td>ACTVT</td><td>01, 02</td></tr> </tbody> </table>					Transaction(s)	Authorization Objects	Fields	Values	FB75—Enter Outgoing Credit Memos	F_BKPF_BLA	ACTVT	01, 02	F_BKPF_BUK	ACTVT	01, 02	F_BKPF_GSB	ACTVT	01, 02	F_BKPF_KOA	ACTVT	01, 02	
Transaction(s)	Authorization Objects	Fields	Values																						
FB75—Enter Outgoing Credit Memos	F_BKPF_BLA	ACTVT	01, 02																						
	F_BKPF_BUK	ACTVT	01, 02																						
	F_BKPF_GSB	ACTVT	01, 02																						
	F_BKPF_KOA	ACTVT	01, 02																						
DSS01 DSS06	Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with the enterprise's policy and in a timely manner.	3.5.1 In SAP ERP it is possible to configure the system so that when a document is entered, a reference document is required. A reference to a source document ensures accurate copying of details, including the customer number, material numbers, pricing date, quantities, payment and shipping terms. It is common for the mandatory reference field for document types not to be defined when the system is first implemented. Often, a document that has been created in SAP ERP needs to reference a document that was created in a different system. For example, a credit note created in SAP ERP may relate to an invoice created in a billing system. However, if all documents are created using SAP ERP, the system should be configured with a mandatory reference field. To test if this field is in use, use transaction VOV8—Document Type Maintenance, look for all sales document types that relate to sales order returns and credit requests. Double-click on one of the document types and determine if there is a Reference Mandatory Field in the General Control section of the screen. The list of possible values is as follows: <table border="1"> <thead> <tr> <th>Value</th> <th>Reference</th> </tr> </thead> <tbody> <tr> <td>Blank</td> <td>No reference required</td> </tr> <tr> <td>A</td> <td>With reference to an inquiry</td> </tr> <tr> <td>B</td> <td>With reference to a quotation</td> </tr> <tr> <td>C</td> <td>With reference to a sales order</td> </tr> <tr> <td>E</td> <td>Scheduling agreement reference</td> </tr> <tr> <td>G</td> <td>With reference to a quantity contract</td> </tr> <tr> <td>M</td> <td>With reference to a billing document</td> </tr> </tbody> </table> Verify that the value has been set to M , and repeat the testing steps for all of the other relevant document types.	Value	Reference	Blank	No reference required	A	With reference to an inquiry	B	With reference to a quotation	C	With reference to a sales order	E	Scheduling agreement reference	G	With reference to a quantity contract	M	With reference to a billing document							
Value	Reference																								
Blank	No reference required																								
A	With reference to an inquiry																								
B	With reference to a quotation																								
C	With reference to a sales order																								
E	Scheduling agreement reference																								
G	With reference to a quantity contract																								
M	With reference to a billing document																								

Audit/Accrual Program for SAP ERP Revenue Business Cycle												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes												
Ref.	Assurance Steps and Guidance			Issue Cross-reference								
				Comment								
		<p>Discuss with management the reference field settings in place for the selected document types, and determine if the configuration values in place are set as management intended.</p>										
	DSS06	<p>Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with the enterprise's policy and in a timely manner.</p> <p>3.5.2 In SAP ERP it is possible to configure the system to block all sales documents from further processing by assigning shipping and/or billing blocks. It is also possible to customize the system to block specific types of sales documents for specific customers. This ensures that credit notes and/or debit notes are processed only with the correct authorization. The system can be configured to trigger Workflow actions to correct any issues in a timely manner.</p> <p>Blocks should be set at the sales document type level. Delivery block at the header level is effective only if it has been assigned to the corresponding delivery type during customization (table TVLSP). Independent of this assignment, the delivery block must be effective at the schedule line level.</p> <p>Review the configuration settings for delivery and billing blocks online using the IMG as follows:</p> <p>Shipping— Use transaction code SPRO to display the IMG menu and follow path: Logistics Execution → Shipping → Deliveries → Define Reasons for Blocking in Shipping.</p> <p>Billing— Use transaction code SPRO to display the IMG menu and follow path: Sales and Distribution → Billing → Billing Documents → Define Blocking Reason for Billing.</p> <p>Determine whether the settings support the processing of credits in line with the enterprise's credit management policy and are consistent with management's intention.</p> <p>Use transaction code SUIM—User Information System to test user access to sales order and delivery release. SD documents can be released in the SAP ERP system using the following transactions:</p> <ul style="list-style-type: none"> • VKM1—Blocked SD Documents • VKM2—Release SD Documents • VKM3—Sales Document for sales documents release • VKM4—SD Documents for SD documents release • VKM5—Delivery for delivery release <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>VKM1— Blocked SD Documents</td><td>V_KNKK_FRE</td><td>ACTVT</td><td>03, 23 (maintain)</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	VKM1— Blocked SD Documents	V_KNKK_FRE	ACTVT	03, 23 (maintain)		
Transaction(s)	Authorization Objects	Fields	Values									
VKM1— Blocked SD Documents	V_KNKK_FRE	ACTVT	03, 23 (maintain)									

Audit/Accuracy Program for SAP ERP Revenue Business Cycle								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes								
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment
			VKM2— Release SD Documents VKM3— Sales Document for sales documents release VKM4— SD Documents for SD documents release VKM5— Delivery for delivery release	V_VBUK_FRE	ACTVT	03, 23 (maintain)		
B-3.6c	<p>Agree on the process work products¹² (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess</u> to what extent the process work products are available.</p> <p>Process Invoice processing inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.</p>							
	Process Practice	Work Products			Assessment Step			

¹² For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: *Enabling Processes*.

Audit/Accrual Program for SAP ERP Revenue Business Cycle							
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes							
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment		
B-3.7c	Invoice processing	<ul style="list-style-type: none"> • Deliveries not yet invoiced report • List of invoices not released to accounting 		Apply appropriate audit techniques to determine the existence and appropriate use of each work product.			
	<p>Agree on the process capability level to be achieved by the process.</p> <p><i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i></p>						
SAP ERP Revenue process: Collecting and processing cash receipts							
B-3.1d	<u>Understand the Process context.</u>						
B-3.2d	<u>Understand the Process purpose.</u>						
B-3.3d	<u>Understand all process stakeholders</u> and their roles.						
B-3.4d	Collecting and processing cash receipts stakeholders:						
	<p>Understand the Process goals and related metrics¹³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.</p> <p>The Process Collecting and processing cash receipts has four defined process goals. The following activities can be performed to assess whether the goals are achieved.</p>						
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step			
	Cash receipts are entered accurately, completely and in a timely manner.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
	Cash receipts are valid and are not duplicated.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
	Cash discounts are calculated and recorded accurately.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
	Timely collection of cash receipts is monitored.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
B-3.5d	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:						
	Reference Process	Collecting and processing cash receipts	<p>Criteria:</p> <p>4.1 Cash receipts are entered accurately, completely and in a timely manner.</p> <p>4.2 Cash receipts are valid and are not duplicated.</p> <p>4.3 Cash discounts are calculated and recorded accurately.</p> <p>4.4 Timely collection of cash receipts is monitored.</p>				
	Reference Process	Good Practice	Assessment Step		Issue Cross-reference		

¹³ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	Practices¹⁴				
	DSS01 DSS06	Cash receipts are entered accurately, completely and in a timely manner.	4.1.1 Take a sample of bank reconciliations and test for adequate clearance of reconciling items and approval by finance management.		
	DSS06	Cash receipts are entered accurately, completely and in a timely manner.	4.1.2 Execute transaction code FI12—Change House Bank/Bank Accounts and ascertain to which bank accounts a cash receipt can be posted. Determine whether this is consistent with management's intentions.		
	DSS01 DSS06	Cash receipts are valid and are not duplicated.	4.2.1 Review the AR reconciliation and determine whether there are any amounts unallocated or any reconciling items. Determine the aging of these items, and ask management the reasons for these items remaining unallocated or unreconciled.		
	APO12 DSS01 DSS06	Cash discounts are calculated and recorded accurately.	4.3.1 Review the settings in place for tolerance levels for allowable cash discounts and cash payment differences by using the following transactions: <ul style="list-style-type: none">• Transaction code OBA4—User Tolerances to determine the tolerance groups that have been set up for users and the tolerance limits that have been set for those groups• Transaction code OB57—Assign Users to Tolerance Group to determine the users who have been allocated to the groups previously identified Discuss with management the settings in place for tolerance levels for allowable cash discounts and cash payment differences. Determine whether the configuration in place agrees with management's intentions.		
	APO12 DSS01 DSS06	Timely collection of cash receipts is monitored.	4.4.1 Use transaction code F.21—Customer Open Items (also accessible using transaction code SA38 and program RFDEPL00) to review customer open items. The report lists each item and the amount owed. At the end of the listing, the total amount still to be collected is calculated. Transaction code S_ALR_87009956—Customer Open Item Analysis (days overdue analysis, also accessible through transaction code SA38 and program RFDOPR10) can be used to review accounts receivable overdue items. For each balance overdue, the report shows the days in arrears and amount overdue. A number of selection criteria can be specified when running the report, such as open items at a key date, customer account, company code, balance and overdue items balance. Determine whether these reports are reviewed and actioned regularly by locating evidence of their review or through corroborative inquiry with management.		
B-3.6d	<u>Agree on the process work products¹⁵</u> (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess</u> to what extent the process work products are available.				
	Collecting and processing cash receipts inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.	
	Process Practice	Work Products	Assessment Step		
	Collecting and processing cash receipts	<ul style="list-style-type: none">• Open payment advise listing• Unapplied cash report• List of Cash Application Adjustments	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		
B-3.7d	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can</i>				

¹⁴ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Revenue Business Cycle audit/assurance program.

¹⁵ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Revenue Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
	<i>be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>		
Audit/Accurance Program for SAP ERP Revenue Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Organisational Structures			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-4	Obtain understanding of each Organisational Structure in scope and set suitable assessment criteria: For each Organisational Structure in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the Organisational Structure .		
Organisational Structure: Sales and Use Tax department			
B-4.1a	<u>Understand the Organisational Structure context.</u> <i>Identify and document all elements that can help to understand the context in which the Financial accounting organization has to operate, including:</i> <ul style="list-style-type: none"> • The overall organisation • Management/process framework • History of the role/structure • Contribution of the Organisational Structure to achievement of goals 		
B-4.2a	<u>Understand all stakeholders of the Organisational Structure/function.</u> <i>Determine through documentation review (policies, management communications, etc.) the key stakeholders of the Financial accounting organization.</i> <ul style="list-style-type: none"> • Incumbent of the role and/or members of the Organisational Structure • Other key stakeholders affected by the decisions of the Organisational Structure/role 		
B-4.3a	<u>Understand the goals of the Organisational Structure</u> , the related metrics and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals.		
Organisational Structure Goal		Assessment Step	
Determine through interviews with key stakeholders and documentation review the goals of the Sales and Use Tax department organization, i.e., the decisions for which they are accountable ^{16,17} .		This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 	
B-4.4a	<u>Agree on the expected good practices for the Organisational Structure against which it will be assessed.</u> <u>Assess the Organisational Structure design</u> , i.e., assess the extent to which expected good practices are applied.		
Good Practice		Criteria	Assessment Step
Operating principles		<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles.

¹⁶ The RACI charts in COBIT 5: *Enabling Processes* can be leveraged as a starting point for the expected goals of a role or Organisational Structure.

¹⁷ The Organisational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organisational Structure assuming the same responsibilities and accountability should be considered.

Audit/Accrual Program for SAP ERP Revenue Business Cycle						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes						
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment	
B-4.5a		meaningful.	<ul style="list-style-type: none"> Verify that meeting reports/minutes are available and are meaningful. 			
	Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.			
	Span of control	<ul style="list-style-type: none"> The span of control of the Organisational Structure is defined. The span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. The span of control is in line with the overall enterprise governance arrangements. 	<ul style="list-style-type: none"> Verify whether the span of control of the Organisational Structure is defined. Assess whether the span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. Verify and assess whether the span of control is in line with the overall enterprise governance arrangements. 			
	Level of authority/decision rights	<ul style="list-style-type: none"> Decision rights of the Organisational Structure are defined and documented. Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue). 	<ul style="list-style-type: none"> Verify that decision rights of the Organisational Structure are defined and documented. Verify whether decision rights of the Organisational Structure are complied with and respected. 			
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.			
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.			
<u>Understand</u> the life cycle and agree on expected values. <u>Assess</u> the extent to which the Organisational Structure life cycle is managed.						
Life-Cycle Element		Criteria	Assessment Step			
Mandate		<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well-understood mandate. 			
Monitoring		<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 			
B-4.1 to B-4.5	Repeat steps B-4.1 through B-4.5 for all remaining Organisational structures in scope.					
	Repeat the steps described above for the remaining Organisational structures:					
<ul style="list-style-type: none"> Sales department Accounts receivable Credit Warehouse Shipping Marketing and Pricing 						

Audit/Accurance Program for SAP ERP Revenue Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref.	Assurance Step and Guidance			Issue Cross-reference
B-5	Obtain understanding of the Culture, Ethics and Behaviour in scope. Assess Culture, Ethics and Behaviour.			
Culture, Ethics and Behaviour: Risk and compliance aware culture				
B-5.1a	<u>Understand the Culture, Ethics and Behaviour context.</u> <ul style="list-style-type: none"> • <i>What the overall corporate Culture is like</i> • <i>Understand the interconnection with other enablers in scope:</i> <ul style="list-style-type: none"> - <i>Identify roles and structures that could be affected by the Culture.</i> - <i>Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.</i> 			
B-5.2a	<u>Understand the major stakeholders of the Culture, Ethics and Behaviour: Risk and compliance aware culture</u> <i>Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.</i>			
B-5.3a	<u>Understand the goals for the Culture, Ethics and Behaviour, and the related metrics</u> and agree on expected values. Assess whether the Culture, Ethics and Behaviour goals (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour. In the context of Risk and compliance aware culture , the following Culture, Ethics and Behaviour are desired:	Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. For a representative sample of individuals, perform the following assessment steps.		
Desired Behaviour (Culture, Ethics and Behaviour Goal)		Assessment Step		
The enterprise is aware of the compliance requirements it must abide.				
Employees understand their role in maintaining compliance.				
Identified risk are properly addressed.				
Controls are in place to ensure compliance with internal and external requirements.				
B-5.4a	<u>Understand the life cycle stages of the Culture, Ethics and Behaviour</u> , and agree on the relevant criteria. Assess to what extent the Culture, Ethics and Behaviour life cycle is managed. <small>(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)</small>			
B-5.5a	<u>Understand good practice when dealing with Culture, Ethics and Behaviour</u> , and agree on relevant criteria. Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied.			
Good Practice		Criteria	Assessment Step	
Communication, enforcement and rules		Existence and quality of the communication	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.	
Incentives and rewards		Existence and application of appropriate rewards and incentives	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.	
Awareness		Awareness of desired Behaviours	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.	
B-5.1 to B-5.5	Repeat steps B-5.1 through B-5.5 for all remaining Culture, Ethics and Behaviour in scope.			
B-5.1 to B-5.5	Repeat the steps described above for the remaining Culture, Ethics and Behaviour:			

Audit/Assurance Program for SAP ERP Revenue Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Culture, Ethics and Behaviour			
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment
	<ul style="list-style-type: none">• Enabling of continuous improvement• Accountability• Discipline to follow instructions		

Audit/Accrual Program for SAP ERP Revenue Business Cycle																																																																																				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																																																																																				
Ref.	Assurance Steps and Guidance			Issue Cross-reference																																																																																
B-6	Obtain understanding of the Information Items in scope. Assess Information Items.																																																																																			
Information Item: Data integrity procedures																																																																																				
B-6.1a	<p><u>Understand the Information item context:</u></p> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> - <i>Used by which processes?</i> - <i>Which Organisational Structures are involved?</i> - <i>Which services/applications are involved?</i> 																																																																																			
B-6.2a	<p><u>Understand the major stakeholders of the Information item.</u> <u>Understand the stakeholders for the Information item, i.e., identify the:</u></p> <ul style="list-style-type: none"> • <i>Information producer</i> • <i>Information custodian</i> • <i>Information consumer</i> <p><i>Stakeholders should be at the appropriate organisational level.</i></p>																																																																																			
B-6.3a	<p><u>Understand the major quality criteria for the Information item, the related metrics and agree on expected values.</u> <u>Assess whether the Information item quality criteria (outcomes) are achieved, i.e., assess the effectiveness of the Information item.</u></p> <p>Leverage the COBIT 5 Information enabler model¹⁸ focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand.</p> <p>Mark the quality dimensions with a ‘✓’ that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p>		The assurance professional will, by using appropriate auditing techniques, verify all quality criteria in scope and assess whether the criteria are met.																																																																																	
<table border="1"> <thead> <tr> <th>Quality Dimension</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> <th></th> </tr> </thead> <tbody> <tr><td>Accuracy</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Objectivity</td><td></td><td></td><td></td><td></td></tr> <tr><td>Believability</td><td></td><td></td><td></td><td></td></tr> <tr><td>Reputation</td><td></td><td></td><td></td><td></td></tr> <tr><td>Relevancy</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Completeness</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Currency</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Amount of information</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Concise representation</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Consistent representation</td><td></td><td></td><td></td><td></td></tr> <tr><td>Interpretability</td><td></td><td></td><td></td><td></td></tr> <tr><td>Understandability</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Manipulation</td><td></td><td></td><td></td><td></td></tr> <tr><td>Availability</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Restricted access</td><td>✓</td><td></td><td></td><td></td></tr> </tbody> </table>					Quality Dimension	Key Criteria	Description	Assessment Step		Accuracy	✓				Objectivity					Believability					Reputation					Relevancy	✓				Completeness	✓				Currency	✓				Amount of information	✓				Concise representation	✓				Consistent representation					Interpretability					Understandability	✓				Manipulation					Availability	✓				Restricted access	✓			
Quality Dimension	Key Criteria	Description	Assessment Step																																																																																	
Accuracy	✓																																																																																			
Objectivity																																																																																				
Believability																																																																																				
Reputation																																																																																				
Relevancy	✓																																																																																			
Completeness	✓																																																																																			
Currency	✓																																																																																			
Amount of information	✓																																																																																			
Concise representation	✓																																																																																			
Consistent representation																																																																																				
Interpretability																																																																																				
Understandability	✓																																																																																			
Manipulation																																																																																				
Availability	✓																																																																																			
Restricted access	✓																																																																																			

¹⁸ COBIT 5 framework, appendix G, p.81-84

Audit/Accurance Program for SAP ERP Revenue Business Cycle																															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																															
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment																										
B-6.4a	<p>Understand the life cycle stages of the Information item, and agree on the relevant criteria. Assess to what extent the Information item life cycle is managed.</p> <p>The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.</p> <ul style="list-style-type: none"> When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently. When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. <p>Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Life Cycle Stage</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Plan</td><td>✓</td><td></td><td></td></tr> <tr> <td>Design</td><td>✓</td><td></td><td></td></tr> <tr> <td>Build/acquire</td><td>✓</td><td></td><td></td></tr> <tr> <td>Use/operate</td><td>✓</td><td></td><td></td></tr> <tr> <td>Evaluate/monitor</td><td>✓</td><td></td><td></td></tr> <tr> <td>Update/dispose</td><td>✓</td><td></td><td></td></tr> </tbody> </table>	Life Cycle Stage	Key Criteria	Description	Assessment Step	Plan	✓			Design	✓			Build/acquire	✓			Use/operate	✓			Evaluate/monitor	✓			Update/dispose	✓				
Life Cycle Stage	Key Criteria	Description	Assessment Step																												
Plan	✓																														
Design	✓																														
Build/acquire	✓																														
Use/operate	✓																														
Evaluate/monitor	✓																														
Update/dispose	✓																														
B-6.5a	<p>Understand important attributes of the Information item and expected values. Assess the Information item design, i.e., assess the extent to which expected good practices are applied.</p> <p>Good practices for Information items are defined as a series of attributes for the Information item¹⁹. The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.</p> <p>Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Attribute</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Physical</td><td></td><td></td><td></td></tr> <tr> <td>Empirical</td><td></td><td></td><td></td></tr> <tr> <td>Syntactic</td><td></td><td></td><td></td></tr> <tr> <td>Semantic</td><td></td><td></td><td></td></tr> <tr> <td>Pragmatic</td><td>✓</td><td></td><td></td></tr> <tr> <td>Social</td><td></td><td></td><td></td></tr> </tbody> </table>	Attribute	Key Criteria	Description	Assessment Step	Physical				Empirical				Syntactic				Semantic				Pragmatic	✓			Social					
Attribute	Key Criteria	Description	Assessment Step																												
Physical																															
Empirical																															
Syntactic																															
Semantic																															
Pragmatic	✓																														
Social																															
B-6.1 to B-6.5	Repeat steps B-6.1 through B-6.5 for all remaining Information items in scope.																														
	<p>Repeat the steps described above for the remaining Information items:</p> <ul style="list-style-type: none"> Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis Retention requirements Record of transactions Training manuals Job aids 																														

¹⁹ COBIT 5 framework, appendix G, p. 81-84

Audit/Accuracy Program for SAP ERP Revenue Business Cycle																								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Services, Infrastructures and Applications																								
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment																			
B-7	Obtain understanding of the Services, Infrastructure and Applications in scope. Assess Services, Infrastructure and Applications.																							
Services, Infrastructure and Applications: Master data maintenance group																								
B-7.1a	<u>Understand the Services, Infrastructure and Applications</u> context. <i>Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.</i>																							
B-7.2a	<u>Understand the major stakeholders of the Services, Infrastructure and Applications.</u> <i>Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.</i>																							
B-7.3a	<u>Understand the major goals for the Services, Infrastructure and Applications</u> , the related metrics and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.																							
<table border="1"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th><th></th><th></th></tr> </thead> <tbody> <tr> <td>Service description</td><td> <ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders </td><td> <ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. </td><td></td><td></td></tr> <tr> <td>Service level definition</td><td>Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness </td><td> <ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. </td><td></td><td></td></tr> <tr> <td>Contribution to related enablers, IT and enterprise goals</td><td>The Service contributes to the achievement of related enabler and IT-related and enterprise goals.</td><td>Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.</td><td></td><td></td></tr> </tbody> </table>					Goal	Criteria	Assessment Step			Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 			Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 			Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.		
Goal	Criteria	Assessment Step																						
Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 																						
Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 																						
Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.																						
B-7.4a	<u>Understand good practice related to the Services, Infrastructure and Applications and expected values.</u> <u>Assess the Services, Infrastructure and Applications design</u> , i.e., assess to what extent expected good practices are applied. <i>Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework²⁰ to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented:</i> <ul style="list-style-type: none"> Buy/build decision needs to be taken. Use of the Service needs to be clear. 																							
<table border="1"> <thead> <tr> <th>Good Practice</th><th>Criteria</th><th>Assessment Step</th><th></th><th></th></tr> </thead> <tbody> <tr> <td>Sourcing (buy/build)</td><td>A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.</td><td> <ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. </td><td></td><td></td></tr> <tr> <td>Use</td><td>The use of the Service needs to be clear: <ul style="list-style-type: none"> When it needs to be used and by whom </td><td> <ul style="list-style-type: none"> Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be </td><td></td><td></td></tr> </tbody> </table>					Good Practice	Criteria	Assessment Step			Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. 			Use	The use of the Service needs to be clear: <ul style="list-style-type: none"> When it needs to be used and by whom 	<ul style="list-style-type: none"> Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be 							
Good Practice	Criteria	Assessment Step																						
Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. 																						
Use	The use of the Service needs to be clear: <ul style="list-style-type: none"> When it needs to be used and by whom 	<ul style="list-style-type: none"> Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be 																						

²⁰ COBIT 5 framework, appendix G, p.85-86

Audit/Assurance Program for SAP ERP Revenue Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Information Items					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> The required compliance levels with the Service's output 	<ul style="list-style-type: none"> used. Verify that actual use is in line with requirement above. Verify that the actual Service output is adequately used. Verify that Service levels are monitored and achieved. 		
B-7.1 to B-7.4	<p>Repeat steps B-7.1 through B-7.4 for all remaining Services, Infrastructure and Applications in scope.</p> <p>Repeat the steps described above for the remaining Services, Infrastructure and Applications:</p> <ul style="list-style-type: none"> SAP ERP System Change management SAP training 				

Audit/Accrual Program for SAP ERP Revenue Business Cycle																					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																					
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment																		
B-8	Obtain understanding of the People, Skills and Competencies in scope. Assess People, Skills and Competencies.																				
People, Skill and Competency: Proficiency using SAP Sales and Distribution, Treasury (Cash Applications), Accounts Receivable and Credit Modules																					
B-8.1a	<p><u>Understand</u> the People, Skills and Competencies context. <i>Understand the context of the Skill/Competency, i.e.:</i></p> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> – <i>In which roles and structures is the Skill/Competency used? (See also B-4.1.)</i> <p><i>Which behaviours are associated with the Skill/Competency?</i></p>																				
B-8.2a	<p><u>Understand</u> the major stakeholders for the People, Skills and Competencies. <i>Identify to whom in the organisation the skill requirement applies.</i></p>																				
B-8.3a	<p><u>Understand</u> the major goals for the People, Skills and Competencies, the related metrics and agree on expected values. <i>Assess</i> whether the People, Skills and Competencies goals (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.</p> <p>For the People, Skills and Competencies: Proficiency using SAP Sales and Distribution, Treasury (Cash Applications), Accounts Receivable and Credit Modules, the following goals and associated criteria can be addressed.</p> <table border="1"> <thead> <tr> <th>Goal</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Experience</td> <td></td> <td rowspan="7">Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.</td> </tr> <tr> <td>Education</td> <td></td> </tr> <tr> <td>Qualification</td> <td></td> </tr> <tr> <td>Knowledge</td> <td></td> </tr> <tr> <td>Technical skills</td> <td></td> </tr> <tr> <td>Behavioural skills</td> <td></td> </tr> <tr> <td>Number of people with appropriate skill level</td> <td></td> </tr> </tbody> </table>	Goal	Criteria	Assessment Step	Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	Education		Qualification		Knowledge		Technical skills		Behavioural skills		Number of people with appropriate skill level			
Goal	Criteria	Assessment Step																			
Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.																			
Education																					
Qualification																					
Knowledge																					
Technical skills																					
Behavioural skills																					
Number of people with appropriate skill level																					
B-8.4a	<p><u>Understand</u> the life cycle stages of the People, Skills and Competencies, and agree the relevant criteria. <i>Assess</i> to what extent the People, Skills and Competencies life cycle is managed.</p> <p>For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07.</p> <table border="1"> <thead> <tr> <th>Life Cycle Element</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Plan</td> <td>Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.</td> <td>Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.</td> </tr> <tr> <td>Design</td> <td> Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to </td> <td> Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill. </td> </tr> </tbody> </table>	Life Cycle Element	Criteria	Assessment Step	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.											
Life Cycle Element	Criteria	Assessment Step																			
Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.																			
Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.																			

Audit/Accuracy Program for SAP ERP Revenue Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
		knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.		
	Build	Practice APO07.03 activity 4 (Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 4 is implemented in relation to this skill.	
	Operate	Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.	
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.	
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.	
	B-8.5a	Understand good practice related to the People, Skills and Competencies and expected values. Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.		
Good Practice	Criteria	Assessment Step		
Skill set and Competencies are defined.	<ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 			
Skill levels are defined.	<ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. Assess the process for 360-degree performance evaluations. 			

Audit/Assurance Program for SAP ERP Revenue Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
People, Skills and Competencies			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-8.1 to B-8.5	<p>Repeat steps B-8.1 through B-8.5 for all remaining People, Skills and Competencies in scope.</p> <p>Repeat the steps described above for the remaining People, Skills and Competencies:</p> <ul style="list-style-type: none"> • Master data management skills • Order to Cash process skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 		

Audit/Accurance Program for SAP ERP Revenue Business Cycle		
Phase C—Communicate the Results of the Assessment		
Ref.	Assurance Step	Guidance
C-1	Document exceptions and gaps.	
C-1.1	Understand and document weaknesses and their impact on the achievement of process goals.	<ul style="list-style-type: none"> Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	<ul style="list-style-type: none"> Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. Point out the consequence of noncompliance with regulatory requirements and contractual agreements. Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
C-2	Communicate the work performed and findings.	
C-2.1	Communicate the work performed.	<ul style="list-style-type: none"> Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	<ul style="list-style-type: none"> Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. Use benchmarking and survey results to compare the enterprise's performance with others. Use extensive graphics to illustrate the issues. Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	

Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
1. Master Data Maintenance							
1.1 Changes made to master data are valid, complete, accurate and timely.							
1.1.1 Does relevant management, other than the initiators, check online reports of master data additions and changes back to source documentation on a sample basis?					DSS01 DSS06		
1.1.2 Have configurable controls in SAP been designed into processes to maintain the integrity of master data?					DSS06		
1.2 Master data remain current and pertinent.							
1.2.1 Does management periodically review master data to check their accuracy and timeliness?					DSS01 DSS06		
1.3 Access to master data changes is properly maintained.							
1.3.1 Is access to create and change master data restricted to authorized individuals?					DSS05 DSS06		
1.4 Changes to master data are properly authorized.							
1.4.1 Are all requests to create or update master data records approved and copies retained as evidence of validity?					BAI06		
1.4.2 Does relevant management conduct periodic reconciliation between changes to the master data and source documents?					DSS01 DSS06		
1.4.3 Are Inactive customer accounts on the database locked to avoid sales orders against those accounts?					DSS06		
2. Sales Order Processing							
2.1 Sales orders are processed with valid prices and terms, and processing is complete, accurate and timely.							

Revenue Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.1.1 Is the ability to create, change or delete sales orders, contracts and delivery schedules restricted to authorized personnel?					DSS05 DSS06
2.1.2 Has the ability to modify sales pricing information been restricted to authorized personnel? (Refer to master data integrity 1.3.1.)					DSS05 DSS06
2.1.3 Has the system been configured to limit the overwriting of prices compared to the price master data (SAP allows for no changes or a certain tolerance level)? Has the system been configured such that a sales order is blocked for further processing when the customer either gets too low a price or the price the sales person gives is not satisfactory? (Refer to master data integrity 1.1.2.)					DSS06
2.1.4 Are fax orders reconciled periodically between the system and fax printouts to reduce the risk of duplicate orders?					DSS01 DSS06
2.2 Sales orders are processed within approved customer credit limits.					
2.2.1 Has the SAP ERP software been configured to disallow the processing of sales orders that exceed customer credit limits?					DSS06
2.3 Order entry data are completely and accurately transferred to the shipping and invoicing activities.					

Revenue Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.3.1 Are reports of open sales documents prepared and monitored to check for timely shipment?					DSS01 MEA01
2.3.2 Are sales orders with the delivery block reviewed and monitored for timely shipment?					DSS01 MEA01
3. Shipping, Invoicing, Returns and Adjustments					
3.1 Controls are in place to prevent duplicate shipments or delay in the shipping of goods to customers.					
3.1.1 Does the SAP ERP software match goods shipped to open line items on an open sales order and close each line item as the goods are shipped, thereby preventing further shipments for those line items?					APO06 DSS01
3.1.2 Are available shipping reports used to assist in controlling the shipping process?					APO06 DSS01
3.2 Invoices are generated using authorized terms and prices and are accurately calculated and recorded.					
3.2.1 Does the SAP ERP software automatically calculate invoice amounts and post invoices based on configuration data?					DSS06
3.3 All goods shipped are invoiced in a timely manner.					
3.3.1 Are reports of goods shipped but not invoiced and uninvoiced debit and credit note requests prepared and investigated promptly?					APO13 DSS06

Revenue Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.3.2 Is the ability to create, change or delete picking slips, delivery notes and goods issues restricted to authorized personnel?					DSS05
3.3.3 Are reports of invoices issued but not posted in FI prepared and investigated promptly?					APO13 DSS06
3.4 Credit notes and adjustments to accounts receivable are accurately calculated and recorded.					
3.4.1 Is the ability to create, change or delete sales order return and credit requests and subsequent credit note transactions restricted to authorized personnel?					DSS05
3.5 Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with the enterprise's policy and in a timely manner.					
3.5.1 Are sales order returns and credit request transactions matched to invoices?					DSS01 DSS06
3.5.2 Have processing controls, including a billing block or a delivery block, been configured to block credit memos or free-of-charge subsequent delivery documents that do not comply with the enterprise's policy on credits or returns?					DSS06
4. Collecting and Processing Cash Receipts					
4.1 Cash receipts are entered accurately, completely and in a timely manner.					
4.1.1 Are bank statement reconciled to the GL regularly?					DSS01 DSS06
4.1.2 Has the system been configured to not allow processing of cash receipts outside of approved bank accounts?					DSS06

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
4.2 Cash receipts are valid and are not duplicated.					
4.2.1 Are receipts allocated to a customer's account supported by a remittance advice that cross-references to an invoice number? Is any unallocated cash or amount received that is not cross-referenced to an invoice number immediately followed up with the customer?					DSS01 DSS06
4.3 Cash discounts are calculated and recorded accurately.					
4.3.1 Have tolerance levels for allowable cash discounts and cash payment differences in the SAP ERP system been defined such that amounts in excess of such levels cannot be entered into the SAP ERP system?					APO12 DSS01 DSS06
4.4 Timely collection of cash receipts is monitored.					
4.4.1 Are customer open items and accounts receivable aging reports prepared and analyzed regularly?					APO12 DSS01 DSS06

SAP ERP

Expenditure Business Cycle
Audit/Assurance Program



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP ERP Expenditure Business Cycle Audit/Assurance Program* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP's kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: <http://www.isaca.org/sap-erp-4th-edition>
Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center
Follow ISACA on Twitter: <https://twitter.com/ISACANews>
Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOOfficial>
Like ISACA on Facebook: www.facebook.com/ISACAHQ

Acknowledgements

ISACA wishes to recognize

Project Leaders

Benjamin Fitts, CPA, Deloitte & Touche LLP, USA
Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA
Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA
Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Eva Sweet, CISA, CISM, ISACA, USA

Researchers

Syed Aamir Aarfi, Deloitte & Touche LLP, USA
Carlos Amaya, CISA, Deloitte & Touche LLP, USA
Dan Argynov, PMP, Deloitte & Touche LLP, USA
Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA
David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA
Ramamallikarjunaraao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA
Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA
Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA
Sagnik Mukherjee, Deloitte & Touche LLP, USA
Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA
Sonik Shah, Deloitte & Touche LLP, USA
Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA
Shweta Srivastava, Deloitte & Touche LLP, USA
Anurag Tewary, Deloitte & Touche LLP, USA
Percy Tsai, CPA, Deloitte & Touche LLP, USA
Ravi Maddela Veeriah, Deloitte & Touche LLP, USA
Sravan Vemana, Deloitte & Touche LLP, USA
Anukool Vyas, Deloitte & Touche LLP, USA

Expert Reviewers

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA
Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada
Mayank Garg, CISA, NetApp, USA
Ricci leong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Jim Koveos, CISA, MBA, AmerisourceBergen, USA
Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia
Samuel LIM S.C., CISA, Auditor General's Office, Singapore
Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia
Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General's Office, Singapore
Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia
Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia
Paul O'Donnell, Ernst & Young, Canada
Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico
John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US
Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico
Naved Rehman, CISA, CRISC, MS-IS, SAPauditCoach, US
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US
Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico
Jovari St. Victor, CISA, CPA, Sunera, LLC, US
Surapong Surabotsopon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,
KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico
Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand
David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President
Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cythus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK
Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil
Jotham Nyamari, CISA, Deloitte, USA
James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK
Gurvinder Singh, CISA, CISM, CRISC, Australia
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore
Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

SAP ERP Expenditure Business Cycle Audit/Assurance Program

Introduction

This document contains an example audit/assurance program, **based on** the generic structure developed in section 2B of *COBIT 5 for Assurance*¹.

The engagement approach is based on, but **differs slightly** from the generic approach described in *COBIT 5 for Assurance*:

- The engagement approach described in this audit/assurance program is **focused on a business process** consequently no group of COBIT 5 processes dominates as primary processes and the lower-level processes are widespread, for evaluation purposes, the high-level COBIT 5 processes will be used as references.
- The assurance steps in this audit/assurance program are specific to the subject matter under review; therefore most of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources availableprocess audit/assurance program.

Assurance Engagement: SAP ERP Expenditure Business Cycle

Assurance Topic

The topic covered by this assurance engagement is the SAP ERP Expenditure Business Cycle.

Business Impact and Risk

SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical processes.

Risk resulting from ineffective or incorrect configurations or use of SAP could result in some of the following:

- Disclosure of privileged information
- Single points of failure
- Low data quality
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements

Goal of the Review

The objective of the SAP ERP audit/assurance review is to provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise's SAP ERP architecture.

Scoping

The review will focus on configuration of the relevant SAP ERP components and modules within the enterprise. The selection of the specific components and modules will be based upon the risk introduced to the enterprise by these components and modules.

From a process reference model (PRM) perspective, the following domains and processes apply to this audit and assurance programme:

- BAI02 Manage requirements definition
- BAI03 Manage solution identification and build

¹ See www.isaca.org/COBIT/Pages/Assurance-product-page.aspx for more information on *COBIT 5 for Assurance*.

- DSS01 Manage operations
- DSS05 Manage security services
- DSS06 Manage business process controls

Minimum Audit Skills

This review is considered highly technical. The IS audit and assurance professional must have an understanding of SAP best practice processes and requirements and be highly conversant in SAP tools, exposures and functionality. It should not be assumed that an audit and assurance professional holding the CISA designation has the requisite skills to perform this review.

Testing SAP Security

To determine which users have access to the relevant authorizations used in this audit program, use one of the following methods:

1. Use transaction code SUIM → Users → Users by Complex Selection Criteria
2. Use transaction code S_BCE_68001417
3. Use transaction code SA38 and the program RSUSR002. This method allows the user to specify a transaction code, a “valid to” date for users, and up to three other authorization objects (which also may be the authorization object for transaction code S_TCODE) with associated values (two values under an AND relationship and three values under an OR relationship).
This method is generally sufficient for testing logical access security in relation to SAP ERP application infrastructure areas, but it is less suitable when large numbers of authorizations must be reviewed, such as in segregation of duties analysis and in some of the more complex areas of business cycle controls.
4. Use transaction code SUIM → Users → Users with Critical Authorizations (also accessible with program RSUSR008_009_NEW, which replaces programs RSUSR008 and RSUSR009 and transaction codes SU98 and/or SU99, for SAP Web AS 6.20 and later). This method offers improvements such as allowing differentiation between SAP defaults for critical data for different business areas, extended combination options for critical authorization data, improved performance, display of user filters and more analysis options for users in the result list.

Audit/Assurance Program for SAP ERP Expenditure Business Cycle					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
A-1	Determine the stakeholders of the assurance initiative and their stakes .				
A-1.1	<u>Identify</u> the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	Intended user(s) of the assurance report	<p>Board/audit committee: Needs assurance over the effectiveness and efficiency of SAP ERP processes within the enterprise.</p> <p>Chief financial officer (CFO): Needs assurance that internal controls for financial applications work as intended.</p> <p>Risk managers: Need assurance that controls intended to address previously identified risk are working as intended. The results from the audit should be used to update the risk registry as needed.</p> <p>Security managers: Need to identify gaps in the security plans for SAP applications.</p> <p>Owners / shareholders: Part or all of the SAP ERP assurance report may be included in statutory reporting.</p> <p>Regulators: Part or all of SAP ERP reporting may need to be disclosed to respective authorities</p>		
A-1.2	Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	Accountable and responsible parties for the subject matter	<p>Business executives: The individuals responsible for identifying requirements, approving design and managing performance. These people are, together with IT management, responsible for managing the correct and controlled use of SAP ERP services—in line with good practices.</p> <p>Business process owners: Responsible for defining application and technical requirements. Responsible for data classification.</p> <p>IT management: Responsible for managing the correct and controlled use of SAP ERP services—together with the business executives.</p>		
A-2	<u>Determine</u> the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities (i.e., not achieving the enterprise goals).		<p>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.</p> <p>Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.</p> <p>Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</p> <p>Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.</p>		
A-2.1	<u>Understand</u> the enterprise strategy and priorities.		<i>Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.</i>		

Audit/Accrual Program for SAP ERP Expenditure Business Cycle				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
A-2.2	<u>Understand</u> the internal context of the enterprise.	<p><i>Identify all internal environmental factors that could influence the performance and contents of the SAP ERP Expenditure Business Cycle.</i></p> <ul style="list-style-type: none"> • Review prior report, if one exists, verify completion of any agreed-on corrections, and note remaining deficiencies. Determine whether: <ul style="list-style-type: none"> – Senior management has assigned responsibilities for information, its processing, and its use – User management is responsible for providing information that supports the entity's objectives and policies – Information systems management is responsible for providing the capabilities necessary for the achievement of the defined information systems objectives and the policies of the entity – Senior management approves plans for development and acquisition of information systems – There are procedures to ensure that the information system being developed or acquired meets user requirements – There are procedures to ensure that information systems, programs, and configuration changes are tested adequately prior to implementation – All personnel involved in the system acquisition and configuration activities receive adequate training and supervision – There are procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards – User management participates in the conversion of data from the existing system to the new system – Final approval is obtained from user management prior to going live with a new information/upgraded system – There are procedures to document and schedule all changes to information systems (including key ABAP programs) – There are procedures to ensure that only authorized changes are initiated – There are procedures to ensure that only authorized, tested, and documented changes to information systems are accepted into the production client – There are procedures to allow for and control emergency changes – There are procedures for the approval, monitoring, and control of the acquisition and upgrade of hardware and systems software – There is a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated – The organizational structure, established by senior management, provides for an appropriate segregation of incompatible functions – The database, application, and presentation servers are located in a physically separate and protected environment (i.e., a data center) – Emergency, backup, and recovery plans are documented and tested on a regular basis to ensure that they remain current and operational – Backup and recovery plans allow users of information systems to resume operations in the event of an interruption – Application controls are designed with regard to any weaknesses in segregation, security, development, and processing controls that may affect the information system – Access to the Implementation Guide (IMG) during production has been restricted – The production client settings have been flagged to not allow changes to programs and 		

Audit/Assurance Program for SAP ERP Expenditure Business Cycle							
Phase A—Determine Scope of the Assurance Initiative							
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment		
		<p>configuration</p> <ul style="list-style-type: none"> • Identify the significant risk and determine the key controls <ul style="list-style-type: none"> - Develop a high-level process flow diagram and overall understanding of the Expenditure Business Cycle Module, including the following subprocesses: <ul style="list-style-type: none"> a. Master data maintenance b. Purchasing c. Invoice processing d. Processing disbursements - Assess the key risk, determine key controls or control weaknesses, and test controls (refer to the sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> a. The controls culture of the organization (e.g., a just-enough-control philosophy). b. The need to exercise judgment to determine the key controls in the process and whether the controls structure is adequate. (Any weaknesses in the control structure should be reported to executive management and resolved.) • Gain an understanding of the SAP ERP environment (The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles) <p>In particular, the following information is important:</p> <ul style="list-style-type: none"> - Version and release of SAP ERP implemented - Total number of named users (for comparison with logical access security testing results) - Number of SAP instances and clients - Accounting period, company codes, and chart of accounts - Identification of the components being used (Human Capital Management, Financials, Operations, Corporate Services) - Whether the organization has created any locally developed ABAP programs or reports - Details of the risk assessment approach taken in the organization to identify and prioritize risk - Copies of the organization's key security policies and standards <p>Obtain details of the following:</p> <ul style="list-style-type: none"> - Organizational Management Model as it relates to sales/revenue activity, i.e., sales organizational unit structure in SAP ERP and company sales organizational chart (required when evaluating the results of access security control testing) - An interview of the systems implementation team, if possible, and process design documentation for sales and distribution 					
A-2.3	<u>Understand</u> the external context of the enterprise.	<i>Identify all external environmental factors that could influence the performance and contents of the SAP ERP Expenditure Business Cycle.</i>					
A-2.4	Given the overall assurance objective, translate the identified strategic priorities into concrete <u>objectives</u> for the assurance engagement.	<p>The following goals are retained as key goals to be supported, in reflection of enterprise strategy and priorities:</p> <table border="1"> <tr> <td>Key goals</td><td>Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality </td></tr> </table>		Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality 		
Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality 						

Audit/Assurance Program for SAP ERP Expenditure Business Cycle					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
		<ul style="list-style-type: none"> • EG15 Compliance with internal policies <p>IT-related goals:</p> <ul style="list-style-type: none"> • ITG01 Alignment of IT and business strategy • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG09 IT Agility • ITG10 Security of information, processing infrastructure and applications • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG15 IT compliance with internal policies • ITG16 Competent and motivated business and IT personnel 			
		<p>Additional goals</p>			
A-2.5	Define the organizational boundaries of the assurance initiative.	<p><i>Describe the organizational boundaries of the assurance engagement, i.e., to which organizational entities the review is limited. All other aspects of scope limitation are identified during phase A-3.</i></p> <ul style="list-style-type: none"> • The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment. • Obtain information and form an understanding of the business reasons underlying the audit. • Identify the senior business resources responsible for the review. • Identify the senior IT audit/assurance resource responsible for the review. • Establish the process for suggesting and implementing changes to the audit/assurance program, and list the authorizations required. • Identify any limitations and/or constraints affecting the audit of specific systems and subsystems. • Identify and third party services, applications, platforms and infrastructure elements that may not be or only partially be accessible. • Identify any legal, regulatory or contractual constraints on audit. • Identify any industrial relations based or end user based audit constraints. 			

Audit/Accurance Program for SAP ERP Expenditure Business Cycle								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
A-3	Determine the enablers in scope and the instance(s) of the enablers in scope.	COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.						
A-3.1	<u>Define the Principles, Policies and Frameworks</u> in scope.	<p>Guiding principles and policies include:</p> <ul style="list-style-type: none"> • Policy for Master Data Maintenance • ISMS policy • Legal and regulatory compliance requirements 						
A-3.2	<p><u>Define which Processes</u> are in scope of the review.</p> <p>Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of process goals • Application of process good practices • Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments) 	<p><i>COBIT 5: Enabling Processes</i> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed.</p> <table border="1"> <tr> <td>Key processes</td><td> <ul style="list-style-type: none"> • Master data maintenance • Purchasing • Invoice processing • Processing disbursements </td></tr> <tr> <td>Additional processes</td><td> <ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance </td></tr> </table>	Key processes	<ul style="list-style-type: none"> • Master data maintenance • Purchasing • Invoice processing • Processing disbursements 	Additional processes	<ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance 		
Key processes	<ul style="list-style-type: none"> • Master data maintenance • Purchasing • Invoice processing • Processing disbursements 							
Additional processes	<ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance 							
A-3.3	<p><u>Define which Organisational Structures</u> will be in scope.</p> <p>Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of Organisational Structure goals, i.e., decisions • Application of Organisational Structures good practices 	<p>Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail.</p> <table border="1"> <tr> <td>Key Organisational Structures</td><td> <ul style="list-style-type: none"> • Purchasing • Accounts payable • Warehouse • Receiving • Accounting • Quality (QA) </td></tr> <tr> <td>Additional Organisational Structures</td><td> <ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Tax department • Change Management Office </td></tr> </table>	Key Organisational Structures	<ul style="list-style-type: none"> • Purchasing • Accounts payable • Warehouse • Receiving • Accounting • Quality (QA) 	Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Tax department • Change Management Office 		
Key Organisational Structures	<ul style="list-style-type: none"> • Purchasing • Accounts payable • Warehouse • Receiving • Accounting • Quality (QA) 							
Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Tax department • Change Management Office 							

Audit/Accrual Program for SAP ERP Expenditure Business Cycle								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
A-3.4	<u>Define the Culture, Ethics and Behaviour</u> aspects in scope.	<p>In the context of this engagement, the following enterprise-wide culture and behaviours are in scope:</p> <ul style="list-style-type: none"> • Risk and compliance aware culture • Enabling of continuous improvement • Accountability • Discipline to follow instructions 						
A-3.5	<u>Define the Information items</u> in scope. Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of Information goals, i.e., quality criteria of the information items • Application of Information good practices (Information attributes) 	<p>Based on the subject matter of this audit/assurance program, the following Information items have been identified as key items.</p> <table border="1"> <tr> <td>Key Information Items</td><td> <ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids </td></tr> <tr> <td>Additional Information Items</td><td> <ul style="list-style-type: none"> • Organizational charts </td></tr> </table>	Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 	Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 		
Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 							
Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 							
A-3.6	<u>Define the Services, Infrastructure and Applications</u> in scope.	<p>In the context of this assignment, and taking into account the goals identified in A-2.4, the following services and related applications or infrastructure could be considered in scope of the review:</p> <ul style="list-style-type: none"> • Master data maintenance group • SAP ERP System • Change management • SAP training 						
A-3.7	<u>Define the People, Skills and Competencies</u> in scope. Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of skills set goals • Application of skills set and competencies good practices 	<p>In the context of this engagement, taking into account key processes and key roles, the following skill sets are included in scope:</p> <ul style="list-style-type: none"> • Proficiency using the SAP Purchasing, Accounts Payable, Returns and Credit notes functionality • Master data management skills • Expenditure skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 						

Audit/Accrual Program for SAP ERP Expenditure Business Cycle																											
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference																							
B-1	Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.																										
B-1.1	<p>Obtain (and agree on) metrics for enterprise goals and expected values of the metrics. Assess whether enterprise goals in scope are achieved.</p> <p>Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.</p> <p>Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</p> <p>The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>Enterprise Goal</th> <th>Metric</th> <th>Expected Outcome (Ex)</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>EG03 Managed business risk (safeguarding of assets)</td> <td> <ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG04 Compliance with external laws and regulations</td> <td> <ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG07 Business service continuity and availability</td> <td> <ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG11 Optimisation of business process functionality</td> <td> <ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG15 Compliance with internal policies</td> <td> <ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>	Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step	EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG04 Compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG04 Compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
B-1.2	<p>Obtain (and agree on) metrics for IT-related goals and expected values of the metrics and assess whether IT-related goals in scope are achieved.</p> <p>The following metrics and expected values are agreed on for the key IT-related goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>IT-related Goal</th> <th>Metric</th> <th>Expected Outcome (Ex)</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>ITG01 Alignment of IT</td> <td> <ul style="list-style-type: none"> Percent of enterprise strategic goals and </td> <td>Agree on the expected values for the</td> <td>In this step, the related metrics for</td> </tr> </tbody> </table>			IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step	ITG01 Alignment of IT	<ul style="list-style-type: none"> Percent of enterprise strategic goals and 	Agree on the expected values for the	In this step, the related metrics for																
IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
ITG01 Alignment of IT	<ul style="list-style-type: none"> Percent of enterprise strategic goals and 	Agree on the expected values for the	In this step, the related metrics for																								

Audit/Assurance Program for SAP ERP Expenditure Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	and business strategy	<ul style="list-style-type: none"> requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services Percent of IT value drivers mapped to business value drivers 	<i>IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment Number of non-compliance issues relating to contractual agreements with IT service providers Coverage of compliance assessments 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG04 Managed IT-related business risk	<ul style="list-style-type: none"> Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent of enterprise risk assessments including IT-related risk Frequency of update of risk profile 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG08 Adequate use of applications, information and technology solutions	<ul style="list-style-type: none"> Percent of business process owners satisfied with supporting IT products and services Level of business user understanding of how technology solutions support their processes Satisfaction level of business users with training and user manuals Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG09 IT Agility	<ul style="list-style-type: none"> Level of satisfaction of business executives with IT's responsiveness to new requirements 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether</i>	

Audit/Assurance Program for SAP ERP Expenditure Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> Number of critical business processes supported by up-to-date infrastructure and applications Average time to turn strategic IT objectives into an agreed-on and approved initiative 	<i>will take place.</i>	<i>the defined criteria are achieved.</i>	
ITG10 Security of information, processing infrastructure and applications	<ul style="list-style-type: none"> Number of security incidents causing financial loss, business disruption or public embarrassment Number of IT services with outstanding security requirements Time to grant, change and remove access privileges, compared to agreed-on service levels Frequency of security assessment against latest standards and guidelines 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
ITG12 Enablement and support of business processes by integrating applications and technology into business processes	<ul style="list-style-type: none"> Number of business processing incidents caused by technology integration errors Number of business process changes that need to be delayed or reworked because of technology integration issues Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues Number of applications or critical infrastructures operating in silos and not integrated 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
ITG14 Availability of reliable and useful information for decision making	<ul style="list-style-type: none"> Level of business user satisfaction with quality and timeliness (or availability) of management information Number of business process incidents caused by non-availability of information Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
ITG15 IT compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices Frequency of policies review and update 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
ITG16 Competent and motivated business and IT personnel	<ul style="list-style-type: none"> Percent of staff whose IT-related skills are sufficient for the competency required for their role Percent of staff satisfied with their IT-related roles 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		

Audit/Assurance Program for SAP ERP Expenditure Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	• Number of learning/training hours per staff member				

Audit/Accrual Program for SAP ERP Expenditure Business Cycle

Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks

Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-2	Obtain an understanding of the Principles, Policies and Frameworks in scope and set suitable assessment criteria. Assess Principles, Policies and Frameworks.		
Principles, policies and frameworks: Policy for Master Data Maintenance			
B-2.1a	<u>Understand the Principles, Policies and Frameworks context.</u> <i>Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks</i>		
B-2.2a	<u>Understand the stakeholders of the Principles, Policies and Frameworks.</u> <i>Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.</i>		
B-2.3a	<u>Understand the goals for the Principles, Policies and Frameworks</u> , and the related metrics and agree on expected values. Assess whether the Principles, Policies and Frameworks goals (outcomes) are achieved, i.e., assess the effectiveness of the Principles, Policies and Frameworks . Goal: The organization has defined, disseminated and deployed management policies supporting SAP master data maintenance .	Perform the assurance steps using the example criteria described below.	
Goal	Criteria	Assessment Step	
Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.	
Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> • A regular validation of all policies whether they are still up to date • An indication of the policies' expiration date or date of last update 	Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> • A regular validation of all policies whether they are still up to date • An indication of the policies' expiration date or date of last update 	
Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.	
Availability	<ul style="list-style-type: none"> • Policies are available to all stakeholders. • Policies are easy to navigate and have a logical and hierarchical structure. 	<ul style="list-style-type: none"> • Verify that policies are available to all stakeholders. • Verify that policies are easy to navigate and have a logical and hierarchical structure. 	
B-2.4a	<u>Understand the life cycle stages of the Principles, Policies and Frameworks</u> , and agree on the relevant criteria. Assess to what extent the Principles, Policies and Frameworks life cycle is managed. <i>The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01 Manage the IT management framework.</i>		
B-2.5a	<u>Understand good practices related to the Principles, Policies and Frameworks</u> and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. <i>The assurance professional will, by using appropriate auditing techniques assess the following aspects.</i>		
Good Practice	Criteria	Assessment Step	
Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.	
Exception and escalation	<ul style="list-style-type: none"> • The exception and escalation procedure is explained and commonly known. • The exception and escalation procedure has not become the de facto standard procedure. 	<ul style="list-style-type: none"> • Verify that the exception and escalation procedure is described, explained and commonly known. • Through observation of a representative sample, verify that the exception and escalation procedure has not become de 	

Audit/Assurance Program for SAP ERP Expenditure Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
	Compliance	The compliance checking mechanism and non-compliance consequences are clearly described and enforced.	facto standard procedure. Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.	
B-2.1 to B-2.5	Repeat steps B-2.1 through B-2.5 for all remaining Principles, Policies and Frameworks in scope. Repeat the steps described above for the remaining Principles, Policies and Frameworks: <ul style="list-style-type: none">• ISMS policy• Legal and regulatory compliance requirements			

Audit/Accurance Program for SAP ERP Expenditure Business Cycle															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes															
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment										
B-3	Obtain understanding of the Processes in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes.														
SAP ERP Expenditure process²: Master data maintenance															
B-3.1a	<u>Understand the Process context.</u>														
B-3.2a	<u>Understand the Process purpose.</u>														
B-3.3a	<u>Understand all process stakeholders</u> and their roles. This is equivalent to understanding the real RACI chart of the process. <i>Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.</i>														
	The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement:														
Master data maintenance stakeholders:															
B-3.4a	<u>Understand the Process goals</u> and related metrics³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.														
The Process Master data maintenance has two defined process goal.		The following activities can be performed to assess whether the goals are achieved.													
<table border="1"> <thead> <tr> <th>Process Goal</th> <th>Related Metrics</th> <th>Criteria/Expected Value</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Master data records are valid, complete, accurate and timely.</td> <td><i>Determine the metrics that can be used to assess the achievement of the Process goals.</i></td> <td><i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i></td> <td><i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i></td> </tr> <tr> <td>Inventory master data remains current and pertinent.</td> <td><i>Determine the metrics that can be used to assess the achievement of the Process goals.</i></td> <td><i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i></td> <td><i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i></td> </tr> </tbody> </table>			Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	Master data records are valid, complete, accurate and timely.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	Inventory master data remains current and pertinent.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step												
Master data records are valid, complete, accurate and timely.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>												
Inventory master data remains current and pertinent.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>												
B-3.5a	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement: Define and agree on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.) Agree on the process practices that should be in place (process design). <u>Assess</u> the process design , i.e., assess to what extent: <ul style="list-style-type: none"> • Expected process practices are applied. • Accountability and responsibility are assigned and assumed. 														
	COBIT 5 Processes⁴ are described in <i>COBIT 5: Enabling Processes</i> . Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are: <ul style="list-style-type: none"> • A sound process design 														

² Because this is a business process audit/assurance program, several of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources available.

³ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

⁴ For this audit/assurance program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the SAP ERP Expenditure Business Cycle processes in scope.

Audit/Assurance Program for SAP ERP Expenditure Business Cycle																										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																										
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																				
	<ul style="list-style-type: none"> The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented. 																									
	Reference Process	Master data maintenance	<p>Criteria:</p> <p>1.1 Changes made to master data are valid, complete, accurate and timely. 1.2 Master data remains current and pertinent.</p>																							
	Reference Process Practices ⁵	Good Practice	<p style="text-align: center;">Assessment Step</p>																							
	DSS01 DSS06	Changes made to master data are valid, complete, accurate and timely.	<p>1.1.1 On a sample basis, review standard reports and transactions against authorized source documents to assess the accuracy and timeliness of change maintenance applied to master data records. The transaction code S_ALR_87010039—Display Changes to Vendors (also accessible through transaction code SA38—ABAP Reporting and program RFKABL00) can be used to produce a list of the changes made to selected vendor master records. Review a sample of changes to vendor master records for the appropriateness of the changes and compare back to source documents for accuracy.</p> <p>Determine whether any sensitive fields are defined to require approval by a user ID other than the one initiating the change. To review fields configured for dual control, use transaction code SPRO to display the IMG menu and follow the path: Financial Accounting (New) → Accounts Receivables & Accounts Payables → Vendor Accounts→ Master Data → Preparation for Creating Master Data-Define Sensitive Fields for Dual Control (Vendors).</p>																							
	DSS06	Changes made to master data are valid, complete, accurate and timely.	<p>1.1.2 Review the enterprise policy and process design specifications regarding access to maintain master data. Test user access to transactions to create and maintain vendor master data (note that data can be maintained from finance, purchasing or centrally).</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Task</th><th style="text-align: center;">Finance</th><th style="text-align: center;">Purchasing</th><th style="text-align: center;">Centrally</th></tr> </thead> <tbody> <tr> <td>Create Vendor</td><td style="text-align: center;">FK01</td><td style="text-align: center;">MK01</td><td style="text-align: center;">KK01</td></tr> <tr> <td>Change Vendor</td><td style="text-align: center;">FK02</td><td style="text-align: center;">MK02</td><td style="text-align: center;">KK02</td></tr> <tr> <td>Block/Unblock Vendor</td><td style="text-align: center;">FK05</td><td style="text-align: center;">MK05</td><td style="text-align: center;">KK05</td></tr> <tr> <td>Mark Vendor for Deletion</td><td style="text-align: center;">FK06</td><td style="text-align: center;">MK06</td><td style="text-align: center;">KK06</td></tr> </tbody> </table> <p>Proper enforcement of a segregation of duties strategy improves controls surrounding master data maintenance. Use transaction code SUIM—User Information System to test user access to transactions to maintain vendor pricing information:</p> <ul style="list-style-type: none"> • Create Purchase Information Record—ME11 • Change Purchase Information Record—ME12 • Flag Information Record for Deletion—ME15 • Create Condition—MEK1 • Change Condition—MEK2 				Task	Finance	Purchasing	Centrally	Create Vendor	FK01	MK01	KK01	Change Vendor	FK02	MK02	KK02	Block/Unblock Vendor	FK05	MK05	KK05	Mark Vendor for Deletion	FK06	MK06	KK06
Task	Finance	Purchasing	Centrally																							
Create Vendor	FK01	MK01	KK01																							
Change Vendor	FK02	MK02	KK02																							
Block/Unblock Vendor	FK05	MK05	KK05																							
Mark Vendor for Deletion	FK06	MK06	KK06																							

⁵ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Expenditure Business Cycle audit/assurance program.

Audit/Accurance Program for SAP ERP Expenditure Business Cycle																																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																	
Ref.	Assurance Steps and Guidance					Issue Cross-reference	Comment																										
			<ul style="list-style-type: none"> Create Condition With Reference—MEK4 <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>ME11— Create Purchase Information Record</td><td>M_EINF_EKG M_EINF_EKO M_EINF_WRK V_KOND_VEA V_KONH_EKO V_KONH_VKS</td><td>ACTVT ACTVT ACTVT ACTVT ACTVT ACTVT</td><td>01 01 01 01 01 01</td></tr> <tr> <td>ME12— Change Purchase Information Record</td><td>M_EINF_EKG M_EINF_EKO M_EINF_WRK V_KOND_VEA V_KONH_EKO V_KONH_VKS</td><td>ACTVT ACTVT ACTVT ACTVT ACTVT ACTVT</td><td>02 02 02 02 02 02</td></tr> <tr> <td>ME15— Flag Information Record for Deletion</td><td>M_EINF_EKG M_EINF_EKO M_EINF_WRK</td><td>ACTVT ACTVT ACTVT</td><td>06 06 06</td></tr> <tr> <td>MEK1— Create Condition</td><td>V_KOND_VEA V_KONH_EKO V_KONH_VKS</td><td>ACTVT ACTVT ACTVT</td><td>01 01 01</td></tr> <tr> <td>MEK2— Change Condition</td><td>V_KOND_VEA V_KONH_EKO V_KONH_VKS</td><td>ACTVT ACTVT ACTVT</td><td>02 02 02</td></tr> <tr> <td>MEK4— Create Condition With Reference</td><td>V_KONH_EKO V_KONH_VKS</td><td>ACTVT ACTVT</td><td>01, 02 01, 02</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	ME11— Create Purchase Information Record	M_EINF_EKG M_EINF_EKO M_EINF_WRK V_KOND_VEA V_KONH_EKO V_KONH_VKS	ACTVT ACTVT ACTVT ACTVT ACTVT ACTVT	01 01 01 01 01 01	ME12— Change Purchase Information Record	M_EINF_EKG M_EINF_EKO M_EINF_WRK V_KOND_VEA V_KONH_EKO V_KONH_VKS	ACTVT ACTVT ACTVT ACTVT ACTVT ACTVT	02 02 02 02 02 02	ME15— Flag Information Record for Deletion	M_EINF_EKG M_EINF_EKO M_EINF_WRK	ACTVT ACTVT ACTVT	06 06 06	MEK1— Create Condition	V_KOND_VEA V_KONH_EKO V_KONH_VKS	ACTVT ACTVT ACTVT	01 01 01	MEK2— Change Condition	V_KOND_VEA V_KONH_EKO V_KONH_VKS	ACTVT ACTVT ACTVT	02 02 02	MEK4— Create Condition With Reference	V_KONH_EKO V_KONH_VKS	ACTVT ACTVT	01, 02 01, 02		
Transaction(s)	Authorization Objects	Fields	Values																														
ME11— Create Purchase Information Record	M_EINF_EKG M_EINF_EKO M_EINF_WRK V_KOND_VEA V_KONH_EKO V_KONH_VKS	ACTVT ACTVT ACTVT ACTVT ACTVT ACTVT	01 01 01 01 01 01																														
ME12— Change Purchase Information Record	M_EINF_EKG M_EINF_EKO M_EINF_WRK V_KOND_VEA V_KONH_EKO V_KONH_VKS	ACTVT ACTVT ACTVT ACTVT ACTVT ACTVT	02 02 02 02 02 02																														
ME15— Flag Information Record for Deletion	M_EINF_EKG M_EINF_EKO M_EINF_WRK	ACTVT ACTVT ACTVT	06 06 06																														
MEK1— Create Condition	V_KOND_VEA V_KONH_EKO V_KONH_VKS	ACTVT ACTVT ACTVT	01 01 01																														
MEK2— Change Condition	V_KOND_VEA V_KONH_EKO V_KONH_VKS	ACTVT ACTVT ACTVT	02 02 02																														
MEK4— Create Condition With Reference	V_KONH_EKO V_KONH_VKS	ACTVT ACTVT	01, 02 01, 02																														
DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.3 Determine whether the configurable control settings for vendor account groups address the risk pertaining to the validity, completeness and accuracy of master data and whether the settings have been set in accordance with management's intentions. View the settings online using the IMG as follows: Execute transaction code OBD3—C FI Maintain Table T077K and ascertain whether account groups have been set up covering one-time vendor or other vendor accounts. For high-risk account groups such as one-time vendors, check whether authorization has been marked as a required field. Determine whether these																															

Audit/Accurance Program for SAP ERP Expenditure Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.6a			settings are consistent with management's intentions.		
	APO10 DSS01	Changes made to master data are valid, complete, accurate and timely.	1.1.4 Extract a list of vendor account names from table LFA1 using transaction code SE16N—General Table Display (fields: NAME1 for the name, LIFNR for the vendor number). Review a sample for compliance with the enterprise's naming convention. View or search the list (using scan search software tools, if available) for potential duplicates.		
	DSS01 DSS06	Master data remains current and pertinent.	1.2.1 Using transaction code F.40—A/P: Account List (also accessible using transaction code SA38—ABAP Reports and program RFKKVZ00), determine whether the appropriate management report displays or produces a list of vendors. Confirm evidence of management's review of the data on a rotating basis for ongoing pertinence.		
B-3.6a	<u>Agree on the process work products</u> ⁶ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.				
	Process Master data maintenance inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.	
	Process Practice	Work Products	Assessment Step		
B-3.7a	Master data maintenance	<ul style="list-style-type: none"> Master data add/change/delete request forms Master data maintenance procedures Master data maintenance reports List of SAP users with master data access 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		
	<u>Agree on the process capability level</u> to be achieved by the process.				
	<i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				
SAP ERP Expenditure process: Purchasing					
B-3.1b	<u>Understand the Process context.</u>				
B-3.2b	<u>Understand the Process purpose.</u>				
B-3.3b	<u>Understand all process stakeholders</u> and their roles.				
	Purchasing stakeholders:				
B-3.4b	Understand the <u>Process goals</u> and related <u>metrics</u> ⁷ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.				
	The Process Purchasing has three defined process goals.		The following activities can be performed to assess whether the goals are achieved.		
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	
	Purchase order entry and changes are valid, complete, accurate and timely.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
Goods are received only for valid		Determine the metrics that can be	Agree on the expected values for	In this step, the related metrics for	

⁶ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

⁷ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Expenditure Business Cycle																																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																	
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																											
B-3.5b	purchase orders and goods receipts are recorded completely, accurately and in a timely manner.	used to assess the achievement of the Process goals.	the Process goal metrics, i.e., the values against which the assessment will take place.	each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																													
	Defective goods are returned to suppliers in a timely manner.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																													
<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement:																																	
DSS05 DSS06	Reference Process	Purchasing	Criteria: 2.1 Purchase order entry and changes are valid, complete, accurate and timely. 2.2 Goods are received only for valid purchase orders and goods receipts are recorded completely, accurately and in a timely manner. 2.3 Defective goods are returned to suppliers in a timely manner.																														
	Reference Process Practices ⁸	Good Practice	Assessment Step			Issue Cross-reference																											
			2.1.1 Review the enterprise policy and process design specifications regarding access to transactions for PRs and POs. Use transaction code SUIM—User Information System to test user access to: <ul style="list-style-type: none">• Create PR—ME51 or ME51N• Change PR—ME52 or ME52N• Release PR—ME54 or ME54N• Collective Release of PR—ME55	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>ME51/ME51N— Create PR</td><td>M_BANF_BSA</td><td>ACTVT</td><td>01</td></tr> <tr> <td></td><td>M_BANF_EKG</td><td>ACTVT</td><td>01</td></tr> <tr> <td></td><td>M_BANF_EKO</td><td>ACTVT</td><td>01</td></tr> <tr> <td></td><td>M_BANF_WRK</td><td>ACTVT</td><td>01</td></tr> </tbody> </table> <p>Also test user access to transactions ME52/ME52N, ME54/ME54N and ME55/ME55N with the same authorization objects as above, but with ACTVT field values of 02, 03 and 08, respectively.</p> <ul style="list-style-type: none">• Create PO, Vendor Known—ME21 or ME21N• Change PO—ME22 or ME22N <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>ME21/ME21N—Create PO,</td><td>M_BEST_BSA</td><td>ACTVT</td><td>01</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	ME51/ME51N— Create PR	M_BANF_BSA	ACTVT	01		M_BANF_EKG	ACTVT	01		M_BANF_EKO	ACTVT	01		M_BANF_WRK	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values	ME21/ME21N—Create PO,	M_BEST_BSA	ACTVT	01	
Transaction(s)	Authorization Objects	Fields	Values																														
ME51/ME51N— Create PR	M_BANF_BSA	ACTVT	01																														
	M_BANF_EKG	ACTVT	01																														
	M_BANF_EKO	ACTVT	01																														
	M_BANF_WRK	ACTVT	01																														
Transaction(s)	Authorization Objects	Fields	Values																														
ME21/ME21N—Create PO,	M_BEST_BSA	ACTVT	01																														

⁸ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Expenditure Business Cycle audit/assurance program.

Audit/Accuracy Program for SAP ERP Expenditure Business Cycle																																									
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																									
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment																																	
			<table border="1"> <tr> <td>Vendor Known</td> <td>M_BEST_EKG</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>M_BEST_EKO</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>M_BANF_WRK</td> <td>ACTVT</td> <td>01</td> </tr> </table> <p>Also test user access to transactions ME22/ME22N with the same authorization objects as above, but with ACTVT field value of 02.</p> <ul style="list-style-type: none"> • Maintain PO Supplement—ME24 • Create PO, Vendor Unknown—ME25 • Create Stock Transport Order—ME27 <table border="1"> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> <tr> <td>ME24/ME24N—Maintain PO Supplement</td> <td>M_RAHM_BSA M_RAHM_EKO</td> <td>ACTVT</td> <td>01 01</td> </tr> </table> <p>Also test user access to transactions ME25/ME25N and ME27 with the same authorization objects as above, but with ACTVT field values of 01 and 09, respectively.</p> <ul style="list-style-type: none"> • Create Outline Purchase Agreement—ME31 <table border="1"> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> <tr> <td>ME31—Create Outline Purchase Agreement</td> <td>M_RAHM_BSA M_RAHM_EKG M_RAHM_EKO</td> <td>ACTVT</td> <td>02 02 02</td> </tr> </table> <ul style="list-style-type: none"> • Change Outline Agreement—ME32 • Maintain Outline Agreement Supplement—ME34 <table border="1"> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> <tr> <td>ME32— Change Outline Agreement ME34— Maintain Outline Agreement Supplement</td> <td>M_RAHM_BSA M_RAHM_EKO</td> <td>ACTVT</td> <td>02 02</td> </tr> </table>	Vendor Known	M_BEST_EKG	ACTVT	01		M_BEST_EKO	ACTVT	01		M_BANF_WRK	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values	ME24/ME24N—Maintain PO Supplement	M_RAHM_BSA M_RAHM_EKO	ACTVT	01 01	Transaction(s)	Authorization Objects	Fields	Values	ME31—Create Outline Purchase Agreement	M_RAHM_BSA M_RAHM_EKG M_RAHM_EKO	ACTVT	02 02 02	Transaction(s)	Authorization Objects	Fields	Values	ME32— Change Outline Agreement ME34— Maintain Outline Agreement Supplement	M_RAHM_BSA M_RAHM_EKO	ACTVT	02 02		
Vendor Known	M_BEST_EKG	ACTVT	01																																						
	M_BEST_EKO	ACTVT	01																																						
	M_BANF_WRK	ACTVT	01																																						
Transaction(s)	Authorization Objects	Fields	Values																																						
ME24/ME24N—Maintain PO Supplement	M_RAHM_BSA M_RAHM_EKO	ACTVT	01 01																																						
Transaction(s)	Authorization Objects	Fields	Values																																						
ME31—Create Outline Purchase Agreement	M_RAHM_BSA M_RAHM_EKG M_RAHM_EKO	ACTVT	02 02 02																																						
Transaction(s)	Authorization Objects	Fields	Values																																						
ME32— Change Outline Agreement ME34— Maintain Outline Agreement Supplement	M_RAHM_BSA M_RAHM_EKO	ACTVT	02 02																																						
APO10 DSS01	Purchase order entry and changes are valid, complete, accurate and timely.	2.1.2 Through discussions with management, determine the (types of) materials for which source lists should be available in the system. Also, determine materials for which a source list should not be present. Examine a selection of materials and ask to see the corresponding																																							

Audit/Accuracy Program for SAP ERP Expenditure Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
			<p>source list to corroborate the performance of the control activity in the appropriate accounting period. Transaction code ME06— Analyze Source List can be used to create reports on all material items and whether they belong to a source list. Transaction code ME0M— Source List for Material indicates all material items and any associated vendors (including historic data). To use ME0M, a material or a range of materials must be specified. Click on the Select the Material By Material Group tab to get a list of materials. Select the sample of orders and check against source list reports to determine whether specific materials have been procured with unlisted vendors.</p>		
DSS06	Purchase order entry and changes are valid, complete, accurate and timely.	2.1.3 Obtain a sufficient understanding of the system configuration to assess the adequacy of the release strategy as defined and implemented by the enterprise as well as the functioning and effectiveness of established policies, procedures, standards and guidance. View the settings online using the IMG as follows:	<ul style="list-style-type: none"> • Release Procedure POs—Use transaction code SPRO to display the IMG menu and follow the path: Materials Management → Purchasing → Purchase Order → Release Procedure for Purchase Orders→ Define Release Procedure for Purchase Orders • Release Procedure for Purchase Requisitions (with classification)— Use transaction code SPRO to display the IMG menu and follow the path: Material Management → Purchasing → Purchase Requisitions → Release Procedure → Procedure With Classification → Set Up Procedure With Classification <ul style="list-style-type: none"> - Select the Release Strategy option. Select the strategies one by one by double-clicking on the strategy. Note the release codes that are shown; authorization (authorization objects M_BANF_FRG and M_EINK_FRG) for these release codes should be checked. - Click on the Classification button. This will show the conditions under which the purchase document will be blocked. Ascertain whether these conditions comply with management's intentions. • Release Procedure PRs (without classification)—Use transaction code SPRO to display the IMG menu and follow the path: Material Management → Purchasing → Purchase Requisitions → Release Procedure → Set Up Procedure Without Classification <ul style="list-style-type: none"> - Select the Release Points Prerequisites option. Note the release codes that are shown; authorization for these release codes should be checked. Go back to the previous screen and select the Determination of Release Strategy option. This will show the conditions under which the purchase document will be blocked. Ascertain whether these conditions comply with management's intentions. • Use transaction code SUIM—User Information System to test user access to transactions for release strategies: <ul style="list-style-type: none"> - Release (Approve) Purchasing Order—ME28 or ME29N - Release (Approve) Outline Agreement—ME35 - Release (Approve) Scheduling Agreement—ME35L - Release (Approve) Contract—ME35K - Release PR—ME54/ME54N - Collective Release of PRs—ME55 		
DSS06	Goods are received only for valid purchase orders and goods receipts are recorded completely, accurately and in a timely manner.	2.2.1 Run the transaction code VL10B—Purchase Orders Due for Delivery (also accessible using transaction code SA38—ABAP Reporting and program RM06EM00) to produce a listing of outstanding POs. Ascertain from management whether there are reasons for any long outstanding items on the report.			
DSS05	Goods are received only for valid	2.2.2 Use transaction code SUIM—User Information System to test user access to transactions			

Audit/Accuracy Program for SAP ERP Expenditure Business Cycle																																																									
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																									
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																																																			
	DSS06	purchase orders and goods receipts are recorded completely, accurately and in a timely manner.	<p>for GR:</p> <ul style="list-style-type: none"> • Post Goods Receipt for PO—MB01 • Goods movement—MIGO • Post Goods Receipt for PO Unknown—MB0A • Goods Movement (MM)—MIGO_GO • Goods Movement (Inventory Mgt.)—MIGO_GI • Transfer Posting—MIGO_TR • GR for Production Order—MB31 • Other Goods Receipts—MB1C • Cancel Material Document—MBST <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>MB01— Post Goods Receipt for PO</td><td>M_MSEG_BWE</td><td>ACTVT</td><td>01</td></tr> <tr> <td>MB0A— Post Goods Receipt for PO Unknown</td><td>M_MSEG_WWE</td><td>ACTVT</td><td>01</td></tr> <tr> <td>MIGO— Goods movement</td><td></td><td></td><td></td></tr> <tr> <td>MIGO_GO— Goods Movement (MM)</td><td></td><td></td><td></td></tr> <tr> <td>MB31— GR for Production Order</td><td>M_RAHM_BSA</td><td>ACTVT</td><td>01</td></tr> <tr> <td></td><td>M_RAHM_EKO</td><td>ACTVT</td><td>01</td></tr> <tr> <td>MB1C— Other Goods Receipts</td><td>M_MSEG_BWA</td><td>ACTVT</td><td>01</td></tr> <tr> <td></td><td>M_MSEG_BWE</td><td>ACTVT</td><td>01</td></tr> <tr> <td></td><td>M_MSEG_WWA</td><td>ACTVT</td><td>01</td></tr> <tr> <td>MBST— Cancel Material Document</td><td>M_MSEG_BMB</td><td>ACTVT</td><td>01</td></tr> <tr> <td>MIGO_GI— Goods Movement (Inventory Mgt.)</td><td>M_MSEG_WMB</td><td>ACTVT</td><td>01</td></tr> <tr> <td>MIGO_TR— Transfer Posting</td><td></td><td></td><td></td></tr> </tbody> </table> <p>Test user access to high-risk movement types 561 through 566. These special movement types reflect the initial stock entry in the SAP ERP system at the time of conversion to the SAP ERP system.</p>	Transaction(s)	Authorization Objects	Fields	Values	MB01— Post Goods Receipt for PO	M_MSEG_BWE	ACTVT	01	MB0A— Post Goods Receipt for PO Unknown	M_MSEG_WWE	ACTVT	01	MIGO— Goods movement				MIGO_GO— Goods Movement (MM)				MB31— GR for Production Order	M_RAHM_BSA	ACTVT	01		M_RAHM_EKO	ACTVT	01	MB1C— Other Goods Receipts	M_MSEG_BWA	ACTVT	01		M_MSEG_BWE	ACTVT	01		M_MSEG_WWA	ACTVT	01	MBST— Cancel Material Document	M_MSEG_BMB	ACTVT	01	MIGO_GI— Goods Movement (Inventory Mgt.)	M_MSEG_WMB	ACTVT	01	MIGO_TR— Transfer Posting					
Transaction(s)	Authorization Objects	Fields	Values																																																						
MB01— Post Goods Receipt for PO	M_MSEG_BWE	ACTVT	01																																																						
MB0A— Post Goods Receipt for PO Unknown	M_MSEG_WWE	ACTVT	01																																																						
MIGO— Goods movement																																																									
MIGO_GO— Goods Movement (MM)																																																									
MB31— GR for Production Order	M_RAHM_BSA	ACTVT	01																																																						
	M_RAHM_EKO	ACTVT	01																																																						
MB1C— Other Goods Receipts	M_MSEG_BWA	ACTVT	01																																																						
	M_MSEG_BWE	ACTVT	01																																																						
	M_MSEG_WWA	ACTVT	01																																																						
MBST— Cancel Material Document	M_MSEG_BMB	ACTVT	01																																																						
MIGO_GI— Goods Movement (Inventory Mgt.)	M_MSEG_WMB	ACTVT	01																																																						
MIGO_TR— Transfer Posting																																																									
	APO11 DSS01	Defective goods are returned to suppliers in a timely manner.	2.3.1 Ascertain from management the movement type used to block processing and for returning rejected goods to suppliers (e.g., movement type 122). Execute transaction code MB51—Material Document List with the appropriate movement type. Determine whether there are any long outstanding materials pending return to suppliers and/or receipt of appropriate credits.																																																						
	DSS06	Defective goods are returned to suppliers in a timely manner.	2.3.2 Test the field status of the GR and IR fields using transaction code SPRO to display the IMG menu and follow the path: Material Management → Purchasing → Purchase order → Define Screen Layout at Document Level. These fields should be set as required to																																																						

Audit/Accrual Program for SAP ERP Expenditure Business Cycle											
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes											
Ref.	Assurance Steps and Guidance			Issue Cross-reference							
	ensure that GRs and invoices keyed are matched and recorded in the GR/IR account.										
B-3.6b	<p><u>Agree on the process work products</u>⁹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design).</p> <p>Assess to what extent the process work products are available.</p> <p>Process Purchasing inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.</p>										
	<table border="1"> <thead> <tr> <th>Process Practice</th><th>Work Products</th></tr> </thead> <tbody> <tr> <td>Purchasing</td><td> <ul style="list-style-type: none"> Number of aged purchase requisitions not converted to a purchase order. </td></tr> </tbody> </table>		Process Practice	Work Products	Purchasing	<ul style="list-style-type: none"> Number of aged purchase requisitions not converted to a purchase order. 	<p>Criteria: All listed work products should demonstrably exist and be used.</p>				
Process Practice	Work Products										
Purchasing	<ul style="list-style-type: none"> Number of aged purchase requisitions not converted to a purchase order. 										
<table border="1"> <thead> <tr> <th>Process Practice</th><th>Work Products</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Purchasing</td><td> <ul style="list-style-type: none"> Number of aged purchase requisitions not converted to a purchase order. </td><td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td></tr> </tbody> </table>		Process Practice	Work Products	Assessment Step	Purchasing	<ul style="list-style-type: none"> Number of aged purchase requisitions not converted to a purchase order. 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.				
Process Practice	Work Products	Assessment Step									
Purchasing	<ul style="list-style-type: none"> Number of aged purchase requisitions not converted to a purchase order. 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.									
B-3.7b	<p><u>Agree on the process capability level</u> to be achieved by the process.</p> <p>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</p>										
SAP ERP Expenditure process: Invoice processing											
B-3.1c	<u>Understand the Process context.</u>										
B-3.2c	<u>Understand the Process purpose.</u>										
B-3.3c	<u>Understand all process stakeholders</u> and their roles.										
	Invoice processing stakeholders:										
B-3.4c	<u>Understand the Process goals</u> and related metrics ¹⁰ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.										
	The Process Invoice processing has five defined process goal.		The following activities can be performed to assess whether the goals are achieved.								
	<table border="1"> <thead> <tr> <th>Process Goal</th><th>Related Metrics</th><th>Criteria/Expected Value</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Amounts posted to accounts payable represent goods or services received.</td><td>Determine the metrics that can be used to assess the achievement of the Process goals.</td><td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>		Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	Amounts posted to accounts payable represent goods or services received.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step								
Amounts posted to accounts payable represent goods or services received.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.								
<table border="1"> <tbody> <tr> <td>Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.</td><td>Determine the metrics that can be used to assess the achievement of the Process goals.</td><td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>		Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.						
Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.								
<table border="1"> <tbody> <tr> <td>Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner.</td><td>Determine the metrics that can be used to assess the achievement of the Process goals.</td><td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>		Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.						
Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.								
<table border="1"> <tbody> <tr> <td>Unauthorized and/or invalid supplier invoices are not entered.</td><td>Determine the metrics that can be used to assess the achievement of the Process goals.</td><td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>		Unauthorized and/or invalid supplier invoices are not entered.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.						
Unauthorized and/or invalid supplier invoices are not entered.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.								

⁹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

¹⁰ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Assurance Program for SAP ERP Expenditure Business Cycle																																																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																	
Ref.	Assurance Steps and Guidance				Issue Cross-reference																																												
					Comment																																												
	Duplicate invoices are not entered, and payment is not made more than once.	Determine the metrics that can be used to assess the achievement of the Process goals.	assessment will take place. Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	the defined criteria are achieved. In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																																													
B-3.5c	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:	Reference Process	Invoice processing	Criteria: 3.1 Amounts posted to accounts payable represent goods or services received. 3.2 Accounts payable amounts are calculated completely and accurately and recorded in a timely manner. 3.3 Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner. 3.4 Unauthorized and/or invalid supplier invoices are not entered. 3.5 Duplicate invoices are not entered, and payment is not made more than once.																																													
	Reference Process Practices ¹¹	Good Practice	Assessment Step			Issue Cross-reference																																											
	DSS05	Amounts posted to accounts payable represent goods or services received.	3.1.1 Use transaction code SUIM—User Information System to test user access to transactions for invoice processing: • Functionality: Create and/or change invoice – Enter Invoice—MRHR, MIRO, MR01, FB60 <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>MRHR— Enter Invoice</td> <td>F_BKPF_BUK</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>F_BKPF_GSB</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>MIRO— Enter Invoice</td> <td>M_RECH_AKZ</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>M_RECH_WRK</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>MR01— Enter Invoice</td> <td>F_BKPF_KOA</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>FB60— Enter Invoice</td> <td>F_BKPF_BEK</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>F_BKPF_BUK</td> <td>ACTVT</td> <td>01</td> </tr> </tbody> </table> – Change Invoice—FB02 <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>FB02— Change Invoice</td> <td>F_BKPF_BLA</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td></td> <td>F_BKPF_KOA</td> <td>ACTVT</td> <td>02</td> </tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	MRHR— Enter Invoice	F_BKPF_BUK	ACTVT	01		F_BKPF_GSB	ACTVT	01	MIRO— Enter Invoice	M_RECH_AKZ	ACTVT	01		M_RECH_WRK	ACTVT	01	MR01— Enter Invoice	F_BKPF_KOA	ACTVT	01	FB60— Enter Invoice	F_BKPF_BEK	ACTVT	01		F_BKPF_BUK	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values	FB02— Change Invoice	F_BKPF_BLA	ACTVT	02		F_BKPF_KOA	ACTVT	02		Comment
Transaction(s)	Authorization Objects	Fields	Values																																														
MRHR— Enter Invoice	F_BKPF_BUK	ACTVT	01																																														
	F_BKPF_GSB	ACTVT	01																																														
MIRO— Enter Invoice	M_RECH_AKZ	ACTVT	01																																														
	M_RECH_WRK	ACTVT	01																																														
MR01— Enter Invoice	F_BKPF_KOA	ACTVT	01																																														
FB60— Enter Invoice	F_BKPF_BEK	ACTVT	01																																														
	F_BKPF_BUK	ACTVT	01																																														
Transaction(s)	Authorization Objects	Fields	Values																																														
FB02— Change Invoice	F_BKPF_BLA	ACTVT	02																																														
	F_BKPF_KOA	ACTVT	02																																														

¹¹ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Expenditure Business Cycle audit/assurance program.

Audit/Accrual Program for SAP ERP Expenditure Business Cycle																					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																					
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment															
		<ul style="list-style-type: none"> – Process Blocked Invoices—MR02 <table border="1" style="margin-top: 10px; width: 100%;"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>MR02— Process Blocked Invoices</td><td>M_RECH_SPG</td><td>ACTVT</td><td>02</td></tr> </tbody> </table> <ul style="list-style-type: none"> – Cancel Invoice—MR08 – Enter Credit Memo—MRHG <table border="1" style="margin-top: 10px; width: 100%;"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>MR08— Cancel Invoice MRHG— Enter Credit Memo</td><td>F_BKPF_KOA</td><td>ACTVT</td><td>01</td></tr> </tbody> </table>				Transaction(s)	Authorization Objects	Fields	Values	MR02— Process Blocked Invoices	M_RECH_SPG	ACTVT	02	Transaction(s)	Authorization Objects	Fields	Values	MR08— Cancel Invoice MRHG— Enter Credit Memo	F_BKPF_KOA	ACTVT	01
Transaction(s)	Authorization Objects	Fields	Values																		
MR02— Process Blocked Invoices	M_RECH_SPG	ACTVT	02																		
Transaction(s)	Authorization Objects	Fields	Values																		
MR08— Cancel Invoice MRHG— Enter Credit Memo	F_BKPF_KOA	ACTVT	01																		
DSS06	Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.	<p>3.2.1 View the settings online using the IMG as follows: Define Screen Layout at Document Level—Use transaction code SPRO to display the IMG menu and follow the path: Materials Management → Purchasing → Purchase Order → Define Screen Layout at Document. Select ME21 and ME21N (create purchase order) and then select GR/IR control. Determine whether GR/IR control has been set globally to required entry. If the GR/IR control indicator has not been set globally for all vendors, determine whether it has been set for particular vendors by displaying table LFM1 and field name WEBRE using transaction SE16N—General Table Display. Where GR/IR control has not been set, ascertain from management whether there are any reasons.</p>																			
DSS06	Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.	<p>3.2.2 Check tolerance limits for price variances and message settings for invoice verification (online matching) as follows:</p> <ul style="list-style-type: none"> • Price variance settings for GR—Use transaction code SPRO to display the IMG menu and follow the path: Materials Management → Purchasing → Purchase Order → Set tolerance limits. Access the tolerance limits defined. Double-click on the entries that relate to the company being audited. Two entries need to be checked: one for tolerance key PE (price) and one for tolerance key SE (discount). Note the values displayed: lower and upper limits may be specified as a percentage value (PE allows setting an absolute value.) Ascertain whether the values noted comply with management's intentions. • Three-way Match Tolerance Settings—Accessed through transaction code OMR6—Tolerance limits: Inv. Verification. Confirm with management the variances allowed before an invoice is blocked and test the values for the tolerance keys. <ul style="list-style-type: none"> – AN Amount for item without order reference – AP Amount for item with order reference – BD Form small differences automatically – BR Percentage OPUn variance (IR before GR) – BW Percentage OPUn variance (GR before IR) – DQ Exceed amount: quantity variance – DW Quantity variance when GR quantity = zero – KW Variance from condition value – PP Price variance – PS Price variance: estimated price – ST Date variance (value x days) 																			

Audit/Accruals Program for SAP ERP Expenditure Business Cycle																					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment																
			<ul style="list-style-type: none"> - VP Moving average price variance • Message settings—View the settings online using transaction code SPRO to display the IMG menu and follow the path: Materials Management → Purchasing→ Environment Data → Define Attributes of System Messages. Click on the Position button and enter values 00, 06 and 207 (message for price variance) and press Enter. Note the value in the category field. Possible values are W for warning, and E for error. Ascertain whether the values noted comply with management's intentions. 																		
	DSS01	Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.	3.2.3 Using transaction code S_P6B_12000135—List of GR/IR Balances (also accessible using transaction code SA38—ABAP Reporting and program RM07MSAL), determine whether GR/IR account balances are periodically executed and reviewed.																		
	DSS06	Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.	3.2.4 Check that there are appropriate procedures in place to investigate unmatched POs. In particular, long outstanding items should be followed up and cleared. Similar to testing technique 2.2.1, run the transaction code SA38—ABAP Reporting and program RM06EM00 to produce a listing of outstanding POs.																		
	APO11 DSS06	Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.	3.2.5 Ascertain with the management and confirm that authorized individuals are given access to transaction code MR11—GR/IR account maintenance, which allows postings to GL (write off differences). Use transaction code SUIM—User Information System to review the following authorization codes and activities.																		
			<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="3">MR11— GR/IR account maintenance</td><td>F_BKPF_BLA</td><td>ACTVT</td><td>02</td></tr> <tr> <td>F_BKPF_BUK</td><td>ACTVT</td><td>02</td></tr> <tr> <td>F_BKPF_GSB</td><td>NA</td><td>NA</td></tr> </tbody> </table> <p>Similar to testing technique 2.2.1, run the transaction code SA38—ABAP Reporting and program RM06EM00 to produce a listing of outstanding POs.</p>	Transaction(s)	Authorization Objects	Fields	Values	MR11— GR/IR account maintenance	F_BKPF_BLA	ACTVT	02	F_BKPF_BUK	ACTVT	02	F_BKPF_GSB	NA	NA				
Transaction(s)	Authorization Objects	Fields	Values																		
MR11— GR/IR account maintenance	F_BKPF_BLA	ACTVT	02																		
	F_BKPF_BUK	ACTVT	02																		
	F_BKPF_GSB	NA	NA																		
	DSS05	Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner.	3.3.1 Use transaction code SUIM—User Information System to test user access to directly post invoices to vendor accounts. <ul style="list-style-type: none"> • Enter Credit Memo—MRHG <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>MRHG—Enter Credit Memo</td><td>F_BKPF_KOA</td><td>ACTVT</td><td>01</td></tr> </tbody> </table> <ul style="list-style-type: none"> • Enter Invoice—MRHR, MIRO, MR01 <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>MRHR— Enter Invoice</td><td>F_BKPF_KOA</td><td>ACTVT</td><td>01</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	MRHG—Enter Credit Memo	F_BKPF_KOA	ACTVT	01	Transaction(s)	Authorization Objects	Fields	Values	MRHR— Enter Invoice	F_BKPF_KOA	ACTVT	01		
Transaction(s)	Authorization Objects	Fields	Values																		
MRHG—Enter Credit Memo	F_BKPF_KOA	ACTVT	01																		
Transaction(s)	Authorization Objects	Fields	Values																		
MRHR— Enter Invoice	F_BKPF_KOA	ACTVT	01																		

Audit/Accuracy Program for SAP ERP Expenditure Business Cycle																																																																					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																																					
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment																																																													
			MR01— Enter Invoice MIRO— Enter Invoice	M_RECH_AKZ M_RECH_WRK	ACTVT ACTVT	01 01																																																															
DSS05 DSS06	Unauthorized and/or invalid supplier invoices are not entered.	3.4.1 Determine with the management if there is any workflow configured for park and post functionality and check the user access for the listed transaction codes.	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="5">FBV0—Post Parked Document</td><td>F_BKPF_BUK</td><td>ACTVT</td><td>01, 06</td></tr> <tr> <td>F_BKPF_GSB</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F_BKPF_KOA</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F_FAGL_SEG</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F_BKPF_BLA</td><td>ACTVT</td><td>01, 10</td></tr> <tr> <td rowspan="5">FV60—Park Incoming Invoices</td><td>F_BKPF_BEK</td><td>ACTVT</td><td>77</td></tr> <tr> <td>F_BKPF_BES</td><td>ACTVT</td><td>77</td></tr> <tr> <td>F_BKPF_BLA</td><td>ACTVT</td><td>77</td></tr> <tr> <td>F_BKPF_BUK</td><td>ACTVT</td><td>77</td></tr> <tr> <td>F_BKPF_GSB</td><td>ACTVT</td><td>77</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	FBV0—Post Parked Document	F_BKPF_BUK	ACTVT	01, 06	F_BKPF_GSB	ACTVT	01	F_BKPF_KOA	ACTVT	01	F_FAGL_SEG	ACTVT	01	F_BKPF_BLA	ACTVT	01, 10	FV60—Park Incoming Invoices	F_BKPF_BEK	ACTVT	77	F_BKPF_BES	ACTVT	77	F_BKPF_BLA	ACTVT	77	F_BKPF_BUK	ACTVT	77	F_BKPF_GSB	ACTVT	77	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="6">FB60—Enter Incoming Invoices</td><td>F_BKPF_BEK</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F_BKPF_BLA</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F_BKPF_BUK</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F_BKPF_GSB</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F_BKPF_KOA</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F_SKA1_BUK</td><td>ACTVT</td><td>01</td></tr> <tr> <td>F-43—Enter Vendor Invoice</td><td>F_BKPF_BEK</td><td>ACTVT</td><td>01</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	FB60—Enter Incoming Invoices	F_BKPF_BEK	ACTVT	01	F_BKPF_BLA	ACTVT	01	F_BKPF_BUK	ACTVT	01	F_BKPF_GSB	ACTVT	01	F_BKPF_KOA	ACTVT	01	F_SKA1_BUK	ACTVT	01	F-43—Enter Vendor Invoice	F_BKPF_BEK	ACTVT	01		
Transaction(s)	Authorization Objects	Fields	Values																																																																		
FBV0—Post Parked Document	F_BKPF_BUK	ACTVT	01, 06																																																																		
	F_BKPF_GSB	ACTVT	01																																																																		
	F_BKPF_KOA	ACTVT	01																																																																		
	F_FAGL_SEG	ACTVT	01																																																																		
	F_BKPF_BLA	ACTVT	01, 10																																																																		
FV60—Park Incoming Invoices	F_BKPF_BEK	ACTVT	77																																																																		
	F_BKPF_BES	ACTVT	77																																																																		
	F_BKPF_BLA	ACTVT	77																																																																		
	F_BKPF_BUK	ACTVT	77																																																																		
	F_BKPF_GSB	ACTVT	77																																																																		
Transaction(s)	Authorization Objects	Fields	Values																																																																		
FB60—Enter Incoming Invoices	F_BKPF_BEK	ACTVT	01																																																																		
	F_BKPF_BLA	ACTVT	01																																																																		
	F_BKPF_BUK	ACTVT	01																																																																		
	F_BKPF_GSB	ACTVT	01																																																																		
	F_BKPF_KOA	ACTVT	01																																																																		
	F_SKA1_BUK	ACTVT	01																																																																		
F-43—Enter Vendor Invoice	F_BKPF_BEK	ACTVT	01																																																																		
DSS05 DSS06	Unauthorized and/or invalid supplier invoices are not entered.	3.4.2 Use transaction code SUIM—User Information System to test the user access and confirm that only authorized individuals have access to the below transaction codes for directly posting vendor invoices in SAP ERP.																																																																			

Audit/Accrual Program for SAP ERP Expenditure Business Cycle																																						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																						
Ref.	Assurance Steps and Guidance					Issue Cross-reference	Comment																															
				<table border="1"> <tr><td>F_BKPF_BES</td><td>ACTVT</td><td>01</td></tr> <tr><td>F_BKPF_BLA</td><td>ACTVT</td><td>01</td></tr> <tr><td>F_BKPF_BUK</td><td>ACTVT</td><td>01</td></tr> <tr><td>F_BKPF_GSB</td><td>ACTVT</td><td>01</td></tr> <tr><td>F_BKPF_KOA</td><td>ACTVT</td><td>01</td></tr> <tr><td>MIRO—Enter Incoming Invoice</td><td>M_RECH_AKZ</td><td>ACTVT</td><td>02</td></tr> <tr><td></td><td>M_RECH_WRK</td><td>ACTVT</td><td>01</td></tr> </table>	F_BKPF_BES	ACTVT	01	F_BKPF_BLA	ACTVT	01	F_BKPF_BUK	ACTVT	01	F_BKPF_GSB	ACTVT	01	F_BKPF_KOA	ACTVT	01	MIRO—Enter Incoming Invoice	M_RECH_AKZ	ACTVT	02		M_RECH_WRK	ACTVT	01											
F_BKPF_BES	ACTVT	01																																				
F_BKPF_BLA	ACTVT	01																																				
F_BKPF_BUK	ACTVT	01																																				
F_BKPF_GSB	ACTVT	01																																				
F_BKPF_KOA	ACTVT	01																																				
MIRO—Enter Incoming Invoice	M_RECH_AKZ	ACTVT	02																																			
	M_RECH_WRK	ACTVT	01																																			
				<p>Use transaction code SUIM—User Information System to test user access to release PO invoices or edit FI invoices that have been blocked:</p> <ul style="list-style-type: none"> Release Blocked Invoices—MRBR <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr><td>MRBR—Release Blocked Invoices</td><td>M_RECH_EKG</td><td>ACTVT</td><td>02</td></tr> </tbody> </table> <p>• Change Document—FB02</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr><td>FB02—Change Document</td><td>F_BKPF_BLA</td><td>ACTVT</td><td>02</td></tr> <tr><td></td><td>F_BKPF_KOA</td><td>ACTVT</td><td>02</td></tr> </tbody> </table> <p>• Change Line Items—FB09</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr><td>FB09—Change Line Items</td><td>F_BKPF_KOA</td><td>ACTVT</td><td>02</td></tr> </tbody> </table> <p>Also confirm:</p> <ul style="list-style-type: none"> Whether there is an account type restriction set in the authorization for the listed transactions If the document type field is maintained as not modifiable using editing options or screen layout, it prevents the ability to change the document type and makes it impossible to post a vendor invoice via the alternate transaction codes listed in the following table. <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> </table>	Transaction(s)	Authorization Objects	Fields	Values	MRBR—Release Blocked Invoices	M_RECH_EKG	ACTVT	02	Transaction(s)	Authorization Objects	Fields	Values	FB02—Change Document	F_BKPF_BLA	ACTVT	02		F_BKPF_KOA	ACTVT	02	Transaction(s)	Authorization Objects	Fields	Values	FB09—Change Line Items	F_BKPF_KOA	ACTVT	02	Transaction(s)	Authorization Objects	Fields	Values		
Transaction(s)	Authorization Objects	Fields	Values																																			
MRBR—Release Blocked Invoices	M_RECH_EKG	ACTVT	02																																			
Transaction(s)	Authorization Objects	Fields	Values																																			
FB02—Change Document	F_BKPF_BLA	ACTVT	02																																			
	F_BKPF_KOA	ACTVT	02																																			
Transaction(s)	Authorization Objects	Fields	Values																																			
FB09—Change Line Items	F_BKPF_KOA	ACTVT	02																																			
Transaction(s)	Authorization Objects	Fields	Values																																			

Audit/Assurance Program for SAP ERP Expenditure Business Cycle								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes								
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment
			F-02—Enter G/L Account Posting	F_BKPF_BEK	ACTVT	01		
				F_BKPF_BLA	ACTVT	01		
				F_BKPF_BUK	ACTVT	01		
				F_BKPF_GSB	ACTVT	01		
				F_KMT_MGMT	ACTVT	01, 02		
				F_SKA1_BUK	ACTVT	01		
			F-22—Enter Customer Invoice	F_BKPF_BED	ACTVT	01		
				F_BKPF_BES	ACTVT	01		
				F_BKPF_BUK	ACTVT	01		
				F_BKPF_GSB	ACTVT	01		
				F_BKPF_KOA	ACTVT	01		
			FB50—G/L Acct Pstg: Single Screen Trans.	F_BKPF_BES	ACTVT	01		
				F_BKPF_BLA	ACTVT	01		
				F_BKPF_BUK	ACTVT	01		
				F_BKPF_GSB	ACTVT	01		
				F_BKPF_KOA	ACTVT	01		
DSS01 DSS06	Duplicate invoices are not entered, and payment is not made more than once.	3.5.1 Duplicate Invoice Check: In standard SAP ERP, when processing non-PO-based invoices, the duplicate invoice check is activated via a check box at the vendor master data level, which will consider the fields (vendor code, document date, reference field, company code and currency) at the time of posting an invoice. If the duplicate is identified, then the system will issue an error or warning message based on configuration. Confirm with management the list of vendors for whom this must be activated, and validate with the system configuration by using the transaction code SE16N—General Table Display and table LFB1field REPRF. <ul style="list-style-type: none">• In standard SAP ERP, the duplicate invoice check for PO-based invoices is activated using transaction code SPRO to display the IMG menu and follow the path: Material Management → Logistics Invoice Verification → Incoming Invoice → Set Check for Duplicate Invoices. This duplicate check must be activated at the company code level, and the fields that can be checked are:<ul style="list-style-type: none">– Check company code– Check reference number– Check invoice date						

Audit/Assurance Program for SAP ERP Expenditure Business Cycle										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes										
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment					
B-3.6c	<p>Agree on the process work products¹² (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.</p>									
	<p>Process Invoice processing inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.</p> <table border="1"> <thead> <tr> <th>Process Practice</th> <th>Work Products</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Invoice processing</td> <td> <ul style="list-style-type: none"> GR/IR difference report Blocked invoice report </td> <td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td> </tr> </tbody> </table>			Process Practice	Work Products	Assessment Step	Invoice processing	<ul style="list-style-type: none"> GR/IR difference report Blocked invoice report 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.	
Process Practice	Work Products	Assessment Step								
Invoice processing	<ul style="list-style-type: none"> GR/IR difference report Blocked invoice report 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.								
B-3.7c	<p>Agree on the process capability level to be achieved by the process.</p> <p><i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i></p>									
SAP ERP Expenditure process: Processing disbursements										
B-3.1d	Understand the Process context .									
B-3.2d	Understand the Process purpose .									
B-3.3d	Understand all process stakeholders and their roles.									
Processing disbursements stakeholders:										
B-3.4d	Understand the Process goals and related metrics ¹³ and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process.									
	The Process Processing disbursements has one defined process goals.		The following activities can be performed to assess whether the goals are achieved.							
Process Goal		Related Metrics	Criteria/Expected Value	Assessment Step						
Disbursements are made only for goods and services received, are calculated and recorded accurately, and distributed to the appropriate suppliers in a timely manner.		Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.						
B-3.5d	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement: Expected process practices are applied. Accountability and responsibility are assigned and assumed.									
	Reference Process	Processing disbursements	Criteria: 4.1 Disbursements are made only for goods and services received, are calculated and recorded accurately, and are distributed to the appropriate suppliers in a timely manner.							
	Reference Process Practices ¹⁴	Good Practice	Assessment Step	Issue Cross-reference	Comment					
	APO01 DSS01	Disbursements are made only for goods and services received, are	4.1.1 Use transaction code SUIM—User Information System to test user access to transactions to process disbursements:							

¹² For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*.

¹³ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

¹⁴ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Expenditure Business Cycle audit/assurance program.

Audit/Accurance Program for SAP ERP Expenditure Business Cycle																										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																										
Ref.	Assurance Steps and Guidance					Issue Cross-reference																				
DSS06	calculated and recorded accurately, and are distributed to the appropriate suppliers in a timely manner.	<ul style="list-style-type: none"> Automatic Scheduling of Payment Transactions—F110S Parameters for Automatic Payment—F110 		<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>F110— Parameters for Automatic Payment</td><td>F_REGU_KOA</td><td>ACTVT</td><td>01, 02, 03, 11, 12</td></tr> <tr> <td>F110S— Automatic Scheduling of Payment Transactions</td><td></td><td></td><td>13, 14, 15, 21, 23</td></tr> <tr> <td>F-58— Payment With Printout</td><td>F_BKPF_KOA</td><td>ACTVT</td><td>24, 25, 31</td></tr> <tr> <td></td><td></td><td></td><td>01</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	F110— Parameters for Automatic Payment	F_REGU_KOA	ACTVT	01, 02, 03, 11, 12	F110S— Automatic Scheduling of Payment Transactions			13, 14, 15, 21, 23	F-58— Payment With Printout	F_BKPF_KOA	ACTVT	24, 25, 31				01		
Transaction(s)	Authorization Objects	Fields	Values																							
F110— Parameters for Automatic Payment	F_REGU_KOA	ACTVT	01, 02, 03, 11, 12																							
F110S— Automatic Scheduling of Payment Transactions			13, 14, 15, 21, 23																							
F-58— Payment With Printout	F_BKPF_KOA	ACTVT	24, 25, 31																							
			01																							
<ul style="list-style-type: none"> Payment With Printout—F-58 																										
<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>F-58— Payment With Printout</td><td>F_BKPF_KOA</td><td>ACTVT</td><td>01</td></tr> </tbody> </table>				Transaction(s)	Authorization Objects	Fields	Values	F-58— Payment With Printout	F_BKPF_KOA	ACTVT	01															
Transaction(s)	Authorization Objects	Fields	Values																							
F-58— Payment With Printout	F_BKPF_KOA	ACTVT	01																							
DSS06	Disbursements are made only for goods and services received, are calculated and recorded accurately, and are distributed to the appropriate suppliers in a timely manner.	4.1.2 Access transaction code SE16N—General Table Display to check the table RBKP_BLOCKED for the blocked invoices. As this is a standard SAP ERP inherent control, testing this control using sampling of payment transactions is optional.																								
DSS06	Disbursements are made only for goods and services received, are calculated and recorded accurately, and are distributed to the appropriate suppliers in a timely manner.	4.1.3 Ascertain with management whether the release procedures are configured and check the configuration using transaction code SPRO to display the IMG menu and follow the path: Financial Accounting → Accounts Receivable and Accounts Payable → Business Transactions → Release for Payment.																								
B-3.6d	<u>Agree on the process work products</u> ¹⁵ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.																									
	Processing disbursements inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.																						
	Process Practice Processing disbursements	Work Products <ul style="list-style-type: none"> Aging of uncleared checks 		Assessment Step Apply appropriate audit techniques to determine the existence and appropriate use of each work product.																						
B-3.7d																										
B-3.7d	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>																									

¹⁵ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Expenditure Business Cycle															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment															
Organisational Structures															
Ref.	Assurance Steps and Guidance		Issue Cross-reference												
B-4	Obtain understanding of each Organisational Structure in scope and set suitable assessment criteria: For each Organisational Structure in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the Organisational Structure .														
Organisational Structure: Purchasing															
B-4.1a	<u>Understand the Organisational Structure context.</u> <i>Identify and document all elements that can help to understand the context in which the Purchasing organization has to operate, including:</i> <ul style="list-style-type: none"> • The overall organisation • Management/process framework • History of the role/structure • Contribution of the Organisational Structure to achievement of goals 														
B-4.2a	<u>Understand all stakeholders of the Organisational Structure/function.</u> <i>Determine through documentation review (policies, management communications, etc.) the key stakeholders of the Purchasing organization.</i> <ul style="list-style-type: none"> • Incumbent of the role and/or members of the Organisational Structure • Other key stakeholders affected by the decisions of the Organisational Structure/role 														
B-4.3a	<u>Understand the goals of the Organisational Structure</u> , the related metrics and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals.														
<table border="1"> <thead> <tr> <th>Organisational Structure Goal</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Determine through interviews with key stakeholders and documentation review the goals of the Purchasing organization, i.e., the decisions for which they are accountable^{16,17}.</td><td> This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. </td></tr> </tbody> </table>				Organisational Structure Goal	Assessment Step	Determine through interviews with key stakeholders and documentation review the goals of the Purchasing organization, i.e., the decisions for which they are accountable ^{16,17} .	This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 								
Organisational Structure Goal	Assessment Step														
Determine through interviews with key stakeholders and documentation review the goals of the Purchasing organization, i.e., the decisions for which they are accountable ^{16,17} .	This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 														
B-4.4a	<u>Agree on the expected good practices for the Organisational Structure</u> against which it will be assessed. <u>Assess the Organisational Structure design</u> , i.e., assess the extent to which expected good practices are applied.														
<table border="1"> <thead> <tr> <th>Good Practice</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Operating principles</td><td> <ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. </td><td> <ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. </td></tr> <tr> <td>Composition</td><td>The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td><td>Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td></tr> <tr> <td>Span of control</td><td> <ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. </td><td> <ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. </td></tr> </tbody> </table>				Good Practice	Criteria	Assessment Step	Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 	Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Span of control	<ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. 	<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined.
Good Practice	Criteria	Assessment Step													
Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 													
Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.													
Span of control	<ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. 	<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. 													

¹⁶ The RACI charts in COBIT 5: *Enabling Processes* can be leveraged as a starting point for the expected goals of a role or Organisational Structure.

¹⁷ The Organisational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organisational Structure assuming the same responsibilities and accountability should be considered.

Audit/Accrual Program for SAP ERP Expenditure Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-4.5a		<ul style="list-style-type: none"> The span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. The span of control is in line with the overall enterprise governance arrangements. 	<ul style="list-style-type: none"> Assess whether the span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. Verify and assess whether the span of control is in line with the overall enterprise governance arrangements. 		
	Level of authority/decision rights	<ul style="list-style-type: none"> Decision rights of the Organisational Structure are defined and documented. Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue). 	<ul style="list-style-type: none"> Verify that decision rights of the Organisational Structure are defined and documented. Verify whether decision rights of the Organisational Structure are complied with and respected. 		
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.		
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.		
B-4.5a	<u>Understand</u> the life cycle and agree on expected values. <u>Assess</u> the extent to which the Organisational Structure life cycle is managed.				
Life-Cycle Element		Criteria	Assessment Step		
B-4.1 to B-4.5	Mandate	<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well understood mandate. 		
	Monitoring	<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 		
B-4.1 to B-4.5	Repeat steps B-4.1 through B-4.5 for all remaining Organisational structures in scope.				
	Repeat the steps described above for the remaining Organisational structures:				
	<ul style="list-style-type: none"> Accounts payable Warehouse Receiving Accounting Quality (QA) 				

Audit/Accurance Program for SAP ERP Expenditure Business Cycle						
Phase —Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment						
Culture, Ethics and Behaviour						
Ref.	Assurance Step and Guidance		Issue Cross-reference	Comment		
B-5	Obtain understanding of the Culture, Ethics and Behaviour in scope. Assess Culture, Ethics and Behaviour.					
Culture, Ethics and Behaviour: Risk and compliance aware culture						
B-5.1a	<u>Understand the Culture, Ethics and Behaviour context.</u> <ul style="list-style-type: none"> • <i>What the overall corporate Culture is like</i> • <i>Understand the interconnection with other enablers in scope:</i> <ul style="list-style-type: none"> - <i>Identify roles and structures that could be affected by the Culture.</i> - <i>Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.</i> 					
B-5.2a	<u>Understand the major stakeholders of the Culture, Ethics and Behaviour: Risk and compliance aware culture</u> <i>Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.</i>					
B-5.3a	<u>Understand the goals for the Culture, Ethics and Behaviour, and the related metrics</u> and agree on expected values. Assess whether the Culture, Ethics and Behaviour goals (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour. In the context of Risk and compliance aware culture , the following Culture, Ethics and Behaviour are desired:		Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. For a representative sample of individuals, perform the following assessment steps.			
Desired Behaviour (Culture, Ethics and Behaviour Goal)		Assessment Step				
The enterprise is aware of the compliance requirements it must abide						
Employees understand their role in maintaining compliance						
Identified risk are properly address						
Controls are in place to ensure compliance with internal and external requirements						
B-5.4a	<u>Understand the life cycle stages of the Culture, Ethics and Behaviour</u> , and agree on the relevant criteria. Assess to what extent the Culture, Ethics and Behaviour life cycle is managed. <small>(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)</small>					
B-5.5a	<u>Understand good practice when dealing with Culture, Ethics and Behaviour</u> , and agree on relevant criteria. Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied.					
Good Practice		Criteria				
Communication, enforcement and rules		Existence and quality of the communication				
Incentives and rewards		Existence and application of appropriate rewards and incentives				
Awareness		Awareness of desired Behaviours				
B-5.1 to B-5.5		Repeat steps B-5.1 through B-5.5 for all remaining Culture, Ethics and Behaviour in scope. Repeat the steps described above for the remaining Culture, Ethics and Behaviour: <ul style="list-style-type: none">• Enabling of continuous improvement• Accountability				

Audit/Assurance Program for SAP ERP Expenditure Business Cycle			
Phase —Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Culture, Ethics and Behaviour			
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment
	<ul style="list-style-type: none">• Discipline to follow instructions		

Audit/Accrual Program for SAP ERP Expenditure Business Cycle																																																							
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																																																							
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment																																																				
B-6	Obtain understanding of the Information Items in scope. Assess Information Items.																																																						
Information Item: Data integrity procedures																																																							
B-6.1a	<u>Understand</u> the Information item context : <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> - <i>Used by which processes?</i> - <i>Which Organisational Structures are involved?</i> - <i>Which services/applications are involved?</i> 																																																						
B-6.2a	<u>Understand</u> the major stakeholders of the Information item . <i>Understand the stakeholders for the Information item, i.e., identify the:</i> <ul style="list-style-type: none"> • <i>Information producer</i> • <i>Information custodian</i> • <i>Information consumer</i> <p><i>Stakeholders should be at the appropriate organisational level.</i></p>																																																						
B-6.3a	<u>Understand</u> the major quality criteria for the Information item, the related metrics and agree on expected values. <u>Assess</u> whether the Information item quality criteria (outcomes) are achieved, i.e., assess the effectiveness of the Information item. <p>Leverage the COBIT 5 Information enabler model¹⁸ focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand.</p> <p>Mark the quality dimensions with a ‘✓’ that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Quality Dimension</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Accuracy</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Objectivity</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Believability</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Reputation</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Relevancy</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Completeness</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Currency</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Amount of information</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Concise representation</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Consistent representation</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Interpretability</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Understandability</td> <td>✓</td> <td></td> <td></td> </tr> </tbody> </table>	Quality Dimension	Key Criteria	Description	Assessment Step	Accuracy	✓			Objectivity				Believability				Reputation				Relevancy	✓			Completeness	✓			Currency	✓			Amount of information	✓			Concise representation	✓			Consistent representation				Interpretability				Understandability	✓				
Quality Dimension	Key Criteria	Description	Assessment Step																																																				
Accuracy	✓																																																						
Objectivity																																																							
Believability																																																							
Reputation																																																							
Relevancy	✓																																																						
Completeness	✓																																																						
Currency	✓																																																						
Amount of information	✓																																																						
Concise representation	✓																																																						
Consistent representation																																																							
Interpretability																																																							
Understandability	✓																																																						

¹⁸ COBIT 5 framework, appendix G, p.81-84

Audit/Accurance Program for SAP ERP Expenditure Business Cycle																															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																															
Information Items																															
Ref.	Assurance Steps and Guidance				Issue Cross-reference																										
	Manipulation																														
	Availability	✓																													
	Restricted access	✓																													
B-6.4a	<p><u>Understand</u> the life cycle stages of the Information item, and agree on the relevant criteria. <u>Assess</u> to what extent the Information item life cycle is managed.</p> <p>The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.</p> <ul style="list-style-type: none"> When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently. When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. <p>Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Life Cycle Stage</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Plan</td><td>✓</td><td></td><td></td></tr> <tr> <td>Design</td><td>✓</td><td></td><td></td></tr> <tr> <td>Build/acquire</td><td>✓</td><td></td><td></td></tr> <tr> <td>Use/operate</td><td>✓</td><td></td><td></td></tr> <tr> <td>Evaluate/monitor</td><td>✓</td><td></td><td></td></tr> <tr> <td>Update/dispose</td><td>✓</td><td></td><td></td></tr> </tbody> </table>	Life Cycle Stage	Key Criteria	Description	Assessment Step	Plan	✓			Design	✓			Build/acquire	✓			Use/operate	✓			Evaluate/monitor	✓			Update/dispose	✓				
Life Cycle Stage	Key Criteria	Description	Assessment Step																												
Plan	✓																														
Design	✓																														
Build/acquire	✓																														
Use/operate	✓																														
Evaluate/monitor	✓																														
Update/dispose	✓																														
B-6.5a	<p><u>Understand</u> important attributes of the Information item and expected values. <u>Assess</u> the Information item design, i.e., assess the extent to which expected good practices are applied.</p> <p>Good practices for Information items are defined as a series of attributes for the Information item¹⁹. The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.</p> <p>Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Attribute</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Physical</td><td></td><td></td><td></td></tr> <tr> <td>Empirical</td><td></td><td></td><td></td></tr> <tr> <td>Syntactic</td><td></td><td></td><td></td></tr> <tr> <td>Semantic</td><td></td><td></td><td></td></tr> <tr> <td>Pragmatic</td><td>✓</td><td></td><td></td></tr> <tr> <td>Social</td><td></td><td></td><td></td></tr> </tbody> </table>	Attribute	Key Criteria	Description	Assessment Step	Physical				Empirical				Syntactic				Semantic				Pragmatic	✓			Social					
Attribute	Key Criteria	Description	Assessment Step																												
Physical																															
Empirical																															
Syntactic																															
Semantic																															
Pragmatic	✓																														
Social																															
B-6.1 to B-6.5	Repeat steps B-6.1 through B-6.5 for all remaining Information items in scope.																														
	<p>Repeat the steps described above for the remaining Information items:</p> <ul style="list-style-type: none"> Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis 																														

¹⁹ COBIT 5 framework, appendix G, p. 81-84

Audit/Assurance Program for SAP ERP Expenditure Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Information Items			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
	<ul style="list-style-type: none">• Retention requirements• Record of transactions• Training manuals• Job aids		

Audit/Accurance Program for SAP ERP Expenditure Business Cycle																								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																								
Ref.	Assurance Steps and Guidance			Issue Cross-reference																				
B-7	Obtain understanding of the Services, Infrastructure and Applications in scope. Assess Services, Infrastructure and Applications.																							
Services, Infrastructure and Applications: Master data maintenance group																								
B-7.1a	<u>Understand the Services, Infrastructure and Applications</u> context. <i>Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.</i>																							
B-7.2a	<u>Understand the major stakeholders of the Services, Infrastructure and Applications.</u> <i>Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.</i>																							
B-7.3a	<u>Understand the major goals for the Services, Infrastructure and Applications</u> , the related metrics and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.																							
<table border="1"> <thead> <tr> <th>Goal</th> <th>Criteria</th> <th>Assessment Step</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>Service description</td> <td> <ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders </td> <td> <ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. </td> <td></td> <td></td> </tr> <tr> <td>Service level definition</td> <td>Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness </td> <td> <ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. </td> <td></td> <td></td> </tr> <tr> <td>Contribution to related enablers, IT and enterprise goals</td> <td>The Service contributes to the achievement of related enabler and IT-related and enterprise goals.</td> <td>Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.</td> <td></td> <td></td> </tr> </tbody> </table>					Goal	Criteria	Assessment Step			Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 			Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 			Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.		
Goal	Criteria	Assessment Step																						
Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 																						
Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 																						
Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.																						
B-7.4a	Understand good practice related to the Services, Infrastructure and Applications and expected values. Assess the Services, Infrastructure and Applications design, i.e., assess to what extent expected good practices are applied. Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework ²⁰ to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented: <ul style="list-style-type: none"> Buy/build decision needs to be taken. Use of the Service needs to be clear. 																							
<table border="1"> <thead> <tr> <th>Good Practice</th> <th>Criteria</th> <th>Assessment Step</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>Sourcing (buy/build)</td> <td>A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.</td> <td> <ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business </td> <td></td> <td></td> </tr> </tbody> </table>					Good Practice	Criteria	Assessment Step			Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business 												
Good Practice	Criteria	Assessment Step																						
Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business 																						

²⁰ COBIT 5 framework, appendix G, p.85-86

Audit/Assurance Program for SAP ERP Expenditure Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Services, Infrastructures and Applications					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
			case. <ul style="list-style-type: none"> • Verify that the sourcing decision has been duly executed. 		
	Use	The use of the Service needs to be clear: <ul style="list-style-type: none"> • When it needs to be used and by whom • The required compliance levels with the Service's output 	<ul style="list-style-type: none"> • Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used. • Verify that actual use is in line with requirement above. • Verify that the actual Service output is adequately used. • Verify that Service levels are monitored and achieved. 		
B-7.1 to B-7.4	Repeat steps B-7.1 through B-7.4 for all remaining Services, Infrastructure and Applications in scope. Repeat the steps described above for the remaining Services, Infrastructure and Applications: <ul style="list-style-type: none"> • SAP ERP support and maintenance • SAP training • Tax department • Accounting department 				

Audit/Accrual Program for SAP ERP Expenditure Business Cycle																						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																						
People, Skills and Competencies																						
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment																			
B-8	Obtain understanding of the People, Skills and Competencies in scope. Assess People, Skills and Competencies.																					
People, Skill and Competency: Proficiency using the SAP Purchasing, Accounts Payable, Returns and Credit notes functionality																						
B-8.1a	<p><u>Understand</u> the People, Skills and Competencies context. <i>Understand the context of the Skill/Competency, i.e.:</i></p> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> – <i>In which roles and structures is the Skill/Competency used? (See also B-4.1.)</i> <p><i>Which behaviours are associated with the Skill/Competency?</i></p>																					
B-8.2a	<p><u>Understand</u> the major stakeholders for the People, Skills and Competencies. <i>Identify to whom in the organisation the skill requirement applies.</i></p>																					
B-8.3a	<p><u>Understand</u> the major goals for the People, Skills and Competencies, the related metrics and agree on expected values. <u>Assess</u> whether the People, Skills and Competencies goals (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.</p> <p>For the People, Skills and Competencies: Proficiency using the SAP Expenditure Module, the following goals and associated criteria can be addressed.</p> <table border="1"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Experience</td><td></td><td rowspan="6">Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.</td></tr> <tr> <td>Education</td><td></td></tr> <tr> <td>Qualification</td><td></td></tr> <tr> <td>Knowledge</td><td></td></tr> <tr> <td>Technical skills</td><td></td></tr> <tr> <td>Behavioural skills</td><td></td></tr> <tr> <td>Number of people with appropriate skill level</td><td></td><td></td></tr> </tbody> </table>	Goal	Criteria	Assessment Step	Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	Education		Qualification		Knowledge		Technical skills		Behavioural skills		Number of people with appropriate skill level				
Goal	Criteria	Assessment Step																				
Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.																				
Education																						
Qualification																						
Knowledge																						
Technical skills																						
Behavioural skills																						
Number of people with appropriate skill level																						
B-8.4a	<p><u>Understand</u> the life cycle stages of the People, Skills and Competencies, and agree the relevant criteria. Assess to what extent the People, Skills and Competencies life cycle is managed.</p> <p>For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07.</p>	<p>For the People, Skills and Competencies at hand the assurance professional will perform the following assessment steps.</p> <table border="1"> <thead> <tr> <th>Life Cycle Element</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Plan</td><td>Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.</td><td>Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.</td></tr> <tr> <td>Design</td><td> Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the </td><td> Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill. </td></tr> </tbody> </table>	Life Cycle Element	Criteria	Assessment Step	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.											
Life Cycle Element	Criteria	Assessment Step																				
Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.																				
Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.																				

Audit/Accurance Program for SAP ERP Expenditure Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
People, Skills and Competencies				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
		development of skills and competencies.) is implemented in relation to this skill.		Comment
	Build	Practice APO07.03 activity 4 (Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 4 is implemented in relation to this skill.	
	Operate	Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.	
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.	
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.	
B-8.5a	<u>Understand good practice related to the People, Skills and Competencies</u> and expected values. Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.			
Good Practice		Criteria	Assessment Step	
Skill set and Competencies are defined.		<ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 	Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	
Skill levels are defined.		<ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. 	Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	

Audit/Assurance Program for SAP ERP Expenditure Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
People, Skills and Competencies				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
		<ul style="list-style-type: none"> Assess the process for 360-degree performance evaluations. 		Comment
B-8.1 to B-8.5	Repeat steps B-8.1 through B-8.5 for all remaining People, Skills and Competencies in scope.			
	Repeat the steps described above for the remaining People, Skills and Competencies:	<ul style="list-style-type: none"> Master data management skills Expenditure skills and experience Proficiency running SAP reports Understanding of data classification policies Understanding of data integrity procedures 		

Audit/Accurance Program for SAP ERP Expenditure Business Cycle		
Phase C—Communicate the Results of the Assessment		
Ref.	Assurance Step	Guidance
C-1	Document exceptions and gaps.	
C-1.1	Understand and document weaknesses and their impact on the achievement of process goals.	<ul style="list-style-type: none"> Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	<ul style="list-style-type: none"> Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. Point out the consequence of noncompliance with regulatory requirements and contractual agreements. Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
C-2	Communicate the work performed and findings.	
C-2.1	Communicate the work performed.	<ul style="list-style-type: none"> Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	<ul style="list-style-type: none"> Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. Use benchmarking and survey results to compare the enterprise's performance with others. Use extensive graphics to illustrate the issues. Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	

Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
1. Master Data Maintenance							
1.1 Changes made to master data are valid, complete, accurate and timely.							
1.1.1 Does relevant management, other than the initiators, check online reports of master data additions and changes back to source documentation on a sample basis?					DSS01 DSS06		
1.1.2 Is access to create and change master data restricted to authorized individuals? Are user accounts validated against HR lists and access in alignment with role requirements? Are user accounts reviewed by management in line with the enterprise's policy?					DSS06		
1.1.3 Have configurable controls been designed into the process to maintain the integrity of master data?					DSS06		
1.1.4 Is a naming convention used for vendor names (e.g., according to letterhead) to minimize the risk of establishing duplicated vendor master records?					APO10 DSS01		
1.2 Master data remain current and pertinent.							
1.2.1 Does management periodically review master data to check their accuracy?					DSS01 DSS06		
2. Purchasing							
2.1 Purchase order entry and changes are valid, complete, accurate and timely.							

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.1.1 Is the ability to create, change or cancel purchase requisitions, purchase orders and outline agreements (standing purchase orders) restricted to authorized personnel?					DSS05 DSS06
2.1.2 Does the SAP ERP source list functionality allow specified materials to be purchased only from vendors included in the source list for the specified material?					APO10 DSS01
2.1.3 Is the SAP ERP release strategy used to authorize purchase requisitions, purchase orders, outline agreements (standing purchase orders) and unusual purchases (e.g., capital outlays)?					DSS06
2.2 Goods are received only for valid purchase orders, and goods receipts are recorded completely, accurately and in a timely manner.					
2.2.1 When goods received are matched to open purchase orders, are receipts with no purchase order or those that exceed the purchase order quantity by more than an established amount investigated? Does management review exception reports of goods not received on time for recorded purchases?					DSS06
2.2.2 Is the ability to input, change or cancel goods received transactions restricted to authorized inbound logistics/raw materials personnel?					DSS05 DSS06

Expenditure Business Cycle ICQ

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.3 Defective goods are returned to suppliers in a timely manner.					
2.3.1 Are rejected raw materials adequately segregated from other raw materials in a quality assurance bonding area, and are they regularly monitored (assigned a movement type of 122) to ensure timely return to suppliers?					APO11 DSS01
2.3.2 Is SAP ERP configured to control the background posting accurately?					DSS06
3. Invoice Processing					
3.1 Amounts posted to accounts payable represent goods or services received.					
3.1.1 Is the ability to input, change, cancel or release vendor invoices for payment restricted to authorized personnel?					DSS05
Is the ability to input vendor invoices that do not have a purchase order and/or a goods receipt as support further restricted to authorized personnel?					
3.2 Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.					
3.2.1 Is the SAP ERP software configured to perform a three-way match?					DSS06
3.2.2 Is the SAP ERP software configured with quantity and price tolerance limits?					DSS06
3.2.3 Is the GR/IR account regularly reconciled?					DSS01 DSS06
3.2.4 Are reports of outstanding purchase orders regularly reviewed?					DSS01 DSS06

Expenditure Business Cycle ICQ

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.2.5 Are supplier invoices and credit notes that are received at, before or after the end of a statutory accounting period reviewed and/or reconciled?					APO11 DSS06
3.3 Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner.					
3.3.1 Is the ability to input, change, cancel or release credit notes restricted to authorized personnel?					DSS05
3.4 Unauthorized and/or invalid supplier invoices are not entered.					
3.4.1 Is segregation of duties enforced by using park and post workflow functionality to ensure that responsibility and accountability are segregated among the designated teams?					DSS05 DSS06
3.4.2 Is the ability to post vendor invoices in the system directly and to release the invoices restricted to authorized personnel?					DSS05 DSS06
3.5 Duplicate invoices are not entered, and payment is not made more than once.					
3.5.1 Is duplicate invoice check activated for non-PO-based and for PO-based invoicing?					DSS01 DSS06
4. Processing Disbursements					
4.1 Disbursements are made only for goods and services received, are calculated and recorded accurately, and are distributed to the appropriate suppliers in a timely manner.					
4.1.1 Does management approve the SAP ERP payment run parameter specification?					APO01 DSS01 DSS06

Expenditure Business Cycle ICQ

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
4.1.2 Does the SAP ERP software restrict payment to blocked invoices until the blocked invoices are released manually?					DSS06
4.1.3 Do the payment release procedures provide segregation of duties control, which includes dual as well as triple-level controls?					DSS06

SAP ERP

Inventory Business Cycle
Audit/Assurance Program



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP ERP Inventory Business Cycle Audit/Accurance Program* (the ‘Work’) primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP’s kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: <http://www.isaca.org/sap-erp-4th-edition>

Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOFFICIAL>

Like ISACA on Facebook: www.facebook.com/ISACAHQ

Acknowledgements

ISACA wishes to recognize

Project Leaders

Benjamin Fitts, CPA, Deloitte & Touche LLP, USA
Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA
Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA
Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Eva Sweet, CISA, CISM, ISACA, USA

Researchers

Syed Aamir Aarfi, Deloitte & Touche LLP, USA
Carlos Amaya, CISA, Deloitte & Touche LLP, USA
Dan Argynov, PMP, Deloitte & Touche LLP, USA
Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA
David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA
Ramamallikarjunarao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA
Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA
Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA
Sagnik Mukherjee, Deloitte & Touche LLP, USA
Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA
Sonik Shah, Deloitte & Touche LLP, USA
Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA
Shweta Srivastava, Deloitte & Touche LLP, USA
Anurag Tewary, Deloitte & Touche LLP, USA
Percy Tsai, CPA, Deloitte & Touche LLP, USA
Ravi Maddela Veeriah, Deloitte & Touche LLP, USA
Sravan Vemana, Deloitte & Touche LLP, USA
Anukool Vyas, Deloitte & Touche LLP, USA

Expert Reviewers

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA
Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada
Mayank Garg, CISA, NetApp, USA
Ricci leong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Jim Koveos, CISA, MBA, AmerisourceBergen, USA
Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia
Samuel LIM S.C., CISA, Auditor General's Office, Singapore
Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia
Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General's Office, Singapore
Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia
Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia
Paul O'Donnell, Ernst & Young, Canada
Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico
John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US
Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico
Naved Rehman, CISA, CRISC, MS-IS, SAPAuditCoach, US
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US
Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico
Jovari St. Victor, CISA, CPA, Sunera, LLC, US
Surapong Surabotsoon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,
KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico
Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand
David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President
Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKLoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK
Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil
Jotham Nyamari, CISA, Deloitte, USA
James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK
Gurvinder Singh, CISA, CISM, CRISC, Australia
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore
Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

SAP ERP Inventory Business Cycle Audit/Assurance Program

Introduction

This document contains an example audit/assurance program, **based on** the generic structure developed in section 2B of *COBIT 5 for Assurance*¹.

The engagement approach is based on, but **differs slightly** from the generic approach described in *COBIT 5 for Assurance*:

- The engagement approach described in this audit/assurance program is **focused on a business process** consequently no group of COBIT 5 processes dominates as primary processes and the lower-level processes are widespread, for evaluation purposes, the high-level COBIT 5 processes will be used as references.
- The assurance steps in this audit/assurance program are specific to the subject matter under review; therefore most of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources availableprocess audit/assurance program.

Assurance Engagement: SAP ERP Inventory Business Cycle

Assurance Topic

The topic covered by this assurance engagement is the SAP ERP Inventory Business Cycle.

Business Impact and Risk

SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical processes.

Risk resulting from ineffective or incorrect configurations or use of SAP could result in some of the following:

- Disclosure of privileged information
- Single points of failure
- Low data quality
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements

Goal of the Review

The objective of the SAP ERP audit/assurance review is to provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise's SAP ERP architecture.

Scoping

The review will focus on configuration of the relevant SAP ERP components and modules within the enterprise. The selection of the specific components and modules will be based upon the risk introduced to the enterprise by these components and modules.

From a process reference model (PRM) perspective, the following domains and processes apply to this audit and assurance programme:

- BAI02 *Manage requirements definition*
- BAI03 *Manage solution identification and build*
- DSS01 *Manage Operations*
- DSS05 *Manage security services*
- DSS06 *Manage business process controls*

¹ See www.isaca.org/COBIT/Pages/Assurance-product-page.aspx for more information on *COBIT 5 for Assurance*.

Minimum Audit Skills

This review is considered highly technical. The IS audit and assurance professional must have an understanding of SAP best practice processes and requirements and be highly conversant in SAP tools, exposures and functionality. It should not be assumed that an audit and assurance professional holding the CISA designation has the requisite skills to perform this review.

Testing SAP Security

To determine which users have access to the relevant authorizations used in this audit program, use one of the following methods:

1. Use transaction code SUIM → Users → Users by Complex Selection Criteria
2. Use transaction code S_BCE_68001417
3. Use transaction code SA38 and the program RSUSR002. This method allows the user to specify a transaction code, a "valid to" date for users, and up to three other authorization objects (which also may be the authorization object for transaction code S_TCODE) with associated values (two values under an AND relationship and three values under an OR relationship).
This method is generally sufficient for testing logical access security in relation to SAP ERP application infrastructure areas, but it is less suitable when large numbers of authorizations must be reviewed, such as in segregation of duties analysis and in some of the more complex areas of business cycle controls.
4. Use transaction code SUIM → Users → Users with Critical Authorizations (also accessible with program RSUSR008_009_NEW, which replaces programs RSUSR008 and RSUSR009 and transaction codes SU98 and/or SU99, for SAP Web AS 6.20 and later). This method offers improvements such as allowing differentiation between SAP defaults for critical data for different business areas, extended combination options for critical authorization data, improved performance, display of user filters and more analysis options for users in the result list.

Audit/Accurance Program for SAP ERP Inventory Business Cycle					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
A-1	Determine the stakeholders of the assurance initiative and their stakes .				
A-1.1	<u>Identify</u> the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	Intended user(s) of the assurance report	<p>Board/audit committee: Needs assurance over the effectiveness and efficiency of SAP ERP processes within the enterprise.</p> <p>Chief financial officer (CFO): Needs assurance that internal controls for financial applications work as intended.</p> <p>Risk managers: Need assurance that controls intended to address previously identified risk are working as intended. The results from the audit should be used to update the risk registry as needed.</p> <p>Security managers: Need to identify gaps in the security plans for SAP applications.</p> <p>Owners / shareholders: Part or all of the SAP ERP assurance report may be included in statutory reporting.</p> <p>Regulators: Part or all of SAP ERP reporting may need to be disclosed to respective authorities.</p>		
A-1.2	Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	Accountable and responsible parties for the subject matter	<p>Business executives: The individuals responsible for identifying requirements, approving design and managing performance. These people are, together with IT management, responsible for managing the correct and controlled use of SAP ERP services—in line with good practices.</p> <p>Business process owners: Responsible for defining application and technical requirements. Responsible for data classification.</p> <p>IT management: Responsible for managing the correct and controlled use of SAP ERP services—together with the business executives.</p>		
A-2	<u>Determine</u> the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities (i.e., not achieving the enterprise goals).		<p>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.</p> <p>Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.</p> <p>Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</p> <p>Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.</p>		
A-2.1	<u>Understand</u> the enterprise strategy and priorities.		<i>Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.</i>		

Audit/Assurance Program for SAP ERP Inventory Business Cycle				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
A-2.2	<u>Understand</u> the internal context of the enterprise.	<p><i>Identify all internal environmental factors that could influence the performance and contents of the SAP ERP Inventory Module.</i></p> <ul style="list-style-type: none"> • Review prior report, if one exists, verify completion of any agreed-on corrections, and note remaining deficiencies. Determine whether: <ul style="list-style-type: none"> – Senior management has assigned responsibilities for information, its processing, and its use – User management is responsible for providing information that supports the entity's objectives and policies – Information systems management is responsible for providing the capabilities necessary for the achievement of the defined information systems objectives and the policies of the entity – Senior management approves plans for development and acquisition of information systems – There are procedures to ensure that the information system being developed or acquired meets user requirements – There are procedures to ensure that information systems, programs and configuration changes are tested adequately prior to implementation – All personnel involved in the system acquisition and configuration activities receive adequate training and supervision – There are procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards – User management participates in the conversion of data from the existing system to the new system – Final approval is obtained from user management prior to going live with a new information/upgraded system – There are procedures to document and schedule all changes to information systems (including key ABAP programs) – There are procedures to ensure that only authorized changes are initiated – There are procedures to ensure that only authorized, tested and documented changes to information systems are accepted into the production client – There are procedures to allow for and control emergency changes – There are procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software – There is a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated – The organizational structure, established by senior management, provides for an appropriate segregation of incompatible functions – The database, application and presentation servers are located in a physically separate and protected environment (i.e., a data center) – Emergency, backup and recovery plans are documented and tested on a regular basis to ensure that they remain current and operational – Backup and recovery plans allow users of information systems to resume operations in the event of an interruption – Application controls are designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system – Access to the Implementation Guide (IMG) during production has been restricted – The production client settings have been flagged to not allow changes to programs and 		

Audit/Accurance Program for SAP ERP Inventory Business Cycle							
Phase A—Determine Scope of the Assurance Initiative							
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment		
		<p>configuration</p> <ul style="list-style-type: none"> • Identify the significant risk and determine the key controls <ul style="list-style-type: none"> - Develop a high-level process flow diagram and overall understanding of the Inventory Module, including the following subprocesses: <ul style="list-style-type: none"> a. Master data maintenance b. Raw materials management c. Producing and costing inventory d. Handling and shipping finished goods - Assess the key risk, determine key controls or control weaknesses, and test controls (refer to the sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> a. The controls culture of the organization (e.g., a just-enough-control philosophy). b. The need to exercise judgment to determine the key controls in the process and whether the controls structure is adequate. (Any weaknesses in the control structure should be reported to executive management and resolved.) • Gain an understanding of the SAP ERP environment (The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles) <p>In particular, the following information is important:</p> <ul style="list-style-type: none"> - Version and release of SAP ERP implemented - Total number of named users (for comparison with logical access security testing results) - Number of SAP instances and clients - Accounting period, company codes and chart of accounts - Identification of the components being used (Human Capital Management, Financials, Operations, Corporate Services) - Whether the organization has created any locally developed ABAP programs or reports - Details of the risk assessment approach taken in the organization to identify and prioritize risk - Copies of the organization's key security policies and standards <p>Obtain details of the following:</p> <ul style="list-style-type: none"> - Organizational Management Model as it relates to sales/revenue activity, i.e., sales organizational unit structure in SAP ERP and company sales organizational chart (required when evaluating the results of access security control testing) - An interview of the systems implementation team, if possible, and process design documentation for sales and distribution 					
A-2.3	<u>Understand</u> the external context of the enterprise.	<i>Identify all external environmental factors that could influence the performance and contents of the SAP ERP Inventory Module.</i>					
A-2.4	Given the overall assurance objective, translate the identified strategic priorities into concrete <u>objectives</u> for the assurance engagement.	The following goals are retained as key goals to be supported, in reflection of enterprise strategy and priorities: <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px; vertical-align: top;">Key goals</td> <td style="padding: 5px; vertical-align: top;">Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality </td> </tr> </table>		Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality 		
Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality 						

Audit/Accurance Program for SAP ERP Inventory Business Cycle					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
		<ul style="list-style-type: none"> • EG15 Compliance with internal policies <p>IT-related goals:</p> <ul style="list-style-type: none"> • ITG01 Alignment of IT and business strategy • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG09 IT Agility • ITG10 Security of information, processing infrastructure and applications • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG15 IT compliance with internal policies • ITG16 Competent and motivated business and IT personnel 			
		<p>Additional goals</p>			
A-2.5	Define the organizational boundaries of the assurance initiative.	<p><i>Describe the organizational boundaries of the assurance engagement, i.e., to which organizational entities the review is limited. All other aspects of scope limitation are identified during phase A-3.</i></p> <ul style="list-style-type: none"> • The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment. • Obtain information and form an understanding of the business reasons underlying the audit. • Identify the senior business resources responsible for the review. • Identify the senior IT audit/assurance resource responsible for the review. • Establish the process for suggesting and implementing changes to the audit/assurance program, and list the authorizations required. • Identify any limitations and/or constraints affecting the audit of specific systems and subsystems. • Identify and third party services, applications, platforms and infrastructure elements that may not be or only partially be accessible. • Identify any legal, regulatory or contractual constraints on audit. • Identify any industrial relations based or end user based audit constraints. 			

Audit/Accurance Program for SAP ERP Inventory Business Cycle								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
A-3	Determine the enablers in scope and the instance(s) of the enablers in scope.	COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.						
A-3.1	<u>Define the Principles, Policies and Frameworks</u> in scope.	<p>Guiding principles and policies include:</p> <ul style="list-style-type: none"> • Policy for Master Data Maintenance • ISMS policy • Legal and regulatory compliance requirements 						
A-3.2	<p><u>Define which Processes</u> are in scope of the review.</p> <p>Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of process goals • Application of process good practices • Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments) 	<p><i>COBIT 5: Enabling Processes</i> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed.</p> <table border="1"> <tr> <td>Key processes</td><td> <ul style="list-style-type: none"> • Master Data Maintenance • Raw Materials Management • Producing and Costing Inventory • Handling and Shipping Finished Goods </td></tr> <tr> <td>Additional processes</td><td> <ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI04 Manage Availability and Capacity • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance </td></tr> </table>	Key processes	<ul style="list-style-type: none"> • Master Data Maintenance • Raw Materials Management • Producing and Costing Inventory • Handling and Shipping Finished Goods 	Additional processes	<ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI04 Manage Availability and Capacity • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance 		
Key processes	<ul style="list-style-type: none"> • Master Data Maintenance • Raw Materials Management • Producing and Costing Inventory • Handling and Shipping Finished Goods 							
Additional processes	<ul style="list-style-type: none"> • APO01 Mange the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI04 Manage Availability and Capacity • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance 							
A-3.3	<p><u>Define which Organisational Structures</u> will be in scope.</p> <p>Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of Organisational Structure goals, i.e., decisions • Application of Organisational Structures good practices 	<p>Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail.</p> <table border="1"> <tr> <td>Key Organisational Structures</td><td> <ul style="list-style-type: none"> • Warehouse • Quality • Shipping • Financial accounting • Tax department • General Accounting • Treasury </td></tr> <tr> <td>Additional Organisational Structures</td><td> <ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Tax department </td></tr> </table>	Key Organisational Structures	<ul style="list-style-type: none"> • Warehouse • Quality • Shipping • Financial accounting • Tax department • General Accounting • Treasury 	Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Tax department 		
Key Organisational Structures	<ul style="list-style-type: none"> • Warehouse • Quality • Shipping • Financial accounting • Tax department • General Accounting • Treasury 							
Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Tax department 							

Audit/Accurance Program for SAP ERP Inventory Business Cycle									
Phase A—Determine Scope of the Assurance Initiative									
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment				
A-3.4	<u>Define the Culture, Ethics and Behaviour</u> aspects in scope.	<ul style="list-style-type: none"> Change Management Office <p>In the context of this engagement, the following enterprise-wide culture and behaviours are in scope:</p> <ul style="list-style-type: none"> Risk and compliance aware culture Enabling of continuous improvement Accountability Discipline to follow instructions 							
A-3.5	<u>Define the Information items</u> in scope. Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> Achievement of Information goals, i.e., quality criteria of the information items Application of Information good practices (Information attributes) 	<p>Based on the subject matter of this audit/assurance program, the following Information items have been identified as key items.</p> <table border="1"> <tr> <td>Key Information Items</td><td> <ul style="list-style-type: none"> Data integrity procedures Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis Retention requirements Record of transactions Training manuals Job aids </td></tr> <tr> <td>Additional Information Items</td><td> <ul style="list-style-type: none"> Organizational charts </td></tr> </table>		Key Information Items	<ul style="list-style-type: none"> Data integrity procedures Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis Retention requirements Record of transactions Training manuals Job aids 	Additional Information Items	<ul style="list-style-type: none"> Organizational charts 		
Key Information Items	<ul style="list-style-type: none"> Data integrity procedures Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis Retention requirements Record of transactions Training manuals Job aids 								
Additional Information Items	<ul style="list-style-type: none"> Organizational charts 								
A-3.6	<u>Define the Services, Infrastructure and Applications</u> in scope.	<p>In the context of this assignment, and taking into account the goals identified in A-2.4, the following services and related applications or infrastructure could be considered in scope of the review:</p> <ul style="list-style-type: none"> SAP ERP System Master data maintenance Change management SAP training 							
A-3.7	<u>Define the People, Skills and Competencies</u> in scope. Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> Achievement of skills set goals Application of skills set and competencies good practices 	<p>In the context of this engagement, taking into account key processes and key roles, the following skill sets are included in scope:</p> <ul style="list-style-type: none"> Proficiency using the SAP Materials Management Module Master data management skills Materials management skills and experience Proficiency running SAP reports Understanding of data classification policies Understanding of data integrity procedures 							

Audit/Accuracy Program for SAP ERP Inventory Business Cycle																											
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment																						
B-1	Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.																										
B-1.1	<p><u>Obtain</u> (and <u>agree on</u>) metrics for enterprise goals and expected values of the metrics. <u>Assess</u> whether enterprise goals in scope are achieved.</p> <p>Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.</p> <p>Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</p> <p>The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>Enterprise Goal</th><th>Metric</th><th>Expected Outcome (Ex)</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>EG03 Managed business risk (safeguarding of assets)</td><td> <ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG04 Compliance with external laws and regulations</td><td> <ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG07 Business service continuity and availability</td><td> <ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG11 Optimisation of business process functionality</td><td> <ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG15 Compliance with internal policies</td><td> <ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>	Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step	EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG04 Compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG04 Compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
B-1.2	<p><u>Obtain</u> (and <u>agree on</u>) metrics for IT-related goals and expected values of the metrics and <u>assess</u> whether IT-related goals in scope are achieved.</p> <p>The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>IT-related Goal</th><th>Metric</th><th>Expected Outcome (Ex)</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>ITG01 Alignment of IT and business strategy</td><td> <ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals </td><td>Agree on the expected values for the IT-related goal metrics, i.e.,</td><td>In this step, the related metrics for each goal will be reviewed and an</td></tr> </tbody> </table>	IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step	ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals 	Agree on the expected values for the IT-related goal metrics, i.e.,	In this step, the related metrics for each goal will be reviewed and an																		
IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals 	Agree on the expected values for the IT-related goal metrics, i.e.,	In this step, the related metrics for each goal will be reviewed and an																								

Audit/Accuracy Program for SAP ERP Inventory Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services Percent of IT value drivers mapped to business value drivers 	<i>the values against which the assessment will take place.</i>	<i>assessment will be made whether the defined criteria are achieved.</i>	
ITG02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment Number of non-compliance issues relating to contractual agreements with IT service providers Coverage of compliance assessments 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
ITG04 Managed IT-related business risk	<ul style="list-style-type: none"> Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent of enterprise risk assessments including IT-related risk Frequency of update of risk profile 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
ITG07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
ITG08 Adequate use of applications, information and technology solutions	<ul style="list-style-type: none"> Percent of business process owners satisfied with supporting IT products and services Level of business user understanding of how technology solutions support their processes Satisfaction level of business users with training and user manuals Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
ITG09 IT Agility	<ul style="list-style-type: none"> Level of satisfaction of business executives with IT's responsiveness to new requirements Number of critical business processes supported by up-to-date infrastructure and applications Average time to turn strategic IT objectives into an agreed-on and approved initiative 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		

Audit/Accuracy Program for SAP ERP Inventory Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	ITG10 Security of information, processing infrastructure and applications	<ul style="list-style-type: none"> Number of security incidents causing financial loss, business disruption or public embarrassment Number of IT services with outstanding security requirements Time to grant, change and remove access privileges, compared to agreed-on service levels Frequency of security assessment against latest standards and guidelines 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG12 Enablement and support of business processes by integrating applications and technology into business processes	<ul style="list-style-type: none"> Number of business processing incidents caused by technology integration errors Number of business process changes that need to be delayed or reworked because of technology integration issues Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues Number of applications or critical infrastructures operating in silos and not integrated 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG14 Availability of reliable and useful information for decision making	<ul style="list-style-type: none"> Level of business user satisfaction with quality and timeliness (or availability) of management information Number of business process incidents caused by non-availability of information Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG15 IT compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices Frequency of policies review and update 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG16 Competent and motivated business and IT personnel	<ul style="list-style-type: none"> Percent of staff whose IT-related skills are sufficient for the competency required for their role Percent of staff satisfied with their IT-related roles Number of learning/training hours per staff member 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	

Audit/Accuracy Program for SAP ERP Inventory Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-2	Obtain an understanding of the Principles, Policies and Frameworks in scope and set suitable assessment criteria. Assess Principles, Policies and Frameworks.		
Principles, policies and frameworks: Policy for Master Data Maintenance			
B-2.1a	<u>Understand the Principles, Policies and Frameworks context.</u> <i>Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks</i>		
B-2.2a	<u>Understand the stakeholders of the Principles, Policies and Frameworks.</u> <i>Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.</i>		
B-2.3a	<u>Understand the goals for the Principles, Policies and Frameworks</u> , and the related metrics and agree on expected values. Assess whether the Principles, Policies and Frameworks goals (outcomes) are achieved, i.e., assess the effectiveness of the Principles, Policies and Frameworks . Goal: The organization has defined, disseminated and deployed management policies supporting SAP master data maintenance .	Perform the assurance steps using the example criteria described below.	
Goal	Criteria	Assessment Step	
Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.	
Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none">A regular validation of all policies whether they are still up to dateAn indication of the policies' expiration date or date of last update	Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none">A regular validation of all policies whether they are still up to dateAn indication of the policies' expiration date or date of last update	
Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.	
Availability	<ul style="list-style-type: none">Policies are available to all stakeholders.Policies are easy to navigate and have a logical and hierarchical structure.	<ul style="list-style-type: none">Verify that policies are available to all stakeholders.Verify that policies are easy to navigate and have a logical and hierarchical structure.	
B-2.4a	<u>Understand the life cycle stages of the Principles, Policies and Frameworks</u> , and agree on the relevant criteria. Assess to what extent the Principles, Policies and Frameworks life cycle is managed. <i>The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01 Manage the IT management framework.</i>		
B-2.5a	<u>Understand good practices related to the Principles, Policies and Frameworks</u> and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. <i>The assurance professional will, by using appropriate auditing techniques assess the following aspects.</i>		
Good Practice	Criteria	Assessment Step	
Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.	
Exception and escalation	<ul style="list-style-type: none">The exception and escalation procedure is explained and commonly known.	<ul style="list-style-type: none">Verify that the exception and escalation procedure is described, explained and commonly known.Through observation of a representative sample, verify that the	

Audit/Assurance Program for SAP ERP Inventory Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> The exception and escalation procedure has not become the de facto standard procedure. 	exception and escalation procedure has not become <i>de facto</i> standard procedure.		
	Compliance	The compliance checking mechanism and non-compliance consequences are clearly described and enforced.	Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.		
B-2.1 to B-2.5	Repeat steps B-2.1 through B-2.5 for all remaining Principles, Policies and Frameworks in scope. Repeat the steps described above for the remaining Principles, Policies and Frameworks: <ul style="list-style-type: none"> ISMS policy Legal and regulatory compliance requirements 				

Audit/Accurance Program for SAP ERP Inventory Business Cycle						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment
B-3	Obtain understanding of the Processes in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes.					
SAP ERP Inventory process²: Master data maintenance						
B-3.1a	<u>Understand the Process context.</u>					
B-3.2a	<u>Understand the Process purpose.</u>					
B-3.3a	<u>Understand</u> all process stakeholders and their roles. This is equivalent to understanding the real RACI chart of the process. <i>Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.</i> The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement: Master data maintenance stakeholders:					
B-3.4a	<u>Understand the Process goals</u> and related metrics³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process. The Process Master data maintenance has three defined process goal.				The following activities can be performed to assess whether the goals are achieved.	
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	Issue Cross-reference	Comment	
Master data records are valid, complete, accurate and timely	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>			
Inventory master data remains current and pertinent	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>			
Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>			
B-3.5a	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement: <u>Define</u> and <u>agree</u> on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.) <u>Agree</u> on the process practices that should be in place (process design). <u>Assess</u> the process design , i.e., assess to what extent: <ul style="list-style-type: none"> • Expected process practices are applied. 					

² Because this is a business process audit/assurance program, several of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources available.

³ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

Audit/Accurance Program for SAP ERP Inventory Business Cycle																																																		
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																		
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																																												
	<ul style="list-style-type: none"> • Accountability and responsibility are assigned and assumed. <p>Evaluate Master data maintenance</p> <p>COBIT 5 Processes⁴ are described in <i>COBIT 5: Enabling Processes</i>. Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are:</p> <ul style="list-style-type: none"> • A sound process design <p>The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented.</p>																																																	
	<table border="1"> <tr> <td>Reference Process</td> <td>Master data maintenance</td> <td>Criteria: 1.1 Changes made to master data are valid, complete, accurate and timely. 1.2 Inventory master data remains current and pertinent. 1.3 Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.</td> <td></td> <td></td> <td></td> </tr> </table>				Reference Process	Master data maintenance	Criteria: 1.1 Changes made to master data are valid, complete, accurate and timely. 1.2 Inventory master data remains current and pertinent. 1.3 Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.																																											
Reference Process	Master data maintenance	Criteria: 1.1 Changes made to master data are valid, complete, accurate and timely. 1.2 Inventory master data remains current and pertinent. 1.3 Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.																																																
	<table border="1"> <tr> <th>Reference Process Practices⁵</th> <th>Good Practice</th> <th colspan="2">Assessment Step</th> <th>Issue Cross-reference</th> <th>Comment</th> </tr> <tr> <td>DSS06</td> <td>Changes made to master data are valid, complete, accurate and timely.</td> <td colspan="2">1.1.1 Confirm that management executes transaction code MM04—Display Material Change Documents periodically and compares against source documents. Request a sample of source documents for evidence of comparison to inventory file updates.</td> <td></td><td></td></tr> <tr> <td>DSS05 DSS06</td> <td>Changes made to master data are valid, complete, accurate and timely.</td> <td colspan="2">1.1.2 Review enterprise policies and process design specifications regarding access to maintain master data. Use transaction code SUIM to test user access to create (transaction code MM01), maintain (transaction code MM02) and delete (transaction code MM06) material master data.</td> <td></td><td></td></tr> <tr> <td>DSS06</td> <td>Changes made to master data are valid, complete, accurate and timely.</td> <td colspan="2"> <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td rowspan="2">MM01—Create Material &</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td rowspan="2">MM02—Change Material &</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td rowspan="2">MM06—Flag Material for Deletion</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>06</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>06</td> </tr> </tbody> </table> 1.1.3 Determine whether the configurable control settings address the risk pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management's intentions. Use transaction code SPRO to display the IMG menu and follow the path as follows: <ul style="list-style-type: none"> • Material types: Logistics—General → Material Master → Basic Settings → Material </td> <td></td><td></td></tr> </table>	Reference Process Practices ⁵	Good Practice	Assessment Step		Issue Cross-reference	Comment	DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.1 Confirm that management executes transaction code MM04—Display Material Change Documents periodically and compares against source documents. Request a sample of source documents for evidence of comparison to inventory file updates.				DSS05 DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.2 Review enterprise policies and process design specifications regarding access to maintain master data. Use transaction code SUIM to test user access to create (transaction code MM01), maintain (transaction code MM02) and delete (transaction code MM06) material master data.				DSS06	Changes made to master data are valid, complete, accurate and timely.	<table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td rowspan="2">MM01—Create Material &</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td rowspan="2">MM02—Change Material &</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td rowspan="2">MM06—Flag Material for Deletion</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>06</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>06</td> </tr> </tbody> </table> 1.1.3 Determine whether the configurable control settings address the risk pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management's intentions. Use transaction code SPRO to display the IMG menu and follow the path as follows: <ul style="list-style-type: none"> • Material types: Logistics—General → Material Master → Basic Settings → Material 		Transaction(s)	Authorization Objects	Fields	Values	MM01—Create Material &	M_MATE_MAR	ACTVT	01	M_MATE_STA	ACTVT	01	MM02—Change Material &	M_MATE_MAR	ACTVT	02	M_MATE_STA	ACTVT	02	MM06—Flag Material for Deletion	M_MATE_MAR	ACTVT	06	M_MATE_STA	ACTVT	06		
Reference Process Practices ⁵	Good Practice	Assessment Step		Issue Cross-reference	Comment																																													
DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.1 Confirm that management executes transaction code MM04—Display Material Change Documents periodically and compares against source documents. Request a sample of source documents for evidence of comparison to inventory file updates.																																																
DSS05 DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.2 Review enterprise policies and process design specifications regarding access to maintain master data. Use transaction code SUIM to test user access to create (transaction code MM01), maintain (transaction code MM02) and delete (transaction code MM06) material master data.																																																
DSS06	Changes made to master data are valid, complete, accurate and timely.	<table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td rowspan="2">MM01—Create Material &</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td rowspan="2">MM02—Change Material &</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td rowspan="2">MM06—Flag Material for Deletion</td> <td>M_MATE_MAR</td> <td>ACTVT</td> <td>06</td> </tr> <tr> <td>M_MATE_STA</td> <td>ACTVT</td> <td>06</td> </tr> </tbody> </table> 1.1.3 Determine whether the configurable control settings address the risk pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management's intentions. Use transaction code SPRO to display the IMG menu and follow the path as follows: <ul style="list-style-type: none"> • Material types: Logistics—General → Material Master → Basic Settings → Material 		Transaction(s)	Authorization Objects	Fields	Values	MM01—Create Material &	M_MATE_MAR	ACTVT	01	M_MATE_STA	ACTVT	01	MM02—Change Material &	M_MATE_MAR	ACTVT	02	M_MATE_STA	ACTVT	02	MM06—Flag Material for Deletion	M_MATE_MAR	ACTVT	06	M_MATE_STA	ACTVT	06																						
Transaction(s)	Authorization Objects	Fields	Values																																															
MM01—Create Material &	M_MATE_MAR	ACTVT	01																																															
	M_MATE_STA	ACTVT	01																																															
MM02—Change Material &	M_MATE_MAR	ACTVT	02																																															
	M_MATE_STA	ACTVT	02																																															
MM06—Flag Material for Deletion	M_MATE_MAR	ACTVT	06																																															
	M_MATE_STA	ACTVT	06																																															

⁴ For this audit/assurance program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the SAP ERP Inventory processes in scope.

⁵ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Inventory audit/assurance program.

Audit/Accuracy Program for SAP ERP Inventory Business Cycle																			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																			
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment														
			<p>Types → Define Attributes of Material Types</p> <ul style="list-style-type: none"> Industry sector: Logistics—General → Material Master → Field Selection → Define Industry Sectors and Industry Sector-Specific Field Selection Default price types: Execute transaction code OMW1—C RM-MAT MW Price Control, and determine whether default settings have been applied for the price control for material records. 																
	DSS01 DSS06	Changes made to master data are valid, complete, accurate and timely.	<p>1.1.4 Determine whether appropriate management is reviewing the Materials List (transaction code MM60), or equivalent, by material type and confirm evidence of management's review of the data on a periodic basis for accuracy and ongoing validity.</p> <p>Request evidence that management reviews periodically material master data (purchasing materials only) to verify whether the over delivery tolerance has been configured according to enterprise policies.</p> <p>Material master data tolerances are configured under the purchasing tab. Use transaction code MM01—Create Material or MM03—Display Material and review tolerance limits for a sample of material master records. Verify with management if the limits follow enterprise policies.</p>																
	DSS06	Inventory master data remains current and pertinent.	<p>1.2.1 Determine if the enterprise uses negative stocks for especial materials. Note: the standard SAP ERP settings do not allow negative stocks. The Neg. stocks allowed indicator has to be enabled to display the field in material master records. To configure negative stocks use transaction code SPRO to display the IMG menu and follow the path: Material Management→ Inventory Management and Physical Inventory→ Goods issue/transfer posting→ allow negative stocks (select plant and storage location).</p> <p>The indicator to allow negative stock must be enabled in the material master record of the specific materials for which negative stocks are allowed. Select a sample of material master records that allow negative stocks and confirm that management approved the configuration according to enterprise policies.</p>																
	DSS05	Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.	<p>1.3.1 Review enterprise policy and process design specifications regarding access to maintain BOM and process order settlement rules. Use transaction code SUIM—User Information System to test user access to create (transaction code CS01), change (transaction code CS02), make mass changes to (transaction code CS20), change single-layered work breakdown structure (WBS) BOM (transaction code CS72), change multilevel WBS BOM (transaction code CS75), and change multilevel WBS BOM using the browser (transaction code CSPB).</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td rowspan="2">CS01—Create Material BOM</td><td>C_AENR_RV1</td><td>ACTVT</td><td>01</td></tr> <tr> <td>C_STUE_BER</td><td>ACTVT</td><td>01</td></tr> <tr> <td>CS02—Change Material BOM</td><td>C_STUE_BER</td><td>ACTVT</td><td>02</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	CS01—Create Material BOM	C_AENR_RV1	ACTVT	01	C_STUE_BER	ACTVT	01	CS02—Change Material BOM	C_STUE_BER	ACTVT	02	
Transaction(s)	Authorization Objects	Fields	Values																
CS01—Create Material BOM	C_AENR_RV1	ACTVT	01																
	C_STUE_BER	ACTVT	01																
CS02—Change Material BOM	C_STUE_BER	ACTVT	02																

Audit/Accuracy Program for SAP ERP Inventory Business Cycle										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes										
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment		
B-3.6a	DSS06	Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.	1.3.2 Take a sample of BOM updates using transaction CS80— Change Documents for Material BOM and compare to authorized source documentation.	C_STUE_WRK	ACTVT	02				
				CS20— Mass Change: Initial Screen	C_STUE_BER	ACTVT				
				CS72—Change WBS BOM	C_STUE_BER	ACTVT				
					C_STUE_WRK	ACTVT				
					C_AENR_BGR	ACTVT				
				CS75— Change multilevel WBS BOM	C_STUE_BER	ACTVT				
					C_STUE_WRK	ACTVT				
					C_AENR_BGR	ACTVT				
				Test user access to transaction CSPB—Start WBS BOM Browser.						
				Test user access to change settlement rules (user transaction code COR2 and follow the menu path: Logistic → Production—Process → Process Order → Process Order→ Change (enter the process order number and press Enter) →Header→ Settlement Rule.						
B-3.7a				Agree on the process work products ⁶ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.						
				Process Master data maintenance inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.		Criteria: All listed work products should demonstrably exist and be used.				
				Process Practice	Work Products	Assessment Step				
				Master data maintenance	<ul style="list-style-type: none"> • Master data add/change/delete request forms • Master data maintenance procedures • Master data maintenance reports • List of SAP users with master data access 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.				
B-3.7a				Agree on the process capability level to be achieved by the process.						
				<i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>						
SAP ERP Inventory process: Raw materials management										
B-3.1b	Understand the Process context .									

⁶ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accuracy Program for SAP ERP Inventory Business Cycle																													
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																													
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																							
B-3.2b	<u>Understand the Process purpose.</u>																												
B-3.3b	<u>Understand all process stakeholders</u> and their roles: Raw materials management stakeholders:																												
B-3.4b	<u>Understand the Process goals</u> and related metrics ⁷ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process. The Process Raw materials management has three defined process goals.																												
<table border="1"> <thead> <tr> <th>Process Goal</th> <th>Related Metrics</th> <th>Criteria/Expected Value</th> <th>Assessment Step</th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>Inventory is salable, usable, and adequately safeguarded</td> <td> <ul style="list-style-type: none"> Slow moving inventory report Zero turns inventory report Number and value of miscellaneous adjustments Number and value of scrap adjustments </td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> <td></td> <td></td> </tr> <tr> <td>Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner</td> <td> <ul style="list-style-type: none"> Number and value of miscellaneous adjustments Number and value of scrap adjustments </td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> <td></td> <td></td> </tr> <tr> <td>Defective raw materials are returned to suppliers in a timely manner</td> <td> <ul style="list-style-type: none"> Number of material returns to vendor with average # of days since receipt of same PO line. </td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> <td></td> <td></td> </tr> </tbody> </table>						Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step			Inventory is salable, usable, and adequately safeguarded	<ul style="list-style-type: none"> Slow moving inventory report Zero turns inventory report Number and value of miscellaneous adjustments Number and value of scrap adjustments 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner	<ul style="list-style-type: none"> Number and value of miscellaneous adjustments Number and value of scrap adjustments 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			Defective raw materials are returned to suppliers in a timely manner	<ul style="list-style-type: none"> Number of material returns to vendor with average # of days since receipt of same PO line. 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step																										
Inventory is salable, usable, and adequately safeguarded	<ul style="list-style-type: none"> Slow moving inventory report Zero turns inventory report Number and value of miscellaneous adjustments Number and value of scrap adjustments 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																										
Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner	<ul style="list-style-type: none"> Number and value of miscellaneous adjustments Number and value of scrap adjustments 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																										
Defective raw materials are returned to suppliers in a timely manner	<ul style="list-style-type: none"> Number of material returns to vendor with average # of days since receipt of same PO line. 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																										
B-3.5b	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement: Evaluate Raw materials management <table border="1"> <thead> <tr> <th>Reference Process</th> <th>Raw materials management</th> <th>Criteria:</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td> 2.1 Inventory is salable, usable and adequately safeguarded. 2.2 Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. 2.3 Defective raw materials are returned to suppliers in a timely manner. </td> <td></td> </tr> <tr> <th>Reference Process Practices⁸</th> <th>Good Practice</th> <th>Assessment Step</th> <th>Issue Cross-reference</th> <th>Comment</th> </tr> <tr> <td>APO11 BAI04 DSS01 DSS06</td> <td>Inventory is salable, usable, and adequately safeguarded.</td> <td> 2.1.1 Confirm that the MRP process takes into account stock on hand, forecast requirements, economic order quantities and back orders. Confirm that data elements for MRP have been created as follows: <ul style="list-style-type: none"> Material master Bill of materials </td> <td></td> <td></td> </tr> </tbody> </table>				Reference Process	Raw materials management	Criteria:				2.1 Inventory is salable, usable and adequately safeguarded. 2.2 Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. 2.3 Defective raw materials are returned to suppliers in a timely manner.		Reference Process Practices ⁸	Good Practice	Assessment Step	Issue Cross-reference	Comment	APO11 BAI04 DSS01 DSS06	Inventory is salable, usable, and adequately safeguarded.	2.1.1 Confirm that the MRP process takes into account stock on hand, forecast requirements, economic order quantities and back orders. Confirm that data elements for MRP have been created as follows: <ul style="list-style-type: none"> Material master Bill of materials 									
Reference Process	Raw materials management	Criteria:																											
		2.1 Inventory is salable, usable and adequately safeguarded. 2.2 Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner. 2.3 Defective raw materials are returned to suppliers in a timely manner.																											
Reference Process Practices ⁸	Good Practice	Assessment Step	Issue Cross-reference	Comment																									
APO11 BAI04 DSS01 DSS06	Inventory is salable, usable, and adequately safeguarded.	2.1.1 Confirm that the MRP process takes into account stock on hand, forecast requirements, economic order quantities and back orders. Confirm that data elements for MRP have been created as follows: <ul style="list-style-type: none"> Material master Bill of materials 																											

⁷ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

⁸ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Inventory audit/accuracy program.

Audit/Accuracy Program for SAP ERP Inventory Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
			<ul style="list-style-type: none"> • Work centers • Routings • Demand management <p>Review the MRP configuration using transaction code SPRO to open the IMG menu and follow path: Material Management→Production Material →Requirement Planning. Validate with management that the settings meet production specifications.</p>		
	BAI04 DSS06	Inventory is salable, usable, and adequately safeguarded.	<p>2.1.2 Use transaction code MB5M—BBD/Prod. Date and ascertain the reason for an old stock being held (shelf life list).</p> <p>Use transaction code MC50— Analysis of Dead Stock (i.e., stock quantity held in excess of production demands).</p> <p>Request evidence that management is reviewing this information on a regular basis.</p>		
	APO11 DSS01	Inventory is salable, usable, and adequately safeguarded.	<p>2.1.3 Through interviews and observation, confirm that the quality department tests samples of raw materials, and rejected materials are adequately segregated into a separate quality assurance holding area and regularly monitored by the quality department personnel to ensure timely return to suppliers.</p> <p>Obtain evidence that materials are returned to suppliers.</p>		
	DSS01 DSS06	Inventory is salable, usable, and adequately safeguarded.	<p>2.1.4 Use transaction code MC46—Analysis of Slow-Moving Item to identify stock that has not been used for a certain period of time. Obtain evidence that management reviews of slow-turnover inventory and takes appropriate steps to address any unsalable materials.</p>		
	DSS05 DSS06	Inventory is salable, usable, and adequately safeguarded.	<p>2.1.5 Inquire about the processes for shipping and receiving materials and obtain any documented procedures. Validate that personnel follows the process as described by management.</p> <p>Obtain evidence that all inbound and outbound movements are accompanied by the necessary documentation.</p>		
	DSS05 DSS06	Inventory is salable, usable, and adequately safeguarded.	<p>2.1.6 Inquire about the processes for receiving and storing materials and obtain any documented procedures. Validate that personnel follows the process as described by management.</p> <p>Request to visit one or more areas designated to receive deliveries of raw materials and assess if physical security controls are in place to restrict access to authorized personnel only.</p> <p>Obtain evidence that physical security procedures are properly followed.</p>		
	DSS05 DSS06	Inventory is salable, usable, and adequately safeguarded.	<p>2.1.7 Use testing technique 2.1.6 to test physical security controls for storage areas.</p>		
	DSS01 DSS06	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	<p>2.2.1 Review the reconciliation of the GR and/or IR accounts. Using transaction code MB5S—Display List of GR/IR Balances determine whether GR/IR account balances are periodically executed and reviewed. Check that there are appropriate procedures in place to investigate unmatched POs. In particular, long outstanding items should be followed up</p>		

Audit/Assurance Program for SAP ERP Inventory Business Cycle																		
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																		
Ref.	Assurance Steps and Guidance			Issue Cross-reference														
				Comment														
		<p>and cleared. Also check with the management and confirm that authorized individuals are given access to transaction code MR11—GR/IR account maintenance, which allows postings to GL (write off differences).</p> <p>Use transaction code SUIM—User Information System to review the following authorization codes and activities:</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="3">MR11— GR/IR Account Maintenance</td><td>F_BKPF_BLA</td><td>ACTVT</td><td>02</td></tr> <tr> <td>F_BKPF_BUK</td><td>ACTVT</td><td>02</td></tr> <tr> <td>F_BKPF_GSB</td><td></td><td></td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	MR11— GR/IR Account Maintenance	F_BKPF_BLA	ACTVT	02	F_BKPF_BUK	ACTVT	02	F_BKPF_GSB				
Transaction(s)	Authorization Objects	Fields	Values															
MR11— GR/IR Account Maintenance	F_BKPF_BLA	ACTVT	02															
	F_BKPF_BUK	ACTVT	02															
	F_BKPF_GSB																	
DSS01 DSS06	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	<p>2.2.2 Use transaction code ME2M—Purchase Orders by Material to create a report of outstanding POs and ascertain from management whether there are reasons for any long-outstanding items on the report.</p> <p>Request evidence that management review periodically the list of open good receipt notes, POs and invoices and follows up on outstanding items as necessary.</p>																
APO11 DSS01	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	2.2.3 Request evidence that documents are marked as matched or paid, once matched or upon payment of the invoice, to prevent reuse.																
DSS06	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	2.2.4 Request evidence that management review periodically exception reports of good not received on time and that an investigation is initiated to identify problems.																
DSS06	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	<p>2.2.5 Request evidence that goods received without a matching purchase order and overages are investigated before posting to the system and approving payment.</p> <p>Request evidence that management reviews periodically material master data (purchasing materials only) to verify whether the overdelivery tolerance has been configured according to enterprise policies.</p> <p>Use transaction code MM01—Create Material or MM03—Display Material and review tolerance limits for a sample of material master records. Verify with management whether the limits follow enterprise policies.</p>																
DSS05	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	<p>2.2.6 Use transaction code SUIM—User Information System to test user access to transactions for GR:</p> <ul style="list-style-type: none"> • Post Goods Receipt for PO—MB01 • Goods movement—MIGO • Post Goods Receipt for PO Unknown—MB0A • Goods Movement (MM)—MIGO_GO • Goods Movement (Inventory Mgt.)—MIGO_GI • Transfer Posting—MIGO_TR • GR for Production Order—MB31 																

Audit/Accuracy Program for SAP ERP Inventory Business Cycle																																												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																												
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																																						
		<ul style="list-style-type: none"> • Other Goods Receipts—MB1C • Cancel Material Document—MBST <table border="1" style="margin-top: 10px; width: 100%;"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>MB01— Post Goods Receipt for PO MB0A— Post Goods Receipt for PO Unknown MIGO— Goods movement MIGO_GO— Goods Movement (MM)</td> <td>M_MSEG_BWE</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>M_MSEG_WWE</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>MB31— GR for Production Order</td> <td>M_RAHM_BSA</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>M_RAHM_EKO</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>MB1C— Other Goods Receipts</td> <td>M_MSEG_BWA</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>M_MSEG_BWE</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>M_MSEG_WWA</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>MBST— Cancel Material Document MIGO_GI— Goods Movement (Inventory Mgt.) MIGO_TR— Transfer Posting</td> <td>M_MSEG_BMB</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td></td> <td>M_MSEG_WMB</td> <td>ACTVT</td> <td>01</td> </tr> </tbody> </table> <p style="margin-top: 10px;">Test user access to high-risk movement types 561 through 566. These special movement types reflect the initial stock entry in the SAP ERP system at the time of conversion to the SAP ERP system.</p>	Transaction(s)	Authorization Objects	Fields	Values	MB01— Post Goods Receipt for PO MB0A— Post Goods Receipt for PO Unknown MIGO— Goods movement MIGO_GO— Goods Movement (MM)	M_MSEG_BWE	ACTVT	01		M_MSEG_WWE	ACTVT	01	MB31— GR for Production Order	M_RAHM_BSA	ACTVT	01		M_RAHM_EKO	ACTVT	01	MB1C— Other Goods Receipts	M_MSEG_BWA	ACTVT	01		M_MSEG_BWE	ACTVT	01		M_MSEG_WWA	ACTVT	01	MBST— Cancel Material Document MIGO_GI— Goods Movement (Inventory Mgt.) MIGO_TR— Transfer Posting	M_MSEG_BMB	ACTVT	01		M_MSEG_WMB	ACTVT	01		
Transaction(s)	Authorization Objects	Fields	Values																																									
MB01— Post Goods Receipt for PO MB0A— Post Goods Receipt for PO Unknown MIGO— Goods movement MIGO_GO— Goods Movement (MM)	M_MSEG_BWE	ACTVT	01																																									
	M_MSEG_WWE	ACTVT	01																																									
MB31— GR for Production Order	M_RAHM_BSA	ACTVT	01																																									
	M_RAHM_EKO	ACTVT	01																																									
MB1C— Other Goods Receipts	M_MSEG_BWA	ACTVT	01																																									
	M_MSEG_BWE	ACTVT	01																																									
	M_MSEG_WWA	ACTVT	01																																									
MBST— Cancel Material Document MIGO_GI— Goods Movement (Inventory Mgt.) MIGO_TR— Transfer Posting	M_MSEG_BMB	ACTVT	01																																									
	M_MSEG_WMB	ACTVT	01																																									
DSS01	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	<p>2.2.7 Review the process for physical stock takes to confirm the complete, accurate, valid and timely recording of adjustments as a result of the stock-takes.</p> <p>Obtain evidence that count of physical inventory on a continuous basis is conducted by persons independent of day-to-day custody or recording of inventory.</p>																																										
DSS01 DSS06	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	<p>2.2.8 Obtain evidence that physical inventory counts are reconciled to inventory records, and inventory records are reconciled to the GL (through transfer documents in the SAP ERP system). Validate that changes to the quantities of the inventory take place when they are moved (for sale to customer, rework, transfer, etc.). Movement type configuration dictates whether a material movement will update the material quantity.</p> <p>Review material quantity changes and/or movements and corresponding movement types via transaction MB51—Material Document List, which allows for the review of changes to several materials at the same time. Transaction code MB59— Material Doc. List allows for the search on multiple materials by a particular range of dates for material movement types starting with 5 (i.e., 5*).</p>																																										

Audit/Accuracy Program for SAP ERP Inventory Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.6b			Obtain a sample of inventory file updates using transaction code MB59 and compare the results to authorized source documentation. Inventory adjustment forms should be sequentially numbered and the sequence accounted for.		
	DSS06	Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.	2.2.9 Obtain evidence that for raw materials and/or finished goods that are batch managed, there is an appropriate matching and accounting batch management strategy, including a periodic investigation on date expired, short expiration and defective batches, which are correctly matched with returned stock transactions.		
	APO11 DSS01	Defective raw materials are returned to suppliers in a timely manner.	2.3.1 Obtain evidence that rejected raw material is segregated in a specific holding area. Ascertain from management the movement type used to block processing and for returning rejected goods to suppliers (e.g., movement type 122).		
	APO10 DSS01	Defective raw materials are returned to suppliers in a timely manner	2.3.2 Execute transaction code MB51—Material Document List with the appropriate movement type. Determine whether there are any long outstanding materials pending return to suppliers and/or receipt of appropriate credits. Ascertain from management whether there are reasons for keeping the defective materials		
B-3.6b	<u>Agree on the process work products</u> ⁹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess</u> to what extent the process work products are available.				
	Process Raw materials management inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.		Criteria: All listed work products should demonstrably exist and be used.		
	Process Practice	Work Products	Assessment Step		
	Raw materials management	<ul style="list-style-type: none"> List of miscellaneous adjustments List of scrap adjustments 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		
B-3.7b	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				
SAP ERP Inventory process: Producing and costing inventory					
B-3.1c	<u>Understand the Process context.</u>				
B-3.2c	<u>Understand the Process purpose.</u>				
B-3.3c	<u>Understand all process stakeholders</u> and their roles:				
	Producing and costing inventory stakeholders:				
B-3.4c	<u>Understand the Process goals</u> and related <u>metrics</u> ¹⁰ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.				
	The Process Producing and costing inventory has one defined process goal.			The following activities can be performed to assess whether the goals are achieved.	
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step		
Transfers of materials to/from	<ul style="list-style-type: none"> Production order settlement 	Agree on the expected values for	In this step, the related metrics for		

⁹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

¹⁰ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Inventory Business Cycle																																							
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																							
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																																	
	production, production costs, and defective products/scrap are valid and recorded accurately, completely and in the appropriate period	completion rate • Number of aged production orders • Number of open production orders by month	<i>the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>																																			
B-3.5c	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement. Evaluate Producing and costing inventory <table border="1"> <thead> <tr> <th>Reference Process</th> <th>Producing and costing inventory</th> <th>Criteria: 3.1 Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.</th> <th>Assessment Step</th> <th>Issue Cross-reference</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td>DSS01</td> <td>Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.</td> <td>3.1.1 Review the policy and procedures concerning receiving and transfer of materials and confirm that the previously described controls are in place and operating. Obtain evidence that inventories and transfers received are compared to source documentation (e.g., pick list used to record movements of inventory in the financial records and recorded in the appropriate period).</td> <td></td> <td></td> <td></td> </tr> <tr> <td>APO11 DSS01</td> <td>Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.</td> <td>3.1.2 Review the policy and procedures for the accounting of in-transit inventory and confirm that the described controls are in place and operating. Obtain evidence that management reviews the inventory-in-transit reports to ensure that amounts are cleared and reconciled. Confirm that inbound accounts net off outbound accounts for transfers from other facilities.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>DSS01</td> <td>Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.</td> <td>3.1.3 Confirm that default price types have been established for all materials. Use transaction code OMW1— C RM-MAT MW Price Control, and determine whether default settings have been applied for the price control for material records.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>APO11</td> <td>Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.</td> <td>3.1.4 Review records of scrapped and reworked items and checks whether such items have been correctly identified and properly recorded in the appropriate accounting period.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>APO12 DSS06</td> <td>Transfers of materials to/from production, production costs and</td> <td>3.1.5 Test the tolerances for physical inventory differences: Use transaction code OMJ2— Maintain Phys.Inv.Tolmce->Employee, compare defined tolerances to organizational policy and judge for reasonableness.</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Reference Process	Producing and costing inventory	Criteria: 3.1 Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	Assessment Step	Issue Cross-reference	Comment	DSS01	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.1 Review the policy and procedures concerning receiving and transfer of materials and confirm that the previously described controls are in place and operating. Obtain evidence that inventories and transfers received are compared to source documentation (e.g., pick list used to record movements of inventory in the financial records and recorded in the appropriate period).				APO11 DSS01	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.2 Review the policy and procedures for the accounting of in-transit inventory and confirm that the described controls are in place and operating. Obtain evidence that management reviews the inventory-in-transit reports to ensure that amounts are cleared and reconciled. Confirm that inbound accounts net off outbound accounts for transfers from other facilities.				DSS01	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.3 Confirm that default price types have been established for all materials. Use transaction code OMW1— C RM-MAT MW Price Control, and determine whether default settings have been applied for the price control for material records.				APO11	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.4 Review records of scrapped and reworked items and checks whether such items have been correctly identified and properly recorded in the appropriate accounting period.				APO12 DSS06	Transfers of materials to/from production, production costs and	3.1.5 Test the tolerances for physical inventory differences: Use transaction code OMJ2— Maintain Phys.Inv.Tolmce->Employee, compare defined tolerances to organizational policy and judge for reasonableness.					
Reference Process	Producing and costing inventory	Criteria: 3.1 Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	Assessment Step	Issue Cross-reference	Comment																																		
DSS01	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.1 Review the policy and procedures concerning receiving and transfer of materials and confirm that the previously described controls are in place and operating. Obtain evidence that inventories and transfers received are compared to source documentation (e.g., pick list used to record movements of inventory in the financial records and recorded in the appropriate period).																																					
APO11 DSS01	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.2 Review the policy and procedures for the accounting of in-transit inventory and confirm that the described controls are in place and operating. Obtain evidence that management reviews the inventory-in-transit reports to ensure that amounts are cleared and reconciled. Confirm that inbound accounts net off outbound accounts for transfers from other facilities.																																					
DSS01	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.3 Confirm that default price types have been established for all materials. Use transaction code OMW1— C RM-MAT MW Price Control, and determine whether default settings have been applied for the price control for material records.																																					
APO11	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.4 Review records of scrapped and reworked items and checks whether such items have been correctly identified and properly recorded in the appropriate accounting period.																																					
APO12 DSS06	Transfers of materials to/from production, production costs and	3.1.5 Test the tolerances for physical inventory differences: Use transaction code OMJ2— Maintain Phys.Inv.Tolmce->Employee, compare defined tolerances to organizational policy and judge for reasonableness.																																					

¹¹ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Inventory audit/assurance program.

Audit/Accuracy Program for SAP ERP Inventory Business Cycle																																																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																																										
		defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	<p>Note: when transaction code OMJ2 is executed, the screen will provide two options for maintenance of inventory tolerance settings, either by physical inventory tolerance groups or by user name. If the company has adopted inventory tolerance control at the group level, execute transaction code OMJ2 and click physical inventory tolerance groups. If the tolerance has been set by specific users, select User Name.</p>																																													
DSS05	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.	3.1.6 Review enterprise policy and process design specifications regarding access to maintain BOM and process order settlement rules. Use transaction code SUIM—User Information System to test user access to create (transaction code CS01), change (transaction code CS02), make mass changes to (transaction code CS20), change single layered work breakdown structure BOM (transaction code CS72), change multilevel WBS BOM (transaction code CS75), and change multilevel work breakdown structure BOM using the browser (transaction code CSPB).	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="2">CS01—Create Material BOM</td><td>C_AENR_RV1</td><td>ACTVT</td><td>01</td></tr> <tr> <td>C_STUE_BER</td><td>ACTVT</td><td>01</td></tr> <tr> <td rowspan="2">CS02—Change Material BOM</td><td>C_STUE_BER</td><td>ACTVT</td><td>02</td></tr> <tr> <td>C_STUE_WRK</td><td>ACTVT</td><td>02</td></tr> <tr> <td>CS20— Mass Change: Initial Screen</td><td>C_STUE_BER</td><td>ACTVT</td><td>02</td></tr> <tr> <td rowspan="3">CS72—Change WBS BOM</td><td>C_STUE_BER</td><td>ACTVT</td><td>02</td></tr> <tr> <td>C_STUE_WRK</td><td>ACTVT</td><td>02</td></tr> <tr> <td>C_AENR_BGR</td><td>ACTVT</td><td>22</td></tr> <tr> <td rowspan="3">CS75— Change multilevel WBS BOM</td><td>C_STUE_BER</td><td>ACTVT</td><td>02</td></tr> <tr> <td>C_STUE_WRK</td><td>ACTVT</td><td>02</td></tr> <tr> <td>C_AENR_BGR</td><td>ACTVT</td><td>22</td></tr> </tbody> </table> <p>Test user access to transaction CSPB—Start WBS BOM Browser</p> <p>Test user access to change settlement rules (user transaction code COR2 and follow the menu path: Logistic → Production—Process → Process Order → Process Order → Change (enter the process order number and press Enter) → Header → Settlement Rule</p> <p>Take a sample of BOM updates using transaction CS80— Change Documents for Material BOM and compare to authorized source documentation.</p>	Transaction(s)	Authorization Objects	Fields	Values	CS01—Create Material BOM	C_AENR_RV1	ACTVT	01	C_STUE_BER	ACTVT	01	CS02—Change Material BOM	C_STUE_BER	ACTVT	02	C_STUE_WRK	ACTVT	02	CS20— Mass Change: Initial Screen	C_STUE_BER	ACTVT	02	CS72—Change WBS BOM	C_STUE_BER	ACTVT	02	C_STUE_WRK	ACTVT	02	C_AENR_BGR	ACTVT	22	CS75— Change multilevel WBS BOM	C_STUE_BER	ACTVT	02	C_STUE_WRK	ACTVT	02	C_AENR_BGR	ACTVT	22			
Transaction(s)	Authorization Objects	Fields	Values																																													
CS01—Create Material BOM	C_AENR_RV1	ACTVT	01																																													
	C_STUE_BER	ACTVT	01																																													
CS02—Change Material BOM	C_STUE_BER	ACTVT	02																																													
	C_STUE_WRK	ACTVT	02																																													
CS20— Mass Change: Initial Screen	C_STUE_BER	ACTVT	02																																													
CS72—Change WBS BOM	C_STUE_BER	ACTVT	02																																													
	C_STUE_WRK	ACTVT	02																																													
	C_AENR_BGR	ACTVT	22																																													
CS75— Change multilevel WBS BOM	C_STUE_BER	ACTVT	02																																													
	C_STUE_WRK	ACTVT	02																																													
	C_AENR_BGR	ACTVT	22																																													
DSS05	Transfers of materials	3.1.7 Use transaction code SUIM—User Information System to test user access to issue goods																																														

Audit/Accrual Program for SAP ERP Inventory Business Cycle												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes												
Ref.	Assurance Steps and Guidance					Issue Cross-reference	Comment					
		to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.		and to posting of transfers among plants:								
				<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>MB1A—Goods Withdrawal, MB1B—Transfer Posting</td><td>M_MSEG_BWA M_MSEG_WWA</td><td>ACTVT ACTVT</td><td>01 01</td></tr> </tbody> </table>	Transaction(s)			Authorization Objects	Fields	Values	MB1A—Goods Withdrawal, MB1B—Transfer Posting	M_MSEG_BWA M_MSEG_WWA
Transaction(s)	Authorization Objects	Fields	Values									
MB1A—Goods Withdrawal, MB1B—Transfer Posting	M_MSEG_BWA M_MSEG_WWA	ACTVT ACTVT	01 01									
	DSS05	Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.		3.1.8 Use transaction code SUIM—User Information System to test user access to create or change work centers.								
				<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>CR01—Create Work Center CR02—Change Work Center</td><td>C_ARPL_WRK C_ARPL_WRK</td><td>ACTVT ACTVT</td><td>01 02</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects		Fields	Values	CR01—Create Work Center CR02—Change Work Center	C_ARPL_WRK C_ARPL_WRK	ACTVT ACTVT
Transaction(s)	Authorization Objects	Fields	Values									
CR01—Create Work Center CR02—Change Work Center	C_ARPL_WRK C_ARPL_WRK	ACTVT ACTVT	01 02									
B-3.6c	<u>Agree on the process work products</u> ¹² (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.											
	Process Producing and costing inventory inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.				Criteria: All listed work products should demonstrably exist and be used.							
	<table border="1"> <thead> <tr> <th>Process Practice</th><th>Work Products</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Producing and costing inventory</td><td>• Production order settlement log</td><td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td></tr> </tbody> </table>							Process Practice	Work Products	Assessment Step	Producing and costing inventory	• Production order settlement log
Process Practice	Work Products	Assessment Step										
Producing and costing inventory	• Production order settlement log	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.										
B-3.7c												
<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>												
					SAP ERP Inventory process: Handling and shipping finished goods							
B-3.1d	<u>Understand the Process context.</u>											
B-3.2d	<u>Understand the Process purpose.</u>											
B-3.3d	<u>Understand all process stakeholders</u> and their roles .											
	Handling and shipping finished goods stakeholders:											
B-3.4d	<u>Understand the Process goals</u> and related <u>metrics</u> ¹³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the <u>effectiveness</u> of the process.											
	The Process Handling and shipping finished goods has three defined process goals.			The following activities can be								

¹² For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: *Enabling Processes*.

¹³ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

Audit/Accuracy Program for SAP ERP Inventory Business Cycle															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes															
Ref.	Assurance Steps and Guidance					Issue Cross-reference									
Process Goal			Related Metrics	Criteria/Expected Value	Assessment Step										
Finished goods received from production are recorded completely and accurately in the appropriate period			<ul style="list-style-type: none"> Number of open production orders by month Number of materials backlogged by month 		Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.										
Goods returned by customers are accepted in accordance with the organization's policies			<ul style="list-style-type: none"> Number of customer returns by month Number of customer returns without Return Authorization Numbers (RMAs) 		Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.										
Shipments are recorded accurately, in a timely manner and in the appropriate period			<ul style="list-style-type: none"> Percentage of on-time shipping by storage location per week 		Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.										
B-3.5d	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement. Evaluate Handling and shipping finished goods <table border="1"> <thead> <tr> <th>Reference Process</th> <th>Handling and shipping finished goods</th> <th>Criteria:</th> </tr> </thead> <tbody> <tr> <td>APO12</td> <td>4.1 Finished goods received from production are recorded completely and accurately in the appropriate period.</td> </tr> <tr> <td>DSS01</td> <td>4.2 Goods returned by customers are accepted in accordance with the enterprise's policies.</td> </tr> <tr> <td>DSS06</td> <td>4.3 Shipments are recorded accurately, in a timely manner and in the appropriate period.</td> </tr> </tbody> </table>						Reference Process	Handling and shipping finished goods	Criteria:	APO12	4.1 Finished goods received from production are recorded completely and accurately in the appropriate period.	DSS01	4.2 Goods returned by customers are accepted in accordance with the enterprise's policies.	DSS06	4.3 Shipments are recorded accurately, in a timely manner and in the appropriate period.
Reference Process	Handling and shipping finished goods	Criteria:													
APO12	4.1 Finished goods received from production are recorded completely and accurately in the appropriate period.														
DSS01	4.2 Goods returned by customers are accepted in accordance with the enterprise's policies.														
DSS06	4.3 Shipments are recorded accurately, in a timely manner and in the appropriate period.														
Reference Process Practices ¹⁴	Good Practice	Assessment Step				Issue Cross-reference									
APO12 DSS01 DSS06	Finished goods received from production are recorded completely and accurately in the appropriate period.	4.1.1 Test inventory stock-take procedures. Confirm that management executes transaction code MM04—Display Material Change Documents periodically and compares against source documents. Request a sample of source documents for evidence of comparison to inventory file updates.													
DSS05 DSS06	Finished goods received from production are recorded completely and accurately in the appropriate period.	4.1.2 Review enterprise policy and process design specifications regarding access to maintain BOM and process order settlement rules. Use transaction code SUIM—User Information System to test user access to create (transaction code CS01), change (transaction code CS02), make mass changes to (transaction code CS20), change single layered work breakdown structure BOM (transaction code CS72), change multilevel WBS BOM (transaction code CS75), and change multilevel work breakdown structure BOM using the browser (transaction code CSPB).													
<table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>CS01—Create Material BOM</td> <td>C_AENR_RV1</td> <td>ACTVT</td> <td>01</td> </tr> </tbody> </table>							Transaction(s)	Authorization Objects	Fields	Values	CS01—Create Material BOM	C_AENR_RV1	ACTVT	01	
Transaction(s)	Authorization Objects	Fields	Values												
CS01—Create Material BOM	C_AENR_RV1	ACTVT	01												

¹⁴ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Inventory audit/accuracy program.

Audit/Accuracy Program for SAP ERP Inventory Business Cycle															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes															
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment							
APO11	Goods returned by customers are accepted in accordance with the enterprise's policies.			C_STUE_BER	ACTVT	01									
				CS02—Change Material BOM	C_STUE_BER	ACTVT	02								
					C_STUE_WRK	ACTVT	02								
				CS20— Mass Change: Initial Screen	C_STUE_BER	ACTVT	02								
				CS72—Change WBS BOM	C_STUE_BER	ACTVT	02								
					C_STUE_WRK	ACTVT	02								
					C_AENR_BGR	ACTVT	22								
				CS75— Change multilevel WBS BOM	C_STUE_BER	ACTVT	02								
					C_STUE_WRK	ACTVT	02								
					C_AENR_BGR	ACTVT	22								
<p>Test user access to transaction CSPB—Start WBS BOM Browser.</p> <p>Test user access to change settlement rules (user transaction code COR2 and follow the menu path: Logistic → Production—Process → Process Order → Process Order → Change (enter the process order number and press Enter) → Header → Settlement Rule.</p> <ul style="list-style-type: none"> Take a sample of BOM updates using transaction CS80— Change Documents for Material BOM and compare to authorized source documentation. 															
APO11	Goods returned by customers are accepted in accordance with the enterprise's policies.		<p>4.2.1 Review the policies and procedures for receiving inventory back into the warehouse. Review some returns of inventory and ensure that they are supported with adequate documentation from the quality inspector. Ascertain from management the movement type used for goods returned from customers.</p> <p>Use transaction code MB51—Material Doc. List with the appropriate material movement type. Determine whether there are any long outstanding materials pending the return to inventory and/or provision of appropriate credits.</p>												
APO11	Goods returned by customers are accepted in accordance with the enterprise's policies.		<p>4.2.2 Obtain evidence that the QA team inspects the returned goods before a credit note can be issued.</p>												
DSS01 DSS05	Shipments are recorded accurately, in a timely manner and in the appropriate period.		<p>4.3.1 Use transaction code SUIM—User Information System to test user access to transfer stock among plants (transaction code LT04) or change outbound delivery (transaction code VL02N).</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>LT04—Create TO from TR</td> <td>L_TCODE</td> <td>TCD</td> <td>LT04</td> </tr> </tbody> </table>					Transaction(s)	Authorization Objects	Fields	Values	LT04—Create TO from TR	L_TCODE	TCD	LT04
Transaction(s)	Authorization Objects	Fields	Values												
LT04—Create TO from TR	L_TCODE	TCD	LT04												

Audit/Accrual Program for SAP ERP Inventory Business Cycle									
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes									
Ref.	Assurance Steps and Guidance							Issue Cross-reference	Comment
				VL02N—Change Outbound Delivery	V_LIKP_VST	ACTVT	02		
	DSS05	Shipments are recorded accurately, in a timely manner and in the appropriate period.		4.3.2 Take a sample of the delivery due list and owed to customer report and test for evidence of management action. Review settings using transaction code OMWB—C MM-IV Autom. Acct. Assgt. (Simu.) to get the configuration screen for MM account assignments, use transaction key GBB and confirm that accounts assignments are set to valid COGS accounts.					
	DSS01	Shipments are recorded accurately, in a timely manner and in the appropriate period.		4.3.3 Review the policies and procedures for picking and shipping goods. Review a sample of shipments and ensure that they are supported with adequate documentation from the person matching physical quantity to order quantity.					
	DSS01	Shipments are recorded accurately, in a timely manner and in the appropriate period.		4.3.4 Request copies of the SAP ERP reports delivery due list and owed to customer report and confirm that these reports have been reviewed by the appropriate personnel to ensure timely shipment of goods.					
	DSS06	Shipments are recorded accurately, in a timely manner and in the appropriate period.		4.3.5 Use transaction key GBB and confirm that accounts assignments are set to valid COGS accounts.					
B-3.6d	<u>Agree on the process work products</u> ¹⁵ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess to what extent the process work products are available.</u> Handling and shipping finished goods inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.								
	Process Practice Handling and shipping finished goods		Work Products <ul style="list-style-type: none"> • Past due delivery report 			Assessment Step Criteria: All listed work products should demonstrably exist and be used.			
B-3.7d	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>								

¹⁵ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accrual Program for SAP ERP Inventory Business Cycle															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment															
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment												
B-4	<p>Obtain understanding of each Organisational Structure in scope and set suitable assessment criteria: For each Organisational Structure in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the Organisational Structure.</p> <p>Organisational Structure: Warehouse</p>														
B-4.1a	<p><u>Understand</u> the Organisational Structure context. <i>Identify and document all elements that can help to understand the context in which the Financial accounting organization has to operate, including:</i></p> <ul style="list-style-type: none"> • The overall organisation • Management/process framework • History of the role/structure • Contribution of the Organisational Structure to achievement of goals 														
B-4.2a	<p><u>Understand</u> all stakeholders of the Organisational Structure/function. Determine through documentation review (policies, management communications, etc.) the key stakeholders of the Financial accounting organization.</p> <ul style="list-style-type: none"> • Incumbent of the role and/or members of the Organisational Structure • Other key stakeholders affected by the decisions of the Organisational Structure/role 														
B-4.3a	<p><u>Understand</u> the goals of the Organisational Structure, the related metrics and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals.</p> <table border="1"> <thead> <tr> <th>Organisational Structure Goal</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Determine through interviews with key stakeholders and documentation review the goals of the Warehouse organization, i.e., the decisions for which they are accountable^{16,17}.</td> <td> <p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. </td></tr> </tbody> </table>	Organisational Structure Goal	Assessment Step	Determine through interviews with key stakeholders and documentation review the goals of the Warehouse organization, i.e., the decisions for which they are accountable ^{16,17} .	<p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 										
Organisational Structure Goal	Assessment Step														
Determine through interviews with key stakeholders and documentation review the goals of the Warehouse organization, i.e., the decisions for which they are accountable ^{16,17} .	<p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 														
B-4.4a	<p><u>Agree</u> on the expected good practices for the Organisational Structure against which it will be assessed. <u>Assess</u> the Organisational Structure design, i.e., assess the extent to which expected good practices are applied.</p> <table border="1"> <thead> <tr> <th>Good Practice</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Operating principles</td> <td> <ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. </td> <td> <ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. </td></tr> <tr> <td>Composition</td> <td>The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td> <td>Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td></tr> <tr> <td>Span of control</td> <td> <ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. </td> <td> <ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. </td></tr> </tbody> </table>	Good Practice	Criteria	Assessment Step	Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 	Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Span of control	<ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. 	<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. 		
Good Practice	Criteria	Assessment Step													
Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 													
Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.													
Span of control	<ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. 	<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. 													

¹⁶ The RACI charts in COBIT 5: *Enabling Processes* can be leveraged as a starting point for the expected goals of a role or Organisational Structure.

¹⁷ The Organisational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organisational Structure assuming the same responsibilities and accountability should be considered.

Audit/Accuracy Program for SAP ERP Inventory Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Organisational Structures					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-4.5a		<ul style="list-style-type: none"> The span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. The span of control is in line with the overall enterprise governance arrangements. 	<ul style="list-style-type: none"> Assess whether the span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. Verify and assess whether the span of control is in line with the overall enterprise governance arrangements. 		
	Level of authority/decision rights	<ul style="list-style-type: none"> Decision rights of the Organisational Structure are defined and documented. Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue). 	<ul style="list-style-type: none"> Verify that decision rights of the Organisational Structure are defined and documented. Verify whether decision rights of the Organisational Structure are complied with and respected. 		
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.		
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.		
B-4.1 to B-4.5	<u>Understand</u> the life cycle and agree on expected values. <u>Assess</u> the extent to which the Organisational Structure life cycle is managed.				
	Life-Cycle Element	Criteria	Assessment Step		
	Mandate	<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well understood mandate. 		
B-4.1 to B-4.5	Monitoring	<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 		
	Repeat steps B-4.1 through B-4.5 for all remaining Organisational structures in scope. Repeat the steps described above for the remaining Organisational structures: <ul style="list-style-type: none"> Quality Shipping Financial accounting Tax department General accounting Treasury 				

Audit/Accuracy Program for SAP ERP Inventory Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment
B-5	Obtain understanding of the Culture, Ethics and Behaviour in scope. Assess Culture, Ethics and Behaviour.		
Culture, Ethics and Behaviour: Risk and compliance aware culture			
B-5.1a	<u>Understand the Culture, Ethics and Behaviour context.</u> <ul style="list-style-type: none"> • <i>What the overall corporate Culture is like</i> • <i>Understand the interconnection with other enablers in scope:</i> <ul style="list-style-type: none"> - <i>Identify roles and structures that could be affected by the Culture.</i> - <i>Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.</i> 		
B-5.2a	<u>Understand the major stakeholders of the Culture, Ethics and Behaviour: Risk and compliance aware culture</u> <i>Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.</i>		
B-5.3a	<u>Understand the goals for the Culture, Ethics and Behaviour</u> , and the related metrics and agree on expected values. Assess whether the Culture, Ethics and Behaviour goals (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour. In the context of Risk and compliance aware culture , the following Culture, Ethics and Behaviour are desired:	Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. For a representative sample of individuals, perform the following assessment steps.	
Desired Behaviour (Culture, Ethics and Behaviour Goal)		Assessment Step	
The enterprise is aware of the compliance requirements it must abide			
Employees understand their role in maintaining compliance			
Identified risk are properly address			
Controls are in place to ensure compliance with internal and external requirements			
B-5.4a	<u>Understand</u> the life cycle stages of the Culture, Ethics and Behaviour , and agree on the relevant criteria. Assess to what extent the Culture, Ethics and Behaviour life cycle is managed. <small>(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)</small>		
B-5.5a	<u>Understand</u> good practice when dealing with Culture, Ethics and Behaviour , and agree on relevant criteria. Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied.		
Good Practice		Criteria	Assessment Step
Communication, enforcement and rules		Existence and quality of the communication	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.
Incentives and rewards		Existence and application of appropriate rewards and incentives	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.
Awareness		Awareness of desired Behaviours	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.
B-5.1 to	Repeat steps B-5.1 through B-5.5 for all remaining Culture, Ethics and Behaviour in scope.		

Audit/Assurance Program for SAP ERP Inventory Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment
B-5.5	<p>Repeat the steps described above for the remaining Culture, Ethics and Behaviour:</p> <ul style="list-style-type: none"> • Enabling of continuous improvement • Accountability • Discipline to follow instructions 		

Audit/Accrual Program for SAP ERP Inventory Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-6	Obtain understanding of the Information Items in scope. Assess Information Items.		
Information Item: Data integrity procedures			
B-6.1a	<u>Understand the Information item context:</u> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> - <i>Used by which processes?</i> - <i>Which Organisational Structures are involved?</i> - <i>Which services/applications are involved?</i> 		
B-6.2a	<u>Understand the major stakeholders of the Information item.</u> <i>Understand the stakeholders for the Information item, i.e., identify the:</i> <ul style="list-style-type: none"> • <i>Information producer</i> • <i>Information custodian</i> • <i>Information consumer</i> <i>Stakeholders should be at the appropriate organisational level.</i>		
B-6.3a	<u>Understand the major quality criteria for the Information item, the related metrics and agree on expected values.</u> <u>Assess whether the Information item quality criteria (outcomes) are achieved, i.e., assess the effectiveness of the Information item.</u> Leverage the COBIT 5 Information enabler model ¹⁸ focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand. Mark the quality dimensions with a ‘✓’ that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.	The assurance professional will, by using appropriate auditing techniques, verify all quality criteria in scope and assess whether the criteria are met.	
Quality Dimension	Key Criteria	Description	Assessment Step
Accuracy	✓		
Objectivity			
Believability			
Reputation			
Relevancy	✓		
Completeness	✓		
Currency	✓		
Amount of information	✓		
Concise representation	✓		
Consistent representation			
Interpretability			
Understandability	✓		
Manipulation			
Availability	✓		
Restricted access	✓		

¹⁸ COBIT 5 framework, appendix G, p.81-84

Audit/Accuracy Program for SAP ERP Inventory Business Cycle																															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																															
Ref.	Assurance Steps and Guidance			Issue Cross-reference																											
B-6.4a	<p>Understand the life cycle stages of the Information item, and agree on the relevant criteria. Assess to what extent the Information item life cycle is managed.</p> <p>The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.</p> <ul style="list-style-type: none"> When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently. When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. <p>Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Life Cycle Stage</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Plan</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Design</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Build/acquire</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Use/operate</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Evaluate/monitor</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Update/dispose</td> <td>✓</td> <td></td> <td></td> </tr> </tbody> </table>	Life Cycle Stage	Key Criteria	Description	Assessment Step	Plan	✓			Design	✓			Build/acquire	✓			Use/operate	✓			Evaluate/monitor	✓			Update/dispose	✓				
Life Cycle Stage	Key Criteria	Description	Assessment Step																												
Plan	✓																														
Design	✓																														
Build/acquire	✓																														
Use/operate	✓																														
Evaluate/monitor	✓																														
Update/dispose	✓																														
B-6.5a	<p>Understand important attributes of the Information item and expected values. Assess the Information item design, i.e., assess the extent to which expected good practices are applied.</p> <p>Good practices for Information items are defined as a series of attributes for the Information item¹⁹. The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.</p> <p>Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Attribute</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Physical</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Empirical</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Syntactic</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Semantic</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Pragmatic</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Social</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Attribute	Key Criteria	Description	Assessment Step	Physical				Empirical				Syntactic				Semantic				Pragmatic	✓			Social					
Attribute	Key Criteria	Description	Assessment Step																												
Physical																															
Empirical																															
Syntactic																															
Semantic																															
Pragmatic	✓																														
Social																															
B-6.1 to B-6.5	<p>Repeat steps B-6.1 through B-6.5 for all remaining Information items in scope.</p> <p>Repeat the steps described above for the remaining Information items:</p> <ul style="list-style-type: none"> Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis Retention requirements Record of transactions Training manuals Job aids 																														

¹⁹ COBIT 5 framework, appendix G, p. 81-84

Audit/Accuracy Program for SAP ERP Inventory Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Services, Infrastructure and Applications				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-7	Obtain understanding of the Services, Infrastructure and Applications in scope. Assess Services, Infrastructure and Applications.			
Services, Infrastructure and Applications: SAP ERP System				
B-7.1a	<u>Understand the Services, Infrastructure and Applications</u> context. <i>Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.</i>			
B-7.2a	<u>Understand the major stakeholders of the Services, Infrastructure and Applications.</u> <i>Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.</i>			
B-7.3a	<u>Understand the major goals for the Services, Infrastructure and Applications</u> , the related metrics and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.			
Goal Assessment Step				
	Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 	
	Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 	
	Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.	
B-7.4a	<u>Understand good practice related to the Services, Infrastructure and Applications and expected values.</u> <u>Assess the Services, Infrastructure and Applications</u> design, i.e., assess to what extent expected good practices are applied. <i>Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework²⁰ to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented:</i> <ul style="list-style-type: none"> Buy/build decision needs to be taken. Use of the Service needs to be clear. 			
Good Practice Assessment Step				
	Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. 	

²⁰ COBIT 5 framework, appendix G, p.85-86

Audit/Assurance Program for SAP ERP Inventory Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
				Comment
		<ul style="list-style-type: none"> Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. 		
	Use	<p>The use of the Service needs to be clear:</p> <ul style="list-style-type: none"> When it needs to be used and by whom The required compliance levels with the Service's output 	<ul style="list-style-type: none"> Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used. Verify that actual use is in line with requirement above. Verify that the actual Service output is adequately used. Verify that Service levels are monitored and achieved. 	
B-7.1 to B-7.4	<p>Repeat steps B-7.1 through B-7.4 for all remaining Services, Infrastructure and Applications in scope.</p> <p>Repeat the steps described above for the remaining Services, Infrastructure and Applications:</p> <ul style="list-style-type: none"> Master data maintenance Change management SAP training 			

Audit/Accuracy Program for SAP ERP Inventory Business Cycle																					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																					
People, Skills and Competencies																					
Ref.	Assurance Steps and Guidance		Issue Cross-reference																		
B-8	Obtain understanding of the People, Skills and Competencies in scope. Assess People, Skills and Competencies.																				
People, Skill and Competency: Proficiency using the SAP Inventory Module																					
B-8.1a	<u>Understand the People, Skills and Competencies</u> context. <i>Understand the context of the Skill/Competency, i.e.:</i> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> – <i>In which roles and structures is the Skill/Competency used? (See also B-4.1.)</i> <i>Which behaviours are associated with the Skill/Competency?</i>																				
B-8.2a	<u>Understand the major stakeholders</u> for the People, Skills and Competencies. <i>Identify to whom in the organisation the skill requirement applies.</i>																				
B-8.3a	<u>Understand the major goals</u> for the People, Skills and Competencies , the related metrics and agree on expected values. <i>Assess whether the People, Skills and Competencies goals (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.</i> For the People, Skills and Competencies: Proficiency using the SAP Inventory Module , the following goals and associated criteria can be addressed.																				
	<table border="1"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr><td>Experience</td><td></td><td rowspan="10">Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.</td></tr> <tr><td>Education</td><td></td></tr> <tr><td>Qualification</td><td></td></tr> <tr><td>Knowledge</td><td></td></tr> <tr><td>Technical skills</td><td></td></tr> <tr><td>Behavioural skills</td><td></td></tr> <tr><td>Number of people with appropriate skill level</td><td></td></tr> </tbody> </table>		Goal	Criteria	Assessment Step	Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	Education		Qualification		Knowledge		Technical skills		Behavioural skills		Number of people with appropriate skill level		
Goal	Criteria	Assessment Step																			
Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.																			
Education																					
Qualification																					
Knowledge																					
Technical skills																					
Behavioural skills																					
Number of people with appropriate skill level																					
B-8.4a	<u>Understand the life cycle</u> stages of the People, Skills and Competencies , and agree the relevant criteria. <i>Assess to what extent the People, Skills and Competencies life cycle is managed.</i>																				
	For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07.		For the People, Skills and Competencies at hand the assurance professional will perform the following assessment steps.																		
	<table border="1"> <thead> <tr> <th>Life Cycle Element</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Plan</td><td>Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.</td><td>Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.</td></tr> <tr> <td>Design</td><td> Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill. </td><td> Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill. </td></tr> <tr> <td>Build</td><td>Practice APO07.03 activity 4 (Identify gaps between</td><td>Assess whether practice APO07.03 activity 4 is implemented in</td></tr> </tbody> </table>		Life Cycle Element	Criteria	Assessment Step	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.	Build	Practice APO07.03 activity 4 (Identify gaps between	Assess whether practice APO07.03 activity 4 is implemented in							
Life Cycle Element	Criteria	Assessment Step																			
Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.																			
Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.																			
Build	Practice APO07.03 activity 4 (Identify gaps between	Assess whether practice APO07.03 activity 4 is implemented in																			

Audit/Accuracy Program for SAP ERP Inventory Business Cycle												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment												
People, Skills and Competencies												
Ref.	Assurance Steps and Guidance			Issue Cross-reference								
				Comment								
		required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	relation to this skill.									
	Operate	Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.									
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.									
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.									
B-8.5a	<p>Understand good practice related to the People, Skills and Competencies and expected values. Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.</p> <table border="1"> <thead> <tr> <th>Good Practice</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Skill set and Competencies are defined.</td><td> <ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. </td><td></td></tr> <tr> <td>Skill levels are defined.</td><td> <ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. Assess the process for 360-degree performance evaluations. </td><td></td></tr> </tbody> </table>			Good Practice	Criteria	Assessment Step	Skill set and Competencies are defined.	<ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 		Skill levels are defined.	<ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. Assess the process for 360-degree performance evaluations. 	
Good Practice	Criteria	Assessment Step										
Skill set and Competencies are defined.	<ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 											
Skill levels are defined.	<ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. Assess the process for 360-degree performance evaluations. 											
B-8.1 to B-8.5	<p>Repeat steps B-8.1 through B-8.5 for all remaining People, Skills and Competencies in scope.</p> <p>Repeat the steps described above for the remaining People, Skills and Competencies:</p> <ul style="list-style-type: none"> Proficiency using the SAP Materials Management Module Master data management skills Materials management skills and experience 											

Audit/Assurance Program for SAP ERP Inventory Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
People, Skills and Competencies			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
	<ul style="list-style-type: none">• Proficiency running SAP reports• Understanding of data classification policies• Understanding of data integrity procedures		

Audit/Accuracy Program for SAP ERP Inventory Business Cycle		
Phase C—Communicate the Results of the Assessment		
Ref.	Assurance Step	Guidance
C-1	Document exceptions and gaps.	
C-1.1	Understand and document weaknesses and their impact on the achievement of process goals.	<ul style="list-style-type: none"> Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	<ul style="list-style-type: none"> Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. Point out the consequence of noncompliance with regulatory requirements and contractual agreements. Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
C-2	Communicate the work performed and findings.	
C-2.1	Communicate the work performed.	<ul style="list-style-type: none"> Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	<ul style="list-style-type: none"> Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. Use benchmarking and survey results to compare the enterprise's performance with others. Use extensive graphics to illustrate the issues. Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	

Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
1. Master Data Maintenance							
1.1 Changes made to master data are valid, complete, accurate and timely.							
1.1.1 Does relevant management, other than the initiators, check online reports of master data additions and changes back to source documentation on a sample basis?					DSS06		
1.1.2 Have the creation and maintenance of master data been assigned and restricted to a dedicated area within the enterprise that understands how they may affect organizational processes as well as the importance of timely changes?					DSS05 DSS06		
1.1.3 Have configurable controls been designed into the process to maintain the integrity of master data?					DSS06		
1.1.4 Does management periodically review master data to check that the overdelivery tolerance is different from zero percent or the unlimited delivery option is set?					DSS01 DSS06		
1.2 Inventory master data remain current and pertinent.							
1.2.1 Does management periodically review master data to check their accuracy?					DSS06		
1.3 Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.							
1.3.1 Is the ability to create, change or delete the bill of materials restricted to authorized personnel?					DSS05		

Inventory Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
1.3.2 Does relevant management, other than the initiators, check online reports of bill of materials or settlement rule additions and changes back to source documentation on a sample basis?					DSS06
2. Raw Materials Management					
2.1 Inventory is salable, usable and adequately safeguarded.					
2.1.1 Are raw material requirements planned based on forecast orders and production plans, and does the system functionality monitor and maintain inventory levels in accordance with the enterprise's policies?					APO11 BAI04 DSS01 DSS06
2.1.2 Is the salability of finished goods and usability of raw materials (including shelf-life dates) assessed regularly during continuous inventory counts, and are any scrapped goods or raw materials appropriately approved?					BAI04 DSS06
2.1.3 Does the quality department test a sample of raw materials, and are rejected raw materials adequately segregated from other raw materials into a separate quality assurance holding area and regularly monitored by the quality department personnel to ensure timely return to suppliers?					APO11 DSS01
2.1.4 Does management review reports of slow-turnover inventory to ensure that it is still salable or usable?					DSS01 DSS06

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.1.5 Do goods inbound/outbound personnel monitor all incoming and outgoing vehicles and ensure that all goods leaving the premises are accompanied by duly completed documentation (e.g., intercompany stock transfer order, delivery docket or goods returned note)?					DSS05 DSS06
2.1.6 Are goods delivered only to designated, physically secure loading bays within the warehouses, and are they accepted only by authorized inbound logistic/raw materials personnel?					DSS05 DSS06
2.1.7 Is inventory stored in properly secured (gates locked at night and premises alarmed), environmentally conditioned warehouse locations where access is restricted to authorized personnel?					DSS05 DSS06
2.2 Raw materials are received and accepted only with valid purchase orders and are recorded accurately and in a timely manner.					
2.2.1 Are goods received matched online with purchase order details and/or invoices?					DSS01 DSS06
2.2.2 Are long-outstanding goods receipt notes, purchase orders and/or invoices investigated on a timely basis and accrued as appropriate?					DSS01 DSS06
2.2.3 Are documents canceled once or on payment of the invoice matched to prevent reuse?					APO11 DSS01

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.2.4 Does management review exception reports of goods not received on time for recorded purchases?					DSS06
2.2.5 When goods received are matched to open purchase orders, are receipts with no purchase orders, or those that exceed the purchase order quantity by more than an established amount, investigated?					DSS06
2.2.6 Is the ability to input, change or cancel goods received transactions restricted to authorized inbound logistics/raw materials personnel?					DSS05
2.2.7 Do persons independent of day-to-day custody or recording of inventory count physical inventory on a continuous inventory basis?					DSS01
2.2.8 Are inventory counts reconciled to inventory records and inventory records reconciled to the GL?					DSS01 DSS06
2.2.9 Do raw materials/finished goods that are batch managed have a matching and accounting with an appropriate batch management strategy?					DSS06
2.3 Defective raw materials are returned to suppliers in a timely manner.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.3.1 Are rejected raw materials adequately segregated from other raw materials in a quality assurance holding area, and are they regularly monitored (assigned a movement type of 122) to ensure timely return to suppliers?					APO11 DSS01
2.3.2 Are defective raw materials received from suppliers logged and recorded in the quality management system, and is the log monitored to ensure that the defective goods are returned promptly and credit is received in a timely manner?					APO10 DSS01
3. Producing and Costing Inventory					
3.1 Transfers of materials to/from production, production costs and defective products/scrap are valid and recorded accurately, completely and in the appropriate period.					
3.1.1 Are inventories received, including transfers, counted and compared to the pick list (that is used to record movements of inventory in the financial records) by personnel in the area assuming responsibility for the inventory (e.g., production, goods storage), and are they recorded in the appropriate period?					DSS01
3.1.2 Does management reconcile the inventory-in-transit accounts regularly, and do these accounts net off against other plants' outgoing inventory-in-transit accounts?					APO11 DSS01

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.1.3 Is an appropriate costing method used for raw materials at purchase order price, and is the raw materials costing rolled into finished goods on a monthly basis?					DSS01
3.1.4 Does the quality department, based on its knowledge of day-to-day activities, review records of scrapped and reworked items and check whether such items have been correctly identified and properly recorded in the appropriate accounting period?					APO11
3.1.5 Are tolerances for physical inventory differences configured to users from posting differences that exceed the tolerance?					APO12 DSS06
3.1.6 Is the ability to create or change bills of material restricted to authorized personnel?					DSS05
3.1.7 Is access to the material transfers and adjustments transactions appropriately restricted to authorized personnel?					DSS05
3.1.8 Is the ability to create or change work centers restricted to authorized personnel?					DSS05
4. Handling and Shipping Finished Goods					
4.1 Finished goods received from production are recorded completely and accurately in the appropriate period.					
4.1.1 Do persons independent of day-to-day custody or recording of inventory count physical inventory on a continuous inventory basis? (Refer to master data integrity1.1.2.)					APO12 DSS01 DSS06

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
4.1.2 Is the changing of the settlement rules restricted to authorized users? (Refer to bill of materials integrity1.3.1.)					DSS05 DSS06
4.2 Goods returned by customers are accepted in accordance with the enterprise's policies.					
4.2.1 Are quality control inspections performed for finished goods returned by customers and/ or received from production to assess whether such goods should be returned to inventory, reworked or scrapped?					APO11
4.2.2 Does the quality assurance team inspect the goods before a credit note can be issued?					APO11
4.3 Shipments are recorded accurately, in a timely manner and in the appropriate period.					
4.3.1 Is access restricted to transferring stock between plants or executing the Post Goods Issue that creates the intercompany stock transfer advice and/or generates an electronic (EDI) or manual invoice?					DSS01 DSS05
4.3.2 Do outbound logistics/finished goods personnel monitor all incoming and outgoing vehicles and ensure that all goods leaving the premises are accompanied by duly completed documentation (e.g., delivery docket or goods returned note)?					DSS05

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
4.3.3 Before goods are shipped, are the details of the approved order compared to actual goods prepared for shipment by an individual independent of the order picking process?					DSS01
4.3.4 Are the SAP ERP reports (delivery due list and owed-to-customer report) of open sales documents prepared and monitored to ensure timely shipment?					DSS01
4.3.5 Does the SAP ERP account assignment configuration ensure that amounts for shipped goods are posted to the appropriate COGS account?					DSS06

SAP ERP

Financial Accounting FI Module
Audit/Assurance Program



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP ERP Financial Accounting FI Module Audit/Accurance Program* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP's kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: <http://www.isaca.org/sap-erp-4th-edition>

Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOFFICIAL>

Like ISACA on Facebook: www.facebook.com/ISACAHQ

Acknowledgements

ISACA wishes to recognize

Project Leaders

Benjamin Fitts, CPA, Deloitte & Touche LLP, USA
Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA
Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA
Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Eva Sweet, CISA, CISM, ISACA, USA

Researchers

Syed Aamir Aarfi, Deloitte & Touche LLP, USA
Carlos Amaya, CISA, Deloitte & Touche LLP, USA
Dan Argynov, PMP, Deloitte & Touche LLP, USA
Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA
David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA
Ramamallikarjunarao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA
Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA
Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA
Sagnik Mukherjee, Deloitte & Touche LLP, USA
Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA
Sonik Shah, Deloitte & Touche LLP, USA
Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA
Shweta Srivastava, Deloitte & Touche LLP, USA
Anurag Tewary, Deloitte & Touche LLP, USA
Percy Tsai, CPA, Deloitte & Touche LLP, USA
Ravi Maddela Veeriah, Deloitte & Touche LLP, USA
Sravan Vemana, Deloitte & Touche LLP, USA
Anukool Vyas, Deloitte & Touche LLP, USA

Expert Reviewers

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA
Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada
Mayank Garg, CISA, NetApp, USA
Ricci leong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Jim Koveos, CISA, MBA, AmerisourceBergen, USA
Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia
Samuel LIM S.C., CISA, Auditor General's Office, Singapore
Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia
Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General's Office, Singapore
Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia
Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia
Paul O'Donnell, Ernst & Young, Canada
Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico
John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US
Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico
Naved Rehman, CISA, CRISC, MS-IS, SAPauditCoach, US
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US
Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico
Jovari St. Victor, CISA, CPA, Sunera, LLC, US
Surapong Surabotsoon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,
KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico
Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand
David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President
Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKLoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK
Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil
Jotham Nyamari, CISA, Deloitte, USA
James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK
Gurvinder Singh, CISA, CISM, CRISC, Australia
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore
Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

SAP ERP Financial Accounting FI Module Audit/Accurance Program

Introduction

This document contains an example audit/assurance program, **based on** the generic structure developed in section 2B of *COBIT 5 for Assurance*¹.

The engagement approach is based on, but **differs slightly** from the generic approach described in *COBIT 5 for Assurance*:

- The engagement approach described in this audit/assurance program **is focused on a business process** consequently no group of COBIT 5 processes dominates as primary processes and the lower-level processes are widespread, for evaluation purposes, the high-level COBIT 5 processes will be used as references.
- The assurance steps in this audit/assurance program are specific to the subject matter under review; therefore most of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources availableprocess audit/assurance program.

Assurance Engagement: SAP ERP Financial Accounting FI Module

Assurance Topic

The topic covered by this assurance engagement is the SAP ERP Financial Accounting FI Module.

Business Impact and Risk

SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical processes.

Risk resulting from ineffective or incorrect configurations or use of SAP could result in some of the following:

- Disclosure of privileged information
- Single points of failure
- Low data quality
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements

Goal of the Review

The objective of the SAP ERP audit/assurance review is to provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise's SAP ERP architecture.

Scoping

The review will focus on configuration of the relevant SAP ERP components and modules within the enterprise. The selection of the specific components and modules will be based upon the risk introduced to the enterprise by these components and modules.

From a process reference model (PRM) perspective, the following domains and processes apply to this audit and assurance programme:

- BAI02 *Manage requirements definition*
- BAI03 *Manage solution identification and build*

¹ See www.isaca.org/COBIT/Pages/Assurance-product-page.aspx for more information on *COBIT 5 for Assurance*.

- DSS01 *Manage operations*
- DSS05 *Manage security services*
- DSS06 *Manage business process controls*

Testing SAP Security

To determine which users have access to the relevant authorizations used in this audit program, use one of the following methods:

1. Use transaction code SUIM → Users → Users by Complex Selection Criteria
2. Use transaction code S_BCE_68001417
3. Use transaction code SA38 and the program RSUSR002. This method allows the user to specify a transaction code, a "valid to" date for users, and up to three other authorization objects (which also may be the authorization object for transaction code S_TCODE) with associated values (two values under an AND relationship and three values under an OR relationship).
This method is generally sufficient for testing logical access security in relation to SAP ERP application infrastructure areas, but it is less suitable when large numbers of authorizations must be reviewed, such as in segregation of duties analysis and in some of the more complex areas of business cycle controls.
4. Use transaction code SUIM → Users → Users with Critical Authorizations (also accessible with program RSUSR008_009_NEW, which replaces programs RSUSR008 and RSUSR009 and transaction codes SU98 and/or SU99, for SAP Web AS 6.20 and later). This method offers improvements such as allowing differentiation between SAP defaults for critical data for different business areas, extended combination options for critical authorization data, improved performance, display of user filters and more analysis options for users in the result list.

Audit/Accrual Program for SAP ERP Financial Accounting FI Module					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
A-1	Determine the stakeholders of the assurance initiative and their stakes .				
A-1.1	<u>Identify</u> the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	Intended user(s) of the assurance report	<p>Board/audit committee: Needs assurance over the effectiveness and efficiency of SAP ERP processes within the enterprise.</p> <p>Chief financial officer (CFO): Needs assurance that internal controls for financial applications work as intended.</p> <p>Risk managers: Need assurance that controls intended to address previously identified risk are working as intended. The results from the audit should be used to update the risk registry as needed.</p> <p>Security managers: Need to identify gaps in the security plans for SAP applications.</p> <p>Owners / shareholders: Part or all of the SAP ERP assurance report may be included in statutory reporting.</p> <p>Regulators: Part or all of SAP ERP reporting may need to be disclosed to respective authorities</p>		
A-1.2	Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	Accountable and responsible parties for the subject matter	<p>Business executives: The individuals responsible for identifying requirements, approving design and managing performance. These people are, together with IT management, responsible for managing the correct and controlled use of SAP ERP services—in line with good practices.</p> <p>Business process owners: Responsible for defining application and technical requirements. Responsible for data classification.</p> <p>IT management: Responsible for managing the correct and controlled use of SAP ERP services—together with the business executives.</p>		
A-2	<u>Determine</u> the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities (i.e., not achieving the enterprise goals).		<p>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.</p> <p>Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.</p> <p>Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</p> <p>Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.</p>		
A-2.1	<u>Understand</u> the enterprise strategy and priorities.		<i>Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.</i>		

Audit/Assurance Program for SAP ERP Financial Accounting FI Module				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
A-2.2	<u>Understand</u> the internal context of the enterprise.	<p><i>Identify all internal environmental factors that could influence the performance and contents of the SAP ERP Financial Accounting Module.</i></p> <ul style="list-style-type: none"> • Review prior audit report, if one exists, verify completion of any agreed-on corrections, and note remaining deficiencies. Determine whether: <ul style="list-style-type: none"> - Senior management has assigned responsibilities for information, its processing, and its use - User management is responsible for providing information that supports the entity's objectives and policies - Information systems management is responsible for providing the capabilities necessary for the achievement of the defined information systems objectives and the policies of the entity - Senior management approves plans for development and acquisition of information systems - There are procedures to ensure that the information system being developed or acquired meets user requirements - There are procedures to ensure that information systems, programs, and configuration changes are tested adequately prior to implementation - All personnel involved in the system acquisition and configuration activities receive adequate training and supervision - There are procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards - User management participates in the conversion of data from the existing system to the new system - Final approval is obtained from user management prior to going live with a new information/upgraded system - There are procedures to document and schedule all changes to information systems (including key ABAP programs) - There are procedures to ensure that only authorized changes are initiated - There are procedures to ensure that only authorized, tested and documented changes to information systems are accepted into the production client - There are procedures to allow for and control emergency changes - There are procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software - There is a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated - The organizational structure, established by senior management, provides for an appropriate segregation of incompatible functions - The database, application and presentation servers are located in a physically separate and protected environment (i.e., a data center) - Emergency, backup and recovery plans are documented and tested on a regular basis to ensure that they remain current and operational - Backup and recovery plans allow users of information systems to resume operations in the event of an interruption - Application controls are designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system - Access to the Implementation Guide (IMG) during production has been restricted - The production client settings have been flagged to not allow changes to programs and 		

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module							
Phase A—Determine Scope of the Assurance Initiative							
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment		
		<p>configuration</p> <ul style="list-style-type: none"> • Identify the significant risk and determine the key controls <ul style="list-style-type: none"> - Develop a high-level process flow diagram and overall understanding of the Financial accounting module, including the following subprocesses: <ul style="list-style-type: none"> a. Master data maintenance b. General ledger c. Bank accounting d. Asset accounting - Assess the key risk, determine key controls or control weaknesses, and test controls (refer to the sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> a. The controls culture of the organization (e.g., a just-enough-control philosophy). b. The need to exercise judgment to determine the key controls in the process and whether the controls structure is adequate. (Any weaknesses in the control structure should be reported to executive management and resolved.) • Gain an understanding of the SAP ERP environment (The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles) <p>In particular, the following information is important:</p> <ul style="list-style-type: none"> - Version and release of SAP ERP implemented - Total number of named users (for comparison with logical access security testing results) - Number of SAP instances and clients - Accounting period, company codes, and chart of accounts - Identification of the components being used (Human Capital Management, Financials, Operations, Corporate Services) - Whether the organization has created any locally developed ABAP programs or reports - Details of the risk assessment approach taken in the organization to identify and prioritize risk - Copies of the organization's key security policies and standards <p>Obtain details of the following:</p> <ul style="list-style-type: none"> - Organizational Management Model as it relates to sales/revenue activity, i.e., sales organizational unit structure in SAP ERP and company sales organizational chart (required when evaluating the results of access security control testing) - An interview of the systems implementation team, if possible, and process design documentation for sales and distribution 					
A-2.3	<u>Understand</u> the external context of the enterprise.	<i>Identify all external environmental factors that could influence the performance and contents of the SAP ERP Financial Accounting FI Module.</i>					
A-2.4	Given the overall assurance objective, <u>translate</u> the identified strategic priorities into concrete <u>objectives</u> for the assurance engagement.	<p>The following goals are retained as key goals to be supported, in reflection of enterprise strategy and priorities:</p> <table border="1"> <tr> <td>Key goals</td> <td>Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability </td> </tr> </table>		Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability 		
Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability 						

Audit/Accrual Program for SAP ERP Financial Accounting FI Module					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step		Guidance	Issue Cross-reference	Comment
			<ul style="list-style-type: none"> • EG11 Optimisation of business process functionality • EG15 Compliance with internal policies <p>IT-related goals:</p> <ul style="list-style-type: none"> • ITG01 Alignment of IT and business strategy • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG09 IT Agility • ITG10 Security of information, processing infrastructure and applications • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG15 IT compliance with internal policies • ITG16 Competent and motivated business and IT personnel 		
			Additional goals		
A-2.5	Define the organizational boundaries of the assurance initiative.		<p><i>Describe the organizational boundaries of the assurance engagement, i.e., to which organizational entities the review is limited. All other aspects of scope limitation are identified during phase A-3.</i></p> <ul style="list-style-type: none"> • The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment. • Obtain information and form an understanding of the business reasons underlying the audit. • Identify the senior business resources responsible for the review. • Identify the senior IT audit/assurance resource responsible for the review. • Establish the process for suggesting and implementing changes to the audit/assurance program, and list the authorizations required. • Identify any limitations and/or constraints affecting the audit of specific systems and subsystems. • Identify any third-party services, applications, platforms and infrastructure elements that may not be or only partially be accessible. • Identify any legal, regulatory or contractual constraints on audit. • Identify any industrial relations-based or end user-based audit constraints. 		

Audit/Accrual Program for SAP ERP Financial Accounting FI Module									
Phase A—Determine Scope of the Assurance Initiative									
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment				
A-3	Determine the enablers in scope and the instance(s) of the enablers in scope.	COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.							
A-3.1	<u>Define the Principles, Policies and Frameworks</u> in scope.	<p>Guiding principles and policies include:</p> <ul style="list-style-type: none"> • Policy for Master Data Maintenance • Information security management system (ISMS) policy • Legal and regulatory compliance requirements 							
A-3.2	<u>Define which Processes</u> are in scope of the review. Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of process goals • Application of process good practices • Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments) 	<p><i>COBIT 5: Enabling Processes</i> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed.</p> <table border="1"> <tr> <td>Key processes</td><td> <ul style="list-style-type: none"> • General Ledger (FI-GL) • Bank Accounting (FI-BL) • Asset Accounting (FI-AA) </td></tr> <tr> <td>Additional processes</td><td> <ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA03 Monitor, Evaluate and Assess Compliance With External Requirements </td></tr> </table>		Key processes	<ul style="list-style-type: none"> • General Ledger (FI-GL) • Bank Accounting (FI-BL) • Asset Accounting (FI-AA) 	Additional processes	<ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA03 Monitor, Evaluate and Assess Compliance With External Requirements 		
Key processes	<ul style="list-style-type: none"> • General Ledger (FI-GL) • Bank Accounting (FI-BL) • Asset Accounting (FI-AA) 								
Additional processes	<ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA03 Monitor, Evaluate and Assess Compliance With External Requirements 								
A-3.3	<u>Define which Organisational Structures</u> will be in scope. Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of Organisational Structure goals, i.e., decisions • Application of Organisational Structures good practices 	Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail. <table border="1"> <tr> <td>Key Organisational Structures</td><td> <ul style="list-style-type: none"> • Financial accounting • Tax department • General Accounting • Treasury </td></tr> <tr> <td>Additional Organisational Structures</td><td> <ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office </td></tr> </table>		Key Organisational Structures	<ul style="list-style-type: none"> • Financial accounting • Tax department • General Accounting • Treasury 	Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office 		
Key Organisational Structures	<ul style="list-style-type: none"> • Financial accounting • Tax department • General Accounting • Treasury 								
Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office 								
A-3.4	<u>Define the Culture, Ethics and Behaviour</u> aspects in scope.	In the context of this engagement, the following enterprise-wide culture and behaviours are in scope: <ul style="list-style-type: none"> • Risk- and compliance-aware culture • Enabling of continuous improvement 							

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
		<ul style="list-style-type: none"> • Accountability • Discipline to follow instructions 						
A-3.5	<p><u>Define the Information items</u> in scope.</p> <p>Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of Information goals, i.e., quality criteria of the information items • Application of Information good practices (Information attributes) 	<p>Based on the subject matter of this audit/accuracy program, the following Information items have been identified as key items.</p> <table border="1"> <tr> <td>Key Information Items</td><td> <ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids </td></tr> <tr> <td>Additional Information Items</td><td> <ul style="list-style-type: none"> • Organizational charts </td></tr> </table>	Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 	Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 		
Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 							
Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 							
A-3.6	<u>Define the Services, Infrastructure and Applications</u> in scope.	<p>In the context of this assignment, and taking into account the goals identified in A-2.4, the following services and related applications or infrastructure could be considered in scope of the review:</p> <ul style="list-style-type: none"> • SAP ERP System • Master data maintenance • Change management • SAP training 						
A-3.7	<p><u>Define the People, Skills and Competencies</u> in scope.</p> <p>Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of skills set goals • Application of skills set and competencies good practices 	<p>In the context of this engagement, taking into account key processes and key roles, the following skill sets are included in scope:</p> <ul style="list-style-type: none"> • Proficiency using the SAP Financial Accounting Module • Master data management skills • Financial accounting skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 						

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																											
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment																						
B-1	Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.																										
B-1.1	<p><u>Obtain</u> (and <u>agree on</u>) metrics for enterprise goals and expected values of the metrics. <u>Assess</u> whether enterprise goals in scope are achieved.</p> <p>Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.</p> <p>Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</p> <p>The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>Enterprise Goal</th><th>Metric</th><th>Expected Outcome (Ex)</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>EG03 Managed business risk (safeguarding of assets)</td><td> <ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG04 Compliance with external laws and regulations</td><td> <ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG07 Business service continuity and availability</td><td> <ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG11 Optimisation of business process functionality</td><td> <ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG15 Compliance with internal policies</td><td> <ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>	Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step	EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG04 Compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG04 Compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
B-1.2	<p><u>Obtain</u> (and <u>agree on</u>) metrics for IT-related goals and expected values of the metrics and <u>assess</u> whether IT-related goals in scope are achieved.</p> <p>The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>IT-related Goal</th><th>Metric</th><th>Expected Outcome (Ex)</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>ITG01 Alignment of IT and business strategy</td><td> <ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals </td><td>Agree on the expected values for the IT-related goal metrics, i.e.,</td><td>In this step, the related metrics for each goal will be reviewed and an</td></tr> </tbody> </table>	IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step	ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals 	Agree on the expected values for the IT-related goal metrics, i.e.,	In this step, the related metrics for each goal will be reviewed and an																		
IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals 	Agree on the expected values for the IT-related goal metrics, i.e.,	In this step, the related metrics for each goal will be reviewed and an																								

Audit/Accrual Program for SAP ERP Financial Accounting FI Module						
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment
		<ul style="list-style-type: none"> Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services Percent of IT value drivers mapped to business value drivers 	<i>the values against which the assessment will take place.</i>	<i>assessment will be made whether the defined criteria are achieved.</i>		
ITG02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment Number of non-compliance issues relating to contractual agreements with IT service providers Coverage of compliance assessments 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>			
ITG04 Managed IT-related business risk	<ul style="list-style-type: none"> Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent of enterprise risk assessments including IT-related risk Frequency of update of risk profile 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>			
ITG07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>			
ITG08 Adequate use of applications, information and technology solutions	<ul style="list-style-type: none"> Percent of business process owners satisfied with supporting IT products and services Level of business user understanding of how technology solutions support their processes Satisfaction level of business users with training and user manuals Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>			
ITG09 IT Agility	<ul style="list-style-type: none"> Level of satisfaction of business executives with IT's responsiveness to new requirements Number of critical business processes supported by up-to-date infrastructure and applications Average time to turn strategic IT objectives into an agreed-on and approved initiative 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>			

Audit/Accrual Program for SAP ERP Financial Accounting FI Module					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	ITG10 Security of information, processing infrastructure and applications	<ul style="list-style-type: none"> Number of security incidents causing financial loss, business disruption or public embarrassment Number of IT services with outstanding security requirements Time to grant, change and remove access privileges, compared to agreed-on service levels Frequency of security assessment against latest standards and guidelines 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG12 Enablement and support of business processes by integrating applications and technology into business processes	<ul style="list-style-type: none"> Number of business processing incidents caused by technology integration errors Number of business process changes that need to be delayed or reworked because of technology integration issues Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues Number of applications or critical infrastructures operating in silos and not integrated 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG14 Availability of reliable and useful information for decision making	<ul style="list-style-type: none"> Level of business user satisfaction with quality and timeliness (or availability) of management information Number of business process incidents caused by non-availability of information Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG15 IT compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices Frequency of policies review and update 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG16 Competent and motivated business and IT personnel	<ul style="list-style-type: none"> Percent of staff whose IT-related skills are sufficient for the competency required for their role Percent of staff satisfied with their IT-related roles Number of learning/training hours per staff member 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	

Audit/Accrual Program for SAP ERP Financial Accounting FI Module			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-2	Obtain an understanding of the Principles, Policies and Frameworks in scope and set suitable assessment criteria. Assess Principles, Policies and Frameworks.		
Principles, policies and frameworks: Policy for Master Data Maintenance			
B-2.1a	<u>Understand the Principles, Policies and Frameworks context.</u> <i>Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks</i>		
B-2.2a	<u>Understand the stakeholders of the Principles, Policies and Frameworks.</u> <i>Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.</i>		
B-2.3a	<u>Understand the goals for the Principles, Policies and Frameworks</u> , and the related metrics and agree on expected values. Assess whether the Principles, Policies and Frameworks goals (outcomes) are achieved, i.e., assess the effectiveness of the Principles, Policies and Frameworks . Goal: The organization has defined, disseminated and deployed management policies supporting SAP master data maintenance .	Perform the assurance steps using the example criteria described below.	
Goal	Criteria	Assessment Step	
Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.	
Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> • A regular validation of all policies whether they are still up to date • An indication of the policies' expiration date or date of last update 	Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> • A regular validation of all policies whether they are still up to date • An indication of the policies' expiration date or date of last update 	
Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.	
Availability	<ul style="list-style-type: none"> • Policies are available to all stakeholders. • Policies are easy to navigate and have a logical and hierarchical structure. 	<ul style="list-style-type: none"> • Verify that policies are available to all stakeholders. • Verify that policies are easy to navigate and have a logical and hierarchical structure. 	
B-2.4a	<u>Understand the life cycle stages of the Principles, Policies and Frameworks</u> , and agree on the relevant criteria. Assess to what extent the Principles, Policies and Frameworks life cycle is managed. <i>The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01 Manage the IT management framework.</i>		
B-2.5a	<u>Understand good practices related to the Principles, Policies and Frameworks</u> and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. <i>The assurance professional will, by using appropriate auditing techniques assess the following aspects.</i>		
Good Practice	Criteria	Assessment Step	
Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.	
Exception and escalation	<ul style="list-style-type: none"> • The exception and escalation procedure is explained and commonly known. • The exception and escalation procedure 	<ul style="list-style-type: none"> • Verify that the exception and escalation procedure is described, explained and commonly known. 	

Audit/Assurance Program for SAP ERP Financial Accounting FI Module					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		has not become the de facto standard procedure.	<ul style="list-style-type: none"> Through observation of a representative sample, verify that the exception and escalation procedure has not become <i>de facto</i> standard procedure. 		
	Compliance	The compliance checking mechanism and non-compliance consequences are clearly described and enforced.	Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.		
B-2.1 to B-2.5	Repeat steps B-2.1 through B-2.5 for all remaining Principles, Policies and Frameworks in scope. Repeat the steps described above for the remaining Principles, Policies and Frameworks: <ul style="list-style-type: none"> ISMS policy Legal and regulatory compliance requirements 				

Audit/Accurance Program for SAP ERP Financial Accounting FI Module															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes															
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment										
B-3	Obtain understanding of the Processes in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes.														
SAP ERP Financial Accounting process²: General Ledger															
B-3.1a	<u>Understand the Process context.</u>														
B-3.2a	<u>Understand the Process purpose.</u>														
B-3.3a	<u>Understand</u> all process stakeholders and their roles. This is equivalent to understanding the real RACI chart of the process. <i>Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.</i> The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement: General Ledger stakeholders:														
B-3.4a	<u>Understand the Process goals</u> and related metrics³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process. The Process General Ledger has two defined process goals.			The following activities can be performed to assess whether the goals are achieved.											
<table border="1"> <thead> <tr> <th>Process Goal</th> <th>Related Metrics</th> <th>Criteria/Expected Value</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>GL postings are valid, complete, accurate and timely</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>All transactions and events are recorded in the correct accounting period</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>				Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	GL postings are valid, complete, accurate and timely	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	All transactions and events are recorded in the correct accounting period	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step												
GL postings are valid, complete, accurate and timely	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.												
All transactions and events are recorded in the correct accounting period	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.												
B-3.5a	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement: Define and agree on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.) <u>Agree</u> on the process practices that should be in place (process design). <u>Assess</u> the process design , i.e., assess to what extent: <ul style="list-style-type: none"> • Expected process practices are applied. • Accountability and responsibility are assigned and assumed. <u>Evaluate</u> General Ledger														

² Because this is a business process audit/assurance program, several of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes (BAI02 Manage requirements definition, BAI03 Manage solution identification and build, DSS05 Manage security services, DSS06 Manage business process controls) can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources available.

³ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

Audit/Accrual Program for SAP ERP Financial Accounting FI Module																						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																						
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment																	
	<p>COBIT 5 Processes⁴ are described in <i>COBIT 5: Enabling Processes</i>. Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are:</p> <ul style="list-style-type: none"> • A sound process design • The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented. <p>Each practice is typically implemented through a number of activities, and a well-designed process will implement all these practices and activities.</p>																					
	Reference Process	General Ledger	Criteria: 1.1 Changes made to master data are valid, complete, accurate and timely. 1.2 Master data remains current and pertinent. 1.3 GL postings are valid, complete, accurate and timely. 1.4 All transactions and events that should be recorded are recorded in the correct accounting period. 1.5 Changes in business and accounting principles do not affect the general ledger (GL).																			
	Reference Process Practices ⁵	Good Practice	Assessment Step		Issue Cross-reference	Comment																
	DSS01 DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.1 On a sample basis, review standard reports and transactions against authorized source documents to assess the accuracy and timeliness of change maintenance that is applied to master data records. The following transaction codes, along with the program names, can be used to produce a list of the changes made to selected FI master records. Users should review a sample of master records to ensure that no audit logs can be modified. (Note: Programs can be executed directly using transaction code SA38—ABAP Reporting).																			
	APO01 DSS05	Changes made to master data are valid, complete, accurate and timely.	<table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Description</th> <th>Program</th> </tr> </thead> <tbody> <tr> <td>S_ALR_87012308</td> <td>GL master data changes</td> <td>RFSABL00</td> </tr> <tr> <td>S_ALR_87012037</td> <td>Asset master data changes</td> <td>RAAEND01</td> </tr> <tr> <td>S_P00_07000008</td> <td>Bank master data changes</td> <td>RFBKABL0</td> </tr> </tbody> </table> <p>1.1.2 Review organizational policy and process design specifications regarding access to maintain master data as shown below. Use transaction code SUIM—User Information System to test user access to the following transaction codes: FS00—Account Master Record Maintenance. Central view (both COA segment and company code segment) FSS0—Account Master Record in Company Code Segment FSP0—Account Master Record in Chart of Accounts segment</p> <p>Proper enforcement of a segregation of duties strategy improves controls surrounding master data maintenance. The enterprise should test user access to transactions to maintain master data as follows.</p> <table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> </table>	Transaction (s)	Description	Program	S_ALR_87012308	GL master data changes	RFSABL00	S_ALR_87012037	Asset master data changes	RAAEND01	S_P00_07000008	Bank master data changes	RFBKABL0	Transaction (s)	Authorization Objects	Fields	Values			
Transaction (s)	Description	Program																				
S_ALR_87012308	GL master data changes	RFSABL00																				
S_ALR_87012037	Asset master data changes	RAAEND01																				
S_P00_07000008	Bank master data changes	RFBKABL0																				
Transaction (s)	Authorization Objects	Fields	Values																			

⁴ For this audit/accrual program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the SAP ERP Financial Accounting FI processes in scope.

⁵ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Financial Accounting FI Module audit/accrual program.

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment
	FS00—Account Master Record Maintenance	F_SKA1_BES	ACTVT	01, 02, 03, 05, 06		
		F_SKA1_BUK	ACTVT	01, 02, 03, 05, 06		
		F_SKA1_KTP	ACTVT	01, 02, 03, 05, 06		
	FS01—GL Account: Maintain Centrally—Create	F_SKA1_KTP	ACTVT	01		
	FS02—GL Account: Maintain Centrally—Change	F_SKA1_KTP	ACTVT	02		
	FS05—GL Account: Maintain Centrally—Block	F_SKA1_KTP	ACTVT	05		
	FS06—GL Account: Maintain Centrally—Delete	F_SKA1_KTP	ACTVT	06		
	FSP1—GL Account: Maintain COA—Create	F_SKA1_KTP	ACTVT	01		
	FSP2—GL Account: Maintain COA—Change	F_SKA1_KTP	ACTVT	02		
	FSP5—GL Account: Maintain COA—Block	F_SKA1_KTP	ACTVT	05		
	FSP6—GL Account: Maintain COA—Delete	F_SKA1_KTP	ACTVT	06		
	FSS1—GL Account: Maintain Company Code—Create	F_SKA1_BUK	ACTVT	01		
	FSS2—GL Account: Maintain Company Code—Change	F_SKA1_BUK	ACTVT	02		
	FSS5—GL Account: Maintain Company Code—Block	F_SKA1_BUK	ACTVT	05		
	FSS6—GL Account: Maintain Company Code—Delete	F_SKA1_BUK	ACTVT	06		
	OB_GLACC11—GL Mass Maintenance					
	AS01—Create Asset Master Record	A_S_ANLKL	ACTVT	01		
	AS02—Change Asset Master Record	A_S_ANLKL	ACTVT	02		
	AS05—Block Asset Master Record	A_S_ANLKL	ACTVT	05		
	AS06—Delete Asset Record and/or Mark for Deletion	A_S_ANLKL	ACTVT	06		

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes								
Ref.	Assurance Steps and Guidance					Issue Cross-reference	Comment	
			AS11—Create Asset Subnumber	A_S_ANLKL	ACTVT	01		
			AS21—Create Asset Group	A_S_ANLGR	ACTVT	01		
			AS22—Change Asset Group	A_S_ANLGR	ACTVT	02		
			AS24—Create Asset Group Subnumber	A_S_ANLGR	ACTVT	04		
			AS25—Block Group Asset	A_S_ANLGR	ACTVT	05		
			AS26—Delete Group Asset	A_S_ANLGR	ACTVT	06		
			AS81—Create Legacy Asset Group	A_S_ANLGR	ACTVT	01		
			AS82—Change Legacy Asset Group	A_S_ANLGR	ACTVT	02		
			AS84—Create Legacy Asset Group Subnumber	A_S_ANLGR	ACTVT	04		
			AS91—Create Legacy Asset	A_S_ANLKL	ACTVT	01		
			AS92—Change Legacy Asset	A_S_ANLKL	ACTVT	02		
			AS94—Create Legacy Asset Subnumber	A_S_ANLKL	ACTVT	04		
			AT01—Create Asset Master Record—Depreciation Area	A_S_ANLKL	ACTVT	01		
			AT02—Change Asset Master Record—Depreciation Area	A_S_ANLKL	ACTVT	02		
			FI01—Create Bank	F_BNKA_MAN	ACTVT	01		
			FI02—Change Bank	F_BNKA_MAN	ACTVT	02		
			FI06—Set Flag to Delete Bank	F_BNKA_MAN	ACTVT	06		
DSS06	Changes made to master data are valid, complete, accurate and timely.	1.1.3 Determine whether the configurable control settings address the risk pertaining to the validity, completeness and accuracy of master data and whether the settings are in accordance with management intentions.	<ul style="list-style-type: none"> • Access the settings online to customize IMG, as follows. Use transaction code OBD4— C FI Maintain Table T077S to check GL account groups for appropriate field status maintenance and number range assignments. • To validate the combination of house bank ID, account ID and GL account access, use transaction code FI12—Change House Bank/Bank Accounts or check the table T012K via transaction code SE16N—General Table Display. • The automated transfer of bank data can be validated by verifying the bank directory table BNKA via transaction code SE16N—General Table Display with the background job logs from program RFBVBIC_0 or RFBVALL_0, which update the banking records. 					

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																
Ref.	Assurance Steps and Guidance			Issue Cross-reference												
				Comment												
			<ul style="list-style-type: none"> Review the definition of screen layout for asset master data or asset depreciation areas using transaction code SPRO to display the IMG menu and follow path: Financial Accounting → Asset Accounting → Master Data → Screen Layout. Use transaction code AW01N —Asset Explorer to compare depreciation areas (planned and actual depreciation postings). 													
DSS06	Master data remains current and pertinent.	1.2.1 Use the transaction codes and programs shown below to determine whether the appropriate management report displays or produces a list of master data records. Confirm evidence of management review of the master data on a rotating basis.	<table border="1"> <thead> <tr> <th>Transaction (s)</th><th>Description</th><th>Program</th></tr> </thead> <tbody> <tr> <td>S_ALR_87012328</td><td>GL Account List</td><td>RFSKVZ00</td></tr> <tr> <td>S_P99_41000166</td><td>Bank Directory</td><td>RFBKVZ00</td></tr> <tr> <td>AR02</td><td>Asset History Sheet</td><td>RAGITT_ALV01</td></tr> </tbody> </table>	Transaction (s)	Description	Program	S_ALR_87012328	GL Account List	RFSKVZ00	S_P99_41000166	Bank Directory	RFBKVZ00	AR02	Asset History Sheet	RAGITT_ALV01	
Transaction (s)	Description	Program														
S_ALR_87012328	GL Account List	RFSKVZ00														
S_P99_41000166	Bank Directory	RFBKVZ00														
AR02	Asset History Sheet	RAGITT_ALV01														
DSS05	GL postings are valid, complete, accurate and timely.	1.3.1 Review organizational policy and process design specifications regarding the testing of user access to transactions for posting journal entries. Transaction codes with similar authorization checks are grouped together, as seen below, due to the number of transaction codes that allow for the posting of journal. Each of the transaction codes should be tested separately. For any groups with F_BKPF_KOA and multiple ACTVT values, test F_BKPF_KOA field ACTVT with a value of 01 and test F_BKPF_BUK with all values listed:	<ul style="list-style-type: none"> F.07—G/L: Balance Carryforward F.07—G/L: Balance Carryforward F.19—G/L: Goods/Invoice Received Clearing F.56—Delete Recurring Document F.57—G/L: Delete Sample Documents F.5E—G/L: Post Balance Sheet Adjustment F.80—Mass Reversal of Documents F.81—Reverse Posting for Accr./Defer.Docs F-01—Enter Sample Document F-02—Enter G/L Account Posting F-03—Clear G/L Account F-04—Post with Clearing F-34—Post Collection FB01—Post Document FB01L—General Posting for Ledger Group FB02—Change Document FB05—Post with Clearing FB08—Reverse Document FB11—Post Held Document FB15—Assign Items FB41—Post Tax Payable FB50—G/L Account Posting: Single Screen Transaction FB50L—Enter G/L Account Document for Ledger Group FBCJ—Cash Journal FBD1—Enter Recurring Entry FBD2—Change Recurring Entry 													

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																																											
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference																																							
	<ul style="list-style-type: none"> FBD5—Realize Recurring Entry FBD9—Enter Recurring Entry FBR1—Post With Reference Document FBR2—Post Document FBRA—Reset Cleared Items FBS1—Enter Accrual/Deferral Document FBU2—Change Intercompany Document FBU8—Reverse Cross-Company Code Document <table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>F.80, F-01, F-02, F-04, F-34, FB01, FB01L, FB05, FB11, FB41, FBD1, FBD9, FBR1, FBR2, FBU8</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>F.5E, F-03, FB08, FBD5</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>01, 02</td> </tr> <tr> <td>FB02, FBD2</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td>F.07, FB1S, FBS1</td> <td>F_BKPF_BUK</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>F.19, F.81, FB50L, FBRA</td> <td>F_BKPF_BUK</td> <td>ACTVT</td> <td>01, 02</td> </tr> <tr> <td>F.56, F.57, FB02</td> <td>F_BKPF_BUK</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td>FB50</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>01, 02, 10</td> </tr> <tr> <td>FBCJ</td> <td>F_BKPF_BUK</td> <td>ACTVT</td> <td>01, 02, 10, 33</td> </tr> <tr> <td>FBV0</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>01, 06, 77</td> </tr> </tbody> </table>	Transaction (s)	Authorization Objects	Fields	Values	F.80, F-01, F-02, F-04, F-34, FB01, FB01L, FB05, FB11, FB41, FBD1, FBD9, FBR1, FBR2, FBU8	F_BKPF_KOA F_BKPF_BUK	ACTVT	01	F.5E, F-03, FB08, FBD5	F_BKPF_KOA F_BKPF_BUK	ACTVT	01, 02	FB02, FBD2	F_BKPF_KOA F_BKPF_BUK	ACTVT	02	F.07, FB1S, FBS1	F_BKPF_BUK	ACTVT	01	F.19, F.81, FB50L, FBRA	F_BKPF_BUK	ACTVT	01, 02	F.56, F.57, FB02	F_BKPF_BUK	ACTVT	02	FB50	F_BKPF_KOA F_BKPF_BUK	ACTVT	01, 02, 10	FBCJ	F_BKPF_BUK	ACTVT	01, 02, 10, 33	FBV0	F_BKPF_KOA F_BKPF_BUK	ACTVT	01, 06, 77		
Transaction (s)	Authorization Objects	Fields	Values																																								
F.80, F-01, F-02, F-04, F-34, FB01, FB01L, FB05, FB11, FB41, FBD1, FBD9, FBR1, FBR2, FBU8	F_BKPF_KOA F_BKPF_BUK	ACTVT	01																																								
F.5E, F-03, FB08, FBD5	F_BKPF_KOA F_BKPF_BUK	ACTVT	01, 02																																								
FB02, FBD2	F_BKPF_KOA F_BKPF_BUK	ACTVT	02																																								
F.07, FB1S, FBS1	F_BKPF_BUK	ACTVT	01																																								
F.19, F.81, FB50L, FBRA	F_BKPF_BUK	ACTVT	01, 02																																								
F.56, F.57, FB02	F_BKPF_BUK	ACTVT	02																																								
FB50	F_BKPF_KOA F_BKPF_BUK	ACTVT	01, 02, 10																																								
FBCJ	F_BKPF_BUK	ACTVT	01, 02, 10, 33																																								
FBV0	F_BKPF_KOA F_BKPF_BUK	ACTVT	01, 06, 77																																								
BAI10 DSS06	GL postings are valid, complete, accurate and timely	1.3.2 Through discussions with management, determine the status for the line-item level fields for which one of the HDRO needs to be maintained. Check the actual status maintained for the fields in the field status variant by using transaction code OBC4—C FI Maintain Table T004V.																																									
BAI10 DSS06	GL postings are valid, complete, accurate and timely	1.3.3 Ascertain from management the document types and posting keys used, and then check the system configuration using the details below.																																									
		<table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Table</th> </tr> </thead> <tbody> <tr> <td>OBA7— Define Document Types</td> <td>T003</td> </tr> <tr> <td>OB41— Define Posting Keys</td> <td>TBSL</td> </tr> </tbody> </table>	Transaction (s)	Table	OBA7— Define Document Types	T003	OB41— Define Posting Keys	TBSL																																			
Transaction (s)	Table																																										
OBA7— Define Document Types	T003																																										
OB41— Define Posting Keys	TBSL																																										
DSS01 DSS06	GL postings are valid, complete, accurate and timely	1.3.4 To complete a reconciliation of the subledger accounts for AP (or AR), the user must first determine which GL accounts have been assigned as a reconciliation account in the vendor or customer master data. For vendors, use transaction code SE16N—General Table Display to review table LFB1 (for customers table KNB1).																																									

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																								
Ref.	Assurance Steps and Guidance			Issue Cross-reference																				
				Comment																				
		<p>Prepare a list of the reconciliation accounts for(Customers & Vendors) and extract the output of open items of the accounts using transaction code FAGLL03 (separate extracts for AR and AP); these totals can then be compared with the output of table BSIK for AP and table BSID for AR. Similarly, for the cleared items, an extract needs to be taken for all of the cleared items of the AP & AR reconciliation accounts from FAGLL03 & compared with the output of tables BSAK for AP & BSAD for AR. Run two reports for each table because the values are listed in absolute values.</p> <p>Run one report once for S in the Debit/Credit field (SHKZG), and run the second report with H. Subtraction of H transactions from the S transactions should be equal to the sum of the reconciliation accounts for the given area (AR or AP). Determine, with management, a dedicated person or team to perform manual reconciliation on a periodic basis, and check the reconciliation based on sampling.</p>																						
DSS01 DSS06	GL postings are valid, complete, accurate and timely	<p>1.3.5 Review organizational policy and process design specifications regarding testing user access to parking journal entries. Use transaction code SUIM—User Information System to test user access and segregation of duties using the access listed in testing technique 1.3.1.</p> <table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Authorization Objects</th> <th>Field</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>F-65—Preliminary Posting</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>77</td> </tr> <tr> <td>FBV1—Park Document</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>77</td> </tr> <tr> <td>FBV2—Change Parked Document</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>77</td> </tr> <tr> <td>FV50—Park G/L Account Items</td> <td>F_BKPF_KOA F_BKPF_BUK</td> <td>ACTVT</td> <td>77</td> </tr> </tbody> </table> <p>Note: Transaction code FBV5—Document Changes of Parked Document can also be used to display the changes made to parked documents.</p>	Transaction (s)	Authorization Objects	Field	Values	F-65—Preliminary Posting	F_BKPF_KOA F_BKPF_BUK	ACTVT	77	FBV1—Park Document	F_BKPF_KOA F_BKPF_BUK	ACTVT	77	FBV2—Change Parked Document	F_BKPF_KOA F_BKPF_BUK	ACTVT	77	FV50—Park G/L Account Items	F_BKPF_KOA F_BKPF_BUK	ACTVT	77		
Transaction (s)	Authorization Objects	Field	Values																					
F-65—Preliminary Posting	F_BKPF_KOA F_BKPF_BUK	ACTVT	77																					
FBV1—Park Document	F_BKPF_KOA F_BKPF_BUK	ACTVT	77																					
FBV2—Change Parked Document	F_BKPF_KOA F_BKPF_BUK	ACTVT	77																					
FV50—Park G/L Account Items	F_BKPF_KOA F_BKPF_BUK	ACTVT	77																					
DSS05	GL postings are valid, complete, accurate and timely	<p>1.3.6 Use transaction code SUIM—User Information System to test user access to the following transaction codes:</p> <table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Authorization Objects</th> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>OC41— Maintain Exchange Rates</td> <td>S_TABU_DIS</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td>OB08— C FI Maintain Table <small>TCURR</small></td> <td>S_TABU_DIS</td> <td>ACTVT</td> <td>02</td> </tr> <tr> <td>S_BCE_68000174— C FI Maintain Table TCURR</td> <td>S_TABU_DIS</td> <td>ACTVT</td> <td>02</td> </tr> </tbody> </table>	Transaction (s)	Authorization Objects	Field	Value	OC41— Maintain Exchange Rates	S_TABU_DIS	ACTVT	02	OB08— C FI Maintain Table <small>TCURR</small>	S_TABU_DIS	ACTVT	02	S_BCE_68000174— C FI Maintain Table TCURR	S_TABU_DIS	ACTVT	02						
Transaction (s)	Authorization Objects	Field	Value																					
OC41— Maintain Exchange Rates	S_TABU_DIS	ACTVT	02																					
OB08— C FI Maintain Table <small>TCURR</small>	S_TABU_DIS	ACTVT	02																					
S_BCE_68000174— C FI Maintain Table TCURR	S_TABU_DIS	ACTVT	02																					
DSS01	GL postings are valid,	1.3.7 Use transaction code SE13—Maintain Technical Settings (Tables) or transaction code																						

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																							
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																							
Ref.	Assurance Steps and Guidance			Issue Cross-reference																			
	DSS06	complete, accurate and timely	SE16N— General Table Display and table DD09L to confirm that table TCURR is configured to log changes: 1. Use transaction codes OC41—Maintain Exchange Rates or transaction code OB08—C FI Maintain Table TCURR. 2. Click on Utilities. 3. Click on Change Logs 4. Enter the dates for the period for which the user wants to validate the changes. 5. Execute the report. Change logs can also be reviewed using transaction code SCU3—Table History and table TCURR. Determine whether management reviews a sample of changes to exchange rates above a certain percentage in regard to the volume and value of foreign currency transactions for the organization.																				
	DSS05	GL postings are valid, complete, accurate and timely	1.3.8 Use transaction code SUIM—User Information System to test user access to the exchange rate ratio configuration and the rounding value configuration, as seen below. <table border="1" data-bbox="777 763 1628 959"> <thead> <tr> <th>Transaction (s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>OB90— C FI Maintain Table</td><td>S_TABU_DIS</td><td>ACTVT</td><td>02</td></tr> <tr> <td>OBBS— C FI Maintain Table</td><td>S_TABU_DIS</td><td>ACTVT</td><td>02</td></tr> <tr> <td rowspan="2">SM30— Call View Maintenance</td><td>S_TABU_DIS</td><td>ACTVT</td><td>02</td></tr> <tr> <td>S_TABU_DIS</td><td>DICBERCLS</td><td>02</td></tr> </tbody> </table>	Transaction (s)	Authorization Objects	Fields	Values	OB90— C FI Maintain Table	S_TABU_DIS	ACTVT	02	OBBS— C FI Maintain Table	S_TABU_DIS	ACTVT	02	SM30— Call View Maintenance	S_TABU_DIS	ACTVT	02	S_TABU_DIS	DICBERCLS	02	
Transaction (s)	Authorization Objects	Fields	Values																				
OB90— C FI Maintain Table	S_TABU_DIS	ACTVT	02																				
OBBS— C FI Maintain Table	S_TABU_DIS	ACTVT	02																				
SM30— Call View Maintenance	S_TABU_DIS	ACTVT	02																				
	S_TABU_DIS	DICBERCLS	02																				
	BAI10 DSS06	All transactions and events that should be recorded are recorded in the correct accounting period.	1.4.1 Generate the posting periods open or close configuration (using the transaction codes OB52—C FI Maintain Table T001B or transaction code SE16N—General Table Display and table T001B) and the fiscal year variant configuration setting (using transaction codes OB29—C FI Fiscal Year Variants or SE16N—General Table Display and table V_T009_A). Determine whether these settings comply with management intentions.																				
	DSS01 DSS06	All transactions and events that should be recorded are recorded in the correct accounting period.	1.4.2 Use transaction code SE13—Maintain Technical Settings (Tables) or transaction code SE16N—General Table Display and table DD09L to see whether table T001B is configured for the logging of changes. Determine whether management reviews changes to posting periods after periods are closed.																				
	DSS05 DSS06	All transactions and events that should be recorded are recorded in the correct accounting period.	1.4.3 Review settings in table T001B (open period configuration) to ensure that only authorized personnel has access to modify the table.																				
	DSS05 DSS06	All transactions and events that should be recorded are recorded in the correct accounting period.	1.4.4 Ascertain from management that the group of users with access to change table T001B have a valid business need and access has been properly approved before is granted.																				
	DSS01 DSS06	All transactions and events that should be recorded are recorded in the correct accounting period.	1.4.5 Ascertain from management whether any special scenario in the business activated additional ledgers during the fiscal year or during the year end. Determine whether any responsible team/person monitored the postings during the critical period. Obtain the review logs applicable to those periods and validate. Look for any exceptions.																				

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module											
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes											
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment					
B-3.6a	APO12 DSS06 MEA03	Changes in business and accounting principles do not affect the general ledger (GL).	1.5.1 Discuss with management any recent changes in the business process that have led to changes in the accounting principles. Verify whether these changes are reflected in the GL.								
	BAI10 DSS06	Changes in business and accounting principles do not affect the general ledger (GL).	1.5.2 Ascertain with management whether the enterprise requires multiple accounting principles. Using transaction code FAGL_ACTIVATION, verify whether a new GL has been activated. If the business requires multiple accounting principles, then verify whether leading (OL) and nonleading ledgers have been activated using transaction code SPRO to display the IMG menu and follow path: Financial Accounting (New) → Financial Accounting Global Settings (New) → Ledgers → Ledger → Define Ledgers for GL Accounting.								
<u>Agree</u> on the process work products ⁶ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available. Process General Ledger inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.											
Process Practice		Work Products		Assessment Step							
Master data maintenance		<ul style="list-style-type: none"> • Master data add/change/delete request forms • Master data maintenance procedures • Master data maintenance reports • List of SAP users with master data access 		Apply appropriate audit techniques to determine the existence and appropriate use of each work product.							
General ledger posting		<ul style="list-style-type: none"> • Journal entries • General ledger reports • Accounting procedures • List of SAP users with access to the general ledger 		Apply appropriate audit techniques to determine the existence and appropriate use of each work product.							
B-3.7a	<u>Agree</u> on the process capability level to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>										
SAP ERP Financial Accounting process: Bank accounting											
B-3.1b	<u>Understand</u> the Process context.										
B-3.2b	<u>Understand</u> the Process purpose.										
B-3.3b	<u>Understand</u> all process stakeholders and their roles.										
Bank accounting stakeholders: Understand the Process goals and related metrics ⁷ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process. The Process Bank accounting has one defined process goal.											
Process Goal		Related Metrics		Criteria/Expected Value		Assessment Step					

⁶ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*.

⁷ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment
	Accurate, complete, valid and timely processing of banking transactions	<ul style="list-style-type: none"> Number of errors reported by the bank Number of duplicate payments identified Number of days to pay invoices 	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
B-3.5b	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement: Evaluate Bank Accounting		Reference Process Bank accounting Criteria: 2.1 Formats of interchange of structure data used by the bank and the organization's lockbox are compatible. 2.2 Data file (BAI/BAI2) with payment information from the connecting banks is promptly received. 2.3 Open invoices are cleared on time. 2.4 Duplicate payment files are not received from banks. 2.5 Lockbox matches the check amount with the total invoices listed. 2.6 Manual linkage of payment with open invoices is accurate, valid or timely. 2.7 Invoices are not left unpaid for a considerable time.			
	Reference Process Practices⁸	Good Practice	Assessment Step		Issue Cross-reference	Comment
	DSS01 DSS05	Formats of interchange of structure data used by the bank and the organization's lockbox are compatible.	2.1.1 Obtain the interconnection agreement with the house bank from management. <ul style="list-style-type: none"> Verify whether the format of the data exchange between the systems has been specified in the agreement. Review the file format from current or archived data from the server in SAP using standard transaction code AL11—Display SAP Directories, and ascertain whether the format is consistent with the agreement. 			
	DSS01 DSS06	Data file (BAI/BAI2) with payment information from the connecting banks is promptly received.	2.2.1 Obtain the name of the job that runs for data exchange between systems (program RFEBLB00 is typically one of the standard load programs used). Using transaction code SM37—Overview of Job Selection, confirm that alerts and/or notifications are sent to the appropriate job owners when a program fails to load data.			
	DSS01 DSS06	Data file (BAI/BAI2) with payment information from the connecting banks is promptly received.	2.2.2 Using the job name found in control 2.2.1 and transaction code SM37— Overview of Job Selection, review a sample of the logs that are generated by the background jobs to validate the timeliness and correct format of the data received.			
	BAI10	Open invoices are cleared on time.	2.3.1 Using the job name found in control 2.2.1 and transaction code SM37— Overview of Job Selection in SAP, confirm that the background jobs are configured to run at appropriate intervals, and the status of the jobs can be validated.			
	DSS01 DSS06	Open invoices are cleared on time.	2.3.2 Using the job name found in control 2.2.1 and transaction code SM37— Overview of Job Selection in SAP, validate that management is reviewing the output and/or log of the lockbox program after each scheduled run via transaction code SM37.			
	DSS06	Duplicate payment files are not received from banks.	2.4.1 Review the period-end logs and compare the balance of documents for invoice document types and payment document types to check for any variance (standard document type for customer invoice is DR, and standard payment document type for customer is DZ). Verify with the accounting team whether any custom document types are used or whether the standard			

⁸ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Financial Accounting FI Module audit/accuracy program.

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.6b			customer payment history report can be executed to display the payments list.		
	DSS01 DSS06	Lockbox matches the check amount with the total invoices listed.	2.5.1 Ascertain whether a process is in place for a team or individual to validate and compare the incoming BAI/BAI2 format data file with the scanned check images.		
	DSS01 DSS06	Lockbox matches the check amount with the total invoices listed.	2.5.2 Refer to testing technique 2.1.1 to validate the incoming file is correct.		
	DSS01 DSS06	Lockbox matches the check amount with the total invoices listed.	2.5.3 After the lockbox program completes processing the lockbox files from banks (transaction code FLBP—Post Lockbox Data and program RFEBLB30), the system generates a posting log report, which contains the details for applied, partially applied, on account and unprocessed items. Execute the transaction code FEBA_LOCKBOX to check the status of the available lockbox items.		
	DSS01 DSS06	Lockbox matches the check amount with the total invoices listed.	2.5.4 Verify whether personnel are assigned to review the status of the items and manually correct the unapplied item by using the transaction code FEBA_LOCKBOX, lockbox postprocessing. This transaction allows activities to be performed manually to link the open items with the incoming payments.		
	DSS05	Manual linkage of payment with open invoices is accurate, valid, or timely.	2.6.1 Use transaction code SUIM—User Information System to test user access to transaction codes FEBA_LOCKBOX (it is the same transaction as FEBAN and program SAPLNEW_FEBA).		
	DSS05	Manual linkage of payment with open invoices is accurate, valid, or timely.	2.6.2 Determine whether the AR processing team tasks are segregated, so that the invoicing team does not have access to the FEBA_LOCKBOX transaction code.		
	DSS01 DSS06	Manual linkage of payment with open invoices is accurate, valid, or timely.	2.6.3 Assess whether periodic review and sign-off is documented by management after review of the lockbox process for the period, based on the frequency defined by the enterprise.		
	DSS01 DSS06	Manual linkage of payment with open invoices is accurate, valid, or timely.	2.6.4 Use transaction code S_ALR_87012168 to display the report for Due Date Analysis for Open Item and determine whether management review this report for aging items. Request evidence of appropriate follow up actions. This also can be executed using transaction code SA38—ABAP Reporting with program PAZLJ6JB1S3514OL9BS4WZ61KX.		
	DSS01 DSS06	Invoices are not left unpaid for a considerable time.	2.7.1 Use testing technique 2.6.4 to verify whether management reviews the AR aging report to detect invoices that have been open for an extended period of time. Request evidence of appropriate follow-up actions.		
B-3.6b	Agree on the process work products ⁹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.				
	Process Bank accounting inputs and outputs. The most relevant (and not assessed as information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.	
	Process Practice	Work Products	Assessment Step		
	Bank accounting	<ul style="list-style-type: none"> • Bank interface configuration requirement definition • Transaction error reports • Invoice aging reports • Bank statements 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		

⁹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.7b	Agree on the process capability level to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				
SAP ERP Financial Accounting process: Asset accounting					
B-3.1c	<u>Understand the Process context.</u>				
B-3.2c	<u>Understand the Process purpose.</u>				
B-3.3c	<u>Understand all process stakeholders</u> and their roles. Asset accounting stakeholders:				
B-3.4c	<u>Understand the Process goals</u> and related metrics ¹⁰ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.				
	The Process Asset accounting has three defined process goals.			The following activities can be performed to assess whether the goals are achieved.	
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	
	Asset transactions (acquisitions, transfers and retirements) are valid, complete, accurate and timely	<ul style="list-style-type: none"> Number of records posted incorrectly Transaction posted after the closing period 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Physical assets are completely and/or accurately recorded in the system	<ul style="list-style-type: none"> Number of errors in physical asset recording Number of physical assets that are not recorded 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Depreciation is applied accurately on the assets	<ul style="list-style-type: none"> Number of errors in depreciation accounting 	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
B-3.5c	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement: Evaluate Asset Accounting				
	Reference Process	Asset accounting	Criteria: 3.1 Asset transactions (acquisitions, transfers, and retirements) are valid, complete, accurate and timely. 3.2 Physical assets are completely and/or accurately recorded in the system. 3.3 Depreciation is applied accurately on the assets.		
	Reference Process Practices ¹¹	Good Practice	Assessment Step		Issue Cross-reference

¹⁰ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

¹¹ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Financial Accounting audit/accuracy program.

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																
Ref.	Assurance Steps and Guidance			Issue Cross-reference												
	DSS05 DSS06	Asset transactions (acquisitions, transfers and retirements) are valid, complete, accurate, and timely.	3.1.1 Review organizational policy and process design specifications to test user access to asset accounting transactions. Use transaction code SUIM—User Information System to test user access to the following transactions: Asset Acquisition <table border="1"><thead><tr><th>Transaction</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr></thead><tbody><tr><td>AB01—Create Asset Transaction ABNA—Post-Capitalization ABNAN—Post-Capitalization ABNC—Enter Post-Capitalization ABZE—Acquisition from in-house Production ABZK—Acquisition from Purchase with Vendor ABZO—Asset Acquisition Automated Offset Posting ABZON—Acquis. w/Autom. Offsetting Entry ABZP—Acquisition from affiliated company ABZV—Asset Acquis. Posted w/Clearing Acct AIBU—Transfer Asset under Const. F-90—Acquisition from purchase w. vendor F-91—Asset Acquisition Posted with Clearing Account Scrapping ABNE—Subsequent Revenue ABNK—Subsequent Costs F-92—Asset Retirement from Sale with Customer</td><td>A_B_ANLKL</td><td>ACTVT</td><td>01</td></tr></tbody></table> Asset Disposition <table border="1"><thead><tr><th>Transaction</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr></thead></table>	Transaction	Authorization Objects	Fields	Values	AB01—Create Asset Transaction ABNA—Post-Capitalization ABNAN—Post-Capitalization ABNC—Enter Post-Capitalization ABZE—Acquisition from in-house Production ABZK—Acquisition from Purchase with Vendor ABZO—Asset Acquisition Automated Offset Posting ABZON—Acquis. w/Autom. Offsetting Entry ABZP—Acquisition from affiliated company ABZV—Asset Acquis. Posted w/Clearing Acct AIBU—Transfer Asset under Const. F-90—Acquisition from purchase w. vendor F-91—Asset Acquisition Posted with Clearing Account Scrapping ABNE—Subsequent Revenue ABNK—Subsequent Costs F-92—Asset Retirement from Sale with Customer	A_B_ANLKL	ACTVT	01	Transaction	Authorization Objects	Fields	Values	Comment
Transaction	Authorization Objects	Fields	Values													
AB01—Create Asset Transaction ABNA—Post-Capitalization ABNAN—Post-Capitalization ABNC—Enter Post-Capitalization ABZE—Acquisition from in-house Production ABZK—Acquisition from Purchase with Vendor ABZO—Asset Acquisition Automated Offset Posting ABZON—Acquis. w/Autom. Offsetting Entry ABZP—Acquisition from affiliated company ABZV—Asset Acquis. Posted w/Clearing Acct AIBU—Transfer Asset under Const. F-90—Acquisition from purchase w. vendor F-91—Asset Acquisition Posted with Clearing Account Scrapping ABNE—Subsequent Revenue ABNK—Subsequent Costs F-92—Asset Retirement from Sale with Customer	A_B_ANLKL	ACTVT	01													
Transaction	Authorization Objects	Fields	Values													

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment								
			ABAD—Asset Retirement from Sale with Customer ABAON—Asset Sale Without Customer ABAD_OLD—Asset Retire from Sale with Customer ABAO—Asset Sale Without Customer ABAV—Asset Retirement by Scrapping ABAVN—Asset Retirement by Scrapping ABNE—Subsequent Revenue ABNK—Subsequent Costs F-92—Asset Retirement from Sale with Customer	A_B_ANLKL	ACTVT	01										
			Changes to Asset Subledger <table border="1"> <thead> <tr> <th>Transaction</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td> AB08—Reverse Line Items ABAA—Unplanned Depreciation ABAW—Balance Sheet Revaluation ABCO—Adjustment Posting to Areas ABGF—Credit Memo in Year after Invoice ABGL—Enter Credit Memo in Year of Invoice ABIF—Investment Support ABMA—Manual Depreciation ABMR—Manual Transfer of Reserves ABMW—Reverse Asset Transfer Using Document Number ABSO—Miscellaneous Transactions ABT1—Intercompany Asset Transfer </td><td>A_B_ANLKL</td><td>ACTVT</td><td>01</td></tr> </tbody> </table>	Transaction	Authorization Objects	Fields	Values	AB08—Reverse Line Items ABAA—Unplanned Depreciation ABAW—Balance Sheet Revaluation ABCO—Adjustment Posting to Areas ABGF—Credit Memo in Year after Invoice ABGL—Enter Credit Memo in Year of Invoice ABIF—Investment Support ABMA—Manual Depreciation ABMR—Manual Transfer of Reserves ABMW—Reverse Asset Transfer Using Document Number ABSO—Miscellaneous Transactions ABT1—Intercompany Asset Transfer	A_B_ANLKL	ACTVT	01					
Transaction	Authorization Objects	Fields	Values													
AB08—Reverse Line Items ABAA—Unplanned Depreciation ABAW—Balance Sheet Revaluation ABCO—Adjustment Posting to Areas ABGF—Credit Memo in Year after Invoice ABGL—Enter Credit Memo in Year of Invoice ABIF—Investment Support ABMA—Manual Depreciation ABMR—Manual Transfer of Reserves ABMW—Reverse Asset Transfer Using Document Number ABSO—Miscellaneous Transactions ABT1—Intercompany Asset Transfer	A_B_ANLKL	ACTVT	01													

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																		
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																		
Ref.	Assurance Steps and Guidance					Issue Cross-reference												
			Changes to Asset Subledger (cont.) <table border="1"> <thead> <tr> <th>Transaction</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>ABUB—Transfer Between Areas ABUM—Transfer within Company Code ABUMN—Transfer within Company Code ABZS—Enter Write-UP ABZU—Write-UP AFAB—Post Depreciation AFABN—Post Depreciation AFAR—Recalculated Depreciation AIST—Reverse Settlement of AuC AR29—FI-AA Manual Revaluation</td> <td>A_B_ANLKL</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>AB02—Change Asset Document</td> <td>A_B_ANLKL</td> <td>ACTVT</td> <td>02</td> </tr> </tbody> </table>				Transaction	Authorization Objects	Fields	Values	ABUB—Transfer Between Areas ABUM—Transfer within Company Code ABUMN—Transfer within Company Code ABZS—Enter Write-UP ABZU—Write-UP AFAB—Post Depreciation AFABN—Post Depreciation AFAR—Recalculated Depreciation AIST—Reverse Settlement of AuC AR29—FI-AA Manual Revaluation	A_B_ANLKL	ACTVT	01	AB02—Change Asset Document	A_B_ANLKL	ACTVT	02
Transaction	Authorization Objects	Fields	Values															
ABUB—Transfer Between Areas ABUM—Transfer within Company Code ABUMN—Transfer within Company Code ABZS—Enter Write-UP ABZU—Write-UP AFAB—Post Depreciation AFABN—Post Depreciation AFAR—Recalculated Depreciation AIST—Reverse Settlement of AuC AR29—FI-AA Manual Revaluation	A_B_ANLKL	ACTVT	01															
AB02—Change Asset Document	A_B_ANLKL	ACTVT	02															
DSS06	Asset transactions (acquisitions, transfers and retirements) are valid, complete, accurate, and timely.	3.1.2 Access standard period controls using transaction code OAVS—CAM View Maint. Period Rule (table T090R). Obtain the periods in which the asset transactions need to be posted, and accordingly compare the period control codes in depreciation keys that are assigned to asset master data with the actual postings. (Asset postings can be viewed through the asset explorer, transaction code AW01N.)																
DSS01 DSS06	Asset transactions (acquisitions, transfers and retirements) are valid, complete, accurate, and timely.	3.1.3 Use transaction code AO90—Account Assignment Acquisitions (table T095), verify whether the account determination that is configured in the system is consistent with management intentions and that postings in the system reflect the appropriate GL accounts.																
DSS01 DSS06	Physical assets are completely and/or accurately recorded in the system.	3.2.1 Ascertain whether a report of noncapitalized assets, which is generated using the transaction code S_ALR_87012048—Asset Transactions, is reviewed by management and whether appropriate action is taken if variances are identified.																
DSS01 DSS06	Depreciation is applied accurately on the assets.	3.3.1 Use transaction SPRO to display the IMG menu and follow the path: Financial Accounting → Asset Accounting → Organizational Structure → Copy Reference Chart of Depreciation Areas (copy or delete chart of depreciation areas). Validate the actual system postings. Note: Values maintained for depreciation areas that are based on business requirements can be reviewed using transaction code SE16N—General Table Display and table T093.																

Audit/Accrual Program for SAP ERP Financial Accounting FI Module								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes								
Ref.	Assurance Steps and Guidance			Issue Cross-reference				
B-3.6c	<p><u>Agree</u> on the process work products¹² (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.</p> <p>Asset accounting inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.</p>							
	<table border="1"> <thead> <tr> <th>Process Practice</th> <th>Work Products</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Asset accounting</td> <td> <ul style="list-style-type: none"> • Asset accounting procedures • Physical inventory reports • Depreciation reports • List of SAP users with asset accounting access </td> <td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td> </tr> </tbody> </table>		Process Practice	Work Products	Assessment Step	Asset accounting	<ul style="list-style-type: none"> • Asset accounting procedures • Physical inventory reports • Depreciation reports • List of SAP users with asset accounting access 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.
Process Practice	Work Products	Assessment Step						
Asset accounting	<ul style="list-style-type: none"> • Asset accounting procedures • Physical inventory reports • Depreciation reports • List of SAP users with asset accounting access 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.						
<p><u>Agree</u> on the process capability level to be achieved by the process.</p> <p><i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i></p>								

¹² For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: *Enabling Processes*.

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment															
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment												
B-4	<p>Obtain understanding of each Organisational Structure in scope and set suitable assessment criteria: For each Organisational Structure in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the Organisational Structure.</p>														
Organisational Structure: Financial accounting															
B-4.1a	<p><u>Understand the Organisational Structure context.</u> <i>Identify and document all elements that can help to understand the context in which the Financial accounting organization has to operate, including:</i></p> <ul style="list-style-type: none"> • The overall organisation • Management/process framework • History of the role/structure • Contribution of the Organisational Structure to achievement of goals 														
B-4.2a	<p><u>Understand all stakeholders of the Organisational Structure/function.</u> Determine through documentation review (policies, management communications, etc.) the key stakeholders of the Financial accounting organization.</p> <ul style="list-style-type: none"> • Incumbent of the role and/or members of the Organisational Structure • Other key stakeholders affected by the decisions of the Organisational Structure/role 														
B-4.3a	<p><u>Understand the goals of the Organisational Structure</u>, the related metrics and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals.</p> <table border="1"> <thead> <tr> <th>Organisational Structure Goal</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Determine through interviews with key stakeholders and documentation review the goals of the Financial accounting organization, i.e., the decisions for which they are accountable^{13,14}.</td> <td> <p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> - They have contributed to the achievement of the IT-related and enterprise goals as anticipated. - Decisions are duly executed on a timely basis. </td></tr> </tbody> </table>	Organisational Structure Goal	Assessment Step	Determine through interviews with key stakeholders and documentation review the goals of the Financial accounting organization, i.e., the decisions for which they are accountable ^{13,14} .	<p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> - They have contributed to the achievement of the IT-related and enterprise goals as anticipated. - Decisions are duly executed on a timely basis. 										
Organisational Structure Goal	Assessment Step														
Determine through interviews with key stakeholders and documentation review the goals of the Financial accounting organization, i.e., the decisions for which they are accountable ^{13,14} .	<p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> - They have contributed to the achievement of the IT-related and enterprise goals as anticipated. - Decisions are duly executed on a timely basis. 														
B-4.4a	<p><u>Agree on the expected good practices for the Organisational Structure</u> against which it will be assessed. <u>Assess the Organisational Structure design</u>, i.e., assess the extent to which expected good practices are applied.</p> <table border="1"> <thead> <tr> <th>Good Practice</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Operating principles</td> <td> <ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. </td> <td> <ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. </td></tr> <tr> <td>Composition</td> <td>The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td> <td>Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td></tr> <tr> <td>Span of control</td> <td> <ul style="list-style-type: none"> • The span of control of the Organisational Structure is defined. • The span of control is adequate, i.e., the </td> <td> <ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. • Assess whether the span of control is </td></tr> </tbody> </table>	Good Practice	Criteria	Assessment Step	Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 	Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Span of control	<ul style="list-style-type: none"> • The span of control of the Organisational Structure is defined. • The span of control is adequate, i.e., the 	<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. • Assess whether the span of control is 		
Good Practice	Criteria	Assessment Step													
Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 													
Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.													
Span of control	<ul style="list-style-type: none"> • The span of control of the Organisational Structure is defined. • The span of control is adequate, i.e., the 	<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. • Assess whether the span of control is 													

¹³ The RACI charts in COBIT 5: Enabling Processes can be leveraged as a starting point for the expected goals of a role or Organisational Structure.

¹⁴ The Organisational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organisational Structure assuming the same responsibilities and accountability should be considered.

Audit/Accruals Program for SAP ERP Financial Accounting FI Module											
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Organisational Structures											
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment						
B-4.5a		<p>Organisational Structure has the right to make all decisions it should.</p> <ul style="list-style-type: none"> The span of control is in line with the overall enterprise governance arrangements. 	<p>adequate, i.e., the Organisational Structure has the right to make all decisions it should.</p> <ul style="list-style-type: none"> Verify and assess whether the span of control is in line with the overall enterprise governance arrangements. 								
	Level of authority/decision rights	<ul style="list-style-type: none"> Decision rights of the Organisational Structure are defined and documented. Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue). 	<ul style="list-style-type: none"> Verify that decision rights of the Organisational Structure are defined and documented. Verify whether decision rights of the Organisational Structure are complied with and respected. 								
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.								
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.								
<p><u>Understand the life cycle and agree on expected values.</u> Assess the extent to which the Organisational Structure life cycle is managed.</p> <table border="1"> <thead> <tr> <th>Life-Cycle Element</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Mandate</td> <td> <ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. </td> <td> <ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well-understood mandate. </td> </tr> <tr> <td>Monitoring</td> <td> <ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. </td> <td> <ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. </td> </tr> </tbody> </table>	Life-Cycle Element	Criteria	Assessment Step	Mandate	<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well-understood mandate. 	Monitoring	<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 		
Life-Cycle Element	Criteria	Assessment Step									
Mandate	<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well-understood mandate. 									
Monitoring	<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 									
B-4.1 to B-4.5	Repeat steps B-4.1 through B-4.5 for all remaining Organisational structures in scope.										
	Repeat the steps described above for the remaining Organisational structures:										
		<ul style="list-style-type: none"> Tax department General accounting Treasury 									

Audit/Accruals Program for SAP ERP Financial Accounting Module			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment
B-5	Obtain understanding of the Culture, Ethics and Behaviour in scope. Assess Culture, Ethics and Behaviour.		
Culture, Ethics and Behaviour: Risk and compliance aware culture			
B-5.1a	<u>Understand</u> the Culture, Ethics and Behaviour context. <ul style="list-style-type: none"> • <i>What the overall corporate Culture is like</i> • <i>Understand the interconnection with other enablers in scope:</i> <ul style="list-style-type: none"> - <i>Identify roles and structures that could be affected by the Culture.</i> - <i>Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.</i> 		
B-5.2a	<u>Understand</u> the major stakeholders of the Culture, Ethics and Behaviour: Risk and compliance aware culture <i>Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.</i>		
B-5.3a	<u>Understand</u> the goals for the Culture, Ethics and Behaviour , and the related metrics and agree on expected values. Assess whether the Culture, Ethics and Behaviour goals (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour. In the context of Risk and compliance aware culture , the following Culture, Ethics and Behaviour are desired:	Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. For a representative sample of individuals, perform the following assessment steps.	
Desired Behaviour (Culture, Ethics and Behaviour Goal)		Assessment Step	
The enterprise is aware of the compliance requirements it must abide.			
Employees understand their role in maintaining compliance.			
Identified risk are properly addressed.			
Controls are in place to ensure compliance with internal and external requirements.			
B-5.4a	<u>Understand</u> the life cycle stages of the Culture, Ethics and Behaviour , and agree on the relevant criteria. Assess to what extent the Culture, Ethics and Behaviour life cycle is managed. <i>(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)</i>		
B-5.5a	<u>Understand</u> good practice when dealing with Culture, Ethics and Behaviour , and agree on relevant criteria. Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied.		
Good Practice		Criteria	Assessment Step
Communication, enforcement and rules		Existence and quality of the communication	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.
Incentives and rewards		Existence and application of appropriate rewards and incentives	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.
Awareness		Awareness of desired Behaviours	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.

Audit/Assurance Program for SAP ERP Financial Accounting Module			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment
B-5.1 to B-5.5	<p>Repeat steps B-5.1 through B-5.5 for all remaining Culture, Ethics and Behaviour in scope.</p> <p>Repeat the steps described above for the remaining Culture, Ethics and Behaviour:</p> <ul style="list-style-type: none"> • Enabling of continuous improvement • Accountability • Discipline to follow instructions 		

Audit/Accuracy Program for SAP ERP Financial Accounting Module																																																							
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																																																							
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment																																																				
B-6	Obtain understanding of the Information Items in scope. Assess Information Items.																																																						
Information Item: Data integrity procedures																																																							
B-6.1a	<u>Understand the Information item context:</u> <ul style="list-style-type: none"> • Where and when is it used? • For what purpose is it used? • Understand the connection with other enablers in scope, e.g.: <ul style="list-style-type: none"> - Used by which processes? - Which Organisational Structures are involved? - Which services/applications are involved? 																																																						
B-6.2a	<u>Understand the major stakeholders of the Information item.</u> <i>Understand the stakeholders for the Information item, i.e., identify the:</i> <ul style="list-style-type: none"> • Information producer • Information custodian • Information consumer <p><i>Stakeholders should be at the appropriate organisational level.</i></p>																																																						
B-6.3a	<u>Understand the major quality criteria for the Information item, the related metrics and agree on expected values.</u> <u>Assess whether the Information item quality criteria (outcomes) are achieved, i.e., assess the effectiveness of the Information item.</u> <p>Leverage the COBIT 5 Information enabler model¹⁵ focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand.</p> <p>Mark the quality dimensions with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Quality Dimension</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Accuracy</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Objectivity</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Believability</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Reputation</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Relevancy</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Completeness</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Currency</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Amount of information</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Concise representation</td> <td>✓</td> <td></td> <td></td> </tr> <tr> <td>Consistent representation</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Interpretability</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Understandability</td> <td>✓</td> <td></td> <td></td> </tr> </tbody> </table>	Quality Dimension	Key Criteria	Description	Assessment Step	Accuracy	✓			Objectivity				Believability				Reputation				Relevancy	✓			Completeness	✓			Currency	✓			Amount of information	✓			Concise representation	✓			Consistent representation				Interpretability				Understandability	✓				
Quality Dimension	Key Criteria	Description	Assessment Step																																																				
Accuracy	✓																																																						
Objectivity																																																							
Believability																																																							
Reputation																																																							
Relevancy	✓																																																						
Completeness	✓																																																						
Currency	✓																																																						
Amount of information	✓																																																						
Concise representation	✓																																																						
Consistent representation																																																							
Interpretability																																																							
Understandability	✓																																																						

¹⁵ COBIT 5 framework, appendix G, p.81-84

Audit/Accrual Program for SAP ERP Financial Accounting Module																															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																															
Information Items																															
Ref.	Assurance Steps and Guidance				Issue Cross-reference																										
	Manipulation																														
	Availability	✓																													
	Restricted access	✓																													
B-6.4a	<p><u>Understand</u> the life cycle stages of the Information item, and agree on the relevant criteria. <u>Assess</u> to what extent the Information item life cycle is managed.</p> <p>The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.</p> <ul style="list-style-type: none"> When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently. When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. <p>Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Life Cycle Stage</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Plan</td><td>✓</td><td></td><td></td></tr> <tr> <td>Design</td><td>✓</td><td></td><td></td></tr> <tr> <td>Build/acquire</td><td>✓</td><td></td><td></td></tr> <tr> <td>Use/operate</td><td>✓</td><td></td><td></td></tr> <tr> <td>Evaluate/monitor</td><td>✓</td><td></td><td></td></tr> <tr> <td>Update/dispose</td><td>✓</td><td></td><td></td></tr> </tbody> </table>	Life Cycle Stage	Key Criteria	Description	Assessment Step	Plan	✓			Design	✓			Build/acquire	✓			Use/operate	✓			Evaluate/monitor	✓			Update/dispose	✓				
Life Cycle Stage	Key Criteria	Description	Assessment Step																												
Plan	✓																														
Design	✓																														
Build/acquire	✓																														
Use/operate	✓																														
Evaluate/monitor	✓																														
Update/dispose	✓																														
B-6.5a	<p><u>Understand</u> important attributes of the Information item and expected values. <u>Assess</u> the Information item design, i.e., assess the extent to which expected good practices are applied.</p> <p>Good practices for Information items are defined as a series of attributes for the Information item¹⁶. The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.</p> <p>Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Attribute</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Physical</td><td></td><td></td><td></td></tr> <tr> <td>Empirical</td><td></td><td></td><td></td></tr> <tr> <td>Syntactic</td><td></td><td></td><td></td></tr> <tr> <td>Semantic</td><td></td><td></td><td></td></tr> <tr> <td>Pragmatic</td><td>✓</td><td></td><td></td></tr> <tr> <td>Social</td><td></td><td></td><td></td></tr> </tbody> </table>	Attribute	Key Criteria	Description	Assessment Step	Physical				Empirical				Syntactic				Semantic				Pragmatic	✓			Social					
Attribute	Key Criteria	Description	Assessment Step																												
Physical																															
Empirical																															
Syntactic																															
Semantic																															
Pragmatic	✓																														
Social																															
B-6.1 to B-6.5	Repeat steps B-6.1 through B-6.5 for all remaining Information items in scope.																														
	<p>Repeat the steps described above for the remaining Information items:</p> <ul style="list-style-type: none"> Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis Retention requirements 																														

¹⁶ COBIT 5 framework, appendix G, p. 81-84

Audit/Assurance Program for SAP ERP Financial Accounting Module			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Information Items			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
	<ul style="list-style-type: none">• Record of transactions• Training manuals• Job aids		

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Services, Infrastructures and Applications				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-7	Obtain understanding of the Services, Infrastructure and Applications in scope. Assess Services, Infrastructure and Applications.			
Services, Infrastructure and Applications: SAP ERP System				
B-7.1a	<u>Understand the Services, Infrastructure and Applications</u> context. <i>Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.</i>			
B-7.2a	<u>Understand the major stakeholders</u> of the Services, Infrastructure and Applications . <i>Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.</i>			
B-7.3a	<u>Understand the major goals</u> for the Services, Infrastructure and Applications , the related metrics and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.			
Goal				
Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 		
Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 		
Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.		
B-7.4a	Understand good practice related to the Services, Infrastructure and Applications and expected values. Assess the Services, Infrastructure and Applications design, i.e., assess to what extent expected good practices are applied. Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework ¹⁷ to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented: <ul style="list-style-type: none"> Buy/build decision needs to be taken. Use of the Service needs to be clear. 			
Good Practice				
Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business 		

¹⁷ COBIT 5 framework, appendix G, p.85-86

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Services, Infrastructure and Applications					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	
				Comment	
			<p>case.</p> <ul style="list-style-type: none"> • Verify that the sourcing decision has been duly executed. 		
	Use	The use of the Service needs to be clear: <ul style="list-style-type: none"> • When it needs to be used and by whom • The required compliance levels with the Service's output 	<ul style="list-style-type: none"> • Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used. • Verify that actual use is in line with requirement above. • Verify that the actual Service output is adequately used. • Verify that Service levels are monitored and achieved. 		
B-7.1 to B-7.4	Repeat steps B-7.1 through B-7.4 for all remaining Services, Infrastructure and Applications in scope.				
	Repeat the steps described above for the remaining Services, Infrastructure and Applications: <ul style="list-style-type: none"> • Master data maintenance • Change management • SAP training 				

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module																			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																			
People, Skills and Competencies																			
Ref.	Assurance Steps and Guidance		Issue Cross-reference																
B-8	Obtain understanding of the People, Skills and Competencies in scope. Assess People, Skills and Competencies.																		
People, Skill and Competency: Proficiency using the SAP Financial Accounting Module																			
B-8.1a	<u>Understand the People, Skills and Competencies</u> context. <i>Understand the context of the Skill/Competency, i.e.:</i> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> – <i>In which roles and structures is the Skill/Competency used? (See also B-4.1.)</i> <i>Which behaviours are associated with the Skill/Competency?</i>																		
B-8.2a	<u>Understand the major stakeholders</u> for the People, Skills and Competencies. <i>Identify to whom in the organisation the skill requirement applies.</i>																		
B-8.3a	<u>Understand the major goals</u> for the People, Skills and Competencies , the related metrics and agree on expected values. <i>Assess whether the People, Skills and Competencies goals (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.</i> For the People, Skills and Competencies: Proficiency using the SAP Financial Accounting Module , the following goals and associated criteria can be addressed. <table border="1" data-bbox="242 791 1108 1003"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr><td>Experience</td><td></td><td rowspan="8">Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.</td></tr> <tr><td>Education</td><td></td></tr> <tr><td>Qualification</td><td></td></tr> <tr><td>Knowledge</td><td></td></tr> <tr><td>Technical skills</td><td></td></tr> <tr><td>Behavioural skills</td><td></td></tr> </tbody> </table>		Goal	Criteria	Assessment Step	Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	Education		Qualification		Knowledge		Technical skills		Behavioural skills		
Goal	Criteria	Assessment Step																	
Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.																	
Education																			
Qualification																			
Knowledge																			
Technical skills																			
Behavioural skills																			
B-8.4a	<u>Understand the life cycle</u> stages of the People, Skills and Competencies , and agree the relevant criteria. <i>Assess to what extent the People, Skills and Competencies life cycle is managed.</i>																		
	For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07. <table border="1" data-bbox="242 1101 1108 1486"> <thead> <tr> <th>Life Cycle Element</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr><td>Plan</td><td>Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.</td><td>Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.</td></tr> <tr><td>Design</td><td> Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill. </td><td> Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill. </td></tr> </tbody> </table>		Life Cycle Element	Criteria	Assessment Step	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.								
Life Cycle Element	Criteria	Assessment Step																	
Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.																	
Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.																	

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment								
People, Skills and Competencies								
Ref.	Assurance Steps and Guidance				Issue Cross-reference			
	Build	Practice APO07.03 activity 4 (Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 4 is implemented in relation to this skill.					
B-8.5a	Operate	Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.					
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.					
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.					
	<u>Understand good practice related to the People, Skills and Competencies and expected values.</u> Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.							
Good Practice		Criteria	Assessment Step					
Skill set and Competencies are defined.		<ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 						
Skill levels are defined.		<ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. Assess the process for 360-degree performance evaluations. 						
Repeat steps B-8.1 through B-8.5 for all remaining People, Skills and Competencies in scope.								
Repeat the steps described above for the remaining People, Skills and Competencies:								
<ul style="list-style-type: none"> Master data management skills Financial accounting skills and experience 								

Audit/Assurance Program for SAP ERP Financial Accounting FI Module			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
People, Skills and Competencies			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
	<ul style="list-style-type: none">• Proficiency running SAP reports• Understanding of data classification policies• Understanding of data integrity procedures		

Audit/Accuracy Program for SAP ERP Financial Accounting FI Module		
Phase C—Communicate the Results of the Assessment		
Ref.	Assurance Step	Guidance
C-1	Document exceptions and gaps.	
C-1.1	Understand and document weaknesses and their impact on the achievement of process goals.	<ul style="list-style-type: none"> Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	<ul style="list-style-type: none"> Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. Point out the consequence of noncompliance with regulatory requirements and contractual agreements. Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
C-2	Communicate the work performed and findings.	
C-2.1	Communicate the work performed.	<ul style="list-style-type: none"> Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	<ul style="list-style-type: none"> Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. Use benchmarking and survey results to compare the enterprise's performance with others. Use extensive graphics to illustrate the issues. Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	

Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
1. General Ledger							
1.1 Changes made to master data are valid, complete, accurate and timely.							
1.1.1 Are reports of changes to master data compared to authorized source documents and/or a manual log of requested changes to ensure they were input accurately and on a timely basis?					DSS01 DSS06		
1.1.2 Does the enterprise review policy and process design specifications regarding access to maintain master data?					APO01 DSS05		
1.1.3 Do the configurable control settings address the risk pertaining to the validity, completeness and accuracy of master data and ensure that they have been set in accordance with management intentions?					DSS06		
1.2 Master data remain current and pertinent.							
1.2.1 Does the appropriate management report display or produce a list of master data records and confirm evidence of management's review of the master data on a rotating basis?					DSS06		
1.3 GL postings are valid, complete, accurate and timely							
1.3.1 Is the ability to record and change GL postings restricted to authorized personnel?					DSS05		
1.3.2 Is the field status (as H, D, R and O) maintained at line item level for a GL document before posting the document?					BAI10 DSS06		

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
1.3.3 Are Document Type and Posting Keys configured to control the header and line item values to maintain consistency and integrity while posting documents?					BAI10 DSS06
1.3.4 Are GL postings periodically reconciled with the subledgers to ensure the accuracy of the ledger documents?					DSS01 DSS06
1.3.5 Are the entries reviewed prior to posting in the system?					DSS01 DSS06
1.3.6 Is the ability to update exchange rates restricted to authorized personnel?					DSS05
1.3.7 Is the table TCURR (exchange rates) set to log all changes and are changes reviewed periodically?					DSS01 DSS06
1.3.8 Has management approved values in the centrally maintained exchange rate table?					DSS05
1.4 All transactions and events that should be recorded are recorded in the correct accounting period.					
1.4.1 Are Fiscal Year Variant and Posting Period Variant configured to prevent the posting of documents in the wrong fiscal year or posting period?					BAI10 DSS06
1.4.2 Is table T001B (open-period configuration) set to log all changes and are these changes reviewed periodically?					DSS01 DSS06

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
1.4.3 Is the ability to modify the open period configuration table restricted to authorized personnel?					DSS05 DSS06
1.4.4 Is any special authorization given to a limited set of users through authorization groups, so they can open or close posting periods in case of any special scenario in business where additional periods need to be kept open for certain period of time until the data are migrated to new ledgers?					DSS05 DSS06
1.4.5 Does the enterprise have a dedicated team/person responsible for periodic reviews to validate the accuracy in posted data to the correct period and ledger?					DSS01 DSS06
1.5 Changes in business and accounting principles do not affect the general ledger (GL).					
1.5.1 Are proposed changes to the enterprise internal cost accounting system, government tax law changes, etc., analyzed to determine any impact on the business?					APO12 DSS06 MEA03
1.5.2 Does management require multiple accounting principles for business?					BAI10 DSS06
2. Bank Accounting					
2.1 Formats of interchange of structure data used by the bank and the enterprise's lockbox are compatible.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.1.1 Are Information Interconnection Agreements established between the enterprise and the connecting bank to decide upon the common set of protocols and formats used for information interchange?					DSS01 DSS05
2.2 Data file (BAI/BAI2) with payment information from the connecting banks is promptly received.					
2.2.1 Are notifications and alerts sent to designated teams when data from the bank are not received as expected?					DSS01 DSS06
2.2.2 Is the log of data receipts from the bank reviewed to validate the timeliness and correct format of the data received?					DSS01 DSS06
2.3 Open invoices are cleared on time.					
2.3.1 Is the background process configured to run the lockbox processing based on a fixed schedule?					BAI10
2.3.2 Is the output/log of the lockbox program reviewed by the relevant management after each time it is executed?					DSS01 DSS06
2.4 Duplicate payment files are not received from banks.					
2.4.1 Is the duplicate file validation program configured as a background process to check parameters for detecting delicacy?					DSS06
2.5 Lockbox matches the check amount with the total invoices listed.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.5.1 Are data received by lockbox from the bank and the payment information by the customer compared at the bank to check for accuracy?					DSS01 DSS06
2.5.2 Is the maximum number of parameters for a single payment that is transmitted by the bank and received by lockbox based on the Information Interconnection Agreement?					DSS01 DSS06
2.5.3 Is the payment advice of the unmatched payment information retained as a flag for manual review?					DSS01 DSS06
2.5.4 Are personnel assigned to review the status of the items, and manually correct the unapplied item?					DSS01 DSS06
2.6 Manual linkage of payment with open invoices is accurate, valid or timely.					
2.6.1 Is the ability to link the payment from the bank with open invoices restricted to authorized personnel?					DSS05
2.6.2 Is segregation of duties enforced to ensure that Responsibility and Accountability are segregated among the designated teams?					DSS05
2.6.3 Are closed invoices and payment information from the bank periodically reviewed to check for accuracy and appropriateness?					DSS01 DSS06

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.6.4 Is the aging report reviewed periodically to check for any open unpaid invoice for which the payment is not linked?					DSS01 DSS06
2.7 Invoices are not left unpaid for a considerable time.					
2.7.1 Is the AR aging report (transaction code S_ALR_87012168) used to detect any invoices that have been left open for an extended time period?					DSS01 DSS06
3. Asset Accounting					
3.1 Asset transactions (acquisitions, transfers and retirements) are valid, complete, accurate and timely.					
3.1.1 Is the ability to record and change Asset Transactions, including changes to the chart of depreciation restricted to authorized personnel?					DSS05 DSS06
3.1.2 Is period control configured to determine the posting dates of business transactions based on predefined rules to calculate accurate depreciation?					DSS06
3.1.3 Is the automated account determination process configured to identify the associated GL account based on the asset class (e.g., building, machine, goodwill) and transaction type (e.g., acquisition, accumulated depreciation, gain/loss on sale)?					DSS01 DSS06
3.2 Physical assets are completely and/or accurately recorded in the system.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.2.1 Is the Directory of Unposted Assets periodically reviewed and are appropriate actions taken in case of variance?					DSS01 DSS06
3.3 Depreciation is applied accurately on the assets.					
3.3.1 Is the chart of depreciation, which contains depreciation areas for company codes, configured to assist in the accurate calculation of depreciation and posting to the respective accounts on the GL within appropriate accounting periods?					DSS01 DSS06

SAP ERP

Managerial Accounting CO Module
Audit/Assurance Program



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP ERP Managerial Accounting CO Module Audit/Accurance Program* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP's kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: <http://www.isaca.org/sap-erp-4th-edition>
Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center
Follow ISACA on Twitter: <https://twitter.com/ISACANews>
Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOOfficial>
Like ISACA on Facebook: www.facebook.com/ISACAHQ

Acknowledgements

ISACA wishes to recognize

Project Leaders

Benjamin Fitts, CPA, Deloitte & Touche LLP, USA
Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA
Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA
Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Eva Sweet, CISA, CISM, ISACA, USA

Researchers

Syed Aamir Aarfi, Deloitte & Touche LLP, USA
Carlos Amaya, CISA, Deloitte & Touche LLP, USA
Dan Argynov, PMP, Deloitte & Touche LLP, USA
Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA
David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA
Ramamallikarjunaraao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA
Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA
Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA
Sagnik Mukherjee, Deloitte & Touche LLP, USA
Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA
Sonik Shah, Deloitte & Touche LLP, USA
Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA
Shweta Srivastava, Deloitte & Touche LLP, USA
Anurag Tewary, Deloitte & Touche LLP, USA
Percy Tsai, CPA, Deloitte & Touche LLP, USA
Ravi Maddela Veeriah, Deloitte & Touche LLP, USA
Sravan Vemana, Deloitte & Touche LLP, USA
Anukool Vyas, Deloitte & Touche LLP, USA

Expert Reviewers

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA
Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada
Mayank Garg, CISA, NetApp, USA
Ricci Leong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Jim Koveos, CISA, MBA, AmerisourceBergen, USA
Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia
Samuel Lim S.C., CISA, Auditor General's Office, Singapore
Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia
Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General's Office, Singapore
Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia
Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia
Paul O'Donnell, Ernst & Young, Canada
Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico
John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US
Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico
Naved Rehman, CISA, CRISC, MS-IS, SAPAuditCoach, US
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US
Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico
Jovari St. Victor, CISA, CPA, Sunera, LLC, US
Surapong Surabotsopon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,
KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico
Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand
David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President
Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cythus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK
Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil
Jotham Nyamari, CISA, Deloitte, USA
James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK
Gurvinder Singh, CISA, CISM, CRISC, Australia
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore
Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

SAP ERP Managerial Accounting CO Module Audit/Assurance Program

Introduction

This document contains an example audit/assurance program, **based on** the generic structure developed in section 2B of *COBIT 5 for Assurance*¹.

The engagement approach is based on, but **differs slightly** from the generic approach described in *COBIT 5 for Assurance*:

- The engagement approach described in this audit/assurance program is **focused on a business process** consequently no group of COBIT 5 processes dominates as primary processes and the lower-level processes are widespread, for evaluation purposes, the high-level COBIT 5 processes will be used as references.
- The assurance steps in this audit/assurance program are specific to the subject matter under review; therefore most of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources availableprocess audit/assurance program.

Assurance Engagement: SAP ERP Managerial Accounting CO Module

Assurance Topic

The topic covered by this assurance engagement is the SAP ERP Managerial Accounting CO Module.

Business Impact and Risk

SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical processes.

Risk resulting from ineffective or incorrect configurations or use of SAP could result in some of the following:

Disclosure of privileged information

- Single points of failure
- Low data quality
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements

Goal of the Review

The objective of the SAP ERP audit/assurance review is to provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise's SAP ERP architecture.

Scoping

The review will focus on configuration of the relevant SAP ERP components and modules within the enterprise. The selection of the specific components and modules will be based upon the risk introduced to the enterprise by these components and modules.

From a process reference model (PRM) perspective, the following enabling processes apply to this audit and assurance programme:

- BAI02 Manage requirements definition
- BAI03 Manage solution identification and build

¹ See www.isaca.org/COBIT/Pages/Assurance-product-page.aspx for more information on *COBIT 5 for Assurance*.

- DSS01 Manage operations
- DSS05 Manage security services
- DSS06 Manage business process controls

Testing SAP Security

To determine which users have access to the relevant authorizations used in this audit program, use one of the following methods:

1. Use transaction code SUIM → Users → Users by Complex Selection Criteria
2. Use transaction code S_BCE_68001417
3. Use transaction code SA38 and the program RSUSR002. This method allows the user to specify a transaction code, a “valid to” date for users, and up to three other authorization objects (which also may be the authorization object for transaction code S_TCODE) with associated values (two values under an AND relationship and three values under an OR relationship).
This method is generally sufficient for testing logical access security in relation to SAP ERP application infrastructure areas, but it is less suitable when large numbers of authorizations must be reviewed, such as in segregation of duties analysis and in some of the more complex areas of business cycle controls.
4. Use transaction code SUIM → Users → Users with Critical Authorizations (also accessible with program RSUSR008_009_NEW, which replaces programs RSUSR008 and RSUSR009 and transaction codes SU98 and/or SU99, for SAP Web AS 6.20 and later). This method offers improvements such as allowing differentiation between SAP defaults for critical data for different business areas, extended combination options for critical authorization data, improved performance, display of user filters and more analysis options for users in the result list.

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
A-1	Determine the stakeholders of the assurance initiative and their stakes .				
A-1.1	<u>Identify</u> the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	Intended user(s) of the assurance report	<p>Board/audit committee: Needs assurance over the effectiveness and efficiency of SAP ERP processes within the enterprise.</p> <p>Chief financial officer (CFO): Needs assurance that internal controls for financial applications work as intended.</p> <p>Risk managers: Need assurance that controls intended to address previously identified risk are working as intended. The results from the audit should be used to update the risk registry as needed.</p> <p>Security managers: Need to identify gaps in the security plans for SAP applications.</p> <p>Owners / shareholders: Part or all of the SAP ERP assurance report may be included in statutory reporting.</p> <p>Regulators: Part or all of SAP ERP reporting may need to be disclosed to respective authorities</p>		
A-1.2	Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	Accountable and responsible parties for the subject matter	<p>Business executives: The individuals responsible for identifying requirements, approving design and managing performance. These people are, together with IT management, responsible for managing the correct and controlled use of SAP ERP services—in line with good practices.</p> <p>Business process owners: Responsible for defining application and technical requirements. Responsible for data classification.</p> <p>IT management: Responsible for managing the correct and controlled use of SAP ERP services—together with the business executives.</p>		
A-2	<u>Determine</u> the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities (i.e., not achieving the enterprise goals).	<p>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.</p> <p>Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.</p> <p>Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</p> <p>Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.</p>			
A-2.1	<u>Understand</u> the enterprise strategy and priorities.	<p><i>Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.</i></p>			

Audit/Assurance Program for SAP ERP Managerial Accounting CO Module				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
A-2.2	<u>Understand</u> the internal context of the enterprise.	<p><i>Identify all internal environmental factors that could influence the performance and contents of the SAP ERP Managerial Accounting CO Module.</i></p> <ul style="list-style-type: none"> • Review prior audit report, if one exists, verify completion of any agreed-on corrections and note remaining deficiencies. Determine whether: <ul style="list-style-type: none"> - Senior management has assigned responsibilities for information, its processing and its use - User management is responsible for providing information that supports the entity's objectives and policies - Information systems management is responsible for providing the capabilities necessary for the achievement of the defined information systems objectives and the policies of the entity - Senior management approves plans for development and acquisition of information systems - There are procedures to ensure that the information system being developed or acquired meets user requirements - There are procedures to ensure that information systems, programs and configuration changes are tested adequately prior to implementation - All personnel involved in the system acquisition and configuration activities receive adequate training and supervision - There are procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards - User management participates in the conversion of data from the existing system to the new system - Final approval is obtained from user management prior to going live with a new information/upgraded system - There are procedures to document and schedule all changes to information systems (including key ABAP programs) - There are procedures to ensure that only authorized changes are initiated - There are procedures to ensure that only authorized, tested and documented changes to information systems are accepted into the production client - There are procedures to allow for and control emergency changes - There are procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software - There is a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated - The organizational structure, established by senior management, provides for an appropriate segregation of incompatible functions - The database, application and presentation servers are located in a physically separate and protected environment (i.e., a data center) - Emergency, backup and recovery plans are documented and tested on a regular basis to ensure that they remain current and operational - Backup and recovery plans allow users of information systems to resume operations in the event of an interruption - Application controls are designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system - Access to the Implementation Guide (IMG) during production has been restricted - The production client settings have been flagged to not allow changes to programs and 		

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
		<p>configuration</p> <ul style="list-style-type: none"> • Identify the significant risk and determine the key controls <ul style="list-style-type: none"> – Develop a high-level process flow diagram and overall understanding of the Managerial Accounting CO module, including the following subprocesses: <ul style="list-style-type: none"> a. Master data maintenance b. Cost element/cost center accounting/internal orders c. Profit center accounting d. COPA/product costing/activity-based costing – Assess the key risk, determine key controls or control weaknesses, and test controls (refer to the sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> a. The controls culture of the organization (e.g., a just-enough-control philosophy). b. The need to exercise judgment to determine the key controls in the process and whether the controls structure is adequate. (Any weaknesses in the control structure should be reported to executive management and resolved.) • Gain an understanding of the SAP ERP environment (The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles) <p>In particular, the following information is important:</p> <ul style="list-style-type: none"> – Version and release of SAP ERP implemented – Total number of named users (for comparison with logical access security testing results) – Number of SAP instances and clients – Accounting period, company codes and chart of accounts – Identification of the components being used (Human Capital Management, Financials, Operations, Corporate Services) – Whether the organization has created any locally developed ABAP programs or reports – Details of the risk assessment approach taken in the organization to identify and prioritize risk – Copies of the organization's key security policies and standards <p>Obtain details of the following:</p> <ul style="list-style-type: none"> – Organizational Management Model as it relates to sales/revenue activity, i.e., sales organizational unit structure in SAP ERP and company sales organizational chart (required when evaluating the results of access security control testing) – An interview of the systems implementation team, if possible, and process design documentation for sales and distribution 			
A-2.3	Understand the external context of the enterprise.	<i>Identify all external environmental factors that could influence the performance and contents of the SAP ERP Managerial Accounting CO Module.</i>			
A-2.4	Given the overall assurance objective, translate the identified strategic priorities into concrete <u>objectives</u> for the assurance engagement.	The following goals are retained as key goals to be supported, in reflection of enterprise strategy and priorities:			
		Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with external laws and regulations 		

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step		Guidance	Issue Cross-reference	Comment
			<ul style="list-style-type: none"> • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality • EG15 Compliance with internal policies <p>IT-related goals:</p> <ul style="list-style-type: none"> • ITG01 Alignment of IT and business strategy • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG09 IT Agility • ITG10 Security of information, processing infrastructure and applications • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG15 IT compliance with internal policies • ITG16 Competent and motivated business and IT personnel 		
		Additional goals			
A-2.5	<u>Define</u> the organizational boundaries of the assurance initiative.		<p><i>Describe the organizational boundaries of the assurance engagement, i.e., to which organizational entities the review is limited. All other aspects of scope limitation are identified during phase A-3.</i></p> <ul style="list-style-type: none"> • The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment. • Obtain information and form an understanding of the business reasons underlying the audit • Identify the senior business resources responsible for the review. • Identify the senior IT audit/assurance resource responsible for the review. • Establish the process for suggesting and implementing changes to the audit/assurance program, and list the authorizations required. • Identify any limitations and/or constraints affecting the audit of specific systems and subsystems. • Identify any third-party services, applications, platforms and infrastructure elements that may not be or only partially be accessible. • Identify any legal, regulatory or contractual constraints on audit. • Identify any industrial relations-based or end user-based audit constraints. 		

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
A-3	Determine the enablers in scope and the instance(s) of the enablers in scope.	COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.						
A-3.1	<u>Define the Principles, Policies and Frameworks</u> in scope.	<p>Guiding principles and policies include:</p> <ul style="list-style-type: none"> • Policy for Master Data Maintenance • Information security management system (ISMS) policy • Legal and regulatory compliance requirements 						
A-3.2	<p><u>Define which Processes</u> are in scope of the review.</p> <p>Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of process goals • Application of process good practices • Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments) 	<p><i>COBIT 5: Enabling Processes</i> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed.</p> <table border="1"> <tr> <td>Key processes</td><td> <ul style="list-style-type: none"> • Cost and revenue element accounting • Cost center accounting • Activity-based costing • Internal orders • Product cost controlling • Profitability analysis • Profit center accounting </td></tr> <tr> <td>Additional processes</td><td> <ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls </td></tr> </table>	Key processes	<ul style="list-style-type: none"> • Cost and revenue element accounting • Cost center accounting • Activity-based costing • Internal orders • Product cost controlling • Profitability analysis • Profit center accounting 	Additional processes	<ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls 		
Key processes	<ul style="list-style-type: none"> • Cost and revenue element accounting • Cost center accounting • Activity-based costing • Internal orders • Product cost controlling • Profitability analysis • Profit center accounting 							
Additional processes	<ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls 							
A-3.3	<p><u>Define which Organisational Structures</u> will be in scope.</p> <p>Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of Organisational Structure goals, i.e., decisions • Application of Organisational Structures good practices 	<p>Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail.</p> <table border="1"> <tr> <td>Key Organisational Structures</td><td> <ul style="list-style-type: none"> • Cost/Manufacturing Accounting Group • Material Pricing • Corporate Controlling </td></tr> <tr> <td>Additional Organisational Structures</td><td> <ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office • Human resources • Manufacturing </td></tr> </table>	Key Organisational Structures	<ul style="list-style-type: none"> • Cost/Manufacturing Accounting Group • Material Pricing • Corporate Controlling 	Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office • Human resources • Manufacturing 		
Key Organisational Structures	<ul style="list-style-type: none"> • Cost/Manufacturing Accounting Group • Material Pricing • Corporate Controlling 							
Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • Master data maintenance group • SAP ERP support and maintenance • SAP training • Change Management Office • Human resources • Manufacturing 							

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
A-3.4	<u>Define the Culture, Ethics and Behaviour</u> aspects in scope.	<p>In the context of this engagement, the following enterprise-wide culture and behaviours are in scope:</p> <ul style="list-style-type: none"> • Risk- and compliance-aware culture • Enabling of continuous improvement • Accountability • Discipline to follow instructions 						
A-3.5	<u>Define the Information items</u> in scope. Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of Information goals, i.e., quality criteria of the information items • Application of Information good practices (Information attributes) 	<p>Based on the subject matter of this audit/assurance program, the following Information items have been identified as key items.</p> <table border="1"> <tr> <td>Key Information Items</td><td> <ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids </td></tr> <tr> <td>Additional Information Items</td><td> <ul style="list-style-type: none"> • Organizational charts </td></tr> </table>	Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 	Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 		
Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 							
Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 							
A-3.6	<u>Define the Services, Infrastructure and Applications</u> in scope.	<p>In the context of this assignment, and taking into account the goals identified in A-2.4, the following services and related applications or infrastructure could be considered in scope of the review:</p> <ul style="list-style-type: none"> • Master data maintenance group • SAP ERP System • SAP training • Change management 						
A-3.7	<u>Define the People, Skills and Competencies</u> in scope. Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of skills set goals • Application of skills set and competencies good practices 	<p>In the context of this engagement, taking into account key processes and key roles, the following skill sets are included in scope:</p> <ul style="list-style-type: none"> • Proficiency using the SAP Controlling Module • Master data management skills • Controlling module skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 						

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module																											
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference																							
B-1	Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.																										
B-1.1	<p>Obtain (and agree on) metrics for enterprise goals and expected values of the metrics. Assess whether enterprise goals in scope are achieved.</p> <p>Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.</p> <p>Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</p> <p>The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>Enterprise Goal</th> <th>Metric</th> <th>Expected Outcome</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>EG03 Managed business risk (safeguarding of assets)</td> <td> <ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG04 Compliance with externals laws and regulations</td> <td> <ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG07 Business service continuity and availability</td> <td> <ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG11 Optimisation of business process functionality</td> <td> <ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG15 Compliance with internal policies</td> <td> <ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>	Enterprise Goal	Metric	Expected Outcome	Assessment Step	EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG04 Compliance with externals laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Enterprise Goal	Metric	Expected Outcome	Assessment Step																								
EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG04 Compliance with externals laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
B-1.2	<p>Obtain (and agree on) metrics for IT-related goals and expected values of the metrics and assess whether IT-related goals in scope are achieved.</p> <p>The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>IT-related Goal</th> <th>Metric</th> <th>Expected Outcome</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>ITG01 Alignment of IT and business strategy</td> <td> <ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services </td> <td>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>	IT-related Goal	Metric	Expected Outcome	Assessment Step	ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																		
IT-related Goal	Metric	Expected Outcome	Assessment Step																								
ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> Percent of IT value drivers mapped to business value drivers 		criteria are achieved.	
	ITG02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment Number of non-compliance issues relating to contractual agreements with IT service providers Coverage of compliance assessments 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG04 Managed IT-related business risk	<ul style="list-style-type: none"> Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent of enterprise risk assessments including IT-related risk Frequency of update of risk profile 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG08 Adequate use of applications, information and technology solutions	<ul style="list-style-type: none"> Percent of business process owners satisfied with supporting IT products and services Level of business user understanding of how technology solutions support their processes Satisfaction level of business users with training and user manuals Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG09 IT Agility	<ul style="list-style-type: none"> Level of satisfaction of business executives with IT's responsiveness to new requirements Number of critical business processes supported by up-to-date infrastructure and applications Average time to turn strategic IT objectives into an agreed-on and approved initiative 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG10 Security of information, processing infrastructure and applications	<ul style="list-style-type: none"> Number of security incidents causing financial loss, business disruption or public embarrassment Number of IT services with outstanding security requirements Time to grant, change and remove access privileges, compared to agreed-on service levels 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	ITG12 Enablement and support of business processes by integrating applications and technology into business processes	<ul style="list-style-type: none"> Frequency of security assessment against latest standards and guidelines Number of business processing incidents caused by technology integration errors Number of business process changes that need to be delayed or reworked because of technology integration issues Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues Number of applications or critical infrastructures operating in silos and not integrated 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG14 Availability of reliable and useful information for decision making	<ul style="list-style-type: none"> Level of business user satisfaction with quality and timeliness (or availability) of management information Number of business process incidents caused by non-availability of information Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG15 IT compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices Frequency of policies review and update 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG16 Competent and motivated business and IT personnel	<ul style="list-style-type: none"> Percent of staff whose IT-related skills are sufficient for the competency required for their role Percent of staff satisfied with their IT-related roles Number of learning/training hours per staff member 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-2	Obtain an understanding of the Principles, Policies and Frameworks in scope and set suitable assessment criteria. Assess Principles, Policies and Frameworks.			
Principles, policies and frameworks: Policy for Master Data Maintenance				
B-2.1a	<u>Understand the Principles, Policies and Frameworks context.</u> <i>Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks</i>			
B-2.2a	<u>Understand the stakeholders of the Principles, Policies and Frameworks.</u> <i>Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.</i>			
B-2.3a	<u>Understand the goals for the Principles, Policies and Frameworks</u> , and the related metrics and agree on expected values. Assess whether the Principles, Policies and Frameworks goals (outcomes) are achieved, i.e., assess the effectiveness of the Principles, Policies and Frameworks . Goal: The organization has defined, disseminated and deployed management policies supporting SAP master data maintenance .			
Goal		Criteria	Assessment Step	
Comprehensiveness	The set of policies is comprehensive in its coverage.		Verify that the set of policies is comprehensive in its coverage.	
Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none">• A regular validation of all policies whether they are still up to date• An indication of the policies' expiration date or date of last update		Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none">• A regular validation of all policies whether they are still up to date• An indication of the policies' expiration date or date of last update	
Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.		Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.	
Availability	<ul style="list-style-type: none">• Policies are available to all stakeholders.• Policies are easy to navigate and have a logical and hierarchical structure.		<ul style="list-style-type: none">• Verify that policies are available to all stakeholders.• Verify that policies are easy to navigate and have a logical and hierarchical structure.	
B-2.4a	<u>Understand the life cycle stages of the Principles, Policies and Frameworks</u> , and agree on the relevant criteria. Assess to what extent the Principles, Policies and Frameworks life cycle is managed. <i>The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01 Manage the IT management framework.</i>			
B-2.5a	<u>Understand good practices related to the Principles, Policies and Frameworks</u> and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. <i>The assurance professional will, by using appropriate auditing techniques assess the following aspects.</i>			
Good Practice		Criteria	Assessment Step	
Scope and validity	The scope is described and the validity date is indicated.		Verify that the scope of the framework is described and the validity date is indicated.	
Exception and escalation	<ul style="list-style-type: none">• The exception and escalation procedure is explained and commonly known.• The exception and escalation procedure has not become the de facto standard procedure.		<ul style="list-style-type: none">• Verify that the exception and escalation procedure is described, explained and commonly known.• Through observation of a representative sample, verify that the exception and escalation procedure has not become <i>de facto</i> standard procedure.	
Compliance	The compliance checking mechanism and non-compliance consequences are clearly described and enforced.		Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.	

Audit/Assurance Program for SAP ERP Managerial Accounting CO Module			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-2.1 to B-2.5	<p>Repeat steps B-2.1 through B-2.5 for all remaining Principles, Policies and Frameworks in scope.</p> <p>Repeat the steps described above for the remaining Principles, Policies and Frameworks:</p> <ul style="list-style-type: none">• ISMS policy• Legal and regulatory compliance requirements		

Audit/Accurance Program for SAP ERP Managerial Accounting CO Module																		
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																		
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment															
B-3	Obtain understanding of the Processes in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes.																	
SAP ERP Controlling process²: Master data maintenance																		
B-3.1a	<u>Understand the Process context.</u>																	
B-3.2a	<u>Understand the Process purpose.</u>																	
B-3.3a	<p><u>Understand all process stakeholders</u> and their roles. This is equivalent to understanding the real RACI chart of the process. <i>Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.</i></p> <p>The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement:</p> <p>Master data maintenance stakeholders:</p>																	
B-3.4a	<p><u>Understand the Process goals</u> and related metrics³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.</p> <table border="1"> <tr> <td colspan="2">The Process Master data maintenance has two defined process goal.</td><td>The following activities can be performed to assess whether the goals are achieved.</td></tr> <tr> <th>Process Goal</th><th>Related Metrics</th><th>Criteria/Expected Value</th><th>Assessment Step</th></tr> <tr> <td>Changes made to master data are valid, complete, accurate and timely.</td><td>Determine the metrics that can be used to assess the achievement of the Process goals.</td><td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>Master data remains current and pertinent.</td><td>Determine the metrics that can be used to assess the achievement of the Process goals.</td><td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </table>	The Process Master data maintenance has two defined process goal.		The following activities can be performed to assess whether the goals are achieved.	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	Changes made to master data are valid, complete, accurate and timely.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	Master data remains current and pertinent.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
The Process Master data maintenance has two defined process goal.		The following activities can be performed to assess whether the goals are achieved.																
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step															
Changes made to master data are valid, complete, accurate and timely.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.															
Master data remains current and pertinent.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.															
B-3.5a	<p><u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement: <u>Define</u> and <u>agree</u> on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.)</p> <p><u>Agree</u> on the process practices that should be in place (process design). <u>Assess</u> the process design, i.e., assess to what extent:</p> <ul style="list-style-type: none"> • Expected process practices are applied. • Accountability and responsibility are assigned and assumed. <p>Evaluate Master data maintenance</p>																	

² Because this is a business process audit/assurance program, several of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources available.

³ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

Audit/Accurance Program for SAP ERP Managerial Accounting CO Module																				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																				
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment															
	<p>COBIT 5 Processes⁴ are described in <i>COBIT 5: Enabling Processes</i>. Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are:</p> <ul style="list-style-type: none"> • A sound process design <p>The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented.</p>																			
	Reference Process	Master data maintenance	Criteria: 1.1 Changes made to master data are valid, complete, accurate and timely. 1.2 Master data remains current and pertinent.																	
	Reference Process Practices ⁵	Good Practice	Assessment Step		Issue Cross-reference	Comment														
	BAI06 DSS01 DSS06	Changes made to master data are valid, complete, accurate and timely	1.1.1 On a sample basis, review standard reports and transactions against authorized source documents to assess the accuracy and timeliness of change maintenance applied to master data records. The following transaction codes along with the program names can be used to produce a list of the changes made to selected CO master records. Users should review a sample of master records to ensure that no audit logs can be modified. (Note: Programs can be executed directly using transaction code SA38—ABAP Reporting). <table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Description</th> <th>Program</th> </tr> </thead> <tbody> <tr> <td>KA05</td> <td>Cost Element Master Data Changes</td> <td>SAPMKMAA</td> </tr> <tr> <td>KS05</td> <td>Cost Center Master Data Changes</td> <td>SAPMKMAA</td> </tr> <tr> <td>6KEA</td> <td>Profit Center Master Data Changes</td> <td>SAPMKECA</td> </tr> <tr> <td>KL05</td> <td>Activity Type Master Data Changes</td> <td>SAPMKMAA</td> </tr> </tbody> </table> For internal orders, use transaction code KO03—Display Internal Orders and click on Environment → Changes (within changes, there is an option to view the changes for the entire order, field, or status).	Transaction (s)	Description	Program	KA05	Cost Element Master Data Changes	SAPMKMAA	KS05	Cost Center Master Data Changes	SAPMKMAA	6KEA	Profit Center Master Data Changes	SAPMKECA	KL05	Activity Type Master Data Changes	SAPMKMAA		
Transaction (s)	Description	Program																		
KA05	Cost Element Master Data Changes	SAPMKMAA																		
KS05	Cost Center Master Data Changes	SAPMKMAA																		
6KEA	Profit Center Master Data Changes	SAPMKECA																		
KL05	Activity Type Master Data Changes	SAPMKMAA																		
	DSS05	Changes made to master data are valid, complete, accurate and timely	1.1.2 Review enterprise policy and process design specifications regarding access to maintain master data. Proper enforcement of a segregation of duties strategy is needed to properly control master data maintenance. Use transaction code SUIM—User Information System to test user access to the following transaction codes to maintain master data. <table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>KA01—Create Cost Element</td> <td>K_CSKB</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>KA02—Change Cost Element</td> <td>K_CSKB</td> <td>ACTVT</td> <td>02</td> </tr> </tbody> </table>	Transaction (s)	Authorization Objects	Fields	Values	KA01—Create Cost Element	K_CSKB	ACTVT	01	KA02—Change Cost Element	K_CSKB	ACTVT	02					
Transaction (s)	Authorization Objects	Fields	Values																	
KA01—Create Cost Element	K_CSKB	ACTVT	01																	
KA02—Change Cost Element	K_CSKB	ACTVT	02																	

⁴ For this audit/assurance program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the SAP ERP Managerial Accounting CO Module processes in scope.

⁵ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Managerial Accounting CO Module audit/assurance program.

Audit/Accuracy Program for SAP ERP Managerial Accounting CO Module							
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes							
Ref.	Assurance Steps and Guidance					Issue Cross-reference	Comment
			KA04—Delete Cost Element	K_CSKB	ACTVT	06	
			KA06—Create Secondary Cost Element	K_CSKB	ACTVT	01	
			KE51—Create Profit Center	K_PCAR_REP K_PCAS_PRC	ACTVT	01	
			KE52—Change Profit Center	K_PCAR_REP K_PCAS_PRC	ACTVT	02	
			KE54—Delete Profit Centers	K_PCAR_REP K_PCAS_PRC	ACTVT	06	
			KO01—Create Internal Order	K_ORDER	CO_ACTION	0001	
			KO02—Change Internal Order	K_ORDER	CO_ACTION	0002	
			KO04—Order Manager	K_ORDER	CO_ACTION	0001, 0002, 0006	
			KS01—Create Cost Center	K_CSKS	ACTVT	01	
			KS02—Change Cost Center	K_CSKS	ACTVT	02	
			KS04—Delete Cost Center	K_CSKS	ACTVT	06	
			CP01—Create Business Process	K_ABC	ACTVT	01	
			CP02—Change Business Process	K_ABC	ACTVT	02	
			CP04—Delete Business Process	K_ABC	ACTVT	06	
			KL01—Create Activity Type	K_CSLA	ACTVT	01	
			KL02—Change Activity Type	K_CSLA	ACTVT	02	
			KL04—Delete Activity Type	K_CSLA	ACTVT	06	
			KK01—Create Statistical Key Figure	K_KA03	ACTVT	01	
			KK02—Change Statistical Key Figure	K_KA03	ACTVT	02	
			KK03DEL—Delete Statistical Key Figure	K_KA03	ACTVT	06	
BAI10	Changes made to master data are valid, complete, accurate and timely	1.1.3 Determine whether the configurable control settings address the risk pertaining to the validity, completeness and accuracy of master data and whether the settings are in accordance with management intentions. Access the settings online to customize IMG using transaction code OB13—C FI Maintain Table T004 to check the cost element creation settings that are specified in the COA definition. To validate the configuration for cost center categories, use transaction code SPRO to					

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes										
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment					
			<p>display the IMG menu and follow the path: Controlling → Cost Center Accounting → Master Data → Cost Centers → Define Cost Center Categories.</p> <p>Determine, with management, the fields that have been maintained as time dependent, and check the system settings using transaction code SPRO to display the IMG menu and follow the path: Controlling → Profit Center Accounting → Master Data → Profit Center → Specify Time Dependent Fields for Profit Centers.</p> <p>Take a sample of profit centers for which changes have been made, and execute the change report (transaction code 6KEA) to see the changes for time-dependent fields.</p>							
	DSS06	Master data remains current and pertinent.	1.2.1 Determine, with management, whether a process is in place to validate the master data approvals and/or changes on a periodic basis. Check the evidence of management review and approval for the sample of changes, and verify the changes using the testing technique 1.1.1.							
	DSS06	Master data remains current and pertinent.	1.2.2 Inquire, with management, to understand the design of the structure of the cost and profit centers, and verify the assignments in the system using the transaction codes: <ul style="list-style-type: none"> • KCH6N— EC-PCA—Display Standard Hierarchy • OKENN— Display Standard Hierarchy 							
	DSS06	Master data remains current and pertinent.	1.2.3 Ascertain with management whether there is a periodic process in place to review the existing design of the CO objects master data, make changes to the design if required by the business, review the changes made and check for validity. Investigate any suspected changes.							
B-3.6a	<p><u>Agree on the process work products</u>⁶ (inputs and outputs as defined in the process practices description) that are expected to be present (process design).</p> <p>Assess to what extent the process work products are available.</p>									
	Process Master data maintenance inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.		Criteria: All listed work products should demonstrably exist and be used.							
	<table border="1"> <thead> <tr> <th>Process Practice</th><th>Work Products</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Master data maintenance</td><td> <ul style="list-style-type: none"> • Master data add/change/delete request forms • Master data maintenance procedures • Master data maintenance reports • List of SAP users with master data access </td><td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td></tr> </tbody> </table>		Process Practice	Work Products	Assessment Step	Master data maintenance	<ul style="list-style-type: none"> • Master data add/change/delete request forms • Master data maintenance procedures • Master data maintenance reports • List of SAP users with master data access 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		
Process Practice	Work Products	Assessment Step								
Master data maintenance	<ul style="list-style-type: none"> • Master data add/change/delete request forms • Master data maintenance procedures • Master data maintenance reports • List of SAP users with master data access 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.								
B-3.7a	<p><u>Agree on the process capability level</u> to be achieved by the process.</p> <p><i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i></p>									
SAP ERP Controlling process: Cost element/cost center accounting/internal orders										
B-3.1b	Understand the Process context.									
B-3.2b	Understand the Process purpose.									
B-3.3b	Understand all process stakeholders and their roles.									

⁶ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module																									
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																									
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																			
	Cost element/cost center accounting/internal orders stakeholders:																								
B-3.4b	<p><u>Understand</u> the Process goals and related metrics⁷ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.</p> <p>The Process Cost element/cost center accounting/internal order has four defined process goals.</p> <table border="1"> <thead> <tr> <th>Process Goal</th> <th>Related Metrics</th> <th>Criteria/Expected Value</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>FI to CO postings are valid, complete, accurate and timely.</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>All transactions and events that should be recorded are recorded in the correct accounting period.</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>Changes in business and accounting principles do not affect internal reporting.</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>Postings to appropriate cost centers are valid and accurate.</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>					Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	FI to CO postings are valid, complete, accurate and timely.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	All transactions and events that should be recorded are recorded in the correct accounting period.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	Changes in business and accounting principles do not affect internal reporting.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	Postings to appropriate cost centers are valid and accurate.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step																						
FI to CO postings are valid, complete, accurate and timely.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																						
All transactions and events that should be recorded are recorded in the correct accounting period.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																						
Changes in business and accounting principles do not affect internal reporting.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																						
Postings to appropriate cost centers are valid and accurate.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																						
B-3.5b	<p><u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement.</p> <p>Validate Cost element/cost center accounting/internal orders</p> <table border="1"> <thead> <tr> <th>Reference Process</th> <th>Cost element/cost center accounting/internal orders</th> <th>Criteria: 2.1 FI to CO postings are valid, complete, accurate and timely. 2.2 All transactions and events that should be recorded are recorded in the correct accounting period. 2.3 Changes in business and accounting principles do not affect internal reporting. 2.4 Postings to appropriate cost centers are valid and accurate.</th> </tr> </thead> <tbody> <tr> <th>Reference Process Practices⁸</th> <th>Good Practice</th> <th>Assessment Step</th> <th>Issue Cross-reference</th> <th>Comment</th> </tr> <tr> <td>DSS05 DSS06</td> <td>FI to CO postings are valid, complete, accurate and timely.</td> <td>2.1.1 Select a sample of FI postings using SAP transaction code FB03—Select Document List. Enter appropriate company code and posting dates. For the selected documents, verify that they were posted to a valid CO cost object.</td> <td></td> <td></td> </tr> <tr> <td>DSS01 DSS06</td> <td>FI to CO postings are valid, complete, accurate and timely.</td> <td>2.1.2 Check the actual cost center postings via transaction code KSB1—Cost Centers: Actual Line Items; filter the output with the activity type. Take a sampling of actual postings of activities to the cost center, and verify the relationship between the activity type and the cost center with the following assignments:</td> <td></td> <td></td> </tr> </tbody> </table>					Reference Process	Cost element/cost center accounting/internal orders	Criteria: 2.1 FI to CO postings are valid, complete, accurate and timely. 2.2 All transactions and events that should be recorded are recorded in the correct accounting period. 2.3 Changes in business and accounting principles do not affect internal reporting. 2.4 Postings to appropriate cost centers are valid and accurate.	Reference Process Practices ⁸	Good Practice	Assessment Step	Issue Cross-reference	Comment	DSS05 DSS06	FI to CO postings are valid, complete, accurate and timely.	2.1.1 Select a sample of FI postings using SAP transaction code FB03—Select Document List. Enter appropriate company code and posting dates. For the selected documents, verify that they were posted to a valid CO cost object.			DSS01 DSS06	FI to CO postings are valid, complete, accurate and timely.	2.1.2 Check the actual cost center postings via transaction code KSB1—Cost Centers: Actual Line Items; filter the output with the activity type. Take a sampling of actual postings of activities to the cost center, and verify the relationship between the activity type and the cost center with the following assignments:				
Reference Process	Cost element/cost center accounting/internal orders	Criteria: 2.1 FI to CO postings are valid, complete, accurate and timely. 2.2 All transactions and events that should be recorded are recorded in the correct accounting period. 2.3 Changes in business and accounting principles do not affect internal reporting. 2.4 Postings to appropriate cost centers are valid and accurate.																							
Reference Process Practices ⁸	Good Practice	Assessment Step	Issue Cross-reference	Comment																					
DSS05 DSS06	FI to CO postings are valid, complete, accurate and timely.	2.1.1 Select a sample of FI postings using SAP transaction code FB03—Select Document List. Enter appropriate company code and posting dates. For the selected documents, verify that they were posted to a valid CO cost object.																							
DSS01 DSS06	FI to CO postings are valid, complete, accurate and timely.	2.1.2 Check the actual cost center postings via transaction code KSB1—Cost Centers: Actual Line Items; filter the output with the activity type. Take a sampling of actual postings of activities to the cost center, and verify the relationship between the activity type and the cost center with the following assignments:																							

⁷ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

⁸ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Managerial Accounting CO Module audit/assurance program.

Audit/Accuracy Program for SAP ERP Managerial Accounting CO Module													
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes													
Ref.	Assurance Steps and Guidance				Issue Cross-reference								
			<ul style="list-style-type: none"> Cost center categories to cost center (transaction code KS03—Display Cost Center) master data Cost center category to activity type (transaction code KL03—Display Activity Type) master data 										
BAI10	FI to CO postings are valid, complete, accurate and timely.	2.1.3 Inquire with management about the process to open and close CO periods. Use transaction code OKP1—Maintain Period Lock to verify that the locks are configured and up to date according to management intentions.	<table border="1"> <thead> <tr> <th>Transaction (s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>OKP1—Maintain Period Lock</td><td>S_TABU_DIS</td><td>ACTVT</td><td>02</td></tr> </tbody> </table>		Transaction (s)	Authorization Objects	Fields	Values	OKP1—Maintain Period Lock	S_TABU_DIS	ACTVT	02	
Transaction (s)	Authorization Objects	Fields	Values										
OKP1—Maintain Period Lock	S_TABU_DIS	ACTVT	02										
BAI10 DSS06	FI to CO postings are valid, complete, accurate and timely.	2.1.4 Use transaction code OBY6—C FI Maintain Table T001 to review the company code global settings. Confirm that the business area field is mandatory for all the cost centers created under that company code.											
BAI10	All transactions and events that should be recorded are recorded in the correct accounting period.	2.2.1 Use the testing steps described in control 2.1.3											
BAI10 DSS06	Changes in business and accounting principles do not affect internal reporting	2.3.1 Discuss with management recent changes in the business process that resulted in changes in the management accounting structure. Verify whether these changes are reflected in the actual postings. Use transaction code FB03—Display Document to view FI documents posted in GL. When the FI document is displayed, click on Environment → Document Environment → Relationship Browser to view CO documents and the hierarchy configuration in the system. Cost center standard hierarchy can be accessed via transaction code OKEON—Change Standard Hierarchy, and profit center hierarchy can be accessed via transaction code KCH3—Display Profit Center Hierarchy. For example, the following changes should be reflected in the actual FI/CO documents that are posted in the system: <ul style="list-style-type: none"> If there is a change in the process of making payments from new or changed house banks If the payments are made from new or additional check lots with different number ranges Delimitation or addition of new controlling objects, etc. 											
DSS06	Postings to appropriate cost centers are valid and accurate	2.4.1 Use transaction code GGB0—Validation Maintenance to access validation rules, and assess whether rules are configured according to management design based on the configured rules for CO objects (cost centers, profit centers, internal orders, etc.). Validate with the actual system posting via reports (e.g., execute transaction code FBL1N—Vendor Line-item Report, transaction code FBL3N—GL Line-item Report and FBL5N—Customer Line-item Report).											
DSS06	Postings to appropriate cost centers are valid and accurate	2.4.2 Use transaction code GGB1—Substitution Maintenance to access substitution rules, and assess whether rules are configured according to management design based on the configured rules for CO objects (cost centers, profit centers, internal orders, etc.). Validate with the actual system posting via reports (e.g., execute transaction code FBL1N—Vendor											

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
			Line item Report, transaction code FBL3N—GL Line Item Report and transaction code FBL5N—Customer Line Item Report.	
B-3.6b	<u>Agree on the process work products</u> ⁹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess</u> to what extent the process work products are available.			
	Process Cost element/cost center accounting/internal orders inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.
	Process Practice	Work Products	Assessment Step	
	Cost element/cost center accounting/internal orders	• List of changes to cost center/cost element/internal orders	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.	
B-3.7b	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>			
SAP ERP Controlling process: Profit center accounting				
B-3.1c	<u>Understand the Process context.</u>			
B-3.2c	<u>Understand the Process purpose.</u>			
B-3.3c	<u>Understand all process stakeholders</u> and their roles.			
	Profit center accounting stakeholders:			
B-3.4c	<u>Understand the Process goals</u> and related metrics ¹⁰ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.			
	The Process Profit center accounting has one defined process goal.		The following activities can be performed to assess whether the goals are achieved.	
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step
	Postings to appropriate profit centers/segments are valid and accurate.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.
B-3.5c	<u>Agree on suitable criteria</u> to evaluate all processes in scope of the assurance engagement.			
	Validate Profit center accounting			
	Reference Process	Profit center accounting	Criteria: 3.1 Postings to appropriate profit centers/segments are valid and accurate.	
	Reference Process Practices ¹¹	Good Practice	Assessment Step	Issue Cross-reference
	APO11 DSS06	Postings to appropriate profit centers/segments are	3.1.1 Use transaction code 1KE4—Assignment Monitor to analyze the assignment of profit centers with various objects. The same transaction code can also be used to generate the list of	Comment

⁹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: *Enabling Processes*.

¹⁰ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

¹¹ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Managerial Accounting CO Module audit/assurance program.

Audit/Accuracy Program for SAP ERP Managerial Accounting CO Module								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes								
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment		
B-3.6c		valid and accurate.	profit centers without any cost centers. Assess whether the output is configured according to management design. Transaction code KS13—Cost Centers: Master Data Report can also be used to check the list of assignments for cost centers to profit centers.					
	APO11 DSS06	Postings to appropriate profit centers/segments are valid and accurate.	3.1.2 Assignment of segments to profit centers can be validated using the transaction code KE5X—Cost Center: Master Data Index.					
	APO11 DSS06	Postings to appropriate profit centers/segments are valid and accurate.	3.1.3 If change requests for profit center extensions to new or existing company codes are received, compare the requests with the actual system configuration by accessing profit center master data display using transaction code KE53—Display Profit Center. Differences between the requests and configuration should be investigated.					
B-3.6c	<u>Agree on the process work products</u> ¹² (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess to what extent the process work products are available.</u> Process Profit center accounting inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.							
	Process Practice Profit center accounting			Work Products <ul style="list-style-type: none"> Profit center create/change form Review of new and/or changed profit centers in prior period Assessment Step Apply appropriate audit techniques to determine the existence and appropriate use of each work product.				
B-3.7c	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>							
SAP ERP Controlling process: Profitability Analysis, Product Costing and Activity-based Costing								
B-3.1d	<u>Understand the Process context.</u>							
B-3.2d	<u>Understand the Process purpose.</u>							
B-3.3d	<u>Understand all process stakeholders</u> and their roles.. Profitability Analysis, Product Costing and Activity-based Costing stakeholders:							
B-3.4d	<u>Understand the Process goals</u> and related metrics ¹³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process. The Process Profitability Analysis, Product Costing and Activity-based Costing has three defined process goals.							
	Process Goal Adjustments to customer data and product data within COPA have been properly approved or booked.		Related Metrics Determine the metrics that can be used to assess the achievement of the Process goals.		Criteria/Expected Value Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	Assessment Step <i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
	Valid, accurate, or complete product		Determine the metrics that can be		Agree on the expected values for	<i>In this step, the related metrics</i>		

¹² For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*.

¹³ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module																						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																
	costing would result in proper reporting.	used to assess the achievement of the Process goals.	the Process goal metrics, i.e., the values against which the assessment will take place.	for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																		
	Changes made to inventory costing are authorized and valid.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																		
B-3.5d	<p>Agree on suitable criteria to evaluate all processes in scope of the assurance engagement.</p> <p>Validate Profitability Analysis, Product Costing and Activity-based Costing</p> <table border="1"> <tr> <td>Reference Process</td><td>Profitability Analysis, Product Costing and Activity-based Costing</td><td>Criteria: 4.1 Adjustments to customer data and product data within CO-PA have been properly approved or booked. 4.2 Valid, accurate, or complete product costing would result in proper reporting. 4.3 Authorized and/or valid changes are made to inventory costing.</td></tr> </table>					Reference Process	Profitability Analysis, Product Costing and Activity-based Costing	Criteria: 4.1 Adjustments to customer data and product data within CO-PA have been properly approved or booked. 4.2 Valid, accurate, or complete product costing would result in proper reporting. 4.3 Authorized and/or valid changes are made to inventory costing.														
Reference Process	Profitability Analysis, Product Costing and Activity-based Costing	Criteria: 4.1 Adjustments to customer data and product data within CO-PA have been properly approved or booked. 4.2 Valid, accurate, or complete product costing would result in proper reporting. 4.3 Authorized and/or valid changes are made to inventory costing.																				
	Reference Process Practices¹⁴	Good Practice	Assessment Step			Issue Cross-reference	Comment															
	DSS05 DSS06	Adjustments to customer data and product data within COPA have been properly approved or booked.	<p>4.1.1 Use transaction code SUM—User Information System to test user access to the following transaction codes.</p> <table border="1"> <thead> <tr> <th>Transaction (s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>KE21—Create CO-PA Line Item</td> <td>K_KEI_TC</td> <td>ACTVT</td> <td>01</td> </tr> <tr> <td>KEA5 —Maintain Characteristics</td> <td>K_KEA_TC</td> <td>ACTVT</td> <td>01,02,06</td> </tr> <tr> <td>KEA6—Edit Value Fields</td> <td>K_KEA_TC</td> <td>ACTVT</td> <td>01,02,06</td> </tr> </tbody> </table>			Transaction (s)	Authorization Objects	Fields	Values	KE21—Create CO-PA Line Item	K_KEI_TC	ACTVT	01	KEA5 —Maintain Characteristics	K_KEA_TC	ACTVT	01,02,06	KEA6—Edit Value Fields	K_KEA_TC	ACTVT	01,02,06	
Transaction (s)	Authorization Objects	Fields	Values																			
KE21—Create CO-PA Line Item	K_KEI_TC	ACTVT	01																			
KEA5 —Maintain Characteristics	K_KEA_TC	ACTVT	01,02,06																			
KEA6—Edit Value Fields	K_KEA_TC	ACTVT	01,02,06																			
BAI10 DSS06	Adjustments to customer data and product data within COPA have been properly approved or booked.	<p>4.1.2 Use transaction code SPRO to display the IMG menu and follow the path: Controlling → Profitability Analysis → Structures → Define Profitability → Segment Characteristics.</p> <p>Transaction code KEQ3—Maintain Characteristics for Segment Level can also be used to validate the restrictions for characteristic values that are assigned to profitability segments. The possible restrictions defined for each characteristic value are:</p> <ol style="list-style-type: none"> 1. Not used—The characteristic is not taken into account when profitability segments are created. 2. Costing based—The characteristic is only taken into account in costing-based profitability analysis. 3. Account-based and costing-based—The characteristic is taken into account for both account-based profitability analysis and costing-based profitability analysis. <p>Each of these restrictions is used to generate the profitability analysis report.</p>																				
BAI10	Valid, accurate, or	4.2.1 Determine, with the management, whether any customization made in the system is triggered																				

¹⁴ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Controlling Managerial Accounting CO audit/assurance program.

Audit/Accuracy Program for SAP ERP Managerial Accounting CO Module																												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																												
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																						
	DSS06	complete product costing would result in proper reporting.	<p>when a production order status is changed to DLV (goods received against production order), using the transaction code CO11N—Enter Time Ticket for Production Order. This can automate the sequence of executing the transactions (KGI2—Act. Overhead: Int. Order Ind. Pro, KKS2—Variances—Product Cost by Lot (I) and KO88—Actual Settlement: Order) in the background.</p> <p>Use transaction code SUIM—User Information System to test user access to the following transaction codes.</p> <table border="1"> <thead> <tr> <th>Transaction (s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>KGI2—Act. Overhead: Int.Order Ind.Pro</td><td>K_VRGNG</td><td>ACTVT</td><td>16,48</td></tr> <tr> <td>KKS2—Variances—Product Cost by Lot (I)</td><td>K_VRGNG</td><td>ACTVT</td><td>16,48</td></tr> <tr> <td rowspan="2">KO88—Actual Settlement—Order</td><td>K_VRGNG</td><td>ACTVT</td><td>16,48</td></tr> <tr> <td>S_ALV_LAYO</td><td>ACTVT</td><td>23</td></tr> </tbody> </table> <p>By executing these transactions in the background, the calculation for the production order is automated, and the overhead costs are calculated accurately. To test the result of the background job, management should review and verify through the spool or log that is generated by the system after completion of that custom program execution.</p>	Transaction (s)	Authorization Objects	Fields	Values	KGI2—Act. Overhead: Int.Order Ind.Pro	K_VRGNG	ACTVT	16,48	KKS2—Variances—Product Cost by Lot (I)	K_VRGNG	ACTVT	16,48	KO88—Actual Settlement—Order	K_VRGNG	ACTVT	16,48	S_ALV_LAYO	ACTVT	23						
Transaction (s)	Authorization Objects	Fields	Values																									
KGI2—Act. Overhead: Int.Order Ind.Pro	K_VRGNG	ACTVT	16,48																									
KKS2—Variances—Product Cost by Lot (I)	K_VRGNG	ACTVT	16,48																									
KO88—Actual Settlement—Order	K_VRGNG	ACTVT	16,48																									
	S_ALV_LAYO	ACTVT	23																									
	DSS01 DSS06	Authorized and/or valid changes are made to inventory costing.	<p>4.3.1 Confirm with the management whether a team or personnel review the activity rate for the allocation using the transaction code KP27—Display Activity Types, on a periodic basis, to determine whether allocation rates are accurate.</p> <p>Use transaction code SUIM—User Information System to test user access to change the activity rates using the following transaction code:</p> <table border="1"> <thead> <tr> <th>Transaction (s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="6">KP26—Change Plan Data for Activity Types</td><td>K_CCA</td><td>CO_ACTION</td><td>0001, 0002, 0006, 1002</td></tr> <tr> <td>K_CSKB_PLA</td><td>ACTVT</td><td>02</td></tr> <tr> <td>K_CSKS_PLA</td><td>ACTVT</td><td>02</td></tr> <tr> <td>K_CSKS_SET</td><td>ACTVT</td><td>02</td></tr> <tr> <td>K_KA09_KVS</td><td>ACTVT</td><td>72</td></tr> <tr> <td>K_TKA50</td><td>ACTVT</td><td>16</td></tr> </tbody> </table>	Transaction (s)	Authorization Objects	Fields	Values	KP26—Change Plan Data for Activity Types	K_CCA	CO_ACTION	0001, 0002, 0006, 1002	K_CSKB_PLA	ACTVT	02	K_CSKS_PLA	ACTVT	02	K_CSKS_SET	ACTVT	02	K_KA09_KVS	ACTVT	72	K_TKA50	ACTVT	16		
Transaction (s)	Authorization Objects	Fields	Values																									
KP26—Change Plan Data for Activity Types	K_CCA	CO_ACTION	0001, 0002, 0006, 1002																									
	K_CSKB_PLA	ACTVT	02																									
	K_CSKS_PLA	ACTVT	02																									
	K_CSKS_SET	ACTVT	02																									
	K_KA09_KVS	ACTVT	72																									
	K_TKA50	ACTVT	16																									

Audit/Assurance Program for SAP ERP Managerial Accounting CO Module										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes										
Ref.	Assurance Steps and Guidance			Issue Cross-reference						
B-3.6d	<p>Agree on the process work products¹⁵ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.</p> <p>Profitability Analysis, Product Costing and Activity-based Costing inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.</p> <table border="1"> <thead> <tr> <th>Process Practice</th> <th>Work Products</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Cost and revenue element accounting</td> <td> <ul style="list-style-type: none"> List of changes to costing characteristics </td> <td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td> </tr> </tbody> </table>			Process Practice	Work Products	Assessment Step	Cost and revenue element accounting	<ul style="list-style-type: none"> List of changes to costing characteristics 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.	
Process Practice	Work Products	Assessment Step								
Cost and revenue element accounting	<ul style="list-style-type: none"> List of changes to costing characteristics 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.								
B-3.7d	<p>Agree on the process capability level to be achieved by the process.</p> <p><i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i></p>									

¹⁵ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: *Enabling Processes*.

Audit/Accruals Program for SAP ERP Managerial Accounting CO Module												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment												
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment									
B-4	<p>Obtain understanding of each Organisational Structure in scope and set suitable assessment criteria: For each Organisational Structure in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the Organisational Structure.</p>											
Organisational Structure: Cost/Manufacturing Accounting Group												
B-4.1a	<p><u>Understand the Organisational Structure context.</u> <i>Identify and document all elements that can help to understand the context in which the Cost/Manufacturing accounting group organization has to operate, including:</i></p> <ul style="list-style-type: none"> • The overall organisation • Management/process framework • History of the role/structure • Contribution of the Organisational Structure to achievement of goals 											
B-4.2a	<p><u>Understand all stakeholders of the Organisational Structure/function.</u> <i>Determine through documentation review (policies, management communications, etc.) the key stakeholders of the Cost/Manufacturing accounting group organization.</i></p> <ul style="list-style-type: none"> • Incumbent of the role and/or members of the Organisational Structure • Other key stakeholders affected by the decisions of the Organisational Structure/role 											
B-4.3a	<p><u>Understand the goals of the Organisational Structure</u>, the related metrics and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; background-color: #e0e0e0;">Organisational Structure Goal</th><th style="text-align: center; background-color: #e0e0e0;">Assessment Step</th></tr> </thead> <tbody> <tr> <td>Determine through interviews with key stakeholders and documentation review the goals of the Cost/Manufacturing accounting group organization, i.e., the decisions for which they are accountable^{16,17}.</td><td> <p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. </td></tr> </tbody> </table>	Organisational Structure Goal	Assessment Step	Determine through interviews with key stakeholders and documentation review the goals of the Cost/Manufacturing accounting group organization, i.e., the decisions for which they are accountable ^{16,17} .	<p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 							
Organisational Structure Goal	Assessment Step											
Determine through interviews with key stakeholders and documentation review the goals of the Cost/Manufacturing accounting group organization, i.e., the decisions for which they are accountable ^{16,17} .	<p>This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to:</p> <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 											
B-4.4a	<p><u>Agree on the expected good practices for the Organisational Structure</u> against which it will be assessed. <u>Assess the Organisational Structure design</u>, i.e., assess the extent to which expected good practices are applied.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; background-color: #e0e0e0;">Good Practice</th><th style="text-align: center; background-color: #e0e0e0;">Criteria</th><th style="text-align: center; background-color: #e0e0e0;">Assessment Step</th></tr> </thead> <tbody> <tr> <td>Operating principles</td><td> <ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. </td><td> <ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. </td></tr> <tr> <td>Composition</td><td>The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td><td>Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td></tr> </tbody> </table>	Good Practice	Criteria	Assessment Step	Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 	Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.		
Good Practice	Criteria	Assessment Step										
Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 										
Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.										

¹⁶ The RACI charts in COBIT 5: Enabling Processes can be leveraged as a starting point for the expected goals of a role or Organisational Structure.

¹⁷ The Organisational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organisational Structure assuming the same responsibilities and accountability should be considered.

Audit/Accruals Program for SAP ERP Managerial Accounting CO Module					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-4.5a	Span of control	<ul style="list-style-type: none"> The span of control of the Organisational Structure is defined. The span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. The span of control is in line with the overall enterprise governance arrangements. 	<ul style="list-style-type: none"> Verify whether the span of control of the Organisational Structure is defined. Assess whether the span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. Verify and assess whether the span of control is in line with the overall enterprise governance arrangements. 		
	Level of authority/decision rights	<ul style="list-style-type: none"> Decision rights of the Organisational Structure are defined and documented. Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue). 	<ul style="list-style-type: none"> Verify that decision rights of the Organisational Structure are defined and documented. Verify whether decision rights of the Organisational Structure are complied with and respected. 		
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.		
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.		
B-4.1 to B-4.5	<u>Understand the life cycle and agree on expected values.</u> <u>Assess the extent to which the Organisational Structure life cycle is managed.</u>				
	Life-Cycle Element	Criteria	Assessment Step		
	Mandate	<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well-understood mandate. 		
B-4.1 to B-4.5	Monitoring	<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 		
	Repeat steps B-4.1 through B-4.5 for all remaining Organisational structures in scope.				
B-4.1 to B-4.5	Repeat the steps described above for the remaining Organisational structures:				
	<ul style="list-style-type: none"> Material Pricing Corporate Controlling 				

Audit/Accruals Program for SAP ERP Managerial Accounting CO Module												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment												
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment									
B-5	Obtain understanding of the Culture, Ethics and Behaviour in scope. Assess Culture, Ethics and Behaviour.											
Culture, Ethics and Behaviour: Risk and compliance aware culture												
B-5.1a	<u>Understand the Culture, Ethics and Behaviour context.</u> <ul style="list-style-type: none"> • <i>What the overall corporate Culture is like</i> • <i>Understand the interconnection with other enablers in scope:</i> <ul style="list-style-type: none"> - <i>Identify roles and structures that could be affected by the Culture.</i> - <i>Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.</i> 											
B-5.2a	<u>Understand the major stakeholders of the Culture, Ethics and Behaviour: Risk and compliance aware culture</u> <i>Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.</i>											
B-5.3a	<u>Understand the goals for the Culture, Ethics and Behaviour, and the related metrics</u> and agree on expected values. <u>Assess whether the Culture, Ethics and Behaviour goals</u> (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour. In the context of Risk and compliance aware culture , the following Culture, Ethics and Behaviour are desired:	Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. For a representative sample of individuals, perform the following assessment steps.										
Desired Behaviour (Culture, Ethics and Behaviour Goal)		Assessment Step										
The enterprise is aware of the compliance requirements it must abide												
Employees understand their role in maintaining compliance												
Identified risk are properly address												
Controls are in place to ensure compliance with internal and external requirements												
B-5.4a	<u>Understand the life cycle stages of the Culture, Ethics and Behaviour, and agree on the relevant criteria.</u> <u>Assess to what extent the Culture, Ethics and Behaviour life cycle is managed.</u> <i>(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)</i>											
B-5.5a	<u>Understand good practice when dealing with Culture, Ethics and Behaviour, and agree on relevant criteria.</u> <u>Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied.</u> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; width: 33%;">Good Practice</th><th style="text-align: center; width: 33%;">Criteria</th><th style="text-align: center; width: 33%;">Assessment Step</th></tr> </thead> <tbody> <tr> <td>Communication, enforcement and rules</td><td>Existence and quality of the communication</td><td rowspan="3" style="vertical-align: top;">Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.</td></tr> <tr> <td>Incentives and rewards</td><td>Existence and application of appropriate rewards and incentives</td></tr> <tr> <td>Awareness</td><td>Awareness of desired Behaviours</td></tr> </tbody> </table>	Good Practice	Criteria	Assessment Step	Communication, enforcement and rules	Existence and quality of the communication	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.	Incentives and rewards	Existence and application of appropriate rewards and incentives	Awareness	Awareness of desired Behaviours	
Good Practice	Criteria	Assessment Step										
Communication, enforcement and rules	Existence and quality of the communication	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.										
Incentives and rewards	Existence and application of appropriate rewards and incentives											
Awareness	Awareness of desired Behaviours											
B-5.1 to B-5.5	Repeat steps B-5.1 through B-5.5 for all remaining Culture, Ethics and Behaviour in scope.											
	Repeat the steps described above for the remaining Culture, Ethics and Behaviour: <ul style="list-style-type: none"> • Enabling of continuous improvement • Accountability • Discipline to follow instructions 											

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module																																																															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																																																															
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment																																																												
B-6	Obtain understanding of the Information Items in scope. Assess Information Items.																																																														
Information Item: Data integrity procedures																																																															
B-6.1a	<u>Understand</u> the Information item context : <ul style="list-style-type: none"> • Where and when is it used? • For what purpose is it used? • Understand the connection with other enablers in scope, e.g.: <ul style="list-style-type: none"> - Used by which processes? - Which Organisational Structures are involved? - Which services/applications are involved? 																																																														
B-6.2a	<u>Understand</u> the major stakeholders of the Information item . Understand the stakeholders for the Information item, i.e., identify the: <ul style="list-style-type: none"> • Information producer • Information custodian • Information consumer <i>Stakeholders should be at the appropriate organisational level.</i>																																																														
B-6.3a	<u>Understand</u> the major quality criteria for the Information item, the related metrics and agree on expected values. Assess whether the Information item quality criteria (outcomes) are achieved, i.e., assess the effectiveness of the Information item. Leverage the COBIT 5 Information enabler model ¹⁸ focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand. Mark the quality dimensions with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.	The assurance professional will, by using appropriate auditing techniques, verify all quality criteria in scope and assess whether the criteria are met.																																																													
<table border="1"> <thead> <tr> <th>Quality Dimension</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr><td>Accuracy</td><td>✓</td><td></td><td></td></tr> <tr><td>Objectivity</td><td></td><td></td><td></td></tr> <tr><td>Believability</td><td></td><td></td><td></td></tr> <tr><td>Reputation</td><td></td><td></td><td></td></tr> <tr><td>Relevancy</td><td>✓</td><td></td><td></td></tr> <tr><td>Completeness</td><td>✓</td><td></td><td></td></tr> <tr><td>Currency</td><td>✓</td><td></td><td></td></tr> <tr><td>Amount of information</td><td>✓</td><td></td><td></td></tr> <tr><td>Concise representation</td><td>✓</td><td></td><td></td></tr> <tr><td>Consistent representation</td><td></td><td></td><td></td></tr> <tr><td>Interpretability</td><td></td><td></td><td></td></tr> <tr><td>Understandability</td><td>✓</td><td></td><td></td></tr> <tr><td>Manipulation</td><td></td><td></td><td></td></tr> <tr><td>Availability</td><td>✓</td><td></td><td></td></tr> </tbody> </table>				Quality Dimension	Key Criteria	Description	Assessment Step	Accuracy	✓			Objectivity				Believability				Reputation				Relevancy	✓			Completeness	✓			Currency	✓			Amount of information	✓			Concise representation	✓			Consistent representation				Interpretability				Understandability	✓			Manipulation				Availability	✓		
Quality Dimension	Key Criteria	Description	Assessment Step																																																												
Accuracy	✓																																																														
Objectivity																																																															
Believability																																																															
Reputation																																																															
Relevancy	✓																																																														
Completeness	✓																																																														
Currency	✓																																																														
Amount of information	✓																																																														
Concise representation	✓																																																														
Consistent representation																																																															
Interpretability																																																															
Understandability	✓																																																														
Manipulation																																																															
Availability	✓																																																														

¹⁸ COBIT 5 framework, appendix G, p.81-84

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
Ref.	Assurance Step and Guidance			Issue Cross-reference	Comment
	Restricted access	✓			
B-6.4a	<p><u>Understand the life cycle</u> stages of the Information item, and agree on the relevant criteria. <u>Assess</u> to what extent the Information item life cycle is managed.</p> <p>The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.</p> <ul style="list-style-type: none">When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently.When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.				
	Life Cycle Stage	Key Criteria	Description	Assessment Step	
	Plan	✓			
	Design	✓			
	Build/acquire	✓			
	Use/operate	✓			
	Evaluate/monitor	✓			
	Update/dispose	✓			
B-6.5a	<p><u>Understand</u> important attributes of the Information item and expected values. <u>Assess</u> the Information item design, i.e., assess the extent to which expected good practices are applied.</p> <p>Good practices for Information items are defined as a series of attributes for the Information item¹⁹. The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.</p> <p>Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p>				
	Attribute	Key Criteria	Description	Assessment Step	
	Physical				
	Empirical				
	Syntactic				
	Semantic				
	Pragmatic	✓			
	Social				
B-6.1 to B-6.5	Repeat steps B-6.1 through B-6.5 for all remaining Information items in scope.				
	Repeat the steps described above for the remaining Information items:				
	<ul style="list-style-type: none">Data classification guidelinesData security and control guidelinesAssigned responsibilities for resource managementAccess logsAllocated roles and responsibilitiesAllocated levels of authorityAllocated access rightsEvidence or error correction and remediationError reports and root cause analysisRetention requirementsRecord of transactionsTraining manualsJob aids				

¹⁹ COBIT 5 framework, appendix G, p. 81-84

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module																								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Services, Infrastructure and Applications																								
Ref.	Assurance Steps and Guidance			Issue Cross-reference																				
B-7	Obtain understanding of the Services, Infrastructure and Applications in scope. Assess Services, Infrastructure and Applications.																							
Services, Infrastructure and Applications: Master data maintenance group																								
B-7.1a	<u>Understand the Services, Infrastructure and Applications</u> context. <i>Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.</i>																							
B-7.2a	<u>Understand the major stakeholders of the Services, Infrastructure and Applications.</u> <i>Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.</i>																							
B-7.3a	<u>Understand the major goals for the Services, Infrastructure and Applications</u> , the related metrics and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.																							
<table border="1"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th><th></th><th></th></tr> </thead> <tbody> <tr> <td>Service description</td><td> <ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders </td><td> <ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. </td><td></td><td></td></tr> <tr> <td>Service level definition</td><td> Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness </td><td> <ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. </td><td></td><td></td></tr> <tr> <td>Contribution to related enablers, IT and enterprise goals</td><td>The Service contributes to the achievement of related enabler and IT-related and enterprise goals.</td><td>Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.</td><td></td><td></td></tr> </tbody> </table>					Goal	Criteria	Assessment Step			Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 			Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 			Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.		
Goal	Criteria	Assessment Step																						
Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 																						
Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 																						
Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.																						
B-7.4a	<u>Understand good practice related to the Services, Infrastructure and Applications and expected values.</u> <u>Assess the Services, Infrastructure and Applications</u> design, i.e., assess to what extent expected good practices are applied. <i>Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework²⁰ to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented:</i> <ul style="list-style-type: none"> Buy/build decision needs to be taken. Use of the Service needs to be clear. 																							
<table border="1"> <thead> <tr> <th>Good Practice</th><th>Criteria</th><th>Assessment Step</th><th></th><th></th></tr> </thead> <tbody> <tr> <td>Sourcing (buy/build)</td><td>A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.</td><td> <ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. </td><td></td><td></td></tr> </tbody> </table>					Good Practice	Criteria	Assessment Step			Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. 												
Good Practice	Criteria	Assessment Step																						
Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. 																						

²⁰ COBIT 5 framework, appendix G, p.85-86

Audit/Assurance Program for SAP ERP Managerial Accounting CO Module				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Culture, Ethics and Behaviour				
Ref.	Assurance Step and Guidance			Issue Cross-reference
	Use	The use of the Service needs to be clear: <ul style="list-style-type: none">• When it needs to be used and by whom• The required compliance levels with the Service's output	<ul style="list-style-type: none">• Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used.• Verify that actual use is in line with requirement above.• Verify that the actual Service output is adequately used.• Verify that Service levels are monitored and achieved.	
B-7.1 to B-7.4	<p>Repeat steps B-7.1 through B-7.4 for all remaining Services, Infrastructure and Applications in scope.</p> <p>Repeat the steps described above for the remaining Services, Infrastructure and Applications:</p> <ul style="list-style-type: none">• SAP ERP System• SAP training• Change management			

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module																				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																				
People, Skills and Competencies																				
Ref.	Assurance Steps and Guidance			Issue Cross-reference																
B-8	Obtain understanding of the People, Skills and Competencies in scope. Assess People, Skills and Competencies.			Comment																
People, Skill and Competency: Proficiency using the SAP Controlling Module																				
B-8.1a	<p><u>Understand the People, Skills and Competencies</u> context. <i>Understand the context of the Skill/Competency, i.e.,:</i></p> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> – <i>In which roles and structures is the Skill/Competency used? (See also B-4.1.)</i> <p><i>Which behaviours are associated with the Skill/Competency?</i></p>																			
B-8.2a	<p><u>Understand the major stakeholders</u> for the People, Skills and Competencies. <i>Identify to whom in the organisation the skill requirement applies.</i></p>																			
B-8.3a	<p><u>Understand the major goals</u> for the People, Skills and Competencies, the related metrics and <u>agree</u> on expected values. <u>Assess</u> whether the People, Skills and Competencies goals (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.</p> <p>For the People, Skills and Competencies: Proficiency using the SAP Controlling Module, the following goals and associated criteria can be addressed.</p> <table border="1"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Experience</td><td></td><td rowspan="7">Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.</td></tr> <tr> <td>Education</td><td></td></tr> <tr> <td>Qualification</td><td></td></tr> <tr> <td>Knowledge</td><td></td></tr> <tr> <td>Technical skills</td><td></td></tr> <tr> <td>Behavioural skills</td><td></td></tr> <tr> <td>Number of people with appropriate skill level</td><td></td></tr> </tbody> </table>	Goal	Criteria	Assessment Step	Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	Education		Qualification		Knowledge		Technical skills		Behavioural skills		Number of people with appropriate skill level		
Goal	Criteria	Assessment Step																		
Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.																		
Education																				
Qualification																				
Knowledge																				
Technical skills																				
Behavioural skills																				
Number of people with appropriate skill level																				
B-8.4a	<p><u>Understand the life cycle</u> stages of the People, Skills and Competencies, and agree the relevant criteria. <u>Assess</u> to what extent the People, Skills and Competencies life cycle is managed.</p> <p>For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07.</p> <table border="1"> <thead> <tr> <th>Life Cycle Element</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Plan</td><td>Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.</td><td>Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.</td></tr> <tr> <td>Design</td><td>Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to</td><td>Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.</td></tr> </tbody> </table>	Life Cycle Element	Criteria	Assessment Step	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.										
Life Cycle Element	Criteria	Assessment Step																		
Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.																		
Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.																		

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
People, Skills and Competencies					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.			
	Build	Practice APO07.03 activity 4 (Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 4 is implemented in relation to this skill.		
	Operate	Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.		
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.		
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.		
B-8.5a	Understand good practice related to the People, Skills and Competencies and expected values. Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.				
	Good Practice	Criteria	Assessment Step		
	Skill set and Competencies are defined.	<ul style="list-style-type: none"> • Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. • Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. • Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 			
	Skill levels are defined.	<ul style="list-style-type: none"> • Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and 			

Audit/Assurance Program for SAP ERP Managerial Accounting CO Module				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
People, Skills and Competencies				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
		current Skill levels. <ul style="list-style-type: none"> • Assess the process for 360-degree performance evaluations. 		
B-8.1 to B-8.5	Repeat steps B-8.1 through B-8.5 for all remaining People, Skills and Competencies in scope. Repeat the steps described above for the remaining People, Skills and Competencies: <ul style="list-style-type: none"> • Master data management skills • Controlling module skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 			

Audit/Accrual Program for SAP ERP Managerial Accounting CO Module		
Phase C—Communicate the Results of the Assessment		
Ref.	Assurance Step	Guidance
C-1	Document exceptions and gaps.	
C-1.1	Understand and document weaknesses and their impact on the achievement of process goals.	<ul style="list-style-type: none"> Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	<ul style="list-style-type: none"> Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. Point out the consequence of noncompliance with regulatory requirements and contractual agreements. Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
C-2	Communicate the work performed and findings.	
C-2.1	Communicate the work performed.	<ul style="list-style-type: none"> Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	<ul style="list-style-type: none"> Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. Use benchmarking and survey results to compare the enterprise's performance with others. Use extensive graphics to illustrate the issues. Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	

Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
1. Master Data Maintenance							
1.1. Changes made to master data are valid, complete, accurate and timely.							
1.1.1 Are reports detailing changes to master data compared to authorized source documents and/or a manual log of requested changes to ensure that they were input accurately and on a timely basis?					BAI06 DSS01 DSS06		
1.1.2 Is access to create and change master data restricted to authorized personnel?					DSS05		
1.1.3 Are configurable controls used to maintain the integrity of master data?					BAI10		
1.2. Master data remain current and pertinent.							
1.2.1 Does management conduct a periodic review of master data to check for accuracy and appropriateness?					DSS06		
1.2.2 Are cost centers and cost center groups assigned to cost center hierarchy, and are profit centers and profit center groups assigned to hierarchy?					DSS06		
1.2.3 Is the validity of all master records updated/reviewed by a dedicated team on a periodic basis?					DSS06		
2. Cost Element/Cost Center Accounting/Internal Orders							
2.1 FI to CO postings are valid, complete, accurate and timely.							
2.1.1 Is the system configured to automatically post from FI to CO using primary cost elements to ensure real-time transfer of posting data from FI to CO?					DSS05 DSS06		

Managerial Accounting (SAP CO) ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.1.2 Is the system configured to use cost center categories to control the posting of particular activity types only for particular cost centers?					DSS01 DSS06
2.1.3 Is the system configured to use period lock configuration to control the timing of posting of various controlling transactions to controlling objects for the period?					BAI10
2.1.4 Is the system configured to activate the “Business area fin. statements” check in company code global settings (OBY6) to ensure that the business area field becomes mandatory for all the cost centers created under that company code?					BAI10 DSS06
2.2 All transactions and events that should be recorded are recorded in the correct accounting period.					
2.2.1 Refer to control number 2.1.3.					
2.3 Changes in business and accounting principles do not affect internal reporting.					
2.3.1 Are any proposed changes to accounting principles analyzed to determine any impact on the business and determine whether system changes are necessary?					BAI10 DSS06
2.4 Postings to appropriate cost centers are valid and accurate.					
2.4.1 Is the system configured to activate validations at the FI line item level to ensure that an error/warning message will be triggered when posting to inappropriate cost centers?					DSS06

Managerial Accounting (SAP CO) ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.4.2 Is the system configured to activate substitution rules at the FI line item level to ensure that appropriate cost centers are automatically populated/substituted based on the substitution rules?					DSS06
3. Profit Center Accounting					
3.1 Postings to appropriate profit centers/segments are valid and accurate.					
3.1.1 Is the system configured to assign profit centers to cost centers and automatically derived from cost center master data to the FI line items during document postings?					APO11 DSS06
3.1.2 Is the system configured to assign segments to profit centers, which are automatically derived to FI line items during document postings?					APO11 DSS06
3.1.3 Is the system configured to extend company codes to profit center master data in order to post transactions of a particular company code to the profit center?					APO11 DSS06
4. Profitability Analysis/Product Costing/Activity-based Costing					
4.1 Adjustments to customer data and product data within CO-PA have been properly approved or booked.					
4.1.1 Is access to repost a document/maintain characteristics via transaction KE21 (create CO-PA line item), KEA5 (maintain characteristics), and KEA6 (edit field values) restricted to a dedicated team or personnel?					DSS05 DSS06

Managerial Accounting (SAP CO) ICQ

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
4.1.2 Are restrictions configured for each characteristic values that are assigned to profitability segments?					BAI10 DSS06
4.2 Valid, accurate or complete product costing would result in proper reporting.					
4.2.1 Can customized enhancement be used to control the automatic calculation of the overhead costs associated with a production order, and then the variance and perform the settlement (to finished goods pricing) calculated for all production orders?					BAI10 DSS06
4.3 Authorized and/or valid changes are made to inventory costing.					
4.3.1 Is the activity rate for the allocation reviewed on a periodic basis to check that allocation rates are accurate?					DSS01 DSS06

SAP ERP

Human Capital Management Business Cycle
Audit/Assurance Program



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP ERP Human Capital Management Business Cycle Audit/Assurance Program* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP's kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: <http://www.isaca.org/sap-erp-4th-edition>

Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOOfficial>

Like ISACA on Facebook: www.facebook.com/ISACAHQ

Acknowledgements

ISACA wishes to recognize

Project Leaders

Benjamin Fitts, CPA, Deloitte & Touche LLP, USA
Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA
Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA
Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Eva Sweet, CISA, CISM, ISACA, USA

Researchers

Syed Aamir Aarfi, Deloitte & Touche LLP, USA
Carlos Amaya, CISA, Deloitte & Touche LLP, USA
Dan Argynov, PMP, Deloitte & Touche LLP, USA
Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA
David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA
Ramamallikarjunaraao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA
Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA
Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA
Sagnik Mukherjee, Deloitte & Touche LLP, USA
Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA
Sonik Shah, Deloitte & Touche LLP, USA
Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA
Shweta Srivastava, Deloitte & Touche LLP, USA
Anurag Tewary, Deloitte & Touche LLP, USA
Percy Tsai, CPA, Deloitte & Touche LLP, USA
Ravi Maddela Veeriah, Deloitte & Touche LLP, USA
Sravan Vemana, Deloitte & Touche LLP, USA
Anukool Vyas, Deloitte & Touche LLP, USA

Expert Reviewers

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA
Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada
Mayank Garg, CISA, NetApp, USA
Ricci Leong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Jim Koveos, CISA, MBA, AmerisourceBergen, USA
Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia
Samuel Lim S.C., CISA, Auditor General's Office, Singapore
Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia
Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General's Office, Singapore
Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia
Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia
Paul O'Donnell, Ernst & Young, Canada
Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico
John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US
Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico
Naved Rehman, CISA, CRISC, MS-IS, SAPAuditCoach, US
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US
Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico
Jovari St. Victor, CISA, CPA, Sunera, LLC, US
Surapong Surabotsopon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,
KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico
Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand
David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President
Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cythus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK
Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil
Jotham Nyamari, CISA, Deloitte, USA
James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK
Gurvinder Singh, CISA, CISM, CRISC, Australia
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore
Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

SAP ERP Human Capital Management Business Cycle Audit/Assurance Program

Introduction

This document contains an example audit/assurance program, **based on** the generic structure developed in section 2B of *COBIT 5 for Assurance*¹.

The engagement approach is based on, but **differs slightly** from the generic approach described in *COBIT 5 for Assurance*:

- The engagement approach described in this audit/assurance program is **focused on a business process** consequently no group of COBIT 5 processes dominates as primary processes and the lower-level processes are widespread, for evaluation purposes, the high-level COBIT 5 processes will be used as references.
- The assurance steps in this audit/assurance program are specific to the subject matter under review; therefore most of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources availableprocess audit/assurance program.

Assurance Engagement: SAP ERP Human Capital Management Business Cycle

Assurance Topic

The topic covered by this assurance engagement is the SAP ERP Human Capital Management Business Cycle.

Business Impact and Risk

SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical processes.

Risk resulting from ineffective or incorrect configurations or use of SAP could result in some of the following:

- Disclosure of privileged information
- Single points of failure
- Low data quality
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements

Goal of the Review

The objective of the SAP ERP audit/assurance review is to provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise's SAP ERP architecture.

Scoping

The review will focus on configuration of the relevant SAP ERP components and modules within the enterprise. The selection of the specific components and modules will be based upon the risk introduced to the enterprise by these components and modules.

From a process reference model (PRM) perspective, the following domains and processes apply to this audit and assurance programme:

- BAI02 Manage requirements definition
- BAI03 Manage solution identification and build

¹ See www.isaca.org/COBIT/Pages/Assurance-product-page.aspx for more information on *COBIT 5 for Assurance*.

- DSS01 *Manage operations*
- DSS05 *Manage security services*
- DSS06 *Manage business process controls*

Testing SAP Security

To determine which users have access to the relevant authorizations used in this audit program, use one of the following methods:

1. Use transaction code SUIM → Users → Users by Complex Selection Criteria
2. Use transaction code S_BCE_68001417
3. Use transaction code SA38 and the program RSUSR002. This method allows the user to specify a transaction code, a “valid to” date for users, and up to three other authorization objects (which also may be the authorization object for transaction code S_TCODE) with associated values (two values under an AND relationship and three values under an OR relationship).
This method is generally sufficient for testing logical access security in relation to SAP ERP application infrastructure areas, but it is less suitable when large numbers of authorizations must be reviewed, such as in segregation of duties analysis and in some of the more complex areas of business cycle controls.
4. Use transaction code SUIM → Users → Users with Critical Authorizations (also accessible with program RSUSR008_009_NEW, which replaces programs RSUSR008 and RSUSR009 and transaction codes SU98 and/or SU99, for SAP Web AS 6.20 and later). This method offers improvements such as allowing differentiation between SAP defaults for critical data for different business areas, extended combination options for critical authorization data, improved performance, display of user filters and more analysis options for users in the result list.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle						
Phase A—Determine Scope of the Assurance Initiative						
Ref.	Assurance Step	Guidance			Issue Cross-reference	Comment
A-1	Determine the stakeholders of the assurance initiative and their stakes .					
A-1.1	<u>Identify</u> the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	Intended user(s) of the assurance report	<p>Board/audit committee: Needs assurance over the effectiveness and efficiency of SAP ERP processes within the enterprise.</p> <p>Chief financial officer (CFO): Needs assurance that internal controls for financial applications work as intended.</p> <p>Risk managers: Need assurance that controls intended to address previously identified risk are working as intended. The results from the audit should be used to update the risk registry as needed.</p> <p>Security managers: Need to identify gaps in the security plans for SAP applications.</p> <p>Owners / shareholders: Part or all of the SAP ERP assurance report may be included in statutory reporting.</p> <p>Regulators: Part or all of SAP ERP reporting may need to be disclosed to respective authorities</p>			
A-1.2	Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	Accountable and responsible parties for the subject matter	<p>Business executives: The individuals responsible for identifying requirements, approving design and managing performance. These people are, together with IT management, responsible for managing the correct and controlled use of SAP ERP services—in line with good practices.</p> <p>Business process owners: Responsible for defining application and technical requirements. Responsible for data classification.</p> <p>IT management: Responsible for managing the correct and controlled use of SAP ERP services—together with the business executives.</p>			
A-2	Determine the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities (i.e., not achieving the enterprise goals).		<p>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.</p> <p>Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.</p> <p>Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</p> <p>Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.</p>			
A-2.1	Understand the enterprise strategy and priorities.		<i>Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.</i>			

Audit/Assurance Program for SAP ERP Human Capital Management Business Cycle				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
A-2.2	<u>Understand</u> the internal context of the enterprise.	<p><i>Identify all internal environmental factors that could influence the performance and contents of the SAP ERP Human Capital Management Business Cycle Module.</i></p> <ul style="list-style-type: none"> • Review prior report, if one exists, verify completion of any agreed-on corrections, and note remaining deficiencies. Determine whether: <ul style="list-style-type: none"> - Senior management has assigned responsibilities for information, its processing and its use - User management is responsible for providing information that supports the entity's objectives and policies - Information systems management is responsible for providing the capabilities necessary for the achievement of the defined information systems objectives and the policies of the entity - Senior management approves plans for development and acquisition of information systems - There are procedures to ensure that the information system being developed or acquired meets user requirements - There are procedures to ensure that information systems, programs and configuration changes are tested adequately prior to implementation - All personnel involved in the system acquisition and configuration activities receive adequate training and supervision - There are procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards - User management participates in the conversion of data from the existing system to the new system - Final approval is obtained from user management prior to going live with a new information/upgraded system - There are procedures to document and schedule all changes to information systems (including key ABAP programs) - There are procedures to ensure that only authorized changes are initiated - There are procedures to ensure that only authorized, tested and documented changes to information systems are accepted into the production client - There are procedures to allow for and control emergency changes - There are procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software - There is a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated - The organizational structure, established by senior management, provides for an appropriate segregation of incompatible functions - The database, application and presentation servers are located in a physically separate and protected environment (i.e., a data center) - Emergency, backup and recovery plans are documented and tested on a regular basis to ensure that they remain current and operational - Backup and recovery plans allow users of information systems to resume operations in the event of an interruption - Application controls are designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system - Access to the Implementation Guide (IMG) during production has been restricted - The production client settings have been flagged to not allow changes to programs and 		

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle									
Phase A—Determine Scope of the Assurance Initiative									
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment					
		<p>configuration</p> <ul style="list-style-type: none"> • Identify the significant risk and determine the key controls <ul style="list-style-type: none"> – Develop a high-level process flow diagram and overall understanding of the HR Module, including the following subprocesses: <ul style="list-style-type: none"> a. Organizational management b. Personnel administration c. Time management d. Payroll management risk e. Travel management f. Enterprise compensation management g. Employee self-service and manager self service – Assess the key risk, determine key controls or control weaknesses, and test controls (refer to the sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> a. The controls culture of the organization (e.g., a just-enough-control philosophy). b. The need to exercise judgment to determine the key controls in the process and whether the controls structure is adequate. (Any weaknesses in the control structure should be reported to executive management and resolved.) • Gain an understanding of the SAP ERP environment (The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles) <p>In particular, the following information is important:</p> <ul style="list-style-type: none"> – Version and release of SAP ERP implemented – Total number of named users (for comparison with logical access security testing results) – Number of SAP instances and clients – Accounting period, company codes and chart of accounts – Identification of the components being used (Human Capital Management, Financials, Operations, Corporate Services) – Whether the organization has created any locally developed ABAP programs or reports – Details of the risk assessment approach taken in the organization to identify and prioritize risk – Copies of the organization's key security policies and standards <p>Obtain details of the following:</p> <ul style="list-style-type: none"> – Organizational Management Model as it relates to sales/revenue activity, i.e., sales organizational unit structure in SAP ERP and company sales organizational chart (required when evaluating the results of access security control testing) – An interview of the systems implementation team, if possible, and process design documentation for sales and distribution 							
A-2.3	<u>Understand</u> the external context of the enterprise.	<i>Identify all external environmental factors that could influence the performance and contents of the SAP ERP Human Capital Management Business Cycle Module.</i>							
A-2.4	Given the overall assurance objective, translate the identified strategic priorities into concrete <u>objectives</u> for the assurance engagement.	<p>The following goals are retained as key goals to be supported, in reflection of enterprise strategy and priorities:</p> <table border="1"> <tr> <td>Key goals</td> <td>Enterprise goals:</td> </tr> <tr> <td></td> <td> <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) </td> </tr> </table>	Key goals	Enterprise goals:		<ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) 			
Key goals	Enterprise goals:								
	<ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) 								

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step		Guidance	Issue Cross-reference	Comment
			<ul style="list-style-type: none"> • EG04 Compliance with external laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality • EG15 Compliance with internal policies <p>IT-related goals:</p> <ul style="list-style-type: none"> • ITG01 Alignment of IT and business strategy • ITG02 IT compliance and support for business compliance with external laws and regulations • ITG04 Managed IT-related business risk • ITG07 Delivery of IT services in line with business requirements • ITG08 Adequate use of applications, information and technology solutions • ITG09 IT Agility • ITG10 Security of information, processing infrastructure and applications • ITG12 Enablement and support of business processes by integrating applications and technology into business processes • ITG14 Availability of reliable and useful information for decision making • ITG15 IT compliance with internal policies • ITG16 Competent and motivated business and IT personnel 		
		Additional goals			
A-2.5	Define the organizational boundaries of the assurance initiative.		<p><i>Describe the organizational boundaries of the assurance engagement, i.e., to which organizational entities the review is limited. All other aspects of scope limitation are identified during phase A-3.</i></p> <ul style="list-style-type: none"> • The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment. • Obtain information and form an understanding of the business reasons underlying the audit • Identify the senior business resources responsible for the review. • Identify the senior IT audit/assurance resource responsible for the review. • Establish the process for suggesting and implementing changes to the audit/assurance program, and list the authorizations required. • Identify any limitations and/or constraints affecting the audit of specific systems and subsystems. • Identify and third party services, applications, platforms and infrastructure elements that may not be or only partially be accessible. • Identify any legal, regulatory or contractual constraints on audit. • Identify any industrial relations based or end user based audit constraints. 		

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
A-3	Determine the enablers in scope and the instance(s) of the enablers in scope.	COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.						
A-3.1	Define the Principles, Policies and Frameworks in scope.	<p>Guiding principles and policies include:</p> <ul style="list-style-type: none"> • Policy for Master Data Maintenance • ISMS policy • Legal and regulatory compliance requirements • Hiring Policy • Termination Policy 						
A-3.2	<p>Define which Processes are in scope of the review.</p> <p>Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of process goals • Application of process good practices • Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments) 	<p><i>COBIT 5: Enabling Processes</i> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed.</p> <table border="1"> <tr> <td>Key processes</td><td> <ul style="list-style-type: none"> • Personnel Administration • Time Management • Payroll • Organizational Management • Travel Management • Enterprise Compensation Management • End-user Service Delivery: Employee Self-service and Manager Self-service </td></tr> <tr> <td>Additional processes</td><td> <ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls </td></tr> </table>	Key processes	<ul style="list-style-type: none"> • Personnel Administration • Time Management • Payroll • Organizational Management • Travel Management • Enterprise Compensation Management • End-user Service Delivery: Employee Self-service and Manager Self-service 	Additional processes	<ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls 		
Key processes	<ul style="list-style-type: none"> • Personnel Administration • Time Management • Payroll • Organizational Management • Travel Management • Enterprise Compensation Management • End-user Service Delivery: Employee Self-service and Manager Self-service 							
Additional processes	<ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO06 Manage Budget and Cost • APO07 Manage Human Resources • APO10 Manage Suppliers • APO11 Manage Quality • APO12 Manage Risk • APO13 Manage Security • BAI02 Manage Requirements Definition • BAI03 Manage Solution Identification and Build • BAI06 Manage Changes • DSS01 Manage Operations • DSS05 Manage Security Services • DSS06 Manage Business Process Controls 							
A-3.3	<p>Define which Organisational Structures will be in scope.</p> <p>Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of Organisational Structure goals, i.e., decisions • Application of Organisational Structures good practices 	<p>Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail.</p> <table border="1"> <tr> <td>Key Organisational Structures</td><td> <ul style="list-style-type: none"> • Human Resources • Benefits • Training Department </td></tr> <tr> <td>Additional Organisational Structures</td><td> <ul style="list-style-type: none"> • IT Operations • SAP ERP support and maintenance • SAP training • Change Management Office • Finance </td></tr> </table>	Key Organisational Structures	<ul style="list-style-type: none"> • Human Resources • Benefits • Training Department 	Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • SAP ERP support and maintenance • SAP training • Change Management Office • Finance 		
Key Organisational Structures	<ul style="list-style-type: none"> • Human Resources • Benefits • Training Department 							
Additional Organisational Structures	<ul style="list-style-type: none"> • IT Operations • SAP ERP support and maintenance • SAP training • Change Management Office • Finance 							

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle								
Phase A—Determine Scope of the Assurance Initiative								
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment				
A-3.4	<u>Define the Culture, Ethics and Behaviour</u> aspects in scope.	In the context of this engagement, the following enterprise-wide culture and behaviours are in scope: <ul style="list-style-type: none"> • Risk and compliance aware culture • Enabling of continuous improvement • Accountability • Discipline to follow instructions 						
A-3.5	<u>Define the Information items</u> in scope. Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of Information goals, i.e., quality criteria of the information items • Application of Information good practices (Information attributes) 	Based on the subject matter of this audit/assurance program, the following Information items have been identified as key items. <table border="1"> <tr> <td>Key Information Items</td><td> <ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids </td></tr> <tr> <td>Additional Information Items</td><td> <ul style="list-style-type: none"> • Organizational charts </td></tr> </table>	Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 	Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 		
Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 							
Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 							
A-3.6	<u>Define the Services, Infrastructure and Applications</u> in scope.	In the context of this assignment, and taking into account the goals identified in A-2.4, the following services and related applications or infrastructure could be considered in scope of the review: <ul style="list-style-type: none"> • Master data maintenance group • SAP ERP support and maintenance • SAP training • Payroll • Accounting department 						
A-3.7	<u>Define the People, Skills and Competencies</u> in scope. Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of skills set goals • Application of skills set and competencies good practices 	In the context of this engagement, taking into account key processes and key roles, the following skill sets are included in scope: <ul style="list-style-type: none"> • Proficiency using the SAP HR Module • Master data management skills • HR skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 						

Audit/Assurance Program for SAP ERP Human Capital Management Business Cycle																										
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics																										
Ref.	Assurance Steps and Guidance			Issue Cross-reference																						
B-1	Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.																									
B-1.1	<p>Obtain (and agree on) metrics for enterprise goals and expected values of the metrics. Assess whether enterprise goals in scope are achieved.</p> <p>Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.</p> <p>Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</p> <p>The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>Enterprise Goal</th> <th>Metric</th> <th>Expected Outcome (Ex)</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>EG03 Managed business risk (safeguarding of assets)</td> <td> <ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG04 Compliance with externals laws and regulations</td> <td> <ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG07 Business service continuity and availability</td> <td> <ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>EG11 Optimisation of business process functionality</td> <td> <ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities </td> <td></td> <td></td> </tr> <tr> <td>EG15 Compliance with internal policies</td> <td> <ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices </td> <td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>	Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step	EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG04 Compliance with externals laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 			EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step																							
EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																							
EG04 Compliance with externals laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																							
EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																							
EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 																									
EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																							
B-1.2	<p>Obtain (and agree on) metrics for IT-related goals and expected values of the metrics and assess whether IT-related goals in scope are achieved.</p> <p>The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>IT-related Goal</th> <th>Metric</th> <th>Expected Outcome (Ex)</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>ITG01 Alignment of IT and business strategy</td> <td> <ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services </td> <td>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>	IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step	ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																	
IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step																							
ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and services 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																							

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> Percent of IT value drivers mapped to business value drivers 		achieved.	
	ITG02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment Number of non-compliance issues relating to contractual agreements with IT service providers Coverage of compliance assessments 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG04 Managed IT-related business risk	<ul style="list-style-type: none"> Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent of enterprise risk assessments including IT-related risk Frequency of update of risk profile 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG08 Adequate use of applications, information and technology solutions	<ul style="list-style-type: none"> Percent of business process owners satisfied with supporting IT products and services Level of business user understanding of how technology solutions support their processes Satisfaction level of business users with training and user manuals Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG09 IT Agility	<ul style="list-style-type: none"> Level of satisfaction of business executives with IT's responsiveness to new requirements Number of critical business processes supported by up-to-date infrastructure and applications Average time to turn strategic IT objectives into an agreed-on and approved initiative 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	ITG10 Security of information, processing infrastructure and applications	<ul style="list-style-type: none"> Number of security incidents causing financial loss, business disruption or public embarrassment Number of IT services with outstanding security requirements Time to grant, change and remove access privileges, compared to agreed-on service levels 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	ITG12 Enablement and support of business processes by integrating applications and technology into business processes	<ul style="list-style-type: none"> Frequency of security assessment against latest standards and guidelines Number of business processing incidents caused by technology integration errors Number of business process changes that need to be delayed or reworked because of technology integration issues Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues Number of applications or critical infrastructures operating in silos and not integrated 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG14 Availability of reliable and useful information for decision making	<ul style="list-style-type: none"> Level of business user satisfaction with quality and timeliness (or availability) of management information Number of business process incidents caused by non-availability of information Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG15 IT compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices Frequency of policies review and update 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG16 Competent and motivated business and IT personnel	<ul style="list-style-type: none"> Percent of staff whose IT-related skills are sufficient for the competency required for their role Percent of staff satisfied with their IT-related roles Number of learning/training hours per staff member 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-2	Obtain an understanding of the Principles, Policies and Frameworks in scope and set suitable assessment criteria. Assess Principles, Policies and Frameworks.		
Principles, policies and frameworks: Policy for Master Data Maintenance			
B-2.1a	<u>Understand the Principles, Policies and Frameworks context.</u> <i>Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks</i>		
B-2.2a	<u>Understand the stakeholders of the Principles, Policies and Frameworks.</u> <i>Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.</i>		
B-2.3a	<u>Understand the goals for the Principles, Policies and Frameworks</u> , and the related metrics and agree on expected values. Assess whether the Principles, Policies and Frameworks goals (outcomes) are achieved, i.e., assess the effectiveness of the Principles, Policies and Frameworks . Goal: The organization has defined, disseminated and deployed management policies supporting SAP master data maintenance .	Perform the assurance steps using the example criteria described below.	
Goal	Criteria	Assessment Step	
Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.	
Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 	Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 	
Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.	
Availability	<ul style="list-style-type: none"> Policies are available to all stakeholders. Policies are easy to navigate and have a logical and hierarchical structure. 	<ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. 	
B-2.4a	<u>Understand the life cycle stages of the Principles, Policies and Frameworks</u> , and agree on the relevant criteria. Assess to what extent the Principles, Policies and Frameworks life cycle is managed. <i>The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01 Manage the IT management framework.</i>		
B-2.5a	<u>Understand good practices related to the Principles, Policies and Frameworks</u> and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. <i>The assurance professional will, by using appropriate auditing techniques assess the following aspects.</i>		
Good Practice	Criteria	Assessment Step	
Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.	
Exception and escalation	<ul style="list-style-type: none"> The exception and escalation procedure is explained and commonly known. The exception and escalation procedure has not become the de facto standard procedure. 	<ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. Through observation of a representative sample, verify that the exception and escalation procedure has not become <i>de facto</i> standard procedure. 	

Audit/Assurance Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	Compliance	The compliance checking mechanism and non-compliance consequences are clearly described and enforced.	Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.		
B-2.1 to B-2.5	Repeat steps B-2.1 through B-2.5 for all remaining Principles, Policies and Frameworks in scope. Repeat the steps described above for the remaining Principles, Policies and Frameworks: <ul style="list-style-type: none">• ISMS policy• Legal and regulatory compliance requirements• Hiring Policy• Termination Policy				

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-3	Obtain understanding of the Processes in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes.			
SAP ERP HR process²: Personnel Administration				
B-3.1a	<u>Understand the Process context.</u>			
B-3.2a	<u>Understand the Process purpose.</u>			
B-3.3a	<u>Understand</u> all process stakeholders and their roles. This is equivalent to understanding the real RACI chart of the process. <i>Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.</i> The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement: Personnel Administration stakeholders:			
B-3.4a	<u>Understand</u> the Process goals and related metrics ³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process. The Process Personnel Administration has six defined process goal.			The following activities can be performed to assess whether the goals are achieved.
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	
HR master data is valid, complete and accurate.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
HR master data is current and pertinent.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
HR Master data is secure.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
Nonexistent or duplicate employee is not added to payroll.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
Termination dates are accurately reported.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
Employee is deactivated when employment is terminated.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	

² Because this is a business process audit/assurance program, several of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources available.

³ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.5a	<p>Agree on suitable criteria to evaluate all processes in scope of the assurance engagement: Define and agree on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.)</p> <p><u>Agree</u> on the process practices that should be in place (process design). <u>Assess</u> the process design, i.e., assess to what extent:</p> <ul style="list-style-type: none"> • Expected process practices are applied. • Accountability and responsibility are assigned and assumed. <p>COBIT 5 Processes⁴ are described in <i>COBIT 5: Enabling Processes</i>. Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are:</p> <ul style="list-style-type: none"> • A sound process design • The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented. 				
	Reference Process	Personnel Administration	Criteria: 1.1 HR master data are valid, complete and accurate. 1.2 HR master data are current and pertinent. 1.3 HR Master data are secure. 1.4 Nonexistent or duplicate employee is not added to payroll. 1.5 Termination dates are accurately reported. 1.6 Employee is deactivated when employment is terminated.		
	Reference Process Practices ⁵	Good Practice	Assessment Step	Issue Cross-reference	Comment
	DSS01 DSS06	HR master data are valid, complete and accurate.	<p>1.1.1 Use transaction code PSOC—Job Reporting to access the job catalog in the system.</p> <p>Use transaction code PO03—Maintain Job to view jobs in the system. Obtain confirmation and evidence from management that the stored job catalog is reviewed on a regular basis.</p> <p>The SAP ERP HR module must be configured to compare information, such as last name, first name and date of birth, against existing records during the entry of new employees. The option Activate Concurrent Employees for Personnel Administration must be enabled to activate the comparison of new employee information being entered against the existing records, and to prevent duplicate records. Once configured, SAP will, by default, show possible matches against both active and inactive records.</p> <p>To validate use transaction code SPRO to display the IMG menu and follow path: Personnel Management→Personnel Administration→Customizing Procedures→Dynamic Actions, the option Activate Concurrent Employees for Personnel Administration must be enabled.</p> <p>Obtain evidence that HR employees are properly trained to create and maintain employee records.</p>		
	DSS05 DSS06	HR master data are valid, complete and accurate.	1.1.2 Use transaction code S_AHR_61016380 to execute the infotype audit report RPWAUD00 and assess whether changes to sensitive and critical master records (personnel number, start-end		

⁴ For this audit/assurance program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the SAP ERP Human Capital Management Business Cycle processes in scope.

⁵ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Human Capital Management Business Cycle audit/assurance program.

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																
Ref.	Assurance Steps and Guidance			Issue Cross-reference												
		<p>date, date of birth, bank account details, etc.,) have been adequately authorized and are correct.</p> <p>Verify that the system has been configured to provide a sufficient audit trail for changes to key infotypes. Logging changes to infotypes is important for accountability and review for inaccurate or incorrect changes. Use transaction code SE16N—General Table Display to review the following tables and values:</p> <table border="1"> <thead> <tr> <th>Table Name</th><th>Table Field Values</th></tr> </thead> <tbody> <tr> <td rowspan="2">V_T585A— Infotypes With Documents</td><td>A 0001 Organizational Assignment</td></tr> <tr><td>A 0002 Personal Data</td></tr> <tr> <td rowspan="3">V_T585B— Field Group Definition</td><td>0001 Organizational Assignment 01 ABKRS</td></tr> <tr><td>0001 Organizational Assignment 01 WERKS</td></tr> <tr><td>0002 Personal Data 02 GBDAT</td></tr> <tr> <td rowspan="2">V_T585C— Field Group Characteristics</td><td>A 0001 Organizational Assignment 01 S 00</td></tr> <tr><td>A 0002 Personal Data 02 S 00</td></tr> </tbody> </table> <p>Run report RPUAUD00 and check the changes to infotypes, such as IT0001, IT0002 and other applicable infotypes.</p> <p>Refer to testing technique 4.1.1 to test controls related to organizational structure updates.</p>	Table Name	Table Field Values	V_T585A— Infotypes With Documents	A 0001 Organizational Assignment	A 0002 Personal Data	V_T585B— Field Group Definition	0001 Organizational Assignment 01 ABKRS	0001 Organizational Assignment 01 WERKS	0002 Personal Data 02 GBDAT	V_T585C— Field Group Characteristics	A 0001 Organizational Assignment 01 S 00	A 0002 Personal Data 02 S 00		
Table Name	Table Field Values															
V_T585A— Infotypes With Documents	A 0001 Organizational Assignment															
	A 0002 Personal Data															
V_T585B— Field Group Definition	0001 Organizational Assignment 01 ABKRS															
	0001 Organizational Assignment 01 WERKS															
	0002 Personal Data 02 GBDAT															
V_T585C— Field Group Characteristics	A 0001 Organizational Assignment 01 S 00															
	A 0002 Personal Data 02 S 00															
BAI10	HR master data are valid, complete and accurate.	1.1.3 Determine whether data fields are defined in the SAP ERP system as mandatory so that the completeness of each HR master record is maintained correctly. The mandatory fields, which are systematically defined, can be identified via the following steps: 1. Use transaction code PA30—Maintain HR Master Data to obtain a list of available infotypes, and find the infotype for which the mandatory field must be tested. 2. Display the infotype, press F1 on a field and click on the Technical Details button. From the technical information screen that is displayed, make note of the screen number. 3. Use transaction code SPRO to display the IMG menu and follow path: Personnel Management → Personnel Administration → Customizing User Interface → Change Screen Modifications, and select the entries for the screen identified in step 2 to view field status.														
DSS01 DSS06	HR master data are valid, complete and accurate.	1.1.4 Confirm that a subsequent review of new employee details is conducted by an HR supervisor on a periodic basis. Obtain evidence of the review.														
DSS05 DSS06	HR master data are valid, complete and accurate.	1.1.5 Use transaction code SUIM—User Information System to identify users and test access to transaction PA30— Maintain HR Master Data:														
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Transaction(s)</td> <td style="padding: 2px;">Authorization Objects</td> <td style="padding: 2px;">Fields</td> <td style="padding: 2px;">Values</td> </tr> </table>					Transaction(s)	Authorization Objects	Fields	Values								
Transaction(s)	Authorization Objects	Fields	Values													

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																
Ref.	Assurance Steps and Guidance							Issue Cross-reference	Comment							
			PA30—Maintain HR Master Data	P_ORGIN	INFTY	*										
				P_ORGIN	SUBTY	*										
				P_ORGIN	AUTHC	W, M										
				P_ORGIN	PERSA	*										
				P_ORGIN	PERSG	*										
				P_ORGIN	PERSK	*										
				P_ORGIN	VDSK!	*										
DSS06	HR master data are current and pertinent.	1.2.1 Use transaction code S_AHR_61016369 or PAR2—Employee List to generate a system report of all current employees. Use this report to identify duplicate employees or data integrity issues.														
BAI06 DSS05 DSS06	HR master data are current and pertinent.	1.2.2 Refer to testing techniques 1.1.5 and 1.2.3.														
BAI06	HR master data are current and pertinent.	<p>1.2.3 Approvals authorizing HR master data changes should be recorded and retained. For example:</p> <ul style="list-style-type: none"> Approval emails could be stored in hard copy or soft copy. The automated help desk ticketing system can be used to track HR master data changes. <p>Determine the method used to request and document master data change request. Obtain evidence that changes to master data are properly authorized, recorded and stored.</p>														
DSS01 DSS06	HR master data are current and pertinent.	<p>1.2.4 Review the mandatory HR master data of all employees using transaction code S_AHR_61016369 or PAR2—Employee List.</p> <p>Alternatively, from the IMG menu follow the path: Human Resources→Personnel Admin→Info System→Report Selection to select the report to display the complete employee list.</p>														
DSS05 DSS06	HR Master data are secure.	1.3.1 Refer to testing technique 1.1.5														
DSS05 DSS06	HR Master data are secure.	<p>1.3.2 Test authorization checks using transaction code OOAC—HR: Authorization main switch and check the value of AUTSW—ORGIN (the switch is on if the value is 1 and off if the value is 0 for authorization object P_ORGIN). Determine if the switch for the user ID's being tested is appropriate.</p> <p>If P_ORGIN is on, verify that the access mode for the authorization is appropriate: M (matchcode), R (read), S (symmetric), E (enqueue), D (dequeue), W (write) and * (all operations).</p> <p>Use transaction code SUIM—User Information System to test access to transaction code PA30—Maintain HR Master Data, which should be restricted by authorization object P_PERNR and will prevent users from editing their own master records.</p>														
		<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PA30—Maintain HR Master Data</td><td>P_PERNR</td><td>AUTHC</td><td>M, R,S, E, D, W, *</td></tr> </tbody> </table>							Transaction(s)	Authorization Objects	Fields	Values	PA30—Maintain HR Master Data	P_PERNR	AUTHC	M, R,S, E, D, W, *
Transaction(s)	Authorization Objects	Fields	Values													
PA30—Maintain HR Master Data	P_PERNR	AUTHC	M, R,S, E, D, W, *													

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle									
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes									
Ref.	Assurance Steps and Guidance							Issue Cross-reference	Comment
					P_PERNR	PSIGN	I, E		
					P_PERNR	INFTY	*		
					P_PERNR	SUBTY	*		
DSS06	Nonexistent or duplicate employee is not added to payroll.	1.4.1 Refer to testing technique 1.1.1							
DSS01 DSS06	Termination dates are accurately reported.	1.5.1 Backdated termination date notification is an SAP ERP standard feature that can be tested by entering a backdate termination date, while creating a new dummy employee. An error message should appear to recommend entering the current date or a date in the future.							
DSS01 DSS06	Termination dates are accurately reported.	<p>1.5.2 Use transaction code SWDD—Workflow Builder and in the information area, click on the down arrow and type Termination to display the termination workflow. Validate that the workflow has been properly configured to use the standard template and forms (template WS18900010, forms ISR_HRASR_STU1, ISR_HRASR_STU2, ISR_HRASR_STU3 and ISR_HRASR_STU4).</p> <ul style="list-style-type: none"> • The employee starts the termination process in Form STU1. • The personnel officer approves Form STU1. • The manager enters the raw version of reference in Form STU2. • The HR Administrator enters missing data for termination in Form STU3. • The personnel officer checks complete details updated in Form STU4. • The manager and employee receive mail for process completion. 							
DSS01 DSS06	Termination dates are accurately reported.	1.5.3 Confirm that relevant managers verify current employees using system-generated lists of current employees per department, area or cost center. This type of review verifies or helps in detection of employees who have been transferred or terminated and for whom information regarding the transfer or termination has not been recorded in the system.							
DSS01 DSS06	Termination dates are accurately reported.	1.5.4 Confirm that the SAP ERP has been programmed to automatically make changes to the status of employees to terminate at record termination date.							
DSS01 DSS06	Termination dates are accurately reported.	1.5.5 Select a random sample of terminated employees using transaction codes S_L9C_94000095 for headcount changes and S_ALR_87013611 for cost center manager and verify that any termination payment was properly calculated and further payments have not been disbursed.							
DSS01 DSS06	Employee is deactivated when employment is terminated.	<p>1.6.1 Confirm that an individual who does not have access to terminate employees reviews on a periodic basis, the report of terminated employees to check that all termination dates were accurately entered, with reference to termination documentation (e.g., resignation letter). Obtain evidence that discrepancies have been reported and addressed accordingly. The report of terminated employees can be generated by using transaction code PAR2—Employee List with relevant inputs and employment status as 0 or table PA0000 with STAT2 data as 0.</p>							
DSS05	Employee is deactivated when employment is terminated.	<p>1.6.2 Use transaction code PA30 —Maintain HR Master Data or PO13—Maintain Position to ensure that access has been removed from terminated employees based on the roles assigned to the user position previously assigned to the terminated employee.</p> <p>If system access is granted using role-based security, ensure that security personnel have removed access from terminated employees. The report of terminated employees can be generated by using transaction code PAR2—Employee List with relevant inputs and employment status as 0 or table PA0000 with STAT2 data as 0.</p>							

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-3.6a	<u>Agree</u> on the process work products ⁶ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess</u> to what extent the process work products are available. <u>Process Personnel Administration</u> inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			
	Process Practice Personnel Administration		Work Products <ul style="list-style-type: none"> • New Hire Report • Termination report • Employee change report 	Assessment Step Apply appropriate audit techniques to determine the existence and appropriate use of each work product.
	<u>Agree</u> on the process capability level to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>			
SAP ERP HR process: Time Management				
B-3.1b	<u>Understand</u> the Process context .			
B-3.2b	<u>Understand</u> the Process purpose .			
B-3.3b	<u>Understand</u> all process stakeholders and their roles.			
	Time Management stakeholders:			
B-3.4b	<u>Understand</u> the Process goals and related metrics ⁷ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.			
	The Process Time Management has four defined process goals.		The following activities can be performed to assess whether the goals are achieved.	
	Process Goal Accurate, complete and timely entry of employee time data.	Related Metrics <i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	Criteria/Expected Value <i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>
	Unapproved leave or leave is not taken outside of entitlements.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>
	Established employee shifts are updated accurately.	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>
	Time recorded in prior periods is amended accurately and with appropriate	<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>	<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>

⁶ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

⁷ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.5b	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement: Accountability and responsibility are assigned and assumed.				
	Reference Process	Time Management	Criteria: 2.1 Accurate, complete and timely entry of employee time data. 2.2 Unapproved leave or leave is not taken outside of entitlements. 2.3 Established employee shifts are updated accurately. 2.4 Time recorded in prior periods is amended accurately and with appropriate authority.		
	Reference Process Practices ⁸	Good Practice	Assessment Step		Issue Cross-reference
	DSS01 DSS06	Accurate, complete and timely entry of employee time data.	2.1.1 Task TS20000460 (CATS: Approval by superior) gives the supervisor or manager details of an employee as the workflow recipient. It is a standard SAP HR feature workflow. The details of the workflow that are configured, along with the recipient of the time sheet for approval (infotype 0328 is used for time approval), can be observed using transaction code SPRO to display the IMG menu and follow path: CA Cross-application Components → Time Sheet → Setting for All User Interfaces → The Approval Procedure → Workflow for the Time Sheet.		
	BAI10	Accurate, complete and timely entry of employee time data.	2.1.2 Standard enhancement CATS0006 to confirm the time sheet can be viewed by using transaction code CMOD—Enhancements and searching for CATS0006. A manual review of this enhancement should be done to check its functionality. The time management status in the planned working time infotype (0007) in every record for hourly employees should not be set to zero because this will exclude employees from time evaluation.		
	BAI10	Accurate, complete and timely entry of employee time data.	2.1.3 Test the configuration of automatic notifications for time reports due using the CA path: CA Cross-application Components → Time Sheet → Setting for All User Interfaces → The Approval Procedure → Workflow. In the Methods group box, select Method Definitions and choose Display Overview. Select the method CCMS_OnAlert_Email and choose Edit Data. Check whether the details, such as sender, recipient and recipient type ID, are filled in correctly.		
	DSS01	Accurate, complete and timely entry of employee time data.	2.1.4 Review time evaluation reports for missing time after the time reporting deadline using: <ul style="list-style-type: none">• Transaction code PT_EDT_TEDT (ABAP Program name—RPTEDT00) for time statement• Transaction code PT60—Time Evaluation (report RPTIME00—for positive time)• Transaction code PT_QTA00 (RPTQTA00—for negative time) Obtain evidence that follow up with the employee and the employee's immediate supervisor for any discrepancies has been properly affected.		
	DSS01	Unapproved leave or leave is not taken outside of entitlements.	2.2.1 Use transaction code PE03—HR: Features and input the name of the feature that is to be reviewed (LVTYP and/or QUOMO). Under Sub Objects, click on the Decision Tree radio button. Click on the button with the eyeglasses marked Display. A decision tree graphic will be available. Determine whether HR features LVTYP and/or QUOMO have been configured for the country grouping in the scope of the audit according to management's intentions. Identify the personnel subgroups configured for the country grouping in the scope. Use transaction code SPRO to display the IMG menu and follow path: Personnel Time Management → Time Data Recording and Administrations → Absences → Absence Catalog → Define Absence Types. For each personnel group documented in the above step, determine the configuration of the absences types defined in the system. Confirm that absence types exist for personnel groups and are consistent with management's intentions.		
	BAI10	Unapproved leave or leave	2.2.2 Follow the path to generate an absence report: Human Resources → Time Management →		

⁸ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Human Capital Management Business Cycle audit/assurance program.

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle																									
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																									
Ref.	Assurance Steps and Guidance			Issue Cross-reference																					
				Comment																					
	DSS6	is not taken outside of entitlements.	Administration → Information Systems → Report Selection → Absence → Absence Data Overview or use transaction code PT64—Absence List (the absence report can be generated for any time period by providing the time period range). Review the logs maintained for this activity performed by any HR personnel.																						
	BAI10 DSS01	Unapproved leave or leave is not taken outside of entitlements.	<p>2.2.3 Review the leave framework using transaction code PTARQ—Test Environment for Leave Request.</p> <p>Review the workflow for leave types following the path: PTARQ → Customizing → Employee Self-service → Service-specific Settings → Working Time → Leave Request → Processing Processes → Specify Processing Processes for Types of Leave → Define Absences/Processing Processes.</p> <p>Observe whether a rule exists or not in the workflow by observing the path followed by the leave request.</p>																						
	DSS05 DSS06	Established employee shifts are updated accurately.	<p>2.3.1 Work schedules are recorded in infotype 1011. Use transaction code SUIM—User Information System to test access to key transaction codes, such as PA61—Maintain Time Data. Use of authorization object P_PERNR should be incorporated into the user's security so that no employee has access to update his/her own standard work roster.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="4">PA61—Maintain Time Data</td><td>P_PERNR</td><td>AUTHC</td><td>M, R, S, E, D, W, *</td></tr> <tr> <td>P_PERNR</td><td>PSIGN</td><td>I, E</td></tr> <tr> <td>P_PERNR</td><td>INFTY</td><td>0007, *</td></tr> <tr> <td>P_PERNR</td><td>SUBTY</td><td>*</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	PA61—Maintain Time Data	P_PERNR	AUTHC	M, R, S, E, D, W, *	P_PERNR	PSIGN	I, E	P_PERNR	INFTY	0007, *	P_PERNR	SUBTY	*					
Transaction(s)	Authorization Objects	Fields	Values																						
PA61—Maintain Time Data	P_PERNR	AUTHC	M, R, S, E, D, W, *																						
	P_PERNR	PSIGN	I, E																						
	P_PERNR	INFTY	0007, *																						
	P_PERNR	SUBTY	*																						
	DSS05 DSS06	Established employee shifts are updated accurately.	2.3.2 Confirm that employee shifts can only be updated in the system following approval by an appropriate authority. Obtain evidence that a record of all approval requests (hard copy or soft copy) is kept as reference.																						
	DSS05	Time recorded in prior periods is amended accurately and with appropriate authority.	<p>2.4.1 Use transaction code SUIM—User Information System to test access to transactions PAUX and PC00_M99_PA03_CORR as follows.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="4">PAUX—Adjustment Workbench</td><td>P_PERNR</td><td>AUTHC</td><td>W,S,D,E</td></tr> <tr> <td>P_PERNR</td><td>PSIGN</td><td>E</td></tr> <tr> <td>P_PERNR</td><td>INFTY</td><td>0007</td></tr> <tr> <td>P_PERNR</td><td>SUBTY</td><td>*</td></tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> </table>	Transaction(s)	Authorization Objects	Fields	Values	PAUX—Adjustment Workbench	P_PERNR	AUTHC	W,S,D,E	P_PERNR	PSIGN	E	P_PERNR	INFTY	0007	P_PERNR	SUBTY	*	Transaction(s)	Authorization Objects	Fields	Values	
Transaction(s)	Authorization Objects	Fields	Values																						
PAUX—Adjustment Workbench	P_PERNR	AUTHC	W,S,D,E																						
	P_PERNR	PSIGN	E																						
	P_PERNR	INFTY	0007																						
	P_PERNR	SUBTY	*																						
Transaction(s)	Authorization Objects	Fields	Values																						

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle																					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																					
Ref.	Assurance Steps and Guidance							Issue Cross-reference	Comment												
			PC00_M99_PA03_CORR—Corrections	P_TCODE	TCD	PC00_M99_PA03_CORR															
	DSS05	Time recorded in prior periods is amended accurately and with appropriate authority.	2.4.2 Refer to testing technique 2.4.1																		
	BAI10	Time recorded in prior periods is amended accurately and with appropriate authority.	2.4.3 Use transaction code PUOC_13—Off-cycle Workbench Australia to generate a report that lists all prior-period adjustments processed on a monthly basis. Determine whether this report has been reviewed by the HR administrator to determine the appropriateness of adjustments processed.																		
	DSS01 DSS05	Time recorded in prior periods is amended accurately and with appropriate authority.	2.4.4 Determine whether the enterprise decided to create the authorization group, and if the group requested a list of employees restricted from that authorization group. Use transaction code SUI User Information System to test access as follows.																		
			<table border="1"> <thead> <tr> <th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>S_TABU_DIS</td><td>ACTVT</td><td>02</td></tr> <tr> <td></td><td>DICBERCLS</td><td></td></tr> <tr> <td></td><td colspan="2">Authorization group associated with table CATSDB</td></tr> </tbody> </table>							Authorization Objects	Fields	Values	S_TABU_DIS	ACTVT	02		DICBERCLS			Authorization group associated with table CATSDB	
Authorization Objects	Fields	Values																			
S_TABU_DIS	ACTVT	02																			
	DICBERCLS																				
	Authorization group associated with table CATSDB																				
B-3.6b	<u>Agree</u> on the process work products ⁹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.																				
	Process Time Management inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.					Criteria: All listed work products should demonstrably exist and be used.															
	Process Practice		Work Products			Assessment Step															
	Time Management		<ul style="list-style-type: none"> • Time summary report • Time variance report based on hours scheduled versus hours worked 			Apply appropriate audit techniques to determine the existence and appropriate use of each work product.															
B-3.7b	<u>Agree</u> on the process capability level to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>																				
SAP ERP HR process: Payroll Management																					
B-3.1c	<u>Understand</u> the Process context .																				
B-3.2c	<u>Understand</u> the Process purpose .																				
B-3.3c	<u>Understand</u> all process stakeholders and their roles.																				
	Payroll Management stakeholders:																				
B-3.4c	<u>Understand</u> the Process goals and related metrics ¹⁰ and define expected Process values (criteria), and assess whether the Process goals are achieved,																				

⁹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
The Process Time management has ten defined process goal. Process Goal	i.e., assess the effectiveness of the process.		The following activities can be performed to assess whether the goals are achieved.		
	Related Metrics		Criteria/Expected Value		
	Payroll calculation is accurate and complete.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Employee wages paid in foreign currency are calculated correctly.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Leave accrual rates are established accurately.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Statutory obligations for payment of taxation are not breached.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Salary sacrifice arrangements are appropriately managed.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Methodology for performance payment is established.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Employee benefits are managed and administered in accordance with employee agreements.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Payroll system reconciles to the GL.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	

¹⁰ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.5c	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:				
	Reference Process	Payroll Management	Criteria: 3.1 Payroll calculation is accurate and complete. 3.2 Employee wages paid in foreign currency are calculated correctly. 3.3 Leave accrual rates are established accurately. 3.4 Statutory obligations for payment of taxation are not breached. 3.5 Salary sacrifice arrangements are appropriately managed. 3.6 Methodology for performance payment is established. 3.7 Employee benefits are managed and administered in accordance with employee agreements. 3.8 Payroll system reconciles to the GL. 3.9 Executive payroll is adequately segregated. 3.10 Correct electronic funds transfer EFT payments.		
	Reference Process Practices ¹¹	Good Practice	Assessment Step	Issue Cross-reference	Comment
	DSS01	Payroll calculation is accurate and complete.	3.1.1 Review system logs to determine if the HR administration team conducts a test before posting payroll to the GL.		
	DSS01 DSS06	Payroll calculation is accurate and complete.	3.1.2 Review payroll results that have not posted to the GL using transaction code PC00_M19_CIPC to view unposted payroll results. Obtain evidence that management uses the report to address any unposted payroll results.		
	DSS01 DSS06	Payroll calculation is accurate and complete.	3.1.3 Confirm that management reviews periodically report RPUAUD00 at a minimum for sensitive infotypes such as 1005 (planned compensation), 0007 (planned working time), 0008 (basic pay), 0016 (contract elements), 2006 (absence quotas). Note: Infotypes for this test are determined by the modules used (time, compensation, benefits, performance management, sales incentives, etc.).		
	BAI10 DSS06	Payroll calculation is accurate and complete.	3.1.4 Confirm with the process owner whether any standard forms are used for <i>ad hoc</i> pay changes. If standard forms are used, obtain a sample of approvals for <i>ad hoc</i> pay changes.		
	DSS05	Payroll calculation is accurate and complete.	3.1.5 Use transaction code SUIM—User Information System to test access to transaction codes PUOC_10—Off-Cycle Workbench USA and PC00_M99_CALC—International Payroll.		
	BAI10	Payroll calculation is accurate and complete.	3.1.6 Use transaction code PE03—HR: Features and input the name of the feature that is to be reviewed (ABKRS—payroll area). Under Sub Objects, click on the Decision Tree radio button. Click on the button with the eyeglasses marked Display. A decision tree graphic will be available. Determine the payroll areas that are currently in use at the enterprise. Use transaction code SPRO to display the IMG menu and follow path: Payroll → Payroll: USA Basic Settings → Payroll Organization → Assign New Payroll Accounting Areas to Period Modifier. Select Create Control Record, and determine the payroll accounting areas configuration used by the enterprise. Determine whether the payroll accounting area and associated control record are configured in ABKRS according to management's intentions.		
	BAI06 BAI10 DSS05	Payroll calculation is accurate and complete.	3.1.7 Use transaction code SUIM—User Information System to test access to transaction codes PE01 (Maintain Payroll Schemas), PE01N (Editor for Payroll Schemas), PE02 (Maintain Calculation Rules), PE02N (Editor for PC Rules) and PE04 (Create Functions and Operations) as follows:		

¹¹ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Human Capital Management audit/assurance program.

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle																																										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																										
Ref.	Assurance Steps and Guidance					Issue Cross-reference	Comment																																			
			<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PE01— Maintain Payroll Schemas, PE01N— Editor for Payroll Schemas</td><td>P_PCLX</td><td>AUTHC</td><td>U</td></tr> <tr> <td></td><td>P_PCLX</td><td>RELID</td><td>PS</td></tr> <tr> <td>PE02— Maintain Calculation Rules PE02N— Editor for PC Rules</td><td>P_TCODE</td><td>TCD</td><td>PE02</td></tr> <tr> <td>PE04— Create Functions and Operations</td><td>P_TCODE</td><td>TCD</td><td>PE04</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	PE01— Maintain Payroll Schemas, PE01N— Editor for Payroll Schemas	P_PCLX	AUTHC	U		P_PCLX	RELID	PS	PE02— Maintain Calculation Rules PE02N— Editor for PC Rules	P_TCODE	TCD	PE02	PE04— Create Functions and Operations	P_TCODE	TCD	PE04																			
Transaction(s)	Authorization Objects	Fields	Values																																							
PE01— Maintain Payroll Schemas, PE01N— Editor for Payroll Schemas	P_PCLX	AUTHC	U																																							
	P_PCLX	RELID	PS																																							
PE02— Maintain Calculation Rules PE02N— Editor for PC Rules	P_TCODE	TCD	PE02																																							
PE04— Create Functions and Operations	P_TCODE	TCD	PE04																																							
BAI10 DSS01	Employee wages paid in foreign currency are calculated correctly.	3.2.1 Use transaction code SE38 and report RPUEMUXX—Change in Payroll Currency and Conversion of Amounts and determine whether the currency mentioned is appropriate or not.																																								
BAI10 DSS01 DSS05	Leave accrual rates are established accurately.	<p>3.3.1 Check whether the rule exists to stop accruing leave once the maximum amount has been reached by following the path: Time Management → Time Evaluation → Time Evaluation Settings → Set Personnel Area Groupings for Time Recording.</p> <p>If the rule exists, verify that the system stops accruing further leaves using testing data. Infotypes, such as absence quotas (2006), planned working time (0007), basic pay (0008) and contract elements (0016) must be used to enable accurate calculation of leave accruals.</p> <p>Use transaction code SUIM—User Information System to test access to update the rule and transaction code PT_BPC10 as follows.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PT_BPC10—Leave Accrual and Quota Deduction</td><td>P_PERNR</td><td>AUTHC</td><td>R,M</td></tr> <tr> <td></td><td>P_PERNR</td><td>PSIGN</td><td>I</td></tr> <tr> <td></td><td>P_PERNR</td><td>INFTY</td><td>*</td></tr> <tr> <td></td><td>P_PERNR</td><td>SUBTY</td><td>*</td></tr> <tr> <td></td><td>P_PERNR</td><td>AUTHC</td><td>W,S,D,E</td></tr> <tr> <td></td><td>P_PERNR</td><td>PSIGN</td><td>E</td></tr> <tr> <td></td><td>P_PERNR</td><td>INFTY</td><td>0007, 0008, 0016, 2006</td></tr> <tr> <td></td><td>P_PERNR</td><td>SUBTY</td><td>*</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	PT_BPC10—Leave Accrual and Quota Deduction	P_PERNR	AUTHC	R,M		P_PERNR	PSIGN	I		P_PERNR	INFTY	*		P_PERNR	SUBTY	*		P_PERNR	AUTHC	W,S,D,E		P_PERNR	PSIGN	E		P_PERNR	INFTY	0007, 0008, 0016, 2006		P_PERNR	SUBTY	*				
Transaction(s)	Authorization Objects	Fields	Values																																							
PT_BPC10—Leave Accrual and Quota Deduction	P_PERNR	AUTHC	R,M																																							
	P_PERNR	PSIGN	I																																							
	P_PERNR	INFTY	*																																							
	P_PERNR	SUBTY	*																																							
	P_PERNR	AUTHC	W,S,D,E																																							
	P_PERNR	PSIGN	E																																							
	P_PERNR	INFTY	0007, 0008, 0016, 2006																																							
	P_PERNR	SUBTY	*																																							
DSS01 DSS06	Leave accrual rates are established accurately.	3.3.2 Transaction code PT_QTA00—Generate Absence Quotas is used to generate the absence quotas for the employee's infotype IT2006 for a given period. The user normally enters the																																								

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle																																											
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference																																							
				Comment																																							
			<p>start date and end date only to determine the interval to which the absence entitlements shall be generated. Managers should review this report to identify excessive or negative balances. The report RPILVA00 (leave accruals) can be used to manually review employee leave accruals. The review should be performed by cost center managers to assess for reasonableness against known periods of leave, which employees have taken. A further review should be performed by HR to identify any excessive or negative balances.</p>																																								
DSS01 DSS06	Statutory obligations for payment of taxation are not breached.	3.4.1 The amount of fringe benefit tax (FBT) payable is self-assessed by the entity. Prior to lodgment of the annual FBT return, a detailed review should be undertaken by an appropriate person to determine: <ul style="list-style-type: none"> • Confirmation that a fringe benefit that has been provided is accurate • Where a fringe benefit has been provided, the applicable rates and thresholds have been accurately applied in the calculation outlined within the return. Test the process to approve of the FBT calculation by selecting a sample of FBT calculation approval details.																																									
DSS01 DSS06	Statutory obligations for payment of taxation are not breached.	3.4.2 Payroll should be configured to reflect country-specific requirements. The bank details and postal code are checked for further system validation. <p>Use transaction code SPRO to display the IMG menu and follow path: General Settings → Set Countries → Set Country Specific Checks. Select the Country Code used and determine whether the bank details and postal code are checked for further system validation.</p>																																									
BAI10 DSS01 DSS06	Salary sacrifice arrangements are appropriately managed.	3.5.1 Access to maintain employee salary sacrifice is granted using transaction code PA30—Maintain HR Master Data and access to infotype 0008 (basic pay) and 0589 (reimbursements). Use transaction code SUIM—User Information System to test as follows. <table border="1" data-bbox="792 946 1584 1460"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td rowspan="7">PA30— Maintain HR Master Data (Modify)</td> <td>P_ORGIN</td> <td>INFTY</td> <td>0014</td> </tr> <tr> <td>P_ORGIN</td> <td>SUBTY</td> <td>*</td> </tr> <tr> <td>P_ORGIN</td> <td>AUTHC</td> <td>W, M</td> </tr> <tr> <td>P_ORGIN</td> <td>PERSA</td> <td>*</td> </tr> <tr> <td>P_ORGIN</td> <td>PERSG</td> <td>*</td> </tr> <tr> <td>P_ORGIN</td> <td>PERSK</td> <td>*</td> </tr> <tr> <td>P_ORGIN</td> <td>VDSK!</td> <td>*</td> </tr> <tr> <td rowspan="4">PA20—Display HR Master Data (View)</td> <td>P_ORGIN</td> <td>INFTY</td> <td>0014</td> </tr> <tr> <td>P_ORGIN</td> <td>SUBTY</td> <td>*</td> </tr> <tr> <td>P_ORGIN</td> <td>AUTHC</td> <td>R, M</td> </tr> <tr> <td>P_ORGIN</td> <td>PERSA</td> <td>*</td> </tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	PA30— Maintain HR Master Data (Modify)	P_ORGIN	INFTY	0014	P_ORGIN	SUBTY	*	P_ORGIN	AUTHC	W, M	P_ORGIN	PERSA	*	P_ORGIN	PERSG	*	P_ORGIN	PERSK	*	P_ORGIN	VDSK!	*	PA20—Display HR Master Data (View)	P_ORGIN	INFTY	0014	P_ORGIN	SUBTY	*	P_ORGIN	AUTHC	R, M	P_ORGIN	PERSA	*		
Transaction(s)	Authorization Objects	Fields	Values																																								
PA30— Maintain HR Master Data (Modify)	P_ORGIN	INFTY	0014																																								
	P_ORGIN	SUBTY	*																																								
	P_ORGIN	AUTHC	W, M																																								
	P_ORGIN	PERSA	*																																								
	P_ORGIN	PERSG	*																																								
	P_ORGIN	PERSK	*																																								
	P_ORGIN	VDSK!	*																																								
PA20—Display HR Master Data (View)	P_ORGIN	INFTY	0014																																								
	P_ORGIN	SUBTY	*																																								
	P_ORGIN	AUTHC	R, M																																								
	P_ORGIN	PERSA	*																																								

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle																																			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																			
Ref.	Assurance Steps and Guidance							Issue Cross-reference	Comment																										
				P_ORGIN	PERSG	*																													
				P_ORGIN	PERSK	*																													
				P_ORGIN	AUTHC	*																													
BAI10 DSS01 DSS05	Salary sacrifice arrangements are appropriately managed.	3.5.2 The information about the salary structure of employees from the SAP system can be obtained by going to transaction code S_AHR_61015608. This audit log should mention the number of entries checked and the number of discrepancies found. A team of HR personnel should manually review and retain an audit log. Select a sample of employees and check the log details for them to determine if data is accurate. Discuss any discrepancies with management and find the root cause.																																	
BAI10 DSS01	Methodology for performance payment is established.	3.6.1 Access to edit infotype 0015 should be properly restricted to appropriate personnel only. Use transaction code SUIM—User Information System to test access as follows.	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="7">PA30— Maintain HR Master Data (Modify)</td><td>P_ORGIN</td><td>INFTY</td><td>0015</td></tr> <tr> <td>P_ORGIN</td><td>SUBTY</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>AUTHC</td><td>W, M</td></tr> <tr> <td>P_ORGIN</td><td>PERSA</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSG</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSK</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>VDSK!</td><td>*</td></tr> </tbody> </table>							Transaction(s)	Authorization Objects	Fields	Values	PA30— Maintain HR Master Data (Modify)	P_ORGIN	INFTY	0015	P_ORGIN	SUBTY	*	P_ORGIN	AUTHC	W, M	P_ORGIN	PERSA	*	P_ORGIN	PERSG	*	P_ORGIN	PERSK	*	P_ORGIN	VDSK!	*
Transaction(s)	Authorization Objects	Fields	Values																																
PA30— Maintain HR Master Data (Modify)	P_ORGIN	INFTY	0015																																
	P_ORGIN	SUBTY	*																																
	P_ORGIN	AUTHC	W, M																																
	P_ORGIN	PERSA	*																																
	P_ORGIN	PERSG	*																																
	P_ORGIN	PERSK	*																																
	P_ORGIN	VDSK!	*																																
DSS05	Employee benefits are managed and administered in accordance with employee agreements.	3.7.1 Benefits are entered via transaction code HRBEN0001—Enrollment in the relevant benefit infotype for the employee in SAP. Access to this transaction must be restricted to authorized users only (HR administration team). Use transaction code SUIM—User Information System to test access as follows:	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="6">HRBEN0001—Enrollment</td><td>P_ORGIN</td><td>INFTY</td><td>0014</td></tr> <tr> <td>P_ORGIN</td><td>SUBTY</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>AUTHC</td><td>W, M</td></tr> <tr> <td>P_ORGIN</td><td>PERSA</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSG</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSK</td><td>*</td></tr> </tbody> </table>							Transaction(s)	Authorization Objects	Fields	Values	HRBEN0001—Enrollment	P_ORGIN	INFTY	0014	P_ORGIN	SUBTY	*	P_ORGIN	AUTHC	W, M	P_ORGIN	PERSA	*	P_ORGIN	PERSG	*	P_ORGIN	PERSK	*			
Transaction(s)	Authorization Objects	Fields	Values																																
HRBEN0001—Enrollment	P_ORGIN	INFTY	0014																																
	P_ORGIN	SUBTY	*																																
	P_ORGIN	AUTHC	W, M																																
	P_ORGIN	PERSA	*																																
	P_ORGIN	PERSG	*																																
	P_ORGIN	PERSK	*																																

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle																			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																			
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment											
				P_ORGIN	VDSK!	*													
DSS01 DSS06	Employee benefits are managed and administered in accordance with employee agreements.	3.7.2 Transaction code SE16—Data Browser, SM30—Call View Maintenance and SM31—Call View Maintenance, which can provide access to payroll tables, should be restricted using authorization object S_TABU_DIS. Use transaction code SUIM—User Information System to test access as follows	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SM30— Call View Maintenance, SM31— Call View Maintenance</td><td>S_TABU_DIS</td><td>ACTVT</td><td>02</td></tr> <tr> <td>SM30— Call View Maintenance, SM31— Call View Maintenance</td><td>S_TABU_DIS</td><td>DICBERCLS</td><td>Authorization group associated with tables (T52CO, T501 and T001P)</td></tr> </tbody> </table> <p>Testing technique 3.7.1 addresses access to transaction code HRBEN0001—Enrollment.</p>				Transaction(s)	Authorization Objects	Fields	Values	SM30— Call View Maintenance, SM31— Call View Maintenance	S_TABU_DIS	ACTVT	02	SM30— Call View Maintenance, SM31— Call View Maintenance	S_TABU_DIS	DICBERCLS	Authorization group associated with tables (T52CO, T501 and T001P)	
Transaction(s)	Authorization Objects	Fields	Values																
SM30— Call View Maintenance, SM31— Call View Maintenance	S_TABU_DIS	ACTVT	02																
SM30— Call View Maintenance, SM31— Call View Maintenance	S_TABU_DIS	DICBERCLS	Authorization group associated with tables (T52CO, T501 and T001P)																
DSS01 DSS06	Payroll system reconciles to the GL.	3.8.1 Obtain confirmation that The Posting to Accounting: Payroll Results Not Posted report via transaction PC00_M99_PA03_CHECK is reviewed on a regular basis. Any payroll results not posted are actioned in a timely manner. Take a sample of results not posted and confirm that all were addressed before the next pay cycle.																	
DSS01 DSS06	Payroll system reconciles to the GL.	3.8.2 Review key exception-based reports to identify exceptions in payroll processing. Use transaction code SA38 and review the following reports: RPCLJNU0 (payroll journal) RPURECG0 (run-to-run reconciliation report) RPCEDT00 (payroll exceptions) RPUAUD00 (logged changes in infotype data) Verify that the HR administration team reviews exception reports to identify and errors in a timely manner. Select a sample of reports and determine whether the process is working effectively																	
DSS05	Payroll system reconciles to the GL.	3.8.3 Refer to testing technique 3.8.2. Other useful reports to review prior to finalization of the payroll include: <ul style="list-style-type: none"> • Transaction code S_ALR_87013611 should be reviewed by cost center managers to identify significant irregularities in payroll actual to budgeted costs • The infotype audit report RPUAUD00, which can be accessed by transaction code S_AHR_61016380, enables the review of employee changes, including new employees, terminated employees and transfers. The report can be reviewed to ensure that only current and valid employees are included in the pay run. • Run-to-run reconciliation report RPURECG0 (transaction code SE38) enables the 																	

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle																										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																										
Ref.	Assurance Steps and Guidance			Issue Cross-reference																						
		identification of unusual payroll results that differ from previous payrolls. Select a sample of reports and determine if the appropriate personnel reviews them as necessary to identify and correct errors.																								
DSS05	Executive payroll is adequately segregated.	3.9.1 Use transaction code SE16—Data Browser to confirm that only authorized employees have access to authorization object P_ORIGIN with field PERSK (Employee sub group) set for levels 01 (officers), 02 (VP) and 03 (directors). Note: Sub group 03 is not always considered executive.																								
DSS05	Executive payroll is adequately segregated.	3.9.2 Use transaction code SUIM—User Information System to test access to the following transaction codes to identify users who can execute payroll: <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="2">PU03—Change Payroll Status</td><td>P_TCODE</td><td>TCD</td><td>PU03</td></tr> <tr> <td>P_ORGIN</td><td>AUTHC</td><td>S, E, W</td></tr> <tr> <td>PU01— Delete current payroll result</td><td>P_PCLX</td><td>AUTHC</td><td>U</td></tr> <tr> <td rowspan="2">PA03—Maintain Personnel Control Record</td><td>P_TCODE</td><td>TCD</td><td>PA03</td></tr> <tr> <td>P_PCR</td><td>ACTVT</td><td>01, 02, 06</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	PU03—Change Payroll Status	P_TCODE	TCD	PU03	P_ORGIN	AUTHC	S, E, W	PU01— Delete current payroll result	P_PCLX	AUTHC	U	PA03—Maintain Personnel Control Record	P_TCODE	TCD	PA03	P_PCR	ACTVT	01, 02, 06		
Transaction(s)	Authorization Objects	Fields	Values																							
PU03—Change Payroll Status	P_TCODE	TCD	PU03																							
	P_ORGIN	AUTHC	S, E, W																							
PU01— Delete current payroll result	P_PCLX	AUTHC	U																							
PA03—Maintain Personnel Control Record	P_TCODE	TCD	PA03																							
	P_PCR	ACTVT	01, 02, 06																							
DSS01 DSS06	Correct electronic funds transfer EFT payments.	3.10.1 Security of EFT is related to the technology used to interface with the bank. If an XML file or EDIFACT message is used, the auditor needs to view that the secure channel was used to transfer the file and that the file was transferred to a secure storage where it was picked up by the bank application. This type of configuration is called asynchronous. If a middle application was used (e.g., SAP PI) the auditor needs to confirm that valid Banking Adapters were used to set the connection between SAP HCM and the banking application. This type of configuration is called synchronous. Usually, that means that if not processed correctly, the banking system will send a notification through SAP PI to the system administrator and an official within HR. The system administrator must coordinate with HR and, after the mistake is fixed, will need to reexecute the load manually. Select a sample of exception reports and confirm that processing errors have been identified and corrected in timely manner.																								
B-3.6c	<u>Agree on the process work products</u> ¹² (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess to what extent the process work products are available.</u>																									
	Process Payroll Management inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.																						
Process Practice		Work Products	Assessment Step																							
Payroll Management		• Payroll Summary Report • Payroll Detail Report	Apply appropriate audit techniques to determine the existence and appropriate use of																							

¹² For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: *Enabling Processes*.

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle							
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes							
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment	
B-3.7c	<ul style="list-style-type: none"> • Payroll Variance Report 		each work product.				
	<p>Agree on the process capability level to be achieved by the process.</p> <p>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</p>						
SAP ERP HR process: Organizational Management							
B-3.1d	Understand the Process context .						
B-3.2d	Understand the Process purpose .						
B-3.3d	Understand all process stakeholders and their roles.						
Organizational Management risk stakeholders:							
B-3.4d	<p>Understand the Process goals and related metrics¹³ and define expected Process values (criteria), and assess whether the Process goals are achieved, i.e., assess the effectiveness of the process.</p> <p>The Process Organizational Management has five defined process goals.</p>						
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step			
	Organizational chart in SAP HCM accurately reflects current employees and their positions	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
	Organizational chart is set up according to relationships between employees, positions, organizational units and work centers.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
	Job catalog is defined and configured correctly.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
	Positions created/maintained are valid and assigned correct relationship	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
	Integration between Personnel Administration and Personnel Development is set up correctly.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.			
B-3.5d	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:						
	Reference Process	Organizational Management	Criteria: 4.1 Organizational chart in SAP HCM accurately reflects current employees and their positions. 4.2 Organizational chart is set up according to relationships between employees, positions, organizational units and work centers. 4.3 Job catalog is defined and configured correctly. 4.4 Positions created/maintained are valid and assigned correct relationship attributes. 4.5 Integration between Personnel Administration and Personnel Development is set up correctly.				
	Reference	Good Practice	Assessment Step		Issue	Comment	

¹³ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle																																																					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																																					
Ref.	Assurance Steps and Guidance				Issue Cross-reference																																																
Process Practices ¹⁴					Cross-reference																																																
BAI06 DSS05	Organizational chart in SAP HCM accurately reflects current employees and their positions.	<p>4.1.1 The organizational structure can be updated or changed by transaction codes PPOM and PPOM_OLD. Unauthorized personnel should not have access to these transaction codes. Use transaction code SUIM—User Information System to test access to maintain the organizational chart as follows.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="7">PPOM—Maintain Organizational Plan</td><td>P_ORGIN</td><td>INFTY</td><td>0001</td></tr> <tr> <td>P_ORGIN</td><td>SUBTY</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>AUTHC</td><td>W, M</td></tr> <tr> <td>P_ORGIN</td><td>PERSA</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSG</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSK</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>VDSK!</td><td>*</td></tr> <tr> <td rowspan="7">PPOM_OLD—Maintain Organizational Plan</td><td>P_ORGIN</td><td>INFTY</td><td>0001</td></tr> <tr> <td>P_ORGIN</td><td>SUBTY</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>AUTHC</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSA</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSG</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>PERSK</td><td>*</td></tr> <tr> <td>P_ORGIN</td><td>VDSK!</td><td>*</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	PPOM—Maintain Organizational Plan	P_ORGIN	INFTY	0001	P_ORGIN	SUBTY	*	P_ORGIN	AUTHC	W, M	P_ORGIN	PERSA	*	P_ORGIN	PERSG	*	P_ORGIN	PERSK	*	P_ORGIN	VDSK!	*	PPOM_OLD—Maintain Organizational Plan	P_ORGIN	INFTY	0001	P_ORGIN	SUBTY	*	P_ORGIN	AUTHC	*	P_ORGIN	PERSA	*	P_ORGIN	PERSG	*	P_ORGIN	PERSK	*	P_ORGIN	VDSK!	*			
Transaction(s)	Authorization Objects	Fields	Values																																																		
PPOM—Maintain Organizational Plan	P_ORGIN	INFTY	0001																																																		
	P_ORGIN	SUBTY	*																																																		
	P_ORGIN	AUTHC	W, M																																																		
	P_ORGIN	PERSA	*																																																		
	P_ORGIN	PERSG	*																																																		
	P_ORGIN	PERSK	*																																																		
	P_ORGIN	VDSK!	*																																																		
PPOM_OLD—Maintain Organizational Plan	P_ORGIN	INFTY	0001																																																		
	P_ORGIN	SUBTY	*																																																		
	P_ORGIN	AUTHC	*																																																		
	P_ORGIN	PERSA	*																																																		
	P_ORGIN	PERSG	*																																																		
	P_ORGIN	PERSK	*																																																		
	P_ORGIN	VDSK!	*																																																		
DSS01 DSS06	Organizational chart is set up according to relationships between employees, positions, organizational units and work centers.	<p>4.2.1 Use transaction code S_AHR_61016512—Report Structure Without Persons and/or S_AHR_61016513—Report Structure With Persons to access the hierarchy structure stored in the SAP HR system. Obtain confirmation from management that the stored organizational chart is correct.</p>																																																			
BAI10 DSS06	Organizational chart is set up according to relationships between employees, positions, organizational units and work centers.	<p>4.2.2 Review the organizational structure for accuracy. Transaction code OOOE—Use Overview of Organizational Units or Use transaction code SPRO to display the IMG menu and follow the path: Personnel Management → Organizational Management → Edit Organizational Plan. The following objects are required to access.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> </table>	Transaction(s)	Authorization Objects	Fields	Values																																															
Transaction(s)	Authorization Objects	Fields	Values																																																		

¹⁴ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Human Capital Management Business Cycle audit/assurance program.

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle																					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																					
Ref.	Assurance Steps and Guidance							Issue Cross-reference	Comment												
				OOOE— Use Overview of Organizational Units		P_TCODE	TCD	*													
	DSS01 DSS06	Job catalog is defined and configured correctly.	4.3.1 Use transaction code PSOC—Job Reporting to access the job catalog stored and transaction code PO03—Maintain Job to view system configuration. Obtain confirmation from management that the stored job catalog is reviewed on a regular basis.																		
	DSS01 DSS06	Positions created/maintained are valid and assigned correct relationship attributes.	4.4.1 View the relationships configuration using menu path: Human Resources → Organizational Management → Detailed Maintenance → Organizational Unit → Active status → Relationships → Overview and confirm with management the relationships have been configured accurately. Use transaction code SUIM—User Information System to test user access to transaction code PP01—Maintain Plan Date (Menu Guided) as follows.																		
			<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PP01— Maintain Plan Date</td><td>P_TCODE</td><td>TCD</td><td>*</td></tr> <tr> <td></td><td>S_TCODE</td><td>TCD</td><td>*</td></tr> </tbody> </table>				Transaction(s)	Authorization Objects	Fields	Values	PP01— Maintain Plan Date	P_TCODE	TCD	*		S_TCODE	TCD	*			
Transaction(s)	Authorization Objects	Fields	Values																		
PP01— Maintain Plan Date	P_TCODE	TCD	*																		
	S_TCODE	TCD	*																		
	DSS01 DSS06	Integration between Personnel Administration and Personnel Development is set up correctly.	4.5.1 Download Scales, Qualification Catalog and Careers configured in the system using transaction codes PPQD—Qualifications, PPCP—Career and PPSP—Succession or structure code PMQDY. Obtain review sign-off on qualifications, profiles and decay meter on a regular basis. Confirm that data in the system and in the required documentation match. Note: Prior to version 4.6, personnel management and personnel planning and development were separate submodules.																		
B-3.6d	<u>Agree</u> on the process work products ¹⁵ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess</u> to what extent the process work products are available.																				
	Organizational Management inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.					Criteria: All listed work products should demonstrably exist and be used.															
	Process Practice Organizational Management		Work Products <ul style="list-style-type: none"> Organizational chart Employee list by department 		Assessment Step Apply appropriate audit techniques to determine the existence and appropriate use of each work product.																
B-3.7d	<u>Agree</u> on the process capability level to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>																				
SAP ERP HR process: Travel Management																					
B-3.1e	<u>Understand</u> the Process context .																				

¹⁵ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment
B-3.2e	<u>Understand the Process purpose.</u>					
B-3.3e	<u>Understand all process stakeholders</u> and their roles. Travel management stakeholders:					
B-3.4e	<u>Understand the Process goals</u> and related <u>metrics</u> ¹⁶ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.					
	The Process Travel Management has two defined process goal.		The following activities can be performed to assess whether the goals are achieved.			
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step		
	Accurate and complete entry of employee travel data.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
	The travel management system reconciles to the GL.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement:					
	Reference Process	Travel management	Criteria: 5.1 Accurate and complete entry of employee travel data. 5.2 The travel management system reconciles to the GL.			
	Reference Process Practices ¹⁷	Good Practice	Assessment Step			Issue Cross-reference
	BAI10 DSS01 DSS06	Accurate and complete entry of employee travel data.	<p>5.1.1 Use transaction code SWDD—Workflow Builder to view the workflow for Travel Management. This workflow is a standard feature in SAP ERP. Travel workflow can also be assessed using transaction code PR05—Travel Expense Manager or following the path: Accounting → Financial Accounting → Travel Management → Travel Expenses → Travel Expense Manager. The different stages in the workflow are:</p> <ul style="list-style-type: none"> • Approve request—The pending request will appear in the SAP mailbox of the approver. • Approval notification—Use transaction code SBWP, and go to the inbox. • Enter trip details—Use transaction code PR05. • Settling a trip—Use transaction code PR05. <p>Select a sample of trip requests and verify that they were approved by the appropriate manager.</p>			
	DSS01 DSS06	Accurate and complete entry of employee travel data	5.1.2 Approvers receive the relevant details of the trip in their SAP inbox for approval or rejection. Select a sample of trips and observe approval or rejection by the manager (access the workflow configuration using transaction code SWDD—Workflow Builder, click on the down arrow under the information area on the top left. This will populate a window, which will show all standard workflows in terms of module. Press Ctrl + F and enter the word Travel to view			

¹⁶ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

¹⁷ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Human Capital Management Business Cycle audit/accuracy program.

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
			the required workflow). Request a sample of employees to create requests and ask for approval by their user IDs. The approval process can be observed by checking the approver's SAP mailbox for the request to approve or reject the request.		
	DSS06	The travel management system reconciles to the GL.	5.2.1 Travel expenses are transferred to financial accounting (FI) after approval for posting to the relevant GL accounts. This is performed through transaction codes PFRI—Create Posting Run and PRRW—Posting Run Management. Payments are processed through payroll (check or direct deposit). Transaction codes PRDX, PRD1 and FDTA are for direct deposit, PRPY for payroll and PRCU for check printing. Select a sample of travel expenses approved in the audit period and test that the steps followed are in line with the ones mentioned above.		
B-3.6e	<u>Agree on the process work products</u> ¹⁸ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.				
	Process Travel management inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.			Criteria: All listed work products should demonstrably exist and be used.	
	Process Practice		Work Products	Assessment Step	
	Travel management		<ul style="list-style-type: none"> • Detailed Travel Report • Unreimbursed Expenses Report 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.	
B-3.7e	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				
SAP ERP HR process: Enterprise compensation management					
B-3.1f	Understand the Process context .				
B-3.2f	Understand the Process purpose .				
B-3.3f	Understand all process stakeholders and their roles.				
	Enterprise compensation management stakeholders:				
B-3.4f	Understand the Process goals and related metrics ¹⁹ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.				
	The Process Enterprise compensation management has three defined process goal.		The following activities can be performed to assess whether the goals are achieved.		
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	
	Employee master file is invalid, incomplete and/or inaccurate	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	

¹⁸ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: *Enabling Processes*.

¹⁹ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment
	Performance incentives promote inaccurate financial reporting and/or unethical behavior	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
	Sensitive information in personnel files may be disclosed and/or compromised	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
B-3.5f	<u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement:					
	Reference Process	Enterprise compensation management	Criteria: 6.1 Employee master file is valid, complete and accurate. 6.2 Performance incentives promote accurate financial reporting and ethical behavior. 6.3 Sensitive information in personnel files is not disclosed and/or compromised.			
	Reference Process Practices ²⁰	Good Practice	Assessment Step		Issue Cross-reference	Comment
	APO01	Employee master file is valid, complete and accurate.	6.1.1 Obtain evidence of executive leadership review of the annual plan design for base salary, target incentives and long-term incentive plan grant ranges. Ensure evidence of approval by executive leadership.			
	DSS06	Employee master file is valid, complete and accurate.	6.1.2 Use transaction code S_AHR_61016369—Employee List and: 1. Under the area Period, select Up to Today. 2. Under the area Selection: – Employment status: Right click and select the Delete line . – Employment status: [3] - Active – Execute (F8). 3. Filter the list generated to select active employees for the fiscal year under review: – Select the Set Filter button (Ctrl + F5). – Select the field Leaving Date. – Select the Multiple Selection button. – Select the Single Values tab. – Right click and select Maintain Selection Options. – Select the Single Value (=) button. Press the green check mark or press Enter . Input 00/00/0000. – In the next row, right click and select Maintain Selection Options. – Select the Greater Than or Equal To button. Press the green check mark or press Enter . Enter the last date of the fiscal year (or the last day in the audit period under review). – Select the Execute button (F8). – Select the green check mark or press Enter . 4. Use transaction HRCMP0080—Display Total Compensation Statement, select personnel number and double click on employee name to obtain employee compensation history as follows: – Personnel number: Input the personnel number (located in the first column in step 3).			

²⁰ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Human Capital Management Business Cycle audit/assurance program.

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle																											
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference																							
				Comment																							
		<ul style="list-style-type: none"> – Select the green check mark (or press Enter). – Select the date and Preview Period button (located in the center of the screen—the button looks like a calendar). – Start Date: Input the first date in the audit period. – End Date: Input the last date in the audit period. – Press Execute (F8) – Double click on the employee's name on the far left side of the screen under the heading Hit List. This will generate the compensation report. <p>Note: Because the compensation statement is confidential, the auditors may need to obtain the reports from the control owner.</p> <p>Ensure that a compensation statement was available for each employee selected in step 4. Follow up on any issues with the control owner.</p> <p>Note: An issue includes, but is not limited to, an employee who does not have a compensation statement.</p>																									
DSS05	Employee master file is valid, complete and accurate.	<p>6.1.3 Use transaction code SUIM—User Information System to generate a list of users with the ability to perform critical functionalities, such as PO03—Maintain Job :</p> <table border="1" data-bbox="756 866 1550 1165"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td rowspan="6">PO03—Maintain Job</td><td>S_TCODE</td><td>TCD</td><td>PO03</td></tr> <tr> <td>P_TCODE</td><td>TCD</td><td>PO03</td></tr> <tr> <td>P_ORGIN</td><td>INFETY</td><td>1005</td></tr> <tr> <td>P_ORGIN</td><td>AUTHC</td><td>W</td></tr> <tr> <td>PLOG</td><td>OTYPE</td><td>C</td></tr> <tr> <td>PLOG</td><td>INFOTYP</td><td>1005</td></tr> </tbody> </table> <p>Use of authorization object P_PERNR should be incorporated into the user's security so that no employee has access to update his/her own standard work roster.</p> <p>Note: Each query can only run for three authorization objects. These objects will need to be pulled separately into two reports and the users who show up in both reports have access for the transaction(s).</p> <p>Review the list of users to determine whether access is appropriate based on current job responsibilities. Review any discrepancies with the control owner. Use of authorization object P_PERNR should be incorporated into the user's security so that no employee has access to update his/her own standard work roster.</p>	Transaction(s)	Authorization Objects	Fields	Values	PO03—Maintain Job	S_TCODE	TCD	PO03	P_TCODE	TCD	PO03	P_ORGIN	INFETY	1005	P_ORGIN	AUTHC	W	PLOG	OTYPE	C	PLOG	INFOTYP	1005		
Transaction(s)	Authorization Objects	Fields	Values																								
PO03—Maintain Job	S_TCODE	TCD	PO03																								
	P_TCODE	TCD	PO03																								
	P_ORGIN	INFETY	1005																								
	P_ORGIN	AUTHC	W																								
	PLOG	OTYPE	C																								
	PLOG	INFOTYP	1005																								

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle																																										
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																										
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																																				
	DSS05	Employee master file is valid, complete and accurate.	6.1.4 Use transaction code SUIM—User Information System to generate a list of users with the ability to perform critical functionalities such as PECM_CHANGE_STATUS – Change Compensation Process Status:	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PECM_CHANGE_STATUS – Change Compensation Process Status</td><td>S_TCODE</td><td>TCD</td><td>PECM_CHANGE_STATUS</td></tr> <tr> <td></td><td>P_TCODE</td><td>TCD</td><td>PECM_CHANGE_STATUS</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0015</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0267</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0008</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0759</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0761</td></tr> <tr> <td></td><td>P_ORGIN</td><td>AUTHC</td><td>W</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	PECM_CHANGE_STATUS – Change Compensation Process Status	S_TCODE	TCD	PECM_CHANGE_STATUS		P_TCODE	TCD	PECM_CHANGE_STATUS		P_ORGIN	INFTY	0015		P_ORGIN	INFTY	0267		P_ORGIN	INFTY	0008		P_ORGIN	INFTY	0759		P_ORGIN	INFTY	0761		P_ORGIN	AUTHC	W		
Transaction(s)	Authorization Objects	Fields	Values																																							
PECM_CHANGE_STATUS – Change Compensation Process Status	S_TCODE	TCD	PECM_CHANGE_STATUS																																							
	P_TCODE	TCD	PECM_CHANGE_STATUS																																							
	P_ORGIN	INFTY	0015																																							
	P_ORGIN	INFTY	0267																																							
	P_ORGIN	INFTY	0008																																							
	P_ORGIN	INFTY	0759																																							
	P_ORGIN	INFTY	0761																																							
	P_ORGIN	AUTHC	W																																							
	APO01 BAI06	Employee master file is valid, complete and accurate.	6.1.5 Obtain evidence of executive leadership review of the annual plan design for compensation plan changes (e.g., salary adjustments, bonuses, pay scale, etc.). Ensure evidence of approval by executive leadership.																																							
	DSS06	Performance incentives promote accurate financial reporting and ethical behavior.	6.2.1 Obtain Sales Compensation Components and ensure that these components were reviewed, validated and approved by an authoritative source.																																							
	DSS06	Performance incentives promote accurate financial reporting and ethical behavior.	6.2.2 Obtain documentation of annual bonus payout and ensure that review and approval of bonus payouts through Manager Self-service (MSS) prior to payout to employees was done. Corroborate the bonus payout review and approval process with site supervisors.																																							
	DSS06	Performance incentives promote accurate financial reporting and ethical behavior.	6.2.3 Through corroboration with the control owner, gain an understanding of the process of reviewing weekly reports documenting compensation for appropriateness. Through discussion, determine what steps the line supervisor performs to review the document and what information the line supervisor expects to see or not on the report. Document the information obtained. Select a sample of 10 week from the current fiscal year under review. For each week selected, obtain the report which documents compensation. Validate that the report was reviewed by the appropriate supervisor.																																							
	DSS05 DSS06	Sensitive information in personnel files is not disclosed and/or compromised.	6.3.1 Use transaction code SUIM—User Information System to generate a list of users with the ability to view critical functionalities such as PO03—Maintain Job:	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> </table>	Transaction(s)	Authorization Objects	Fields	Values																																		
Transaction(s)	Authorization Objects	Fields	Values																																							

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle																																													
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																													
Ref.	Assurance Steps and Guidance							Issue Cross-reference	Comment																																				
				PO03 PO03— Maintain Job	S_TCODE	TCD	PO03																																						
					P_TCODE	TCD	PO03																																						
					P_ORGIN	INFTY	1005																																						
					P_ORGIN	AUTHC	R																																						
DSS05	Sensitive information in personnel files is not disclosed and/or compromised.	6.3.2 Ensure that SAP HCM is configured to use position-based security. To check whether position-based security is being used, use transaction code PA30—Maintain HR Master Data or PO13—Maintain Position and check that the roles are assigned to the user positions.																																											
DSS06	Sensitive information in personnel files is not disclosed and/or compromised.	6.3.3 Use transaction code SUIM—User Information System to generate a list of users with the ability to perform critical functionalities such as PEPCM_CHANGE_STATUS – Change Compensation Process Status:	<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PEPCM_CHANGE_STATUS</td><td>S_TCODE</td><td>TCD</td><td>PEPCM_CHANGE_STATUS</td></tr> <tr> <td>PEPCM_CHANGE_STATUS – Change Compensation Process Status</td><td>P_TCODE</td><td>TCD</td><td>PEPCM_CHANGE_STATUS</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0015</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0267</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0008</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0759</td></tr> <tr> <td></td><td>P_ORGIN</td><td>INFTY</td><td>0761</td></tr> <tr> <td></td><td>P_ORGIN</td><td>AUTHC</td><td>R</td></tr> </tbody> </table>							Transaction(s)	Authorization Objects	Fields	Values	PEPCM_CHANGE_STATUS	S_TCODE	TCD	PEPCM_CHANGE_STATUS	PEPCM_CHANGE_STATUS – Change Compensation Process Status	P_TCODE	TCD	PEPCM_CHANGE_STATUS		P_ORGIN	INFTY	0015		P_ORGIN	INFTY	0267		P_ORGIN	INFTY	0008		P_ORGIN	INFTY	0759		P_ORGIN	INFTY	0761		P_ORGIN	AUTHC	R
Transaction(s)	Authorization Objects	Fields	Values																																										
PEPCM_CHANGE_STATUS	S_TCODE	TCD	PEPCM_CHANGE_STATUS																																										
PEPCM_CHANGE_STATUS – Change Compensation Process Status	P_TCODE	TCD	PEPCM_CHANGE_STATUS																																										
	P_ORGIN	INFTY	0015																																										
	P_ORGIN	INFTY	0267																																										
	P_ORGIN	INFTY	0008																																										
	P_ORGIN	INFTY	0759																																										
	P_ORGIN	INFTY	0761																																										
	P_ORGIN	AUTHC	R																																										
B-3.6f	<u>Agree</u> on the process work products ²¹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess</u> to what extent the process work products are available. Process Enterprise compensation management inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.																																												
	Process Practice Enterprise compensation management		Work Products <ul style="list-style-type: none"> Summary compensation report Detailed compensation report 			Assessment Step Apply appropriate audit techniques to determine the existence and appropriate use of each work product.																																							

²¹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle																													
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																													
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment																							
B-3.7f	<p>Agree on the process capability level to be achieved by the process.</p> <p>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</p>																												
SAP ERP HR process: Employee self-service and manager self-service																													
B-3.1g	<p><u>Understand the Process context.</u></p>																												
B-3.2g	<p><u>Understand the Process purpose.</u></p>																												
B-3.3g	<p><u>Understand all process stakeholders and their roles.</u></p> <p>Employee self-service and manager self-service stakeholders:</p>																												
B-3.4g	<p><u>Understand the Process goals</u> and related metrics²² and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.</p> <p>The Process Employee self-service and manager self-service has three defined process goal.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Process Goal</th> <th style="text-align: center;">Related Metrics</th> <th style="text-align: center;">Criteria/Expected Value</th> <th style="text-align: center;">Assessment Step</th> </tr> </thead> <tbody> <tr> <td>No excessive or unauthorized access to sensitive HR data.</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>Authorized approval of time, expense or other employee or HR data.</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>Managers Desktop 'Themes' are configured to restrict users from unauthorized access to sensitive information.</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>				Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	No excessive or unauthorized access to sensitive HR data.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	Authorized approval of time, expense or other employee or HR data.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	Managers Desktop 'Themes' are configured to restrict users from unauthorized access to sensitive information.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.									
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step																										
No excessive or unauthorized access to sensitive HR data.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																										
Authorized approval of time, expense or other employee or HR data.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																										
Managers Desktop 'Themes' are configured to restrict users from unauthorized access to sensitive information.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																										
B-3.5g	<p>Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center;">Reference Process</th> <th style="text-align: center;">Employee self-service and manager self-service</th> <th style="text-align: center;">Criteria:</th> <th style="text-align: center;">Assessment Step</th> <th style="text-align: center;">Issue Cross-reference</th> <th style="text-align: center;">Comment</th> </tr> </thead> <tbody> <tr> <td style="background-color: #e0e0e0;">Reference Process Practices²³</td> <td style="background-color: #e0e0e0;">Good Practice</td> <td style="background-color: #e0e0e0;">7.1 No excessive or unauthorized access to sensitive HR data. 7.2 Authorized approval of time, expense or other employee or HR data. 7.3 Managers Desktop 'Themes' are configured to restrict users from unauthorized access to sensitive information.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>DSS05 DSS06</td> <td>No excessive or unauthorized access to sensitive HR data.</td> <td>7.1.1 Use transaction SE16—Data Browser and view table AGR_1251 to view the roles with access to maintain infotypes 0077, 0105, 0016, 0021, 0009 and 0008. View table AGR_USERS to identify users assigned these roles and ascertain whether access is according to management's intentions.</td> <td></td> <td></td> <td></td> </tr> <tr> <td>DSS05</td> <td>No excessive or unauthorized</td> <td>7.1.2 Ensure that SAP HCM is configured to use position-based security. To check whether position-</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Reference Process	Employee self-service and manager self-service	Criteria:	Assessment Step	Issue Cross-reference	Comment	Reference Process Practices ²³	Good Practice	7.1 No excessive or unauthorized access to sensitive HR data. 7.2 Authorized approval of time, expense or other employee or HR data. 7.3 Managers Desktop 'Themes' are configured to restrict users from unauthorized access to sensitive information.				DSS05 DSS06	No excessive or unauthorized access to sensitive HR data.	7.1.1 Use transaction SE16—Data Browser and view table AGR_1251 to view the roles with access to maintain infotypes 0077, 0105, 0016, 0021, 0009 and 0008. View table AGR_USERS to identify users assigned these roles and ascertain whether access is according to management's intentions.				DSS05	No excessive or unauthorized	7.1.2 Ensure that SAP HCM is configured to use position-based security. To check whether position-				
Reference Process	Employee self-service and manager self-service	Criteria:	Assessment Step	Issue Cross-reference	Comment																								
Reference Process Practices ²³	Good Practice	7.1 No excessive or unauthorized access to sensitive HR data. 7.2 Authorized approval of time, expense or other employee or HR data. 7.3 Managers Desktop 'Themes' are configured to restrict users from unauthorized access to sensitive information.																											
DSS05 DSS06	No excessive or unauthorized access to sensitive HR data.	7.1.1 Use transaction SE16—Data Browser and view table AGR_1251 to view the roles with access to maintain infotypes 0077, 0105, 0016, 0021, 0009 and 0008. View table AGR_USERS to identify users assigned these roles and ascertain whether access is according to management's intentions.																											
DSS05	No excessive or unauthorized	7.1.2 Ensure that SAP HCM is configured to use position-based security. To check whether position-																											

²² For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: *Enabling Processes*.

²³ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Human Capital Management Business Cycle audit/assurance program.

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	DSS06	access to sensitive HR data.	based security is being used, use transaction code PA30 Maintain HR Master Data or PO13—Maintain Position and check that the roles are assigned to the user positions.		
	DSS05 DSS06	No excessive or unauthorized access to sensitive HR data.	7.1.3 Use transaction SE16—Data Browser and view table AGR_1251 to view roles with access to change data to accounts other than their own via object P_PERNR. Identify whether these roles are assigned to users by viewing table AGR_USERS.		
	DSS06	Authorized approval of time, expense or other employee or HR data.	7.2.1 Obtain the standard leave form and request a sample of leaves. Confirm that appropriate documentation exists for users' requests for leave. Additional steps may be performed to confirm that no unapproved long-term leaves exist.		
	BAI10 DSS06	Authorized approval of time, expense or other employee or HR data.	7.2.2 Based on the type of requirement for alternate approval, obtain a screenshot of the workflow task being set for Manager Self-service (MSS) using transaction code SPRO to display the IMG menu and follow path: Cross-application Components → Process and Tools for Enterprise Applications → Inbox → Assign Task IDs to POWL Types. Confirm that alternate approval application is configured. Note: Different types of approvals may require different configurations (time versus travel versus leave). Use transaction code SPRO to display the IMG menu and follow path: Cross-application Components → Process and Tools for Enterprise Applications → Inbox → Assign Connected Backend Systems to Inbox to obtain the configuration of different remote function calls (RFCs). Confirm that all systems with approval routes are configured to the alternate approval application.		
	BAI10 DSS05 DSS06	Managers Desktop 'Themes' are configured to restrict users from unauthorized access to sensitive information.	7.3.1 Use transaction code SUIM—User Information System to view that the PD_ALL profile is not assigned to any end users.		
	<u>Agree on the process work products</u> ²⁴ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.				
B-3.6g	Process Employee self-service and manager self-service inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.		Criteria: All listed work products should demonstrably exist and be used.		
	Process Practice	Work Products	Assessment Step		
	Employee self-service and manager self-service	• Employee Change Report • HR Sensitive Access Report	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		
B-3.7g	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				

²⁴ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment															
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment												
B-4	Obtain understanding of each Organisational Structure in scope and set suitable assessment criteria: For each Organisational Structure in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the Organisational Structure .														
Organisational Structure Human Resources															
B-4.1a	<u>Understand the Organisational Structure context.</u> <i>Identify and document all elements that can help to understand the context in which the Financial accounting organization has to operate, including:</i> <ul style="list-style-type: none"> • The overall organisation • Management/process framework • History of the role/structure • Contribution of the Organisational Structure to achievement of goals 														
B-4.2a	<u>Understand all stakeholders of the Organisational Structure/function.</u> <i>Determine through documentation review (policies, management communications, etc.) the key stakeholders of the Financial accounting organization.</i> <ul style="list-style-type: none"> • Incumbent of the role and/or members of the Organisational Structure • Other key stakeholders affected by the decisions of the Organisational Structure/role 														
B-4.3a	<u>Understand the goals of the Organisational Structure</u> , the related metrics and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals.														
<table border="1"> <thead> <tr> <th>Organisational Structure Goal</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Determine through interviews with key stakeholders and documentation review the goals of the Financial accounting organization, i.e., the decisions for which they are accountable^{25,26}.</td> <td> This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. </td> </tr> </tbody> </table>				Organisational Structure Goal	Assessment Step	Determine through interviews with key stakeholders and documentation review the goals of the Financial accounting organization, i.e., the decisions for which they are accountable ^{25,26} .	This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 								
Organisational Structure Goal	Assessment Step														
Determine through interviews with key stakeholders and documentation review the goals of the Financial accounting organization, i.e., the decisions for which they are accountable ^{25,26} .	This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> – They have contributed to the achievement of the IT-related and enterprise goals as anticipated. – Decisions are duly executed on a timely basis. 														
B-4.4a	<u>Agree on the expected good practices for the Organisational Structure</u> against which it will be assessed. <u>Assess the Organisational Structure design</u> , i.e., assess the extent to which expected good practices are applied.														
<table border="1"> <thead> <tr> <th>Good Practice</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Operating principles</td> <td> <ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. </td> <td> <ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. </td> </tr> <tr> <td>Composition</td> <td>The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td> <td>Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.</td> </tr> <tr> <td>Span of control</td> <td> <ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. </td> <td> <ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. </td> </tr> </tbody> </table>				Good Practice	Criteria	Assessment Step	Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 	Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Span of control	<ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. 	<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined.
Good Practice	Criteria	Assessment Step													
Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 													
Composition	The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.													
Span of control	<ul style="list-style-type: none"> • The span of control of The Organisational Structure is defined. 	<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined. 													

²⁵ The RACI charts in COBIT 5: *Enabling Processes* can be leveraged as a starting point for the expected goals of a role or Organisational Structure.

²⁶ The Organisational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organisational Structure assuming the same responsibilities and accountability should be considered.

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Organisational Structures					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-4.5a		<ul style="list-style-type: none"> The span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. The span of control is in line with the overall enterprise governance arrangements. 	<ul style="list-style-type: none"> Assess whether the span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. Verify and assess whether the span of control is in line with the overall enterprise governance arrangements. 		
	Level of authority/decision rights	<ul style="list-style-type: none"> Decision rights of the Organisational Structure are defined and documented. Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue). 	<ul style="list-style-type: none"> Verify that decision rights of the Organisational Structure are defined and documented. Verify whether decision rights of the Organisational Structure are complied with and respected. 		
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.		
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.		
B-4.1 to B-4.5	<u>Understand</u> the life cycle and agree on expected values. <u>Assess</u> the extent to which the Organisational Structure life cycle is managed.				
	Life-Cycle Element	Criteria	Assessment Step		
	Mandate	<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well understood mandate. 		
	Monitoring	<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 		
B-4.1 to B-4.5	Repeat steps B-4.1 through B-4.5 for all remaining Organisational structures in scope.				
	Repeat the steps described above for the remaining Organisational structures: <ul style="list-style-type: none"> Benefits Training Department 				

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment	
B-5	Obtain understanding of the Culture, Ethics and Behaviour in scope. Assess Culture, Ethics and Behaviour.			
Culture, Ethics and Behaviour: Risk and compliance aware culture				
B-5.1a	<u>Understand the Culture, Ethics and Behaviour context.</u> <ul style="list-style-type: none"> • <i>What the overall corporate Culture is like</i> • <i>Understand the interconnection with other enablers in scope:</i> <ul style="list-style-type: none"> - <i>Identify roles and structures that could be affected by the Culture.</i> - <i>Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.</i> 			
B-5.2a	<u>Understand the major stakeholders of the Culture, Ethics and Behaviour: Risk and compliance aware culture</u> <i>Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.</i>			
B-5.3a	<u>Understand the goals for the Culture, Ethics and Behaviour</u> , and the related metrics and agree on expected values. Assess whether the Culture, Ethics and Behaviour goals (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour. In the context of Risk and compliance aware culture , the following Culture, Ethics and Behaviour are desired:	Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. For a representative sample of individuals, perform the following assessment steps.		
Desired Behaviour (Culture, Ethics and Behaviour Goal) The enterprise is aware of the compliance requirements it must abide Employees understand their role in maintaining compliance Identified risk are properly address Controls are in place to ensure compliance with internal and external requirements		Assessment Step		
		•		
		•		
		•		
		•		
B-5.4a	<u>Understand the life cycle stages of the Culture, Ethics and Behaviour</u> , and agree on the relevant criteria. Assess to what extent the Culture, Ethics and Behaviour life cycle is managed. <i>(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)</i>			
B-5.5a	Understand good practice when dealing with Culture, Ethics and Behaviour , and agree on relevant criteria. Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied.			
Good Practice		Criteria	Assessment Step	
Communication, enforcement and rules		Existence and quality of the communication	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.	
Incentives and rewards		Existence and application of appropriate rewards and incentives		
Awareness		Awareness of desired Behaviours		
B-5.1 to B-5.5		Repeat steps B-5.1 through B-5.5 for all remaining Culture, Ethics and Behaviour in scope. Repeat the steps described above for the remaining Culture, Ethics and Behaviour: <ul style="list-style-type: none"> • Enabling of continuous improvement • Accountability • Discipline to follow instructions 		

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle																																																																																				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																																																																																				
Ref.	Assurance Steps and Guidance			Issue Cross-reference																																																																																
				Comment																																																																																
B-6	Obtain understanding of the Information Items in scope. Assess Information Items.																																																																																			
Information Item: Data integrity procedures																																																																																				
B-6.1a	<u>Understand</u> the Information item context : <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> - <i>Used by which processes?</i> - <i>Which Organisational Structures are involved?</i> - <i>Which services/applications are involved?</i> 																																																																																			
B-6.2a	<u>Understand</u> the major stakeholders of the Information item . <i>Understand the stakeholders for the Information item, i.e., identify the:</i> <ul style="list-style-type: none"> • <i>Information producer</i> • <i>Information custodian</i> • <i>Information consumer</i> <i>Stakeholders should be at the appropriate organisational level.</i>																																																																																			
B-6.3a	<u>Understand</u> the major quality criteria for the Information item, the related metrics and agree on expected values. <u>Assess</u> whether the Information item quality criteria (outcomes) are achieved, i.e., assess the effectiveness of the Information item. Leverage the COBIT 5 Information enabler model ²⁷ focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand. Mark the quality dimensions with a ‘✓’ that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.	The assurance professional will, by using appropriate auditing techniques, verify all quality criteria in scope and assess whether the criteria are met.																																																																																		
<table border="1"> <thead> <tr> <th>Quality Dimension</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> <th></th> </tr> </thead> <tbody> <tr><td>Accuracy</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Objectivity</td><td></td><td></td><td></td><td></td></tr> <tr><td>Believability</td><td></td><td></td><td></td><td></td></tr> <tr><td>Reputation</td><td></td><td></td><td></td><td></td></tr> <tr><td>Relevancy</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Completeness</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Currency</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Amount of information</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Concise representation</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Consistent representation</td><td></td><td></td><td></td><td></td></tr> <tr><td>Interpretability</td><td></td><td></td><td></td><td></td></tr> <tr><td>Understandability</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Manipulation</td><td></td><td></td><td></td><td></td></tr> <tr><td>Availability</td><td>✓</td><td></td><td></td><td></td></tr> <tr><td>Restricted access</td><td>✓</td><td></td><td></td><td></td></tr> </tbody> </table>					Quality Dimension	Key Criteria	Description	Assessment Step		Accuracy	✓				Objectivity					Believability					Reputation					Relevancy	✓				Completeness	✓				Currency	✓				Amount of information	✓				Concise representation	✓				Consistent representation					Interpretability					Understandability	✓				Manipulation					Availability	✓				Restricted access	✓			
Quality Dimension	Key Criteria	Description	Assessment Step																																																																																	
Accuracy	✓																																																																																			
Objectivity																																																																																				
Believability																																																																																				
Reputation																																																																																				
Relevancy	✓																																																																																			
Completeness	✓																																																																																			
Currency	✓																																																																																			
Amount of information	✓																																																																																			
Concise representation	✓																																																																																			
Consistent representation																																																																																				
Interpretability																																																																																				
Understandability	✓																																																																																			
Manipulation																																																																																				
Availability	✓																																																																																			
Restricted access	✓																																																																																			

²⁷ COBIT 5 framework, appendix G, p.81-84

Audit/Accrual Program for SAP ERP Human Capital Management Business Cycle																																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Culture, Ethics and Behaviour																																	
Ref.	Assurance Step and Guidance			Issue Cross-reference	Comment																												
B-6.4a	<p>Understand the life cycle stages of the Information item, and agree on the relevant criteria. <u>Assess</u> to what extent the Information item life cycle is managed.</p> <p>The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.</p> <ul style="list-style-type: none"> When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently. When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. <p>Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Life Cycle Stage</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr><td>Plan</td><td>✓</td><td></td><td></td></tr> <tr><td>Design</td><td>✓</td><td></td><td></td></tr> <tr><td>Build/acquire</td><td>✓</td><td></td><td></td></tr> <tr><td>Use/operate</td><td>✓</td><td></td><td></td></tr> <tr><td>Evaluate/monitor</td><td>✓</td><td></td><td></td></tr> <tr><td>Update/dispose</td><td>✓</td><td></td><td></td></tr> </tbody> </table>					Life Cycle Stage	Key Criteria	Description	Assessment Step	Plan	✓			Design	✓			Build/acquire	✓			Use/operate	✓			Evaluate/monitor	✓			Update/dispose	✓		
Life Cycle Stage	Key Criteria	Description	Assessment Step																														
Plan	✓																																
Design	✓																																
Build/acquire	✓																																
Use/operate	✓																																
Evaluate/monitor	✓																																
Update/dispose	✓																																
B-6.5a	<p>Understand important attributes of the Information item and expected values. <u>Assess</u> the Information item design, i.e., assess the extent to which expected good practices are applied.</p> <p>Good practices for Information items are defined as a series of attributes for the Information item²⁸. The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.</p> <p>Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Attribute</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr><td>Physical</td><td></td><td></td><td></td></tr> <tr><td>Empirical</td><td></td><td></td><td></td></tr> <tr><td>Syntactic</td><td></td><td></td><td></td></tr> <tr><td>Semantic</td><td></td><td></td><td></td></tr> <tr><td>Pragmatic</td><td>✓</td><td></td><td></td></tr> <tr><td>Social</td><td></td><td></td><td></td></tr> </tbody> </table>					Attribute	Key Criteria	Description	Assessment Step	Physical				Empirical				Syntactic				Semantic				Pragmatic	✓			Social			
Attribute	Key Criteria	Description	Assessment Step																														
Physical																																	
Empirical																																	
Syntactic																																	
Semantic																																	
Pragmatic	✓																																
Social																																	
B-6.1 to B-6.5	<p>Repeat steps B-6.1 through B-6.5 for all remaining Information items in scope.</p> <p>Repeat the steps described above for the remaining Information items:</p> <ul style="list-style-type: none"> Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis Retention requirements Record of transactions Training manuals Job aids 																																

²⁸ COBIT 5 framework, appendix G, p. 81-84

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-7	Obtain understanding of the Services, Infrastructure and Applications in scope. Assess Services, Infrastructure and Applications.			
Services, Infrastructure and Applications: Master data maintenance group				
B-7.1a	<u>Understand the Services, Infrastructure and Applications</u> context. <i>Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.</i>			
B-7.2a	<u>Understand the major stakeholders</u> of the Services, Infrastructure and Applications . <i>Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.</i>			
B-7.3a	<u>Understand the major goals</u> for the Services, Infrastructure and Applications , the related metrics and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.			
Goal				
	Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 	
	Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 	
	Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.	
B-7.4a	<u>Understand</u> good practice related to the Services, Infrastructure and Applications and expected values. <u>Assess</u> the Services, Infrastructure and Applications design, i.e., assess to what extent expected good practices are applied. <i>Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework²⁹ to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented:</i> <ul style="list-style-type: none"> Buy/build decision needs to be taken. Use of the Service needs to be clear. 			
Good Practice				
	Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken 	

²⁹ COBIT 5 framework, appendix G, p.85-86

Audit/Assurance Program for SAP ERP Human Capital Management Business Cycle				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Culture, Ethics and Behaviour				
Ref.	Assurance Step and Guidance			Issue Cross-reference
				Comment
	Service.	regarding the sourcing of the Service. <ul style="list-style-type: none">• Verify the validity and quality of the business case.• Verify that the sourcing decision has been duly executed.		
	Use	The use of the Service needs to be clear: <ul style="list-style-type: none">• When it needs to be used and by whom• The required compliance levels with the Service's output	<ul style="list-style-type: none">• Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used.• Verify that actual use is in line with requirement above.• Verify that the actual Service output is adequately used.• Verify that Service levels are monitored and achieved.	
B-7.1 to B-7.4	<p>Repeat steps B-7.1 through B-7.4 for all remaining Services, Infrastructure and Applications in scope.</p> <p>Repeat the steps described above for the remaining Services, Infrastructure and Applications:</p> <ul style="list-style-type: none">• SAP ERP support and maintenance• SAP training• Payroll• Accounting department			

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle																				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																				
Ref.	Assurance Steps and Guidance		Issue Cross-reference																	
B-8	Obtain understanding of the People, Skills and Competencies in scope. Assess People, Skills and Competencies.																			
People, Skill and Competency: Proficiency using the SAP HR Module																				
B-8.1a	<p><u>Understand the People, Skills and Competencies</u> context. <i>Understand the context of the Skill/Competency, i.e.,:</i></p> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> - <i>In which roles and structures is the Skill/Competency used? (See also B-4.1.)</i> <p><i>Which behaviours are associated with the Skill/Competency?</i></p>																			
B-8.2a	<p><u>Understand the major stakeholders</u> for the People, Skills and Competencies. <i>Identify to whom in the organisation the skill requirement applies.</i></p>																			
B-8.3a	<p><u>Understand the major goals</u> for the People, Skills and Competencies, the related metrics and agree on expected values. Assess whether the People, Skills and Competencies goals (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.</p> <p>For the People, Skills and Competencies: Proficiency using the SAP HR Module, the following goals and associated criteria can be addressed.</p> <table border="1"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Experience</td><td></td><td rowspan="7">Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.</td></tr> <tr> <td>Education</td><td></td></tr> <tr> <td>Qualification</td><td></td></tr> <tr> <td>Knowledge</td><td></td></tr> <tr> <td>Technical skills</td><td></td></tr> <tr> <td>Behavioural skills</td><td></td></tr> <tr> <td>Number of people with appropriate skill level</td><td></td></tr> </tbody> </table>	Goal	Criteria	Assessment Step	Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.	Education		Qualification		Knowledge		Technical skills		Behavioural skills		Number of people with appropriate skill level		
Goal	Criteria	Assessment Step																		
Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.																		
Education																				
Qualification																				
Knowledge																				
Technical skills																				
Behavioural skills																				
Number of people with appropriate skill level																				
B-8.4a	<p><u>Understand the life cycle</u> stages of the People, Skills and Competencies, and agree the relevant criteria. Assess to what extent the People, Skills and Competencies life cycle is managed.</p> <p>For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07.</p> <table border="1"> <thead> <tr> <th>Life Cycle Element</th><th>Criteria</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Plan</td><td>Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.</td><td>Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.</td></tr> <tr> <td>Design</td><td> Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill. </td><td> Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill. </td></tr> </tbody> </table>	Life Cycle Element	Criteria	Assessment Step	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.										
Life Cycle Element	Criteria	Assessment Step																		
Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.																		
Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.																		

Audit/Accuracy Program for SAP ERP Human Capital Management Business Cycle					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
People, Skills and Competencies					
Ref.	Assurance Steps and Guidance				Issue Cross-reference
	Build	Practice APO07.03 activity 4 (Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 4 is implemented in relation to this skill.		Comment
B-8.5a	Operate	Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.		
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.		
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.		
	<u>Understand good practice related to the People, Skills and Competencies and expected values.</u> Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.				
Good Practice		Criteria	Assessment Step		
Skill set and Competencies are defined.		<ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 			
Skill levels are defined.		<ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. Assess the process for 360-degree performance evaluations. 			

Audit/Assurance Program for SAP ERP Human Capital Management Business Cycle			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-8.1 to B-8.5	<p>Repeat steps B-8.1 through B-8.5 for all remaining People, Skills and Competencies in scope.</p> <p>Repeat the steps described above for the remaining People, Skills and Competencies:</p> <ul style="list-style-type: none"> • Master data management skills • HR skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 		

Audit/Accurance Program for SAP ERP Human Capital Management Business Cycle		
Phase C—Communicate the Results of the Assessment		
Ref.	Assurance Step	Guidance
C-1	Document exceptions and gaps.	
C-1.1	Understand and document weaknesses and their impact on the achievement of process goals.	<ul style="list-style-type: none"> Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	<ul style="list-style-type: none"> Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. Point out the consequence of noncompliance with regulatory requirements and contractual agreements. Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
C-2	Communicate the work performed and findings.	
C-2.1	Communicate the work performed.	<ul style="list-style-type: none"> Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	<ul style="list-style-type: none"> Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. Use benchmarking and survey results to compare the enterprise's performance with others. Use extensive graphics to illustrate the issues. Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	

Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
1. Personnel Administration							
1.1 HR master data are valid, complete and accurate.							
1.1.1 Are validation checks, such as checks for uniqueness, format, length, etc., enabled on certain fields for data integrity?					DSS01 DSS06		
1.1.2 Is access to view, establish, update and delete master data restricted to appropriately authorized users? Is it verified that users with the ability to view master data are also appropriately restricted to reduce the likelihood of inappropriate viewing or distribution of data due to the sensitive nature of HR master data?					DSS05 DSS06		
1.1.3 Are mandatory fields validated to be defined within the system to ensure the completeness of HR master records?					BAI10		
1.1.4 Are regular reviews of the new employee details conducted by an HR Supervisor, especially the review of the new employee creation process? Are necessary evidences obtained to confirm the occurrence of the reviews?					DSS01 DSS06		
1.1.5 Is access to HR master data appropriately assigned, configured and managed?					DSS05 DSS06		
1.2 HR master data are current and pertinent.							

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
1.2.1 Prior to adding a new employee record in the HR master data, is a listing of current employees generated and reviewed by relevant management?					DSS06
1.2.2 Are requirements for authenticity and protecting data integrity in applications implemented?					BAI06 DSS05 DSS06
1.2.3 Are changes made to HR master data substantiated by appropriate documentation (approved by an appropriate authority where relevant)?					BAI06
1.2.4 Are HR master data periodically reviewed by authorized personnel to ensure consistency and ongoing pertinence?					DSS01 DSS06
1.3 HR Master data are secure.					
1.3.1 Is access to add an employee record restricted to authorized personnel?					DSS05 DSS06
1.3.2 Is access to the application and to important transaction codes assigned based on user profiles and/or roles?					DSS05 DSS06
1.4 Nonexistent or duplicate employee is not added to payroll.					
1.4.1 Are validation checks, such as checks for uniqueness, format, length, etc., enabled on certain fields for data integrity?					DSS06
1.5 Termination dates are accurately reported.					

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
1.5.1 Is the system configured such that if a backdated termination date is entered, a notification is generated to reduce the occurrence of backdating of terminations and to accurately process termination payments and calculations?					DSS01 DSS06
1.5.2 Are the workflows configured to approve terminations?					DSS01 DSS06
1.5.3 Is a report consisting of terminations generated on a periodic basis? Does an authorized individual who does not have permission to terminate employees, able to check that termination data are entered accurately?					DSS01 DSS06
1.5.4 Is employee status automatically changed to terminated when the termination date is reached?					DSS01 DSS06
1.5.5 Is verification done to ensure that payments are not disbursed to employees with terminated status?					DSS01 DSS06
1.6 Employee is deactivated when employment is terminated.					
1.6.1 Are department and/or cost center managers periodically provided with a listing of employees for which they are responsible?					DSS01 DSS06
1.6.2 Is a terminated employee's access to systems automatically disabled based on termination date entered?					DSS05
2. Time Management					
2.1 Accurate, complete and timely entry of employee time data.					

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.1.1 Are workflows configured to enable automatic submission of employee time for review by the employee's supervisor or functional manager?					DSS01 DSS06
2.1.2 Are validation checks configured to decrease the likelihood of inaccurate time being entered?					BAI10
2.1.3 Are automated notifications configured to remind/alert users to enter their time report?					BAI10
2.1.4 Does a process exist that ensures that, after the time reporting deadline is reached, the payroll department generates a report incorporating missing time and follows up directly with employees and their functional managers?					DSS01
2.2 Unapproved leave or leave is not taken outside of entitlements.					
2.2.1 Has SAP been configured to reflect all required leave and absence types? Have quotas have been configured for specific leave types, such as sick leave and vacation?					DSS01
2.2.2 Are processes implemented to capture leave requests and generate reports showing any variance between leave recorded and leave requested?					BAI10 DSS06
2.2.3 Are workflows configured to route leaves for approval?					BAI10 DSS01
2.3 Established employee shifts are updated accurately.					

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.3.1 Is access to update employee shift restricted to authorized personnel? Is it ensured that employees do not have access to update their own shift details?					DSS05 DSS06
2.3.2 Are updates to employee shifts only made in the system following approval by authorized personnel?					DSS05 DSS06
2.4 Time recorded in prior periods is amended accurately and with appropriate authority.					
2.4.1 Post submission, does the application restrict employees from being able to edit the time sheet submitted?					DSS05
2.4.2 Is it ensured that employees are not allowed access to process prior-period adjustments?					DSS05
2.4.3 Are workflows configured to approve amendments to time recorded in prior periods?					BAI10
2.4.4 Is a limit imposed on the prior period for which adjustments can be processed?					DSS01 DSS05
3. Payroll					
3.1 Payroll calculation is accurate and complete.					
3.1.1 Is auto-posting functionality utilized to update the GL with the approved payroll results?					DSS01
3.1.2 Are payroll posting results reviewed at the end of each pay cycle? Are payroll transactions posted manually reconciled?					DSS01 DSS06

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.1.3 Is SAP configured with the Infotype Audit Report (RPUAUD00)?					DSS01 DSS06
3.1.4 Are changes to pay rate scales recorded on a standard form and authorized by authoritative source?					BAI10 DSS06
3.1.5 Are restrictions placed to provide only the authorized personnel the ability to process the off-cycle payments?					DSS05
3.1.6 Are SAP payroll accounting area and associated control records configured accurately for each employee?					BAI10
3.1.7 Are rules configured to calculate gross and net pay for employees? Are these protected from being overridden or modified without appropriate authorization?					BAI06 BAI10 DSS05
3.2 Employee wages paid in foreign currency are calculated correctly.					
3.2.1 Is an automated update of foreign exchange rates established with an authorized source to ensure that rates applied are current and accurate?					BAI10 DSS01
3.3 Leave accrual rates are established accurately.					
3.3.1 Are leave accrual rules established? Are they consistent with the employee agreement? Is the system configured to generate an error notification and stop accruing further leaves when the maximum leave accrual amount is reached?					BAI10 DSS01 DSS05

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.3.2 Are employees' leave accruals reviewed by relevant managers to assess for appropriateness of leaves taken by employees and to identify any excessive or negative balances?					DSS01 DSS06
3.4 Statutory obligations for payment of taxation are not breached.					
3.4.1 Is the accuracy and appropriateness of the amount of the Fringe Benefit Tax (FBT) return reviewed and approved by authorized personnel?					DSS01 DSS06
3.4.2 Are payroll edit and validation checks set up to utilize country-specific requirements?					DSS01 DSS06
3.5 Salary sacrifice arrangements are appropriately managed.					
3.5.1 Is the ability to establish and modify salary sacrifice details restricted to authorized personnel and in accordance with segregation of duties requirements?					DSS01 DSS06
3.5.2 Are salary package elements set up and reviewed independently to ensure that the sacrifice component has been captured accurately, and in accordance with the salary sacrifice agreement?					BAI10 DSS01 DSS06
3.6 Methodology for performance payment is established.					

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.6.1 Where bonus payments are based on a percentage of employee base salary or can be calculated using data established in the system, is the automated accrual and payment calculation utilized to reduce the risk of inaccurate accrual and calculation? Where automatically calculated, is the system output independently reviewed by an authorized HR representative for accuracy?					BAI10 DSS01 DSS05
3.7 Employee benefits are managed and administered in accordance with employee agreements.					
3.7.1 Is eligibility for employee benefits correctly established on the basis of pay structure/employee role/employee type?					BAI10 DSS01
3.7.2 Is access to establish benefit plans, enroll employees, create employee-specific information associated with the plans, and amend plans or employee information restricted to appropriately authorized personnel?					DSS05
3.8 Payroll system reconciles to the GL.					
3.8.1 Is the “posting to Accounting: Payroll Results not posted report” via transaction PC00_M99_PA03_CHECK reviewed on a regular basis?					DSS01 DSS06
3.8.2 Are payroll control reports and variance reports reviewed prior to finalization?					DSS01 DSS06

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.8.3 Is it ensured that reports that are reviewed prior to finalization of the payroll include, but are not limited to: <ul style="list-style-type: none">• Payroll exception reports: Lists exception messages (per employee) for a given payroll run• Payroll budget to variance reports: Facilitates variance analysis• Employee changes reports: Highlights new employees, terminated employees and transfers to ensure that only current and valid employees are included in the pay run					DSS01 DSS06
3.9 Executive payroll is adequately segregated.					
3.9.1 Is the executive payroll separated by employee group? Is access to executive payroll highly restricted?					DSS05
3.9.2 Is access to execute payroll restricted to the payroll team?					DSS05
3.10 Correct electronic funds transfer (EFT) payments are made.					
3.10.1 Is the system configured with the process for obtaining dual authorizations for all payments through electronic funds transfer (EFT)? Is the EFT file transferred for processing adequately secured with encryption and secure network channel?					DSS01 DSS06
4. Organizational Management					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
4.1 Organizational chart in SAP HCM accurately reflects current employees and their positions.					
4.1.1 Is the access to update the organizational chart restricted to authorized personnel? Are amendments processed based on appropriately approved documentation?					BAI06 DSS05
4.2 Organizational chart is set up according to relationships between employees, positions, organizational units and work centers.					
4.2.1 Is the organizational chart designed to reflect the hierarchy for each department or organizational unit? Is it reviewed by the appropriate official?					DSS01 DSS06
4.2.2 Is the organizational structure reviewed periodically for accuracy?					DSS01 DSS06
4.3 Job catalog is defined and configured correctly.					
4.3.1 Is the Jobs Catalog based on the job descriptions? Are the jobs in the catalog reviewed on a regular basis?					DSS01 DSS06
4.4 Positions created/maintained are valid and assigned correct relationship attributes.					
4.4.1 Are positions properly linked to the jobs and organizational units? Is complete position information captured for company requirements?					DSS01 DSS06
4.5 Integration between Personnel Administration and Personnel Development is set up correctly.					
4.5.1 Are all positions used in succession planning defined and configured with approved requirements and qualifications?					DSS01 DSS06

Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
5. Travel Management							
5.1 Accurate and complete entry of employee travel data.							
5.1.1 Are workflows configured to track and approve travel requests; make bookings using external reservation systems; and record, reimburse and post travel expenses?					BAI10 DSS01 DSS06		
5.1.2 Are relevant rules, profiles and parameters for travel components reviewed to ensure alignment with travel policies and procedures?					DSS01 DSS06		
5.2 The travel management system reconciles to the GL.							
5.2.1 Is the reconciliation of the travel management system and the GL done on consistent basis?					DSS06		
6. Enterprise Compensation Management							
6.1 Employee master file is valid, complete and accurate.							
6.1.1 Are base/merit compensation guidelines reviewed and approved by senior compensation leadership at the Authoritative Source? Is it verified that merit/merit compensation increases are submitted for approval by HR management prior to activation?					APO01		
6.1.2 Is the system configured with the compensation reports that are available for detailed analysis for an individual employee?					DSS06		
6.1.3 Is access to perform compensation adjustments restricted to authorized users?					DSS05		

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
6.1.4 Is access to change Compensation Matrix and or Salary Structure limited to authorized personnel?					DSS05
6.1.5 Are compensation plan changes (e.g., salary adjustments, bonuses, pay scale, etc.) reviewed and approved by executive leadership management?					APO01 BAI06
6.2 Performance incentives promote accurate financial reporting and ethical behavior.					
6.2.1 Does site leadership review sales compensation components as designed by the Authoritative Source and approve the components to be implemented for their site?					DSS06
6.2.2 Does the line supervisor review the weekly reports that document the compensation (IP [Incentive Pay] and/or commissions) for appropriateness?					DSS06
6.2.3 Are allocations made by the line management for each location's merit/base pay increases reviewed and monitored by the Authoritative Source for compliance with established budget guidelines?					DSS06
6.3 Sensitive information in personnel files is not disclosed and/or compromised.					
6.3.1 Is access to view salary structure limited to employees with direct reports and with authority to make a decision to change compensation?					DSS05 DSS06

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
6.3.2 Is access to view salary for employees with direct reports limited to the level of authority below employees' own level?					DSS05 DSS06
6.3.3 Is access to view sensitive compensation data restricted to authorized HR personnel and to managers that make a decision on compensation changes?					DSS05 DSS06
7. Employee Self-service and Manager Self-service					
7.1 No excessive or unauthorized access to sensitive HR data.					
7.1.1 Is ESS configured to restrict user to only update non-critical personal data, such as telephone number, address and relevant background information?					DSS05 DSS06
7.1.2 Are structural authorization profiles automatically assigned to users, ensuring that access is appropriately restricted?					DSS05 DSS06
7.1.3 Are end users restricted from access to change data to accounts other than their own?					DSS05 DSS06
7.2 Authorized approval of time, expense or other employee or HR data.					
7.2.1 Are standard leave and request forms used and is formal approval required?					DSS06
7.2.2 Is the system configured with alternate approvers in the case that a direct manager of an employee is away on leave or otherwise and is unable to fulfill his/her typical duties?					BAI10 DSS06

Human Capital Management Business Cycle ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
7.3 Managers Desktop “Themes” are configured to restrict users from unauthorized access to sensitive information.					
7.3.1 Is it ensured that no user has access to see all information, including sensitive and personal identifiable information?					BAI10 DSS05 DSS06

SAP ERP

BASIS Administration and Security
Audit/Assurance Program



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP ERP BASIS Administration and Security Audit/Accurance Program* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP's kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: <http://www.isaca.org/sap-erp-4th-edition>

Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOFFICIAL>

Like ISACA on Facebook: www.facebook.com/ISACAHQ

Acknowledgements

ISACA wishes to recognize

Project Leaders

Benjamin Fitts, CPA, Deloitte & Touche LLP, USA
Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA
Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA
Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Eva Sweet, CISA, CISM, ISACA, USA

Researchers

Syed Aamir Aarfi, Deloitte & Touche LLP, USA
Carlos Amaya, CISA, Deloitte & Touche LLP, USA
Dan Argynov, PMP, Deloitte & Touche LLP, USA
Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA
David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA
Ramamallikarjunarao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA
Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA
Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA
Sagnik Mukherjee, Deloitte & Touche LLP, USA
Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA
Sonik Shah, Deloitte & Touche LLP, USA
Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA
Shweta Srivastava, Deloitte & Touche LLP, USA
Anurag Tewary, Deloitte & Touche LLP, USA
Percy Tsai, CPA, Deloitte & Touche LLP, USA
Ravi Maddela Veeriah, Deloitte & Touche LLP, USA
Sravan Vemana, Deloitte & Touche LLP, USA
Anukool Vyas, Deloitte & Touche LLP, USA

Expert Reviewers

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA
Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada
Mayank Garg, CISA, NetApp, USA
Ricci leong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Jim Koveos, CISA, MBA, AmerisourceBergen, USA
Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia
Samuel LIM S.C., CISA, Auditor General's Office, Singapore
Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia
Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General's Office, Singapore
Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia
Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia
Paul O'Donnell, Ernst & Young, Canada
Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico
John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US
Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico
Naved Rehman, CISA, CRISC, MS-IS, SAPauditCoach, US
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US
Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico
Jovari St. Victor, CISA, CPA, Sunera, LLC, US
Surapong Surabotsoon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,
KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico
Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand
David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President
Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President
Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President
Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President
Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President
Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President
Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director
Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director
Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman
Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands
Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK
Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Anthony P. Noble, CISA, Viacom, USA
Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK
Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman
John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA
Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France
Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil
Jotham Nyamari, CISA, Deloitte, USA
James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK
Gurvinder Singh, CISA, CISM, CRISC, Australia
Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore
Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

SAP ERP BASIS Administration and Security Audit/Accurance Program

Introduction

This document contains an example audit/assurance program, **based on** the generic structure developed in section 2B of *COBIT 5 for Assurance*¹.

The engagement approach is based on, but **differs slightly** from the generic approach described in *COBIT 5 for Assurance*:

- The engagement approach described in this audit/assurance program **is focused on a business process** consequently no group of COBIT 5 processes dominates as primary processes and the lower-level processes are widespread, for evaluation purposes, the high-level COBIT 5 processes will be used as references.
- The assurance steps in this audit/assurance program are specific to the subject matter under review; therefore most of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources availableprocess audit/assurance program.

Assurance Engagement: SAP ERP BASIS Administration and Security

Assurance Topic

The topic covered by this assurance engagement is the SAP ERP BASIS Administration and Security.

Business Impact and Risk

SAP is widely used in many enterprises. Improper configuration of SAP could result in an inability for the enterprise to execute its critical processes.

Risk resulting from ineffective or incorrect configurations or use of SAP could result in some of the following:

- Disclosure of privileged information
- Single points of failure
- Low data quality
- Loss of physical assets
- Loss of intellectual property
- Loss of competitive advantage
- Loss of customer confidence
- Violation of regulatory requirements

Goal of the Review

The objective of the SAP ERP audit/assurance review is to provide management with an independent assessment relating to the effectiveness of configuration and security of the enterprise's SAP ERP architecture.

Scoping

The review will focus on configuration of the relevant SAP ERP components and modules within the enterprise. The selection of the specific components and modules will be based upon the risk introduced to the enterprise by these components and modules.

From a process reference model (PRM) perspective, the following domains and processes apply to this audit and assurance programme:

- APO01 Manage the IT management framework
- BAI03 Manage solutions identification and build

¹ See www.isaca.org/COBIT/Pages/Assurance-product-page.aspx for more information on *COBIT 5 for Assurance*.

- BAI06 *Manage changes*
- BAI07 *Manage change acceptance and transitioning*
- BAI10 *Manage configuration*
- DSS01 *Manage operations*
- DSS04 *Manage continuity*
- DSS05 *Manage security services*
- DSS06 *Manage business process controls*
- MEA01 *Monitor, Evaluate and Assess Performance and Conformance*
- MEA02 *Monitor, Evaluate and Assess the System of Internal Control*
- MEA03 *Monitor, Evaluate and Assess Compliance with External Requirements*

Testing SAP Security

To determine which users have access to the relevant authorizations used in this audit program, use one of the following methods:

1. Use transaction code SUIM → Users → Users by Complex Selection Criteria
2. Use transaction code S_BCE_68001417
3. Use transaction code SA38 and the program RSUSR002. This method allows the user to specify a transaction code, a "valid to" date for users, and up to three other authorization objects (which also may be the authorization object for transaction code S_TCODE) with associated values (two values under an AND relationship and three values under an OR relationship).
This method is generally sufficient for testing logical access security in relation to SAP ERP application infrastructure areas, but it is less suitable when large numbers of authorizations must be reviewed, such as in segregation of duties analysis and in some of the more complex areas of business cycle controls.
4. Use transaction code SUIM → Users → Users with Critical Authorizations (also accessible with program RSUSR008_009_NEW, which replaces programs RSUSR008 and RSUSR009 and transaction codes SU98 and/or SU99, for SAP Web AS 6.20 and later). This method offers improvements such as allowing differentiation between SAP defaults for critical data for different business areas, extended combination options for critical authorization data, improved performance, display of user filters and more analysis options for users in the result list.

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
A-1	Determine the stakeholders of the assurance initiative and their stakes .				
A-1.1	<u>Identify</u> the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	Intended user(s) of the assurance report	<p>Board/audit committee: Needs assurance over the effectiveness and efficiency of SAP ERP processes within the enterprise.</p> <p>Chief financial officer (CFO): Needs assurance that internal controls for financial applications work as intended.</p> <p>Risk managers: Need assurance that controls intended to address previously identified risk are working as intended. The results from the audit should be used to update the risk registry as needed.</p> <p>Security managers: Need to identify gaps in the security plans for SAP applications.</p> <p>Owners / shareholders: Part or all of the SAP ERP assurance report may be included in statutory reporting.</p> <p>Regulators: Part or all of SAP ERP reporting may need to be disclosed to respective authorities</p>		
A-1.2	Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	Accountable and responsible parties for the subject matter	<p>Business executives: The individuals responsible for identifying requirements, approving design and managing performance. These people are, together with IT management, responsible for managing the correct and controlled use of SAP ERP services—in line with good practices.</p> <p>Business process owners: Responsible for defining application and technical requirements. Responsible for data classification.</p> <p>IT management: Responsible for managing the correct and controlled use of SAP ERP services—together with the business executives.</p>		
A-2	<u>Determine</u> the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities (i.e., not achieving the enterprise goals).		<p>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.</p> <p>Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.</p> <p>Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</p> <p>Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.</p>		
A-2.1	<u>Understand</u> the enterprise strategy and priorities.	<i>Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.</i>			

Audit/Accurance Program for SAP ERP BASIS Administration and Security				
Phase A—Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
A-2.2	<u>Understand</u> the internal context of the enterprise.	<p><i>Identify all internal environmental factors that could influence the performance and contents of the SAP ERP BASIS Administration and Security Module.</i></p> <ul style="list-style-type: none"> Review prior report, if one exists, verify completion of any agreed-on corrections, and note remaining deficiencies. <p>Determine whether:</p> <ul style="list-style-type: none"> Senior management has assigned responsibilities for information, its processing and its use User management is responsible for providing information that supports the entity's objectives and policies Information systems management is responsible for providing the capabilities necessary for the achievement of the defined information systems objectives and the policies of the entity Senior management approves plans for development and acquisition of information systems There are procedures to ensure that the information system being developed or acquired meets user requirements There are procedures to ensure that information systems, programs and configuration changes are tested adequately prior to implementation All personnel involved in the system acquisition and configuration activities receive adequate training and supervision There are procedures to ensure that information systems are implemented/configured/upgraded in accordance with the established standards User management participates in the conversion of data from the existing system to the new system Final approval is obtained from user management prior to going live with a new information/upgraded system There are procedures to document and schedule all changes to information systems (including key ABAP programs) There are procedures to ensure that only authorized changes are initiated There are procedures to ensure that only authorized, tested and documented changes to information systems are accepted into the production client There are procedures to allow for and control emergency changes There are procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software There is a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated The organizational structure, established by senior management, provides for an appropriate segregation of incompatible functions The database, application and presentation servers are located in a physically separate and protected environment (i.e., a data center) Emergency, backup and recovery plans are documented and tested on a regular basis to ensure that they remain current and operational Backup and recovery plans allow users of information systems to resume operations in the event of an interruption Application controls are designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system Access to the Implementation Guide (IMG) during production has been restricted 		

Audit/Accurance Program for SAP ERP BASIS Administration and Security							
Phase A—Determine Scope of the Assurance Initiative							
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment		
		<ul style="list-style-type: none"> – The production client settings have been flagged to not allow changes to programs and configuration • Identify the significant risk and determine the key controls <ul style="list-style-type: none"> – Develop a high-level process flow diagram and overall understanding of the Basis Module, including the following subprocesses: <ul style="list-style-type: none"> a. Application installation (implementation guide and organizational model) b. Application development (ABAP/4 workbench and transport system) c. Application operations (computing center management system) d. Application security (profile generator and security administration) – Assess the key risk, determine key controls or control weaknesses, and test controls (refer to the sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: <ul style="list-style-type: none"> a. The controls culture of the organization (e.g., a just-enough-control philosophy). b. The need to exercise judgment to determine the key controls in the process and whether the controls structure is adequate. (Any weaknesses in the control structure should be reported to executive management and resolved.) • Gain an understanding of the SAP ERP environment (The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles) <p>In particular, the following information is important:</p> <ul style="list-style-type: none"> – Version and release of SAP ERP implemented – Total number of named users (for comparison with logical access security testing results) – Number of SAP instances and clients – Accounting period, company codes and chart of accounts – Identification of the components being used (Human Capital Management, Financials, Operations, Corporate Services) – Whether the organization has created any locally developed ABAP programs or reports – Details of the risk assessment approach taken in the organization to identify and prioritize risk – Copies of the organization's key security policies and standards <p>Obtain details of the following:</p> <ul style="list-style-type: none"> – Organizational Management Model as it relates to sales/revenue activity, i.e., sales organizational unit structure in SAP ERP and company sales organizational chart (required when evaluating the results of access security control testing) – An interview of the systems implementation team, if possible, and process design documentation for sales and distribution 					
A-2.3	Understand the external context of the enterprise.	<i>Identify all external environmental factors that could influence the performance and contents of the SAP ERP BASIS Administration and Security Module.</i>					
A-2.4	Given the overall assurance objective, translate the identified strategic priorities into concrete objectives for the assurance engagement.	<p>The following goals are retained as key goals to be supported, in reflection of enterprise strategy and priorities:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px;">Key goals</td> <td style="padding: 5px;">Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality </td> </tr> </table>		Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality 		
Key goals	Enterprise goals: <ul style="list-style-type: none"> • EG03 Managed business risk (safeguarding of assets) • EG04 Compliance with externals laws and regulations • EG07 Business service continuity and availability • EG11 Optimisation of business process functionality 						

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase A—Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
A-2.5	<u>Define</u> the organizational boundaries of the assurance initiative.	<ul style="list-style-type: none"> EG15 Compliance with internal policies <p>IT-related goals:</p> <ul style="list-style-type: none"> ITG01 Alignment of IT and business strategy ITG02 IT compliance and support for business compliance with external laws and regulations ITG04 Managed IT-related business risk ITG07 Delivery of IT services in line with business requirements ITG08 Adequate use of applications, information and technology solutions ITG09 IT Agility ITG10 Security of information, processing infrastructure and applications ITG12 Enablement and support of business processes by integrating applications and technology into business processes ITG14 Availability of reliable and useful information for decision making ITG15 IT compliance with internal policies ITG16 Competent and motivated business and IT personnel 			
		Additional goals			
A-2.5	<u>Define</u> the organizational boundaries of the assurance initiative.	<p><i>Describe the organizational boundaries of the assurance engagement, i.e., to which organizational entities the review is limited. All other aspects of scope limitation are identified during phase A-3.</i></p> <ul style="list-style-type: none"> The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment. Obtain information and form an understanding of the business reasons underlying the audit. Identify the senior business resources responsible for the review. Identify the senior IT audit/assurance resource responsible for the review. Establish the process for suggesting and implementing changes to the audit/assurance program, and list the authorizations required. Identify any limitations and/or constraints affecting the audit of specific systems and subsystems. Identify and third party services, applications, platforms and infrastructure elements that may not be or only partially be accessible. Identify any legal, regulatory or contractual constraints on audit. Identify any industrial relations based or end user based audit constraints. 			

Audit/Accurance Program for SAP ERP BASIS Administration and Security									
Phase A—Determine Scope of the Assurance Initiative									
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment				
A-3	Determine the enablers in scope and the instance(s) of the enablers in scope.	COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.							
A-3.1	<u>Define the Principles, Policies and Frameworks</u> in scope.	<p>Guiding principles and policies include:</p> <ul style="list-style-type: none"> • Policy for Master Data Maintenance • ISMS policy • Legal and regulatory compliance requirements 							
A-3.2	<u>Define which Processes</u> are in scope of the review. Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of process goals • Application of process good practices • Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments) 	<p><i>COBIT 5: Enabling Processes</i> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed.</p> <table border="1"> <tr> <td>Key processes</td><td> <ul style="list-style-type: none"> • Implementation Management Guide • Organizational Management Model • ABAP/4 Workbench • Transport Management System • Computer Center Management • Security Administration </td></tr> <tr> <td>Additional processes</td><td> <ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO07 Manage Human Resources • BAI03 Manage Solutions Identification and Build • BAI06 Manage Changes • BAI07 Manage Change Acceptance and Transitioning • BAI10 Manage Configuration • DSS01 Manage Operations • DSS03 Manage Problems • DSS04 Manage Continuity • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance • MEA02 Monitor, Evaluate and Assess the System of Internal Control • MEA03 Monitor, Evaluate and Assess Compliance with External Requirements </td></tr> </table>		Key processes	<ul style="list-style-type: none"> • Implementation Management Guide • Organizational Management Model • ABAP/4 Workbench • Transport Management System • Computer Center Management • Security Administration 	Additional processes	<ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO07 Manage Human Resources • BAI03 Manage Solutions Identification and Build • BAI06 Manage Changes • BAI07 Manage Change Acceptance and Transitioning • BAI10 Manage Configuration • DSS01 Manage Operations • DSS03 Manage Problems • DSS04 Manage Continuity • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance • MEA02 Monitor, Evaluate and Assess the System of Internal Control • MEA03 Monitor, Evaluate and Assess Compliance with External Requirements 		
Key processes	<ul style="list-style-type: none"> • Implementation Management Guide • Organizational Management Model • ABAP/4 Workbench • Transport Management System • Computer Center Management • Security Administration 								
Additional processes	<ul style="list-style-type: none"> • APO01 Manage the IT Management Framework • APO07 Manage Human Resources • BAI03 Manage Solutions Identification and Build • BAI06 Manage Changes • BAI07 Manage Change Acceptance and Transitioning • BAI10 Manage Configuration • DSS01 Manage Operations • DSS03 Manage Problems • DSS04 Manage Continuity • DSS05 Manage Security Services • DSS06 Manage Business Process Controls • MEA01 Monitor, Evaluate and Assess Performance and Conformance • MEA02 Monitor, Evaluate and Assess the System of Internal Control • MEA03 Monitor, Evaluate and Assess Compliance with External Requirements 								
A-3.3	<u>Define which Organisational Structures</u> will be in scope. Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of Organisational Structure goals, i.e., decisions • Application of Organisational Structures good practices 	Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement, and available resources will determine which ones will be reviewed in detail. <table border="1"> <tr> <td>Key Organisational Structures</td><td> <ul style="list-style-type: none"> • Basis team • ABAP team • System administration • Database administration • IT operations </td></tr> <tr> <td>Additional Organisational Structures</td><td> <ul style="list-style-type: none"> • Change management • Human resources </td></tr> </table>		Key Organisational Structures	<ul style="list-style-type: none"> • Basis team • ABAP team • System administration • Database administration • IT operations 	Additional Organisational Structures	<ul style="list-style-type: none"> • Change management • Human resources 		
Key Organisational Structures	<ul style="list-style-type: none"> • Basis team • ABAP team • System administration • Database administration • IT operations 								
Additional Organisational Structures	<ul style="list-style-type: none"> • Change management • Human resources 								
A-3.4	<u>Define the Culture, Ethics and Behaviour</u> aspects in scope.	In the context of this engagement, the following enterprise-wide culture and behaviours are in scope: <ul style="list-style-type: none"> • Risk and compliance aware culture 							

Audit/Accurance Program for SAP ERP BASIS Administration and Security									
Phase A—Determine Scope of the Assurance Initiative									
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment				
		<ul style="list-style-type: none"> • Enabling of continuous improvement • Accountability • Discipline to follow instructions 							
A-3.5	<u>Define the Information items</u> in scope. Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of Information goals, i.e., quality criteria of the information items • Application of Information good practices (Information attributes) 	Based on the subject matter of this audit/assurance program, the following Information items have been identified as key items. <table border="1"> <tr> <td>Key Information Items</td><td> <ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids </td></tr> <tr> <td>Additional Information Items</td><td> <ul style="list-style-type: none"> • Organizational charts </td></tr> </table>		Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 	Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 		
Key Information Items	<ul style="list-style-type: none"> • Data integrity procedures • Data classification guidelines • Data security and control guidelines • Assigned responsibilities for resource management • Access logs • Allocated roles and responsibilities • Allocated levels of authority • Allocated access rights • Evidence or error correction and remediation • Error reports and root cause analysis • Retention requirements • Record of transactions • Training manuals • Job aids 								
Additional Information Items	<ul style="list-style-type: none"> • Organizational charts 								
A-3.6	<u>Define the Services, Infrastructure and Applications</u> in scope.	In the context of this assignment, and taking into account the goals identified in A-2.4, the following services and related applications or infrastructure could be considered in scope of the review:							
A-3.7	<u>Define the People, Skills and Competencies</u> in scope. Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none"> • Achievement of skills set goals • Application of skills set and competencies good practices 	In the context of this engagement, taking into account key processes and key roles, the following skill sets are included in scope: <ul style="list-style-type: none"> • Proficiency using the SAP Basis Module • Database management skills • SAP Security skills and experience • Proficiency running SAP reports • Understanding of data classification policies • Understanding of data integrity procedures 							

Audit/Accurance Program for SAP ERP BASIS Administration and Security																											
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment																						
B-1	Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.																										
B-1.1	<p>Obtain (and agree on) metrics for enterprise goals and expected values of the metrics. Assess whether enterprise goals in scope are achieved.</p> <p>Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.</p> <p>Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</p> <p>The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>Enterprise Goal</th><th>Metric</th><th>Expected Outcome (Ex)</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>EG03 Managed business risk (safeguarding of assets)</td><td> <ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG04 Compliance with externals laws and regulations</td><td> <ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG07 Business service continuity and availability</td><td> <ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG11 Optimisation of business process functionality</td><td> <ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>EG15 Compliance with internal policies</td><td> <ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices </td><td>Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>	Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step	EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG04 Compliance with externals laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Enterprise Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
EG03 Managed business risk (safeguarding of assets)	<ul style="list-style-type: none"> Percent of critical business objectives and services covered by risk assessment Ratio of significant incidents that were not identified in risk assessments vs. total incidents Frequency of update of risk profile 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG04 Compliance with externals laws and regulations	<ul style="list-style-type: none"> Cost of regulatory non-compliance, including settlements and fines Number of regulatory non-compliance issues causing public comment or negative publicity Number of regulatory non-compliance issues relating to contractual agreements with business partners 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG07 Business service continuity and availability	<ul style="list-style-type: none"> Number of customer service interruptions causing significant incidents Business cost of incidents Number of business processing hours lost due to unplanned service interruptions Percent of complaints as a function of committed service availability targets 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG11 Optimisation of business process functionality	<ul style="list-style-type: none"> Frequency of business process capability maturity assessments Trend of assessment results Satisfaction levels of board and executives with business process capabilities 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
EG15 Compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices 	Agree on the expected values for the enterprise goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								
B-1.2	<p>Obtain (and agree on) metrics for IT-related goals and expected values of the metrics and assess whether IT-related goals in scope are achieved.</p> <p>The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>IT-related Goal</th><th>Metric</th><th>Expected Outcome (Ex)</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>ITG01 Alignment of IT and business strategy</td><td> <ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and </td><td>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </tbody> </table>	IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step	ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																		
IT-related Goal	Metric	Expected Outcome (Ex)	Assessment Step																								
ITG01 Alignment of IT and business strategy	<ul style="list-style-type: none"> Percent of enterprise strategic goals and requirements supported by IT strategic goals Level of stakeholder satisfaction with scope of the planned portfolio of programmes and 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																								

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	services <ul style="list-style-type: none"> Percent of IT value drivers mapped to business value drivers 		achieved.		
ITG02 IT compliance and support for business compliance with external laws and regulations	<ul style="list-style-type: none"> Cost of IT non-compliance, including settlements and fines, and the impact of reputational loss Number of IT-related non-compliance issues reported to the board or causing public comment or embarrassment Number of non-compliance issues relating to contractual agreements with IT service providers Coverage of compliance assessments 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
ITG04 Managed IT-related business risk	<ul style="list-style-type: none"> Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment Number of significant IT-related incidents that were not identified in risk assessment Percent of enterprise risk assessments including IT-related risk Frequency of update of risk profile 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
ITG07 Delivery of IT services in line with business requirements	<ul style="list-style-type: none"> Number of business disruptions due to IT service incidents Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels Percent of users satisfied with the quality of IT service delivery 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
ITG08 Adequate use of applications, information and technology solutions	<ul style="list-style-type: none"> Percent of business process owners satisfied with supporting IT products and services Level of business user understanding of how technology solutions support their processes Satisfaction level of business users with training and user manuals Net present value (NPV) showing business satisfaction level of the quality and usefulness of the technology solutions 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
ITG09 IT Agility	<ul style="list-style-type: none"> Level of satisfaction of business executives with IT's responsiveness to new requirements Number of critical business processes supported by up-to-date infrastructure and applications Average time to turn strategic IT objectives into an agreed-on and approved initiative 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
ITG10 Security of information, processing infrastructure and applications	<ul style="list-style-type: none"> Number of security incidents causing financial loss, business disruption or public embarrassment Number of IT services with outstanding security requirements Time to grant, change and remove access 	Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		privileges, compared to agreed-on service levels <ul style="list-style-type: none"> Frequency of security assessment against latest standards and guidelines 			
	ITG12 Enablement and support of business processes by integrating applications and technology into business processes	<ul style="list-style-type: none"> Number of business processing incidents caused by technology integration errors Number of business process changes that need to be delayed or reworked because of technology integration issues Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues Number of applications or critical infrastructures operating in silos and not integrated 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG14 Availability of reliable and useful information for decision making	<ul style="list-style-type: none"> Level of business user satisfaction with quality and timeliness (or availability) of management information Number of business process incidents caused by non-availability of information Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	
	ITG15 IT compliance with internal policies	<ul style="list-style-type: none"> Number of incidents related to non-compliance to policy Percent of stakeholders who understand policies Percent of policies supported by effective standards and working practices Frequency of policies review and update 	<i>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>	

Audit/Accurance Program for SAP ERP BASIS Administration and Security																													
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks																													
Ref.	Assurance Steps and Guidance			Issue Cross-reference																									
B-2	Obtain an understanding of the Principles, Policies and Frameworks in scope and set suitable assessment criteria. Assess Principles, Policies and Frameworks.																												
Principles, policies and frameworks: Policy for Master Data Maintenance																													
B-2.1a	<u>Understand the Principles, Policies and Frameworks context.</u> <i>Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks</i>																												
B-2.2a	<u>Understand the stakeholders of the Principles, Policies and Frameworks.</u> <i>Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.</i>																												
B-2.3a	<u>Understand the goals for the Principles, Policies and Frameworks</u> , and the related metrics and agree on expected values. Assess whether the Principles, Policies and Frameworks goals (outcomes) are achieved, i.e., assess the effectiveness of the Principles, Policies and Frameworks . Goal: The organization has defined, disseminated and deployed management policies supporting SAP master data maintenance .																												
<table border="1"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th><th></th><th></th></tr> </thead> <tbody> <tr> <td>Comprehensiveness</td><td>The set of policies is comprehensive in its coverage.</td><td>Verify that the set of policies is comprehensive in its coverage.</td><td></td><td></td></tr> <tr> <td>Currency</td><td>The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update </td><td>Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update </td><td></td><td></td></tr> <tr> <td>Flexibility</td><td>The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.</td><td>Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.</td><td></td><td></td></tr> <tr> <td>Availability</td><td> <ul style="list-style-type: none"> Policies are available to all stakeholders. Policies are easy to navigate and have a logical and hierarchical structure. </td><td> <ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. </td><td></td><td></td></tr> </tbody> </table>					Goal	Criteria	Assessment Step			Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.			Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 	Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 			Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.			Availability	<ul style="list-style-type: none"> Policies are available to all stakeholders. Policies are easy to navigate and have a logical and hierarchical structure. 	<ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. 		
Goal	Criteria	Assessment Step																											
Comprehensiveness	The set of policies is comprehensive in its coverage.	Verify that the set of policies is comprehensive in its coverage.																											
Currency	The set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 	Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 																											
Flexibility	The set of policies is flexible. It is structured in such a way that it is easy to add or update policies as circumstances require.	Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.																											
Availability	<ul style="list-style-type: none"> Policies are available to all stakeholders. Policies are easy to navigate and have a logical and hierarchical structure. 	<ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. 																											
B-2.4a	<u>Understand the life cycle stages of the Principles, Policies and Frameworks</u> , and agree on the relevant criteria. Assess to what extent the Principles, Policies and Frameworks life cycle is managed. <i>The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01 Manage the IT management framework.</i>																												
B-2.5a	<u>Understand good practices related to the Principles, Policies and Frameworks</u> and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. <i>The assurance professional will, by using appropriate auditing techniques assess the following aspects.</i>																												
<table border="1"> <thead> <tr> <th>Good Practice</th><th>Criteria</th><th>Assessment Step</th><th></th><th></th></tr> </thead> <tbody> <tr> <td>Scope and validity</td><td>The scope is described and the validity date is indicated.</td><td>Verify that the scope of the framework is described and the validity date is indicated.</td><td></td><td></td></tr> <tr> <td>Exception and escalation</td><td> <ul style="list-style-type: none"> The exception and escalation procedure is explained and commonly known. The exception and escalation procedure has not become the de facto standard procedure. </td><td> <ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. <p>Through observation of a representative sample, verify that the exception and escalation procedure has not become <i>de facto</i> standard procedure.</p> </td><td></td><td></td></tr> <tr> <td>Compliance</td><td>The compliance checking mechanism and non-compliance consequences are clearly described and enforced.</td><td>Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.</td><td></td><td></td></tr> </tbody> </table>					Good Practice	Criteria	Assessment Step			Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.			Exception and escalation	<ul style="list-style-type: none"> The exception and escalation procedure is explained and commonly known. The exception and escalation procedure has not become the de facto standard procedure. 	<ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. <p>Through observation of a representative sample, verify that the exception and escalation procedure has not become <i>de facto</i> standard procedure.</p>			Compliance	The compliance checking mechanism and non-compliance consequences are clearly described and enforced.	Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.							
Good Practice	Criteria	Assessment Step																											
Scope and validity	The scope is described and the validity date is indicated.	Verify that the scope of the framework is described and the validity date is indicated.																											
Exception and escalation	<ul style="list-style-type: none"> The exception and escalation procedure is explained and commonly known. The exception and escalation procedure has not become the de facto standard procedure. 	<ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. <p>Through observation of a representative sample, verify that the exception and escalation procedure has not become <i>de facto</i> standard procedure.</p>																											
Compliance	The compliance checking mechanism and non-compliance consequences are clearly described and enforced.	Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.																											

Audit/Assurance Program for SAP ERP BASIS Administration and Security

Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment
Principles, Policies and Frameworks

Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-2.1 to B-2.5	<p>Repeat steps B-2.1 through B-2.5 for all remaining Principles, Policies and Frameworks in scope.</p> <p>Repeat the steps described above for the remaining Principles, Policies and Frameworks:</p> <ul style="list-style-type: none">• ISMS policy• Legal and regulatory compliance requirements		

Audit/Accurance Program for SAP ERP BASIS Administration and Security																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment											
B-3	Obtain understanding of the Processes in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined. Assess the Processes.															
SAP ERP Basis process²: Application configuration (Implementation Management Guide [IMG])																
B-3.1a	<u>Understand the Process context.</u>															
B-3.2a	<u>Understand the Process purpose.</u>															
B-3.3a	<u>Understand</u> all process stakeholders and their roles. This is equivalent to understanding the real RACI chart of the process. <i>Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.</i> The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement: Implementation Management Guide (IMG) stakeholders:															
B-3.4a	<u>Understand the Process goals</u> and related metrics³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process. The Process Implementation Management Guide (IMG) has two defined process goal.			The following activities can be performed to assess whether the goals are achieved.												
<table border="1"> <thead> <tr> <th>Process Goal</th> <th>Related Metrics</th> <th>Criteria/Expected Value</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Configuration changes are made in the development environment and transported to production</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td>Changes to critical number ranges are controlled</td> <td>Determine the metrics that can be used to assess the achievement of the Process goals.</td> <td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> </tbody> </table>					Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	Configuration changes are made in the development environment and transported to production	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	Changes to critical number ranges are controlled	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step													
Configuration changes are made in the development environment and transported to production	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.													
Changes to critical number ranges are controlled	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.													
B-3.5a	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement: Define and agree on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.) <u>Agree</u> on the process practices that should be in place (process design). <u>Assess</u> the process design , i.e., assess to what extent: <ul style="list-style-type: none"> • Expected process practices are applied. • Accountability and responsibility are assigned and assumed. 															
	COBIT 5 Processes⁴ are described in COBIT 5: Enabling Processes . Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are: <ul style="list-style-type: none"> • A sound process design • The reference against which the process will be 			Each practice is typically implemented through a number of activities, and a well-designed process will implement all these practices and activities.												

² Because this is a business process audit/assurance program, several of the assurance steps associated with the COBIT 5 processes identified in step A-3.2 have been omitted. Audit/assurance programs for these processes can be found in the ISACA web site at <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx> and can be included in this audit/assurance program depending on the necessity to include them and on resources available.

³ For COBIT 5 processes, a set of goals and metrics are identified in **COBIT 5: Enabling Processes**.

⁴ For this audit/assurance program, COBIT 5 processes and their related activities are out of scope. Step B-3.5 describes the good practices and assurance steps for the SAP ERP BASIS processes in scope.

Audit/Accurance Program for SAP ERP BASIS Administration and Security																			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																			
Ref.	Assurance Steps and Guidance			Issue Cross-reference															
	assessed in phase B with the criteria as mentioned, i.e., all management practices are expected to be fully implemented.																		
	Reference Process	Implementation Management Guide (IMG)	Criteria: 1.1 Configuration changes are made in the development environment and transported to production.																
	Reference Process Practices ⁵	Good Practice	Assessment Step																
	BAI10 DSS05 DSS06	Configuration changes are made in the development environment and transported to production.	1.1.1 Use transaction code SCC4—Client Administration and double-click on each client being tested. Take note of the entries in the Last Changed By and Date fields as well as review for appropriate client settings. Production clients should reflect the following settings: <ul style="list-style-type: none"> • Client Role: Production • Changes and Transports for Client-Specific Objects: No changes allowed • Cross-Client Object Changes: No changes to Repository and crossclient Customizing objs • Protection: Client Copier and Comparison Tool: No overwriting • CATT and eCATT Restrictions: eCATT and CATT Not Allowed 																
	BAI10 DSS05 DSS06	Configuration changes are made in the development environment and transported to production.	1.1.2 Use transaction code SUIM—User Information System to test user access to the following transaction codes. <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td rowspan="3">SPRO—Customizing – Edit Project</td> <td>S_IMG_ACTV</td> <td></td> <td></td> </tr> <tr> <td>S_TABU_DIS</td> <td></td> <td></td> </tr> <tr> <td>S_TABU_CLI</td> <td></td> <td></td> </tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	SPRO—Customizing – Edit Project	S_IMG_ACTV			S_TABU_DIS			S_TABU_CLI				
Transaction(s)	Authorization Objects	Fields	Values																
SPRO—Customizing – Edit Project	S_IMG_ACTV																		
	S_TABU_DIS																		
	S_TABU_CLI																		
	DSS05 DSS06	Configuration changes are made in the development environment and transported to production.	1.1.3 Use transaction code SUIM—User Information System→Authorizations→Authorizations by Complex Selection Criteria to test user access to the following transaction codes. <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td rowspan="2">SCC4—Client Administration</td> <td>S_TABU_DIS</td> <td>ACTVT Authorization group</td> <td>02. SS</td> </tr> <tr> <td>S_TABU_CLI</td> <td>Cross-client Maintenance</td> <td>X</td> </tr> </tbody> </table> <p style="text-align: right;">There may be a few occasions when there will be a need to make a change directly to the production client without going through the transport path. Any such changes should be investigated thoroughly for business need, management approval, etc.</p>	Transaction(s)	Authorization Objects	Fields	Values	SCC4—Client Administration	S_TABU_DIS	ACTVT Authorization group	02. SS	S_TABU_CLI	Cross-client Maintenance	X					
Transaction(s)	Authorization Objects	Fields	Values																
SCC4—Client Administration	S_TABU_DIS	ACTVT Authorization group	02. SS																
	S_TABU_CLI	Cross-client Maintenance	X																

⁵ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP BASIS audit/assurance program.

Audit/Accurance Program for SAP ERP BASIS Administration and Security											
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes											
Ref.	Assurance Steps and Guidance			Issue Cross-reference							
	<p>If changes have been made to production client settings in the period under review, a log of changes to table T000 should be obtained to determine the nature of such changes obtained via transaction code SCU3—Table History. All changes to these critical settings should be authorized, documented and verified. This critical setting should be reviewed by IT management at least annually.</p> <p>Another alternative to identify changes made directly into production (bypassing the usual transport route) is to use transaction code SCC4— Client Administration → Utilities Menu → Change Logs → Input Data in Evaluation Period (the period for which one needs the direct production change log).</p>										
B-3.6a	<u>Agree on the process work products</u> ⁶ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess to what extent the process work products are available.</u> Process Implementation Management Guide (IMG) inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.										
	<table border="1"> <tr> <th>Process Practice</th><th>Work Products</th><th>Assessment Step</th></tr> <tr> <td>Implementation Management Guide (IMG)</td><td> <ul style="list-style-type: none"> Number of users logged on Number of transactions codes processed SAP database size per week </td><td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td></tr> </table>			Process Practice	Work Products	Assessment Step	Implementation Management Guide (IMG)	<ul style="list-style-type: none"> Number of users logged on Number of transactions codes processed SAP database size per week 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.		
Process Practice	Work Products	Assessment Step									
Implementation Management Guide (IMG)	<ul style="list-style-type: none"> Number of users logged on Number of transactions codes processed SAP database size per week 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.									
<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>											
			SAP ERP Basis process: Application configuration (Organizational Management Model [OMM])								
B-3.1b	<u>Understand the Process context.</u>										
B-3.2b	<u>Understand the Process purpose.</u>										
B-3.3b	<u>Understand all process stakeholders</u> and their roles.										
	Organizational Management Model (OMM) stakeholders:										
B-3.4b	Understand the Process goals and related metrics ⁷ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.										
	The Process Organizational Management Model (OMM) has three defined process goals.		The following activities can be performed to assess whether the goals are achieved.								
	<table border="1"> <tr> <th>Process Goal</th><th>Related Metrics</th><th>Criteria/Expected Value</th><th>Assessment Step</th></tr> <tr> <td>The organizational structure is accurate.</td><td>Determine the metrics that can be used to assess the achievement of the Process goals.</td><td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> </table>		Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	The organizational structure is accurate.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step								
The organizational structure is accurate.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.								
Changes to critical number ranges are controlled.		Determine the metrics that can be used to assess the achievement of									

⁶ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

⁷ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP BASIS Administration and Security						
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes						
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment
			<i>the Process goals.</i>		<i>values against which the assessment will take place.</i>	<i>assessment will be made whether the defined criteria are achieved.</i>
	Relevant company codes are set to Productive in the production environment.		<i>Determine the metrics that can be used to assess the achievement of the Process goals.</i>		<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>
B-3.5b	<u>Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:</u>					
	Reference Process	Organizational Management Model (OMM)	Criteria: 2.1 The organizational structure is accurate. 2.2 Changes to critical number ranges are controlled. 2.3 Relevant company codes are set to Productive in the production environment.			
	Reference Process Practices⁸	Good Practice	Assessment Step			
	APO01 DSS06	The organizational structure is accurate.	2.1.1 Access to the transaction code SPRO—Customizing—Edit Project and the authorization object (S_IMG_ACTV) for the IMG should be restricted in the production environment. Obtain information on the organizational model from the system using transaction code SPRO to display the IMG menu and follow the path: Enterprise Structure or by utilizing the SAP ERP Audit Information System that depicts the OMM graphically. Compare the model to the real enterprise structure and interview management in relation to differences or difficulties that may have emerged during or after the implementation.			
	DSS05 DSS06	Changes to critical number ranges are controlled.	2.2.1 Use transaction code SUIM—User Information System → Authorizations → Authorizations by Complex Selection Criteria to test user access to the following transaction codes: • SPRO—Customizing—Edit Project • SNUM—Number Range Driver • SNRO—Number Range Objects • Parameter transactions that reference SNUM or SNRO			
	APO01 BAI06	Relevant company codes are set to Productive in the production environment.	2.3.1 Transaction code OBR3—C FI Maintain Table T001 contains a list of company codes and indicates whether they have been set to Productive. Review the XProd field in table T001 using transaction code SE16N— General Table Display. Where the XProd field is set to X, the company code has been set to Productive. If company codes have not been set to Productive, investigate the reasons with management.			
	<u>Agree on the process work products⁹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design).</u> <u>Assess to what extent the process work products are available.</u>					
	Process Organizational Management Model (OMM) inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.					Criteria: All listed work products should demonstrably exist and be used.
	Process Practice	Work Products	Assessment Step			
	Organizational Management Model (OMM)		<ul style="list-style-type: none"> Organizational charts Financial statements Consolidation statement 		Apply appropriate audit techniques to determine the existence and appropriate use of each work product.	
	<u>Agree on the process capability level to be achieved by the process.</u>					

⁸ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Basis audit/assurance program.

⁹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in *COBIT 5: Enabling Processes*.

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	<i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				
SAP ERP Basis process: Application development (ABAP/4 Workbench)					
B-3.1c	<u>Understand the Process context.</u>				
B-3.2c	<u>Understand the Process purpose.</u>				
B-3.3c	<u>Understand all process stakeholders</u> and their roles.				
ABAP/4 Workbench stakeholders:					
B-3.4c	<u>Understand the Process goals</u> and related metrics ¹⁰ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the <u>effectiveness</u> of the process. The Process ABAP/4 Workbench has nine defined process goal.			The following activities can be performed to assess whether the goals are achieved.	
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step		
Changes to critical SAP ERP tables are authorized, logged by the system for management monitoring	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Changes made to the data dictionary are authorized and reviewed regularly.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Access to modify and develop queries is restricted.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
The creation or modification of programs is performed in the development system and migrated through the test system to production.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Only authorized customized transactions are available for use in the production environment.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Customized ABAP/4 programs are assigned to authorization groups	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		
Changes to the critical SAP ERP tables are logged by the system, and the periodic review.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.		

¹⁰ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP BASIS Administration and Security											
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes											
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment						
B-3.5c	Data Dictionary Information System reports are generated and reviewed by management.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.							
	Log and trace files are appropriately configured and secured.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.							
Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:											
	Reference Process	ABAP/4 Workbench	Criteria: 3.1 Changes to critical SAP ERP tables are authorized and logged by the system for management monitoring. 3.2 Changes made to the data dictionary are authorized and reviewed regularly. 3.3 Access to modify and develop queries is restricted. 3.4 The creation or modification of programs is performed in the development system and migrated through the test system to production. 3.5 Only authorized customized transactions are available for use in the production environment. 3.6 Customized ABAP/4 programs are assigned to authorization groups. 3.7 Changes to critical SAP ERP tables are logged by the system and are periodically reviewed. 3.8 Data Dictionary Information System reports are generated and reviewed by management. 3.9 Log and trace files are appropriately configured and secured.								
	Reference Process Practices ¹¹	Good Practice	Assessment Step								
	APO01 DSS05	Changes to critical SAP ERP tables are authorized and logged by the system for management monitoring.	3.1.1 Use transaction code SE16N—General Table Display to browse table TDDAT. Input Z* and Y* in the table name field to get a list of customized tables. The authorization field DICBERCLS will specify the table's authorization groups necessary for user access. To maintain a table, the DICBERCLS (authorization field) value in a user's authorization must match the DICBERCLS value for the table in the TDDAT file. The table must also be set in the data dictionary as Display/Maintenance Allowed or Display/Maintenance Allowed with Restrictions. The risk concerning customized tables may be mitigated by restricting access to modify critical tables. Use transaction code SUIM—User Information System → Users → Users by Complex Selection Criteria to test user access to modify critical tables via the following authorization object.								
			<table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>SM30—Call View Maintenance SM31_OLD—Old Table Maintenance</td> <td>S_TABU_DIS</td> <td>ACTVT</td> <td>02</td> </tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	SM30—Call View Maintenance SM31_OLD—Old Table Maintenance	S_TABU_DIS	ACTVT	02
Transaction(s)	Authorization Objects	Fields	Values								
SM30—Call View Maintenance SM31_OLD—Old Table Maintenance	S_TABU_DIS	ACTVT	02								

¹¹ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Basis audit/assurance program.

Audit/Accurance Program for SAP ERP BASIS Administration and Security												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes												
Ref.	Assurance Steps and Guidance			Issue Cross-reference								
				Comment								
		<p>If the table is cross-client, the user master record must contain a third object: S_TABU_CLI (value X).</p> <p>Critical system tables and security tables are assigned to authorization group SS. Both view and update access to group SS should be tightly controlled.</p> <p>Use transaction code SUIM—User Information System → Roles → Roles by Complex Selection Criteria to run a query of roles that have either update (activity 02) or view (activity 03) access to table authorization group SS. Update access activity 02 is required for S_TABU_DIS. Nonsupport personnel should not have update access to the system tables. View access should also be appropriately restricted.</p> <p>The report SUSR_TABLES_WITH_AUTH can be used to determine generic table access for users or single roles.</p>										
BAI06 DSS05 DSS06	Changes made to the data dictionary are authorized and reviewed regularly.	<p>3.2.1 Use transaction code SUIM— User Information System→Authorizations→ Authorizations by Complex Selection Criteria to test user access to the following authorization object.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>SE11—ABAP Dictionary SE12—ABAP/4 Dictionary Display SE15—ABAP/4 Repository Information System SE16—Data Browser SE38—ABAP Editor SE80—Object Navigator</td> <td>S_DEVELOP</td> <td>ACTVT</td> <td>01, 02, 06, 07</td> </tr> </tbody> </table> <p>Note: There may be other authorization objects required depending on how the system has been configured.</p>	Transaction(s)	Authorization Objects	Fields	Values	SE11—ABAP Dictionary SE12—ABAP/4 Dictionary Display SE15—ABAP/4 Repository Information System SE16—Data Browser SE38—ABAP Editor SE80—Object Navigator	S_DEVELOP	ACTVT	01, 02, 06, 07		
Transaction(s)	Authorization Objects	Fields	Values									
SE11—ABAP Dictionary SE12—ABAP/4 Dictionary Display SE15—ABAP/4 Repository Information System SE16—Data Browser SE38—ABAP Editor SE80—Object Navigator	S_DEVELOP	ACTVT	01, 02, 06, 07									
APO01 DSS05	Access to modify and develop queries is restricted.	<p>3.3.1 To be able to create new queries or modify existing ones in the Maintain Queries component, users must have an authorization for the authorization object S_QUERY with the value Change (02) in the roles assigned to their user master records. Without this authorization object, they can only execute existing queries. The components Maintain InfoSets and Maintain User Groups can be accessed only by users authorized with the authorization object S_QUERY with the value Maintain (23).</p> <p>Use transaction code SUIM—User Information System → Authorizations → Authorizations by Complex Selection Criteria to test user access to the following authorization object and identify all users who can create and maintain queries.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>SQ01— SAP Query: Maintain queries</td> <td>S_QUERY</td> <td>ACTVT</td> <td>02</td> </tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	SQ01— SAP Query: Maintain queries	S_QUERY	ACTVT	02		
Transaction(s)	Authorization Objects	Fields	Values									
SQ01— SAP Query: Maintain queries	S_QUERY	ACTVT	02									

Audit/Accurance Program for SAP ERP BASIS Administration and Security														
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes														
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment								
			<p>In addition, use the following authorization object to identify all users who can maintain functional areas and user groups:</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SQ02— SAP Query: Maintain InfoSet SQ03— AP Query: Maintain user groups</td><td>S_QUERY</td><td>ACTVT</td><td>23</td></tr> </tbody> </table> <p>This access should be restricted to limited users only (power users, Basis administrators) because they can expose confidential company information (human resources, financials, pricing and security) to an unauthorized user.</p> <p>End-user specific queries should be converted into custom transaction codes and users should be given access to these custom transaction codes. The same rule applies for the users with transaction codes SE16—Data Browser, SE16N—General Table Display and SE17—General Table Display access.</p>				Transaction(s)	Authorization Objects	Fields	Values	SQ02— SAP Query: Maintain InfoSet SQ03— AP Query: Maintain user groups	S_QUERY	ACTVT	23
Transaction(s)	Authorization Objects	Fields	Values											
SQ02— SAP Query: Maintain InfoSet SQ03— AP Query: Maintain user groups	S_QUERY	ACTVT	23											
DSS01 DSS05 DSS06	The creation or modification of programs is performed in the development system and migrated through the test system to production.	<p>3.4.1 Use transaction code SUIM—User Information System → Authorizations → Authorizations by Complex Selection Criteria to test user access to the following authorization object to obtain a list of users with authority to perform changes in the production system.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SE38— ABAP Editor SE37— ABAP Function Modules SE80—Object Navigator</td><td>S_DEVELOP</td><td>ACTVT</td><td>01, 02, 06</td></tr> </tbody> </table> <p>The ABAP/4 programs that are not assigned to an authorization group may be changed by any user who is assigned a developer's key and the correct object keys. Use transaction code SE16N with table DEVACCESS to identify the developer keys allowed in a client.</p>					Transaction(s)	Authorization Objects	Fields	Values	SE38— ABAP Editor SE37— ABAP Function Modules SE80—Object Navigator	S_DEVELOP	ACTVT	01, 02, 06
Transaction(s)	Authorization Objects	Fields	Values											
SE38— ABAP Editor SE37— ABAP Function Modules SE80—Object Navigator	S_DEVELOP	ACTVT	01, 02, 06											
BAI10 DSS05	Only authorized customized transactions are available for use in the production environment.	<p>3.5.1 By using transaction code SE16N, browse table TSTCT. In the TCODE field, enter Z* and then Y* to identify all of the custom transaction codes. Determine the transaction codes that appear to be test and/or backup codes and follow up with the SAP administrator regarding requirements.</p>												
APO01 DSS05	Customized ABAP/4 programs are assigned to authorization groups.	<p>3.6.1 Use transaction code SE16N to identify customized programs that have not been assigned to an authorization group. Browse the table TRDIR with program name values Z* and then Y* to produce a list of all customized programs. (Note that Z and Y are the standard naming conventions used when creating customized programs.) Filter the list for programs without a value in the authorization group field (SECU).</p> <p>Select a representative sample of customized programs from the list and check the source code to ensure that an authority-check statement is in place. Use transaction code SA38—ABAP Editor to run program RSABAPSC with the selected program name and authority check in the ABAP/4 language commands selection field to display the authority-check</p>												

Audit/Accurance Program for SAP ERP BASIS Administration and Security																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																	
Ref.	Assurance Steps and Guidance				Issue Cross-reference	Comment											
		<p>statements for each sampled program. The results will include any other programs called by the selected program with authority-check statements.</p> <p>Confirm the results of the test with management.</p> <p>Use transaction code SUIM—User Information System → Authorizations → Authorizations by Complex Selection Criteria to test the number of users who have access to execute all programs, independent of the authorization group assigned.</p> <table border="1" data-bbox="844 530 1636 750"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SA38—ABAP Reporting</td><td>S_PROGRAM</td><td>ACTVT</td><td>SUBMIT, BTCSUBMIT</td></tr> <tr> <td>SE37— ABAP Function Modules SE38—ABAP Editor SE80—Object Navigator</td><td>S_DEVELOP</td><td>ACTVT</td><td>16</td></tr> </tbody> </table> <p>Transaction code SA38—ABAP Reporting allows program execution. SE37—ABAP Function Modules allows access to the function builder. SE80—Object Navigator allows object editing. SE38—ABAP Editor allows users to edit the program and run it, creating an additional risk that the program may return inaccurate or incomplete information. Furthermore, allowing a user to run SE38 may lead to unauthorized changes to programs, potentially affecting system integrity.</p> <p>Review the policy, procedures and criteria for establishing program authorization groups, assigning the programs to groups and requiring authority-check statements in programs. Compare the results from testing to established policies, procedures, standards and guidance. (Note that enterprises may use additional transactions, tables, authorization objects, programs and reports to control their systems.)</p>	Transaction(s)	Authorization Objects	Fields	Values	SA38—ABAP Reporting	S_PROGRAM	ACTVT	SUBMIT, BTCSUBMIT	SE37— ABAP Function Modules SE38—ABAP Editor SE80—Object Navigator	S_DEVELOP	ACTVT	16			
Transaction(s)	Authorization Objects	Fields	Values														
SA38—ABAP Reporting	S_PROGRAM	ACTVT	SUBMIT, BTCSUBMIT														
SE37— ABAP Function Modules SE38—ABAP Editor SE80—Object Navigator	S_DEVELOP	ACTVT	16														
BAI07 DSS05	Changes to critical SAP ERP tables are logged by the system and are periodically reviewed.	<p>3.7.1 Review security procedures created by management that identify what tables are being logged and how often these logs are reviewed by management. For changes to be logged, the system profile parameter rec/client must be activated. Check this by reviewing the report RSPARAM and ensuring that the value for this parameter is set to All or to the client numbers that have table logging enabled.</p> <p>Tables that require changes to be logged need to be specified within the table DD09L. In addition to being listed here, critical tables must have the LOG field activated within the technical settings of each individual table. To test this, use transaction code SE16N—General Table Display and browse table DD09L. Tables to be logged should have an X in the PROTOKOLL field. To test each table, enter the specific table as the Table and/or view name in transaction code SE13—Maintain Technical Settings (Tables) and press Display. Review whether the checkbox Log Data Changes is set. Examples of tables that should be logged include:</p> <ul style="list-style-type: none"> • Clients (T000) • Company codes (T001) • Permitted Posting Periods (T001B) 															

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> • Foreign currency exchange rates (TCURR) <p>To test whether this control has been effective, use transaction code RSTBHIST—Table History, which calls program RSTBHIST (table change analysis) to list all changes to tables that have Log Data Changes activated in their technical settings for the period specified. Take a representative sample of changes to this table and compare these to the original supporting information and/or documentation. Obtain explanations for any changes for which supporting information or documentation is not available. Logging all table changes is likely to have a severe, adverse impact on system performance. Therefore, management should identify a refined list of critical tables to log and review.</p>			
DSS01 MEA01	Data Dictionary Information System reports are generated and reviewed by management.	3.8.1 Understand enterprise policies and procedures regarding the review of data dictionary reports. Assess the adequacy of such policies, procedures, standards and guidance, taking into account the frequency with which the review is performed, the level of detail in the reports, other independent data to which management compares the reports, the likelihood that the people performing the review will be able to identify exception items and the nature of exception items that they can be expected to identify.			
BAI10 DSS06	Log and trace files are appropriately configured and secured.	<p>3.9.1 Generate report RSPARAM and review the following parameter settings to obtain the locations of the log and trace files:</p> <ul style="list-style-type: none"> • Rslg/central/file (the active central log file name: Default filename is SLOG.J). • Rslg/central/old_file (the old central log file name: Default filename is SLOGJO). • Rslg/local/file (the local log file name: Default filename is SLOG < SAPSYSTEM number >). • Rstr/file (the absolute path name of the trace file: Trace file name is TRACE < SAP ERP System number >). <p>Obtain a copy of the permissions set on these files at the operating system level, and review it for adequacy.</p> <p>Execute transaction code SM21—Online System Log Analysis and review the logging configuration settings for reasonableness, including the size of each local and central log file.</p>			
B-3.6c	<u>Agree on the process work products</u> ¹² (inputs and outputs as defined in the process practices description) that are expected to be present (process design). <u>Assess to what extent the process work products are available.</u> Process ABAP/4 Workbench inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.				
	Process Practice ABAP/4 Workbench		Work Products <ul style="list-style-type: none"> • RICEFW object list (Report, Interfaces, Conversion, Enhancement, Form, Workflow) Criteria: All listed work products should demonstrably exist and be used.		
B-3.7c	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can</i>				

¹² For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
	<i>be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>				
SAP ERP Basis process: Transport Management System (TMS)					
B-3.1d	<u>Understand the Process context.</u>				
B-3.2d	<u>Understand the Process purpose.</u>				
B-3.3d	<u>Understand all process stakeholders</u> and their roles.				
	Transport Management System (TSM) stakeholders:				
B-3.4d	<u>Understand the Process goals</u> and related metrics ¹³ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the <u>effectiveness</u> of the process.				
	The Process Transport Management System (TSM) has one defined process goal.		The following activities can be performed to assess whether the goals are achieved.		
	Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	
	Application modifications are planned, tested and implemented following a phased approach.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
B-3.5d	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:				
	Reference Process	Transport Management System (TMS)	Criteria: 4.1 Application modifications are planned, tested and implemented following a phased approach.		
	Reference Process Practices ¹⁴	Good Practice	Assessment Step		
	APO01 BAI06 DSS05 DSS06	Application modifications are planned, tested and implemented following a phased approach.	4.1.1 Gain an understanding of the system landscape and client strategy by reviewing: <ul style="list-style-type: none">• Transport procedures between clients and instances• The change control policies and procedures for transporting objects between environments, including the enforcement of the procedures and available documentation• Transports and transport paths to check that appropriate change controls are followed. To view transport routes in the SAP environment, use transaction code STMS and click on Transport Routes for a general view of the current transport route.• A list of object types and procedures for objects that cannot be transported to production (e.g., some configuration, number ranges and master data changes) to ensure that they are documented and reviewed by management• The emergency change procedures• Change & Transport System logs using transaction code SE16—Use Data Browser and table E070 to view transport information.• Transaction code SE16N—General Table Display and table TADIR if repairs have been made directly to the production system Development standards, including naming conventions and development class assignment (using transaction code SE16N and		

¹³ For COBIT 5 processes, a set of goals and metrics are identified in *COBIT 5: Enabling Processes*.

¹⁴ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Basis audit/assurance program.

Audit/Accurance Program for SAP ERP BASIS Administration and Security																	
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																	
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment												
	<p>table TDEVC) for:</p> <ul style="list-style-type: none"> – Security – Programs – Transactions – Screens <ul style="list-style-type: none"> • The access policies over transport through transaction code STMS—Transport Management System and access to critical authorization objects (i.e., objects S_TRANSPRT and ACTVT except 03 and any transport type TTTYPE). (Note that transaction code STMS now controls the movement of objects from one SAP system to another. This was previously performed using transaction code SE06—Set Up Transport Organizer.) 																
B-3.6d	<p><u>Agree on the process work products</u>¹⁵ (inputs and outputs as defined in the process practices description) that are expected to be present (process design).</p> <p><u>Assess</u> to what extent the process work products are available.</p> <p>Transport Management System (TSM) inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.</p>			<p>Criteria: All listed work products should demonstrably exist and be used.</p>													
	<table border="1"> <thead> <tr> <th>Process Practice</th><th>Work Products</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>Transport Management System (TSM)</td><td> <ul style="list-style-type: none"> • List of transports migrated into the production environment every month </td><td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td></tr> </tbody> </table>			Process Practice	Work Products	Assessment Step	Transport Management System (TSM)	<ul style="list-style-type: none"> • List of transports migrated into the production environment every month 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.								
Process Practice	Work Products	Assessment Step															
Transport Management System (TSM)	<ul style="list-style-type: none"> • List of transports migrated into the production environment every month 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.															
B-3.7d	<p><u>Agree on the process capability level</u> to be achieved by the process.</p> <p><i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i></p>																
SAP ERP Basis process: Application operations (Computing Center Management System [CCMS])																	
B-3.1e	<u>Understand the Process context.</u>																
B-3.2e	<u>Understand the Process purpose.</u>																
B-3.3e	<u>Understand</u> all process stakeholders and their roles.																
	Computing Center Management System (CCMS) stakeholders:																
B-3.4e	<p><u>Understand the Process goals</u> and related <u>metrics</u>¹⁶ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process.</p> <p>The Process Computing Center Management System (CCMS) has nine defined process</p>			<p>The following activities can be performed to assess whether the goals are achieved.</p>													
	<table border="1"> <thead> <tr> <th>Process Goal</th><th>Related Metrics</th><th>Criteria/Expected Value</th><th>Assessment Step</th></tr> </thead> <tbody> <tr> <td>The Computing Center Management System (CCMS) is configured appropriately.</td><td>Determine the metrics that can be used to assess the achievement of the Process goals.</td><td>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</td><td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td></tr> <tr> <td>Batch processing operations are</td><td>Determine the metrics that can</td><td>Agree on the expected values for</td><td>In this step, the related metrics for each goal</td></tr> </tbody> </table>			Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step	The Computing Center Management System (CCMS) is configured appropriately.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	Batch processing operations are	Determine the metrics that can	Agree on the expected values for	In this step, the related metrics for each goal		
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step														
The Computing Center Management System (CCMS) is configured appropriately.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.														
Batch processing operations are	Determine the metrics that can	Agree on the expected values for	In this step, the related metrics for each goal														

¹⁵ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

¹⁶ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.5e	secured appropriately.	be used to assess the achievement of the Process goals.	the Process goal metrics, i.e., the values against which the assessment will take place.	will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Default system parameter settings are reviewed and configured to suit the enterprise's environment. Access to lock sensitive transaction codes has been restricted and sensitive transaction codes have been locked.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Sensitive transaction codes are locked in production.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Users are prevented from logging on with trivial or easily guessable passwords.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	The SAP Router is configured to act as a gateway to secure communications into and out of the SAP ERP environment.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	Remote access by software vendors is controlled adequately.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	The technology infrastructure is configured to secure communications and operations in the SAP ERP environment.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
	SAP ERP Remote Function Call (RFC) and Common Programming Interface—Communications (CPI-C) are secured.	Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
B-3.5e	Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:				
	Reference Process	Computing Center Management System (CCMS)	Criteria: 5.1 The Computing Center Management System (CCMS) is configured appropriately. 5.2 Batch processing operations are secured appropriately. 5.3 Default system parameter settings are reviewed and configured to suit the enterprise's environment. Access to lock sensitive transaction codes has been restricted and sensitive transaction codes have been locked. 5.4 Sensitive transaction codes are locked in production. 5.5 Users are prevented from logging on with trivial or easily guessable passwords. 5.6 The SAP Router is configured to act as a gateway to secure communications into and out of the SAP ERP environment.		

Audit/Accurance Program for SAP ERP BASIS Administration and Security												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes												
Ref.	Assurance Steps and Guidance			Issue Cross-reference								
Reference Process Practices ¹⁷	Good Practice	Assessment Step										
		<p>5.7 Remote access by software vendors is controlled adequately. 5.8 The technology infrastructure is configured to secure communications and operations in the SAP ERP environment. 5.9 SAP ERP Remote Function Call (RFC) and Common Programming Interface—Communications (CPI-C) are secured.</p>										
APO01 BAI03 DSS01 DSS05 DSS06	The Computing Center Management System (CCMS) is configured appropriately.	<p>5.1.1 Determine via inquiry whether transaction code RZ04—Maintain SAP Instances was used to set up operation's modes, instances and timetables to ensure that the CCMS displays meaningful data.</p> <p>Use transaction code SUIM— User Information System → Authorizations → Authorizations by Complex Selection Criteria and the following authorization object to generate a list of users with the ability to access the Alert Monitor.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>RZ20—CCMS monitoring</td><td>S_RZL_ADM</td><td>ACTVT</td><td>01, 03</td></tr> </tbody> </table> <p>Determine how the enterprise is monitoring its SAP ERP system. Understand the policies, procedures, standards and guidance regarding the execution of SAPSTART and STOPSAP programs or their equivalent in the enterprise's environment. Ensure that only authorized personnel may execute these programs. Interview the individuals responsible for the control activity. Ask them to describe: the steps involved, including the procedures for defining system and start-up profiles and ensuring that access is restricted to authorized users:</p> <ul style="list-style-type: none"> • Reports and other information, including how they are used • The procedures performed when exceptions or unusual items are encountered • Procedures relating to the clearance of alerts • How the control activity is performed in their absence • Any changes to the control activity during the period of intended reliance, including changes in the individuals who perform the activity <p>Obtain evidence that corroborates the responses to those inquiries by examining documentation, such as lists of users who can execute or modify the system and start-up profiles.</p>	Transaction(s)	Authorization Objects	Fields	Values	RZ20—CCMS monitoring	S_RZL_ADM	ACTVT	01, 03		
Transaction(s)	Authorization Objects	Fields	Values									
RZ20—CCMS monitoring	S_RZL_ADM	ACTVT	01, 03									
BAI07 DSS01 DSS05	Batch processing operations are secured appropriately.	<p>5.2.1 The capability to administer and release background jobs must be restricted through the use of the standard SAP ERP authorization objects. To test this control, use transaction code SUIM—User Information System → Authorizations → Authorizations by Complex Selection Criteria to obtain a list of users with the following authorizations.</p> <ul style="list-style-type: none"> • Batch input: 										

¹⁷ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP Basis audit/assurance program.

Audit/Accurance Program for SAP ERP BASIS Administration and Security

Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes

Ref.	Assurance Steps and Guidance					Issue Cross-reference	Comment																																																			
				<table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SM35—Batch Input Monitoring</td><td>S_BDC_MONI</td><td>BDCAKTI</td><td>DELE, FREE, LOCK, REOG</td></tr> <tr> <td></td><td>S_BDC_MONI</td><td>BDCGROUP</td><td>*</td></tr> </tbody> </table> <ul style="list-style-type: none"> Batch administration: <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SM36— Schedule Background Job</td><td>S_BTCH_ADMIN</td><td>BTCADMIN</td><td>Y</td></tr> </tbody> </table> <ul style="list-style-type: none"> Batch scheduling: <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SM36— Schedule Background Job</td><td>S_BTCH_JOB</td><td>JOBACTION</td><td>DELE, RELE</td></tr> <tr> <td></td><td>S_BTCH_NAM</td><td></td><td>*</td></tr> </tbody> </table> <ul style="list-style-type: none"> Batch processing: <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SM37— Overview of job selection</td><td>S_BTCH_JOB</td><td>JOBACTION</td><td>DELE, RELE, PLAN</td></tr> <tr> <td></td><td>S_BTCH_NAM</td><td>JOBACTION</td><td>*</td></tr> </tbody> </table> <ul style="list-style-type: none"> Event triggering: <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SM64—Manage Background Processing Events</td><td>S_BTCH_ADMIN</td><td>BTCADMIN</td><td>Y</td></tr> </tbody> </table> <p>Determine by corroborative inquiry whether upload programs have been removed from the production environment as appropriate.</p> <p>Check that access to Schedule batch job (transaction code SM36—Schedule Background Job) is appropriately assigned. Of particular importance is that batch jobs are scheduled to be executed by system (non-dialog) users. The level to which this is implemented is dependent on the enterprise's policies and procedures around batch job scheduling. The enterprise's policies and procedures around monitoring of batch jobs and handling of</p>	Transaction(s)	Authorization Objects	Fields	Values	SM35—Batch Input Monitoring	S_BDC_MONI	BDCAKTI	DELE, FREE, LOCK, REOG		S_BDC_MONI	BDCGROUP	*	Transaction(s)	Authorization Objects	Fields	Values	SM36— Schedule Background Job	S_BTCH_ADMIN	BTCADMIN	Y	Transaction(s)	Authorization Objects	Fields	Values	SM36— Schedule Background Job	S_BTCH_JOB	JOBACTION	DELE, RELE		S_BTCH_NAM		*	Transaction(s)	Authorization Objects	Fields	Values	SM37— Overview of job selection	S_BTCH_JOB	JOBACTION	DELE, RELE, PLAN		S_BTCH_NAM	JOBACTION	*	Transaction(s)	Authorization Objects	Fields	Values	SM64—Manage Background Processing Events	S_BTCH_ADMIN	BTCADMIN	Y		
Transaction(s)	Authorization Objects	Fields	Values																																																							
SM35—Batch Input Monitoring	S_BDC_MONI	BDCAKTI	DELE, FREE, LOCK, REOG																																																							
	S_BDC_MONI	BDCGROUP	*																																																							
Transaction(s)	Authorization Objects	Fields	Values																																																							
SM36— Schedule Background Job	S_BTCH_ADMIN	BTCADMIN	Y																																																							
Transaction(s)	Authorization Objects	Fields	Values																																																							
SM36— Schedule Background Job	S_BTCH_JOB	JOBACTION	DELE, RELE																																																							
	S_BTCH_NAM		*																																																							
Transaction(s)	Authorization Objects	Fields	Values																																																							
SM37— Overview of job selection	S_BTCH_JOB	JOBACTION	DELE, RELE, PLAN																																																							
	S_BTCH_NAM	JOBACTION	*																																																							
Transaction(s)	Authorization Objects	Fields	Values																																																							
SM64—Manage Background Processing Events	S_BTCH_ADMIN	BTCADMIN	Y																																																							

Audit/Accurance Program for SAP ERP BASIS Administration and Security												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes												
Ref.	Assurance Steps and Guidance			Issue Cross-reference								
				Comment								
		<p>batch job exceptions should also be determined through corroborative inquiry. Note that users with S_BTCH_JOB object access can manage their own batch jobs. The object S_BTCH_JOB does not provide privileges to manage other jobs. The objects S_BTCH_ADM and S_BTCH_NAM determine the user's ability to manage all jobs, including the jobs created by others. Therefore, it is quite possible for a few power users to create and manage their own jobs. However, the access to manage overall SAP jobs should be restricted to the people with SAP job-handling responsibility.</p>										
BAI07 DSS01	Default system parameter settings are reviewed and configured to suit the enterprise's environment. Access to lock sensitive transaction codes has been restricted and sensitive transaction codes have been locked.	<p>5.3.1 Configure system parameters for each instance using transaction codes RZ10—Maintain Profile Parameters and RZ11—Profile Parameter Maintenance. Ideally, these settings should be synchronized across servers and consistent with IT security policy for the SAP ERP application. It is important, when more than one instance is used and the parameters have not been synchronized, that this test be performed for each instance. Run report RSPARAM via transaction code SA38—ABAP Reporting and review the key parameter settings for appropriateness. Alternatively, execute transaction code TU02—Parameters Changes to obtain the current setting for all hosts and the history of changes to parameters. Set RSPARAM settings for key system parameters to match the enterprise's specifications and provide sufficient control to mitigate the risk of unauthorized access.</p> <p>The capability to configure application server parameters must be restricted through the use of the standard SAP ERP authorization objects. To test this control, use transaction code SUIM—User Information System → Authorizations → Authorizations by Complex Selection Criteria to obtain a list of users with the following authorizations.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>RZ10— Maintain Profile Parameters RZ11— Profile Parameter Maintenance</td><td>S_RZL_ADM</td><td>ACTVT</td><td>01, 03</td></tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	RZ10— Maintain Profile Parameters RZ11— Profile Parameter Maintenance	S_RZL_ADM	ACTVT	01, 03		
Transaction(s)	Authorization Objects	Fields	Values									
RZ10— Maintain Profile Parameters RZ11— Profile Parameter Maintenance	S_RZL_ADM	ACTVT	01, 03									
DSS05	Sensitive transaction codes are locked in production.	<p>5.4.1 Use transaction code SUIM—User Information System to generate a list of all users who have access to locked or unlocked transaction codes in the system (users with the transaction code SM01—Lock Transactions). Review and confirm the list with management to ensure that only authorized users have access. Enter transaction code RSAUDITC_BCE—Display Locked Transactions to display a list of transaction codes which are locked or unlocked. Review sensitive transaction codes to ensure that they have been locked from user access. Such transaction codes include, but are not limited to (see Appendix G for a more comprehensive list of sensitive transactions to be locked):</p> <ul style="list-style-type: none"> • SCC5—Client delete • SCC1—Client copy (may overwrite the production client) • SM49—Execute external OS commands (may allow pass-through to the operating system) • SM69—Maintain external OS commands (may allow pass-through to the operating system) 										
BAI06 DSS05	Users are prevented from logging on with trivial or easily guessable passwords.	5.5.1 All illegal passwords are maintained within table USR40, which can be accessed via transaction code SE16—Data Browser. Review this table to ensure that the disallowed passwords contained in it appear reasonable and are consistent with management's										

Audit/Accurance Program for SAP ERP BASIS Administration and Security												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes												
Ref.	Assurance Steps and Guidance			Issue Cross-reference								
				Comment								
		<p>intentions.</p> <p>View configured password parameters via report RSPARAM (accessed via transaction code SA38—ABAP Reporting).</p> <p>Obtain the last update of these values (to determine whether they have been in place for the entirety of the audit review period) by accessing transaction code TU02—Parameter Changes and selecting History of File.</p>										
	BAI06 DSS01 DSS03 DSS05	<p>The SAP Router is configured to act as a gateway to secure communications into and out of the SAP ERP environment.</p> <p>5.6.1 Request an extract of the SAP router permissions table (e.g., by executing the UNIX command SAP router –L <path>) from the operating system administrator. This list contains the host names and port numbers of the predecessor and successor points on the route and the passwords required to set up the connection.</p> <p>Review this table to ensure that all entries have been authorized by management. This usually can be achieved by obtaining the relevant change control documentation for the last date on which the file was modified. In addition, determine from the listing whether passwords have been established for all entries in the route permission table.</p> <p>Obtain the file permissions set on the SAP Router table and review them to ensure that only authorized users have access to modify the entries within this table.</p> <p>The SAP Router log file can be activated when SAP Router is started. The log will identify instances, such as:</p> <ul style="list-style-type: none"> • Connection from (client name and/or address) • Connection to (partner name and/or address) • Partner service • Start time • End time • Connection requests rejected after checking the route permission table <p>Activate this function by entering the operating system command SAP router –r –G <logfile>. <logfile> is the relative path name specified for the log file. Monitor the remote connections by checking the SAP Router log file and using the Monitoring Users Overview function from the administration menu.</p>										
	BAI06	<p>Remote access by software vendors is controlled adequately.</p> <p>5.7.1 Use transaction code SUIM—User Information System→Authorizations→Authorizations by Complex Selection Criteria to review the system for users with the following authorizations:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: black; color: white;"> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>SM69—Maintain External OS Commands</td> <td>S_RZL_ADMIN</td> <td>ACTVT</td> <td>01</td> </tr> </tbody> </table>	Transaction(s)	Authorization Objects	Fields	Values	SM69—Maintain External OS Commands	S_RZL_ADMIN	ACTVT	01		
Transaction(s)	Authorization Objects	Fields	Values									
SM69—Maintain External OS Commands	S_RZL_ADMIN	ACTVT	01									

Audit/Accurance Program for SAP ERP BASIS Administration and Security														
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes														
Ref.	Assurance Steps and Guidance						Issue Cross-reference	Comment						
			SM49—Execute external OS commands	S_RZL_ADMIN_LOG_COM	ACTVT COMMAND HOST OPSYSTEM	01 Check values								
			Use transaction code SM69 (maintain external commands) and SM49 (execute external commands) to provide the list of commands that have been defined and those that can be executed, respectively. Review for appropriateness.											
	BAI06 BAI10 DSS01 DSS04 DSS05 DSS06 MEA02 MEA03	The technology infrastructure is configured to secure communications and operations in the SAP ERP environment.	5.8.1 Because of the wide variation in remote access facilities available, it is difficult to specify what is acceptable for a particular site. However, management should be aware of the risk involved with remote access and have a specific policy to cover this issue. The policy should be consistent with best practices as outlined previously, and it should be possible to test compliance.	To obtain a list of SAP Service Marketplace users on the production client, enter transaction code OSS1—Logon to SAPNet using the client's administrator ID. Click on the SAPNET icon followed by the Administration icon. Perform an authorization analysis by authorization object view. This will provide a list of all users assigned to SAP Service Marketplace by authorization object. In particular, ensure that management reviews for reasonableness the users who are assigned to administration authorization and open service connections.										
	DSS05	SAP ERP Remote Function Call (RFC) and Common Programming Interface— Communications (CPI-C) are secured.	5.9.1 Execute transaction code SM59— RFC Destinations (Display/Maintain) in all SAP systems in the landscape. This will display the table RFCDES, which controls the communication between systems. The table lists the RFC destinations, which includes all SAP ERP connections on the system. Expand each of the SAP ERP connections, and double-click on each connection to verify that no dialog user ID is listed with its password in the Logon & Security tab.											
B-3.6e	<u>Agree on the process work products</u> ¹⁸ (inputs and outputs as defined in the process practices description) that are expected to be present (process design). Assess to what extent the process work products are available.													
	Computing Center Management System (CCMS) inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.					Criteria: All listed work products should demonstrably exist and be used.								
	Process Practice Computing Center Management System (CCMS)		Work Products <ul style="list-style-type: none"> List of failed batch jobs System parameters report 		Assessment Step Apply appropriate audit techniques to determine the existence and appropriate use of each work product.									
B-3.7e	<u>Agree on the process capability level</u> to be achieved by the process. <i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>													
SAP ERP Basis process: Application security (SA)														
B-3.1f	<u>Understand the Process context.</u>													
B-3.2f	<u>Understand the Process purpose.</u>													

¹⁸ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-3.3f	<u>Understand all process stakeholders</u> and their roles. Application security (SA) stakeholders:				
B-3.4f	<u>Understand the Process goals</u> and related <u>metrics</u> ¹⁹ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the effectiveness of the process. The Process Application security (SA) has seven defined process goals.			The following activities can be performed to assess whether the goals are achieved.	
Process Goal		Related Metrics	Criteria/Expected Value	Assessment Step	
Duties within the security administration environment are adequately segregated.		Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
Adequate security authorization documentation is maintained.		Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
The superuser SAP* is properly secured.		Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
Default users are secured properly.		Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
Access to powerful profiles is restricted.		Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
The authorization group that contains powerful users is restricted.		Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
Changes to Central User Administration (CUA) are authorized and reviewed regularly by management.		Determine the metrics that can be used to assess the achievement of the Process goals.	Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.	
B-3.5f	<u>Agree on suitable criteria to evaluate all processes in scope of the assurance engagement:</u>				
	Reference Process	Application security (SA)	Criteria: 6.1 Duties within the security administration environment are adequately segregated. 6.2 Adequate security authorization documentation is maintained. 6.3 The superuser SAP* is properly secured. 6.4 Default users are secured properly. 6.5 Access to powerful profiles is restricted. 6.6 The authorization group that contains powerful users is restricted. 6.7 Changes to Central User Administration (CUA) are authorized and reviewed regularly by management.		

¹⁹ For COBIT 5 processes, a set of goals and metrics are identified in COBIT 5: Enabling Processes.

Audit/Accurance Program for SAP ERP BASIS Administration and Security																																								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																								
Ref.	Assurance Steps and Guidance			Issue Cross-reference																																				
Reference Process Practices ²⁰	Good Practice	Assessment Step																																						
	<p>APO01 DSS05 DSS06</p> <p>Duties within the security administration environment are adequately segregated.</p>	<p>6.1.1 Determine whether the system administrator tasks are segregated into the following administrator functions. Use transaction code SUIM— User Information System→ Authorizations → Authorizations by Complex Selection Criteria to generate a user lists for the following authorizations.</p> <p>For the Profile Generator:</p> <ul style="list-style-type: none"> • Create and change roles—used to define and update roles <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PFCG—Profile Generator</td><td>S_USER_AGR</td><td>ACTVT</td><td>01, 22</td></tr> </tbody> </table> <ul style="list-style-type: none"> • Transport roles—used to transport or activate roles to or in production <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PFCG—Profile Generator</td><td>S_USER_AGR</td><td>ACTVT</td><td>21</td></tr> </tbody> </table> <ul style="list-style-type: none"> • Assign roles and/or profiles to user master records—used to assign or transfer roles and/or profiles into the user master records for the relevant users <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>PFCG—Profile Generator SU01—User Maintenance</td><td>S_USER_AGR S_USER_GRP</td><td>ACTVT</td><td>22</td></tr> <tr> <td></td><td></td><td></td><td>22</td></tr> </tbody> </table> <p>For user master maintenance:</p> <ul style="list-style-type: none"> • Create, change, lock and/or delete changes: <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SU01—User Maintenance</td><td>S_USER_GRP</td><td>ACTVT</td><td>01, 02, 05, 06</td></tr> </tbody> </table> <p>If full segregation is not possible among the four functions listed above, management should, at minimum, consider segregating the creation of roles and/or profiles and assignment of roles</p>	Transaction(s)	Authorization Objects	Fields	Values	PFCG—Profile Generator	S_USER_AGR	ACTVT	01, 22	Transaction(s)	Authorization Objects	Fields	Values	PFCG—Profile Generator	S_USER_AGR	ACTVT	21	Transaction(s)	Authorization Objects	Fields	Values	PFCG—Profile Generator SU01—User Maintenance	S_USER_AGR S_USER_GRP	ACTVT	22				22	Transaction(s)	Authorization Objects	Fields	Values	SU01—User Maintenance	S_USER_GRP	ACTVT	01, 02, 05, 06		
Transaction(s)	Authorization Objects	Fields	Values																																					
PFCG—Profile Generator	S_USER_AGR	ACTVT	01, 22																																					
Transaction(s)	Authorization Objects	Fields	Values																																					
PFCG—Profile Generator	S_USER_AGR	ACTVT	21																																					
Transaction(s)	Authorization Objects	Fields	Values																																					
PFCG—Profile Generator SU01—User Maintenance	S_USER_AGR S_USER_GRP	ACTVT	22																																					
			22																																					
Transaction(s)	Authorization Objects	Fields	Values																																					
SU01—User Maintenance	S_USER_GRP	ACTVT	01, 02, 05, 06																																					

²⁰ This section lists COBIT 5 activities supporting the assurance steps for the SAP ERP BASIS audit/assurance program.

© 2015 ISACA

All rights reserved.

Audit/Accurance Program for SAP ERP BASIS Administration and Security																																
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes																																
Ref.	Assurance Steps and Guidance			Issue Cross-reference																												
				Comment																												
		<p>and/or profiles. If the segregation of duties option is practical, assess and analyze change documents for users, profiles and authorizations through transaction code SUIM—User Information System→ Change Documents→ For Users/For Profiles/For Authorizations for evidence of review and action by management.</p> <p>Consider identifying which user IDs have created, deleted, locked or unlocked user IDs during the period under review and determine whether such actions were appropriate. Obtain this information through transaction code SUIM—User Information System→ Change Documents→ For Users, entering relevant date parameters and selection criteria.</p> <p>Review access to effect mass changes to user master records (UMRs) as follows.</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SU10—User Mass Maintenance</td><td>S_USER_GRP</td><td>ACTVT</td><td>01, 02, 05, 06</td></tr> <tr> <td>SU12—Mass Changes to User Master Records</td><td>S_USER_PRO</td><td>ACTVT</td><td>01, 02, 05, 06</td></tr> </tbody> </table> <p>Manual maintenance was used prior to the introduction of the Profile Generator for the purpose of role maintenance.</p> <ul style="list-style-type: none"> Authorization maintenance: <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SU03—Maintain Authorizations</td><td>S_USER_AUT</td><td>ACTVT</td><td>01, 02, 07, 22</td></tr> </tbody> </table> <ul style="list-style-type: none"> User maintenance: <table border="1"> <thead> <tr> <th>Transaction(s)</th><th>Authorization Objects</th><th>Fields</th><th>Values</th></tr> </thead> <tbody> <tr> <td>SU02—Maintain Authorization Profiles</td><td>S_USER_PRO</td><td>ACTVT</td><td>01, 02, 07, 22</td></tr> </tbody> </table> <p>Although the transaction codes SU02 and SU03 are still able to be used, SAP recommends the use of PFCG—Profile Generator for role and/or profile maintenance.</p>	Transaction(s)	Authorization Objects	Fields	Values	SU10—User Mass Maintenance	S_USER_GRP	ACTVT	01, 02, 05, 06	SU12—Mass Changes to User Master Records	S_USER_PRO	ACTVT	01, 02, 05, 06	Transaction(s)	Authorization Objects	Fields	Values	SU03—Maintain Authorizations	S_USER_AUT	ACTVT	01, 02, 07, 22	Transaction(s)	Authorization Objects	Fields	Values	SU02—Maintain Authorization Profiles	S_USER_PRO	ACTVT	01, 02, 07, 22		
Transaction(s)	Authorization Objects	Fields	Values																													
SU10—User Mass Maintenance	S_USER_GRP	ACTVT	01, 02, 05, 06																													
SU12—Mass Changes to User Master Records	S_USER_PRO	ACTVT	01, 02, 05, 06																													
Transaction(s)	Authorization Objects	Fields	Values																													
SU03—Maintain Authorizations	S_USER_AUT	ACTVT	01, 02, 07, 22																													
Transaction(s)	Authorization Objects	Fields	Values																													
SU02—Maintain Authorization Profiles	S_USER_PRO	ACTVT	01, 02, 07, 22																													
BAI07 DSS04	Adequate security authorization documentation is maintained.	<p>6.2.1 Review the system design documentation relating to authorizations and profiles; any established policies, procedures, standards and guidance related to the maintenance of profiles and/or authorizations; and the list of profiles and/or authorizations defined in the system.</p> <p>Perform the following tests to ensure the appropriateness of the documentation: Review the process in place when new access is granted, such as who is authorized to approve the access and how the issues concerning segregation of duties are addressed (use of automated tools, such as SAP GRC Access Risk Analysis [ARA] or manual tracking of segregation of duties activities).</p>																														

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		<ul style="list-style-type: none"> Identify users created during the period of review and validate that the new user access has been appropriately approved. The user creation date information is available in the USR02 table. The relevant fields from the USR02 table are: BNAME—User ID ERDAT—Date of user master record creation Validate that there is a periodic process to review user access with the appropriate authority (e.g., module owners). This will identify users who have access to the system without a valid business need. Take a representative sample of profiles and authorizations from the system, and confirm them against the original documentation. Resolve any discrepancies with management. Test changes to authorization and profiles during the audit period, using the SAP ERP change documents for users, profiles and authorizations through transaction code SUIM—User Information System → Change Documents → For Users/For Profiles/For Authorizations. This involves taking a sample of changes from the system and tracing them back to current documentation. Management should be able to provide source documentation for the authorization of these changes. 			
DSS05	The superuser SAP* is properly secured.	<p>6.3.1 To determine whether the SAP* user has been locked, execute transaction code SUIM—User Information System→Authorizations →Authorizations by Complex Selection Criteria. Enter SAP* in the user field and press F8. Verify that the SAP* user group field is Super. Click on the Other View button twice. The user status field for SAP* should say Locked.</p> <p>To test whether the default password has been changed for the account SAP*, execute transaction code SA38—ABAP Reporting and program RSUSR003 (Display Profile Parameters should be unchecked). This report details all clients that have been installed in the SAP ERP instance subject to review. For each client, the report details whether the password used for SAP* is trivial (i.e., set at default).</p> <p>Confirm that SAP* is not created in client 066 (EarlyWatch client).</p>			
DSS05	Default users are secured properly.	6.4.1 To test whether the default password has been changed for these users, execute the SAP ERP report RSUSR003 (Display Profile Parameters should be unchecked) and determine whether the default passwords have been changed in all clients.			
APO01 DSS05 DSS06	Access to powerful profiles is restricted.	<p>6.5.1 Review users assigned to the privileged profiles of SAP_ALL and SAP_NEW for appropriateness. Assign users who have been assigned these superuser profiles to user group Super or an equivalent, which should be maintained by a limited number of BASIS personnel only.</p> <p>To perform this test, use transaction code SUIM—User Information System →Select Users →Users by Complex Selection Criteria. In the Selection Criteria for User section, enter SAP_ALL into the profile name field. Click on the button to the right of the text box. Enter SAP_NEW in the first empty text box. Click on the Copy button. Then, click on Execute. This lists all users with superuser functionality.</p> <p>Similarly, other powerful profiles to check for user access include S_A.SYSTEM (system administration authorizations), S_RZL_ADMIN (CCMS administration authorizations), S_USER_ALL (all user administration authorizations), S_A.USER (BASIS authorizations for BASIS end users), S_ABAP_ALL (all ABAP/4 authorizations) and S_A.ADMIN (system</p>			

Audit/Accurance Program for SAP ERP BASIS Administration and Security												
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes												
Ref.	Assurance Steps and Guidance			Issue Cross-reference								
				Comment								
		<p>operation authorizations). These profiles provide SAP ERP administration and development authorizations.</p> <p>Check the user list identified by this test to ascertain whether individuals who have access to privileged functionality require this access, based on their job responsibilities and established policies, procedures, standards and guidance.</p>										
	APO01 DSS05	<p>The authorization group that contains powerful users is restricted.</p> <p>6.6.1 Identify the system administrators within the enterprise and determine to what user groups their user IDs belong.</p> <p>Use transaction code SUIM—User Information System → Users → Users by Complex Selection Criteria, review the system for users with the following authorizations:</p> <table border="1"> <thead> <tr> <th>Transaction(s)</th> <th>Authorization Objects</th> <th>Fields</th> <th>Values</th> </tr> </thead> <tbody> <tr> <td>SU01—User Maintenance</td> <td>S_USER_GRP</td> <td>ACTVT</td> <td>01, 02, 06</td> </tr> </tbody> </table> <p>The authorization field user group in user master maintenance should be similar to one of the values identified earlier. This is usually the group SUPER.</p> <p>Conduct an independent review of SAP ERP change documents for users, profiles and authorizations through transaction code SUIM—User Information System → Change Documents → For Users/For Profiles/For Authorizations.</p>	Transaction(s)	Authorization Objects	Fields	Values	SU01—User Maintenance	S_USER_GRP	ACTVT	01, 02, 06		
Transaction(s)	Authorization Objects	Fields	Values									
SU01—User Maintenance	S_USER_GRP	ACTVT	01, 02, 06									
	BAI06	<p>Changes to Central User Administration (CUA) are authorized and reviewed regularly by management.</p> <p>6.7.1 Because all enterprises are structured differently and have different requirements, conduct an initial discussion with the enterprise to obtain an understanding of its structure and the configuration requirements for the CUA. To test whether the CUA has been configured appropriately, execute the transaction codes SALE—Display ALE Customizing, SCUA—Central User Administration and SCUM—Central User Administration and review the appropriateness of the configured settings for the enterprise. Also, if the CUA is configured to run in a separate client outside of production, then it should be determined who has administrator access through the CUA master client.</p>										
B-3.6f	<p>Agree on the process work products²¹ (inputs and outputs as defined in the process practices description) that are expected to be present (process design).</p> <p>Assess to what extent the process work products are available.</p>											
	<p>Application security (SA) inputs and outputs. The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.</p> <table border="1"> <thead> <tr> <th>Process Practice</th> <th>Work Products</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Application security (SA)</td> <td> <ul style="list-style-type: none"> List of change security roles List of changed user role assignments List of deactivated users User entitlement review reports Segregation of Duties conflicts </td> <td>Apply appropriate audit techniques to determine the existence and appropriate use of each work product.</td> </tr> </tbody> </table>			Process Practice	Work Products	Assessment Step	Application security (SA)	<ul style="list-style-type: none"> List of change security roles List of changed user role assignments List of deactivated users User entitlement review reports Segregation of Duties conflicts 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.			
Process Practice	Work Products	Assessment Step										
Application security (SA)	<ul style="list-style-type: none"> List of change security roles List of changed user role assignments List of deactivated users User entitlement review reports Segregation of Duties conflicts 	Apply appropriate audit techniques to determine the existence and appropriate use of each work product.										

²¹ For COBIT 5 processes, a set of inputs and outputs for the different management practices are identified in COBIT 5: Enabling Processes.

Audit/Assurance Program for SAP ERP BASIS Administration and Security			
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes			
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment
B-3.7f	<p>Agree on the process capability level to be achieved by the process.</p> <p><i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i></p>		

Audit/Accurance Program for SAP ERP BASIS Administration and Security				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-4	Obtain understanding of each Organisational Structure in scope and set suitable assessment criteria: For each Organisational Structure in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined. Assess the Organisational Structure .			
Organisational Structure: Basis team				
B-4.1a	<u>Understand the Organisational Structure context.</u> <i>Identify and document all elements that can help to understand the context in which the Financial accounting organization has to operate, including:</i> <ul style="list-style-type: none"> • The overall organisation • Management/process framework • History of the role/structure • Contribution of the Organisational Structure to achievement of goals 			
B-4.2a	<u>Understand all stakeholders of the Organisational Structure/function.</u> <i>Determine through documentation review (policies, management communications, etc.) the key stakeholders of the Financial accounting organization.</i> <ul style="list-style-type: none"> • Incumbent of the role and/or members of the Organisational Structure • Other key stakeholders affected by the decisions of the Organisational Structure/role 			
B-4.3a	<u>Understand the goals of the Organisational Structure</u> , the related metrics and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals.			
Organisational Structure Goal		Assessment Step		
Determine through interviews with key stakeholders and documentation review the goals of the Basis team , i.e., the decisions for which they are accountable ^{22,23} .		This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> - They have contributed to the achievement of the IT-related and enterprise goals as anticipated. - Decisions are duly executed on a timely basis. 		
B-4.4a	<u>Agree on the expected good practices for the Organisational Structure</u> against which it will be assessed. <u>Assess the Organisational Structure design</u> , i.e., assess the extent to which expected good practices are applied.			
Good Practice		Criteria		Assessment Step
Operating principles		<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 		<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful.
Composition		The Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.		Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently represented.
Span of control		<ul style="list-style-type: none"> • The span of control of The Organisational Structure is 		<ul style="list-style-type: none"> • Verify whether the span of control of the Organisational Structure is defined.

²² The RACI charts in COBIT 5: *Enabling Processes* can be leveraged as a starting point for the expected goals of a role or Organisational Structure.

²³ The Organisational Structure/role as described may not exist under the same name in the enterprise; in that case, the closest Organisational Structure assuming the same responsibilities and accountability should be considered.

Audit/Accurance Program for SAP ERP BASIS Administration and Security							
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Organisational Structures							
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment		
		<p>defined.</p> <ul style="list-style-type: none"> The span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. The span of control is in line with the overall enterprise governance arrangements. 	<ul style="list-style-type: none"> Assess whether the span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. Verify and assess whether the span of control is in line with the overall enterprise governance arrangements. 				
	Level of authority/decision rights	<ul style="list-style-type: none"> Decision rights of the Organisational Structure are defined and documented. Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue). 	<ul style="list-style-type: none"> Verify that decision rights of the Organisational Structure are defined and documented. Verify whether decision rights of the Organisational Structure are complied with and respected. 				
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.				
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.				
B-4.5a	Understand the life cycle and agree on expected values. Assess the extent to which the Organisational Structure life cycle is managed.						
	Life-Cycle Element	Criteria	Assessment Step				
	Mandate	<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well understood mandate. 				
	Monitoring	<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 				
B-4.1 to B-4.5	Repeat steps B-4.1 through B-4.5 for all remaining Organisational structures in scope.						
	Repeat the steps described above for the remaining Organisational structures:						
	<ul style="list-style-type: none"> System administration Database administration IT operations 						

Audit/Accurance Program for SAP ERP BASIS Administration and Security				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment	
B-5	Obtain understanding of the Culture, Ethics and Behaviour in scope. Assess Culture, Ethics and Behaviour.			
Culture, Ethics and Behaviour: Risk and compliance aware culture				
B-5.1a	<u>Understand the Culture, Ethics and Behaviour context.</u> <ul style="list-style-type: none"> • <i>What the overall corporate Culture is like</i> • <i>Understand the interconnection with other enablers in scope:</i> <ul style="list-style-type: none"> - <i>Identify roles and structures that could be affected by the Culture.</i> - <i>Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.</i> 			
B-5.2a	<u>Understand the major stakeholders of the Culture, Ethics and Behaviour: Risk and compliance aware culture</u> <i>Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.</i>			
B-5.3a	<u>Understand the goals for the Culture, Ethics and Behaviour, and the related metrics</u> and agree on expected values. Assess whether the Culture, Ethics and Behaviour goals (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour. In the context of Risk and compliance aware culture , the following Culture, Ethics and Behaviour are desired:	Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. For a representative sample of individuals, perform the following assessment steps.		
Desired Behaviour (Culture, Ethics and Behaviour Goal)		Assessment Step		
The enterprise is aware of the compliance requirements it must abide		•		
Employees understand their role in maintaining compliance		•		
Identified risk are properly address		•		
Controls are in place to ensure compliance with internal and external requirements		•		
B-5.4a	<u>Understand the life cycle stages of the Culture, Ethics and Behaviour, and agree on the relevant criteria.</u> Assess to what extent the Culture, Ethics and Behaviour life cycle is managed. <i>(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)</i>			
B-5.5a	<u>Understand good practice when dealing with Culture, Ethics and Behaviour, and agree on relevant criteria.</u> Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied.			
Good Practice		Criteria	Assessment Step	
Communication, enforcement and rules		Existence and quality of the communication	Apply appropriate auditing techniques to assess whether the good practice is adequately applied, i.e., assessment criteria are met.	
Incentives and rewards		Existence and application of appropriate rewards and incentives		
Awareness		Awareness of desired Behaviours		
Repeat steps B-5.1 through B-5.5 for all remaining Culture, Ethics and Behaviour in scope.				
Repeat the steps described above for the remaining Culture, Ethics and Behaviour: <ul style="list-style-type: none"> • Enabling of continuous improvement • Accountability • Discipline to follow instructions 				
B-5.1 to B-5.5				

Audit/Accurance Program for SAP ERP BASIS Administration and Security																																																																		
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																																																																		
Ref.	Assurance Steps and Guidance			Issue Cross-reference																																																														
B-6	Obtain understanding of the Information Items in scope. Assess Information Items.																																																																	
Information Item: Data integrity procedures																																																																		
B-6.1a	<u>Understand the Information item context:</u> <ul style="list-style-type: none"> • Where and when is it used? • For what purpose is it used? • Understand the connection with other enablers in scope, e.g.: <ul style="list-style-type: none"> - Used by which processes? - Which Organisational Structures are involved? - Which services/applications are involved? 																																																																	
B-6.2a	<u>Understand the major stakeholders of the Information item.</u> Understand the stakeholders for the Information item, i.e., identify the: <ul style="list-style-type: none"> • Information producer • Information custodian • Information consumer <p>Stakeholders should be at the appropriate organisational level.</p>																																																																	
B-6.3a	<u>Understand the major quality criteria for the Information item, the related metrics and agree on expected values.</u> Assess whether the Information item quality criteria (outcomes) are achieved, i.e., assess the effectiveness of the Information item.		Leverage the COBIT 5 Information enabler model ²⁴ focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand. Mark the quality dimensions with a ‘✓’ that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.	The assurance professional will, by using appropriate auditing techniques, verify all quality criteria in scope and assess whether the criteria are met.																																																														
	<table border="1"> <thead> <tr> <th>Quality Dimension</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr><td>Accuracy</td><td>✓</td><td></td><td></td></tr> <tr><td>Objectivity</td><td></td><td></td><td></td></tr> <tr><td>Believability</td><td></td><td></td><td></td></tr> <tr><td>Reputation</td><td></td><td></td><td></td></tr> <tr><td>Relevancy</td><td>✓</td><td></td><td></td></tr> <tr><td>Completeness</td><td>✓</td><td></td><td></td></tr> <tr><td>Currency</td><td>✓</td><td></td><td></td></tr> <tr><td>Amount of information</td><td>✓</td><td></td><td></td></tr> <tr><td>Concise representation</td><td>✓</td><td></td><td></td></tr> <tr><td>Consistent representation</td><td></td><td></td><td></td></tr> <tr><td>Interpretability</td><td></td><td></td><td></td></tr> <tr><td>Understandability</td><td>✓</td><td></td><td></td></tr> <tr><td>Manipulation</td><td></td><td></td><td></td></tr> <tr><td>Availability</td><td>✓</td><td></td><td></td></tr> <tr><td>Restricted access</td><td>✓</td><td></td><td></td></tr> </tbody> </table>		Quality Dimension	Key Criteria	Description	Assessment Step	Accuracy	✓			Objectivity				Believability				Reputation				Relevancy	✓			Completeness	✓			Currency	✓			Amount of information	✓			Concise representation	✓			Consistent representation				Interpretability				Understandability	✓			Manipulation				Availability	✓			Restricted access	✓		
Quality Dimension	Key Criteria	Description	Assessment Step																																																															
Accuracy	✓																																																																	
Objectivity																																																																		
Believability																																																																		
Reputation																																																																		
Relevancy	✓																																																																	
Completeness	✓																																																																	
Currency	✓																																																																	
Amount of information	✓																																																																	
Concise representation	✓																																																																	
Consistent representation																																																																		
Interpretability																																																																		
Understandability	✓																																																																	
Manipulation																																																																		
Availability	✓																																																																	
Restricted access	✓																																																																	

²⁴ COBIT 5 framework, appendix G, p.81-84

Audit/Accurance Program for SAP ERP BASIS Administration and Security																															
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																															
Ref.	Assurance Step and Guidance			Issue Cross-reference																											
B-6.4a	<p>Understand the life cycle stages of the Information item, and agree on the relevant criteria. <u>Assess</u> to what extent the Information item life cycle is managed.</p> <p>The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.</p> <ul style="list-style-type: none"> When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently. When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. <p>Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Life Cycle Stage</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr><td>Plan</td><td>✓</td><td></td><td></td></tr> <tr><td>Design</td><td>✓</td><td></td><td></td></tr> <tr><td>Build/acquire</td><td>✓</td><td></td><td></td></tr> <tr><td>Use/operate</td><td>✓</td><td></td><td></td></tr> <tr><td>Evaluate/monitor</td><td>✓</td><td></td><td></td></tr> <tr><td>Update/dispose</td><td>✓</td><td></td><td></td></tr> </tbody> </table>	Life Cycle Stage	Key Criteria	Description	Assessment Step	Plan	✓			Design	✓			Build/acquire	✓			Use/operate	✓			Evaluate/monitor	✓			Update/dispose	✓				
Life Cycle Stage	Key Criteria	Description	Assessment Step																												
Plan	✓																														
Design	✓																														
Build/acquire	✓																														
Use/operate	✓																														
Evaluate/monitor	✓																														
Update/dispose	✓																														
B-6.5a	<p>Understand important attributes of the Information item and expected values. <u>Assess</u> the Information item design, i.e., assess the extent to which expected good practices are applied.</p> <p>Good practices for Information items are defined as a series of attributes for the Information item²⁵. The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.</p> <p>Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Attribute</th><th>Key Criteria</th><th>Description</th><th>Assessment Step</th></tr> </thead> <tbody> <tr><td>Physical</td><td></td><td></td><td></td></tr> <tr><td>Empirical</td><td></td><td></td><td></td></tr> <tr><td>Syntactic</td><td></td><td></td><td></td></tr> <tr><td>Semantic</td><td></td><td></td><td></td></tr> <tr><td>Pragmatic</td><td>✓</td><td></td><td></td></tr> <tr><td>Social</td><td></td><td></td><td></td></tr> </tbody> </table>	Attribute	Key Criteria	Description	Assessment Step	Physical				Empirical				Syntactic				Semantic				Pragmatic	✓			Social					
Attribute	Key Criteria	Description	Assessment Step																												
Physical																															
Empirical																															
Syntactic																															
Semantic																															
Pragmatic	✓																														
Social																															
B-6.1 to B-6.5	<p>Repeat steps B-6.1 through B-6.5 for all remaining Information items in scope.</p> <p>Repeat the steps described above for the remaining Information items:</p> <ul style="list-style-type: none"> Data classification guidelines Data security and control guidelines Assigned responsibilities for resource management Access logs Allocated roles and responsibilities Allocated levels of authority Allocated access rights Evidence or error correction and remediation Error reports and root cause analysis Retention requirements Record of transactions Training manuals Job aids 																														

²⁵ COBIT 5 framework, appendix G, p. 81-84

Audit/Accurance Program for SAP ERP BASIS Administration and Security																								
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment																								
Ref.	Assurance Steps and Guidance			Issue Cross-reference																				
B-7	Obtain understanding of the Services, Infrastructure and Applications in scope. Assess Services, Infrastructure and Applications.																							
Services, Infrastructure and Applications: Master data maintenance group																								
B-7.1a	<u>Understand the Services, Infrastructure and Applications</u> context. <i>Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.</i>																							
B-7.2a	<u>Understand the major stakeholders</u> of the Services, Infrastructure and Applications . <i>Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.</i>																							
B-7.3a	<u>Understand the major goals</u> for the Services, Infrastructure and Applications , the related metrics and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.																							
<table border="1"> <thead> <tr> <th>Goal</th><th>Criteria</th><th>Assessment Step</th><th></th><th></th></tr> </thead> <tbody> <tr> <td>Service description</td><td> <ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders </td><td> <ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. </td><td></td><td></td></tr> <tr> <td>Service level definition</td><td>Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness </td><td> <ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. </td><td></td><td></td></tr> <tr> <td>Contribution to related enablers, IT and enterprise goals</td><td>The Service contributes to the achievement of related enabler and IT-related and enterprise goals.</td><td>Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.</td><td></td><td></td></tr> </tbody> </table>					Goal	Criteria	Assessment Step			Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 			Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 			Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.		
Goal	Criteria	Assessment Step																						
Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 																						
Service level definition	Service levels are defined for : <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 																						
Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.																						
B-7.4a	<u>Understand good practice</u> related to the Services, Infrastructure and Applications and expected values. Assess the Services, Infrastructure and Applications design, i.e., assess to what extent expected good practices are applied. Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework ²⁶ to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented: <ul style="list-style-type: none"> Buy/build decision needs to be taken. Use of the Service needs to be clear. 																							
<table border="1"> <thead> <tr> <th>Good Practice</th><th>Criteria</th><th>Assessment Step</th><th></th><th></th></tr> </thead> <tbody> <tr> <td>Sourcing (buy/build)</td><td>A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.</td><td> <ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. </td><td></td><td></td></tr> <tr> <td>Use</td><td>The use of the Service needs to be clear: <ul style="list-style-type: none"> When it needs to be used </td><td> <ul style="list-style-type: none"> Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used. Verify that actual use is in line with requirement above. </td><td></td><td></td></tr> </tbody> </table>					Good Practice	Criteria	Assessment Step			Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. 			Use	The use of the Service needs to be clear: <ul style="list-style-type: none"> When it needs to be used 	<ul style="list-style-type: none"> Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used. Verify that actual use is in line with requirement above. 							
Good Practice	Criteria	Assessment Step																						
Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. Verify that the sourcing decision has been duly executed. 																						
Use	The use of the Service needs to be clear: <ul style="list-style-type: none"> When it needs to be used 	<ul style="list-style-type: none"> Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used. Verify that actual use is in line with requirement above. 																						

²⁶ COBIT 5 framework, appendix G, p.85-86

Audit/Assurance Program for SAP ERP BASIS Administration and Security				
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment				
Ref.	Assurance Step and Guidance			Issue Cross-reference
		and by whom	• Verify that the actual Service output is adequately used. • Verify that Service levels are monitored and achieved.	
B-7.1 to B-7.4	Repeat steps B-7.1 through B-7.4 for all remaining Services, Infrastructure and Applications in scope.	• The required compliance levels with the Service's output		
	Repeat the steps described above for the remaining Services, Infrastructure and Applications:	<ul style="list-style-type: none"> • SAP ERP support and maintenance • SAP training • Tax department • Accounting department 		

Audit/Accurance Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
People, Skills and Competencies					
Ref.	Assurance Steps and Guidance		Issue Cross-reference		
B-8	Obtain understanding of the People, Skills and Competencies in scope. Assess People, Skills and Competencies.		Comment		
People, Skill and Competency: Proficiency using the SAP Basis Module					
B-8.1a	<u>Understand the People, Skills and Competencies</u> context. <i>Understand the context of the Skill/Competency, i.e.:</i> <ul style="list-style-type: none"> • Where and when is it used? • For what purpose is it used? • Understand the connection with other enablers in scope, e.g.: <ul style="list-style-type: none"> - In which roles and structures is the Skill/Competency used? (See also B-4.1.) <i>Which behaviours are associated with the Skill/Competency?</i>				
B-8.2a	<u>Understand</u> the major stakeholders for the People, Skills and Competencies. <i>Identify to whom in the organisation the skill requirement applies.</i>				
B-8.3a	<u>Understand</u> the major goals for the People, Skills and Competencies , the related metrics and <u>agree</u> on expected values. <i>Assess whether the People, Skills and Competencies goals (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.</i>				
	For the People, Skills and Competencies: Proficiency using the SAP Basis Module , the following goals and associated criteria can be addressed.				
	Goal	Criteria	Assessment Step		
	Experience		Apply appropriate auditing techniques to assess whether the People, Skills and Competencies goals are adequately achieved, i.e., that assessment criteria are met.		
	Education				
	Qualification				
	Knowledge				
	Technical skills				
	Behavioural skills				
	Number of people with appropriate skill level				
B-8.4a	<u>Understand</u> the life cycle stages of the People, Skills and Competencies , and agree the relevant criteria. <i>Assess to what extent the People, Skills and Competencies life cycle is managed.</i>				
	For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07.		For the People, Skills and Competencies at hand the assurance professional will perform the following assessment steps.		
	Life Cycle Element	Criteria	Assessment Step		
	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.		
	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill. Practice APO07.03 activity 3 (Provide access to knowledge repositories to support the development of skills and competencies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill. Assess whether practice APO07.03 activity 3 is implemented in relation to this skill.		
	Build	Practice APO07.03 activity 4 (Identify gaps between	Assess whether practice APO07.03 activity 4 is implemented in		

Audit/Accuracy Program for SAP ERP BASIS Administration and Security					
Phase B—Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment					
People, Skills and Competencies					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
		required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	relation to this skill.		
	Operate	Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.		
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.		
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.		
B-8.5a	Understand good practice related to the People, Skills and Competencies and expected values. Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.				
	Good Practice	Criteria	Assessment Step		
	Skill set and Competencies are defined.	<ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 			
	Skill levels are defined.	<ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. Assess the process for 360-degree performance evaluations. 			
B-8.1 to B-8.5	Repeat steps B-8.1 through B-8.5 for all remaining People, Skills and Competencies in scope. Repeat the steps described above for the remaining People, Skills and Competencies: <ul style="list-style-type: none"> Database management skills SAP Security skills and experience Proficiency running SAP reports Understanding of data classification policies Understanding of data integrity procedures 				

Audit/Accurance Program for SAP ERP BASIS Administration and Security		
Phase C—Communicate the Results of the Assessment		
Ref.	Assurance Step	Guidance
C-1	Document exceptions and gaps.	
C-1.1	Understand and document weaknesses and their impact on the achievement of process goals.	<ul style="list-style-type: none"> Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	<ul style="list-style-type: none"> Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. Point out the consequence of noncompliance with regulatory requirements and contractual agreements. Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
C-2	Communicate the work performed and findings.	
C-2.1	Communicate the work performed.	<ul style="list-style-type: none"> Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	<ul style="list-style-type: none"> Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. Use benchmarking and survey results to compare the enterprise's performance with others. Use extensive graphics to illustrate the issues. Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	

Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
1. Application Configuration (Implementation Management Guide [IMG])							
1.1 Configuration changes are made in the development environment and transported to production.							
1.1.1 Has access to the Implementation Management Guide (IMG) in production been restricted?					BAI10 DSS05 DSS06		
Have the production client settings been established to not allow changes to programs and configuration?							
1.1.2 Has access to the enterprise configuration functionality been restricted?					BAI10 DSS05 DSS06		
1.1.3 Has access to the production client been reviewed and validated to restrict access to authorized personnel?					DSS05 DSS06		
2. Application Configuration (Organizational Management Model [OMM])							
2.1 The organizational structure is accurate.							
2.1.1 Was the Organizational Management Model (OMM) well thought out and agreed on early in the implementation, and did the relevant organizational groups assist with key design decisions?					APO01 DSS06		
2.2 Changes to critical number ranges are controlled.							
2.2.1 Has the SAP ERP software security been appropriately configured to restrict the ability to change critical number ranges (i.e., company codes, chart of accounts and accounting period data)?					DSS05 DSS06		
2.3 Relevant company codes are set to Productive in the production environment.							

BASIS Administration and Security ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
2.3.1 Have company codes that are working productively been set to Productive to reduce the risk that deletion programs may reset the company code data by mistake?					APO01 BAI06
3. Application Development (ABAP/4 Workbench)					
3.1 Changes to critical SAP ERP tables are authorized and logged by the system for management monitoring.					
3.1.1 Have all of the customized SAP ERP tables been assigned to the appropriate authorization group?					APO01 DSS05
Has the ability to modify critical tables been appropriately restricted in the production system?					
3.2 Changes made to the data dictionary are authorized and reviewed regularly.					
3.2.1 Are details of modifications to the data dictionary maintained and change control procedures followed?					BAI06 DSS05 DSS06
Has the ability to make changes to the SAP ERP data dictionary been restricted to authorized individuals?					
Have the system parameters been set to allow “No Check” indicators?					
3.3 Access to modify and develop queries is restricted.					
3.3.1 Have authorization groups for creating and running the ABAP/4 queries been appropriately established in the SAP ERP software so that some end users can maintain and execute queries, while others can only execute existing queries?					APO01 DSS05

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.4 The creation or modification of programs is performed in the development system and migrated through the test system to production.					
3.4.1 Has access to directly change production source code within the production environment been restricted?					DSS01 DSS05 DSS06
3.5 Only authorized customized transactions are available for use in the production environment.					
3.5.1 Have the production client settings been established to not allow changes to programs and configuration? Has an authority-check statement been included within customized ABAP/4 programs so the user's authority to access objects is checked at run time?					BAI10 DSS05
3.6 Customized ABAP/4 programs are assigned to authorization groups.					
3.6.1 Have customized ABAP/4 programs been assigned to authorization groups?					APO01 DSS05
3.7 Changes to critical SAP ERP tables are logged by the system and are periodically reviewed.					
3.7.1 Has access to directly change critical SAP ERP tables in production been restricted and monitoring established?					BAI07 DSS05
3.8 Data Dictionary Information System reports are generated and reviewed by management.					
3.8.1 Are SAP ERP Data Dictionary Information System reports (DD reports) regularly generated and reviewed by management?					DSS01 MEA01
3.9 Log and trace files are appropriately configured and secured.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
3.9.1 Is logging appropriately configured, and are log and trace files secured at the operating system level at the location specified within the system profile?					BAI10 DSS06
4. Transport Management System (TMS)					
4.1 Application modifications are planned, tested and implemented following a phased approach.					
4.1.1 Are appropriate change controls procedures followed for all transports? Has the production system change option been set to No Changes Allowed? Has the ability to create and release change requests been segregated?					APO01 BAI06 DSS05 DSS06
5. Application Operations (Computing Center Management System)					
5.1 The Computing Center Management System (CCMS) is configured appropriately.					
5.1.1 Have operation modes, instances and the CCMS timetable been correctly defined, such that the CCMS display is meaningful? Is access to the system and start-up profiles tightly controlled? Are change procedures followed strictly and changes to the profiles well documented?					APO01 BAI03 DSS01 DSS05 DSS06
5.2 Batch processing operations are secured appropriately.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
5.2.1 Have batch input, batch administration and batch processing capabilities been restricted appropriately? Have batch upload programs created to load initial master data and take on balances been deleted from the production environment following go-live?					BAI07 DSS01 DSS05
5.3 Default system parameter settings are reviewed and configured to suit the enterprise's environment. Access to lock sensitive transaction codes has been restricted and sensitive transaction codes have been locked.					
5.3.1 During implementation, did the enterprise set the SAP ERP system profile parameters to appropriate values? Has access to locking and unlocking sensitive transactions codes been restricted?					BAI07 DSS01
5.4 Sensitive transaction codes are locked in production.					
5.4.1 Have sensitive transaction codes been locked in the production environment, and does the enterprise have procedures for locking and unlocking these transaction codes?					DSS05
5.5 Users are prevented from logging on with trivial or easily guessable passwords.					
5.5.1 Has management set up a list of "illegal" passwords that users are not allowed to use?					BAI06 DSS05
5.6 The SAP Router is configured to act as a gateway to secure communications into and out of the SAP ERP environment.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
<p>5.6.1 Is the network protected by the SAP Router and a firewall?</p> <p>Are appropriate change management procedures for any modifications to the SAP Router permission table in place and operating?</p> <p>Is the SAP Router log file used to monitor remote communications activity?</p>					BAI06 DSS01 DSS05 DSS03
5.7 Remote access by software vendors is controlled adequately.					
<p>5.7.1 Is SAP's or the support provider's access restricted to a test/development environment, ideally on a separate file server from the production environment, activated only on request, and all activity logged and reviewed by an individual with the ability to understand the actions that have been taken?</p> <p>Are changes subject to normal testing and migration controls before being implemented on the production system?</p>					BAI06
5.8 The technology infrastructure is configured to secure communications and operations in the SAP ERP environment.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
5.8.1 Has the technology infrastructure been configured to secure communications and operations in the SAP ERP environment? Consider the following areas: <ul style="list-style-type: none">• Firewall• Secure Network Communications (SNC)• Secure Store and Forward (SSF) mechanisms and digital signatures• Workstation security• Operating system and database security					BAI06 BAI10 DSS01 DSS04 DSS05 DSS06 MEA02 MEA03
5.9 SAP ERP Remote Function Call (RFC) and Common Programming Interface— Communications (CPI-C) are secured.					
5.9.1 Have the SAP ERP RFC and CPI-C communications been secured so that any user who makes use of a connection will be prompted to enter a username and password?					DSS05
6. Application Security (SA)					
6.1 Duties within the security administration environment are adequately segregated.					
6.1.1 Has the enterprise allocated the security administration function among different individuals? Has access to make mass changes to user records been appropriately restricted?					APO01 DSS05 DSS06
6.2 Adequate security authorization documentation is maintained.					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
6.2.1 Was original documentation of the SAP ERP authorizations and their use developed and signed off by management during the implementation, and has it been maintained adequately?					BAI07 DSS04
6.3 The superuser SAP* is properly secured.					
6.3.1 Has the SAP* been assigned to the security administrators authorization group to prevent inadvertent deletion, the password changed from the default, all profiles and authorizations deleted, and the user locked?					DSS05
Has the system parameter (login/no_automatic_user_sapstar) been set?					
6.4 Default users are secured properly.					
6.4.1 Have the passwords for the default users DDIC, SAPCPIC, and EarlyWatch been changed from the default?					DSS05
6.5 Access to powerful profiles is restricted.					
6.5.1 Has a new superuser account with the SAP_ALL and SAP_NEW profiles been created with a confidential ID and secret password for emergency use, and has access to powerful profiles been restricted appropriately?					APO01 DSS05 DSS06
Are procedures in place to ensure that use of the SAP_ALL authority is authorized, approved, logged, monitored and reviewed?					

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
6.6 The authorization group that contains powerful users is restricted.					
6.6.1 Has the authorization group that contains powerful users been restricted to the new superuser and a backup?					APO01 DSS05
6.7 Changes to Central User Administration (CUA) are authorized and reviewed regularly by management.					
6.7.1 Are all changes made via the CUA appropriately authorized?					BAI06

SAP ERP

Control Environment ICQ



ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

ISACA has designed and created *SAP ERP Control Environment ICQ* (the 'Work') primarily as an educational resource for assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, assurance professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

While all care has been taken in researching and documenting the techniques described in this text, persons employing these techniques must use their own knowledge and judgment. ISACA and Deloitte, its partners and employees, shall not be liable for any losses and/or damages (whether direct or indirect), costs, expenses or claims whatsoever arising out of the use of the techniques described or reliance on the information in this reference guide.

SAP, SAP R/3, mySAP, SAP R/3 Enterprise, SAP Strategic Enterprise Management (SAP SEM), SAP NetWeaver, ABAP, mySAP Business Suite, mySAP Customer Relationship Management, mySAP Supply Chain Management, mySAP Product Lifecycle Management, mySAP Supplier Relationship Management and other SAP product/services referenced herein are the trademarks or registered trademarks of SAP SE in Germany and in several other countries. The publisher gratefully acknowledges SAP's kind permission to use these trademarks and reproduce selected diagrams and screen shots in this publication. SAP SE is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

© 2015 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: info@isaca.org
Web site: www.isaca.org

Provide feedback: <http://www.isaca.org/sap-erp-4th-edition>

Participate in the ISACA Knowledge Center: www.isaca.org/knowledge-center

Follow ISACA on Twitter: <https://twitter.com/ISACANews>

Join ISACA on LinkedIn: ISACA (Official), <http://linkd.in/ISACAOFFICIAL>

Like ISACA on Facebook: www.facebook.com/ISACAHQ

Acknowledgements

ISACA wishes to recognize

Project Leaders

Benjamin Fitts, CPA, Deloitte & Touche LLP, USA
Jacob Gregg, CISA, CISSP, Deloitte & Touche LLP, USA
Michael Juergens, CISA, CGEIT, CRISC, CGAP, CIA, CRMA, Deloitte & Touche LLP, USA
Michael Kosonog, CISA, CISSP, CITP, CPS, Deloitte & Touche LLP, USA
Nancy A. Cohen, CPA, CIPP/US, ISACA, USA
Eva Sweet, CISA, CISM, ISACA, USA

Researchers

Syed Aamir Aarfi, Deloitte & Touche LLP, USA
Carlos Amaya, CISA, Deloitte & Touche LLP, USA
Dan Argynov, PMP, Deloitte & Touche LLP, USA
Soumya Bikash Sen, CCSK, CISSP, Deloitte & Touche LLP, USA
David Bogatyrev, CISSP, CPA, Deloitte & Touche LLP, USA
Ramamallikarjunarao Chintakunta, CISSP, PMP, Deloitte & Touche LLP, USA
Kranthi Kumar Mitra Gangavarapu, CISSP, Deloitte & Touche LLP, USA
Venkat Praveen Juntipally, SAP FI, Deloitte & Touche LLP, USA
Sagnik Mukherjee, Deloitte & Touche LLP, USA
Sudhakar Sathiyamurthy, CISA CGEIT, CIPP, ITIL, Deloitte & Touche LLP, USA
Sonik Shah, Deloitte & Touche LLP, USA
Dennis Siau, CISA, CIA, CISSP, CPA, Deloitte & Touche LLP, USA
Shweta Srivastava, Deloitte & Touche LLP, USA
Anurag Tewary, Deloitte & Touche LLP, USA
Percy Tsai, CPA, Deloitte & Touche LLP, USA
Ravi Maddela Veeriah, Deloitte & Touche LLP, USA
Sravan Vemana, Deloitte & Touche LLP, USA
Anukool Vyas, Deloitte & Touche LLP, USA

Expert Reviewers

Steve Biskie, CISA, CGMA, CITP, CPA, High Water Advisors, USA
Adrienne C. Chung, CISA, CISM, CRISC, CA, CPA, Chung Consulting & Advisory Ltd., Canada
Mayank Garg, CISA, NetApp, USA
Ricci leong, Ph.D, CISA, CCSK, CEH, CISSP, eWalker Consulting (HK) Ltd., Hong Kong
Guhapriya Iyer, CISA, ACA, Grad.CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Francis Kaitano, CISA, CISM, CISSP, ITIL, MCSD, SCF, New Zealand
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Jim Koveos, CISA, MBA, AmerisourceBergen, USA
Rajni Lalsinghani, CISA, CISM, Department of Human Services, Australia
Samuel LIM S.C., CISA, Auditor General's Office, Singapore
Alfonso Luque Romero, CISA, CISM, Banco de la Republica, Colombia
Lu Miao Chang, CISA, FCA, MCSE, SAP T/C, Auditor General's Office, Singapore
Stane Moskon, CISA, CISM, OSIR d.o.o., Slovenia
Moonga Mumba, CISA, BBA, MSc Computer Forensics, SAP Cert., Zambia Revenue Authority, Zambia
Paul O'Donnell, Ernst & Young, Canada
Fernando Ortiz Guerrero, LIA, Ernst & Young, Mexico
John Ott, CISA, CISSP, CFE, CPA, LPT, AmerisourceBergen, US
Maria del Pilar Pliego Bermudez, CISA, CGEIT, CRISC, CPA, Ernst & Young, Mexico
Naved Rehman, CISA, CRISC, MS-IS, SAPauditCoach, US
Andriy Rybalchenko, CISA, CISM, LLC EastOne, Ukraine
Lily Shue, CISA, CISM, CGEIT, CRISC, LMS Associates, LLC, US
Sergio Raul Solis Garza, CISA, CGEIT, CRISC, ISO 27001 LA, Mexico
Jovari St. Victor, CISA, CPA, Sunera, LLC, US
Surapong Surabotsopon, CISA, CISM, CGEIT, CLS, ITIL, MCSE, mySAP (FICO), PMP,

KasikornBank, PCL, Thailand

Blanca Eva Villarreal Munoz, PMP, Ernst & Young, Mexico

Chakri Wicharn, CISA, CISM, CGEIT, CSPM, ITIL, PMP, Fuji Xerox Co., Ltd., Thailand

David Yeung, CISA, CFE, CIA, Management Consultant, Singapore

ISACA Board of Directors

Robert E Stroud, CGEIT, CRISC, CA, USA, International President

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Vice President

Garry J. Barnes, CISA, CISM, CGEIT, CRISC, Vital Interacts, Australia, Vice President

Robert A. Clyde, CISM, Clyde Computing LLC, USA, Vice President

Ramses Gallego, CISM, CGEIT, CCSK, CISSP, SCPM, Six Sigma Black Belt, Dell, Spain, Vice President

Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA, US House of Representatives, USA, Vice President

Vittal R. Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA, Kumar & Raj, India, Vice President

Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past International President

Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Past International President

Debbie A. Lew, CISA, CRISC, Ernst & Young LLP, USA, Director

Frank K.M. Yam, CISA, CIA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Director

Alexander Zapata Lenis, CISA, CGEIT, CRISC, ITIL, PMP, Grupo Cynthus S.A. de C.V., Mexico, Director

Knowledge Board

Steven A. Babb, CGEIT, CRISC, ITIL, Vodafone, UK, Chairman

Rosemary M. Amato, CISA, CMA, CPA, Deloitte Touche Tohmatsu Ltd., The Netherlands

Neil Patrick Barlow, CISA, CISM, CRISC, CISSP, Capital One, UK

Charlie Blanchard, CISA, CISM, CRISC, CIPP/US, CIPP/E, CISSP, FBCS, ACA, Amgen Inc., USA

Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore

Phil J. Lageschulte, CGEIT, CPA, KPMG LLP, USA

Anthony P. Noble, CISA, Viacom, USA

Jamie Pasfield, CGEIT, ITIL V3, MSP, PRINCE2, Pfizer, UK

Ivan Sanchez Lopez, CISA, CISM, ISO 27001 LA, CISSP, DHL Global Forwarding & Freight, Germany

Guidance and Practices Committee

Philip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA, Chairman

John Jasinski, CISA, CGEIT, ISO20K, ITIL Expert, SSBB, ITSMBP, USA

Yves Marcel Le Roux, CISM, CISSP, CA Technologies, France

Aureo Monteiro Tavares Da Silva, CISM, CGEIT, Brazil

Jotham Nyamari, CISA, Deloitte, USA

James Seaman, CISM, CRISC, A.Inst.IISP, CCP, QSA, RandomStorm Ltd, UK

Gurvinder Singh, CISA, CISM, CRISC, Australia

Siang Jun Julia Yeo, CISA, CRISC, CPA (Australia), MasterCard Asia/Pacific Pte. Ltd., Singapore

Nikolaos Zacharopoulos, CISA, CISSP, MerckGroup, Germany

SAP ERP Control Environment ICQ

SAP ERP Control Environment ICQ							
Control Objectives/Questions	Response			Comments	COBIT 5 References		
	Yes	No	N/A				
SAP ERP Control Environment (IT General Controls)							
1. Establish control over information and information systems.							
1.1 Has senior management established policies and standards governing the information systems of the entity?					APO01		
1.2 Has senior management assigned responsibilities for information, its processing and its use?					APO01		
1.3 Is user management responsible for providing information that supports the entity's objectives and policies?					APO01		
1.4 Is user management responsible for the completeness, accuracy, authorization, security and timeliness of information?					APO11 DSS01		
1.5 Is information systems management responsible for providing the information systems capabilities necessary for achievement of the defined information systems objectives and policies of the entity?					APO02 APO09 BAI04		
1.6 Does senior management approve plans for the development and acquisition of information systems?					APO06 BAI02 BAI06		
1.7 Does senior management monitor the extent to which development/ configuration, operation and control of information systems comply with established policies and plans?					MEA01		

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
1.8 Are there outstanding audit findings from previous years?					MEA01 MEA02
2. Ensure that the information systems selected (whether new implementation or upgrade) meet the needs of the entity.					
2.1 Are there procedures to ensure that decisions to develop or acquire information systems are made in accordance with the objectives and policies of the entity?					APO06 BAI02 BAI06
2.2 Are there procedures to determine costs, savings and benefits before a decision is made to develop or acquire an information system?					APO06 BAI02 BAI06
2.3 Are there procedures to ensure that information systems, programs and configuration changes are adequately tested prior to implementation?					BAI03
3. Ensure that the acquisition and configuration of information systems (whether new implementation or upgrade) are carried out in an efficient and effective manner.					
3.1 Are standards established and enforced to ensure the efficiency and effectiveness of the systems acquisition and configuration process?					BAI01 BAI02 BAI03
3.2 Are there procedures to ensure that all systems are acquired and configured in accordance with the established standards?					BAI03
3.3 Is an approved acquisition plan (project plan) used to measure progress?					BAI01
3.4 Do all personnel involved in system acquisition and configuration activities receive adequate training and supervision?					APO07

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
4. Ensure the efficient and effective implementation or upgrade of information systems.					
4.1 Has responsibility been assigned for implementation, configuration and upgrade of information systems?					APO01
4.2 Are there procedures to ensure the efficiency and effectiveness of the implementation, configuration and upgrade of information systems?					BAI05
4.3 Are there procedures to ensure that information systems are implemented, configured and upgraded in accordance with the established standards?					BAI03
4.4 Is an approved implementation plan used to measure progress?					BAI01
4.5 Is effective control maintained over the conversion of information and the initial operation of the information system?					BAI07
4.6 Does user management participate in the conversion of data from the existing system to the new system?					BAI07
4.7 Is final approval obtained from user management prior to going live with a new implementation and/or upgraded system?					BAI07
5. Ensure the efficient and effective maintenance of information systems.					
5.1 Are there procedures to document and schedule all planned changes to information systems (including key ABAP programs)?					BAI06

SAP ERP Control Environment ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
5.2 Are there procedures to ensure that only authorized changes are initiated?					BAI06
5.3 Are there procedures to ensure and verify that only authorized, tested and documented changes to information systems are accepted into the production client?					BAI06 BAI07
5.4 Are there procedures to report planned information system changes to information systems management and to the users affected?					BAI06 DSS02
5.5 Are there procedures to allow for and control emergency changes?					BAI06
5.6 Are controls in place to prevent and identify unauthorized changes to information systems (including key ABAP programs)?					DSS05
6. Ensure that present and future requirements of users of information systems processing can be met.					
6.1 Are there written agreements between users and information systems processing that define the nature and level of services to be provided?					APO09
6.2 Is there appropriate management reporting within information systems processing?					MEA01
6.3 Does information systems processing management keep senior and user management informed about technical developments that could support the achievement of the objectives and policies of the entity?					BAI03 BAI04

SAP ERP Control Environment ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
6.4 Are there procedures/capacity planning activities to examine the adequacy of information processing resources to meet entity objectives in the future?					BAI04
6.5 Are there periodic planning activities to examine the adequacy of the volume of skilled staff (i.e., operating system, hardware, network and SAP ERP) to support the systems now and in the future?					APO07
6.6 Are there procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software?					BAI03 BAI04
6.7 Is there a process for monitoring the volume of named and concurrent SAP ERP users to ensure that the license agreement is not being violated?					BAI04 MEA03
6.8 If the SAP ERP implementation is not at the most current version, is there a planned upgrade approach?					APO01 BAI03 BAI04
7. Ensure the efficient and effective use of resources within information systems processing.					
7.1 Are budgets for information systems processing activities prepared on a regular basis?					APO06
7.2 Are standards established and enforced to ensure efficient and effective use of information systems processing?					APO01

SAP ERP Control Environment ICQ					
Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
7.3 Is there an incident management process that ensures that information processing problems are detected and corrected on a timely basis?					DSS02 DSS03
7.4 Are users of information systems processing facilities accountable for the resources used by them?					BAI09
8. Ensure that there is an appropriate segregation of incompatible functions within the entity.					
8.1 Does the organizational structure established by senior management provide for an appropriate segregation of incompatible functions? a. Basis administration b. Transport/import c. Developing program change d. Developing role change e. User security administration f. Change monitoring g. User testing h. Authorize change i. Perform change					APO01
9. Ensure that all access to information and information systems is authorized.					
9.1 Are there procedures to ensure and verify that information and information systems are accessed in accordance with established policies and procedures?					APO01
10. Ensure that information systems processing is protected physically from unauthorized access and from accidental or deliberate loss or damage.					
10.1 Are the database, application and presentation servers located in a physically separate and protected environment (i.e., a data center)?					DSS05

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
10.2 Are there procedures to ensure that environmental conditions (such as temperature and humidity) for hardware facilities are adequately controlled?					DSS01
11. Ensure that information processing can be recovered and resumed after operations have been interrupted.					
11.1 Are there procedures to allow information processing to resume operations in the event of an interruption?					DSS04
11.2 Are emergency, backup and recovery plans documented and tested on a regular basis to ensure that they remain current and operational?					DSS04
11.3 Do personnel receive adequate training and supervision in emergency backup and recovery procedures?					DSS04 APO07
12. Ensure that critical user activities can be maintained and recovered following interruption.					
12.1 Are there backup and recovery plans to allow users of information systems to resume operations in the event of an interruption?					DSS04
12.2 Are all information and resources required by users to resume processing backed up regularly?					DSS04
12.3 Do user personnel receive adequate training and supervision in the conduct of the recovery procedures?					DSS04 APO07

Control Objectives/Questions	Response			Comments	COBIT 5 References
	Yes	No	N/A		
12.4 Are application controls designed with regard for any weaknesses in segregation, security, development and processing controls that may affect the information system?					DSS04 DSS05
12.5 Are there procedures to ensure that output is reviewed by users/management for completeness, accuracy and consistency?					DSS04 MEA01
12.6 Is there some method of ensuring that control procedures relating to completeness, accuracy and authorization are ensured?					DSS04 MEA02
12.7 Are there established policies and procedures for record retention?					APO01 DSS04

Assurance Engagement:

Assurance Topic

Business Impact and Risk

Goal of the Review

Scoping

TEMPLATE

Audit/Accurance Program					
Phase A. Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance		Issue Cross-reference	Comment
A-1	Determine the stakeholders of the assurance initiative and their stakes .				
A-1.1	Identify the intended user(s) of the assurance report and their stake in the assurance engagement. This is the assurance objective.	Intended user(s) of the assurance report	Describe the users of the assurance report and their stakes.		
A-1.2	Identify the interested parties, accountable and responsible for the subject matter over which assurance needs to be provided.	Accountable and responsible parties for the subject matter	Describe the accountable and responsible parties for the subject matter over which assurance is to be provided. COBIT 5 includes a summary description of a comprehensive set of roles that can be used as starting point for this audit step (COBIT 5 framework, appendix G, p. 76). COBIT 5 for Assurance also provides a summary description of a comprehensive set of assurance roles in section 2A, chapter 4.		
A-2	Determine the assurance objectives based on assessment of the internal and external environment/context and of the relevant risk and related opportunities (i.e., not achieving the enterprise goals).	<p>Assurance objectives are essentially a more detailed and tangible expression of those enterprise objectives relevant to the subject of the assurance engagement.</p> <p>Enterprise objectives can be formulated in terms of the generic enterprise goals (COBIT 5 framework) or they can be expressed more specifically.</p> <p>Objectives of the assurance engagement can be expressed using the COBIT 5 enterprise goals, the IT-related goals (which relate more to technology), information goals or any other set of specific goals.</p> <p>Objectives of the assurance engagement will consider all three value objective components, i.e., delivering benefits that support strategic objectives, optimizing the risk that strategic objectives are not achieved and optimizing resource levels required to achieve the strategic objectives.</p>			
A-2.1	Understand the enterprise strategy and priorities.	Inquire with executive management or through available documentation (corporate strategy, annual report, etc.) about the enterprise strategy and priorities for the coming period, and document them.			
A-2.2	Understand the internal context of the enterprise.	<p>Identify all internal environmental factors that could influence the performance and contents of the topic of the audit/assurance programme. In addition to the enterprise strategy (discussed in A-2.1), these factors could include:</p> <ul style="list-style-type: none"> • Role of IT in the enterprise—Is IT a strategic differentiator, a functional enabler or a supporting function? • Complexity of the enterprise, including geographical spread, value chain coverage (e.g., in a manufacturing environment)—Does the enterprise manufacture and distribute parts, and/or is it also doing assembly activities? • Complexity of IT—Is IT highly complex (e.g., complex architecture, recent mergers) or is IT simple, standardised and streamlined? • Operating model, i.e., the degree to which the enterprise operates independently or is connected to its clients/suppliers, the degree of centralisation/decentralisation • Degree of change the enterprise is experiencing • Risk appetite—The amount of risk the enterprise is prepared to take (and, hopefully, is capable of absorbing) • Strategic priorities—Is the enterprise going for aggressive growth or is it in cost-cutting mode? • Recognised risk and opportunities—Understanding of internal risk and opportunities that are currently recognised 			

Audit/Accurance Program												
Phase A. Determine Scope of the Assurance Initiative												
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment								
A-2.3	Understand the external context of the enterprise.	<p><i>Identify all external environmental factors that could influence the performance and contents of the topic of the audit/assurance programme. These factors could include:</i></p> <ul style="list-style-type: none"> • Market/industry sector in which the enterprise operates, e.g., operating in the financial sector requires different IT requirements and IT capabilities than does the manufacturing environment • Rate of change going on in the market in which the enterprise operates in—Are business models changing fundamentally? Is the product or service at the end of an important life cycle moment? • Competitive environment in which the enterprise operates • Geopolitical environment—Is the geographical location subject to frequent natural disasters? Does the local political and overall economic context represent an additional risk? • Regulatory environment—Is the enterprise subject to new or stricter IT-related regulations or regulations impacting IT? Are there any other compliance requirements beyond regulation (e.g., industry-specific, contractual)? • Technology status and evolution—Is the enterprise using state-of-the art technology and, more important, how fast are relevant technologies evolving? • Dependency on third parties, e.g., suppliers, outsource providers • Recognised risk and opportunities—Understanding of internal risk and opportunities that are currently recognised 										
A-2.4	Given the overall assurance objective, <u>translate</u> the identified strategic priorities into concrete <u>objectives</u> for the assurance engagement.	<p><i>The level of abstraction/detail of the assurance objectives depends on the actual topic of the assurance engagement. If a fairly broad topic is chosen, e.g., risk management or enterprise governance, translation of these goals can be done at the level of enterprise goals and IT-related goals, as described in the COBIT 5 framework.</i></p> <p><i>If a more specific topic is chosen, e.g., change management, the objectives of the assurance engagement can be described in less abstract, more concrete, terms.</i></p> <p><i>Irrespective of the level of abstraction of the assurance objectives, the following should be observed:</i></p> <ul style="list-style-type: none"> • From the defined objectives of the assurance engagements, it must be possible to identify the enablers that are relevant to achieve the objectives, i.e., starting from the stated assurance objective, the assurance professional should be able to identify processes, policies, information, organisational structures, etc., required to achieve the objective, and therefore what should be included in scope. • The assurance objectives should consider all components of the value objective, i.e., they should consider not only risk, but also delivering benefits, optimising risk and optimizing resources. • To allow for prioritisation, the assurance professional could differentiate between key goals and additional goals. Enterprise and IT-related goals have associated metrics that can be used for setting the criteria (phase B) and during assessment (phase C). <table border="1"> <tr> <td>Key goals</td> <td>Enterprise goals: IT-related goals:</td> <td></td> <td></td> </tr> <tr> <td>Additional goals</td> <td></td> <td></td> <td></td> </tr> </table>	Key goals	Enterprise goals: IT-related goals:			Additional goals					
Key goals	Enterprise goals: IT-related goals:											
Additional goals												
A-2.5	Define the organizational boundaries of the	Describe the organizational boundaries of the assurance engagement, i.e., to which organizational										

Audit/Assurance Program				
Phase A. Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
	assurance initiative.	<i>entities the review is limited. All other aspects of scope limitation are identified during phase A-3.</i>		

Audit/Accurance Program				
Phase A. Determine Scope of the Assurance Initiative				
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment
A-3	Determine the enablers in scope and the instance(s) of the enablers in scope. COBIT 5 identifies seven enabler categories. In this section all seven are covered, and the assurance professional has the opportunity to select enablers from all categories to obtain the most comprehensive scope for the assurance engagement.			
A-3.1	<u>Define the Principles, Policies and Frameworks</u> in scope.			
A-3.2	<u>Define which Processes</u> are in scope of the review. Processes will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none">• Achievement of process goals• Application of process good practices• Existence and quality of work products (inputs and outputs) (insofar not covered by the information items assessments)	<i>COBIT 5: Enabling Processes</i> distinguishes a governance domain with a set of processes and a management domain, with four sets of processes. The processes in scope are identified using the goals cascade and subsequent customization. The resulting lists contain key processes and additional processes to be considered during this assurance engagement. Available resources will determine whether they can all be effectively assessed. Key processes		
		Additional processes		
A-3.3	<u>Define which Organisational Structures</u> will be in scope. Organisational Structures will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none">• Achievement of Organisational Structure goals, i.e., decisions• Application of Organisational Structures good practices	Based on the key processes identified in A-3.2, the following Organisational Structures and functions are considered to be in scope of this assurance engagement. Key priorities and availability of resources will determine how many and which ones will be reviewed in detail. Key Organisational Structures		
		Additional Organisational Structures		
A-3.4	<u>Define the Culture, Ethics and Behaviour</u> aspects in scope.			
A-3.5	<u>Define the Information items</u> in scope. Information items will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on: <ul style="list-style-type: none">• Achievement of Information goals, i.e., quality criteria of the information items• Application of Information good practices (Information attributes)	<i>COBIT 5: Enabling Processes</i> defines a number of inputs and outputs between processes. Based on the key processes identified in A-3.2, the following related inputs and outputs are considered in this section. Key priorities and availability of resources will determine how many and which ones will be reviewed in detail. Key Information Items		
		Additional Information Items		
A-3.6	<u>Define the Services, Infrastructure and Applications</u> in scope.			
A-3.7	<u>Define the People, Skills and Competencies</u> in scope.			

Audit/Accurance Program					
Phase A. Determine Scope of the Assurance Initiative					
Ref.	Assurance Step	Guidance	Issue Cross-reference	Comment	
	<p>Skill sets and competencies will be assessed during phase B of the assurance engagement against the criteria defined in phase A, and assessments will typically focus on:</p> <ul style="list-style-type: none"> • Achievement of skills set goals • Application of skills set and competencies good practices 				

Audit/Accurance Program																								
Phase B. Understand Enablers, Setting Suitable Assessment Criteria and Perform the Assessment Metrics																								
Ref.	Assurance Steps and Guidance				Issue Cross-reference																			
B-1	Agree on metrics and criteria for enterprise goals and IT-related goals. Assess enterprise goals and IT-related goals.																							
B-1.1	<p>Obtain (and agree on) metrics for enterprise goals and expected values of the metrics. Assess whether enterprise goals in scope are achieved.</p> <p>Leverage the list of suggested metrics for the enterprise goals to define, discuss and agree on a set of relevant, customized metrics for the enterprise goals, taking care that the suggested metrics are driven by the performance of the topic of this assurance initiative.</p> <p>Next, agree on the expected values for these metrics, i.e., the values against which the assessment will take place.</p> <p>The following metrics and expected values are agreed on for the key enterprise goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>Enterprise Goal</th> <th>Metric</th> <th>Expected Outcome</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>Agree on the expected values for the Enterprise goal metrics, i.e., the values against which the assessment will take place</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				Enterprise Goal	Metric	Expected Outcome	Assessment Step			Agree on the expected values for the Enterprise goal metrics, i.e., the values against which the assessment will take place	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.												
Enterprise Goal	Metric	Expected Outcome	Assessment Step																					
		Agree on the expected values for the Enterprise goal metrics, i.e., the values against which the assessment will take place	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																					
B-1.2	<p>Obtain (and agree on) metrics for IT-related goals and expected values of the metrics and assess whether IT-related goals in scope are achieved.</p> <p>The following metrics and expected values are agreed for the key IT-related goals defined in step A-2.4.</p> <table border="1"> <thead> <tr> <th>IT-related Goal</th> <th>Metric</th> <th>Expected Outcome</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.</td> <td>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>				IT-related Goal	Metric	Expected Outcome	Assessment Step			Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.												
IT-related Goal	Metric	Expected Outcome	Assessment Step																					
		Agree on the expected values for the IT-related goal metrics, i.e., the values against which the assessment will take place.	In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.																					

IT Audit and Assurance Program																	
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks																	
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment														
B-2	Obtain an understanding of the Principles, Policies and Frameworks in scope and set suitable assessment criteria. Repeat steps B-2.1 through B-2.5 for all remaining Principles, Policies and Frameworks in scope.																
B-2.1	<u>Understand the Principles, Policies and Frameworks context.</u> <i>Obtain and understanding of the overall system of internal control and the associated Principles, Policies and Frameworks</i>																
B-2.2	<u>Understand the stakeholders of the Principles, Policies and Frameworks.</u> <i>Understand the stakeholders in the policies. The stakeholders for the policies include those setting the policies and those who need to be in compliance with the policies.</i>																
B-2.3	<u>Understand the goals for the Principles, Policies and Frameworks</u> , and the related metrics and agree on expected values. Assess whether the Principles, Policies and Frameworks goals (outcomes) are achieved, i.e., assess the effectiveness of the Principles, Policies and Frameworks . In the context of this assurance engagement, the following goals will be reviewed for Principles, Policies and Frameworks :	Perform the assurance steps using the criteria described below.															
	<table border="1"> <thead> <tr> <th>Goal</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Comprehensiveness</td> <td></td><td>Verify that the set of policies is comprehensive in its coverage.</td></tr> <tr> <td>Currency</td> <td></td><td> Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update </td></tr> <tr> <td>Flexibility</td> <td></td><td>Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.</td></tr> <tr> <td>Availability</td> <td></td><td> <ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. </td></tr> </tbody> </table>	Goal	Criteria	Assessment Step	Comprehensiveness		Verify that the set of policies is comprehensive in its coverage.	Currency		Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 	Flexibility		Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.	Availability		<ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. 	
Goal	Criteria	Assessment Step															
Comprehensiveness		Verify that the set of policies is comprehensive in its coverage.															
Currency		Verify that the set of policies is up to date. This at least requires: <ul style="list-style-type: none"> A regular validation of all policies whether they are still up to date An indication of the policies' expiration date or date of last update 															
Flexibility		Verify the flexibility of the set of policies, i.e., that it is structured in such a way that it is easy to add or update policies as circumstances require.															
Availability		<ul style="list-style-type: none"> Verify that policies are available to all stakeholders. Verify that policies are easy to navigate and have a logical and hierarchical structure. 															
B-2.4	<u>Understand</u> the life cycle stages of the Principles, Policies and Frameworks , and agree on the relevant criteria. Assess to what extent the Principles, Policies and Frameworks life cycle is managed. <i>The life cycle of the IT-related policies is managed by the Process APO01. The review of this life cycle is therefore equivalent to a process review of process APO01 Manage the IT management framework.</i>																
B-2.5	<u>Understand</u> good practices related to the Principles, Policies and Frameworks and expected values. Assess the Principles, Policies and Frameworks design, i.e., assess the extent to which expected good practices are applied. <i>The assurance professional will, by using appropriate auditing techniques assess the following aspects.</i>																
	<table border="1"> <thead> <tr> <th>Good Practice</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Scope and validity</td> <td></td><td>Verify that the scope of the framework is described and the validity date is indicated.</td></tr> <tr> <td>Exception and escalation</td> <td></td><td> <ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. Through observation of a representative sample, verify that the exception and escalation procedure has not </td></tr> </tbody> </table>	Good Practice	Criteria	Assessment Step	Scope and validity		Verify that the scope of the framework is described and the validity date is indicated.	Exception and escalation		<ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. Through observation of a representative sample, verify that the exception and escalation procedure has not 							
Good Practice	Criteria	Assessment Step															
Scope and validity		Verify that the scope of the framework is described and the validity date is indicated.															
Exception and escalation		<ul style="list-style-type: none"> Verify that the exception and escalation procedure is described, explained and commonly known. Through observation of a representative sample, verify that the exception and escalation procedure has not 															

IT Audit and Assurance Program					
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Principles, Policies and Frameworks					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
			become de facto standard procedure.		
Compliance			Verify that the compliance checking mechanism and non-compliance consequences are clearly described and enforced.		

IT Audit and Assurance Program													
B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes													
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment								
B-3	<p>Obtain understanding of the Processes in scope and set suitable assessment criteria: for each process in scope (as determined in step A-3.2), additional information is collected and assessment criteria are defined.</p> <p>Repeat steps B-3.1 through B-3.7 for all Processes in scope.</p>												
B-3.1a	<p><u>Understand the Process context.</u></p>												
B-3.2a	<p><u>Understand the Process purpose.</u></p>												
B-3.3a	<p><u>Understand all process stakeholders</u> and their roles. This is equivalent to understanding the real RACI chart of the process. <i>Leverage the COBIT 5 RACI charts for the processes in scope to identify any additional stakeholders that will need to be involved in the assessment. In this assurance step, the translation is made between the theoretical RACI chart entry and the real enterprise.</i></p> <p>The stakeholders of the process are already defined in the RACI chart as a result of step A-3.3. In addition to those stakeholders, this process relies also on the following function(s), which therefore will need to be involved during the assurance engagement:</p>												
B-3.4a	<p><u>Understand the Process goals</u> and related <u>metrics</u>¹ and <u>define</u> expected Process values (criteria), and <u>assess</u> whether the Process goals are achieved, i.e., assess the <u>effectiveness</u> of the process.</p> <p><i>COBIT 5: Enabling Processes</i> have defined process goals, as described in, chapter 5, p. 149. Based on these goals and their related metrics, the following goals and associated metrics are defined for:</p> <table border="1"> <thead> <tr> <th>Process Goal</th> <th>Related Metrics</th> <th>Criteria/Expected Value</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td><i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i></td> <td><i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i></td> </tr> </tbody> </table>			Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step			<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>		
Process Goal	Related Metrics	Criteria/Expected Value	Assessment Step										
		<i>Agree on the expected values for the Process goal metrics, i.e., the values against which the assessment will take place.</i>	<i>In this step, the related metrics for each goal will be reviewed and an assessment will be made whether the defined criteria are achieved.</i>										
B-3.5a	<p><u>Agree</u> on suitable criteria to evaluate all processes in scope of the assurance engagement: <u>Define</u> and <u>agree</u> on the reference process, i.e., determine which base practices a process should at least include. (This usually is just a confirmation of the COBIT 5 processes already identified, unless there is reason for using a different reference process.)</p> <p><u>Agree</u> on the process practices that should be in place (process design). <u>Assess</u> the <u>process design</u>, i.e., assess to what extent:</p> <ul style="list-style-type: none"> • Expected process practices are applied. • Accountability and responsibility are assigned and assumed. 												
	<p>COBIT 5 Processes are described in <i>COBIT 5: Enabling Processes</i>. Each Process requires a number of management practices to be implemented, as described in the process description in the same guide. These are:</p> <ul style="list-style-type: none"> • A sound process design • The reference against which the process will be assessed in phase B with the criteria as mentioned, i.e., all management 												

¹ For COBIT 5 Processes a set of goals and metrics are identified in *COBIT 5 Enabling Processes*.

IT Audit and Assurance Program				
B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Processes				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-3.6a	practices are expected to be fully implemented.			
	Reference Process		Criteria: •	
	Reference Process Practices	Good Practice	Assessment Step	
B-3.6a	<u>Agree on the process work products</u> ² (inputs and outputs as defined in the process practices description) that are expected to be present. <u>Assess</u> to what extent the process work products are available.			
	The most relevant (and not assessed as Information items in scope in section A-3.5) of these work products are identified as follows, as well as the criteria against which they will be assessed, i.e., existence and usage.		Criteria: All listed work products should demonstrably exist and be used.	
	Process Practice	Work Products	Assessment Step	
			Apply appropriate audit techniques to determine the existence and appropriate use of each work product.	
B-3.7a	<u>Agree on the process capability level</u> to be achieved by the process.			
	<i>This step is warranted only if the process under review is a standard COBIT 5 governance or management process to which the ISO/IEC 15504 PAM can be applied. Any other processes, for which no reference practices, work products or outcomes are approved, cannot use this assessment method; therefore, the concept capability level does not apply.</i>			

² For COBIT 5 Processes a set of inputs and outputs for the different management practices are identified in *COBIT 5 Enabling Processes*.

Audit/Accurance Program													
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Organisational Structures													
Ref.	Assurance Steps and Guidance			Issue Cross-reference									
B-4	Obtain understanding of each Organisational Structure in scope and set suitable assessment criteria: For each Organisational Structure in scope (as determined in step A-3.3), additional information is collected and assessment criteria are defined.												
Repeat steps B-4.1 through B-4.5 for all Organisational Structure in scope.													
B-4.1	<p><u>Understand the Organisational structure</u> context. <i>Identify and document all elements that can help to understand the context in which the Organisational structure has to operate, including:</i></p> <ul style="list-style-type: none"> • The overall organisation • Management/process framework • History of the role/structure • Contribution of the Organisational Structure to achievement of goals 												
B-4.2	<p><u>Understand all stakeholders</u> of the Organisational structure/function. <i>Determine through documentation review (policies, management communications, etc.) the key stakeholders of the Organisational structure organization.</i></p> <ul style="list-style-type: none"> • Incumbent of the role and/or members of the Organisational Structure • Other key stakeholders affected by the decisions of the Organisational Structure/role 												
B-4.3	<p><u>Understand the goals</u> of the Organisational Structure, the related metrics and agree on expected values. Understand how these goals contribute to the achievement of the enterprise goals and IT-related goals. Assess whether the organisational structure goals (outcomes) are achieved.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; width: 30%;">Organisational Structure Goal</th> <th style="text-align: center; width: 70%;">Assessment Step</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Determine through interviews with key stakeholders and documentation review the goals of the Organisational structure, i.e., the decisions for which they are accountable^{3,4}.</td> <td style="padding: 5px;">This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> - They have contributed to the achievement of the IT-related and enterprise goals as anticipated. - Decisions are duly executed on a timely basis. </td> </tr> </tbody> </table>			Organisational Structure Goal	Assessment Step	Determine through interviews with key stakeholders and documentation review the goals of the Organisational structure , i.e., the decisions for which they are accountable ^{3,4} .	This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> - They have contributed to the achievement of the IT-related and enterprise goals as anticipated. - Decisions are duly executed on a timely basis. 						
Organisational Structure Goal	Assessment Step												
Determine through interviews with key stakeholders and documentation review the goals of the Organisational structure , i.e., the decisions for which they are accountable ^{3,4} .	This step only applies if specific goals are defined. In that case, the assurance professional will use appropriate auditing techniques to: <ul style="list-style-type: none"> • Identify the decisions made by the Organisational Structure. • Assess whether decisions are appropriately documented and communicated. • Evaluate the decisions by, assessing whether: <ul style="list-style-type: none"> - They have contributed to the achievement of the IT-related and enterprise goals as anticipated. - Decisions are duly executed on a timely basis. 												
B-4.4	<p><u>Agree on the expected good practices</u> for the Organisational Structure against which it will be assessed. Assess the Organisational Structure design, i.e., assess the extent to which expected good practices are applied.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: center; width: 25%;">Good Practice</th> <th style="text-align: center; width: 25%;">Criteria</th> <th style="text-align: center; width: 50%;">Assessment Step</th> </tr> </thead> <tbody> <tr> <td style="padding: 5px;">Operating principles</td> <td style="padding: 5px;"> <ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. </td> <td style="padding: 5px;"> <ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. </td> </tr> <tr> <td style="padding: 5px;">Composition</td> <td style="padding: 5px;">The Organisational Structure's composition is balanced and complete, i.e., all required</td> <td style="padding: 5px;">Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently</td> </tr> </tbody> </table>			Good Practice	Criteria	Assessment Step	Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 	Composition	The Organisational Structure's composition is balanced and complete, i.e., all required	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently	
Good Practice	Criteria	Assessment Step											
Operating principles	<ul style="list-style-type: none"> • Operating principles are documented. • Regular meetings take place as defined in operating principles. • Meeting reports/minutes are available and are meaningful. 	<ul style="list-style-type: none"> • Verify whether operating principles are appropriately documented. • Verify that regular meetings take place as defined in the operating principles. • Verify that meeting reports/minutes are available and are meaningful. 											
Composition	The Organisational Structure's composition is balanced and complete, i.e., all required	Assess whether the Organisational Structure's composition is balanced and complete, i.e., all required stakeholders are sufficiently											

³ The RACI charts in COBIT 5: *Enabling Processes* can be leveraged as a starting point for the expected goals of a role or **Organisational Structure**.

⁴ The **Organisational Structure/role** as described may not exist under the same name in the enterprise; in that case, the closest **Organisational Structure** assuming the same responsibilities and accountability should be considered.

Audit/Accurance Program					
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Organisational Structures					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
B-4.5a	Span of control	stakeholders are sufficiently represented.	represented.		
	Span of control	<ul style="list-style-type: none"> The span of control of The Organisational Structure is defined. The span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. The span of control is in line with the overall enterprise governance arrangements. 	<ul style="list-style-type: none"> Verify whether the span of control of the Organisational Structure is defined. Assess whether the span of control is adequate, i.e., the Organisational Structure has the right to make all decisions it should. Verify and assess whether the span of control is in line with the overall enterprise governance arrangements. 		
	Level of authority/decision rights	<ul style="list-style-type: none"> Decision rights of the Organisation Structure are defined and documented. Decision rights of the Organisational Structure are respected and complied with (also a culture/behaviour issue). 	<ul style="list-style-type: none"> Verify that decision rights of the Organisation Structure are defined and documented. Verify whether decision rights of the Organisational Structure are complied with and respected. 		
	Delegation of authority	Delegation of authority is implemented in a meaningful way.	Verify whether delegation of authority is implemented in a meaningful way.		
	Escalation procedures	Escalation procedures are defined and applied.	Verify the existence and application of escalation procedures.		
Understand the life cycle and agree on expected values. Assess the extent to which the Organisational Structure life cycle is managed.					
Life-Cycle Element		Criteria	Assessment Step		
Mandate		<ul style="list-style-type: none"> The Organisational Structure is formally established. The Organisational Structure has a clear, documented and well-understood mandate. 	<ul style="list-style-type: none"> Verify through interviews and observations that the Organisational Structure is formally established. Verify through interviews and observations that the Organisational Structure has a clear, documented and well understood mandate. 		
Monitoring		<ul style="list-style-type: none"> The performance of the Organisational Structure and its members should be regularly monitored and evaluated by competent and independent assessors. The regular evaluations should result in the required continuous improvements to the Organisational Structure, either in its composition, mandate or any other parameter. 	<ul style="list-style-type: none"> Verify whether the performance of the Organisational Structure and its members is regularly monitored and evaluated by competent and independent assessors. Verify whether the regular evaluations have resulted in improvements to the Organisational Structure, in its composition, mandate or any other parameter. 		

Audit/Accurance Program															
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Culture, Ethics and Behaviour															
Ref.	Assurance Step and Guidance	Issue Cross-reference	Comment												
B-5	<p>Obtain understanding of the Culture, Ethics and Behaviour in scope.</p> <p>Repeat steps B-5.1 through B-5.5 for all remaining Culture, Ethics and Behaviour in scope.</p>														
B-5.1	<p><u>Understand</u> the Culture, Ethics and Behaviour context.</p> <ul style="list-style-type: none"> • <i>What the overall corporate Culture is like</i> • <i>Understand the interconnection with other enablers in scope:</i> <ul style="list-style-type: none"> - <i>Identify roles and structures that could be affected by the Culture.</i> - <i>Identify processes that could be affected by Culture, Ethics and Behaviour, including any processes in scope of the review.</i> 														
B-5.2	<p><u>Understand</u> the major stakeholders of the Culture, Ethics and Behaviour.</p> <p><i>Understand to whom the behaviour requirements will apply, i.e., understand who embodies the roles/structures expected to demonstrate the correct set of Behaviours. This is usually linked to the roles and Organisational Structures identified in scope.</i></p>														
B-5.3	<p><u>Understand</u> the goals for the Culture, Ethics and Behaviour, and the related metrics and agree on expected values.</p> <p>Assess whether the Culture, Ethics and Behaviour goals (outcomes) are achieved, i.e., assess the effectiveness of the Culture, Ethics and Behaviour.</p> <table border="1"> <tr> <td>In the context of this assurance engagement and the behaviour at hand, the desired behaviour, the following Culture, Ethics and Behaviour are desired:</td> <td>Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. • For a representative sample of individuals, perform the following assessment steps. </td> </tr> <tr> <td>Desired Behaviour (Culture, Ethics and Behaviour Goal)</td> <td>Assessment Step</td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> <tr> <td></td> <td></td> </tr> </table>	In the context of this assurance engagement and the behaviour at hand, the desired behaviour , the following Culture, Ethics and Behaviour are desired:	Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. • For a representative sample of individuals, perform the following assessment steps. 	Desired Behaviour (Culture, Ethics and Behaviour Goal)	Assessment Step										
In the context of this assurance engagement and the behaviour at hand, the desired behaviour , the following Culture, Ethics and Behaviour are desired:	Culture and especially Behaviours are associated to individuals and the Organisational Structures of which they are a part, therefore, by using appropriate auditing techniques, the assurance professional will: <ul style="list-style-type: none"> • Identify individuals who must comply with the Behaviours under review. • Identify the Organisational Structures involved. • Assess whether desired Behaviours can be observed. • Assess whether undesirable Behaviours are absent. • For a representative sample of individuals, perform the following assessment steps. 														
Desired Behaviour (Culture, Ethics and Behaviour Goal)	Assessment Step														
B-5.4	<p><u>Understand</u> the life cycle stages of the Culture, Ethics and Behaviour, and agree on the relevant criteria.</p> <p>Assess to what extent the Culture, Ethics and Behaviour life cycle is managed.</p> <p>(This aspect is already covered by the assessment of the good practices, hence no additional separate assurance steps are defined here.)</p>														
B-5.5	<p><u>Understand</u> good practice when dealing with Culture, Ethics and Behaviour, and agree on relevant criteria.</p> <p>Assess the Culture, Ethics and Behaviour design, i.e., assess to what extent expected good practices are applied.</p> <table border="1"> <thead> <tr> <th>Good Practice</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Communication, enforcement and rules</td> <td>Existence and quality of the communication</td> <td></td> </tr> <tr> <td>Incentives and rewards</td> <td>Existence and application of appropriate rewards and incentives</td> <td></td> </tr> <tr> <td>Awareness</td> <td>Awareness of desired Behaviours</td> <td></td> </tr> </tbody> </table>	Good Practice	Criteria	Assessment Step	Communication, enforcement and rules	Existence and quality of the communication		Incentives and rewards	Existence and application of appropriate rewards and incentives		Awareness	Awareness of desired Behaviours			
Good Practice	Criteria	Assessment Step													
Communication, enforcement and rules	Existence and quality of the communication														
Incentives and rewards	Existence and application of appropriate rewards and incentives														
Awareness	Awareness of desired Behaviours														

Audit/Accurance Program																																															
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Information Items																																															
Ref.	Assurance Steps and Guidance	Issue Cross-reference	Comment																																												
B-6	<p>Obtain understanding of the Information Items in scope.</p> <p>Repeat steps B-6.1 through B-6.5 for all remaining Information items in scope.</p>																																														
B-6.1	<p><u>Understand the Information item context:</u></p> <ul style="list-style-type: none"> • Where and when is it used? • For what purpose is it used? • Understand the connection with other enablers in scope, e.g.: <ul style="list-style-type: none"> - Used by which processes? - Which Organisational Structures are involved? - Which services/applications are involved? 																																														
B-6.2	<p><u>Understand the major stakeholders of the Information item.</u> <u>Understand the stakeholders for the Information item, i.e., identify the:</u></p> <ul style="list-style-type: none"> • Information producer • Information custodian • Information consumer <p><i>Stakeholders should be at the appropriate organisational level.</i></p>																																														
B-6.3	<p><u>Understand the major quality criteria for the Information item, the related metrics and agree on expected values.</u> <u>Assess whether the Information item quality criteria (outcomes) are achieved, i.e., assess the effectiveness of the Information item.</u></p> <p>Leverage the COBIT 5 Information enabler model⁵ focusing on the quality goals description to select the most relevant Information quality criteria for the Information item at hand. Document expectations regarding information criteria. The COBIT 5 Information enabler model identifies 15 different quality criteria—although all of them are relevant, it is nonetheless possible and recommended to focus on a subset of the most important criteria for the Information item at hand.</p> <p>Mark the quality dimensions with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p> <table border="1"> <thead> <tr> <th>Quality Dimension</th> <th>Key Criteria</th> <th>Description</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Accuracy</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Objectivity</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Believability</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Reputation</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Relevancy</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Completeness</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Currency</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Amount of information</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Concise representation</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Consistent representation</td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Quality Dimension	Key Criteria	Description	Assessment Step	Accuracy				Objectivity				Believability				Reputation				Relevancy				Completeness				Currency				Amount of information				Concise representation				Consistent representation				<p>The assurance professional will, by using appropriate auditing techniques, verify all quality criteria in scope and assess whether the criteria are met.</p>	
Quality Dimension	Key Criteria	Description	Assessment Step																																												
Accuracy																																															
Objectivity																																															
Believability																																															
Reputation																																															
Relevancy																																															
Completeness																																															
Currency																																															
Amount of information																																															
Concise representation																																															
Consistent representation																																															

⁵ COBIT 5 framework, Appendix G, p.81-84

Audit/Accurance Program				
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Information Items				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
B-6.4a	Interpretability			
	Understandability			
	Manipulation			
	Availability			
	Restricted access			
B-6.4a	<p>Understand the life cycle stages of the Information item, and agree on the relevant criteria. Assess to what extent the Information item life cycle is managed.</p> <p>The life cycle of any Information item is managed through several business and IT-related processes. The scope of this review already includes a review of (IT-related) processes so this aspect does not need to be duplicated here.</p> <ul style="list-style-type: none"> When the Information item is internal to IT, the process review will have covered the life cycle aspects sufficiently. When the Information item also involves other stakeholders outside IT or other non-IT processes, some of the life cycle aspects need to be assessed. <p>Mark the life cycle stages with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p>			
	Life Cycle Stage	Key Criteria	Description	Assessment Step
	Plan			
	Design			
	Build/acquire			
	Use/operate			
	Evaluate/monitor			
	Update/dispose			
B-6.5a	<p>Understand important attributes of the Information item and expected values. Assess the Information item design, i.e., assess the extent to which expected good practices are applied.</p> <p>Good practices for Information items are defined as a series of attributes for the Information item⁶. The assurance professional will, by using appropriate audit techniques, verify all attributes in scope and assess whether the attributes are adequately defined.</p> <p>Mark the attributes with a '✓' that are deemed most important (key criteria), and by consequence will be assessed against the described criteria.</p>			
	Attribute	Key Criteria	Description	Assessment Step
	Physical			
	Empirical			
	Syntactic			
	Semantic			
	Pragmatic			
	Social			

⁶ COBIT 5 framework, appendix G, p. 81-84

Audit/Accurance Program															
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Services, Infrastructures and Applications															
Ref.	Assurance Steps and Guidance			Issue Cross-reference											
B-7	<p>Obtain understanding of the Services, Infrastructure and Applications in scope. Assess Services, Infrastructure and Applications.</p> <p>Repeat steps B-7.1 through B-7.4 for all remaining Services, Infrastructure and Applications in scope.</p>														
B-7.1	<p><u>Understand the Services, Infrastructure and Applications</u> context. <i>Understand the organisational and technological context of this service. Refer to step A-2.2 and A-2.3 and re-use that information to understand the significance of this Service, Infrastructure and Application.</i></p>														
B-7.2	<p><u>Understand the major stakeholders of the Services, Infrastructure and Applications.</u> <i>Understand who will be the major stakeholders of the service, i.e., the sponsor, provider and users. Stakeholders will include a number of organisational roles but could also link to Processes.</i></p>														
B-7.3	<p><u>Understand the major goals for the Services, Infrastructure and Applications</u>, the related metrics and agree on expected values. Assess whether the Services, Infrastructure and Applications goals (outcomes) are achieved, i.e., assess the effectiveness of the Services, Infrastructure and Applications.</p> <table border="1"> <thead> <tr> <th>Goal</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Service description</td> <td> <ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders </td> <td> <ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. </td> </tr> <tr> <td>Service level definition</td> <td> <p>Service levels are defined for :</p> <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness </td> <td> <ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. </td> </tr> <tr> <td>Contribution to related enablers, IT and enterprise goals</td> <td>The Service contributes to the achievement of related enabler and IT-related and enterprise goals.</td> <td>Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.</td> </tr> </tbody> </table>			Goal	Criteria	Assessment Step	Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 	Service level definition	<p>Service levels are defined for :</p> <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 	Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.
Goal	Criteria	Assessment Step													
Service description	<ul style="list-style-type: none"> The Service is clearly described. Roles and responsibilities are clearly defined The Service is available to all potential stakeholders 	<ul style="list-style-type: none"> Verify that the Service exists and is clearly described. Verify that roles and responsibilities are clearly defined. Assess the quality of the Service description and of the Service offered. Verify the accessibility of the Service to all potential stakeholders. 													
Service level definition	<p>Service levels are defined for :</p> <ul style="list-style-type: none"> Quality of the service deliverables Ease to request the service Timeliness 	<ul style="list-style-type: none"> Verify that the following aspects are dealt with in the Service level definitions: <ul style="list-style-type: none"> Quality of the Service deliverables Ease to request the service Timeliness Verify to what extent Service levels are achieved. 													
Contribution to related enablers, IT and enterprise goals	The Service contributes to the achievement of related enabler and IT-related and enterprise goals.	Assess to what extent the Service contributes to the achievement of the related enabler goals and to the overall IT-related and enterprise goals.													
B-7.4	<p><u>Understand good practice related to the Services, Infrastructure and Applications</u> and expected values. Assess the Services, Infrastructure and Applications design, i.e., assess to what extent expected good practices are applied. <i>Leverage the description of Services, Infrastructure and Applications in the COBIT 5 framework⁷ to identify good practices related to Services, Infrastructure And Applications. In general the following practices need to be implemented:</i></p> <ul style="list-style-type: none"> Buy/build decision needs to be taken. Use of the Service needs to be clear. <table border="1"> <thead> <tr> <th>Good Practice</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Sourcing (buy/build)</td> <td>A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.</td> <td> <ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. </td> </tr> </tbody> </table>			Good Practice	Criteria	Assessment Step	Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. 						
Good Practice	Criteria	Assessment Step													
Sourcing (buy/build)	A formal decision—based on a business case—needs to be taken regarding the sourcing of the Service.	<ul style="list-style-type: none"> Verify that a formal decision—based on a business case—was taken regarding the sourcing of the Service. Verify the validity and quality of the business case. 													

⁷ COBIT 5 framework, appendix G, p.85-86

Audit/Accurance Program					
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment Services, Infrastructures and Applications					
Ref.	Assurance Steps and Guidance			Issue Cross-reference	Comment
Use	The use of the Service needs to be clear: <ul style="list-style-type: none"> • When it needs to be used and by whom • The required compliance levels with the Service's output 	<ul style="list-style-type: none"> • Verify that the sourcing decision has been duly executed. • Verify that the use of the Service is clear, i.e., it is known when and by whom the service needs to be used. • Verify that actual use is in line with requirement above. • Verify that the actual Service output is adequately used. • Verify that Service levels are monitored and achieved. 			

Audit/Accurance Program																											
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment People, Skills and Competencies																											
Ref.	Assurance Steps and Guidance			Issue Cross-reference																							
B-8	Obtain understanding of the People, Skills and Competencies in scope. Repeat steps B-8.1 through B-8.5 for all remaining People, Skills and Competencies in scope.																										
B-8.1a	<p><u>Understand the People, Skills and Competencies</u> context. <i>Understand the context of the Skill/Competency, i.e.:</i></p> <ul style="list-style-type: none"> • <i>Where and when is it used?</i> • <i>For what purpose is it used?</i> • <i>Understand the connection with other enablers in scope, e.g.:</i> <ul style="list-style-type: none"> – <i>In which roles and structures is the Skill/Competency used? (See also B-4.1.)</i> <p><i>Which behaviours are associated with the Skill/Competency?</i></p>																										
B-8.2a	<p><u>Understand the major stakeholders</u> for the People, Skills and Competencies. <i>Identify to whom in the organisation the skill requirement applies.</i></p>																										
B-8.3a	<p><u>Understand the major goals</u> for the People, Skills and Competencies, the related metrics and <u>agree</u> on expected values. <i>Assess whether the People, Skills and Competencies goals</i> (outcomes) are achieved, i.e., assess the effectiveness of the People, Skills and Competencies.</p> <table border="1" data-bbox="265 743 2142 992"> <thead> <tr> <th>Goal</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Experience</td> <td></td> <td></td> </tr> <tr> <td>Education</td> <td></td> <td></td> </tr> <tr> <td>Qualification</td> <td></td> <td></td> </tr> <tr> <td>Knowledge</td> <td></td> <td></td> </tr> <tr> <td>Technical skills</td> <td></td> <td></td> </tr> <tr> <td>Behavioural skills</td> <td></td> <td></td> </tr> <tr> <td>Number of people with appropriate skill level</td> <td></td> <td></td> </tr> </tbody> </table>			Goal	Criteria	Assessment Step	Experience			Education			Qualification			Knowledge			Technical skills			Behavioural skills			Number of people with appropriate skill level		
Goal	Criteria	Assessment Step																									
Experience																											
Education																											
Qualification																											
Knowledge																											
Technical skills																											
Behavioural skills																											
Number of people with appropriate skill level																											
B-8.4a	<p><u>Understand the life cycle</u> stages of the People, Skills and Competencies, and agree the relevant criteria. <i>Assess to what extent the People, Skills and Competencies life cycle is managed.</i></p>																										
	<p>For the People, Skills and Competencies at hand, the life cycle phases and associated criteria can be expressed in function of the process APO07.</p>		<p>For the People, Skills and Competencies at hand the assurance professional will perform the following assessment steps.</p>																								
	<table border="1" data-bbox="265 1124 2142 1427"> <thead> <tr> <th>Life Cycle Element</th> <th>Criteria</th> <th>Assessment Step</th> </tr> </thead> <tbody> <tr> <td>Plan</td> <td>Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.</td> <td>Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.</td> </tr> <tr> <td>Design</td> <td>Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill.</td> <td>Assess whether practice APO07.03 activity 2 is implemented in relation to this skill.</td> </tr> <tr> <td></td> <td>Practice APO07.03 activity 3 (Provide access to knowledge)</td> <td>Assess whether practice APO07.03 activity 3 is implemented in</td> </tr> </tbody> </table>			Life Cycle Element	Criteria	Assessment Step	Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.	Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill.		Practice APO07.03 activity 3 (Provide access to knowledge)	Assess whether practice APO07.03 activity 3 is implemented in												
Life Cycle Element	Criteria	Assessment Step																									
Plan	Practice APO07.03 activity 1 (Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT and process goals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 1 is implemented in relation to this skill.																									
Design	Practice APO07.03 activity 2 (Provide formal career planning and professional development to encourage competency development, opportunities for personal advancement and reduced dependence on key individuals.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 2 is implemented in relation to this skill.																									
	Practice APO07.03 activity 3 (Provide access to knowledge)	Assess whether practice APO07.03 activity 3 is implemented in																									

Audit/Accurance Program				
Phase B. Understand Enablers, Set Suitable Assessment Criteria and Perform the Assessment People, Skills and Competencies				
Ref.	Assurance Steps and Guidance			Issue Cross-reference
		repositories to support the development of skills and competencies.) is implemented in relation to this skill.	relation to this skill.	
	Build	Practice APO07.03 activity 4 (Identify gaps between required and available skills and develop action plans to address them on an individual and collective basis, such as training [technical and behavioural skills], recruitment, redeployment and changed sourcing strategies.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 4 is implemented in relation to this skill.	
	Operate	Practice APO07.03 activity 5 (Develop and deliver training programmes based on organisational and process requirements, including requirements for enterprise knowledge, internal control, ethical conduct and security.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 5 is implemented in relation to this skill.	
	Evaluate	Practice APO07.03 activity 6 (Conduct regular reviews to assess the evolution of the skills and competencies of the internal and external resources. Review succession planning.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 6 is implemented in relation to this skill.	
	Update/dispose	Practice APO07.03 activity 7 (Review training materials and programmes on a regular basis to ensure adequacy with respect to changing enterprise requirements and their impact on necessary knowledge, skills and abilities.) is implemented in relation to this skill.	Assess whether practice APO07.03 activity 7 is implemented in relation to this skill.	
B-8.5a	<u>Understand</u> good practice related to the People, Skills and Competencies and expected values. Assess the People, Skills and Competencies design, i.e., assess to what extent expected good practices are applied.			
Good Practice	Criteria	Assessment Step		
Skill set and Competencies are defined.	<ul style="list-style-type: none"> Determine that an inventory of Skills and Competencies is maintained by organisational unit, job function and individual. Evaluate the relevance and the contribution of the Skills and Competencies to the achievement of the goals of the Organisational Structure, and by consequence, IT-related goals and enterprise goals. Evaluate the gap analysis between necessary portfolio of Skills and Competencies and current inventory of skills and capabilities. 			
Skill levels are defined.	<ul style="list-style-type: none"> Assess the flexibility and performance of meeting Skills development to address identified gaps between necessary and current Skill levels. Assess the process for 360-degree performance evaluations. 			

Audit/Accurance Program		
Phase C. Communicate the Results of the Assessment		
Ref.	Assurance Step	Guidance
C-1	Document exceptions and gaps.	
C-1.1	Understand and document weaknesses and their impact on the achievement of process goals.	<ul style="list-style-type: none"> Illustrate the impact of enabler failures or weaknesses with numbers and scenarios of errors, inefficiencies and misuse. Clarify vulnerabilities, threats and missed opportunities that are likely to occur if enablers do not perform effectively.
C-1.2	Understand and document weaknesses and their impact on enterprise goals.	<ul style="list-style-type: none"> Illustrate what the weaknesses would affect (e.g., business goals and objectives, enterprise architecture elements, capabilities, resources). Relate the impact of not achieving the enabler goals to actual cases in the same industry and leverage industry benchmarks. Document the impact of actual enabler weaknesses in terms of bottom-line impact, integrity of financial reporting, hours lost in staff time, loss of sales, ability to manage and react to the market, customer and shareholder requirements, etc. Point out the consequence of noncompliance with regulatory requirements and contractual agreements. Measure the actual impact of disruptions and outages on business processes and objectives, and on customers (e.g., number, effort, downtime, customer satisfaction, cost).
C-2	Communicate the work performed and findings.	
C-2.1	Communicate the work performed.	<ul style="list-style-type: none"> Communicate regularly to the stakeholders identified in A-1 on progress of the work performed.
C-2.2	Communicate preliminary findings to the assurance engagement stakeholders defined in A-1.	<ul style="list-style-type: none"> Document the impact (i.e., customer and financial impact) of errors that could have been caught by effective enablers. Measure and document the impact of rework (e.g., ratio of rework to normal work) as an efficiency measure affected by enabler weaknesses. Measure the actual business benefits and illustrate cost savings of effective enablers after the fact. Use benchmarking and survey results to compare the enterprise's performance with others. Use extensive graphics to illustrate the issues. Inform the person responsible for the assurance activity about the preliminary findings and verify his/her correct understanding of those findings.
C-2.3	Deliver a report (aligned with the terms of reference, scope and agreed-on reporting standards) that supports the results of the initiative and enables a clear focus on key issues and important actions.	