Technical and Risk Management Reference Series

Security, Audit and Control Features

SAP® ERP

3rd Edition

Audit/Assurance Programs and ICQs

ISACA®
Serving IT Governance Professionals

ISACA®
With more than 86,000 constituents in more than 160 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems assurance and security, enterprise governance of IT, and IT-related risk and compliance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA® Journal*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®) and Certified in the Governance of Enterprise IT® (CGEIT®) designations. ISACA developed and continually updates the COBIT®, Val IT™ and Risk IT frameworks, which help IT professionals and enterprise leaders fulfill their IT governance responsibilities and deliver value to the business.

Disclaimer
ISACA has designed and created *Security, Audit and Control Features SAP® ERP, 3rd Edition* (*Technical and Risk Management Reference Series*) Excerpt of the Audit/Assurance Programs and ICQs (the "Work"), primarily as an educational resource for control 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 any 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, security professionals should apply their own professional judgment to the specific control 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 AG 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 AG is not the publisher of this book and is not responsible for it under any aspect of press law.

Reservation of Rights

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

ISBN 978-1-60420-115-4
Security, Audit and Control Features SAP® ERP, 3rd Edition (*Technical and Risk Management Reference Series*)
Excerpt of the Audit/Assurance Programs and ICQs
Printed in the United States of America

Acknowledgments

ISACA wishes to recognize:

Researcher
Mark Sercombe, CISA, CA, CIA, Sponsoring Partner, Deloitte, Australia
Matthew Saines, CISA, CISSP, Deloitte, Australia
Maria Woodyatt, CISA, Deloitte, Australia
Bernadette Louat, CISA, Deloitte, Australia
Najeeba Hossain, Deloitte, Australia
Mark Hickabottom, Ph.D, CISA, Deloitte, UK
Neal J. Velayo, CISA, Deloitte, USA
Iain Muir, CISA, Deloitte, Australia

Project Leaders
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia
Anthony P. Noble, CISA, CCP, Viacom Inc., USA

Expert Reviewers
Akin Akinbosoye, CISA, CISM, CGEIT, PMI-RMP, Healthcare Corporation of America (HCA), USA
Robin Basham, CISA, CGEIT, SOAProjects Inc., USA
Steve Biskie, CISA, CPA, CITP, ConnectINT Solutions, USA; ACL Services, Ltd., Canada
Michael Brinkloev, KPMG, Denmark
Adrienne C. Chung, CISA, CISM, CA, Chungs' Computer Assistance LLP, Canada
Chang Lu Miao, CISA, ACIB, CPA, MCSE, SAP T/C, Auditor-General's Office, Singapore
Mayank Garg, CISA, Atmel Corportation, USA
David T. Green, Ph.D., Governors State University, USA
Guhapriya Iyer, CISA, ACA, Grad CWA, Cerebrus Consulting, India
Babu Jayendran, CISA, FCA, Babu Jayendran Consulting, India
Emma Johari, CISA, KPMG, Australia
Pam Kammermeier, CISA, Altran Control Solutions, USA
Rajni Lalsinghani, CISA, CISM, TechnoSols Consulting Services, Australia
K. K. Mookhey, CISA, CISM, CISSP, Network Intelligence India (NII), India
Stane Moškon, CISA, CISM, VRIS d.o.o., Slovenia
Moonga Mumba, CISA, Zambia Revenue Authority, Zambia
Babu Shekhar Shetty, CISA, CISSP, Timken Pvt. Ltd., India
Surapong Surabotsopon, CISA, CISM, CGEIT, ITIL, Goodyear (Thailand) PCL, Thailand
William G. Teeter, CISA, CGEIT, PMP, USA
Jinu Varghese, CISA, OCA, PricewaterhouseCoopers LLP, Canada
Chakri Wicharn, CISA, CISM, Thailand
David Yeung, CISA, CIA, CFE, KPMG, China

ISACA Board of Directors 2008-2009
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info. SA & CV, Mexico, Vice President
Robert E. Stroud, CGEIT, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Frank Yam, CISA, CCP, CFE, CFSA, CIA, FFA, FHKCS, FHKIoD, Focus Strategic Group Inc., Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Director

Table of Contents

Page

Appendix D. SAP ERP Revenue, Expenditure, Inventory, Basis Audit/Assurance Programs 5
Revenue Audit/Assurance Program 5
Expenditure Audit/Assurance Program 27
Inventory Audit/Assurance Program 50
Basis Audit/Assurance Program 70

Appendix E. SAP ERP Audit ICQs 109
Revenue ICQ 110
Expenditure ICQ 113
Inventory ICQ 116
Basis ICQ 121

Appendix D. SAP ERP Revenue, Expenditure, Inventory, Basis Audit/Assurance Programs

Revenue Business Cycle

I. Introduction

Overview
ISACA developed *ITAF™: A Professional Practices Framework for IT Assurance* as a comprehensive and good-practice-setting model. ITAF provides standards that are designed to be mandatory, and are the guiding principles under which the IT audit and assurance profession operates. The guidelines provide information and direction for the practice of IT audit and assurance. The tools and techniques provide methodologies, and tools and templates to provide direction in the application of IT audit and assurance processes.

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.. This audit/assurance program is intended to be utilized by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF, section 2200—General Standards. The audit/assurance programs are part of ITAF, section 4000—IT Assurance Tools and Techniques.

Control Framework
The audit/assurance programs have been developed in alignment with the COBIT framework—specifically COBIT 4.1—using generally applicable and accepted good practices. They reflect ITAF, sections 3400—IT Management Processes, 3600—IT Audit and Assurance Processes, and 3800—IT Audit and Assurance Management.

Many enterprises have embraced several frameworks at an enterprise level, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework. The importance of the control framework has been enhanced due to regulatory requirements by the US Securities and Exchange Commission (SEC) as directed by the US Sarbanes-Oxley Act of 2002 and similar legislation in other countries. They seek to integrate control framework elements used by the general audit/assurance team into the IT audit and assurance framework. Since COSO is widely used, it has been selected for inclusion in this audit/assurance program. The reviewer may delete or rename columns in the audit program to align with the enterprise's control framework.

IT Governance, Risk and Control
IT governance, risk and control are critical in the performance of any assurance management process. Governance of the process under review will be 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 will be evaluated as steps in the audit/assurance program. Controls are the primary evaluation point in the process. The audit/assurance program will identify the control objectives with steps to determine control design and effectiveness.

Responsibilities of IT Audit and Assurance Professionals
IT audit and assurance professionals are expected to customize this document to the environment in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it is not intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional holds the Certified Information Systems Auditor (CISA) designation, or has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the CISA designation and necessary subject matter expertise to adequately review the work performed.

II. Using This Document

This audit/assurance program was developed to assist the audit and assurance professional in designing and executing a review. Details regarding the format and use of the document follow.

Work Program Steps
The first column of the program describes the steps to be performed. The numbering scheme used provides built-in work paper numbering for ease of cross-reference to the specific work paper for that section. IT audit and assurance professionals are encouraged to make modifications to this document to reflect the specific environment under review.

COBIT Cross-reference
The COBIT cross-reference provides the audit and assurance professional with the ability to refer to the specific COBIT control objective that supports the audit/assurance step. The COBIT control objective should be identified for each audit/assurance step in the section. Multiple cross-references are not uncommon. Processes at lower levels in the work program are too granular to be cross-referenced to COBIT. The audit/assurance program is organized in a manner to facilitate an evaluation through a structure parallel to the development process. COBIT provides in-depth control objectives and suggested control practices at each level. As the professional reviews each control, he/she should refer to COBIT 4.1 or the *IT Assurance Guide: Using COBIT* for good-practice control guidance.

COSO Components
As noted in the introduction, COSO and similar frameworks have become increasingly popular among audit and assurance professionals. This ties the assurance work to the enterprise's control framework. While the IT audit/assurance function has COBIT as a framework, operational audit and assurance professionals use the framework established by the enterprise. Since COSO is the most prevalent internal control framework, it has been included in this document and is a bridge to align IT audit/assurance with the rest of the audit/assurance function. Many audit/assurance organizations include the COSO control components within their report and summarize assurance activities to the audit committee of the board of directors.

For each control, the audit and assurance professional should indicate the COSO component(s) addressed. It is possible, but generally not necessary, to extend this analysis to the specific audit step level.

The original COSO internal control framework contained five components. In 2004, COSO was revised as the *Enterprise Risk Management (ERM) Integrated Framework* and extended to eight components. The primary difference between the two frameworks is the additional focus on ERM and integration into the business decision model. ERM is in the process of being adopted by large enterprises. The two frameworks are compared in **figure AD1**.

Figure AD1—Comparison of COSO Internal Control and ERM Integrated Frameworks

Internal Control Framework	ERM Integrated Framework
Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.	**Internal Environment**: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an enterprise's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
	Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the enterprise's mission and are consistent with its risk appetite.
	Event Identification: Internal and external events affecting achievement of an enterprise's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
Risk Assessment: Every enterprise faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, and thus risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.	**Risk Assessment**: Risks are analyzed, considering the likelihood and impact, as a basis for determining how they could be managed. Risk areas are assessed on an inherent and residual basis.
	Risk Response: Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the enterprise's risk tolerances and risk appetite.
Control Activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the enterprise's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.	**Control Activities:** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders.	**Information and Communication:** Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the enterprise.
Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.	**Monitoring:** The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Information for **figure AD1** was obtained from the COSO web site *www.coso.org/aboutus.htm.*

The original COSO internal control framework addresses the needs of the IT audit and assurance professional: control environment, risk assessment, control activities, information and

communication, and monitoring. As such, ISACA has elected to utilize the five-component model for these audit/assurance programs. As more enterprises implement the ERM model, the additional three columns can be added, if relevant. When completing the COSO component columns, consider the definitions of the components as described in **figure AD1**.

Reference/Hyperlink
Good practices require the audit and assurance professional to create a work paper for each line item, which describes the work performed, issues identified and conclusions. The reference/hyperlink is to be used to cross-reference the audit/assurance step to the work paper that supports it. The numbering system of this document provides a ready numbering scheme for the work papers. If desired, a link to the work paper can be pasted into this column.

Issue Cross-reference
This column can be used to flag a finding/issue that the IT audit and 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).

Comments
The comments column can be used to indicate the waiving of a step or other notations. It is not to be used in place of a work paper describing the work performed.

III. Controls Maturity Analysis

One of the consistent requests of stakeholders who have undergone IT audit/assurance reviews is a desire to understand how their performance compares to good practices. Audit and assurance professionals must provide an objective basis for the review conclusions. Maturity modeling for management and control over IT processes is based on a method of evaluating the organization, so it can be rated from a maturity level of nonexistent (0) to optimized (5). This approach is derived from the maturity model that the Software Engineering Institute (SEI) of Carnegie Mellon University defined for the maturity of software development.

The *IT Assurance Guide: Using COBIT*, appendix VII—Maturity Model for Internal Control, in **figure AD2**, provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimized level. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

Figure AD2—Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Nonexistent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.

Figure AD2—Maturity Model for Internal Control		
Maturity Level	**Status of the Internal Control Environment**	**Establishment of Internal Controls**
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized occasionally.
5 Optimized	An enterprisewide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

The maturity model evaluation is one of the final steps in the evaluation process. The IT audit and assurance professional can address the key controls within the scope of the work program and formulate an objective assessment of the maturity levels of the control practices. The maturity assessment can be a part of the audit/assurance report, and used as a metric from year to year to document progression in the enhancement of controls. However, it must be noted that the perception of the maturity level may vary between the process/IT asset owner and the auditor. Therefore, an auditor should obtain the concerned stakeholder's concurrence before submitting the final report to management.

At the conclusion of the review, once all findings and recommendations are completed, the professional assesses the current state of the COBIT control framework and assigns it a maturity level using the six-level scale. Some practitioners utilize decimals (x.25, x.5, x.75) to indicate gradations in the maturity model. As a further reference, COBIT provides a definition of the maturity designations by control objective. While this approach is not mandatory, the process is provided as a separate section at the end of the audit/assurance program for those enterprises that wish to implement it. It is suggested that a maturity assessment be made at the COBIT control level. To provide further value to the client/customer, the professional can also obtain maturity targets from the client/customer. Using the assessed and target maturity levels, the professional can create an effective graphic presentation that describes the achievement or gaps between the actual and targeted maturity goals.

IV. Assurance and Control Framework

ISACA IT Assurance Framework and Standards

ISACA has long recognized the specialized nature of IT assurance and strives to advance globally applicable standards. Guidelines and procedures provide detailed guidance on how to follow those standards. IT Audit and Assurance Standard S15 IT Controls, and IT Audit and Assurance Guideline G38 Access Controls are relevant to this audit/assurance program.

ISACA Controls Framework

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap among control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises.

Utilizing COBIT as the control framework on which IT audit/assurance activities are based aligns IT audit/assurance with good practices as developed by the enterprise.

Refer to ISACA's *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, published in 2007, for the related control practice value and risk drivers.

V. Executive Summary of Audit/Assurance Focus

SAP ERP Security

The review of SAP helps management ensure that it is secure. Since launching its first product offering almost 30 years ago, SAP has grown globally. It has approximately 12 million users and 96,400 installations in more than 120 countries and is the third-largest independent software company in the world. The company name, SAP, is a German acronym that loosely translates in English to Systems, Applications and Products in data processing.

Before SAP ERP, SAP had two main products: the mainframe system SAP® R/2® and the client/server-based system SAP R/3. Both R/2 and R/3 are targeted to business application solutions and feature complexity, business and organizational experience, and integration. The R/2 and R/3 terminology is sometimes taken to mean release 2 and release 3 respectively; however, this is not the case. The R in R/2 and R/3 means "real time." Release levels are annotated separately to the R/2 or R/3 descriptors. For example, in SAP R/3 4.6B, the 4 is the major release number, the 6 is the minor release number following a major release, and the B is the version within a release.

R/3 was introduced in 1992 with a three-tier architecture paradigm. In recent years, SAP has introduced Service Oriented Architecture (SOA) as part of SAP ERP. This combines ERP with an open technology platform that can integrate SAP and non-SAP systems on the SAP NetWeaver® platform. The current core ERP solution offered by SAP is called SAP Enterprise Central Component (ECC 6.0), referred here as SAP ERP.

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.

Risks 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

Objective and Scope

Objective—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.

Scope—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 risks introduced to the enterprise by these components and modules.

Minimum Audit Skills

This review is considered highly technical. The IT 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.

VI. Revenue Business Cycle Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
A. PRIOR AUDIT/EXAMINATION REPORT FOLLOW-UP									
1. Review prior report, if one exists, verify completion of any agreed-upon corrections and note remaining deficiencies.	ME1								
1.1 Determine whether: • 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 achievement of the defined information systems objectives and 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	ME1								

Audit/Assurance Program Step	CobiT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
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 organization 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 configuration									
B. PRELIMINARY AUDIT STEPS									
1. Gain an understanding of the SAP ERP environment.									
1.1 The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles. In particular, the following information is important: • 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	PO2 PO3 PO4 PO6 PO9 DS2								

Audit/Assurance Program Step	CobiT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
• 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 risks • Copies of the organization's key security policies and standards	DS5 AI2 AI6 ME1 ME2								
1.2 Obtain details of the following: • Organizational Management Model as it relates to sales/revenue activity, i.e., sales organization unit structure in SAP ERP and company sales organization 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	AI1 DS5 DS6								
2. Identify the significant risks and determine the key controls.									
2.1 Develop a high-level process flow diagram and overall understanding of the Revenue processing cycle, including the following subprocesses: • Maintain pricing/customer master data • Sales order processing • Invoice processing • Payment receipt	PO9 AI1 DS13								
2.2 Assess the key risks, determine key controls or control weaknesses, and test controls (refer sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: • The controls culture of the organization (e.g., a just-enough control philosophy) • 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.)	PO9 DS5 DS9 ME2								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
C. DETAILED AUDIT STEPS									
1. Maintain customer/pricing master data.									
1.1 Changes made to master data are valid, complete, accurate and timely.									
1.1.1 Determine whether the following reports of changes to master data have been compared to authorized source documents and/or a manual log of requested changes to ensure they were input accurately and on a timely basis: • For customer master data, use transaction code OV51 (also accessible using 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. • Use transaction code S_ALR_87009993 (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. • Use transaction MM04 to display master data changes for individual materials. • Generate a list of pricing changes using transaction VK12 and subsequently selecting the following path from menu options: Environment > Changes > Change Report. Check the accuracy of changes made to the pricing master records and also the time at which these changes have been applied (which is essential to the effective processing of pricing changes) against authorized source documentation.	AI2 AI6 DS6 DS11			X					
1.1.2 Review organization policy and process design specifications regarding access to maintain master data. Test user access to create and maintain customer, material and pricing master data as follows: • Customer master data—Transaction codes FD01/FD02/FD05/FD06 (Finance), VD01/VD02/VD05/VD06 (Sales),	AI2 AI6 DS5 DS11			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
XD01/XD02/XD05/XD06/XD07/XD99 (Central) • Material master data—Transaction codes MM01 (Create), MM02 (Change), MM06 (Delete) • Pricing master data—Transaction codes VK11 and VK12									
1.1.3 Determine whether the configurable control settings address the risks pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management intentions. View the settings online using the IMG as follows: • Customer Account Groups: Transaction SPRO Menu Path—Financial Accounting > Accounts Receivable & Accounts Payable > Customer Accounts > Master Data> Preparation for Creating Customer Master Data > Define Account Group With Screen Layout (Customers) • Material Types: Transaction SPRO Menu Path—Logistics General > Material Master > Basic Settings > Material Types > Define Attributes of Material Types • Industry Sector: Transaction SPRO Path—Logistics General > Material Master > Field Selection > Define industry sectors and industry-sector specific field selection • Understand the organization's pricing policy and its configuration in SAP ERP (e.g., hard-coded, manual override possible, user enters price). Pricing condition types and records can be reviewed against the organization's pricing policy using the following menu path and transaction codes • Transaction SPRO Menu Path—Sales and Distribution > Basic Functions > Pricing: – V-44 for material price condition record – V-48 for price list type condition records – V-52 for customer-specific condition type	PO9 DS9 DS11 DS12			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1.2 Master data remain current and pertinent.									
1.2.1 Determine whether management runs the following reports, or equivalent, by master data type and confirm evidence of management's review of the data for currency and ongoing pertinence: • Customer master data—Run transaction code F.20 • Material master data—Run transaction code MMS3 • Pricing master data—Run transaction code VK13 Transaction F.32 provides an overview of customers for which no credit limit has been entered. Check the output from transaction F.32 to confirm a credit limit has been set for customers in the range requiring a limit.	PO8 DS3 DS11 ME1			X					
2. Sales Order Purchasing									
2.1. Sales orders are processed with valid prices and terms and processing is complete, accurate and timely.									
2.1.1. Determine whether the ability to create, change or delete sales orders, contracts, and delivery schedules is restricted to authorized personnel by testing access to the following transactions: • Create (VA01)/Change (VA02) Sales Order • Create (VA31)/Change (VA32) Delivery Schedules • Create (VA41)/Change (VA42) Contracts									
2.1.2. Refer to master data integrity point 1.1.2.									
2.1.3. Refer to master data integrity point 1.1.3.									
2.1.4. Understand the policies and procedures regarding reconciliation of sales orders. Review operations activity at selected times and check for evidence that reconciliations are being performed.									
2.2. Orders are processed within approved customer credit limits.									
2.2.1. Determine whether the configurable control settings address the risks 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									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
as follows: • Transaction SPRO Menu Path—Financial Accounting > Accounts Receivable & Accounts Payable > Credit Management > Credit Control Account • Execute transaction OVAK to show the type of credit check performed for the corresponding transaction types in order processing. • Execute transaction OVA7 to determine whether a credit check is performed for appropriate document types being used. • Execute transaction OVAD to show the credit groups that have been assigned to the delivery types being used. • Execute transaction OVA8 to show an overview of defined credit checks for credit control areas.									
2.3. Order entry data are 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 V.00 (also accessible using transaction code SA38 and program RVAUFERR). Review items on the list with the appropriate operational management, and ascertain if there are legitimate reasons for the sales documents that remain incomplete.									
3. Invoice Processing									
3.1. 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 VTLA— Display Copying Control: Sales Document to Delivery Document. Select each combination of delivery type and sales document type, and click the Item button. Double-click on each item category, and verify that the entry for the indicator qty/value pos./neg. 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									

Audit/Assurance Program Step	CobiT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
and sales input for accuracy.									
3.1.2. Determine whether the following shipping reports are used to assist in controlling the shipping process: • Backlog—V.15 • Process Delivery Due List—VL04 • Outbound Deliveries for Picking—VL06 • Outbound Deliveries for Confirmation —VL06C • Outbound Deliveries to be Loaded —VL06L									
3.2. Invoices are generated using authorized terms and prices and are accurately calculated and recorded.									
3.2.1. Display current system settings relating to invoice preparation online using the IMG: Transaction SPRO Menu Path—Sales and Distribution > Billing > 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.									
3.3. All goods shipped are invoiced, in a timely manner.									
3.3.1. Execute transaction VF04—Process Billing Due List. All goods/services 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 in 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.									
3.3.2. Assess user access to picking lists, delivery notes and goods issues by testing access to the following transactions: • Create Single Delivery—VL01 • Process Delivery Due List—VL04 • Change Outbound Deliveries—VL02									
3.3.3. Execute transaction VF03 Display Invoice and click on the expansion button next to the billing document field and select Billing Documents Still to Be Passed Onto Accounting. Obtain									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
explanation for any invoices that appear in this list. Test user access to transactions to enter invoices and confirm this is consistent with staff job roles and management's intentions. • Sales Accounts Receivable Entry—VF01 and VF04 • Finance Entry—FB70									
3.4. Credit notes and adjustments to accounts receivable are accurately calculated and recorded.									
3.4.1. Assess user access to sales order return and credit notes transactions as follows: • Sales entry: Create Sales Document—VA01 • Sales entry: Change Sales Document—VA02 • Finance Entry—FB75									
3.5. Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy and in a timely manner.									
3.5.1. View the sales document types configured by using transaction VOV8. Look for the entire sales document types that relate to sales order returns and credit requests. Double-click on one of these document types. In the General Control section of the screen, there is a reference mandatory field. Verify that the setting has been set to M. Repeat this for all of the other relevant document types. Discuss the reference field settings in place for the selected document types with management. Determine whether the configuration in place is set as management intended.									
3.5.2. Review the configuration settings for delivery and billing blocks online using the IMG as follows: • Shipping: Transaction SPRO Menu Path—Logistics Execution >Shipping > Deliveries > Define Reasons for Blocking in Shipping • Billing: Transaction SPRO Manu Path—Sales and Distribution > Billing > Billing Documents > Define Blocking > Reason for Billing									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
Determine whether the settings support the processing of credits in line with the organization's credit management policy and are consistent with management's intention.									
4. Payment Receipt									
4.1. 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.									
4.1.2. Determine whether the system has been configured to not allow processing of cash receipts outside of approved bank accounts. Execute transaction FI12 and ascertain to which bank accounts a cash receipt can be posted. Determine if this is consistent with management's intentions.									
4.1.3. Use the 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.									
4.2. Cash receipts are valid and are not duplicated.									
4.2.1. Review the accounts receivable reconciliation and determine whether there are any amounts unallocated or any reconciling items. Determine the aging of these items and make inquiry of management as to the reasons for these items remaining unallocated or unreconciled.									
4.3. 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 the following transactions: • OBA4, to determine the tolerance groups that have been set up for users and the tolerance limits that have been set for those groups • OB57, to determine the users who have been allocated to the									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
groups identified earlier Discuss with management the settings that are in place for tolerance levels for allowable cash discounts and cash payment differences. Determine whether the configuration in place agrees with management's intentions.									
4.4. Timely collection of cash receipts is monitored.									
4.3.1. As for 4.1.3, determine whether accounts receivable aging reports are reviewed regularly to ensure that the collection of payments is being performed in a timely manner.									

VII. Maturity Assessment

The maturity assessment is an opportunity for the reviewer to assess the maturity of the processes reviewed. Based on the results of audit/assurance review, and the reviewer's observations, assign a maturity level to each of the following COBIT control practices.

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
AI6.1 Change Standards and Procedures 1. Develop, document and promulgate a change management framework that specifies the policies and processes, including: • Roles and responsibilities • Classification and prioritization of all changes based on business risk • Assessment of impact • Authorization and approval of all changes by the business process owners and IT • Tracking and status of changes • Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention) 2. Establish and maintain version control over all changes. 3. Implement roles and responsibilities that involve business process owners and appropriate technical IT functions. Ensure appropriate segregation of duties. 4. Establish appropriate record management practices and audit trails to record key steps in the change management process. Ensure timely closure of changes. Elevate and report to management changes that are not closed in a timely fashion. 5. Consider the impact of contracted services providers (e.g., of infrastructure, application development and shared services) on the change management process. Consider integration of organizational change management processes with change management processes of service providers. Consider the impact of the organizational change management process on contractual terms and SLAs.				
AI6.2 Impact Assessment, Prioritization and Authorization 1. Develop a process to allow business process owners and IT to request changes to infrastructure, systems or applications. Develop controls to ensure that all such changes arise only through the change request management process. 2. Categorize all requested changes (e.g., infrastructure, operating systems, networks, application systems, purchased/packaged application software). 3. Prioritize all requested changes. Ensure that the change management process identifies both the business and technical needs for the change. Consider legal, regulatory and contractual reasons for the requested change. 4. Assess all requests in a structured fashion. Ensure that the assessment process addresses impact analysis on infrastructure, systems and applications. Consider security, legal, contractual and compliance implications of the requested change. Consider also interdependencies amongst changes. Involve business process owners in the assessment process, as appropriate. 5. Ensure that each change is formally approved by business process owners and IT technical stakeholders, as appropriate.				

COBiT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
AI6.4 Change Status Tracking and Reporting 1. Ensure that a documented process exists within the overall change management process to declare, assess, authorize and record an emergency change. 2. Ensure that emergency changes are processed in accordance with the emergency change element of the formal change management process. 3. Ensure that all emergency access arrangements for changes are appropriately authorized, documented and revoked after the change has been applied. 4. Conduct a postimplementation review of all emergency changes, involving all concerned parties. The review should consider implications for aspects such as further application system maintenance, impact on development and test environments, application software development quality, documentation and manuals, and data integrity.				
DS5.3 Identity Management 1. Establish and communicate policies and procedures to uniquely identify, authenticate and authorize access mechanisms and access rights for all users on a need-to-know/need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved. 2. Ensure that roles and access authorization criteria for assigning user access rights take into account: • Sensitivity of information and applications involved (data classification) • Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements) • Roles and responsibilities as defined within the enterprise • The need-to-have access rights associated with the function • Standard but individual user access profiles for common job roles in the organization • Requirements to guarantee appropriate segregation of duties 3. Establish a method for authenticating and authorizing users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements. 4. Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person. 5. Ensure that a timely information flow is in place that reports changes in jobs (i.e., people in, people out, people change). Grant, revoke and adapt user access rights in co-ordination with human resources and user departments for users who are new, who have left the organization, or who have changed roles or jobs.				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS5.4 User Account Management 1. Ensure that access control procedures include but are not limited to: • Using unique user IDs to enable users to be linked to and held accountable for their actions • Awareness that the use of group IDs results in the loss of individual accountability and are permitted only when justified for business or operational reasons and compensated by mitigating controls. Group IDs must be approved and documented. • Checking that the user has authorization from the system owner for the use of the information system or service, and the level of access granted is appropriate to the business purpose and consistent with the organizational security policy • A procedure to require users to understand and acknowledge their access rights and the conditions of such access • Ensuring that internal and external service providers do not provide access until authorization procedures have been completed • Maintaining a formal record, including access levels, of all persons registered to use the service • A timely and regular review of user IDs and access rights 2. Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorizations for special privileged access rights should be reviewed independently at more frequent intervals.				
DS9.1 Configuration Repository and Baseline 1. Implement a configuration repository to capture and maintain configuration management items. The repository should include hardware; application software; middleware; parameters; documentation; procedures; and tools for operating, accessing and using the systems, services, version numbers and licensing details. 2. Implement a tool to enable the effective logging of configuration management information within a repository. 3. Provide a unique identifier to a configuration item so the item can be easily tracked and related to physical asset tags and financial records. 4. Define and document configuration baselines for components across development, test and production environments, to enable identification of system configuration at specific points in time (past, present and planned). 5. Establish a process to revert to the baseline configuration in the event of problems, if determined appropriate after initial investigation. 6. Install mechanisms to monitor changes against the defined repository and baseline. Provide management reports for exceptions, reconciliation and decision making.				
DS9.2 Identification and Maintenance of Configuration Items 1. Define and implement a policy requiring all configuration items and their attributes and versions to be identified and maintained. 2. Tag physical assets according to a defined policy. Consider using an automated mechanism, such as barcodes.				

COBiT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
3. Define a policy that integrates incident, change and problem management procedures with the maintenance of the configuration repository. 4. Define a process to record new, modified and deleted configuration items and their relative attributes and versions. Identify and maintain the relationships between configuration items in the configuration repository. 5. Establish a process to maintain an audit trail for all changes to configuration items. 6. Define a process to identify critical configuration items in relationship to business functions (component failure impact analysis). 7. Record all assets—including new hardware and software, procured or internally developed—within the configuration management data repository. 8. Define and implement a process to ensure that valid licenses are in place to prevent the inclusion of unauthorized software.				
DS9.3 Configuration Integrity Review 1. To validate the integrity of configuration data, implement a process to ensure that configuration items are monitored. Compare recorded data against actual physical existence, and ensure that errors and deviations are reported and corrected. 2. Using automated discovery tools where appropriate, reconcile actual installed software and hardware periodically against the configuration database, license records and physical tags. 3. Periodically review against the policy for software usage the existence of any software in violation or in excess of current policies and license agreements. Report deviations for correction.				

Expenditure Business Cycle

I. Introduction

Overview
ISACA developed *ITAF™: A Professional Practices Framework for IT Assurance* as a comprehensive and good-practice-setting model. ITAF provides standards that are designed to be mandatory, and are the guiding principles under which the IT audit and assurance profession operates. The guidelines provide information and direction for the practice of IT audit and assurance. The tools and techniques provide methodologies, and tools and templates to provide direction in the application of IT audit and assurance processes.

Purpose
The audit/assurance program is a tool and template to be used as a roadmap for the completion of a specific assurance process. This audit/assurance program is intended to be utilized by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF, section 2200—General Standards. The audit/assurance programs are part of ITAF, section 4000—IT Assurance Tools and Techniques.

Control Framework
The audit/assurance programs have been developed in alignment with the COBIT framework—specifically COBIT 4.1—using generally applicable and accepted good practices. They reflect ITAF, sections 3400—IT Management Processes, 3600—IT Audit and Assurance Processes, and 3800—IT Audit and Assurance Management.

Many enterprises have embraced several frameworks at an enterprise level, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework. The importance of the control framework has been enhanced due to regulatory requirements by the US Securities and Exchange Commission (SEC) as directed by the US Sarbanes-Oxley Act of 2002 and similar legislation in other countries. They seek to integrate control framework elements used by the general audit/assurance team into the IT audit and assurance framework. Since COSO is widely used, it has been selected for inclusion in this audit/assurance program. The reviewer may delete or rename columns in the audit program to align with the enterprise's control framework.

IT Governance, Risk and Control
IT governance, risk and control are critical in the performance of any assurance management process. Governance of the process under review will be 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 will be evaluated as steps in the audit/assurance program. Controls are the primary evaluation point in the process. The audit/assurance program will identify the control objectives with steps to determine control design and effectiveness.

Responsibilities of IT Audit and Assurance Professionals
IT audit and assurance professionals are expected to customize this document to the environment

in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it is not intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional holds the Certified Information Systems Auditor (CISA) designation, or has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the CISA designation and necessary subject matter expertise to adequately review the work performed.

II. Using This Document

This audit/assurance program was developed to assist the audit and assurance professional in designing and executing a review. Details regarding the format and use of the document follow.

Work Program Steps

The first column of the program describes the steps to be performed. The numbering scheme used provides built-in work paper numbering for ease of cross-reference to the specific work paper for that section. IT audit and assurance professionals are encouraged to make modifications to this document to reflect the specific environment under review.

COBIT Cross-reference

The COBIT cross-reference provides the audit and assurance professional with the ability to refer to the specific COBIT control objective that supports the audit/assurance step. The COBIT control objective should be identified for each audit/assurance step in the section. Multiple cross-references are not uncommon. Processes at lower levels in the work program are too granular to be cross-referenced to COBIT. The audit/assurance program is organized in a manner to facilitate an evaluation through a structure parallel to the development process. COBIT provides in-depth control objectives and suggested control practices at each level. As the professional reviews each control, he/she should refer to COBIT 4.1 or the *IT Assurance Guide: Using COBIT* for good-practice control guidance.

COSO Components

As noted in the introduction, COSO and similar frameworks have become increasingly popular among audit and assurance professionals. This ties the assurance work to the enterprise's control framework. While the IT audit/assurance function has COBIT as a framework, operational audit and assurance professionals use the framework established by the enterprise. Since COSO is the most prevalent internal control framework, it has been included in this document and is a bridge to align IT audit/assurance with the rest of the audit/assurance function. Many audit/assurance organizations include the COSO control components within their report and summarize assurance activities to the audit committee of the board of directors.

For each control, the audit and assurance professional should indicate the COSO component(s) addressed. It is possible, but generally not necessary, to extend this analysis to the specific audit step level.

The original COSO internal control framework contained five components. In 2004, COSO was revised as the *Enterprise Risk Management (ERM) Integrated Framework* and extended to eight

components. The primary difference between the two frameworks is the additional focus on ERM and integration into the business decision model. ERM is in the process of being adopted by large enterprises. The two frameworks are compared in **figure AD1**.

Figure AD1—Comparison of COSO Internal Control and ERM Integrated Frameworks	
Internal Control Framework	**ERM Integrated Framework**
Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.	**Internal Environment**: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an enterprise's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
	Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the enterprise's mission and are consistent with its risk appetite.
	Event Identification: Internal and external events affecting achievement of an enterprise's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
Risk Assessment: Every enterprise faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, and thus risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.	**Risk Assessment**: Risks are analyzed, considering the likelihood and impact, as a basis for determining how they could be managed. Risk areas are assessed on an inherent and residual basis.
	Risk Response: Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the enterprise's risk tolerances and risk appetite.
Control Activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the enterprise's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.	**Control Activities:** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders.	**Information and Communication:** Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the enterprise.
Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.	**Monitoring:** The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Information for **figure AD1** was obtained from the COSO web site *www.coso.org/aboutus.htm.*

The original COSO internal control framework addresses the needs of the IT audit and assurance professional: control environment, risk assessment, control activities, information and communication, and monitoring. As such, ISACA has elected to utilize the five-component model for these audit/assurance programs. As more enterprises implement the ERM model, the additional three columns can be added, if relevant. When completing the COSO component

columns, consider the definitions of the components as described in **figure AD1**.

Reference/Hyperlink
Good practices require the audit and assurance professional to create a work paper for each line item, which describes the work performed, issues identified and conclusions. The reference/hyperlink is to be used to cross-reference the audit/assurance step to the work paper that supports it. The numbering system of this document provides a ready numbering scheme for the work papers. If desired, a link to the work paper can be pasted into this column.

Issue Cross-reference
This column can be used to flag a finding/issue that the IT audit and 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).

Comments
The comments column can be used to indicate the waiving of a step or other notations. It is not to be used in place of a work paper describing the work performed.

III. Controls Maturity Analysis

One of the consistent requests of stakeholders who have undergone IT audit/assurance reviews is a desire to understand how their performance compares to good practices. Audit and assurance professionals must provide an objective basis for the review conclusions. Maturity modeling for management and control over IT processes is based on a method of evaluating the organization, so it can be rated from a maturity level of nonexistent (0) to optimized (5). This approach is derived from the maturity model that the Software Engineering Institute (SEI) of Carnegie Mellon University defined for the maturity of software development.

The *IT Assurance Guide: Using COBIT*, appendix VII—Maturity Model for Internal Control, in **figure AD2**, provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimized level. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

Figure AD2—Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Nonexistent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT

Figure AD2—Maturity Model for Internal Control		
Maturity Level	**Status of the Internal Control Environment**	**Establishment of Internal Controls**
	impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized occasionally.
5 Optimized	An enterprisewide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

The maturity model evaluation is one of the final steps in the evaluation process. The IT audit and assurance professional can address the key controls within the scope of the work program and formulate an objective assessment of the maturity levels of the control practices. The maturity assessment can be a part of the audit/assurance report, and used as a metric from year to year to document progression in the enhancement of controls. However, it must be noted that the perception of the maturity level may vary between the process/IT asset owner and the auditor. Therefore, an auditor should obtain the concerned stakeholders' concurrence before submitting the final report to management.

At the conclusion of the review, once all findings and recommendations are completed, the professional assesses the current state of the COBIT control framework and assigns it a maturity level using the six-level scale. Some practitioners utilize decimals (x.25, x.5, x.75) to indicate gradations in the maturity model. As a further reference, COBIT provides a definition of the maturity designations by control objective. While this approach is not mandatory, the process is provided as a separate section at the end of the audit/assurance program for those enterprises that wish to implement it. It is suggested that a maturity assessment be made at the COBIT control level. To provide further value to the client/customer, the professional can also obtain maturity targets from the client/customer. Using the assessed and target maturity levels, the professional can create an effective graphic presentation that describes the achievement or gaps between the actual and targeted maturity goals.

IV. Assurance and Control Framework

ISACA IT Assurance Framework and Standards

ISACA has long recognized the specialized nature of IT assurance and strives to advance globally applicable standards. Guidelines and procedures provide detailed guidance on how to follow those standards. IT Audit/Assurance Standard S15 IT Controls, and IT Audit/Assurance Guideline G38 Access Controls are relevant to this audit/assurance program.

ISACA Controls Framework

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap among control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises.

Utilizing COBIT as the control framework on which IT audit/assurance activities are based aligns IT audit/assurance with good practices as developed by the enterprise.

Refer to ISACA's *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, published in 2007, for the related control practice value and risk drivers.

V. Executive Summary of Audit/Assurance Focus

SAP ERP Security

The review of SAP helps management ensure that it is secure. Since launching its first product offering almost 30 years ago, SAP has grown globally. It has approximately 12 million users and 96,400 installations in more than 120 countries and is the third-largest independent software company in the world. The company name, SAP, is a German acronym that loosely translates in English to Systems, Applications and Products in data processing.

Before SAP ERP, SAP had two main products: the mainframe system SAP® R/2® and the client/server-based system SAP R/3. Both R/2 and R/3 are targeted to business application solutions and feature complexity, business and organizational experience, and integration. The R/2 and R/3 terminology is sometimes taken to mean release 2 and release 3 respectively; however, this is not the case. The R in R/2 and R/3 means "real time." Release levels are annotated separately to the R/2 or R/3 descriptors. For example, in SAP R/3 4.6B, the 4 is the major release number, the 6 is the minor release number following a major release, and the B is the version within a release.

R/3 was introduced in 1992 with a three-tier architecture paradigm. In recent years, SAP has introduced Service Oriented Architecture (SOA) as part of SAP ERP. This combines ERP with an open technology platform that can integrate SAP and non-SAP systems on the SAP NetWeaver® platform. The current core ERP solution offered by SAP is called SAP Enterprise Central Component (ECC 6.0), referred here as SAP ERP.

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.

Risks 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

Objective and Scope

Objective—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.

Scope—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 risks introduced to the enterprise by these components and modules.

Minimum Audit Skills

This review is considered highly technical. The IT 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.

VI. Expenditure Business Cycle Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
A. PRIOR AUDIT/EXAMINATION REPORT FOLLOW-UP									
1.1 Review prior report, if one exists, verify completion of any agreed-upon corrections and note remaining deficiencies.	ME1								
1.2 Determine whether: • 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 achievement of the defined information systems objectives and 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	ME1								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
• 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 organization 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 configuration									
B. PRELIMINARY AUDIT STEPS									
1. Gain an understanding of the SAP ERP environment.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1.1 The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles. In particular, the following information is important: • 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 risks • Copies of the organization's key security policies and standards	PO2 PO3 PO4 PO6 PO9 DS2 DS5 AI2 AI6 ME2								
1.2 Obtain details of the following: • The Organizational Management Model as it relates to expenditure activity, i.e., purchasing organization unit structure in SAP ERP and purchasing/accounts payable organization chart (required when evaluating the results of access security control testing) • An interview of the systems implementation team, if possible, and the process design documentation for materials management	AI1 DS5 DS6								
2. Identify the significant risks and determine the key controls.									
2.1 Develop a high-level process flow diagram and overall understanding of the Expenditure processing cycle, including the following subprocesses: • Master data maintenance • Purchasing • Invoice processing • Processing disbursements	PO9 AI1 DS11								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.2 Assess the key risks, determine key controls or control weaknesses, and test controls (refer to sample testing program below and chapter IV for techniques for testing configurable controls and logical access security) regarding the following factors: • The controls culture of the organization (e.g., a just-enough control philosophy) • 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.)	PO9 DS5 DS9 ME2								
C. DETAILED AUDIT STEPS									
1. Master Data Maintenance									
1.1 Changes made to master data are valid, complete, accurate and timely.									
1.1.1 Determine whether the changes made to the master data are complete, accurate and timely. Using the specified transaction code or SA38, determine whether the following report of changes to master data are 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: • For vendor master data, use transaction code S_ALR_87010039 (also accessible through transaction code SA38 and program RFKABL00) to produce a list of master data changes.	AI6 DS11			X					
1.1.2 Determine whether access to create and change vendor pricing master data is restricted to a dedicated area and to authorized individuals. Review organization policy and process design specifications regarding access to maintain master data. Test user access by using transaction code SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002; refer to chapter 4 on how to test user access) to create and maintain									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
vendor master data as follows: • Finance entry—Transaction codes FK01 (Create), FK02 (Change), FK05 (Block/Unblock), FK06 (Delete) • Purchasing entry—Transaction codes MK01 (Create), MK02 (Change), MK05 (Block/Unblock), MK06 (Delete) • Centralized entry—Transaction codes XK01 (Create), XK02 (Change), XK05 (Block/Unblock), XK06 (Delete) Test user access to transactions to maintain vendor pricing information: • Create info record—ME11 • Change info record—ME12 • Delete info record—ME15 • Create condition—MEK1 • Change condition—MEK2 • Create condition with reference—MEK4									
1.1.3 Determine whether the configurable control settings address the risks pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management intentions. View the settings online using transaction code OBD3 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.	DS9 DS11 DS12			X					
1.1.4 Determine whether a naming convention should be used for vendor names (e.g., as per letterhead) to minimize the risk of establishing duplicated vendor master records. Extract a list of vendor account names from table LFA1 (fields: NAME 1 = name, LIFNR = vendor number). Review a sample for compliance with the organization's naming convention. View or search the list (using scan search software tools, if available) for potential duplicates.	PO9 DS11			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1.2 Inventory master data remain current and pertinent.									
1.2.1 Determine whether management periodically reviews master data to check their currency and ongoing pertinence, and whether the appropriate management displays or produces a list of vendors using report RFKKVZ00 or equivalent. Confirm evidence of management's review of the data on a rotating basis for currency and ongoing pertinence.	DS11 ME1			X					
2. Purchasing									
2.1 Purchase order entry and changes are valid, complete, accurate and timely.									
2.1.1 Determine whether purchase orders are handled with a valid process and terms and if processing is complete, accurate and timely. Determine whether the ability to create, change, or cancel purchase requisitions, purchase orders, and outline agreements (standing purchase orders) is restricted to authorized personnel by testing access to the following transactions: • Create Purchase Requisition—ME51/ME51N • Change Purchase Requisition—ME52/ME52N • Release Purchase Requisition—ME54/ME54N • Collective Release of Purchase Requisition—ME55 • Create Purchase Order, Vendor Known—ME21/ME21N • Change Purchase Order—ME22/ME22N	DS5 DS11			X					
2.1.2 Determine whether the SAP ERP source list functionality allows specified materials to be purchased only from vendors included in the source list for the specified material. Through discussions with management, determine (types of) materials for which source lists should be available in the system. Also, determine (types of) materials for which a source list should not be present. Examine a selection of materials and view the corresponding source list using the following reports to corroborate the performance of the control activity in the	DS11			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
appropriate accounting period: • ME06 reports on all material items and whether they belong to a source list or not. • ME0M shows all material items and any associated vendors (including historic data). To run ME0M, specify a material or a range of materials. Use the match code, click on the Search Help option and choose option J—material by material group—to get a list of materials. • Select the previously mentioned sample of orders and check against source list reports to determine if specific materials have been procured with unlisted vendors.									
2.1.3 Determine whether the SAP ERP release strategy is used to authorize purchase orders, outline agreements (standing purchase orders) and unusual purchases (e.g., capital outlays). Obtain sufficient understanding of the system configuration to assess the adequacy of the release strategy as defined and implemented by the organization, as well as the function and effectiveness of established policies, procedures, standards and guidance. Execute the following transactions to obtain an understanding of the way the system has been configured: • Release procedure: Purchase Orders—Transaction SPRO menu path: Materials Management > Purchasing > Purchase Order > Release Procedure for Purchase Orders > Define Release Procedure for Purchase Orders • Requisitions (with classification)—Transaction SPRO menu path: Material Management > Purchasing > Purchase Requisitions > Release Procedure > Procedure with Classification > Set Up Procedure with Classification – Click on Release Strategy. Select the strategies one by one, by double-clicking on the strategy. Note the release codes that are shown and check authorization (authorization objects M_BANF_FRG and M_EINK_FRG) for these release codes.	DS5 DS9 DS13 ME1			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
– Click on Classification. This will show the conditions under which the purchase document will be blocked. Ascertain if these conditions comply with management's intentions. • Release procedure Purchase Requisitions (without classification)—Transaction SPRO menu path: Material Management > Purchasing > Purchase Requisitions > Release Procedure > Set Up Procedure without Classification – Click on Release Prerequisites. Note the release codes that are shown and check authorization for these release codes. – Re-execute the above SPRO menu path and click on Determination of Release Strategy. This will show the conditions under which the purchase document will be blocked. Ascertain if these conditions comply with management's intentions. • Test user access to transactions for release strategies: – Release Purchase Order—ME28 – Release Outline Agreement—ME35 – Release Purchase Requisition—ME54 – Collective Release of Purchase Requisitions—ME55									
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 Determine whether goods (or materials or equipment) are received only when there are valid purchase orders, or if goods receipts are always recorded completely, accurately and in a timely manner. Determine whether an investigation takes place when receipts have no purchase order or exceed the purchase order quantity by more than an established amount. Does management review exception reports of goods not received on time for recorded purchases? Run transaction code VL10B (also accessible using transaction code SA38 and program RM06EM00) to produce a listing of purchase orders	DS5 DS9			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
outstanding. Ascertain from management if there are any reasons for any long-outstanding items on the report.									
2.2.2 Determine whether order entry data are transferred completely and accurately to the shipping and invoicing activities, and if the ability to input, change or cancel goods received transactions is restricted to authorized inbound logistics/raw materials personnel. Test user access to transactions for goods receipt as follows: • Goods Receipt for Purchase Order —MB01 • Goods Receipts, Purchase Order • Unknown—MB0A • Goods Receipt for Production Order —MB31 • Other Goods Receipts—MB1C • Cancel/Reverse Material Document —MBST Test user access to high-risk movement types transaction code MB1C, authorization object M_MSEG_BWA and fields ACTV and movement types BWART 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.	AI2 DS5 DS11			X					
2.3 Defective goods are returned to suppliers in a timely manner.									
2.3.1 Determine whether defective goods (or materials or equipment) are returned in a timely manner to suppliers, are adequately segregated from other goods in a quality assurance bonding area, and are regularly monitored (assigned a specific movement type, e.g., 122) to ensure timely return to suppliers, and whether credit is received in a timely manner. Ascertain from management the movement type used to block processing and for returning rejected goods to suppliers (e.g., movement type 122). Execute transaction MB51 with the appropriate movement type. Determine if there are any long-outstanding materials	DS2 DS11			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
pending return to suppliers or receipt of appropriate credits.									
3. Invoice Processing									
3.1 Amounts posted to accounts payable represent goods or services received.									
3.1.1 Determine whether amounts posted to accounts payable represent goods or services received; the ability to input, change, cancel or release vendor invoices for payment is restricted to authorized personnel; and the ability to input vendor invoices that do not have a purchase order and/or goods receipt is restricted to authorized personnel. Test user access to transactions for invoice processing: • Enter Invoice—MRHR, MIRO, MR01 • Change Invoice—FB02 • Process Blocked Invoice—MR02 • Cancel Invoice—MR08 • Enter Credit Memo—MRHG	AI6 DS6 DS9			X					
3.2 Accounts payable amounts are calculated completely and accurately and recorded in a timely manner.									
3.2.1 Determine whether the SAP ERP software is configured to perform a three-way match. Transaction SPRO menu path: Materials Management > Purchasing > Purchase Order > Define Screen Layout at Document Level (Change View field selection at document level: Overview) by selecting ME21—Create Purchase Order and then selecting 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, field name WEBRE, using transaction SE16. Where GR/IR Control has not been set, ascertain from management if there are any reasons.	DS5 DS9			X					
3.2.2 Determine whether the SAP ERP software is configured with quantity and price tolerance limits. Check tolerance limits for price variances									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
and message settings for invoice verification (online matching) as follows: • Variance settings: Execute transaction OMR6. The system will show an overview of the defined tolerance limits. Double-click on the entries that relate to the organization being audited. Check two entries: one for tolerance key PE (price) and one for tolerance key SE (discount). Note the values shown. Both a lower and upper limit may be specified as a percentage value. (PE also allows setting of an absolute value.) • Message settings: – Transaction SPRO menu path: Materials Management > Purchasing > Environment Data > Define Attributes of System Messages – Click on the Position button. Enter values 00, 06 and 207 (message for price variance) and press Enter. Note the value in the cat field. Possible values are W for warning and E for error. Ascertain whether the values noted comply with management intentions.	DS9 DS10			X					
3.2.3 Determine if GR/IR account balances using transaction code S_P6B_12000135 (also accessible using transaction code SA38 and program RM07MSAL) are executed and reviewed periodically. Check that there are appropriate procedures in place to investigate unmatched purchase orders. In particular, long-outstanding items should be followed up and cleared.	AI6			X					
3.2.4 Determine whether reports of outstanding purchase orders are reviewed regularly. Run the transaction code SA38 and program RM06EM00 to produce a listing of purchase orders outstanding and review long-outstanding items with management.	PO11			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3.2.5 Determine whether the SAP ERP software restricts the ability to modify the exchange rate table to authorized personnel, management approves values in the centrally maintained exchange rate table and the SAP ERP software automatically calculates foreign currency translations based on values in the centrally maintained exchange rate table. Determine whether management reviews a sample of changes to exchange rates above a certain percentage with regard to the volume and value of foreign currency transactions for the organization. Test user access to the exchange rates and the related authorization objects: • Exchange rate via standard transaction—First, execute transaction SUCU. Click on Position. Enter value V_TCURR and press Enter. Note the value in the authorization group field. Then test user access to transaction code OB08, authorization object: S_TABU_DIS (Class Basis: Administration), field activity: value 02 and field authorization group: value noted with transaction SUCU. • Exchange rate via view maintenance—First, execute transaction SUCU. Click on Position. Enter table name value V_T001R, click on Choose. Note the value in the authorization group field. Do the same for table V_TCURF. Then test user access to transaction codes as follows with authorization object: S_TABU_DIS (Class Basis: Administration), field activity: 02 and field authorization group: value noted with transaction SUCU: • Maintain Table Rounding Units—OB90 • Maintain Table Foreign Currency Ratios—OBBS • Table View Maintenance—SM30	AI6 DS5			X					
3.3 Credit notes and other adjustments are calculated completely and accurately and recorded in a timely manner.									
3.3.1 Determine whether the ability to input, change, cancel or release credit notes is restricted to authorized personnel. Test user access to post									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
invoices directly to vendor accounts: • Enter Credit Note—MRHG • Enter Invoice—MRHR, MIRO, MR01	PO2 DS5			X					
4. Processing Disbursements									
4.1 Disbursements are made only for goods and services received, and are calculated accurately, recorded and distributed to the appropriate suppliers in a timely manner.									
4.1.1 Determine whether disbursements are made only for goods and services received, and are calculated accurately, recorded and distributed to the appropriate suppliers in a timely manner. Determine whether management approves the SAP ERP payment run parameter specification. Test user access to transactions to process disbursements: • Automatic Payment Transactions—F110S • Parameters for Payment —F110 • Payment With Printout—F-58	DS5 PO6			X					
4.1.2 Test user access to blocked invoices : • Change Document—FB02 • Change Line Items—FB09 • Block/Unblock Vendor (Centrally)—XK05 • Block/Unblock Vendor—FK05									

VII. Maturity Assessment

The maturity assessment is an opportunity for the reviewer to assess the maturity of the processes reviewed. Based on the results of audit/assurance review, and the reviewer's observations, assign a maturity level to each of the following COBIT control practices.

COBIT Control Practice	**Assessed Maturity**	**Target Maturity**	**Reference Hyperlink**	**Comments**
AI6.1 Change Standards and Procedures 1. Develop, document and promulgate a change management framework that specifies the policies and processes, including: • Roles and responsibilities • Classification and prioritization of all changes based on business risk • Assessment of impact • Authorization and approval of all changes by the business process owners and IT • Tracking and status of changes • Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention) 2. Establish and maintain version control over all changes. 3. Implement roles and responsibilities that involve business process owners and appropriate technical IT functions. Ensure appropriate segregation of duties. 4. Establish appropriate record management practices and audit trails to record key steps in the change management process. Ensure timely closure of changes. Elevate and report to management changes that are not closed in a timely fashion. 5. Consider the impact of contracted services providers (e.g., of infrastructure, application development and shared services) on the change management process. Consider integration of organizational change management processes with change management processes of service providers. Consider the impact of the organizational change management process on contractual terms and SLAs.				
AI6.2 Impact Assessment, Prioritization and Authorization 1. Develop a process to allow business process owners and IT to request changes to infrastructure, systems or applications. Develop controls to ensure that all such changes arise only through the change request management process. 2. Categorize all requested changes (e.g., infrastructure, operating systems, networks, application systems, purchased/packaged application software). 3. Prioritize all requested changes. Ensure that the change management process identifies both the business and technical needs for the change. Consider legal, regulatory and contractual reasons for the requested change. 4. Assess all requests in a structured fashion. Ensure that the assessment process addresses impact analysis on infrastructure, systems and applications. Consider security, legal, contractual and compliance implications of the requested change. Consider also interdependencies among changes. Involve business process owners in the assessment process, as appropriate. 5. Ensure that each change is formally approved by business process owners and IT technical stakeholders, as appropriate.				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
AI6.4 Change Status Tracking and Reporting 1. Ensure that a documented process exists within the overall change management process to declare, assess, authorize and record an emergency change. 2. Ensure that emergency changes are processed in accordance with the emergency change element of the formal change management process. 3. Ensure that all emergency access arrangements for changes are appropriately authorized, documented and revoked after the change has been applied. 4. Conduct a postimplementation review of all emergency changes, involving all concerned parties. The review should consider implications for aspects such as further application system maintenance, impact on development and test environments, application software development quality, documentation and manuals, and data integrity.				
DS5.3 Identity Management 1. Establish and communicate policies and procedures to uniquely identify, authenticate and authorize access mechanisms and access rights for all users on a need-to-know/need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved. 2. Ensure that roles and access authorization criteria for assigning user access rights take into account: • Sensitivity of information and applications involved (data classification) • Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements) • Roles and responsibilities as defined within the enterprise • The need-to-have access rights associated with the function • Standard but individual user access profiles for common job roles in the organization • Requirements to guarantee appropriate segregation of duties 3. Establish a method for authenticating and authorizing users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements. 4. Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person. 5. Ensure that a timely information flow is in place that reports changes in jobs (i.e., people in, people out, people change). Grant, revoke and adapt user access rights in co-ordination with human resources and user departments for users who are new, who have left the organization, or who have changed roles or jobs.				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS5.4 User Account Management 1. Ensure that access control procedures include but are not limited to: • Using unique user IDs to enable users to be linked to and held accountable for their actions • Awareness that the use of group IDs results in the loss of individual accountability and are permitted only when justified for business or operational reasons and compensated by mitigating controls. Group IDs must be approved and documented. • Checking that the user has authorization from the system owner for the use of the information system or service, and the level of access granted is appropriate to the business purpose and consistent with the organizational security policy • A procedure to require users to understand and acknowledge their access rights and the conditions of such access • Ensuring that internal and external service providers do not provide access until authorization procedures have been completed • Maintaining a formal record, including access levels, of all persons registered to use the service • A timely and regular review of user IDs and access rights 2. Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorizations for special privileged access rights should be reviewed independently at more frequent intervals.				
DS9.1 Configuration Repository and Baseline 1. Implement a configuration repository to capture and maintain configuration management items. The repository should include hardware; application software; middleware; parameters; documentation; procedures; and tools for operating, accessing and using the systems, services, version numbers and licensing details. 2. Implement a tool to enable the effective logging of configuration management information within a repository. 3. Provide a unique identifier to a configuration item so the item can be easily tracked and related to physical asset tags and financial records. 4. Define and document configuration baselines for components across development, test and production environments, to enable identification of system configuration at specific points in time (past, present and planned). 5. Establish a process to revert to the baseline configuration in the event of problems, if determined appropriate after initial investigation. 6. Install mechanisms to monitor changes against the defined repository and baseline. Provide management reports for exceptions, reconciliation and decision making.				
DS9.2 Identification and Maintenance of Configuration Items 1. Define and implement a policy requiring all configuration items and their attributes and versions to be identified and maintained.				

COBIT Control Practice	**Assessed Maturity**	**Target Maturity**	**Reference Hyperlink**	**Comments**
2. Tag physical assets according to a defined policy. Consider using an automated mechanism, such as barcodes. 3. Define a policy that integrates incident, change and problem management procedures with the maintenance of the configuration repository. 4. Define a process to record new, modified and deleted configuration items and their relative attributes and versions. Identify and maintain the relationships between configuration items in the configuration repository. 5. Establish a process to maintain an audit trail for all changes to configuration items. 6. Define a process to identify critical configuration items in relationship to business functions (component failure impact analysis). 7. Record all assets—including new hardware and software, procured or internally developed—within the configuration management data repository. 8. Define and implement a process to ensure that valid licenses are in place to prevent the inclusion of unauthorized software.				
DS9.3 Configuration Integrity Review 1. To validate the integrity of configuration data, implement a process to ensure that configuration items are monitored. Compare recorded data against actual physical existence, and ensure that errors and deviations are reported and corrected. 2. Using automated discovery tools where appropriate, reconcile actual installed software and hardware periodically against the configuration database, license records and physical tags. 3. Periodically review against the policy for software usage the existence of any software in violation or in excess of current policies and license agreements. Report deviations for correction.				

Inventory Business Cycle

I. Introduction

Overview
ISACA developed *ITAF™: A Professional Practices Framework for IT Assurance* as a comprehensive and good-practice-setting model. ITAF provides standards that are designed to be mandatory, and are the guiding principles under which the IT audit and assurance profession operates. The guidelines provide information and direction for the practice of IT audit and assurance. The tools and techniques provide methodologies, and tools and templates to provide direction in the application of IT audit and assurance processes.

Purpose
The audit/assurance program is a tool and template to be used as a roadmap for the completion of a specific assurance process. This audit/assurance program is intended to be utilized by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF, section 2200—General Standards. The audit/assurance programs are part of ITAF, section 4000—IT Assurance Tools and Techniques.

Control Framework
The audit/assurance programs have been developed in alignment with the COBIT framework—specifically COBIT 4.1—using generally applicable and accepted good practices. They reflect ITAF, sections 3400—IT Management Processes, 3600—IT Audit and Assurance Processes, and 3800—IT Audit and Assurance Management.

Many enterprises have embraced several frameworks at an enterprise level, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework. The importance of the control framework has been enhanced due to regulatory requirements by the US Securities and Exchange Commission (SEC) as directed by the US Sarbanes-Oxley Act of 2002 and similar legislation in other countries. They seek to integrate control framework elements used by the general audit/assurance team into the IT audit and assurance framework. Since COSO is widely used, it has been selected for inclusion in this audit/assurance program. The reviewer may delete or rename columns in the audit program to align with the enterprise's control framework.

IT Governance, Risk and Control
IT governance, risk and control are critical in the performance of any assurance management process. Governance of the process under review will be 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 will be evaluated as steps in the audit/assurance program. Controls are the primary evaluation point in the process. The audit/assurance program will identify the control objectives with steps to determine control design and effectiveness.

Responsibilities of IT Audit and Assurance Professionals
IT audit and assurance professionals are expected to customize this document to the environment

in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it is not intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional holds the Certified Information Systems Auditor (CISA) designation, or has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the CISA designation and necessary subject matter expertise to adequately review the work performed.

II. Using This Document

This audit/assurance program was developed to assist the audit and assurance professional in designing and executing a review. Details regarding the format and use of the document follow.

Work Program Steps

The first column of the program describes the steps to be performed. The numbering scheme used provides built-in work paper numbering for ease of cross-reference to the specific work paper for that section. IT audit and assurance professionals are encouraged to make modifications to this document to reflect the specific environment under review.

COBIT Cross-reference

The COBIT cross-reference provides the audit and assurance professional with the ability to refer to the specific COBIT control objective that supports the audit/assurance step. The COBIT control objective should be identified for each audit/assurance step in the section. Multiple cross-references are not uncommon. Processes at lower levels in the work program are too granular to be cross-referenced to COBIT. The audit/assurance program is organized in a manner to facilitate an evaluation through a structure parallel to the development process. COBIT provides in-depth control objectives and suggested control practices at each level. As the professional reviews each control, he/she should refer to COBIT 4.1 or the *IT Assurance Guide: Using COBIT* for good-practice control guidance.

COSO Components

As noted in the introduction, COSO and similar frameworks have become increasingly popular among audit and assurance professionals. This ties the assurance work to the enterprise's control framework. While the IT audit/assurance function has COBIT as a framework, operational audit and assurance professionals use the framework established by the enterprise. Since COSO is the most prevalent internal control framework, it has been included in this document and is a bridge to align IT audit/assurance with the rest of the audit/assurance function. Many audit/assurance organizations include the COSO control components within their report and summarize assurance activities to the audit committee of the board of directors.

For each control, the audit and assurance professional should indicate the COSO component(s) addressed. It is possible, but generally not necessary, to extend this analysis to the specific audit step level.

The original COSO internal control framework contained five components. In 2004, COSO was revised as the *Enterprise Risk Management (ERM) Integrated Framework* and extended to eight

components. The primary difference between the two frameworks is the additional focus on ERM and integration into the business decision model. ERM is in the process of being adopted by large enterprises. The two frameworks are compared in **figure AD1**.

Figure AD1—Comparison of COSO Internal Control and ERM Integrated Frameworks	
Internal Control Framework	**ERM Integrated Framework**
Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.	**Internal Environment**: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an enterprise's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
	Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the enterprise's mission and are consistent with its risk appetite.
	Event Identification: Internal and external events affecting achievement of an enterprise's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
Risk Assessment: Every enterprise faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, and thus risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.	**Risk Assessment**: Risks are analyzed, considering the likelihood and impact, as a basis for determining how they could be managed. Risk areas are assessed on an inherent and residual basis.
	Risk Response: Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the enterprise's risk tolerances and risk appetite.
Control Activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the enterprise's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.	**Control Activities:** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders.	**Information and Communication:** Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the enterprise.
Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.	**Monitoring:** The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Information for **figure AD1** was obtained from the COSO web site *www.coso.org/aboutus.htm.*

The original COSO internal control framework addresses the needs of the IT audit and assurance professional: control environment, risk assessment, control activities, information and communication, and monitoring. As such, ISACA has elected to utilize the five-component model for these audit/assurance programs. As more enterprises implement the ERM model, the additional three columns can be added, if relevant. When completing the COSO component

columns, consider the definitions of the components as described in **figure AD1**.

Reference/Hyperlink

Good practices require the audit and assurance professional to create a work paper for each line item, which describes the work performed, issues identified and conclusions. The reference/hyperlink is to be used to cross-reference the audit/assurance step to the work paper that supports it. The numbering system of this document provides a ready numbering scheme for the work papers. If desired, a link to the work paper can be pasted into this column.

Issue Cross-reference

This column can be used to flag a finding/issue that the IT audit and 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).

Comments

The comments column can be used to indicate the waiving of a step or other notations. It is not to be used in place of a work paper describing the work performed.

III. Controls Maturity Analysis

One of the consistent requests of stakeholders who have undergone IT audit/assurance reviews is a desire to understand how their performance compares to good practices. Audit and assurance professionals must provide an objective basis for the review conclusions. Maturity modeling for management and control over IT processes is based on a method of evaluating the organization, so it can be rated from a maturity level of nonexistent (0) to optimized (5). This approach is derived from the maturity model that the Software Engineering Institute (SEI) of Carnegie Mellon University defined for the maturity of software development.

The *IT Assurance Guide: Using COBIT*, appendix VII—Maturity Model for Internal Control, in **figure AD2**, provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimized level. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

Figure AD2—Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Nonexistent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT

Figure AD2—Maturity Model for Internal Control		
Maturity Level	**Status of the Internal Control Environment**	**Establishment of Internal Controls**
	impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized occasionally.
5 Optimized	An enterprisewide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

The maturity model evaluation is one of the final steps in the evaluation process. The IT audit and assurance professional can address the key controls within the scope of the work program and formulate an objective assessment of the maturity levels of the control practices. The maturity assessment can be a part of the audit/assurance report, and used as a metric from year to year to document progression in the enhancement of controls. However, it must be noted that the perception of the maturity level may vary between the process/IT asset owner and the auditor. Therefore, an auditor should obtain the concerned stakeholder's concurrence before submitting the final report to management.

At the conclusion of the review, once all findings and recommendations are completed, the professional assesses the current state of the COBIT control framework and assigns it a maturity level using the six-level scale. Some practitioners utilize decimals (x.25, x.5, x.75) to indicate gradations in the maturity model. As a further reference, COBIT provides a definition of the maturity designations by control objective. While this approach is not mandatory, the process is provided as a separate section at the end of the audit/assurance program for those enterprises that wish to implement it. It is suggested that a maturity assessment be made at the COBIT control level. To provide further value to the client/customer, the professional can also obtain maturity targets from the client/customer. Using the assessed and target maturity levels, the professional can create an effective graphic presentation that describes the achievement or gaps between the actual and targeted maturity goals.

IV. Assurance and Control Framework

ISACA IT Assurance Framework and Standards

ISACA has long recognized the specialized nature of IT assurance and strives to advance globally applicable standards. Guidelines and procedures provide detailed guidance on how to follow those standards. IT Audit and Assurance Standard S15 IT Controls, and IT Audit and Assurance Guideline G38 Access Controls are relevant to this audit/assurance program.

ISACA Controls Framework

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap among control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises.

Utilizing COBIT as the control framework on which IT audit/assurance activities are based aligns IT audit/assurance with good practices as developed by the enterprise.

Refer to ISACA's *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, published in 2007, for the related control practice value and risk drivers.

V. Executive Summary of Audit/Assurance Focus

SAP ERP Security

The review of SAP helps management ensure that it is secure. Since launching its first product offering almost 30 years ago, SAP has grown globally. It has approximately 12 million users and 96,400 installations in more than 120 countries and is the third-largest independent software company in the world. The company name, SAP, is a German acronym that loosely translates in English to Systems, Applications and Products in data processing.

Before SAP ERP, SAP had two main products: the mainframe system SAP® R/2® and the client/server-based system SAP R/3. Both R/2 and R/3 are targeted to business application solutions and feature complexity, business and organizational experience, and integration. The R/2 and R/3 terminology is sometimes taken to mean release 2 and release 3 respectively; however, this is not the case. The R in R/2 and R/3 means "real time." Release levels are annotated separately to the R/2 or R/3 descriptors. For example, in SAP R/3 4.6B, the 4 is the major release number, the 6 is the minor release number following a major release, and the B is the version within a release.

R/3 was introduced in 1992 with a three-tier architecture paradigm. In recent years, SAP has introduced Service Oriented Architecture (SOA) as part of SAP ERP. This combines ERP with an open technology platform that can integrate SAP and non-SAP systems on the SAP NetWeaver® platform. The current core ERP solution offered by SAP is called SAP Enterprise Central Component (ECC 6.0), referred here as SAP ERP.

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.

Risks 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

Objective and Scope

Objective—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.

Scope—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 risks introduced to the enterprise by these components and modules.

Minimum Audit Skills

This review is considered highly technical. The IT 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.

VI. Inventory Business Cycle Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
A. PRIOR AUDIT/EXAMINATION REPORT FOLLOW-UP									
1. Review prior report, if one exists, verify completion of any agreed-upon corrections and note remaining deficiencies.	ME1								
1.1 Determine whether: • 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 achievement of the defined information systems objectives and 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	ME1								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
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 organization 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 configuration									
B. PRELIMINARY AUDIT STEPS									
1. Gain an understanding of the SAP ERP environment.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1.1 The same background information obtained for the SAP ERP Basis Security audit plan is required for and relevant to the business cycles. In particular, the following information is important: • 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 risks • Copies of the organization's key security policies and standards	PO2 PO3 PO4 PO6 PO9 DS2 DS5 AI2 AI6 ME2								
1.2 Obtain the following relevant business cycle details: • The Organizational Model as it relates to inventory activity, i.e., plant organization unit structure in SAP ERP and manufacturing organization 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 materials and warehouse management	PO4 AI4								
2. Identify the significant risks and determine the key controls.									
2.1 Develop a high-level process flow diagram and overall understanding of the Inventory processing cycle, including the following subprocesses: • Master data maintenance • Raw materials management • Producing and costing inventory • Handling and shipping finished goods	DS6 DS11 DS12 DS13								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.2 Assess the key risks, determine key controls or control weaknesses, and test controls (refer to detailed sample testing program below and chapter 4 for techniques for testing configurable controls and logical access security) regarding the following factors: • The controls culture of the organization (e.g., a just-enough control philosophy) • 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.)	PO9 ME2								
C. DETAILED AUDIT STEPS									
1. Master Data Maintenance									
1.1 Changes made to master data are valid, complete, accurate and timely.									
1.1.1 Take a sample of inventory file updates using transaction MB59, which allows users to perform a search on multiple materials by a particular range of dates and check back to authorized source documentation. Review the process for physical stock-takes to confirm the complete, accurate, valid and timely recording of stock differences.	DS11 DS13			X					
1.1.2 Review organization policy and process design specifications regarding access to maintain material master data. Test user access to the following transaction codes: • Create Material—MM01 • Change Material—MM02 • Flag Material for Deletion—MM06	DS11 DS13			X					
1.1.3 Determine whether the configurable control settings address the risks pertaining to the validity, completeness and accuracy of master data and whether they have been set in accordance with management intentions. View the settings online using the IMG as follows:									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
• Material Types: Transaction SPRO Menu Path—Logistics General > Material Master > Basic Settings > Material Types > Define Attributes of Material Types • Industry Sector: Transaction SPRO Menu Path—Logistics General > Material Master > Field Selection > Define industry sectors and industry-sector-specific field selection • Default Price Types: Execute transaction OMW1 and determine whether default settings have been set for the price type for material records. • Tolerances for physical inventory differences: Execute transaction OMJ2 and compare defined tolerances to organizational policy and judge for reasonableness.	PO9 DS6 DS11 DS12 DS13 ME1 ME2			X					
1.2 Inventory master data remain current and pertinent.									
1.2.1 Determine whether the appropriate management runs the materials list transaction code MM60, or equivalent, by material type and confirm evidence of management's review of the data on a rotating basis for currency and ongoing pertinence.	DS11 ME1 ME4			X					
1.3 Settings or changes to the bill of materials or process order settlement rules are valid, complete, accurate and timely.									
1.3.1 Review organization policy and process design specifications regarding access to maintain bill of materials and process order settlement rules. Test user access to the following transaction codes: • Create Material BOM—CS01 • Change Material BOM—CS02 • Make Mass Changes—CS20 • Change Single-layered BOM—CS72 • Change Multi-layered BOM—CS75 • Change settlement rules—COR2; Nondisplayable transaction code KOBK (refer to menu path: Logistics > Production Process > Process Order > Process Order > Display. Enter the	DS13 ME1			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
process order number and press Enter then go to Header > Settlement Rule)									
1.3.2 Take a sample of BOM updates using transaction CS80 and check back to authorized source documentation.	DS13			X					
2. Raw Materials Management									
2.1 Inventory is salable, usable and safeguarded adequately.									
2.1.1 Confirm that the distribution resource planning (DRP) process takes into account stock on hand, forecast requirements, economic order quantities and back orders. Execute transaction code MB5M and ascertain the reason for any old stock being held (shelf-life list). Use transaction MC46 to identify slow-moving items and MC50 for "dead" stock (i.e., stock that has not been used for a certain period of time). Test that managers are reviewing this information on a regular basis.	DS6 DS13 ME1			X					
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 Test that management executes the report of outstanding purchase orders using transaction ME2L (refer to Expenditure cycle 2.2.1) and follow up on any long-outstanding items.	DS13			X					
2.2.2 Review the reconciliation of the goods received/invoice received account (transaction code MB5S, refer to Expenditure cycle 3.2.3) and confirm that unmatched items have been investigated in a timely manner.	ME1 ME2			X					
2.2.3 Test user access to transactions for goods receipt (refer to Expenditure cycle 2.2.2) as follows: • Goods Receipt for Purchase Order —MB01 • Goods Receipts Purchase Order Unknown—MB0A • Goods Receipt for Order—MB31 • Enter Other Goods Receipts—MB1C • Cancel Material Document—MBST	DS12 DS13 ME1			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
• Goods Movement—MIGO									
2.2.4 Test the controls over inventory stock takes (refer to 1.1.1).									
2.3 Defective raw materials 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 MB51 with the appropriate movement type (refer to Expenditure cycle 2.3.1). Determine if there are any long-outstanding materials pending return to suppliers or receipt of appropriate credits.	DS13			X					
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 Review the policy and procedures concerning the transfer of materials and confirm that the above controls are in place and operating. Test that inventory-in-transit accounts are regularly reviewed to ensure the accounts are cleared and reconciled. Confirm that default price types have been established for all materials (refer to 1.1.3).	DS6 ME2			X					
3.1.2 Test user access to BOMs (refer to 1.3.1).									
3.1.3 Test user access to issue goods (transaction code MB1A), post transfers between plants (transaction code MB1B) and move goods (transaction code MIGO).	DS13 ME1			X					
3.1.4 Test user access to create (transaction code CR01) or change (transaction code CR02) work centers.	DS13 ME1			X					
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 Test inventory stock-take procedures (refer to 1.1.1).	DS13 ME1			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
4.1.2 Test user access to change settlement rules (refer to 1.3.1).	DS13 ME1			X					
4.2 Goods returned by customers are accepted in accordance with the organization's policies	AI4 ME1			X					
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. Execute transaction MB51 with the appropriate movement type. Determine if there are any long-outstanding materials pending return to inventory or provision of appropriate credits.	AI4 ME1			X					
4.3 Shipments are recorded accurately, in a timely manner and in the appropriate period.									
4.3.1 Test user access to Transfer Stock Between Plants (transaction code LT04) or Change Outbound Delivery (transaction code VL02N).	DS13 ME1			X					
4.3.2 Take a sample of the delivery due list and the Owed to Customer report and test for evidence of management action. Review settings, using transaction code OMWB, and confirm that accounts assignments are set to valid COGS accounts.	DS13 ME1 ME4			X					

VII. Maturity Assessment

The maturity assessment is an opportunity for the reviewer to assess the maturity of the processes reviewed. Based on the results of audit/assurance review, and the reviewer's observations, assign a maturity level to each of the following COBIT control practices.

COBIT Control Practice	**Assessed Maturity**	**Target Maturity**	**Reference Hyperlink**	**Comments**
AI6.1 Change Standards and Procedures 1. Develop, document and promulgate a change management framework that specifies the policies and processes, including: • Roles and responsibilities • Classification and prioritization of all changes based on business risk • Assessment of impact • Authorization and approval of all changes by the business process owners and IT • Tracking and status of changes • Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention) 2. Establish and maintain version control over all changes. 3. Implement roles and responsibilities that involve business process owners and appropriate technical IT functions. Ensure appropriate segregation of duties. 4. Establish appropriate record management practices and audit trails to record key steps in the change management process. Ensure timely closure of changes. Elevate and report to management changes that are not closed in a timely fashion. 5. Consider the impact of contracted services providers (e.g., of infrastructure, application development and shared services) on the change management process. Consider integration of organizational change management processes with change management processes of service providers. Consider the impact of the organizational change management process on contractual terms and SLAs.				
AI6.2 Impact Assessment, Prioritization and Authorization 1. Develop a process to allow business process owners and IT to request changes to infrastructure, systems or applications. Develop controls to ensure that all such changes arise only through the change request management process. 2. Categorize all requested changes (e.g., infrastructure, operating systems, networks, application systems, purchased/packaged application software). 3. Prioritize all requested changes. Ensure that the change management process identifies both the business and technical needs for the change. Consider legal, regulatory and contractual reasons for the requested change. 4. Assess all requests in a structured fashion. Ensure that the assessment process addresses impact analysis on infrastructure, systems and applications. Consider security, legal, contractual and compliance implications of the requested change. Consider also interdependencies amongst changes. Involve				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
business process owners in the assessment process, as appropriate. 5. Ensure that each change is formally approved by business process owners and IT technical stakeholders, as appropriate.				
AI6.4 Change Status Tracking and Reporting 1. Ensure that a documented process exists within the overall change management process to declare, assess, authorize and record an emergency change. 2. Ensure that emergency changes are processed in accordance with the emergency change element of the formal change management process. 3. Ensure that all emergency access arrangements for changes are appropriately authorized, documented and revoked after the change has been applied. 4. Conduct a postimplementation review of all emergency changes, involving all concerned parties. The review should consider implications for aspects such as further application system maintenance, impact on development and test environments, application software development quality, documentation and manuals, and data integrity.				
DS5.3 Identity Management 1. Establish and communicate policies and procedures to uniquely identify, authenticate and authorize access mechanisms and access rights for all users on a need-to-know/need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved. 2. Ensure that roles and access authorization criteria for assigning user access rights take into account: • Sensitivity of information and applications involved (data classification) • Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements) • Roles and responsibilities as defined within the enterprise • The need-to-have access rights associated with the function • Standard but individual user access profiles for common job roles in the organization • Requirements to guarantee appropriate segregation of duties 3. Establish a method for authenticating and authorizing users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements. 4. Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person. 5. Ensure that a timely information flow is in place that reports changes in jobs (i.e., people in, people out, people change). Grant, revoke and adapt user access rights in co-ordination with human resources and user departments for users who are new, who have left the organization, or who have changed roles or jobs.				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
DS5.4 User Account Management 1. Ensure that access control procedures include but are not limited to: • Using unique user IDs to enable users to be linked to and held accountable for their actions • Awareness that the use of group IDs results in the loss of individual accountability and are permitted only when justified for business or operational reasons and compensated by mitigating controls. Group IDs must be approved and documented. • Checking that the user has authorization from the system owner for the use of the information system or service, and the level of access granted is appropriate to the business purpose and consistent with the organizational security policy • A procedure to require users to understand and acknowledge their access rights and the conditions of such access • Ensuring that internal and external service providers do not provide access until authorization procedures have been completed • Maintaining a formal record, including access levels, of all persons registered to use the service • A timely and regular review of user IDs and access rights 2. Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorizations for special privileged access rights should be reviewed independently at more frequent intervals.				
DS9.1 Configuration Repository and Baseline 1. Implement a configuration repository to capture and maintain configuration management items. The repository should include hardware; application software; middleware; parameters; documentation; procedures; and tools for operating, accessing and using the systems, services, version numbers and licensing details. 2. Implement a tool to enable the effective logging of configuration management information within a repository. 3. Provide a unique identifier to a configuration item so the item can be easily tracked and related to physical asset tags and financial records. 4. Define and document configuration baselines for components across development, test and production environments, to enable identification of system configuration at specific points in time (past, present and planned). 5. Establish a process to revert to the baseline configuration in the event of problems, if determined appropriate after initial investigation. 6. Install mechanisms to monitor changes against the defined repository and baseline. Provide management reports for exceptions, reconciliation and decision making.				
DS9.2 Identification and Maintenance of Configuration Items 1. Define and implement a policy requiring all configuration items and their attributes and versions to be identified and maintained.				

COBIT Control Practice	**Assessed Maturity**	**Target Maturity**	**Reference Hyperlink**	**Comments**
2. Tag physical assets according to a defined policy. Consider using an automated mechanism, such as barcodes. 3. Define a policy that integrates incident, change and problem management procedures with the maintenance of the configuration repository. 4. Define a process to record new, modified and deleted configuration items and their relative attributes and versions. Identify and maintain the relationships between configuration items in the configuration repository. 5. Establish a process to maintain an audit trail for all changes to configuration items. 6. Define a process to identify critical configuration items in relationship to business functions (component failure impact analysis). 7. Record all assets—including new hardware and software, procured or internally developed—within the configuration management data repository. 8. Define and implement a process to ensure that valid licenses are in place to prevent the inclusion of unauthorized software.				
DS9.3 Configuration Integrity Review 1. To validate the integrity of configuration data, implement a process to ensure that configuration items are monitored. Compare recorded data against actual physical existence, and ensure that errors and deviations are reported and corrected. 2. Using automated discovery tools where appropriate, reconcile actual installed software and hardware periodically against the configuration database, license records and physical tags. 3. Periodically review against the policy for software usage the existence of any software in violation or in excess of current policies and license agreements. Report deviations for correction.				

Basis Cycle

I. Introduction

Overview
ISACA developed *ITAF™: A Professional Practices Framework for IT Assurance* as a comprehensive and good-practice-setting model. ITAF provides standards that are designed to be mandatory, and are the guiding principles under which the IT audit and assurance profession operates. The guidelines provide information and direction for the practice of IT audit and assurance. The tools and techniques provide methodologies, and tools and templates to provide direction in the application of IT audit and assurance processes.

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. This audit/assurance program is intended to be utilized by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF, section 2200—General Standards. The audit/assurance programs are part of ITAF, section 4000—IT Assurance Tools and Techniques.

Control Framework
The audit/assurance programs have been developed in alignment with the COBIT framework—specifically COBIT 4.1—using generally applicable and accepted good practices. They reflect ITAF, sections 3400—IT Management Processes, 3600—IT Audit and Assurance Processes, and 3800—IT Audit and Assurance Management.

Many enterprises have embraced several frameworks at an enterprise level, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework. The importance of the control framework has been enhanced due to regulatory requirements by the US Securities and Exchange Commission (SEC) as directed by the US Sarbanes-Oxley Act of 2002 and similar legislation in other countries. They seek to integrate control framework elements used by the general audit/assurance team into the IT audit and assurance framework. Since COSO is widely used, it has been selected for inclusion in this audit/assurance program. The reviewer may delete or rename the columns in the audit program to align with the enterprise's control framework.

IT Governance, Risk and Control
IT governance, risk and control are critical in the performance of any assurance management process. Governance of the process under review will be 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 will be evaluated as steps in the audit/assurance program. Controls are the primary evaluation point in the process. The audit/assurance program will identify the control objectives with steps to determine control design and effectiveness.

Responsibilities of IT Audit and Assurance Professionals
IT audit and assurance professionals are expected to customize this document to the environment

in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it is not intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional holds the Certified Information Systems Auditor (CISA) designation, or has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the CISA designation and necessary subject matter expertise to adequately review the work performed.

II. Using This Document

This audit/assurance program was developed to assist the audit and assurance professional in designing and executing a review. Details regarding the format and use of the document follow.

Work Program Steps

The first column of the program describes the steps to be performed. The numbering scheme used provides built-in work paper numbering for ease of cross-reference to the specific work paper for that section. IT audit and assurance professionals are encouraged to make modifications to this document to reflect the specific environment under review.

COBIT Cross-reference

The COBIT cross-reference provides the audit and assurance professional with the ability to refer to the specific COBIT control objective that supports the audit/assurance step. The COBIT control objective should be identified for each audit/assurance step in the section. Multiple cross-references are not uncommon. Processes at lower levels in the work program are too granular to be cross-referenced to COBIT. The audit/assurance program is organized in a manner to facilitate an evaluation through a structure parallel to the development process. COBIT provides in-depth control objectives and suggested control practices at each level. As the professional reviews each control, he/she should refer to COBIT 4.1 or the *IT Assurance Guide: Using COBIT* for good-practice control guidance.

COSO Components

As noted in the introduction, COSO and similar frameworks have become increasingly popular among audit and assurance professionals. This ties the assurance work to the enterprise's control framework. While the IT audit/assurance function has COBIT as a framework, operational audit and assurance professionals use the framework established by the enterprise. Since COSO is the most prevalent internal control framework, it has been included in this document and is a bridge to align IT audit/assurance with the rest of the audit/assurance function. Many audit/assurance organizations include the COSO control components within their report and summarize assurance activities to the audit committee of the board of directors.

For each control, the audit and assurance professional should indicate the COSO component(s) addressed. It is possible, but generally not necessary, to extend this analysis to the specific audit step level.

The original COSO internal control framework contained five components. In 2004, COSO was revised as the *Enterprise Risk Management (ERM) Integrated Framework* and extended to eight

components. The primary difference between the two frameworks is the additional focus on ERM and integration into the business decision model. ERM is in the process of being adopted by large enterprises. The two frameworks are compared in **figure AD1**.

Figure AD1—Comparison of COSO Internal Control and ERM Integrated Frameworks	
Internal Control Framework	**ERM Integrated Framework**
Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.	**Internal Environment**: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an enterprise's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
	Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the enterprise's mission and are consistent with its risk appetite.
	Event Identification: Internal and external events affecting achievement of an enterprise's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.
Risk Assessment: Every enterprise faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, and thus risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.	**Risk Assessment**: Risks are analyzed, considering the likelihood and impact, as a basis for determining how they could be managed. Risk areas are assessed on an inherent and residual basis.
	Risk Response: Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the enterprise's risk tolerances and risk appetite.
Control Activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the enterprise's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.	**Control Activities:** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders.	**Information and Communication:** Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the enterprise.
Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.	**Monitoring:** The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Information for **figure AD1** was obtained from the COSO web site *www.coso.org/aboutus.htm.*

The original COSO internal control framework addresses the needs of the IT audit and assurance professional: control environment, risk assessment, control activities, information and communication, and monitoring. As such, ISACA has elected to utilize the five-component model for these audit/assurance programs. As more enterprises implement the ERM model, the additional three columns can be added, if relevant. When completing the COSO component

columns, consider the definitions of the components as described in **figure AD1**.

Reference/Hyperlink

Good practices require the audit and assurance professional to create a work paper for each line item, which describes the work performed, issues identified and conclusions. The reference/hyperlink is to be used to cross-reference the audit/assurance step to the work paper that supports it. The numbering system of this document provides a ready numbering scheme for the work papers. If desired, a link to the work paper can be pasted into this column.

Issue Cross-reference

This column can be used to flag a finding/issue that the IT audit and 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).

Comments

The comments column can be used to indicate the waiving of a step or other notations. It is not to be used in place of a work paper describing the work performed.

III. Controls Maturity Analysis

One of the consistent requests of stakeholders who have undergone IT audit/assurance reviews is a desire to understand how their performance compares to good practices. Audit and assurance professionals must provide an objective basis for the review conclusions. Maturity modeling for management and control over IT processes is based on a method of evaluating the organization, so it can be rated from a maturity level of nonexistent (0) to optimized (5). This approach is derived from the maturity model that the Software Engineering Institute (SEI) of Carnegie Mellon University defined for the maturity of software development.

The *IT Assurance Guide: Using COBIT*, appendix VII—Maturity Model for Internal Control, in **figure AD2**, provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimized level. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

Figure AD2—Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Nonexistent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT

Figure AD2—Maturity Model for Internal Control		
Maturity Level	**Status of the Internal Control Environment**	**Establishment of Internal Controls**
	impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized occasionally.
5 Optimized	An enterprisewide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

The maturity model evaluation is one of the final steps in the evaluation process. The IT audit and assurance professional can address the key controls within the scope of the work program and formulate an objective assessment of the maturity levels of the control practices. The maturity assessment can be a part of the audit/assurance report, and used as a metric from year to year to document progression in the enhancement of controls. However, it must be noted that the perception of the maturity level may vary between the process/IT asset owner and the auditor. Therefore, an auditor should obtain the concerned stakeholder's concurrence before submitting the final report to management.

At the conclusion of the review, once all findings and recommendations are completed, the professional assesses the current state of the COBIT control framework and assigns it a maturity level using the six-level scale. Some practitioners utilize decimals (x.25, x.5, x.75) to indicate gradations in the maturity model. As a further reference, COBIT provides a definition of the maturity designations by control objective. While this approach is not mandatory, the process is provided as a separate section at the end of the audit/assurance program for those enterprises that wish to implement it. It is suggested that a maturity assessment be made at the COBIT control level. To provide further value to the client/customer, the professional can also obtain maturity targets from the client/customer. Using the assessed and target maturity levels, the professional can create an effective graphic presentation that describes the achievement or gaps between the actual and targeted maturity goals.

IV. **Assurance And Control Framework**

ISACA IT Assurance Framework and Standards

ISACA has long recognized the specialized nature of IT assurance and strives to advance globally applicable standards. Guidelines and procedures provide detailed guidance on how to follow those standards. IT Audit/Assurance Standard S15 IT Controls, and IT Audit/ Assurance Guideline G38 Access Controls are relevant to this audit/assurance program.

ISACA Controls Framework

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap among control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises.

Utilizing COBIT as the control framework on which IT audit/assurance activities are based aligns IT audit/assurance with good practices as developed by the enterprise.

Refer to ISACA's *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, published in 2007, for the related control practice value and risk drivers.

V. Executive Summary of Audit/Assurance Focus

SAP ERP Security

The review of SAP helps management ensure that it is secure. Since launching its first product offering almost 30 years ago, SAP has grown globally. It has approximately 12 million users and 96,400 installations in more than 120 countries and is the third-largest independent software company in the world. The company name, SAP, is a German acronym that loosely translates in English to Systems, Applications and Products in data processing.

Before SAP ERP, SAP had two main products: the mainframe system SAP® R/2® and the client/server-based system SAP R/3. Both R/2 and R/3 are targeted to business application solutions and feature complexity, business and organizational experience, and integration. The R/2 and R/3 terminology is sometimes taken to mean release 2 and release 3 respectively; however, this is not the case. The R in R/2 and R/3 means "real time." Release levels are annotated separately to the R/2 or R/3 descriptors. For example, in SAP R/3 4.6B, the 4 is the major release number, the 6 is the minor release number following a major release, and the B is the version within a release.

R/3 was introduced in 1992 with a three-tier architecture paradigm. In recent years, SAP has introduced Service Oriented Architecture (SOA) as part of SAP ERP. This combines ERP with an open technology platform that can integrate SAP and non-SAP systems on the SAP NetWeaver® platform. The current core ERP solution offered by SAP is called SAP Enterprise Central Component (ECC 6.0), referred here as SAP ERP.

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.

Risks 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

Objective and Scope

Objective—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.

Scope—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 risks introduced to the enterprise by these components and modules.

Minimum Audit Skills

This review is considered highly technical. The IT 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.

VI. Basis Cycle Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
A. PRIOR AUDIT/EXAMINATION REPORT FOLLOW-UP									
1. Review prior report, if one exists, verify completion of any agreed-upon corrections and note remaining deficiencies.	ME1								
1.1 Determine whether: • 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 achievement of the defined information systems objectives and 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	ME1								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
• 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 organization 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 configuration									
B. PRELIMINARY AUDIT STEPS									
1. Gain an understanding of the SAP ERP environment.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1.1 Determine what version and release of the SAP ERP software has been implemented. If multiple versions, document the various versions.	PO4								
1.2 Obtain details of the following: • Operating system(s) and platforms • Total number of named users (for comparison with limits specified in contract) • Number of SAP ERP instances and clients • Accounting period, company codes and chart of accounts • Database management system used to store data for the SAP ERP system • Location of the servers and the related LAN/WAN connections (need to verify security and controls, including environmental, surrounding the hardware and the network security controls surrounding the connectivity) and, if possible, copies of network topology diagrams • List of business partners, related organizations and remote locations that are permitted to connect to the ERP environment • Various means used to connect to the ERP environment (e.g., dial-up, remote access server, Internet transaction server) and the network diagram, if available	PO2 PO3 DS2 DS12								
2. In a standard SAP ERP configuration, confirm that separate systems for development, test and production are implemented.	PO2								
2.1 Determine whether: • This approach was taken • The instances are totally separate systems or are within the same system									
2.2 Determine whether the SAP production environment is connected to other SAP or non-SAP systems. If yes, obtain details as to the nature of connectivity, frequency of information transfers, and security and control measures surrounding these transfers (i.e., to ensure accuracy and completeness).	PO2 DS5								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. Identify the components being used (Human Capital Management, Financials, Operations, Corporate Services).	PO2								
3.1 Identify whether the organization has implemented any of the following: • Internet transaction server • Any of the New Dimension products (e.g., Supply Chain Management, Customer Relationship Management, Business Intelligence) • Audit Information System. If implemented, determine how it is used (i.e., only for annual audits or on a regular basis to monitor and report on security issues).	PO2 PO3 ME2								
3.2 Determine whether the organization makes use of any mySAP functionality. If yes, describe the functionality and purpose.	PO2								
3.3 Determine whether the organization has created any locally developed APAB/4 programs/reports or tables. If yes, determine how these programs/reports are used. Depending on the importance/extent of use, review and document the development and change management process surrounding the creation/modification of these programs/reports or tables.	AI2 AI6								
3.4 Obtain copies of the organization's key security policies and standards. Highlight key areas of concern, including: • Information security policy • Sensitivity classification • Logical and physical access control requirements • Network security requirements, including requirements for encryption, firewalls, etc. • Platform security requirements (e.g., configuration requirements)	PO6 DS5 DS12								
3.5 Obtain information regarding any awareness programs that have been delivered to staff on the key security policies and standards. Consider specifically the frequency of delivery and any statistics on the extent of coverage (i.e., what percentage of staff has received the awareness	PO6 DS7								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
training).									
3.6 Maintain authorizations and profiles, for example: • Have job roles, including the related transactions, been defined and documented? • Do procedures for maintaining (creating/changing/deleting) roles exist and are they followed?	PO7 AI4 DS5								
3.7 Determine whether adequate access administration procedures exist in written form. Do any of the following procedures exist within the organization? If yes, document the process and comment on compliance with the policies and standards, and the adequacy of resulting documentation. • Procedures to add/change/delete user master records • Procedures to handle temporary access requests • Procedures to handle emergency access requests • Procedures to remove users who have never logged into the system • Procedures to automatically notify the administration staff when employees holding sensitive or critical positions leave the organization or change positions	PO7 AI4 DS5								
3.8 Obtain copies of the organization's change management policies, processes and procedures, and change documentation. Consider specifically: • Transport processes and procedures, including allowed transport paths • Emergency change processes and procedures • Development standards, including naming conventions, testing requirements and move- to-production requirements	AI4 AI6								
3.9 Determine whether the organization has a defined process for creating and maintaining clients. If yes, obtain copies and documentation related to the creation and maintenance of clients.	PO2 AI6								

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3.10 Determine the organization's approach to SAP Service Marketplace. Verify the extent of access permitted and processes used to request, approve, authenticate, grant, monitor and terminate SAP Service Marketplace access.	DS2 DS5								
4. Review outstanding audit findings, if any, from previous years. Assess impact on current audit.	ME1 ME2								
5. Identify the significant risks and determine the key controls.									
5.1 Obtain details of the risk assessment approach taken in the organization to identify and prioritize risks.	PO9								
5.2 Obtain copies of and review: • Completed risk assessments impacting the SAP ERP environment • Approved requests to deviate from security policies and standards Assess the impact of the above documents on the planning of the SAP ERP audit.	PO9 ME1								
5.3 In the case of a recent implementation/upgrade, obtain a copy of the security implementation plan. Assess whether the plan took into account the protection of critical objects within the organization and segregation of duties. Determine whether an appropriate naming convention (i.e., for profiles) has been developed to help security maintenance and to comply with required SAP ERP naming conventions.	PO3 PO7 DS5								
C. DETAILED AUDIT STEPS									
1. Application Installation (Implementation Guide and Organizational Model)									
1.1 Configuration changes are made in the development environment and transported to production.									
1.1.1 Test that access to the transaction code (SPRO) and the authorization object (S_IMG_ACTV) for the IMG have been restricted in the production environment.									
1.1.2 Restrict access to transaction code SCC4, which controls the									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
production client settings. Execute this transaction code, and double-click on each client being tested. Review each of the settings for appropriateness, including the last changed by and last changed date fields. It is important to note that the No Changes setting should be set for cross-client tables. Protection for the Client Copier and Comparison Tool should be set to No Overwriting. Also ensure that eCAAT and CAAT are set to Not Allowed. Identify changes directly made into production by reviewing a log of changes to table T000. Validate that a business need existed for such direct change and an appropriate change management process was followed.									
1.1.3 Obtain information from the system on the OMM by reviewing tables or by utilizing the SAP ERP Audit Information System, which depicts the OMM graphically (refer to figure 12.5). Compare it to the real organization structure and interview management in relation to differences or difficulties that may have emerged during or after the implementation.									
1.1.4 Test access to the transaction code (SPRO) and the authorization object (S_IMG_ACTV) for the IMG in the production environment.									
1.1.5 Test the following access to validate who can make changes directly to the production client: a) T-code: SCC4 Authorization Object: S_TABU_DIS Activity value: 02 Authorization group: SS Authorization Object: S_TABU_CLI Indicators for cross client: x									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
b) T-code: SCC4 Authorization Object: S_ADMI_FCD Sys Admin function: T000 Authorization Object: S_CTS_ADMI Admin Task: INIT									
1.2 Changes to critical number ranges are controlled.									
1.2.1 Via transaction SUIM, review authorization object S_NUMBER (*) for those users with the following authorization value sets: • Maintain Number Range Intervals—02 • Change Number Range Status—11 • Initialize Number Levels—13 • Maintain Number Range Objects for all Number Range Objects—17									
1.2.2 By using transaction code SE16, browse table TDDAT. In the table name field enter Z* and then Y* to identify all of the custom tables. Determine those tables that have &NC& within the authorization group field. Assess whether these settings (&NC&) are appropriate.									
1.2.3 Test access to modify critical tables via the objects S_TABU_DIS (value 02) and transaction codes SM31 or SM30. If the table is cross-client, the user master record must contain a third object, S _TABU_CLI (value X). Use transaction code SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002) to check for these restrictions. Test access to update tables with authorization group SS, as no one should have update access to this critical systems table.									
2. Application Development (ABAP/4 Workbench and Transport System)									
2.1 Application modifications are planned, tested and implemented in a									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
phased manner.									
2.1.1 Determine the system landscape and client strategy, and review the change control policies and procedures (including documentation) to transport objects between environments. Work with the Basis/Transport Administrator to obtain a random sample of transports and trace back to documentation. Ensure that authorization for the transport was obtained and confirm that the specified transport path was followed. For emergency changes, ensure that the specified emergency process was followed. Confirm that appropriate authorizations were obtained and documentation was subsequently completed. Review the System Change option and confirm it has been set to No Changes Allowed (refer to 1.1.2 above). Review segregation of duties with respect to creating and releasing change requests. Test user access to authorization object S_TRANSPRT and ACTVT; expect 03 and any transport type (TTYPE). Assess the appropriateness of such access in comparison with the users' job functions.	AI6 DS5			X					
2.2 Customized ABAP/4 programs are secured appropriately.									
2.2.1 To identify customized programs that have not been assigned to an authorization group, enter transaction code SE16. Browse the table TRDIR and enter the values of Z* and then Y* in the program name field. This will produce a list of all customized programs, assuming that the organization has followed standard naming convention when customizing programs. Filter this list for programs that do not have a value in the authorization group field (SECU). Concentrate the investigation on users who have SE38, SA38, SE80 and SE37 transaction codes. These users automatically have access to run many of these programs.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.2.2 From this list, select a representative sample of customized programs and check the source code to see whether an authority-check statement has been included. Use transaction code SA38 and run the ABAP/4 program RSABAPSC with the appropriate program name and authority check in the ABAP/4 language commands selection field to display the authority-check statements for each of the sampled programs. Note that the results may include other programs called by the sampled programs with the appropriate authority-check statements. Confirm the results of the test with management.									
2.2.3 Review and assess the value for the parameters below (use RSPARAM report): • Auth/no_check_in_some_cases (Can be either Y or N. If set to the recommended value of Y [permit authorization checks], monitor the content of SU24 carefully to make sure that these entries are set appropriately.) • Auth/rfc_authority_check (recommend set to 2 to permit full checking)	DS5			X					
2.2.4 Use transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002) to test the number of users who have access to execute all programs independent of the authorization group assigned. Enter the authorization object S_PROGRAM with the activity value of SUBMIT or BTCSUBMIT and the authorization object S_TCODE with a transaction code of SA38, SE37, SE38 or SE80.									
2.2.5 Review the policy, procedures and criteria for establishing program authorization groups, assigning the ABAP/4 programs to groups and including authority-check statements in programs. Compare the results from testing to established policies, procedures, standards and guidance (note that organizations may use additional transactions, tables, authorization objects, ABAP/4 programs, and									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
reports to control their systems).									
2.3 The creation or modification of programs is performed in the development system and migrated through the test system to production.									
2.3.1 To produce a list of users who have access to develop programs in the production system, execute transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002) with the authorization object S_DEVELOP, the activity values of 01, 02 or 06. ABAP/4 programs that are not assigned to an authorization group may be changed by any user with authorization for object S_DEVELOP, depending on whether the user has been assigned a developer's key and the correct object keys.									
2.4 Access for making changes to the dictionary is restricted to authorized individuals.									
2.4.1 Execute transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002). Review users with the following authorization to determine whether they are appropriate: Data dictionary object: S_DEVELOP with any of the activity values 01, 02, 06, 07 and access to any of the transaction codes SE11, SE12, SE15, SE16, SE37, SE38, SE80									
2.5 Access to modify and develop queries is restricted.									
2.5.1 Using transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002), enter the authorization object S_QUERY with activity value 02 and transaction code: – SQ01 to identify all users who can create and maintain queries. In addition, use the authorization object S_QUERY with activity value 23 and transaction codes									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
– SQ02 or SQ03 to produce a report identifying all users who can maintain functional areas and user groups. Review the lists with management for reasonableness.									
2.6 Relevant company codes are set to Productive in the production environment.									
2.6.1 Transaction code OBR3 contains a list of company codes and whether they have been set to Productive. This information is also available in table T001 and can be viewed using transaction code SE16. Perform a review of this list. In instances where company codes have not been set to Productive, investigate the reasons with management.									
3. Application Operations (Computing Center Management System)									
3.1 The Computing Center Management System (CCMS) is configured appropriately.									
3.1.1 To ensure that the CCMS displays meaningful data, determine via inquiry whether transaction RZ04 was used to set up operations modes, instances and timetables.									
3.1.2 Determine how the organization 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 organization's environment. Check that only authorized personnel may execute these programs.									
3.1.3 Generate a list of users with the ability to access the Alert Monitor by performing online access authorization testing for these authorization objects S_RZL_ADM, activity values 01 (administrator) and 03 (display) and transaction code, value AL01 (if a 3.x system) or RZ20 (if a 4.x system or SAP ECC system).									
3.2 Batch processing operations are secured appropriately.									
3.2.1 Obtain a list of batch users by executing transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
transaction code SA38 and program RSUSR002) with the following authorizations: • Batch input: transaction code—SM35, authorization object—S_BDC_MONI, field: BDCAKTI, value: DELE, FREE, LOCK, REOG and field: BDCGROUP, value: * • Batch administration: transaction code— SM36/SM37, authorization object—S_BTCH _ADM, field: BTCADMIN, value: Y • Batch scheduling: transaction code— • SM36, authorization object—S_BTCH _JOB, field: JOBACTION, value: DELE, RELE, authorization object—S_BTCH_NAM, value: * • Batch processing: transaction code—SM37, authorization object—S_BTCH _JOB, field: JOBACTION, value: DELE, RELE, PLAN, authorization object—S_BTCH_NAM, value: * • Event triggering: transaction code—SM64, authorization object—S_BTCH _ADM, field: BTCADMIN, value: Y									
3.2.2 Determine by corroborative inquiry that upload programs have been removed from the production environment as appropriate.									
3.3 Default system parameter settings are reviewed and configured to suit the organization's environment.									
3.3.1 Obtain a printout of the values of the following key parameters (run report RSPARAM via transaction code SA38 on each instance, as appropriate) and compare to the requirements as set out in the policies and standards in **figure 12.9**. • Confirm that the system profile parameter files and default.pfl are protected from unauthorized access. Confirm that there is a mechanism/process to ensure that the profiles are regularly checked to ascertain that they have not been changed inappropriately. Obtain any related change documentation and ensure that:									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
– The documentation is authorized. – Related log entries reflect the expected changes. – A current printout of the RSUSR006 report is obtained and reviewed for unusual items or trends. • Determine whether management has a process for frequent monitoring of unsuccessful login attempts and/or locked users via a review of this report. If yes, obtain details on the following frequency of monitoring. • Review a reasonable sample of previously followed-up reports and assess the appropriateness of the follow-up on unusual findings. Run transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002). • Review and follow up on: – Users with original passwords – Users who have not logged in during the last 60 days – Users who have not changed their passwords in the last 60 days (or any duration that is appropriate for the organization) • Obtain a sample of user master records in the production environment and work with the authorization security administrator and the job descriptions to assess segregation of duties (refer to chapter 4 for more guidance) and the appropriateness of the access granted.									
3.3.2 Execute transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002) with the transaction code SM01 to provide a list of all users who have access to lock or unlock transaction codes in the system. Review and confirm this list with management to ensure that only authorized users have access.									
3.3.3 Enter transaction code SM01 to display a list of transaction codes									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
with a check box beside them. A cross in the check box indicates that the transaction code has been locked. Review sensitive transaction codes to ensure that they have been locked from user access. Such transaction codes include but are not limited to: SCC5—Client Delete SCC1—Client Copy (may overwrite the production client) SM49—Execute Logical Commands (may allow pass-through to operating system) SM69—Execute Logical Commands (may allow pass-through to operating system)									
3.4 Users are prevented from logging in with trivial or easily guessable passwords.									
3.4.1 Based on the review of the key security policies, determine whether there are any character combinations (apart from the SAP ERP standards) that the policy has prohibited from use. If yes, obtain a printout of the contents of table USR40 and confirm that the list of "illegal" words is contained therein.	PO6 DS5			X					
3.5 SAP Router is configured to act as a gateway to secure communications into and out of the SAP ERP environment.									
3.5.1 Discuss with the operating system administrators the procedures surrounding changes to SAP Router and the procedures surrounding restarting SAP Router when it goes down.	AI4 DS5 ME1 ME2			X					
3.5.2 Obtain a list of individuals with view and/or change access to the SAP Router binary. Review the list with key management and assess the appropriateness of the segregation of duties.									
3.5.3 Request an extract of the SAP Router permissions table (for example, execute the UNIX command SAP router –L <path>) from the operating system administrator. Review the permissions table with the operating systems administrator. Compare with the network diagram to assess the appropriateness of the IP addresses									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
and with change control documentation to confirm that management has appropriately authorized changes.									
3.5.4 If logging is active, ascertain the frequency with which the logs are reviewed and followed up.									
3.5.5 Obtain a reasonable sample of the logs and review them with the operating systems administrator.									
3.6 Remote access by software vendors is controlled adequately.									
3.6.1 Determine the organization's approach to SAP Service Marketplace. Verify the extent of access permitted and the processes used to request, approve, authenticate, grant, monitor and terminate SAP Service Marketplace access. Check that changes are subject to normal testing and migration controls.	DS2 DS5			X					
3.6.2 Obtain a list of SAP Service Marketplace users on the production client. Enter transaction code OSS1 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 the SAP Service Marketplace by authorization object. In particular, review for reasonableness with management the users who have been assigned to administration authorization and open service connections.									
3.7 SAP ERP Remote Function Call (RFC) and Common Programming Interface—Communications (CPI-C) are secured.									
3.7.1 Ascertain whether the login information (dialog and/or nondialog users) is stored and reviewed. Obtain a representative sample and review to ensure that dialog users are appropriate (i.e., valid employees with authorization) and that nondialog user IDs are appropriate. To do this, execute transaction code SM59. This will display the table RFCDES, which controls the communication between systems. The table lists the RFC destinations, which will include all SAP ERP connections that are on the system. Expand	PO2 AI4 DS5 ME1 ME2			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
each of the SAP ERP connections and double-click on each connection to verify that no dialog user ID is listed with its password.									
3.7.2 Determine whether these systems are protected with the appropriate network measures (e.g., SAP Router/firewall/ routers).									
3.7.3 Assess the strength/adequacy (i.e., robustness) of password measures to authenticate RFC connections.									
3.7.4 Confirm with the SAP ERP security authorization manager that authority checks are included in functional modules called via RFC.									
3.7.5 Via transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002), identify users who have access to transaction code SM59. Assess whether this access is appropriate (work with user access management).									
3.7.6 If using release 4.0 or higher, ascertain whether SNC protection has been applied to RFC calls. If yes, cross-reference to SNC documentation and testing performed earlier.									
3.8 The technology infrastructure is configured to secure communications and operations in the SAP ERP environment.									
3.8.1 Firewall									
3.8.1.1 Discuss with the firewall administrators the procedures surrounding changes to the firewall rules and recovery of firewalls in the event of an outage.	AI4 DS5 ME1 ME2			X					
3.8.1.2 Obtain a list of individuals with view and/or change access to the firewall rules. Review the list with key management and assess the appropriateness of the segregation of duties.	DS5			X					
3.8.1.3 Review the permissions table with the firewall administrator. Compare with network diagram to assess	DS13			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
the appropriateness of the IP addresses.									
3.8.1.4 If logging is set to Logging Active, ascertain the frequency with which the logs are reviewed and followed up.									
3.8.1.5 Obtain a reasonable sample of the logs and review them with the firewalls administrator.									
3.8.2 Secure Network Communications (SNC)									
3.8.2.1 Identify the communication paths that have been protected by SNC/external security product.	AI4 DS5 ME1 ME2			X					
3.8.2.2 Assess whether the level of protection is appropriate for each of the various communication paths. Use the requirements set out in the information security policy and various risk assessments to assist in the assessment.									
3.8.2.3 Review the configuration for each path with the network security administrator for appropriateness.									
3.8.3 Secure Store and Forward (SSF) Mechanisms and Digital Signatures									
3.8.3.1 Determine whether there are any regional laws or regulations with which the organization must comply that govern the use of digital signatures. If yes, confirm that the organization is in compliance.	DS5 ME3			X					
3.8.3.2 Determine whether the organization uses an external product for SSF. If yes: • Ascertain whether the organization uses hardware- or software-based keys. • Describe the controls surrounding issuance and changing of the public and private keys. • Ascertain whether the organization uses self-signed certificates or CA-signed certificates.	PO2 DS5 DS13			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3.8.3.3 If using release 4.5 or higher, determine whether SAPSECULIB is used as the default SSF provider. If yes, determine whether the file SAPSECU.pse is protected from unauthorized access.	DS5			X					
3.8.4 Workstation Security									
3.8.4.1 Via inspection, ensure that staff utilizes the available security measures surrounding workstations/PCs (e.g., screen savers, power-on passwords, third-party security products, physical controls). Consider specifically whether: • Users are able to bypass screen saver/power-on passwords. • Screen savers activate automatically or are (as a rule) activated by users when they leave their work areas.	DS5			X					
3.8.4.2 Regarding virus protection, determine whether: • Virus scanners are used on the network and/or workstations. • Virus signatures are kept up to date. • There is a procedure for disseminating virus education to users.	DS5 DS13			X					
3.8.4.3 Assess adequacy of physical controls. Consider specifically: • Are the workstations in secure/restricted areas? • How is the area secured (e.g., security cards, keys, combination locks)? • Do individuals circumvent these controls (i.e., piggyback at entrance, prop open the door)?	DS5 DS12			X					
3.8.5 Operating System and Database Security									
3.8.5.1 Work with the systems and database administrator to confirm that the default passwords on the standard									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
operating system and database user IDs have been changed, appropriate security parameters have been set and appropriate security procedures are in place and operating.	DS5			X					
4. Application Security (Profile Generator and Security Administration)									
4.1 Duties within the security administration environment are adequately segregated.									
4.1.1 Determine whether the system administrator tasks are segregated into the following administrator functions by generating user lists for the following authorizations using transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002): • For the Profile Generator: – Create and change roles—Used to define and update roles. Use authorization S_USER_AGR with authorization field values of 01 and 02. Test this in conjunction with transaction code PFCG. – Transport roles—Used to transport or activate roles to/in production. Use authorization S_USER_AGR with authorization field value of 21. Test this in conjunction with transaction code PFCG. – Assign roles/profiles to user master records—Used to assign or transfer roles/profiles into the user master records for the relevant users. Use authorization S_USER_AGR with authorization field value of 02 and authorization S_USER_GRP with authorization field value of 22. Test this in conjunction with transaction code PFCG. Also test the manual maintenance of roles/profiles (SU02/SU03) in use prior to PFCG. Authorization Maintenance: Use authorization									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
S_USER_AUT with authorization field value 01, 02, 07, 22. Test this in conjunction with transaction SU03. User Maintenance: Use authorization S_USER_PRO with authorization field value 01, 02, 07, 22. Test this in conjunction with transaction SU02. • For user master maintenance: – Create/change/lock/delete changes: Use authorization object S_USER_GRP with authorization field values of 01, 02, 05, 06. Test this in conjunction with transaction code SU01. – Assign roles/profiles to user master records: Use authorization S_USER_AGR with authorization field value of 02, and authorization S_USER_GRP with authorization field value 22 and 02. If full segregation is not possible among the four functions listed above, management should at minimum consider segregating the creation of roles/profiles and assignment of roles/profiles. If the segregation of duties option is practical, assess SUIM > Change Documents > For Users/For Profiles/For Authorizations (also accessible through transaction code SA38 and programs RSUSR100/101/102) for evidence of review and action by management.									
4.1.2 Test user access to effect mass changes to user master records authorization objects S_USER_GRP and S_USER_ PRO with authorization field values of 01, 02, 05 and 06, and transaction codes SU10 (Delete/Add a Profile for All Users) and SU12 (Delete All Users).									
4.2 Adequate security authorization documentation is maintained.									
4.2.1 Select a random sample of authorized change documentation that									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
pertains to changes to user master records. Run SUIM > Change Documents > For Users (also accessible through transaction code SA38 and program RSUSR100) and assess whether the changes made are as documented.	AI6 DS5 ME1			X					
4.2.2. Select a random sample of authorized change documentation that pertains to changes to profiles. Run SUIM > Change Documents > For Profiles (also accessible through transaction code SA38 and program RSUSR101) and assess whether the changes made are as documented.	AI6 DS5 ME1			X					
4.2.3 Select a random sample of authorized change documentation that pertains to changes to authorizations. Run SUIM > Change Documents > For Authorizations (also accessible through transaction code SA38 and program RSUSR102) and assess whether the changes made are as documented.	AI6 DS5 ME1			X					
4.3 The superuser SAP* is properly secured.									
4.3.1 To determine whether the SAP* user has been locked, execute transaction SA38 (reporting) with transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002). Enter SAP* in the user field and press F8. Verify that the SAP* group field says SUPER. Click twice on the Other View button. The user status field for SAP* should say locked.	DS5			X					
4.3.2 For SAP*, run transaction code SA38 and program RSUSR003 to confirm that: • The ID has been deactivated in all clients and a new superuser created. • The password has been changed from the default (i.e., not trivial).									
4.4 Default users are secured properly.									
4.4.1 To test whether the default password has been changed for DDIC,									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
SAPCPIC and EarlyWatch, execute the SAP ERP report RSUSR003 and determine if the default passwords have been changed. To determine whether the SAPCPIC and EarlyWatch users have been locked, execute transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002). Enter the user name in the user field and press F8. Verify that the group field says SUPER. Click twice on the Other View button. The user status field should say locked.	DS5			X					
4.5 Access to powerful profiles is restricted.									
4.5.1 Review for appropriateness users assigned the privileged profiles of SAP_ALL and SAP_NEW. Users who have been assigned these superuser profiles/roles should be assigned to user group super or equivalent, which should be maintained by a limited number of Basis personnel only. To perform this test, execute transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002). In the part noted as Selection Criteria for User enter SAP_ALL into the profile field. Click on the button to the right of the text box. Enter SAP_NEW in the first empty text box. Click on Copy. This report will list all users who have superuser functionality. Check other powerful profiles for user access: • S_A.SYSTEM (System administration authorizations) • S_RZL_ADMIN (CCMS administration authorizations) • S_USER_ALL (All user administration authorizations) • S_A.USER and S_A.ADMIN (used to administer user master									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
record authorizations) • Check the user list identified by this test to ascertain whether individuals who have access to the previously mentioned functionality require this access, based on their job responsibilities and established policies, procedures, standards and guidance.									
4.6 The authorization group that contains powerful users is restricted.									
4.6.1 Identify the system administrators within the enterprise and determine to which user groups their user IDs belong. Using transaction SUIM > Users > Users by Complex Selection Criteria (also accessible using transaction code SA38 and program RSUSR002), review the system for users with the authorization object S_USER_AGR (Profile Generator environment) with the activity values 01, 02, 21 and 22, and transaction code PFCG or the authorization object S_USER_GRP (manual maintenance) with the activity values of 01, 02, 05 and 06 and the transaction code SU01. The authorization field user group in user master maintenance should be similar to one of the values identified above. This would usually be the group SUPER or ITO-SYSTEM.									
4.7 Changes to Central User Administration (CUA) are authorized and reviewed regularly by management.									
4.7.1 Because all organizations are structured differently and have different requirements, initial discussions with the organization should be conducted to obtain an understanding of the organization's structure and configuration requirements for CUA. To test whether CUA has been configured appropriately, execute the transaction codes SALE, SCUA and SCUM and review the appropriateness of the configured settings for the organization.	DS5			X					
4.8 Changes to critical SAP ERP tables are logged by the system and reviewed by management.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
4.8.1 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 needs to 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 will have table logging enabled. Enter transaction code SE16 and enter table TPROT as the object name along with an X in the PROTFLAG field. This will identify tables that have their changes logged. Run report RSTBPROT (table log) or RSTBHIST (table change analysis), which lists 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 these tables and compare these to the original supporting information/documentation. Obtain explanations for any changes for which supporting information or documentation is not available.	DS5			X					
4.9 Changes made to the data dictionary are authorized and reviewed regularly.									
4.9.1 Understand management's 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 • Level of detail in the reports • Other independent data to which management compares the reports • Likelihood that the person performing the review will be able to identify exception items • Nature of exception items that they can be expected to identify									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
4.10 Access to Systems Administrations Functions is restricted.									
4.10.1 S_ADMI_FCD is an extremely powerful security object that grants access to several critical Basis Administration functions, as well as some functional user functions (such as spool). It should be assigned with great care, and with only the discrete values needed by users. The object defines one authorization field, system administration functions. Test for the following field values. These values should be restricted to Basis group only. • NADM: Network administration (SM54, SM55, SM58, SM59). Only Basis group. • PADM: Process administration (SM50, SM51, SM04); intercept background job (debugging function in background job administration, transaction SM37). Only Basis group. • SM02: Authorization to create, change and delete system messages • UADM: Update administration (SM13) • T000: Create new client (SCC4) • TLCK: Lock/unlock transaction (SM01) • MEMO: Set SAP memory management quota using report RSMEMORY. • COLA: Administration of OLE automation servers and controls - AUDA—Basis audit administration - RSET—Reset/delete data without archiving - SYNC—Reset buffers - UBUF—Reset all user buffers - TCTR—Table control settings throughout the system									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
- Wild card (*), i.e., all values									
4.11 Log and trace files are appropriately configured and secured.									
4.11.1 For Security Audit log, using release 4.0 or higher: • Confirm that the Security Audit log has been activated by running the report RSPARAM and confirming the following parameter values: – Rsau/enable (activates logging on to application server; if the value is 0, it is not active) – Rsau/local/file (specifies the location of the log; confirms that it is appropriately located) – Rsau/max_diskspace/local (specifies the maximum size of the log; confirms that the size is adequate for the organization) • Obtain a listing of events that are logged (can be done via SM20). Review for appropriateness and link to required logging that may be specified in the security policies and standards. • Determine the frequency and thoroughness of the review of the logs. • If possible, obtain a representative sample of the logs and assess the adequacy of the follow-up process and review for unusual items.	DS5 ME1			X					
4.11.2 Review the system log: • Run the report RSPARAM and review the following parameter values to obtain the locations of the log files: – Rslg/local/file (specifies the location of the local log on the application server; default: /usr/sap/<SID>/D20/log/SLOG<SAP_instance_#>) – Rslg/collect_daemon/host (specifies the application server that maintains the central log; default: <hostname of main	DS5 DS10 DS11 DS13 ME1			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
instance>) – Rslg/central/file (specifies the location of the active file for the central log on the application server; default: /usr/sap/<SID>/SYS/global/SLOGJ) – Rslg/central/old_file (specifies the location of the old file for the central log on the application server; default: /usr/sap/<SID>/SYS/global/SLOGJO) – Rslg/max_diskspace/local (specifies the maximum length of the local log; default: 0.5 MB) – Rslg/max_diskspace/central (specifies the maximum length of the central log; default: 2 MB) – Rstr/file (the absolute pathname of the trace file: the trace filename is TRACE<SAP ERP system number>) • Obtain a listing of events that are logged (can be done via SM21). Review for appropriateness (including the size of each local and central log file) and link to required logging, which may be specified in the security policies and standards. • Determine the frequency and thoroughness of the review of the logs. • If possible, obtain a representative sample of the logs and assess the adequacy of the follow-up process and review for unusual items. • Work with the operating system administrator to determine who has permissions to these files. Ensure that the access is appropriate.									

VII. Maturity Assessment

The maturity assessment is an opportunity for the reviewer to assess the maturity of the processes reviewed. Based on the results of audit/assurance review, and the reviewer's observations, assign a maturity level to each of the following COBIT control practices.

COBIT Control Practice	**Assessed Maturity**	**Target Maturity**	**Reference Hyperlink**	**Comments**
AI6.1 Change Standards and Procedures 1. Develop, document and promulgate a change management framework that specifies the policies and processes, including: • Roles and responsibilities • Classification and prioritization of all changes based on business risk • Assessment of impact • Authorization and approval of all changes by the business process owners and IT • Tracking and status of changes • Impact on data integrity (e.g., all changes to data files being made under system and application control rather than by direct user intervention) 2. Establish and maintain version control over all changes. 3. Implement roles and responsibilities that involve business process owners and appropriate technical IT functions. Ensure appropriate segregation of duties. 4. Establish appropriate record management practices and audit trails to record key steps in the change management process. Ensure timely closure of changes. Elevate and report to management changes that are not closed in a timely fashion. 5. Consider the impact of contracted services providers (e.g., of infrastructure, application development and shared services) on the change management process. Consider integration of organizational change management processes with change management processes of service providers. Consider the impact of the organizational change management process on contractual terms and SLAs.				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
AI6.2 Impact Assessment, Prioritization and Authorization 1. Develop a process to allow business process owners and IT to request changes to infrastructure, systems or applications. Develop controls to ensure that all such changes arise only through the change request management process. 2. Categorize all requested changes (e.g., infrastructure, operating systems, networks, application systems, purchased/packaged application software). 3. Prioritize all requested changes. Ensure that the change management process identifies both the business and technical needs for the change. Consider legal, regulatory and contractual reasons for the requested change. 4. Assess all requests in a structured fashion. Ensure that the assessment process addresses impact analysis on infrastructure, systems and applications. Consider security, legal, contractual and compliance implications of the requested change. Consider also interdependencies among changes. Involve business process owners in the assessment process, as appropriate. 5. Ensure that each change is formally approved by business process owners and IT technical stakeholders, as appropriate.				
AI6.4 Change Status Tracking and Reporting 1. Establish a process to allow requestors and stakeholders to track the status of requests throughout the various stages of the change management process. 2. Categorize change requests in the tracking process (e.g., rejected, approved but not yet initiated, approved and in process, and closed). 3. Implement change status reports with performance metrics to enable management review and monitoring of both the detailed status of changes and the overall state (e.g., aged analysis of change requests). Ensure that status reports form an audit trail so changes can subsequently be tracked from inception to eventual disposition. 4. Monitor open changes to ensure that all approved changes are closed in a timely fashion, depending on priority.				
DS5.3 Identity Management 1. Establish and communicate policies and procedures to uniquely identify, authenticate and authorize access mechanisms and access rights for all users on a need-to-know/need-to-have basis, based on predetermined and preapproved roles. Clearly state accountability of any user for any action on any of the systems and/or applications involved. 2. Ensure that roles and access authorization criteria for assigning user access rights take into account: • Sensitivity of information and applications involved (data classification) • Policies for information protection and dissemination (legal, regulatory, internal policies and contractual requirements) • Roles and responsibilities as defined within the enterprise • The need-to-have access rights associated with the function • Standard but individual user access profiles for common job roles in the organization				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
• Requirements to guarantee appropriate segregation of duties 3. Establish a method for authenticating and authorizing users to establish responsibility and enforce access rights in line with sensitivity of information and functional application requirements and infrastructure components, and in compliance with applicable laws, regulations, internal policies and contractual agreements. 4. Define and implement a procedure for identifying new users and recording, approving and maintaining access rights. This needs to be requested by user management, approved by the system owner and implemented by the responsible security person. 5. Ensure that a timely information flow is in place that reports changes in jobs (i.e., people in, people out, people change). Grant, revoke and adapt user access rights in coordination with human resources and user departments for users who are new, who have left the organization, or who have changed roles or jobs.				
DS5.4 User Account Management 1. Ensure that access control procedures include but are not limited to: • Using unique user IDs to enable users to be linked to and held accountable for their actions • Awareness that the use of group IDs results in the loss of individual accountability and are permitted only when justified for business or operational reasons and compensated by mitigating controls. Group IDs must be approved and documented. • Checking that the user has authorization from the system owner for the use of the information system or service, and the level of access granted is appropriate to the business purpose and consistent with the organizational security policy • A procedure to require users to understand and acknowledge their access rights and the conditions of such access • Ensuring that internal and external service providers do not provide access until authorization procedures have been completed • Maintaining a formal record, including access levels, of all persons registered to use the service • A timely and regular review of user IDs and access rights 2. Ensure that management reviews or reallocates user access rights at regular intervals using a formal process. User access rights should be reviewed or reallocated after any job changes, such as transfer, promotion, demotion or termination of employment. Authorizations for special privileged access rights should be reviewed independently at more frequent intervals.				
DS9.1 Configuration Repository and Baseline 1. Implement a configuration repository to capture and maintain configuration management items. The repository should include hardware; application software; middleware; parameters; documentation; procedures; and tools for operating, accessing and using the systems, services, version numbers and licensing details. 2. Implement a tool to enable the effective logging of configuration management information within a repository. 3. Provide a unique identifier to a configuration item so the item can be easily tracked and related to physical				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyperlink	Comments
asset tags and financial records. 4. Define and document configuration baselines for components across development, test and production environments, to enable identification of system configuration at specific points in time (past, present and planned). 5. Establish a process to revert to the baseline configuration in the event of problems, if determined appropriate after initial investigation. 6. Install mechanisms to monitor changes against the defined repository and baseline. Provide management reports for exceptions, reconciliation and decision making.				
DS9.2 Identification and Maintenance of Configuration Items 1. Define and implement a policy requiring all configuration items and their attributes and versions to be identified and maintained. 2. Tag physical assets according to a defined policy. Consider using an automated mechanism, such as barcodes. 3. Define a policy that integrates incident, change and problem management procedures with the maintenance of the configuration repository. 4. Define a process to record new, modified and deleted configuration items and their relative attributes and versions. Identify and maintain the relationships among configuration items in the configuration repository. 5. Establish a process to maintain an audit trail for all changes to configuration items. 6. Define a process to identify critical configuration items in relationship to business functions (component failure impact analysis). 7. Record all assets—including new hardware and software, procured or internally developed—within the configuration management data repository. 8. Define and implement a process to ensure that valid licenses are in place to prevent the inclusion of unauthorized software.				
DS9.3 Configuration Integrity Review 1. To validate the integrity of configuration data, implement a process to ensure that configuration items are monitored. Compare recorded data against actual physical existence, and ensure that errors and deviations are reported and corrected. 2. Using automated discovery tools where appropriate, reconcile actual installed software and hardware periodically against the configuration database, license records and physical tags. 3. Periodically review against the policy for software usage the existence of any software in violation or in excess of current policies and license agreements. Report deviations for correction.				

Appendix E. SAP ERP Audit ICQs

The following internal control questionnaires (ICQs) provide suggested control objectives/ questions to cover for conducting an audit of the three business cycles covered in *Security, Audit and Control Features SAP® ERP: A Technical and Risk Management Reference Guide, 3rd Edition* (Revenue, Inventory and Expenditure), and the SAP Basis component. They also provide references to the relevant COBIT 4.1 control objectives.

Because there may be more than one control per risk, a numbering sequence for risks, controls and testing techniques has been adopted throughout each of the chapters dealing with the auditing of core business cycles or the Basis Application Infrastructure, as shown in the following table.

Numbering Sequence for Risks, Controls and Testing Techniques

Number	Description
Risks	
1.1	Risk number 1 for the first subprocess
1.2	Risk number 2 for the first subprocess
2.1	Risk number 1 for the second subprocess
Controls	
1.1.1	Control number 1 for risk number 1 of the first subprocess
1.1.2	Control number 2 for risk number 1 of the first subprocess
1.2.1	Control number 1 for risk number 2 of the first subprocess
2.1.1	Control number 1 for risk number 1 of the second subprocess
Testing Techniques	
1.1.1	Testing technique for control number 1 for risk number 1 of the first subprocess
1.1.2	Testing technique for control number 2 for risk number 1 of the first subprocess
1.2.1	Testing technique for control number 1 for risk number 2 of the first subprocess
2.1.1	Testing technique for control number 1 for risk number 1 of the second subprocess

Revenue Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**COBIT 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?					DS11
1.1.2 Is access to create and change master data restricted to authorized individuals?					DS5
1.1.3 Have configurable controls been designed into the process to maintain the integrity of master data?					DS9
1.2 Master data remain current and pertinent.					
1.2.1 Does management periodically review master data to check their accuracy?					DS11
1.2.2 Have appropriate credit limits been loaded for customers?					DS2
2. Sales Order Processing					
2.1 Sales orders are processed with valid prices and terms, and processing is complete, accurate and timely.					
2.1.1 Is the ability to create, change or delete sales orders, contracts and delivery schedules restricted to authorized personnel?					AI6 DS5
2.1.2 Has the ability to modify sales pricing information been restricted to authorized personnel (refer to master data integrity 1.1.2)?					DS5
2.1.2 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)?					
2.1.3 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 1.1.3)?					DS9
2.1.4 Are fax orders reconciled periodically between the system and fax printouts to reduce the risk of duplicate orders?					PO8
2.2 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?					DS9

Revenue Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**COBIT References**
	Yes	**No**	**N/A**		
2.3 Order entry data are completely and accurately transferred to the shipping and invoicing activities.					
2.3.1 Are reports of open sales documents prepared and monitored to check for timely shipment?					DS11 ME1
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?					DS6
3.2.1 Are available shipping reports used to assist in controlling the shipping process?					PO11
3.2 Invoices are generated using authorized terms and prices and are calculated and recorded accurately.					
3.2.1 Does the SAP ERP software automatically calculate invoice amounts and post invoices based on configuration data?					AI5
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?					DS5
3.3.2 Is the ability to create, change or delete picking slips, delivery notes and goods issues restricted to authorized personnel?					AI7
3.3.3 Are reports of invoices issued but not posted in FI prepared and investigated promptly?					AI7
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?					DS5
3.5 Credit notes for all goods returned and adjustments to accounts receivable are issued in accordance with organization policy and in a timely manner.					
3.5.1 Are sales order returns and credit request transactions matched to invoices?					

Revenue Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**COBIT References**
	Yes	**No**	**N/A**		
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 organization's policy on credits or returns?					AI2 DS9
4. Collecting and Processing Cash Receipts					
4.1 Cash receipts are entered accurately, completely and in a timely manner.					
4.1.1 Are bank statements reconciled to the general ledger regularly?					
4.1.2 Has the system been configured to not allow processing of cash receipts outside of approved bank accounts?					DS9
4.1.3 Are customer open items and accounts receivable aging reports prepared and analyzed regularly?					AI4
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?					PO4
4.2.1 Is any unallocated cash or amount received that is not cross-referenced to an invoice number immediately followed up with the customer?					DS11
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?					PO8 PO9
4.4 Timely collection of cash receipts is monitored.					
4.4.1 As for 4.1.3, are customer open items and accounts receivable aging reports prepared and analyzed regularly?					PO4 AI4

Expenditure Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**COBIT 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?					PO4 DS11
1.1.2 Is access to create and change master data restricted to authorized individuals?					DS5
1.1.2 Are user accounts validated against HR lists and access in alignment with role requirements?					
1.1.2 Are user accounts reviewed by management in line with organization policy?					
1.1.3 Have configurable controls been designed into the process to maintain the integrity of master data?					DS9
1.1.4 Is a naming convention used for vendor names (e.g., as per letterhead) to minimize the risk of establishing duplicated vendor master records?					DS2
1.2 Inventory master data remain current and pertinent.					
1.2.1 Does management periodically review master data to check their accuracy?					DS11
2. Purchasing					
2.1 Purchase order entry and changes are valid, complete, accurate and timely.					
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?					AI6 DS5
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?					DS2
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)?					AI6
2.2 Goods are received only for valid purchase orders and goods receipts are recorded completely, accurately and in a timely manner.					

Expenditure Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**COBIT References**
	Yes	**No**	**N/A**		
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?					DS6
2.2.1 Does management review exception reports of goods not received on time for recorded purchases?					DS5
2.2.2 Is the ability to input, change or cancel goods received transactions restricted to authorized inbound logistics/raw materials personnel?					DS5
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?					PO4
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?					DS5
3.1.1 Is the ability to input vendor invoices that do not have a purchase order and/or goods receipt as support further restricted to authorized personnel?					DS5
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?					DS9
3.2.2 Is the SAP ERP software configured with quantity and price tolerance limits?					DS9
3.2.3 Is the GR/IR account regularly reconciled?					DS11
3.2.4 Are reports of outstanding purchase orders regularly reviewed?					DS11
3.2.5 Does the SAP ERP software restrict the ability to modify the exchange rate table to authorized personnel?					DS5
3.2.5 Does management approve values in the centrally maintained exchange rate table?					PO6

Expenditure Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**COBIT References**
	Yes	**No**	**N/A**		
3.2.5 Does the SAP ERP software automatically calculate foreign currency translation, based on values in the centrally maintained exchange rate table?					DS11
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?					DS5
4. Processing Disbursements					
4.1 Disbursements are made only for goods and services received and are calculated, recorded and distributed to the appropriate suppliers accurately in a timely manner.					
4.1.1 Does management approve the SAP ERP payment run parameter specification?					PO6
4.1.2 Does the SAP ERP software restrict to authorized personnel the ability to release invoices that have been blocked for payment, either for an individual invoice or for a specified vendor?					DS5

Inventory Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT 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 (using transaction code MM04) of master data additions and changes back to source documentation on a sample basis?					DS11
1.1.1 Do persons independent of day-to-day custody or recording of inventory count physical inventory on a continuous inventory basis?					ME2
1.1.1 Are monthly stock-takes performed?					DS13
1.1.1 Where inventory adjustment forms are used, are they sequentially prenumbered and is the sequence of such forms accounted for?					DS13
1.1.2 Have the creation and maintenance of master data been assigned and restricted to a dedicated area within the organization that understands how they may affect organizational processes and the importance of timely changes?					DS11
1.1.3 Have configurable controls been designed into the process to maintain the integrity of master data?					DS9
1.2 Inventory master data remain current and pertinent.					
1.2.1 Does management periodically review master data to check their accuracy?					DS11
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?					AI6 DS5
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?					PO4
2. Raw Materials Management					
2.1 Inventory is salable, usable and adequately safeguarded.					

Inventory Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
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 organization policies?					DS1 DS3
2.1.1 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?					DS3
2.1.1 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 bonding area and regularly monitored by the quality department personnel to ensure timely return to suppliers?					DS6
2.1.1 Does management review reports of slow-turnover inventory to ensure that it is still salable or usable?					DS11
2.1.1 Do goods inwards/outwards 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)?					DS3
2.1.1 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?					DS3 DS12
2.1.1 Is inventory stored in properly secured (gates locked at night and premises alarmed), environmentally conditioned warehouse locations where access is restricted to authorized personnel?					DS12
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?					DS13

Inventory Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
2.2.1 Are long-outstanding goods receipt notes, purchase orders and/or invoices investigated on a timely basis and accrued as appropriate?					ME2
2.2.1 Are documents cancelled once matched or on payment of the invoice to prevent reuse?					PO8
2.2.1 Does management review exception reports of goods not received on time for recorded purchases?					ME1
2.2.2 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?					PO8
2.2.3 Is the ability to input, change or cancel goods received transactions restricted to authorized inbound logistics/raw materials personnel?					DS5
2.2.4 Do persons independent of day-to-day custody or recording of inventory count physical inventory on a continuous inventory basis?					PO4
2.2.4 Are inventory counts reconciled to inventory records and inventory records reconciled to the general ledger?					PO8
2.3 Defective raw materials 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?					PO4 ME2
2.3.1 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?					DS2
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.					

Inventory Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
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?					DS13
3.1.1 Does management reconcile the inventory-in-transit accounts regularly and do these accounts net off against other plants' outgoing inventory-in-transit accounts?					PO8 DS3
3.1.1 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?					DS13
3.1.1 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?					DS3
3.1.1 Is the ability to create or change bills of material restricted to authorized personnel?					AI6 DS5
3.1.1 Is access to the material transfers and adjustments transactions appropriately restricted to authorized personnel?					AI6 DS5
3.1.1 Is the ability to create or change work centers restricted to authorized personnel?					AI6 DS5
3.1.2 Is the ability to create or change bills of material restricted to authorized personnel?					AI6 DS5
3.1.3 Is access to the material transfers and adjustments transactions appropriately restricted to authorized personnel?					AI6 DS5
3.1.4 Is the ability to create or change work centers restricted to authorized personnel?					AI6 DS5
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 1.1.1)?					PO4

Inventory Business Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
4.1.2 Is the changing of the settlement rules restricted to authorized users (refer to 1.3.1)?					
4.2 Goods returned by customers are accepted in accordance with the organization'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?					PO11 ME1
4.2.1 Does the quality assurance team inspect the goods before a credit note can be issued?					
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?					DS12
4.3.1 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)?					ME1
4.3.1 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?					PO4
4.3.2 Are the SAP ERP reports (delivery due list and owed-to-customer report) of open sales documents prepared and monitored to ensure timely shipment?					DS11
4.3.2 Does the SAP ERP account assignment configuration ensure that amounts for shipped goods are posted to the appropriate COGS account?					

Basis Security Cycle ICQ						
Control Objectives/Questions		**Response**			**Comments**	**COBIT References**
		Yes	**No**	**N/A**		
SAP ERP Control Environment						
A.	**Establish control over information and information systems.**					
A1	Has senior management established policies and standards governing the information systems of the entity?					PO6
A2	Has senior management assigned responsibilities for information, its processing and its use?					PO2
A3	Is user management responsible for providing information that supports the entity's objectives and policies?					PO4
A4	Is user management responsible for the completeness, accuracy, authorization, security and timeliness of information?					PO8 DS11
A5	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?					PO3 DS1 DS3
A6	Does senior management approve plans for development and acquisition of information systems?					PO5
A7	Does senior management monitor the extent to which development/configuration, operation and control of information systems complies with established policies and plans?					ME1
A8	Are there outstanding audit findings from previous years?					ME1 ME2
B.	**Ensure that the information systems selected (whether new implementation or upgrade) meet the needs of the entity.**					
B1	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?					PO5 AI1
B2	Are there procedures to determine costs, savings and benefits before a decision is made to develop or acquire an information system?					AI1
B3	Are there procedures to ensure that the information system being developed or acquired meets user requirements?					AI1
B4	Are there procedures to ensure that information systems, programs and configuration changes are adequately tested prior to implementation?					AI2 AI3

Basis Security Cycle ICQ						
Control Objectives/Questions		**Response**			**Comments**	**COBIT References**
		Yes	**No**	**N/A**		
C.	**Ensure that the acquisition and configuration of information systems (whether new implementation or upgrade) are carried out in an efficient and effective manner.**					
C1	Are standards established and enforced to ensure the efficiency and effectiveness of the systems acquisition and configuration process?					PO10 AI1 AI2
C2	Are there procedures to ensure that all systems are acquired and configured in accordance with the established standards?					AI2
C3	Is an approved acquisition plan (project plan) used to measure progress?					PO10
C4	Do all personnel involved in system acquisition and configuration activities receive adequate training and supervision?					PO7
D.	**Ensure the efficient and effective implementation or upgrade of information systems.**					
D1	Has responsibility been assigned for implementation, configuration and upgrade of information systems?					PO4
D2	Are there procedures to ensure the efficiency and effectiveness of the implementation, configuration and upgrade of information systems?					AI4
D3	Are there procedures to ensure that information systems are implemented, configured and upgraded in accordance with the established standards?					AI3
D4	Is an approved implementation plan used to measure progress?					PO10
D5	Is effective control maintained over the conversion of information and the initial operation of the information system?					AI7
D6	Does user management participate in the conversion of data from the existing system to the new system?					AI7
D7	Is final approval obtained from user management prior to going live with a new implementation and/or upgraded system?					AI7
E.	**Ensure the efficient and effective maintenance of information systems.**					
E1	Are there procedures to document and schedule all planned changes to information systems (including key ABAP programs)?					AI6
E2	Are there procedures to ensure that only authorized changes are initiated?					AI6

Basis Security Cycle ICQ						
Control Objectives/Questions	**Response**			**Comments**	**COBIT References**
	Yes	**No**	**N/A**		
E3 Are there procedures to ensure and verify that only authorized, tested and documented changes to information systems are accepted into the production client?					AI6 AI7
E4 Are there procedures to report planned information systems changes to information systems management and to the users affected?					AI6 DS8
E5 Are there procedures to allow for and control emergency changes?					AI6
E6 Are controls in place to prevent and identify unauthorized changes to information systems (including key ABAP programs)?					AI6 DS5
F. Ensure that present and future requirements of users of information systems processing can be met.					
F1 Are there written agreements between users and information systems processing, defining the nature and level of services to be provided?					DS1
F2 Is there appropriate management reporting within information systems processing?					DS4 ME1
F3 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?					DS3 DS4
F4 Are there procedures/capacity planning activities to examine the adequacy of information processing resources to meet entity objectives in the future?					DS3
F5 Are there periodic planning activities to examine the adequacy of the volume of skilled staff (i.e., operating system, hardware, network, SAP ERP) to support the systems now and in the future?					PO7
F6 Are there procedures for the approval, monitoring and control of the acquisition and upgrade of hardware and systems software?					AI3 DS3
F7 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?					DS3 ME3
F8 If the SAP ERP implementation is not at the most current version, is there a planned upgrade approach?					PO3 AI3 DS3

Basis Security Cycle ICQ						
Control Objectives/Questions		**Response**			**Comments**	**CobiT References**
		Yes	**No**	**N/A**		
G	**Ensure the efficient and effective use of resources within information systems processing.**					
G1	Are budgets for information systems processing activities prepared on a regular basis?					PO5
G2	Are standards established and enforced to ensure efficient and effective use of information systems processing?					PO6
G3	Is there an incident management process that ensures that information processing problems are detected and corrected on a timely basis?					DS5 DS10
G4	Are users of information systems processing facilities accountable for the resources used by them?					DS6
H	**Ensure that there is an appropriate segregation of incompatible functions within the entity.**					
H1	Does the organization structure established by senior management provide for an appropriate segregation of incompatible functions: a. Basis administration b. Transport/import c. Develop program change d. Develop role change e. User security administration f. Change monitoring g. User testing h. Authorize change i. Perform change					PO4
I	**Ensure that all access to information and information systems is authorized.**					
I1	Are there procedures to ensure and verify that information and information systems are accessed in accordance with established policies and procedures?					DS5
J.	**Ensure that information systems processing is protected physically from unauthorized access and from accidental or deliberate loss or damage.**					
J1	Are the database, application and presentation servers located in a physically separate and protected environment (i.e., a data center)?					DS12
J2	Are there procedures to ensure that environmental conditions (such as temperature and humidity) for hardware facilities are adequately controlled?					DS12
K.	**Ensure that information processing can be recovered and resumed after operations have been interrupted.**					
K1	Are there procedures to allow information processing to resume operations in the event of an interruption?					DS4

Basis Security Cycle ICQ						
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
K2 Are emergency, backup and recovery plans documented and tested on a regular basis to ensure that they remain current and operational?					DS4
K3 Do personnel receive adequate training and supervision in emergency backup and recovery procedures?					DS4 DS7
L. Ensure that critical user activities can be maintained and recovered following interruption.					
L1 Are there backup and recovery plans to allow users of information systems to resume operations in the event of an interruption?					DS4
L2 Are all information and resources required by users to resume processing backed up regularly?					DS4 DS11
L3 Do user personnel receive adequate training and supervision in the conduct of the recovery procedures?					DS4 DS7
L4 Are application controls designed with regard to any weaknesses in segregation, security, development and processing controls that may affect the information system?					DS4 DS5
L5 Are there procedures to ensure that output is reviewed by users/management for completeness, accuracy and consistency?					DS4 ME1
L6 Is there some method of ensuring that control procedures relating to completeness, accuracy and authorization are ensured?					DS4 ME2
L7 Are there established policies and procedures for record retention?					PO6 DS4
1. Application Installation (Implementation Guide and Organizational Model)					
1.1 Configuration changes are made in the development environment and transported to production.					
1.1.1 Has access to the Implementation Guide (IMG) in production been restricted?					DS5
1.1.2 Have the production client settings been established to not allow changes to programs and configuration?					DS9
1.2 The Organizational Model has been configured correctly to meet the needs of the organization.					

Basis Security Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
1.2.1 Was the Organizational Model well thought-out and agreed upon early in the implementation and did the relevant organization groups assist with key design decisions?					PO4
1.2.2 Has access to the organization configuration functionality been restricted?					DS5
1.3 Changes to critical number ranges are controlled.					
1.3.1 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)?					DS5
1.3.1 Has the production environment been set so modifications are not possible?					AI6
1.4 Access to system and customizing tables is narrowly restricted.					
1.4.1 Have all of the customized SAP ERP tables been assigned to the appropriate authorization group?					PO4 DS5
1.4.2 Has the ability to modify critical tables been appropriately restricted in the production system?					AI6 DS5
2. Application Development (ABAP/4 Workbench and Transport System)					
2.1 Application modifications are planned, tested and implemented in a phased manner.					
2.1.1 Are appropriate change controls procedures followed for all transports?					AI6
2.1.1 Has the production system change option been set to No Changes Allowed?					AI6
2.1.1 Has the ability to create vs. release change requests been segregated?					PO4
2.2 Customized ABAP/4 programs are secured appropriately.					
2.2.1 Have customized ABAP/4 programs been assigned to authorization groups?					PO4 DS5
2.2.2 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?					AI6
2.3 The creation or modification of programs is performed in the development system and migrated through the test system to production.					

Basis Security Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
2.3.1 Has access to directly change production source code within the production environment been restricted and monitoring established?					AI6
2.4 Access for making changes to the dictionary is restricted to authorized individuals.					
2.4.1 Has the ability to make changes to the SAP ERP data dictionary been restricted and access privileges appropriately assigned based on job responsibilities?					PO4
2.5 Access to modify and develop queries is restricted.					
2.5.1 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?					PO4 DS5
Relevant company codes are set to Productive in the production environment.					
2.6.1 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?					PO4 AI6
3. Application Operations (Computing Center Management System)					
3.1 The Computing Center Management System is configured appropriately.					
3.1.1 Have operation modes, instances and the CCMS timetable been correctly defined, such that the CCMS display is meaningful?					AI2
3.1.1 Is access to the system and start-up profiles tightly controlled?					AI6
3.1.1 Are change procedures followed strictly and changes to the profiles well documented?					AI6 DS11
3.1.1 Has access to the CCMS Alert Monitor been properly secured?					AI6 DS10
3.2 Batch processing operations are secured appropriately.					
3.2.1 Have batch input, batch administration and batch processing capabilities been restricted appropriately?					DS5 DS11

Basis Security Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
3.2.1 Have batch upload programs created to load initial master data and take on balances been deleted from the production environment following go-live?					AI7
3.3 Default system parameter settings are reviewed and configured to suit the organization's environment.					
3.3.1 During implementation, did the organization set the SAP ERP system profile parameters to appropriate values?					AI4
3.4 Critical and sensitive transaction codes are locked in production.					
3.4.1 Have sensitive transaction codes been locked in the production environment and does the organization have procedures for locking and unlocking these transaction codes?					DS5 DS11
3.5 Users are prevented from logging on with trivial or easily guessable passwords.					
3.5.1 Has management set up a list of "illegal" passwords that users are not allowed to use?					DS5 DS13
3.6 SAP Router is configured to act as a gateway to secure communications into and out of the SAP ERP environment.					
3.6.1 Is the network protected by SAP Router and a firewall?					DS5
3.6.1 Are appropriate change management procedures for any modifications to the SAP Router permission table in place and operating?					AI6
3.6.1 Is the SAP Router log file used to monitor remote communications activity?					DS5
3.6.1 Are Secure Network Communications (SNC) and an external security product used to protect the communication among the components of the SAP ERP system?					
3.7 Remote access by software vendors is controlled adequately.					
3.7.1 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?					AI6 DS5

Basis Security Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
3.7.2 Are changes subject to normal testing and migration controls before being implemented on the production system?					AI6
3.8 SAP ERP Remote Function Call (RFC) and Common Programming Interface—Communications (CPI-C) are secured.					
3.8.1 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?					DS5
3.9 The technology infrastructure is configured to secure communications and operations in the SAP ERP environment.					
3.9.1 Has the technology infrastructure been configured to secure communications and operations in the SAP ERP environment? Consider the following areas: • Firewall • Secure Network Communications (SNC) • Secure Store and Forward (SSF) mechanisms and digital signatures • Workstation security • Operating system and database security					PO2 DS5
4. Application Security (Profile Generator and Security Administration)					
4.1 Duties within the security administration environment are adequately segregated.					
4.1.1 Has the organization allocated the security administration function among different individuals?					PO4
4.2 Adequate security authorization documentation is maintained.					
4.2.1 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?					AI7 DS4
4.3 The superuser SAP* is properly secured.					
4.3.1 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?					DS5
4.3.2 Has the system parameter (login/no_automatic_user_ sapstar) been set?					AI6
4.4 Default users are secured properly.					

Basis Security Cycle ICQ					
Control Objectives/Questions	**Response**			**Comments**	**CobiT References**
	Yes	**No**	**N/A**		
4.4.1 Have the passwords for the default users DDIC, SAPCPIC and EarlyWatch been changed from the default?					DS5
4.5 Access to powerful profiles is restricted.					
4.5.1 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?					AI1 DS5
4.5.2 Are procedures in place to ensure that use of the SAP_ALL authority is authorized, approved, logged, monitored and reviewed?					
4.6 The authorization group that contains powerful users is restricted.					
4.6.1 Has the authorization group that contains powerful users been restricted to the new superuser and a backup?					AI3 DS5
4.7 Changes to critical SAP ERP tables are logged by the system and reviewed by management.					
4.7.1 Are all changes to the critical SAP ERP tables logged by the system and does the periodic review of these logs form part of the security procedures for the organization? (Include the list of tables with logging implemented.)					AI6 DS11
4.8 Changes made to the data dictionary are authorized and reviewed regularly.					
4.8.1 Are details of modifications to the data dictionary maintained and change control procedures followed?					AI6 DS11
4.8.2 Are the SAP ERP Data Dictionary Information System reports (DD reports) regularly generated and reviewed by management?					DS11 ME1
4.9 Log and trace files are appropriately configured and secured.					
4.9.1 Is logging appropriately configured and are log and trace files secured at the operating system level at the location specified within the system profile?					DS9

