Technical and Risk Management Reference Series

Security, Audit and Control Features

SAP® ERP

3rd Edition

Excerpt

Table of Contents

1. Forward
2. First section on major SAP Modules and Functionality

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*) (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, control 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.

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*)

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
Tony Hayes, CGEIT, Queensland Government, Australia, Director
Jo Stewart-Rattray, CISA, CISM, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, CSEPS, RSM Bird Cameron, Australia, Director

Acknowledgments *(cont.)*

Assurance Committee 2008-2009
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA, Chair
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia
Richard Brisebois, CISA, CGA, Office of the Auditor General of Canada, Canada
Sergio Fleginsky, CISA, ICI, Uruguay
Robert Johnson, CISA, CISM, CGEIT, CISSP, Executive Consultant, USA
Anthony P. Noble, CISA, CCP, Viacom Inc., USA
Robert G. Parker, CISA, CA, CMC, FCA, Deloittte & Touche LLP (retired), Canada
Erik Pols, CISA, CISM, Shell International—ITCI, Netherlands
Vatsaraman Venkatakrishnan, CISA, CISM, CGEIT, ACA, Emirates Airlines, UAE

Table of Contents

1. Foreword

Enterprise resource planning (ERP) systems, such as SAP ERP, Oracle® E-Business Suite and PeopleSoft® Enterprise, are now pervasive in large enterprises worldwide. An ERP system is a packaged business software system that allows an enterprise to:
- Automate and integrate the majority of its business processes
- Share common data and practices across the entire enterprise
- Produce and access information in a real-time environment

ERP systems continue to transform enterprise business processes by automating manual tasks, such as authorizations, and empowering users to initiate transactions and monitor performance online. As a result, the integrity framework supporting these business processes has been transformed. The level of automated controls and the importance of logical access security and configuration controls have increased. The web enablement of ERP systems and the integration of back-end ERP systems with front-end web-enabled systems continue to transform business process and technical infrastructure risk/control frameworks.

SAP is one of the developers of enterprise applications. Its primary ERP product is SAP ERP Central Component (known as ECC but previously named SAP R/3). This third edition of the technical reference guide on the audit of SAP ERP is one in a series of three technical reference guides providing information relating to the world's three major ERP systems. The other guides in the series focus on Oracle E-Business Suite and PeopleSoft.

Some sections of the guides covering the introduction to ERP and strategic risk management in an ERP environment and directions in ERP audit are common to all three guides. The remaining sections covering ERP product-specific characteristics and auditing techniques are unique to each of the respective technical reference guides.

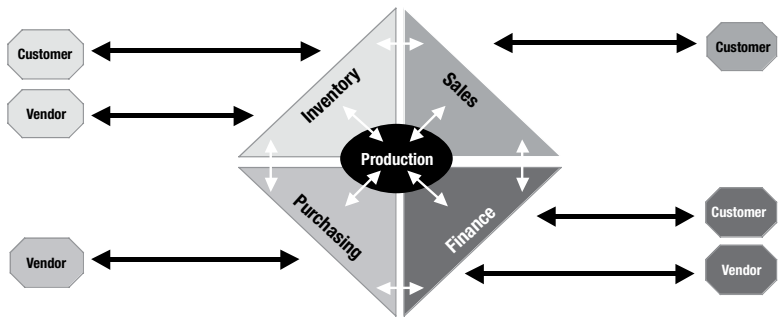
The purpose of the third edition of this research is to update the current best practices and identify future trends in ERP risk and control. The objective is to enable audit, assurance, risk and security professionals (IT and non-IT) to evaluate risks and controls in existing ERP implementations and to facilitate the design and building of better practice controls into system upgrades and enhancements. The publication is designed to be a practical how-to guide based on SAP ECC versions 5.0 and 6.0. However, most of the features and testing techniques described are also applicable to the earlier versions of SAP R/3, namely 4.6c and 4.7, which are also described in the first and second editions of this guide.

The popularity of the earlier editions of this guide confirmed the need for a series of audit guides for these products. Using a definitive approach, the authors sought to provide detail on testing techniques within the ERP products and their execution, rather than generic descriptions of the audit tests to be performed.

2. Introduction to Enterprise Resource Planning Systems and SAP ERP

Before ERP systems were developed, an enterprise's systems typically were set up around functions or departments (e.g., sales, purchasing, inventory, finance), as shown in **figure 2.1**, and not around the business processes (e.g., purchase-to-pay, order-to-cash). Functions evolved independently from each other. Each function may have had an individual application system or a number of systems to support it, with or without interfaces among the systems. This approach resulted in time delays, additional cost, the need for reconciliation, and data redundancy. Frequently, business controls had a significant manual component. Before the widespread use of ERPs, it was common for purchase orders (POs), for example, to be approved when generated. When the invoice arrived, the PO was either printed out again or retrieved from filing and then stapled to the invoice. The invoice was then approved for payment. The documents may have been scrutinized once again and approved during the check payment process.

Figure 2.1—Traditional Environment



- Functions are separate.
- Interface and communication links with other functions
- Variety of systems
- Each function maintains its own master data.
- Duplication of data entry

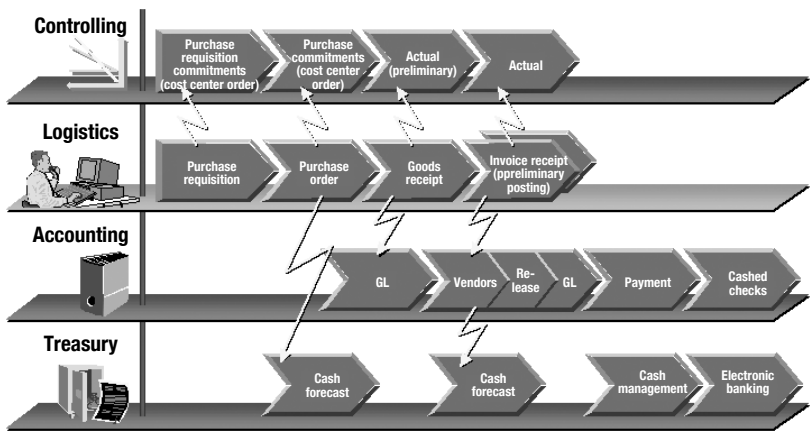
Non-ERP systems also suffer from a design problem. Typically, they are designed around disparate and independent modules that transmit transaction data among themselves by means of interfaces, where the information is normally summarized (e.g., totals or balances only). In such cases, further details of individual transactions often are difficult to ascertain, unlike the ability to drill down provided by ERP systems.

ERP systems have a business process focus. They grew out of the need to integrate separate sales operations planning (SOP) systems, materials resource planning

(MRP) systems (used to integrate material requirements with production, demand and capacity) and financial accounting systems in manufacturing organizations. The integration of these functional capabilities into an online and real-time application system designed to support end-to-end business processes enables enterprises to plan and optimize their resources across the enterprise. Their relational database tables are designed around a complete set of the core functions for an enterprise rather than disparate modules that merely pass transaction data from one module to another. In particular, with the SAP ERP software the Financial Accounting and Controlling modules are tightly integrated into the logistical chain that begins with purchasing and ends in sales and distribution. Every business transaction is recorded in the Financial Accounting and Controlling (or Management Reporting) modules automatically, if configured correctly. For example, consider the purchase of inventory in the SAP ERP software:

- A purchase requisition in the Procurements and Logistics Execution (MM) module creates a commitment in the Financial and Management Accounting, Controlling (CO) module, as shown in **figure 2.2**. This purchase requisition also can be evaluated in the Controlling component.
- The placement of the purchase order (MM module) will then confirm the commitment in CO and in the Treasury Applications (CM) module simultaneously.
- Entering the receipt of the goods ordered in MM will generate an accounting document in Financial and Management Accounting (FI), General Ledger (GL) and CO. The receipt will also update the material masters (stock records) in MM.
- Receipt of the invoice will generate an accounting document in FI accounts payable and also updates CO and CM.

Figure 2.2—ERP Process: Accounts Payable



An ERP environment operates in line with the business, online and in real time. Management has access to online and up-to-date information on how the business is performing. Common and consistent information is shared among application

modules and among users from different departments simultaneously. It has been observed that following implementation of an ERP, enterprises typically report completion of period or year-end closes in one or two days, as opposed to two to three weeks under their legacy system environment. Another key change brought about by the implementation of ERP systems is that the systems are owned and driven by business process owners/end users, with the technical support of information technology, rather than being owned and driven by the IT function alone.

Enterprises implementing ERP systems can achieve significant benefits such as:
- Reductions in inventory
- Redeployment of personnel into more value-producing activities
- Productivity improvements
- Order management cycle improvements
- Financial close/cycle reduction
- IT cost reduction
- Procurement cost reductions
- Cash management improvement
- Transportation/logistics cost reductions
- Hardware and software maintenance reductions
- On-time delivery improvements

The intangible benefits of an ERP implementation—while difficult to quantify—can deliver significant business value through improved enterprise capabilities, including:
- Information/visibility (e.g., drill-down capability, consistent and reliable information across business areas)
- New/improved processes
- Improved customer responsiveness
- Integration and standardization
- Flexibility
- Globalization

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 stands for "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. Although SAP NetWeaver is not covered extensively in this book, it may be in future ISACA publications. The current core ERP solution offered by SAP is called SAP Enterprise Central Component (ECC 6.0), which is referred to in this book as SAP ERP, and will be the key focus of this book. **Figure 2.3** provides an overview of the SAP ERP architecture.

Figure 2.3—SAP ERP Architecture