IS AUDITING GUIDELINE
ENTERPRISE RESOURCE PLANNING (ERP)
SYSTEMS REVIEW DOCUMENT G21

Introduction—The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of the Information Systems Audit and Control Association® (ISACA®) is to advance globally applicable standards to meet this need. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community.

Objectives—The objectives of the ISACA IS Auditing Standards are to inform:
- IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics for IS auditors
- Management and other interested parties of the profession’s expectations concerning the work of practitioners

The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.

Scope and Authority of IS Auditing Standards—The framework for the ISACA IS Auditing Standards provides multiple levels of guidance:
- Standards define mandatory requirements for IS auditing and reporting.
- Guidelines provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.
- Procedures provide examples of procedures an IS auditor might follow in an audit engagement. Procedures should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtain the same results. In determining the appropriateness of any specific procedure, group of procedures or test, IS auditors should apply their own professional judgment to the specific circumstances presented by the particular information systems or technology environment. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements.

The words audit and review are used interchangeably. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.htm.

The ISACA Code of Professional Ethics require members of ISACA and holders of the Certified Information Systems Auditor™ (CISA®) designation to comply with IS Auditing Standards adopted by ISACA. Failure to comply with these standards may result in an investigation into the member’s or CISA holder’s conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

Development of Standards, Guidelines and Procedures—The ISACA Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board also seeks out those with a special expertise or interest in the topic under consideration for consultation, where necessary.

The following CobiT™ resources should be used as a source of best practice guidance:
- Control Objectives—High-level and detailed generic statements of minimum good control
- Control Practices—Practical rationales and how-to-implement guidance for the control objectives
- Audit Guidelines—Guidance for each control area on how to: obtain an understanding, evaluate each control, assess compliance, and substantiate the risk of controls not being met
- Management Guidelines—Guidance on how to assess and improve IT process performance, using maturity models, metrics and critical success factors

Each of these is organised by the IT management process, as defined in the CobiT Framework. CobiT is intended for use by businesses and IT management as well as IS auditors. Its usage allows for the understanding of business objectives and for the communication of best practices and recommendations around a commonly understood and well-respected standard reference.

The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to help identify emerging issues requiring new standards. Any suggestions should be e-mailed (research@isaca.org), faxed (+1.847.253.1443) or mailed (address at the end of this guideline) to ISACA International Headquarters, for the attention of the director of research standards and academic relations.

This material was issued on 1 May 2003.

Information Systems Audit and Control Association 2002-2003 Standards Board
Chair, Claudio Cilli, CISA, CISM, Ph.D., CIA, CISSP KPMG, Italy
Claude Carter, CISA, CA Nova Scotia Auditor General’s Office, Canada
Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay
Alonso Hernandez, CISA, ROAC Colegio Economistias, Spain
Marcelo Hector Gonzalez, CISA Central Bank of Argentina Republic, Argentina
Andrew MacLeod, CISA, FCPC, MACS, PCP, CIA Brisbane City Council, Australia
Peter Niblett, CISA, CA, MIIA, FCPC Day Neilson, Australia
John G. Ott, CISA, CPA Aetna, Inc., USA
Venkatakrishnan Vatsaraman, CISA, ACA, AICWA, CISSP Emirates Airlines, United Arab Emirates
1. **BACKGROUND**

1.1 **Linkage to ISACA Standards**

1.1.1 ISACA IS Auditing Standards, as well as certain of the IS Auditing Guidelines, have direct relevance to the IS auditor’s audit work on ERP systems or ERP system implementation projects.

1.1.2 For example, in accordance with Standard S6 Performance of Audit Work, supervision of the performance of ERP related audit work by subordinate IS or other audit staff for the IS auditor must be subject to sufficient appropriate supervision by the IS auditor.

1.1.3 Further, in those circumstances where the IS auditor is requested or required to be involved in nonaudit roles associated with the ERP systems or implementation project, in addition to the IS Auditing Standards and Guidelines related to S2 Independence and G12 Organisational Relationships and Independence, the IS auditor should review and appropriately consider the applicability of the ISACA Standards for IS Control Professionals.

1.1.4 If the IS auditor is to be involved from an audit or a nonaudit role perspective in the business process reengineering (BPR) activities associated with the implementation and use of an ERP system, ISACA’s IS Auditing Guideline G26 Business Process Re-engineering should be reviewed.

1.1.5 In addition to the pronouncements of ISACA’s Standards Board, its Research Board has or has had a number of projects and deliverables, which are available through the ISACA website (www.isaca.org) and may be of interest to the IS auditor depending on the specific ERP product and other resources being used.

1.2 **Linkage to CoBiT**

1.2.1 The CoBiT Framework states, “It is management’s responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control.”

1.2.2 The CoBiT Management Guidelines provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

1.2.3 The Management Guidelines provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

1.2.4 The Management Guidelines can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

1.2.5 CoBiT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in CoBiT applicable to the scope of the particular audit is based on the choice of specific CoBiT IT processes and consideration of CoBiT’s information criteria.

1.2.6 Refer to the CoBiT reference located in the appendix of this document for the specific objectives or processes of CoBiT that should be considered when reviewing the area addressed by this guidance.

1.3 **Need for Guideline**

1.3.1 ERP systems, which evolved out of manufacturing resource planning systems for the manufacturing industry, use data from a wide range of business areas to provide cross-departmental management and process information. The term ERP is no longer about just planning, rather it refers to core critical business processes of an organisation. Despite principal usefulness of the concept, ERP system implementations can fail to deliver expected results if not adequately managed and controlled. Further, there are emerging trends and changing technologies that support expanded use of ERP systems (such as, web-enabled customer interfaces), which will increase the importance of the security and control consideration for ERP.

1.3.2 The audit of an ERP system requires the IS auditor to have specific knowledge and an understanding of the complex features and integrated processes built into and required for the successful implementation, use and control of specific vendor products.

1.4 **Application of Guideline**

1.4.1 When applying this guideline, the IS auditor should consider its guidance in relation to other ISACA standards and relevant guidelines. The guideline is written as generic rather than a product-specific guidance. The IS auditor will need to consider and adapt the guidance depending on the ERP system and other products/procedures being used.

1.4.2 This guideline sets out information and suggests how the IS auditor should comply with the ISACA Standards and CoBiT when involved in the audit or review of an ERP system or ERP system implementation project.

2. **ENTERPRISE RESOURCE PLANNING (ERP) SYSTEMS**

2.1 **Definitions**

2.1.1 Enterprise resource planning is used, first, to denote the planning and management of resources in an enterprise. Second, it denotes a software system that can be used to manage whole business processes, integrating purchasing, inventory, personnel, customer service, shipping, financial management and other aspects of the business. An ERP system typically is based on a common database, various integrated business process application modules and business analysis tools.

2.2 **Risks and Control Challenges for Implementation of ERP Systems**

2.2.1 ERP systems are implemented to support the operations of an enterprise and, to be successful, must be fully integrated into all
the significant processes and procedures that together enable the enterprise to work effectively. Given the integrated nature of ERPs, they can further add to the risks or challenges of an organisation related to:

- Industry and business environment
- User or management behaviour
- Business processes and procedures
- System functionality
- Application security
- Underlying infrastructure
- Data conversion and integrity
- Ongoing maintenance/business continuity

2.2.2 The risks associated with the implementation and ongoing use of an ERP system cannot be determined or controlled by review of application or technical risks in isolation, but must be considered in conjunction with the business process control objectives of the organisation being served. The challenge to the IS auditor is, therefore, obtaining an understanding of the business and regulatory environment in which the organisation operates and being skilled in the identification of quantifiable application or technical risks and less quantifiable procedural or behavioral risks.

2.2.3 Typically in a large organisation where the quantum of data processed by the ERP is extremely voluminous, the analysis of patterns and trends proves to be extremely useful in ascertaining the efficiency and effectiveness of operations. Most ERPs provide opportunities including specific tools for such extraction and analysis. The use of data analysis tools within the ERP can assist the IS auditor throughout the ERP’s life cycle (i.e., pre- and post-implementation).

2.3 Business Process Reengineering (BPR) and ERP Implementation

2.3.1 BPR and ERP Implementation projects can be thought of as being independent initiatives. In theory, each project could exist within an organisation without the other. In practice, they are often both in process at the same time in an organisation and influenced by and dependent on each other in a myriad of complex relationships often including common design for key business processes. An ERP might be selected to replace an existing system, and the execution of a BPR may be delayed. A BPR might be in place but terminate prior to completion, and an included ERP implementation might continue.

2.3.2 BPR and ERP implementations are often at different stages of their development. A BPR project may be started and several months into the project when it is concluded that an ERP is required to support the new processes, an acquisition project commences. Similarly, a business decision might have been made to acquire a new IT system and an ERP chosen. During the implementation process it may be recognised that the ERP would enable a business reengineering and a BPR initiative’s commencement.

2.3.3 The IS auditor’s primary focus should be with an ERP implementation. However, a concurrent BPR may introduce new risks to the implementation process and often change existing risks, such as:

- The changes proposed by a BPR may require the people affected to behave in a different manner and may engender support, concern and/or even hostility within an organisation. This may be transferred to the ERP implementation project.
- The BPR may drain organisation resources from the ERP implementation.
- Even if the above two risks have no effect on the ERP implementation, unfamiliarity with new processes introduced by the BPR might lead to inadequate process description and suboptimal configuration of the ERP.
- The BPR and ERP may not be well integrated leaving, at best, suboptimal performance and unnecessary expenses.
- Using an ERP as a “change lever” may distract from the BPR. With new, more powerful technology there is a temptation to adopt a process simply because the new technology “can do it,” rather than because it is the optimum business process.

2.3.4 The common steps when performing BPR with special attention to those steps where IT can have a strong effect are as follows:

- Analysis phase—The existing processes, the information and the IT systems currently in use are analysed and, the processes that need to be reengineered are identified. As the use of information and IT can be the levers for dramatic changes in the organisation processes, the IS auditor can provide useful contributions in the early stages of the BPR process.
- Redesign phase—The new processes are redesigned, new information or new ways to use existing information are searched, and the blueprint of the new business system is defined. The “to be model” of the new workflow, as well as how the new information is to be shared across functional areas of the business and the new IT system specifications, can be areas for IS audit coverage.
- Transformation phase—The migration strategy is developed; the migration action plan is created and then executed. The transformation of the IT systems, the introduction of new information and new technologies, and the discarding of old information and IT systems, can be areas for IS audit coverage.

2.4 Application and Use of CoIT

2.4.1 CoIT can be applied in many ways while reviewing ERP systems. The relevance of the various control objectives will differ from organisation to organisation as will the needs of the control structures of such organisations. However a good beginning to applying CoIT during the review would be to address the management IT concerns regarding enterprise packaged solutions (refer to the CoIT Implementation Guide). The Gartner Group has identified some specific concerns of management regarding ERP systems, including:

- Failure to meet user requirements
- Failure to integrate
- Incompatibility with technical infrastructure
- Vendor support problems
- Expensive and complex installations

2.4.2 Relevant control objectives that have been identified by ISACF can be used to address the previously mentioned concerns. In
addition, the IS auditor also could draw up engagement-specific control objectives and engagement-specific audit procedures for these specific control objectives.

3. ACHIEVING EFFECTIVE COMPLIANCE WITH IS AUDITING STANDARDS

3.1 Introductory Comments
3.1.1 For the IS auditor’s initial exposure to, or role in, an ERP system or ERP system implementation project, ISACA’s IS Auditing Standards and IS Auditing Guidelines are very relevant and should be considered and appropriately adhered to by the IS auditor. The IS auditor would be well served to complete a thorough review and analysis of these audit standards and guidelines within the context of the planned role or work on an ERP system and related initiatives.

3.1.2 For purposes of this guideline, only certain of the more relevant IS Auditing Guidelines are specifically referenced. ERPs provide various opportunities for the IS auditor and risks for management that need to be addressed with care and planning. The planning stage for an ERP system or implementation review is critical to a successful audit and sign-off.

3.1.3 The audit of an ERP system or implementation calls for a strategically different approach by the IS auditor. ERPs integrate diversified business processes and, accordingly, may be implemented in conjunction with the conduct of a BPR project. As part of this reengineering, critical control procedures, once used to protect the finances and operations of an organisation, may be changed or eliminated, resulting in entirely new control structures/procedures and related risks.

3.1.4 For ERP systems or implementation projects, the IS auditor also must reengineer the way audits are performed. Risks will have undergone a transformation with regard to the intensity, diversity and the means through which they can occur. These risks arise to some extent due to the integrated program logic and business process functions inherent in ERP software products. Additionally, many of the legacy controls will no longer be applicable, and as such, the IS auditor will need to identify the new control structure.

3.1.5 In planning an IS audit of an ERP system, the IS auditor should give serious consideration to dividing the audit into sections and auditing the sections sequentially, the audit of a whole ERP is a considerable undertaking and may strain IS or other audit resources.

3.2 Audit Charter
3.2.1 The audit charter of the IS audit function may need to be modified as a result of an organisation’s decision to implement an ERP system. For example, BPR considerations associated with effective implementation of an ERP system could require the IS auditor’s scope of work or relationships with other audit functions (such as, financial, operational) to be expanded and more closely integrated (such as, a joint or collaborative audit initiative).

3.2.2 The planned scope for audit by the IS auditor should be defined in accordance with the IS audit charter.

3.2.3 It is imperative that the organisation’s senior and system management fully understand and support the IS auditor’s role(s) as it relates to the ERP system or implementation project. The IS Auditing Guideline G5 Audit Charter, should be reviewed and considered within the context of the ERP system and related initiatives of the organisation.

3.3 Independence
3.3.1 If the IS auditor is to perform or be responsible for nonaudit roles associated with the ERP system or an ERP system implementation project, IS auditing guideline G17 Effect of Nonaudit Role on the IS Auditor’s Independence, should be reviewed and adhered to appropriately.

3.3.2 If the IS auditor is to have a nonaudit role in an ERP system or related initiatives, the IS auditor also should review and appropriately adhere to ISACA’s IS Control Professional Standards.

3.4 Competence
3.4.1 The IS auditor’s long-term audit strategies and plans for an organisation using ERP systems should include aspects that will support the ongoing development and maintenance of IS audit and the IS auditor’s competence as it relates to the ERP. This would include enhancements to the level of skills and knowledge (standard S4) and continuing professional education (standard 040.020).

3.4.2 If an IS auditor does not have the required skills to undertake an IS audit of an ERP system or implementation project, the IS auditor should consider contracting out the audit to a qualified IS auditor. It would be appropriate to include in the contract a requirement for knowledge transfer.

3.4.3 Skills for auditing an ERP system implementation can be acquired by taking ERP audit or product training, getting on the job experience, participating in ERP areas or audit groups.

3.4.4 Specific product-related training and experience (such as, terminology for specific ERP products may be different or mean different things) can be acquired through hands on use and inquiry or observation. Background interviews or briefing by IS management, technical staff and users responsible for the system can assist the IS auditor in understanding the security, control and processing features or risks of the specific ERP system.

3.4.5 The appendix to this guideline provides further guidance on how to address competency gaps.

3.5 Planning

3.5.1 At the outset of an IS audit of an ERP system or ERP system implementation project, the IS auditor should invest sufficient time and effort gathering background knowledge and understanding of the organisation’s existing/planned deployment and gaining control of the ERP system and related resources. The IS auditor would achieve this through product research, direct inquiry of management and other staff, as well as document review procedures.

3.5.2 More specifically, the appendix provides a general overview of the elements of, and basic questions on, an ERP system implementation that the IS auditor may need to consider.

3.5.3 Although ERP systems and implementations are likely to be more integrated and complex than other business systems the IS auditor may have encountered, they involve many organisational management, environmental, application, control considerations and risks similar to the more traditional systems and implementation projects.

3.5.4 It is of particular note that the areas in which an IS auditor might be involved during the audit of an ERP project cover all aspects of an enterprise’s operations. The complete audit of an ERP system will, therefore, require a very broad skill set that is unlikely to be found in one person or one auditing discipline. It is vitally important that the correct mix of auditing skills are involved in an ERP audit review. Audit skills and/or resources from financial, operational and regulatory areas may be needed to complement the IS auditor’s skills.

3.5.5 It is important during planning to consider which, if any, of the ERP processes are extended to the web. With many organisations extending business over the web via enterprise portals and web-based applications on new mobile computing tools, the IS auditor must determine if the ERP being audited fits into this category (i.e., intranet, extranet or Internet). This will affect the performance of audit work and may extend the boundaries of the ERP.

3.5.6 IS auditors should obtain reasonable assurance that management is aware of, and satisfied with, the scope of the audit work to be performed.

3.6 Performance of Work

3.6.1 The IS auditor can use various tools and techniques to audit an ERP environment to address entire populations, flag potential risks and efficiently perform a review. Often the initial design of controls for an ERP system falter over time. Combine this with an evolving environment in which the ERP not only interfaces to/from non-ERP systems, but also may serve as a web-enabled application—where the boundaries of the processes extend beyond the ERP itself, and it becomes apparent that tools and techniques should be considered for:

- Data mining and analysis—ERP products ordinarily come with robust audit related reports, and where these do not exist third-party tools may be used to identify and analyse critical data or samples.
- Separation of duties analysis/authorisation analysis—Information is not restricted to disparate departmental systems, rather the integrated nature of an ERP system results in a high level of risk around security and access privileges. Business rules can be used to identify cases where potential security concerns are flagged for review.
- Workflow/report delivery—Workflow within ERPs can be utilised to deliver exception reports to key individuals for analysis and review. Given that the information is available in real time, root cause analysis is much less complex and corrective business measures can be initiated.
- Upgrades/control intelligence—ERP product suppliers continue to invest in research and development leading to new or enhanced functionality, not to mention ongoing corrections to existing functionality. It is vital the organisation, including the IS auditor, remain current on the ERP’s latest functionality, capacity management and control capabilities. Tools exist to stay abreast on the technical control settings that are available within the ERP whether it is part of the original implementation or an upgrade.

3.6.2 An audit of an ERP could provide assurance covering the area of process integrity. Specific matters to consider are:

- Identify control objectives for processes being implemented.
- Identify and assess potential business risks and financial risks in the processes being implemented.
- Develop and design the most effective and efficient ways of controlling these risks (which implementers generally do not focus on or do not have the expertise to develop).
- Perform an independent analysis of key business activities, comparing organisation processes to leading practices and recommending process improvements.
- Provide assurance that the controls within ERP are appropriate and effective.
- Review the interfaces feeding into ERP from non ERP systems (such as, including legacy, web-based and mobile computing applications).
- Perform audit tests focusing on business process and internal control. Many organisations reengineer business processes during ERP implementation.

ERP Systems Review Guideline Page 5
Review business continuity plans and provide reasonable assurance they have been tested.

3.6.3 An audit of an ERP could provide assurance covering the area of application security. Specific matters to consider are:
- Review standard ERP parameters, including application controls, authorisations and standard security configuration.
- Assess application security to allow processing in an efficient and controlled manner, while protecting valuable data.
- Assess configuration decisions to help provide reasonable assurance of the integrity of business processes and application security.
- Review design documentation for appropriate security and control.
- Assess the security administration process to provide reasonable assurance that access granted is appropriately identified, evaluated and approved.
- Many business processes may be extended out over the intranet, extranet or Internet. The IS auditor should provide reasonable assurance that security processes appropriately address these risks.

3.6.4 An audit of an ERP could provide assurance covering the area of infrastructure integrity. Specific matters to consider are:
- Identify the potential configuration and security risks for the infrastructure components (i.e., hardware, operating system, database management software, networking hardware, Internet and intranet) supporting the application software package.
- Review the ability of the organisation’s IT infrastructure to support the organisation’s practices and future operational goals.
- Identify internal system architecture issues that may cause performance, availability or data integrity challenges.
- Review business recovery plans and provide reasonable assurance they have been tested.

3.6.5 An audit of an ERP could provide assurance covering the area of implementation integrity. Specific matters to consider doing are:
- Provide reasonable assurance of a smooth transition to the new ERP environment, with minimal effect on employees, and without any loss in confidence as to the integrity, security and accuracy of data.
- Identify potential risks connected with the transfer of data from the legacy systems to the new production environment and interfaces with other systems.
- Test and assess the functionality, controls and readiness before “go-live”.
- Assess data quality.
- Assess data conversion and integrity strategies and control procedures.
- Assess testing plan(s) for completeness and for appropriate security and integrity.
- Confirm that testing has involved the intended user community and that the new ERP owner is satisfied that user acceptance is complete.
- Provide independent review of training for completeness of business process and security considerations.
- Provide post-implementation review of effectiveness of the control and security environment and the overall management of the implementation process.
- Assess exception reporting.

3.6.6 The auditing of the ERP implementation can be carried out any time in the life cycle of the project by auditing what has been done until that time and what is planned for the future. Ideally the audit would involve review either on a continuous basis or at several points during the project’s life cycle. To this end, the IS auditor needs an audit framework that addresses the most critical implementation areas where often major risks are hidden, for instance:
- Project management
- Quality management
- Benefit management
- Risk management
- Change management

3.6.7 Project management consists of four phases:
- Management planning—When the project is initiated a management plan is developed, proposed benefits agreed, the project’s scope and the structure of the project are defined.
- Project implementation—Throughout the course of the project the key project management activities of work planning, resource management, project control, project reporting and communication are conducted.
- Project completion—The project should have a predefined and easily identified end point where the ERP system moves from the implementation phase to live operations.
- Derivation of benefit—After implementation, the management of the project changes in nature and transfers to the business owner who has the responsibility for ensuring that the required changes to user behaviour are introduced and benefits obtained.

3.6.8 The project management of an ERP system does not differ significantly or fundamentally from the management of any other large software project. The same concepts apply in the audit of the management of an ERP system implementation, such as:
- Perform an assessment of executive sponsorship and top management support.
- Perform an independent review and analysis of project management activities.
- Independently assess project planning and control as well as quality assurance.
- Provide management the findings regarding resolution of project issues, including time or budget overruns, functionality gaps, and staffing and skill requirement mismatches, as well as other issues relevant to the management of the project.

3.6.9 Quality management, which should be an integral part of all software projects, should not be concerned solely with the quality of the project deliverables, but should cover all activities and deliverables of the ERP projects, such as project planning, design documentation, specifications, procedures, training materials and implementation plans. The quality assurance, which should be carried out as an independent function inside the project organisation, should not be considered an audit activity. On the other hand, during the ERP system implementation, it is essential to audit the effectiveness of the quality management and the quality
assurance.

3.6.10 The business case and the associated benefit realisation plan are the key focal points for the audit of benefit management. They should identify:
- The business objectives of the project and the expected benefits to be achieved. The benefits (both quantitative and non-quantitative) should be specified clearly in a benefits register. The quantified benefits should be broken down into identifiable and measurable elements.
- The planning for the realisation of the benefits and their correlation with the change management of the business processes
- The control procedures, to provide reasonable assurance of the benefits achievement

3.6.11 A benefit management audit that is conducted before the start of the ERP system implementation has the potential to yield significant benefits for a successful ERP project. A benefit realisation review should be conducted some time after the project is completed (typically 18 months).

3.6.12 Risk management is more than just the management of project risks; it is also the management of the risks that the ERP project may place on the business. The IS auditor should be concerned with different types of risk management:
- Risk management relevant to the business processes to be reengineered
- Risk management associated with the project management; the project risks can be either:
  - Inherent, which result from the nature of the project objectives and scope
  - Acquired, which result from the selected methodologies, tools, technique, skills and experience that are applied to the project and to the risk management
- Information security management during the system implementation
- Information security management that is planned after the go live, i.e., during the system operations
- Management of the risks introduced by systems that are external to the ERP project and the risks that the ERP project can cause to third parties. Therefore, the IS auditor should have an enterprise approach that transcends a narrow focus on the specific ERP project.

3.6.13 Organisation realignment, communication, project marketing and personnel training are the key activities for successful project management. The IS auditor also should evaluate, in addition to the previously mentioned activities, the correlation of change management with the other critical implementation areas, especially benefit management (with regard to the benefits to achieve) and risk management (with regard to the potential resistance to change and the information security that is associated with the authorisation of persons according to their newly defined roles). Benefits derived from an ERP implementation ordinarily require that new processes to be designed into the functionality provided by the application, prior to implementation, and that users change their behaviour to suit the newly designed processes after implementation. Audit of the derivation of business benefit, therefore, will continue after the traditional ERP project has been closed.

3.7 Reporting

3.7.1 The reporting processes for stating audit opinion and/or providing audit comment on an ERP project are not inherently different from any other audit reporting processes. Some, or all, of the following reporting mechanisms may be appropriate:
- Regular summary reports to ERP project management meetings or steering committee meetings (perhaps as agenda items)
- Maintenance of a project log tracking audit issues for clarification or control points for resolution
- Formal reports of audit opinion and outstanding issues at defined stages in the project life cycle

4. EFFECTIVE DATE

4.1 This guideline is effective for all information systems audits beginning 1 August 2003. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.htm.

APPENDIX

CoeIT Reference
Selection of the most relevant material in CoeIT applicable to the scope of the particular audit is based on the choice of specific CoeIT IT processes and consideration of CoeIT’s information criteria.

This Guideline has been drafted to avoid limiting its’ application to a particular brand of ERP. It has also been drafted to cover all aspects of an ERP’s use within an organization. Therefore the guideline can be linked to all four of CoeIT’s Domains, Planning and Organization, Acquisition and Implementation, Delivery and Support and Monitoring.

Should a particular audit project be limited by its’ project charter to one aspect of a particular ERP in a particular business entity then, of course, the applicable CoeIT domains and business processes would be correspondingly limited. To illustrate this, the following two examples are provided. These are not intended to be exhaustive and the particular scope of an audit might reasonably alter which processes ought to be included.

Example 1:
An Audit/Review of the Planning and Acquisition of an ERP
Planning and Organization

- PO1 Define a strategic IT plan
- PO2 Define the information architecture
- PO3 Determine the technological direction
- PO4 Define the IT organization and relationships
- PO5 Manage the IT investment
- PO6 Communicate management aims and direction
- PO7 Manage human resources
- PO8 Ensure compliance with external requirements
- PO9 Assess risks
- PO10 Manage projects
- PO11 Manage quality

Acquisition and Implementation

- AI1 Identify solutions
- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology architecture
- AI4 Develop and maintain IT procedures

Example 2: An Audit/Review of a mature ERP system;

Planning and Organization

- PO4 Define the IT organization and relationships
- PO5 Manage the IT investment
- PO7 Manage human resources
- PO8 Ensure compliance with external requirements
- PO9 Assess risks
- PO11 Manage quality

Acquisition and Implementation

- AI2 Acquire and maintain application software
- AI3 Acquire and maintain technology architecture
- AI4 Develop and maintain IT procedures
- AI6 Manage changes

Delivery and Support

- DS1 Define service levels
- DS2 Manage third-party services
- DS3 Manage performance and capacity
- DS4 Ensure continuous service
- DS5 Ensure system security
- DS6 Identify and attribute costs
- DS7 Educate and train users
- DS8 Assist and advise IT customers
- DS9 Manage the configuration
- DS10 Manage problems and incidents
- DS11 Manage data
- DS12 Manage facilities
- DS13 Manage operations

Monitoring

- M1 Monitor the processes
- M2 Assess internal control adequacy
- M3 Obtain independent assurance
- M4 Provide for independent audit
### ERP Knowledge and Skill Requirements

<table>
<thead>
<tr>
<th>Background knowledge of the IS auditor</th>
<th>ERP System</th>
<th>Implementation Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>An understanding of financial and management controls and control risks generally</td>
<td>A thorough understanding of the application of professional IS auditing standards</td>
<td>An understanding of project management practices and controls generally</td>
</tr>
<tr>
<td>A thorough understanding of IT related controls and control risks in the following areas:</td>
<td>IT environment</td>
<td>An understanding of project management practices and controls in the area of IT</td>
</tr>
<tr>
<td>Applications/processing</td>
<td>An understanding of client/server architectures</td>
<td>An understanding of IT-related systems development methodologies and standards, including change management</td>
</tr>
<tr>
<td>An understanding of operating systems and database management systems</td>
<td>A general understanding of ERPs and their design and deployment philosophies, including their effect on the audit trail</td>
<td>An understanding of business process reengineering principles and application of such</td>
</tr>
<tr>
<td>An understanding of the ERP modules and how they are configured, integrated and deployed</td>
<td>An understanding of security and authorisation concepts in an ERP setting</td>
<td></td>
</tr>
<tr>
<td>An understanding of security and authorisation concepts in an ERP setting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Skills of the IS auditor</th>
<th>ERP System</th>
<th>Implementation Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>A seasoned IS audit professional who is able to focus on the key areas of control risk in an ERP setting</td>
<td>An understanding of computer-assisted audit techniques (CAATs) and how to apply them in an ERP setting</td>
<td>Experience in the review and assessment of implementation projects</td>
</tr>
<tr>
<td>An ability to recognise where additional skills/expertise (such as financial and regulatory) are required</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How to Acquire skills</th>
<th>ERP System</th>
<th>Implementation Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification as a professional auditor</td>
<td>Certification as a professional IS auditor, such as CISA</td>
<td>Enroll in specialist training courses focusing on ERP implementation projects and the role of the IS auditor in such projects</td>
</tr>
<tr>
<td>Specialist training courses focusing on both the management and use of ERPs as well as the audit of ERPs</td>
<td>Practical, on-the-job experience</td>
<td></td>
</tr>
<tr>
<td>ERP learning opportunities especially as part of the end-user community</td>
<td>Self study, research, Internet, etc.</td>
<td></td>
</tr>
<tr>
<td>Practical, on-the-job experience</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self study, research, Internet, etc.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
General Elements of and Questions on ERP System Implementation

- What ERP product and modules are or will be used?
  - How are or will the modules be interlinked (such as, data flow across the modules)?

- What database management product(s) are or will be used?
  - How is/will the ERP (be) configured with the DBMS?

- What operating system product(s) are or will be used?
  - How have or will each be configured/implemented and controlled?

- To what level is the ERP web-enabled?
  - What processes are being extended to the web?

- What interfaces or linkages exist/will exist to non-ERP systems internal or external to the organisation?
  - How have or will each function be controlled?

- To what extent have or will ERP functionality and controlling roles or responsibilities be centralised or decentralised?

- How was or will data integrity be controlled and tested by management during the conversion of data from old or non-ERP systems during the ERP implementation?

- To what extent was or will business processes reengineering take place during the ERP implementation project?
  - If not, why not and when will it take place?
  - If so, what changes implemented and why?

- How are the ERP and BPR projects agreeing common process designs?

- What IT hardware and network resources are or will be used and how will they be configured and managed?

- To what extent are the ERP management and technical support roles and responsibilities integrated or separated from other related IT support (such as, database administration, operations)?

- What are or will be the access security policies and standards, and who will be responsible for ongoing management control and support?

- What processes are being adopted to provide reasonable assurance that acceptance of the ERP system and transfer of ownership to user management is complete?

Copyright 2003
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web Site: www.isaca.org