Chapter 11

ERP Security and Implementation Assurance

Objectives

- Become acquainted with the concept of internal control and its objectives
- Differentiate between IT general and application controls
- Understand the process of ERP systems implementation assurance
- Recognize the various IT certifications for professionals involved in ERP implementation
assurance, audit, security, governance, and risk

Introduction

Throughout this book, we've learned that ERP systems are integrated business systems that enable the management, control, and evaluation of operations. At their core, ERP systems process transactions that record journal entries in various modules that ultimately post to the general ledger (GL), from which the financial statements are prepared. Companies provide their financial statements to stakeholders, including investors, financial analysts, governmental agencies, and creditors. The information in these financial statements must be accurate, reliable, and complete. It follows, therefore, that the ERP system and the supporting infrastructure in which it operates must be secure so these goals may be achieved. The security of the ERP system and its underlying technical infrastructure can best be achieved by implementing various policies and procedures, or internal controls, that minimize IT risk.

This chapter introduces the concept of internal control and discusses the various types of controls that need to be present in an ERP environment to minimize IT risk. One category of controls are IT general controls, which include program change controls, logical access controls, and data center controls. Another category of controls is application controls, which are programmed or configured within the ERP software itself, and include checking for invalid input data, configuring the three- way match in the Purchasing module, and controlling employee access in the system. Risks can also occur during the implementation of the ERP system, so many companies will engage a third party to provide an objective assessment of the implementation, known as systems implementation assurance (SIA). Finally, this chapter acquaints the reader with IT certifications that professionals can obtain to demonstrate that they possess the experience and knowledge to meet the challenges of the modern enterprise.

Internal Control

Internal control is the policies and procedures put in place by an organization's board of directors, management, and other personnel to provide "reasonable assurance" regarding achievement in the following objectives:

- Effectiveness and efficiency of operations – includes attaining performance and profitability goals and safeguarding resources

- Reliability of financial reporting – pertains to the preparation of accurate financial statements and other financial data about a firm's performance

- Compliance with applicable laws and regulations – means adhering to those laws and regulations to which the organization is subject

An example of an internal control is having someone other than the

person signing checks perform the bank reconciliation. This type of internal control is a manual control. An **IT control** is a procedure or policy that provides reasonable assurance that the IT used by an organization operates as intended, that data is reliable, and that the organization is in compliance with applicable laws and regulations. IT controls are some of the most important internal controls because of the organization's pervasive reliance upon automated transaction processing. Therefore, IT controls must be designed properly and operate effectively.

Because of the inherent limitations in all internal control systems, an internal control, no matter how well designed and operating, cannot guarantee that an entity's objectives will be met. The concept of "reasonable assurance" acknowledges that limitations, uncertainties, and risk, which no one can predict with absolute precision, can exist in all systems.

In the U.S., public companies, government entities, and companies in regulated industries must be audited. If an auditor identifies issues in a client's internal control structure, the client company must take action to remediate the problems and demonstrate how the original business objectives will now be achieved. By doing so, companies are in a better position to receive an **unqualified audit report** of their year-end financial statements. This report reflects a "clean bill of health" denoting that there is "reasonable assurance" the general ledger accounts are properly valued and internal controls are effective, showing compliance with the Sarbanes-Oxley of Act of 2002 (SOX). As a result of SOX Section 404, management at publicly traded companies must:

- Establish internal controls and procedures over financial reporting
- Document, test, and maintain those internal controls and procedures to guarantee their effectiveness

The Public Company Accounting Oversight Board (PCAOB), created as a result of SOX, is a nonprofit corporation established by Congress to oversee the audits of public companies in order to protect the interests of investors and advance the public interest in the preparation of informative, accurate, independent audit reports. The PCAOB issued Auditing Standard No. 5, which states that the objective of an audit of internal controls over financial reporting is "to express an opinion on the effectiveness of the company's internal controls over financial reporting." The auditor must plan and perform the audit to gather "competent evidence that is sufficient to obtain reasonable assurance about whether material weaknesses exist as of the date specified in management's assessment."

While these requirements are specifically targeted at publicly traded companies, many privately held companies, nonprofit organizations, and governmental agencies also make

efforts to meet these requirements and undertake similar internal control audits for various reasons. For example, such an auditor's report may help a company as it seeks financing. In addition, taking steps toward being "SOX-compliant" can make a company more attractive as a takeover target by lowering the risk for acquisition-minded companies and their underwriters. One of the main reasons, however, for adhering to SOX requirements is focused inward—becoming a healthier, control-conscious organization.

ERP and Internal Controls

Because ERP systems process transactions that affect the financial statements, a company's year- end audit must include an inspection of IT controls that govern the system. As an independent third party, auditors look for any internal control issue that exposes the ERP system and its data to material misstatements of the entity's financial statements.

Modern ERP systems are designed with internal controls in mind. As the foundation of a firm's transactional processing, the ERP system maintains all data pertaining to business processes from beginning to end. Generally, once data is entered, there is no need to re-verify it. Processes are automated and postings do not require human intervention. **Edit checks** occur at the point of data entry to make sure data adheres to specific data standards —checking, for example, for blank fields, negative numbers, and invalid dates. However, many IT controls must be "turned on" through configuration of the system during implementation—the three-way match discussed in Chapter 9 is an example. ERP systems also ensure process integrity by including a log of transactions, or **audit trail**, that records when the transactions were entered and by whom.

However, security problems still exist in every layer of an ERP system: presentation layer, application layer, and database layer. Following are security issues that can exist in the three-tiered architecture of ERP systems.

- Client tier – The presentation layer contains the code responsible for displaying the user interface of the application. Inaccurate data entry may occur accidentally, such as when a transaction is entered incorrectly by a poorly trained employee, or intentionally, such as when an employee purposely alters data in a nefarious scheme to defraud the company. Mistakes and fraudulent entries can become hard to catch once they are in the system. Companies routinely face both of these risks. Employees need to be trained on what data to enter and where and access controls must be built into this layer to allow user input only where it is appropriate.

- Application tier – The integrated nature of ERP applications means that data entered at one stage in the process is carried forward to later stages. The validity of the data entered earlier is implicit, and there is often no re-verification at later stages. Every data field needs to be accurate at all stages of a process. Again, controls at this layer require clear definitions of who should be allowed to do what in the system. Additionally, many activities and updates (postings) occur without human intervention. These activities and postings are based on the configurations made in the ERP system. Therefore, it is critical that during implementation, configurations are made correctly and are in line with the control requirements of the business.

- Database tier – The database layer especially is a prime target because it comprises highly sensitive data, such as intellectual property; personally identifiable consumer and employee data; and financial information. Using a database that is shared across the company enhances data availability and visibility, but the "dark side" is that it also increases the threat that trusted parties, especially employees,

can commit fraud, particularly if their access is not properly controlled and monitored.

Many companies still think information security is only about protecting the physical and network perimeter security, and they overlook security within their systems. They think by having their servers in physically secured rooms and behind network firewalls that the systems are secure. However, this is not the case in today's interconnected world, in which companies share information and processes with their customers, suppliers, and other business partners. As additional modules, legacy systems, and bolt-on technologies are integrated or interfaced with an ERP system, security problems escalate. The next section describes the types of internal controls needed in an ERP environment to reduce IT risk.

IT Application Controls

IT application controls (ITACs) control the input, processing, and output functions of an ERP system by enabling, disabling, or limiting the actions of system users and enforcing business-driven rules and data quality. These controls are either programmed in the system or configured during implementation to facilitate data accuracy, completeness, validity, verifiability, and consistency to help guarantee the confidentiality, integrity, and availability of the ERP application and its associated data. Figure 11-1 describes the three types of ITAC and gives examples of each.

Figure 11-1: Types of Information Technology Application Controls (ITAC)

Description	Control
Input Controls – Ensure that all data input into the system is accurate, complete, and authorized	● Sequence checks to prevent missing transactions ● Drop-down menus to only allow valid items ● Authorization and approval rights for transactions based on user roles ● Override capabilities restricted to only certain users ● Edit checks to ensure accurate, valid, and complete input ● Standardized input screens ● Checks for duplicate entry of data
Processing Controls – Ensure that valid input data is processed accurately and completely	● Automated tracking of changes made to data that associates the change with a specific user; enables the audit trail ● Automated checks of data from feeder systems, a process known as an **interface control** ● Automated tracking of overrides made during processes ● Checks to ensure that automated calculations produce expected results
Output Controls – Ensure that output is	● Distribution of sensitive reports only to appropriate personnel

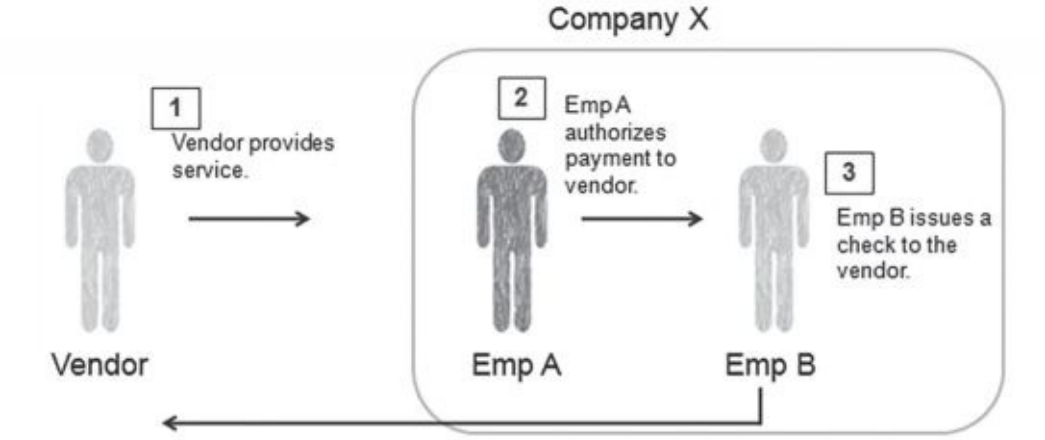
complete, accurate, and distributed only to the appropriate personnel	● Adherence to record retention periods ● Analysis of error reports and corrective action to rectify issues ● All successful transactions posted to subsidiary ledger and summarized in the GL

Segregation of Duties

One of the important ITACs is **segregation of duties (SoD)**, which is the concept of requiring different people to complete different parts of a process. By segregating duties, companies reduce the risk of erroneous and inappropriate actions by their employees. Segregation of duties is a deterrent to fraud because it requires three functions to be kept separate—no one person should (1) approve a transaction, (2) record and reconcile the transaction, and (3) have custody of the assets involving the transaction. When these functions cannot be separated (such as in small companies), other controls must be put in place to compensate for this lack of segregation.

Figure 11-2 presents the SoD in the purchase-to-pay process. Note that Employee A authorizes the payment to the vendor, while Employee B issues the check, or maintains custody of the asset. Presumably, a third employee would keep records by inputting vendor invoices in the ERP system. Another example not shown in the figure is that the person who requisitions the purchase of the service should not be the person who approves the purchase order, and the person who approves the purchase order should not be the person who signs off that the service is complete.

Figure 11-2: Segregation of Duties



Role-Based Access Control

Authorization refers to the level of access a certain user has in the ERP system. In an ERP system, authorization is accomplished through **role-based access control (RBAC)**, which assigns individuals to organizational roles and those roles to specific access in the system. A **role** is a job assignment or function; examples include data entry clerk,

purchasing manager, business analyst, HR manager, and accountant. Authorizations in the ERP system are grouped by role name and restricted only to certain individuals authorized to assume a particular role. A person can be assigned to more than one role, but may be required to act in a single role at any one time. Changing roles may necessitate logging out and then logging in again, or inputting a special role-changing command.

Role-based access control is employed at the company, application, and transaction level. For instance, a certain user may be assigned to the accountant role in Company X within Parent Company
A. That user is authorized to work only in Company X, within the Financial and Management Accounting modules, and within those modules, there are certain transactions and master data that this user can **create, read, update, delete** (known as **CRUD**). Role-based access controls help enforce segregation of duties.

Auditing Information Technology Application Controls (ITAC)

It is very important to subject a company's ERP software to a thorough and detailed audit because transactions involving its money, material, and services are recorded in the application. When evaluating ITACs in an ERP system, the auditor would focus on the modules. The first questions the auditor should ask are "What does this module do?" and "What business process or processes does this module support?" This can be accomplished by studying the operating and work procedures of the organization, including process maps, process narratives, and interviewing key personnel in the business process under investigation.

Once the auditors know what the module does, they can identify the potential risks associated with the business processes in question by asking "What could go wrong?" Then they can see how the risk is handled by asking the question "What controls the risk?" To answer these questions, the auditor must have business and technical knowledge. Auditing of application controls is a complex process and is outside the scope of this book. However, several example ITAC audit steps include:

- Inspection of system configurations in the Purchasing module to make sure quantities and prices are being checked in the three-way match

- Inspection of system configurations to ensure that duplicate vendor invoices are disallowed
and that duplicate vendors cannot be entered into the system

- Inspection of a user access list for employees who can access payroll data and verification that this list reflects those who truly need this access

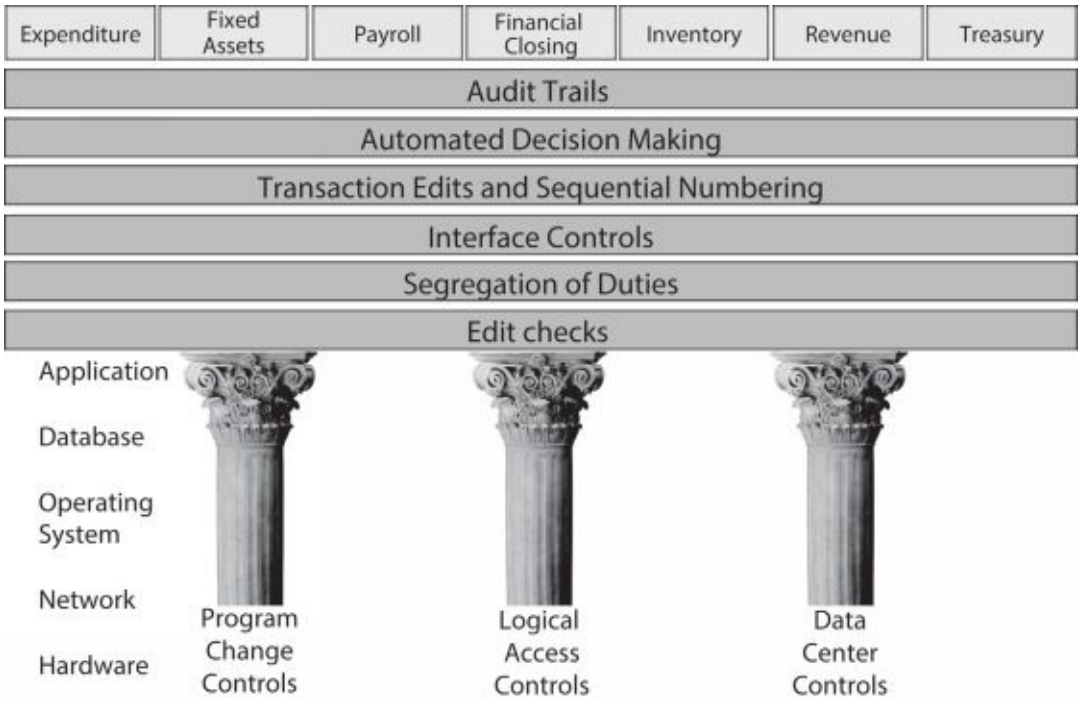
- Verification that audit trails and logs exist to ensure that all transactions can be traced to the
individuals who entered them

IT General Controls

Controls that apply to all systems components, processes, and data for a given organization or IT environment are called **IT general controls (ITGCs)**. These controls work to both secure and validate the data contained in the systems that process financial transactions. The objectives of ITGCs are to ensure the proper development of and changes to applications, databases, and operating systems; controls over logical access to the network and applications; and controls

surrounding the data center. Figure 11-3 shows these three types of ITGC as pillars that support typical application controls in major business processes. They are represented as pillars because, for ITAC to be effective, the auditor must first ascertain that the ITGCs are functioning properly. The rationale is that if the IT environment is not secure, then users cannot feel confident that controls within the applications are functioning properly. The ITGCs are the first line of defense in a secure ERP environment.

Figure 11-3: Relationship between IT General Controls and IT Application Controls



Source: Deloitte

It should be noted that an organization will never have 100 percent assurance that all risks to IT resources are eliminated through IT controls. Because of the costs associated with protecting IT resources, companies must identify the potential risks facing their information systems and perform a cost-benefit analysis to determine the appropriate level of protection. Let's study each of these ITGC pillars in depth.

Program Change Controls

The controls that govern the changes made to programs, including any changes made to the ERP system and underlying database, based upon requests from users or due to general maintenance requirements are called **program change controls**. These controls seek to ensure that the development of and changes to systems are properly designed, tested, validated, and approved prior

to migrating the changes to the production environment. Examples of changes include patches, bug fixes, updates, program code changes and enhancements, and minor upgrades. Deficiencies in program change controls increase the potential for fraudulent or unauthorized changes, transaction processing errors, and incorrect and unexpected application behavior and program logic. For example, a programmer who can authorize a change to the Financial Accounting module of an ERP system and move that change into production has the potential to insert malicious code into the module or change the module in such a way that the financial statements contain errors. This lapse in SoD would create an audit red flag and would lead the auditors to expand the scope of the audit by doing additional testing. In addition, the client would have to remediate the SoD problem, even if no fraud or errors had occurred. ITGCs should be tested early in the audit process, so that in the event problems are detected, the audit team can adjust its approach to testing and the client has the opportunity to remediate the issues.

Figure 11-4: ERP System Landscape

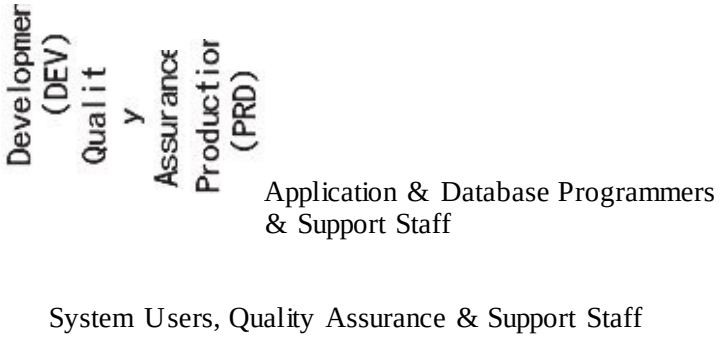


Figure 11-4, also discussed in Chapter 2, depicts the stages through which program changes should progress in an IT environment. The figure also shows the roles that typically have access to each instance. These separate instances serve to control the process of program

change. As changes to the database and ERP system are developed and deployed, the transition from one instance to the next indicates that each change meets objective criteria for promotion. In addition, the controls over program changes should be adequately documented to eliminate all doubt, from the auditor's point of view, that they function properly. It is important that all program changes are documented and auditable and that all unauthorized changes are investigated. Examples of program change controls are listed in Figure 11-5.

Figure 11-5:

Examples of Program Change Controls

Program changes are only initiated with a valid IT or business justification.

An IT manager or management in the business area requesting the change approves the program change prior to development in the DEV instance.

Application programmers should only make changes in the DEV instance. Once work is completed, application programmers should move the program changes to the QA instance.

Depending on the type of program change, functional users and/or IT staff test to make sure the application works correctly in the QA environment. These staff members are separate from programmers/ developers.

Prior to moving changes to PRD, an **impact analysis** is performed to determine the potential effect of the proposed change to other systems and modules as well as to users.

Program changes moved to PRD are scheduled during downtime, and users are notified in advance when the changes will occur.

After testing and sign-off in the QA instance is complete, an IT employee—separate from the employee who developed the change—moves the change to PRD.

Programmers should not have direct access to the PRD instance and should not make changes directly into PRD. Emergency changes into production may be allowed using a temporary firefighter role, which is monitored and logged.

Documentation exists to show proper approvals and procedures in the program change control process.

Source: ISACA

Logical Access Controls

Logical access controls are the policies, procedures, organizational structure, and electronic controls designed to restrict access to information systems and data only to individuals with genuine authority to access the information. These controls are different from **physical access controls**, which refer to a mechanical lock and key or other devices controlling access to a building or room. For instance, a data center would have physical access security mechanisms on the doors, but logical access controls for the ERP system loaded on the servers in the data center.

Logical access is part of a larger concept—that of **identity and access management (IAM)**. IAM refers to the management of individual identities and privileges or permissions within or across system and company boundaries with the goal of increasing security and productivity while reducing costs, downtime, and repetitive administrative tasks. Without a properly functioning IAM, it is very difficult to prove, control, and monitor which users access what information and to determine whether that access is in compliance with internal and external regulations. Privacy concerns, various categories of system users, and multiple information systems compound these issues.

An IAM system performs three main activities. The first is **identification**, which is the

process of describing an individual to a system with a unique user ID. The second activity, **authentication**, involves verifying that a user's claim to a particular identity is, in fact, true. This process is commonly carried out through the combination of user IDs and passwords. Authenticated identities then

become the foundation for the third activity, authorization, or the level of access a particular authenticated user should have to resources controlled by the system. Authorization was discussed earlier in the chapter.

The process of verifying the identity of users through a user ID and a password is authenticated using a knowledge factor, or "what the user *knows*." However, this can be combined with a possession factor, or "what the user *has*," and an inherence factor, or "what only the user *is*," to add more layers of logical access control. Requiring two forms of authentication factor is called **dual-factor authentication** and requiring more than two forms is called **multi- factor authentication**. An example of "what the user has" is using a security card such as an RSA SecurID, which is an authentication token that uses a built-in clock and factory-encoded random key to restrict access to systems. An example of "what only the user is" is **biometric software**, which enhances security by linking a user's unique physical attributes to the data he or she is allowed to access. The user provides a fingerprint or other biometric characteristic to the system, where it is then authenticated against a stored image. Biometrics can also be used for granting physical access to the data center.

Figure 11-6 presents examples of essential logical access controls. Deficiencies in logical access controls can create the potential for viewing unauthorized data, recording fraudulent transactions, overriding ITACs, making unauthorized changes to program calculations, and creating accidental changes to data and information system resources.

Figure 11-6: Examples of Logical Access Controls

Documentation exists to show proper approvals and procedures to grant logical access.
Use of privileged access in applications such as SYSADMIN is limited only to appropriate personnel.
Procedures are put into place to notify IT security personnel when employees change roles and responsibilities or are terminated. Access privileges of such individuals are immediately changed to reflect their new

status.

Roles and responsibilities related to IT security are assigned to appropriate personnel.

Data encryption, firewalls, network segmentation, and other measures are put in place to keep hackers, cyber-criminals, and other outsiders from accessing the ERP system and database.

Effective password management policies, such as periodically changing passwords and requiring passwords that are not easily guessed, are in place and enforced.

Dual-factor or multi-factor authentication is enforced when logging onto the network. Default passwords are effectively replaced upon first login to the ERP system.

Direct access to the ERP database is closed and programmatically prevented. Effective use of HTTPS for remote access is enforced.

Source: ISACA

Data Center Controls

Data center controls help protect computer facilities and resources from environmental hazards, espionage, sabotage, damage, and theft. These controls focus on the physical security of the data center where the servers that support the ERP system are kept. The data center should be audited by an IT audit or assurance professional to make sure that proper controls are in place to provide physical security, protection of data, and reliability and availability of operation (see Figure 11-7). **Reliability** is the ability of a system or component to execute its required functions under stated conditions for a specified period of time. **Availability** is the degree to which a system or component is accessible and operational when it is needed. Reliability factors into availability as does recovery time after a failure occurs. In a data center, having a reliable system design is the most critical variable. However, once a failure does occur, the most important consideration becomes getting the IT equipment and business processes up and running as soon as possible, thus keeping downtime to a minimum.

Figure 11-7: Data Center Controls

Physical Security	Protection of Data	Reliability and Availability
Build on the right spot	Employ redundancy by storing copies of data in multiple locations	Use an uninterruptible power supply (UPS)
Use surveillance cameras	Back up critical data	Use emergency backup generators
Limit entry points and avoid windows	Use fire detection and suppression	Use fiber optic cables
Use biometrics for access	Destroy hard drives when retiring them	Have a disaster recovery plan
Employ 24/7 security and use perimeter fencing	Shred paper	Maintain service-level agreements with customers
Keep a roster of those who are allowed access to the data center	Use proper air conditioning and have redundant utilities	Have a data recovery plan

Source: ISACA

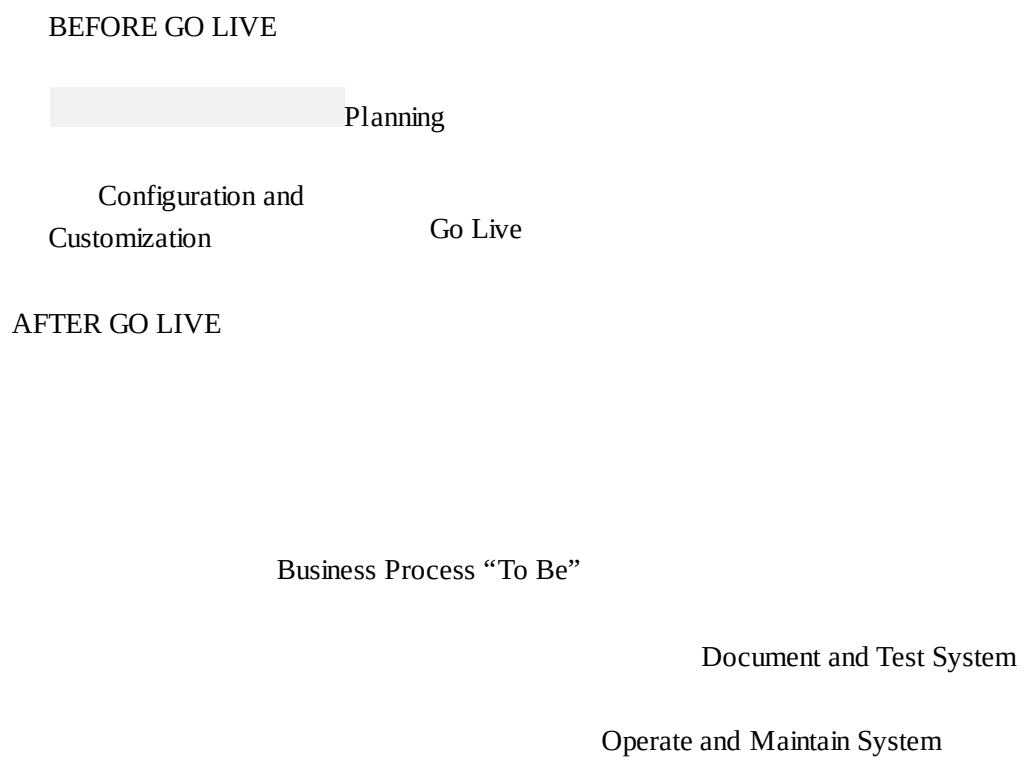
System Implementation Assurance

ERP systems, while achieving great economies of scale and employing many advantages, carry unique risks, many of which can be mitigated if the implementation is executed successfully. Often, companies implementing ERP systems will seek out a third

party to give an unbiased opinion on the progress of the implementation and the work accomplished by the internal project team and consultants. This third-party opinion is called **systems implementation assurance (SIA)** and is an independent assessment of the health and expected outcome of the ERP implementation and corresponding change initiative.

Various entities can do this type of work, but oftentimes the company's internal audit staff or external auditor is engaged to render this objective assurance. This assurance team will act independently of the system integrators with a "dotted line" to the ERP project sponsor and steering committee and operate in an "assess and recommend" mode. Typically, SIA will focus on three main types of risks throughout the ERP life cycle: control risk, project risk, and business risk. These risks happen at various points in the ERP life cycle as shown in Figure 11-8.

Figure 11-8: Points in the ERP Life Cycle Where Assurance is Beneficial



Control Risks

One of the major risks in an implementation is whether the design and implementation of ITGCs and ITACs will satisfy financial reporting, operational, and regulatory requirements. Thus, the organization should take a security mindset from the beginning of the project. Many implementations are not staffed with full-time security and controls experts, and thus these risks are often overlooked. While poor internal controls are not generally the reason ERP projects fail, it could result in a "forthcoming failure" because for a period of time internal controls will be lax. Also, building controls

into the system and around the system after the fact can be very costly. Identifying control risks and putting a plan in place to mitigate these risks should therefore start early.

Assurers should review the project plan and recommend how to incorporate security and controls during the implementation. They should ensure that the design of the configurable controls is done during business process design, rather than identifying and correcting weaknesses after go-live. Assurers will look at many types of control risks in the following key areas:

- ITAC – Has management evaluated the best mix of manual versus automated or configured
controls necessary to accurately and completely capture and validate data?

- ITGC – Do the IT infrastructure and manual IT processes support the new ERP system?

- Data quality – Has the legacy data been successfully migrated to the ERP system, and is it
accurate and in a usable format?

● Interfaces – Do interfaces between the ERP system and other systems transport data properly
to ensure data integrity?

During SIA, assurance teams may find that internal controls are not clearly identified during the requirements and design phase, employees have conflicting user access rights (improper SoD) in the ERP system even after go-live, and privileged user access and/or default system user accounts are not properly managed after go-live. Other findings are that training on security is incomplete and security controls are not negative tested. A **negative test** tests software to ascertain if it is doing something it is not supposed to do, like accepting an all-letter password when the requirement is that the password has at least one number.

Business Risks

Some of the risks to the ERP implementation present themselves early on in the implementation during planning. In this phase, the SIA team will want to evaluate the:

● Business case – Is there a solid business case in place for the ERP investment, and is it aligned with corporate strategy?

● Benefits realization plan – Are there appropriate key performance indicators that back up the business case and will they produce measureable outcomes?

● Organizational structure – Is the project properly structured and does it include a high-level sponsor and steering committee that will proactively lead the desired change?

One of the main business issues found during SIA is that the project is being led by IT with minimal involvement from key functional areas or the project is being handed over too

much to consultants. Another issue found during SIA is that business benefits have not been measured or evaluated post-go-live.

Project Risks

Another major type of risk involves project management. This risk to the implementation involves whether the ERP system will be delivered on time and on budget, whether the system will meet the stated requirements, and whether the employees are adequately prepared for the new system and processes. Assurance on project risks will take place from the beginning of the project through go- live. The SIA team will want to evaluate:

- Project management – Are timelines and resources being effectively managed?

- Project governance – Is there appropriate management support throughout the implementation?

- Functional readiness – Are mechanisms in place to develop functional requirements?

- Technical readiness – Are mechanisms in place to translate the functional requirements into the ERP software (i.e. configuration and customization)?

- Organizational readiness – Are changes to processes being effectively communicated and understood throughout the organization? Is training being conducted effectively?

An ERP project is a massive undertaking, and many things can go wrong. Key issues found during evaluation of project risks include testing defects that remain at go-live, testing that is performed before all data is migrated, and testing scripts that do not match the real-world scenario (and instead are "canned" test scripts). Also, it has often been found that in some implementations, training on the software is inadequate or incomplete and as a result, users have difficulty using the ERP system at pre- and post-go-live. Sometimes it is found that organizational change management strategies are poorly defined or nonexistent, and the project team is too inexperienced.

ISACA Certifications for IT Professionals

The independent, nonprofit, global association engaged in the development, adoption, and use of globally accepted knowledge and best practices in IT is the **Information Systems Audit and Control Association (ISACA)**. ISACA was founded in 1967 by a group of computer auditors who realized there was a need for a centralized source of information to help them do their jobs better. Today, ISACA is the leading organization that disseminates information for IT governance, control, security, and audit professionals. ISACA's IS auditing and IS control standards are followed by a constituency of more than 115,000 practitioners worldwide in more than 180 countries. ISACA members hold various positions, including IS auditor, consultant, educator, IS security professional, regulator, internal auditor, and chief information officer (CIO). Some ISACA members are early in their careers, while others are in senior-ranking positions. ISACA members also work in many different industries, including manufacturing, public accounting, government and public sector, and financial services.

The market for individuals possessing skills relevant for IT audit, assurance, security, risk, and governance has grown. To emphasize their expertise and differentiate themselves in the marketplace, IT professionals and business professionals have become certified by ISACA in one or more of these growing areas of IT. Choosing the most appropriate certification depends on many factors, including a person's level of technical expertise, business experience, education, and desired career path. Obtaining an IT certification is desirous as it confirms knowledge and

experience, quantifies and markets expertise, and demonstrates that the professional has gained and maintained a level of knowledge required to meet the challenges of a modern enterprise. Following is a brief description of ISACA certifications. To obtain and maintain one of these certifications, a candidate must pass an exam, possess the required educational and work experience, undertake continuing professional education, and practice ethical conduct.

CISA

The **Certified Information System Auditor (CISA)** is the flagship certification of ISACA, qualifying an individual as globally proficient in the areas of IS audit, assurance, and security. Established in 1978, the CISA designation showcases a practitioner's information systems (IS) audit experience, skills, and knowledge and demonstrates the capability to manage risks, institute controls, and ensure compliance with laws and regulations. The CISA exam covers five practice areas:

- The process of auditing IS
- Governance and management of IS
- IS acquisition, development, and implementation
- IS operation, maintenance, and support
- Protection of information assets

The largest percentage of the exam, 30 percent, covers protection of information assets, which includes questions regarding ITGC and ITAC. Information regarding the ERP life cycle would be tested in the areas of IS acquisition, development, and implementation and IS operation, maintenance, and support.

CISM

The **Certified Information Security Manager (CISM)** designation uniquely targets the professional who manages, designs, oversees, and assesses an organization's information security program. This certification is for those who understand the relationship between information security and the overarching business objectives, goals, and strategy and is relevant for professionals with management experience. The CISM certification exam covers four practice areas:

- Information security governance

- Information risk management and compliance

- Information security program development and management

- Information security incident management and response

The largest percentage of the exam, 33 percent, covers information risk management and compliance. The exam includes questions on how to integrate risk management throughout the IS life cycle, who to communicate risks to and how, and the role of the IT steering committee. This certification requires a high level of risk and security knowledge and five years of security management experience. Passing the CISA exam prior to taking this exam can substitute for some of the work experience.

CRISC

The **Certified in Risk and Information Systems Control** (**CRISC)** certification is intended to recognize a wide range of IT and business professionals for their knowledge of enterprise risk management (ERM) and their ability to design, implement, monitor, and maintain systems controls to reduce risk. A deep understanding of risk management is necessary for those considering taking this exam. **Risk management**, discussed in Chapter 6, is the identification, analysis, assessment, control, avoidance, minimization, or elimination of unacceptable risks. **IT risk management** applies this concept to the area of IT and information systems. The CRISC exam includes four practice areas:

- IT risk identification
- IT risk assessment
- Risk response and mitigation
- Risk and control monitoring and reporting

The largest percentage of the exam, 28 percent, tests IT risk assessment. Candidates for the CRISC need specific knowledge of risk standards and frameworks, quantitative and qualitative risk evaluation methods, threats and vulnerabilities related to business processes, the ERP life cycle, and project management. One major part of the exam entails identifying the current state of existing controls and evaluating their effectiveness for IT risk mitigation.

CGEIT

The **Certified in the Governance of Enterprise IT (CGEIT)** designates a professional with the knowledge and application of enterprise IT governance principles and practices. This certification recognizes those professionals who have the necessary level of

professional knowledge, skills, and business experience to move to the C-suite if they aren't already there. The core theme of this certification is **IT governance**, which consists of the leadership, organizational structures, and processes that ensure that an organization's technology sustains and extends its strategies and objectives. The CGEIT exam encompasses five practice areas:

-  Framework for the governance of enterprise IT
- Strategic management
- Benefits realization
- Risk optimization
- Resource optimization

The main practice area tested, 25 percent of the exam, is the framework for governance of enterprise IT. Examples of specific knowledge needed across job practice areas include developing a business case for an ERP system, value measurement techniques, IT organizational structure including roles and responsibilities, SIA methodologies, and IT business process improvement techniques.

Summary

ERP systems have many advantages, but they also present many risks to organizations if not successfully implemented and maintained. Properly assessing and managing these risks and putting controls into place is essential to an IT risk management program. IT controls are classified as general or application. IT general controls enhance the IT infrastructure surrounding the ERP system. IT application controls are configured or programmed into the ERP system. Three types of IT general controls are controls over program changes, logical access, and the data center where the ERP system is housed. These controls are pervasive, minimizing IT risks across information systems. IT application controls are designed to prevent inaccurate or fraudulent data from being input into the ERP system as well as to ensure that information is properly processed so that the output is reliable. ERP systems can contain key security vulnerabilities that must be addressed and periodically audited. During an implementation, a company may engage an objective party to give an unbiased opinion as to its efficacy. The end goal of systems implementation assurance

is to maximize the likelihood of the ERP project's success and address any potential risks as early as possible. Many professionals who engage in this type of work become certified by ISACA to greatly enhance their credibility in the marketplace. This chapter ends with a discussion of certifications offered by ISACA that differentiate professionals as knowledgeable and technically competent in various aspects of IT.

Keywords

Audit trail Authentication Authorization Availability Biometric software
Certified in Risk and Information Systems Control (CRISC)

Certified in the Governance of Enterprise IT (CGEIT)

Certified Information Security Manager (CISM)

Certified Information System Auditor (CISA)

Create, read, update, delete (CRUD)

Data center control

Dual-factor authentication

Edit check

Identification

Identity and access management (IAM) Impact analysis
Information Systems Audit and Control Association (ISACA)

Input control

Interface control Internal control
IT application control (ITAC)

IT control

IT general control (ITGC)

IT governance

IT risk management Logical access control Multi-factor authentication

Negative test

Output control Physical access control Processing control

Program change control Reliability

Risk management Role

Role-based access control (RBAC) Segregation of duties (SoD)

Systems implementation assurance (SIA)

Unqualified audit report

Quick Review

1. True/False: IT general controls include program change controls, logical access controls,
and IT application controls.

2. True/False: Identity and access management (IAM) includes three main functions: identification, authentication, and authorization.

3. _____controls help protect computer facilities and resources from environmental hazards, espionage, sabotage, damage, and theft.

4. Programmers should make changes to application software in the __environment.

5. The _____certification qualifies an individual as globally proficient in the area of IS
audit, control, and security.

Questions to Consider

1. List three examples of program change controls that should be implemented to guard against unauthorized changes to the ERP system and database.

2. Explain the concept of role-based access control and how it relates to logical access.

3. Contrast the differences among the elements of identity access management (IAM).

4. What are the three main risk areas focused on in systems implementation assurance? Give an example of each.

5. List three examples of data center controls that should be implemented to protect computer facilities.

References

Bellino, C., Wells, J., Hunt, S., & Horwath, C. (2007). *Global technology audit guide (GTAG) 8: Auditing application controls*. Institute of Internal Auditors. Retrieved from http://www.theiia.org/ bookstore/downloads/ freetomembers/0_1033.dl_gtag8.pdf

COSO. (n.d.). Internal control – Integrated framework. Retrieved from http://www.coso.org/ documents/ Internal%20Control-Integrated%20Framework.pdf

Fowler, R. (2010, October 20). What are some application controls? Retrieved from http://www. isaca.org/Groups/Professional-English/application-controls/Pages/ ViewDiscussion. aspx?PostID=3

Hartman, S. (2012, October 12). Understanding data center reliability, availability and the cost of downtime. Retrieved from http://blog.schneider-electric.com/datacenter/2012/10/12/ understanding-data-center-reliability-availability-and-the-cost-of-downtime/

Herman, B., & Donahue, S. (2012). *The role of internal audit and compliance teams in providing real-time assurance during an SAP implementation, upgrade, or consolidation project.* Dedham, MA: Wellesley Information Services.

ISACA. (2014). CISA glossary. Retrieved from https://www.isaca.org/Knowledge-Center/ Documents/ Glossary/cisa_glossary.pdf

ISACA. (2014). ISACA Certification: IT audit, security, governance and risk. Retrieved from http://www.isaca.org/CERTIFICATION/Pages/default.aspx

Magee, K. (2011, June 14). IT auditing and controls – A look at application controls. Retrieved from http://resources.infosecinstitute.com/itac-application-controls/

PCAOB. (n.d.). PCAOB overseas the auditors of companies to protect investors. Retrieved from http://pcaobus.org/Pages/default.aspx

PRLog. (2009, September 17). *How can we keep our ERP database protected at all times?* Retrieved from http://www.prlog.org/10345486-how-can-we-keep-our-erp-database-protected-at- all-times.html

Privaris. (n.d.) *Biometric software security systems.* Retrieved from http://www.privaris.com/biometric_ software.html

Rothacker, A. (2011, May 13). ERP vulnerabilities differ from those at the database level. Retrieved from http://www.infosecisland.com/blogview/13716-ERP-Vulnerabilities-Differ-from- Those-at-the-Database-Level.html

Rouse, M. (2010). IT controls. Retrieved from

http://searchcompliance.techtarget.com/ definition/IT-controls

SAP. (2013). *SAP Solutions for Governance, Risk, and Compliance*. Retrieved from http://www.sap. com/solutions/sapbusinessobjects/governance-risk-compliance/index.epx

Sayana, S. A. (2004). Auditing security and privacy in ERP applications. Retrieved from http:// www.isaca.org/Journal/Past-Issues/2004/Volume-4/Pages/Auditing-Security-and- Privacy-in-ERP-Applications.aspx

Sayana, S. A. (2002). Auditing general and application controls. Retrieved from http://www.isaca. org/Journal/Past-Issues/2002/Volume-5/Pages/Auditing-General-and-Application- Controls.aspx

Scalet, S. (2005, November 1). *19 ways to build physical security into a data center*. Retrieved from http:// www.csoonline.com/article/220665/_Ways_to_Build_Physical_ Security_into_a_Data_ Center?contentId=220665&slug=www.csoonline

Sullivan, D. (2009). *The definitive guide to security management*. Channel Partner Realtime Publications.
Retrieved from http://www.windowsecurity.com/uplarticle/NetworkSecurity/DGSM- Ch4-Excerpt.pdf

Wikipedia.com. (2014). Identity management systems. Retrieved from http://en.wikipedia.org/ wiki/ Identity_management_systems

Wikipedia.com. (2014). Multi-factor authentication. Retrieved from http://en.wikipedia.org/ wiki/Multi-factor_authentication