STUDY NOTES

ESSENTIALS
MODULE-III
E-303

Information Technology Management, Audit & Control

Prepared By: Junaid Aslam

ICPAP

Institute of Certified Public Accountants of Pakistan

Preface

The purpose of this study guide is to prepare the student for the real-world business use of IT. With this study guideline, the student shall be equipped with enough IT knowledge and be aware of the requirements of the global IT standards that if granted the additional responsibility of managing, auditing or make strategy for IT, the student does not fails.

The approach of this study guide is very much practical oriented, and rather giving the reader the basic definition of the key items, the guideline followed with the procedures to follow in real world and the definitions come in between.

The guide is divided in five categories, Part 1, IT Audit & Planning, discusses the IT audit and step involved in developing IT Audit plan and risk assessment, also provided is a hypothetical company example. The second part cover IT controls, its classification, roles and responsibilities of the concerned, and control Frameworks. The third part, software for business, discusses the software that align with the business targets to maximize profits, like ERP, CRM and SFA, their advantages and how they help the businesses grow. The fourth part is about IT outsourcing. Outsourcing is not just assigning a task to a third party however; the process requires total monitoring and auditing during its lifecycle. The benefits of IT outsourcing are accompanied by the need to manage the complexities, risk, and challenges that come with it. Internal auditors, therefore, can help organizations with a comprehensive review of its outsourcing operations, identify risks, and provide recommendations to better manage the risks. This guide recommends a set of items that should be addressed. Part Five, “Managing and auditing IT Projects", discusses a procedures even more complex i.e. managing the IT project and steps involved during that plus issues that shall be taken care of.

We hope that this study guide will bring the reader one step forward from his colleagues and make him stand out by enabling him with IT knowledge that he be able to handle IT related issue as at a managerial level even better than any other person.

All suggestions, quarries and clarifications for improvement in this study guide would be appreciated.

The author of this study guide has qualified MS in computer science from an International university besides that he also hold MSC degree in Telecom from King College University of London, UK.

Context

IT Audit & Planning

1. What is IT Audit?

An information technology audit, or information systems audit, is an examination of the management controls within an Information technology (IT) infrastructure. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

Another definition for IT Audit can be "the process of collecting and evaluating evidence to determine whether a computer system (information system) safeguards assets, maintains data integrity, achieves organizational goals effectively and consumes resources efficiently."

Information systems are the lifeblood of any large business. As in years past, computer systems do not merely record business transactions, but actually drive the key business processes of the enterprise. In such a scenario, senior management and business managers do have concerns about information systems. The purpose of IS audit is to review and provide feedback, assurances and suggestions. These concerns can be grouped under three broad heads:

1. **Availability**: Will the information systems on which the business is heavily dependent is available for the business at all times when required? Are the systems well protected against all types of losses and disasters?
2. **Confidentiality**: Will the information in the systems be disclosed only to those who have a need to see and use it and not to anyone else?
3. **Integrity**: Will the information provided by the systems always be accurate, reliable and timely? What ensures that no unauthorized modification can be made to the data or the software in the systems?

IT audits are also known as "automated data processing (ADP) audits" and "computer audits". They were formerly called "electronic data processing (EDP) audits".

An IT audit is different from a financial statement audit. While a financial audit's purpose is to evaluate whether an organization is adhering to standard accounting practices, the purposes of an IT audit are to evaluate the system's internal control design and effectiveness. This includes, but is not limited to, efficiency and security protocols, development processes, and IT governance or oversight.

1.1 Types of IT audits

Various authorities have created differing taxonomies to distinguish the various types of IT audits. Goodman & Lawless state that there are three specific systematic approaches to carry out an IT audit:

- **Technological innovation process audit**. This audit constructs a risk profile for existing and new projects. The audit will assess the length and depth of the company's experience in its chosen technologies, as well as its presence in relevant markets, the organization of each project, and the structure of the portion of the industry that deals with this project or product, organization and industry structure.
- **Innovative comparison audit**. This audit is an analysis of the innovative abilities of the company being audited, in comparison to its competitors. This requires examination of company's research and development facilities, as well as its track record in actually producing new products.
- **Technological position audit**: This audit reviews the technologies that the business currently has and that it needs to add. Technologies are characterized as being either "base", "key", "pacing" or "emerging".

Others describe the spectrum of IT audits with five categories of audits:

- **Systems and Applications**: An audit to verify that systems and applications are appropriate, are efficient, and are adequately controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity.
- **Information Processing Facilities**: An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.
- **Systems Development**: An audit to verify that the systems under development meet the objectives of the organization and to ensure that the systems are developed in accordance with generally accepted standards for systems development.
- **Management of IT and Enterprise Architecture**: An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.
- **Client/Server, Telecommunications, Intranets, and Extranets**: An audit to verify that telecommunications controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers.

1.2 Elements of IS Audit

An information system is not just a computer. Today's information systems are complex and have many components that piece together to make a business solution. Assurances about an information system can be obtained only if all the components are evaluated and secured. The proverbial weakest link is the total strength of the chain. The major elements of IS audit can be broadly classified:

1. **Physical and environmental review**—This includes physical security, power supply, air conditioning, humidity control and other environmental factors.
2. **System administration review**—This includes security review of the operating systems, database management systems, all system administration procedures and compliance.
3. **Application software review**—The business application could be payroll, invoicing, a web-based customer order processing system or an enterprise resource planning system that actually runs the business. Review of such application software includes access control and authorizations, validations, error and exception handling, business process flows within the application software and complementary manual controls and procedures. Additionally, a review of the system development lifecycle should be completed.
4. **Network security review**—Review of internal and external connections to the system, perimeter security, firewall review, router access control lists, port scanning and intrusion detection are some typical areas of coverage.
5. **Business continuity review**—This includes existence and maintenance of fault tolerant and redundant hardware, backup procedures and storage, and documented and tested disaster recovery/business continuity plan.
6. **Data integrity review**—The purpose of this is scrutiny of live data to verify adequacy of controls and impact of weaknesses, as noticed from any of the above reviews. Such substantive testing can be done using generalized audit software (e.g., computer assisted audit techniques).

To organize the audit, an audit plan shall be developed.

2. Planning IT Audit

2.1 Summary

As technology becomes more integral to the organization's operations and activities, a major challenge for internal auditors is how to best approach a companywide assessment of IT risks and controls within the scope of their overall assurance and consulting services. Therefore, auditors need to understand the organization's IT environment; the applications and computer operations that are part of the IT infrastructure; how IT applications and operations are managed; and how IT applications and operations link back to the organization.

Completing an inventory of IT infrastructure components will provide auditors with information regarding the infrastructure's vulnerabilities. "The complete inventory of the organization's IT hardware, software, network, and data components forms the foundation for assessing the vulnerabilities within the IT infrastructures that may impact internal controls.". For example, business systems and networks connected to the Internet are exposed to threats that do not exist for self-contained systems and networks.

Once an adequate understanding of the IT environment has been achieved, the chief audit executive (CAE) and the internal audit team can perform the risk assessment and develop the audit plan.

Many organizational factors are considered when developing the audit plan, such as the organization's industry sector, revenue size, type, complexity of business processes, and geographic locations of operations. Two factors having a direct impact on the risk assessment and in determining what is audited within the IT environment are its components and role. For example:

- What technologies are used to perform daily business functions?
- Is the IT environment relatively simple or complex?
- Is the IT environment centralized or decentssralized?
- To what degree are business applications customized?
- Are some or all IT maintenance activities outsourced?
- To what degree does the IT environment change every year?

These IT factors are some of the components CAEs and internal auditors need to understand to adequately assess risks relative to the organization and the creation of the annual audit plan.

In addition to factors impacting the risk assessment, it is important for CAEs and internal auditors to use an approach that ascertains the impact and likelihood of risk occurrence; links back to the business; and defines the high, medium, and low-risk areas through quantitative and qualitative analyses.

IT is in a perpetual state of innovation and change. Unfortunately, IT changes may hinder the IT auditor's efforts to identify and understand the impact of risks. To help IT auditors, CAEs can:

- Perform independent IT risk assessments every year to identify the new technologies that are impacting the organization.
- Become familiar with the IT department's yearly short-term plans and analyze how plan initiatives impact the IT risk assessment.
- Begin each IT audit by reviewing its risk assessment component.
- Be flexible with the IT audit universe — monitor the organization's IT-related risk profile and

adopt audit procedures as it evolves

Several IT governance frameworks exist that can help CAEs and internal audit teams develop the most appropriate risk assessment approach for their organization. These frameworks can help auditors identify where risks reside in the environment and provide guidance on how to manage risks. Some of the most common IT governance frameworks include COBIT, the UK's Office of Government Commerce IT Infrastructure Library (ITIL), and the International Organization for Standardization's (ISO's) 27000 Standard series.

Mapping business processes, inventorying and understanding the IT environment, and performing a companywide risk assessment will enable CAEs and internal auditors to determine what needs to be audited and how often. This GTAG provides information that can help CAEs and internal audit teams identify audit areas in the IT environment that are part of the IT audit universe.

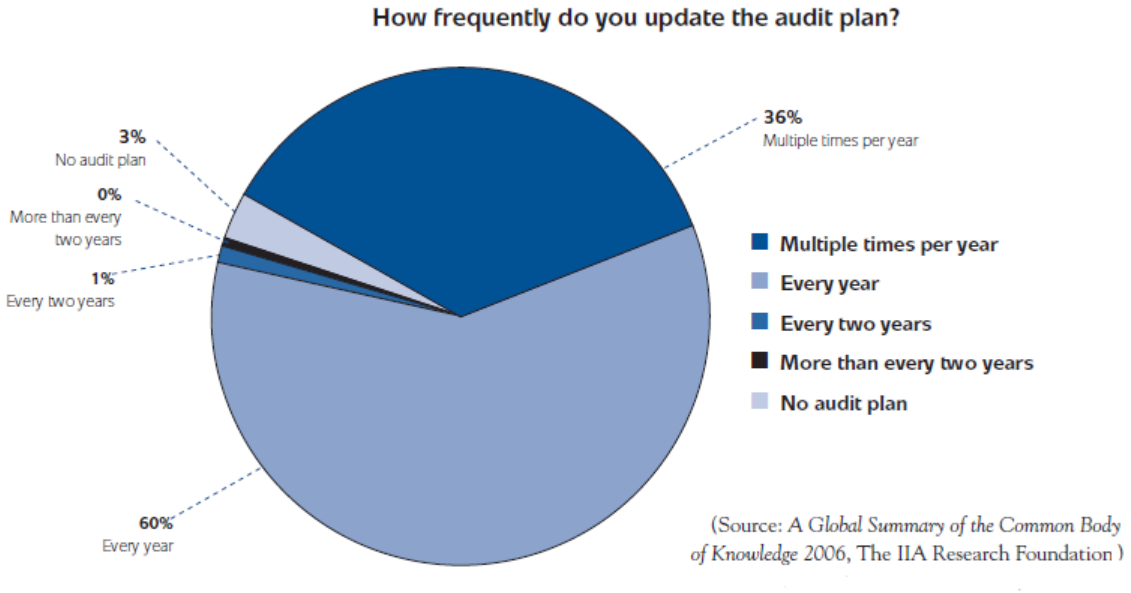
Due to the high degree of organizational reliance on IT, it is crucial that CAEs and internal auditors understand how to create the IT audit plan, the frequency of audits, and the breadth and depth of each audit. To this end, this GTAG can help CAEs and internal auditors:

- Understand the organization and the level of IT support received.
- Define and understand the IT environment.
- Identify the role of risk assessment in determining the IT audit universe.
- Formalize the annual IT audit plan.

Finally, this GTAG provides an example of a hypothetical organization to show CAEs and internal auditors how to execute the steps necessary to define the IT audit universe.

2.2 Introduction

One of the main responsibilities and more difficult tasks of CAEs is to create the organization's audit plan. CAEs must establish risk-based plans on at least an annual basis to determine the priorities of the internal audit activity, which, in turn, should be consistent with the organization's goals and strategies. Furthermore, CAEs should consider consulting engagements based on their potential to add value and improve the organization's operations and risk management activities. These activities have been documented by The HA Research Foundation's Common Body of Knowledge 2006 study, which found that nearly all CAEs interviewed plan their audit activities at least annually, including 36.4 percent who update their audit plan multiple times per year. (Figure 1)



(Source: *A Global Summary of the Common Body of Knowledge 2006*, The IIA Research Foundation)

To develop a risk-based audit plan, CAEs should first perform a companywide risk assessment. The proper execution of an appropriate IT risk assessment — that is part of the overall risk assessment — is a vital component of companywide risk management practices and a critical element for developing an effective audit plan. "For many organizations, information and the technology that supports it represent the organization's most valuable assets. Moreover, in today's competitive and rapidly changing business environment, management has heightened expectations regarding IT delivery functions: Management requires increased quality, functionality and ease of use; decreased delivery time; and continuously improving service levels while demanding that this be accomplished at lower costs."

Regardless of the methodology or frequency of audit planning activities, the CAE and the internal audit team should first gain an understanding of the organization's IT environment before performing the audit. The use of technology is an essential part of an organization's activities. From the collection, processing, and reporting of accounting information to the manufacturing, sales, and distribution of products, virtually every business activity relies on the use of technology to some extent. The use of technology also has evolved to where it is not only supporting a business process but, in many cases, it is integral to controlling the process. As a result, internal controls in processes and activities are becoming more technology-based, while deficiencies and lack of integrity in supporting technologies are impacting the organization's operations and business objectives significantly.

However, the development of an effective, risk-based IT audit plan has been a difficult task for internal auditors, especially when auditors do not have sufficient background in IT.

Results from several HA external quality assessment reviews (QARs) reveal that developing an appropriate IT audit plan is one of the weakest links in internal audit activities. Many times, instead of doing risk-based auditing, internal auditors review what they know or outsource to other companies, letting them decide what to audit.

This guide offers techniques in how to address this challenge — how to determine what should be included in the IT audit scope and how these audit areas could be organized into manageable audit units — to create an effective IT audit plan for the organization.

3 IT Audit Plan Development Process

Defining the annual audit plan should follow a systematic process to ensure all fundamental business aspects and IT-service support activities are understood and considered. Therefore, it is essential that the foundation for the plan be rooted in the organization's objectives, strategies, and business model. Figure 2 depicts a logical work-flow progression using a top-down approach to define the IT audit plan that will be used in this guide.

The first step in defining the annual IT audit plan is to understand the business. As part of this step, auditors need to identify the strategies, company objectives, and business models that will enable them to understand the organization's unique business risks. The audit team also must understand how existing business operations and IT service functions support the organization.

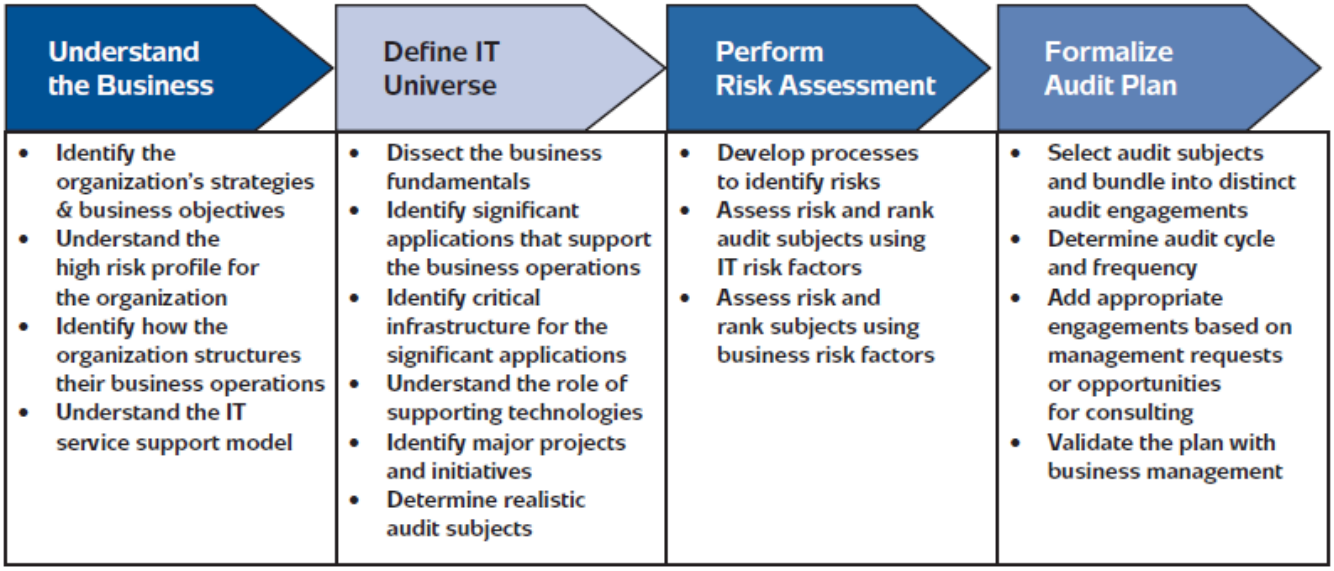


Figure 2. The IT audit plan process

Next, auditors need to define the IT universe. This can be done through a top-down approach that identifies key business objectives and processes, significant applications that support the business processes, the infrastructure needed for the business applications, the organization's service support model for IT, and the role of common supporting technologies such as network devices. By using these technical components, along with an understanding of service support processes and system implementation projects, auditors will be able to create a comprehensive inventory of the IT environment. This inventory, in turn, forms the foundation for assessing the vulnerabilities that may impact internal controls.

After auditors have a clear picture of the organization's IT environment, the third step is to perform the risk assessment — a methodology for determining the likelihood of an event that could hinder the organization from attaining its business goals and objectives in an effective, efficient, and controlled manner.

The information and analysis gained by understanding the organization, inventorying the IT environment, and assessing risks feeds into the final step, formalizing the audit plan. The objective of the audit plan is to determine where to focus the auditor's assurance and consulting work to provide management with objective information to manage the organization's risks and control environment.

The remainder of this chapter follows these four steps and discusses how to define an effective IT audit plan.

3. Understanding the Business

Getting started with the right perspective is paramount to defining an effective IT audit plan. An appropriate perspective to keep in mind is that technology only exists to support and further the organization's objectives and is a risk to the organization if its failure results in the inability to achieve a business objective. Hence, it is important to first understand the organization's objectives, strategies, business model, and the role that technology has in supporting the business. This can be done by identifying the risks found in the technologies used and how each risk might prevent the organization from achieving a business objective. Doing so will result in more meaningful and useful assessments for management.

Furthermore, auditors need to become familiar with the organization's business model. Because each organization has a distinct mission and set of business goals and objectives, business models help auditors to identify the products or services the organization provides, as well as its market base, supply channels, manufacturing and product generation processes, and delivery mechanisms. Having a fundamental knowledge of this information will help auditors understand unique business risks and how technology supports existing business models and mitigates the organization's overall risk profile.

3.1 Organizational Uniqueness

Every organization is different. Even companies operating in the same industry will have different business models, objectives, organizational structures, IT environments, and delivery models. Therefore, audit plans should be defined uniquely for each organization. In addition, the importance of technology might differ within industry segments. Consider the companies that assemble and sell personal computers. Besides using a variety of business models, these companies rely on technology differently to meet business objectives. For instance, the traditional sale distribution model of channeling products through physical stores and resellers require the use of technology to manage operation and accounting activities, while technology reliance is much greater for companies that sell products over the Internet. As a result, the online marketer's revenue stream depends more on the availability of critical IT functionality, which also increases the level of IT risks. As this example illustrates, the way an organization deploys its technology resources and systems creates a unique set of business risks.

3.2 Operating Environment

To become familiar with the organization, auditors first need to understand its objectives and how business processes are structured to achieve objectives (figure 3).

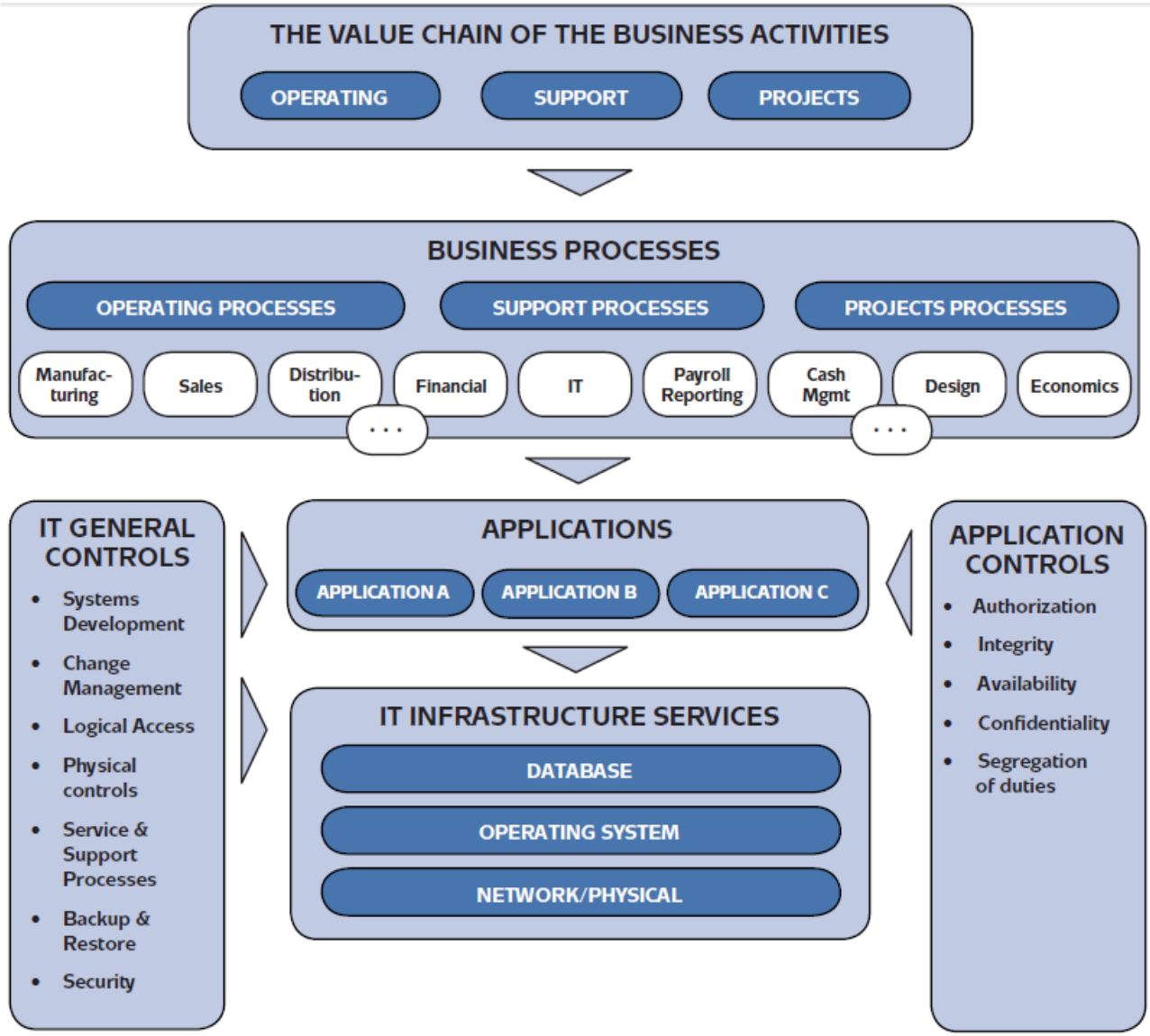


Figure 3. Understanding the IT environment in a business context

Auditors can use different internal resources to identify and understand the organization's goals and objectives, including:

- Mission, vision, and value statements.
- Strategic plans.
- Annual business plans.
- Management performance scorecards.
- Stockholder annual reports and supplements.
- Regulatory filings, such as those submitted to the Securities and Exchange Commission Pakistan(SECP).

After becoming familiar with the organization's entity- level strategic objectives, the next step is to identify the key processes that are critical to the objectives' success. When doing so, auditors need to understand how each business process differs within operating units, support functions, and major organization wide projects, as well as how the process relates and links to entity objectives.

Project processes are unique, but equally important, in ensuring initiatives that add value to the organization are managed and commercialized appropriately. A process is considered key if its

failure prevents the organization from fully achieving the strategic objective to which it is tied. Operating units include core processes through which the organization achieves primary objectives, such as manufacturing, sales, and distribution activities. Support functions include management processes that oversee and support core operational functions, such as governance and compliance activities, finance, human resources, treasury, cash management, and procurement activities.

Once processes are identified, auditors need to outline the significant applications and critical IT infrastructure (e.g., databases, operating systems, networks, and physical environments) supporting these applications. Underlying these applications and IT infrastructure are supporting IT processes, such as systems development life cycles, change management, operations, and security activities. Auditors should note that applications require periodic assessments based on their significance to financial reporting activities, regulatory compliance, or operational requirements.

Examining the operating environment this way (i.e., starting from the top of the organization) will help auditors understand and inventory each critical component. To fully understand the operating environment and its risks also requires a comprehensive understanding of different technology factors that influence and help categorize organizational risks.

3.3 IT Environment Factors

Different factors and analysis techniques should be considered to understand the operational environment and its unique risks. This is because an organization's control environment complexity will have a direct effect on its overall risk profile and system of internal control. Important factors to consider include:

1. The degree of system and geographic centralization (i.e., distribution of IT resources).

The organization's business model may determine the IT function's structure and delivery model. For instance, companies operating with decentralized business units that have the autonomy to make operating decisions may have decentralized IT operations, more diversity of applications, and a larger variety of deployed products. On the other hand, in more centralized companies auditors might find enterprise-based applications and centralized IT infrastructure support. Because risks vary as companies approach either end of the centralization continuum, audit responses should vary accordingly.

When establishing the IT audit universe, consideration should be given to aligning individual audits with the management function that has accountability for that area. A centralized IT delivery model may allow for fewer, but possibly larger, individual audits that are concentrated on core technologies and enterprise applications. Conversely, a decentralized delivery model *could* require more audit engagements to achieve a proper alignment with management accountability.

2. The technologies deployed.

The organization's system architecture diversity will determine the breadth of technical knowledge required within the internal audit function and the number of areas that need to be reviewed. Diversity could be in any and all levels of the IT stack — the key components of an application's technical infrastructure, including its program code, database, operating system, and network infrastructure.

For instance, application program code includes the sets of computer programs, control files, tables,

and user interfaces that provide functionality for specific business operations such as accounting, payroll, and procurement. Other applications could manage critical business information, such as engineering and design project data, legal, and personal medical information. The organization also may have applications that control manufacturing processes commonly called process control systems.

On the other hand, database systems enable the storage, modification, and extraction of data (e.g., Oracle, Microsoft SQL Server, and DB2), while operating systems perform a computer's basic tasks, such as handling operator input; managing internal computer memory; and providing disk drive, display, and peripheral device functions. Examples of operating systems include variations of Windows and UNIX installed in computers and servers. Handheld devices such as personal digital assistants and cell phones also require operating systems.

Finally, networks link computers and enable them to communicate with each other. They consist of physical components, such as switches, routers, firewalls, wiring, and programs that control the routing of data packets. Networks also can be deployed using radio frequency technology, commonly called wireless networks.

All four layers of the stack are essential to enabling automated business functionality and introduce availability, integrity, and confidentiality risks. The degree of risk is based on the criticality of the business activity the technology supports and enables, and on the technology's configuration and deployment. Therefore, the more variety in each of these layers, the higher the organization's risk profile. For instance, it is simpler for IT departments to manage a homogeneous environment of Windows 2003 servers running a SQL Server database for a single enterprise resource planning (ERP) application than a variety of operating systems and database platforms underlying different applications. While ideal, the first scenario might not be practical for a large organization with diverse operations or a decentralized business model. In creating the audit universe, critical IT elements should be identified and assessed as part of the top-down analysis techniques described in this guide.

3. The degree of customization.

Generally, customized implementations add complexity to the management of IT assets. Off-the-shelf software relies primarily on the support of vendors who have a high degree of knowledge and expertise on their products. When vendor software — whether applications, operating systems, or other supporting software — is modified to fit an organization's business need or process, a large amount of ownership is assumed and more risk is introduced into the equation. Generally, organizations should perform a cost-benefit analysis when making the decision to customize third-party software. However, control aspects might not be considered fully in this analysis. In addition, audits of customized implementations also require greater technical knowledge on the part of the auditors.

4. The degree of formalized company policies and standards (i.e., IT governance).

The purpose of an IT governance program is to enable the organization to better manage its day-to-day IT activities and risks through the use of policies and standards. For example, organizations with formalized policies and standards that guide management oversight and help to establish the IT control environment have a better chance of implementing an effective IT governance program. These programs, in turn, are effective when policies and standards are communicated, understood, monitored, enforced, and updated by management.

Policies are general, long-term statements of principle that address management's operational

goals; are intended to have a long-term effect in guiding the development of business rules for specific situations; and can be interpreted and supported by standards, controls, and guidelines. In terms of IT, policies can provide high- level management directives in areas such as intellectual property rights, data protection, retention, and privacy to ensure compliance with laws and regulations and the effective safeguard of data assets.

On the other hand, standards describe a mandatory business process or procedure and provide further direction on how to comply with the policy statement to which they are linked. IT standards are generally technology- neutral and can be further defined by technology-specific controls and guidelines (i.e., configuration settings or procedures) that define how the standard should be implemented.

As a general rule, organizations should establish an ongoing maintenance process for all policies and standards that addresses the latest regulatory mandates. For example, recent changes to the U.S. Federal Rules of Civil Procedure governing the production of evidence in court cases address the discovery and production of electronically stored information. Because of these changes, an organization's level of risk partly depends on its adherence to updated record retention policies and standards that consider the management of electronically stored information.

Different IT governance frameworks and methodologies are available, including COBIT, ISO's 27002 Standard on information security management, the Canadian Institute of Chartered Accountants' IT Control Guidelines, and the Information Security Forum's Standard of Good Practice for Information Security. These frameworks provide a structured way of categorizing control objectives and control areas across the entire control environment. (For additional information on these and other compliance frameworks, auditors can refer to The IA's Information Technology Controls GTAG.5) Organizations can adopt one of these frameworks or use them as a reference when developing their own. Section 5.3 provides information on leading IT governance best practices to help organizations assess the content and effectiveness of these frameworks.

5. **The degree of regulation and compliance.**

Organizations in highly regulated industries generally will have a high-risk profile due to the potential consequences of noncompliance with regulatory mandates. However, successful organizations in highly regulated industries also have disciplined control environments and effective management oversight to ensure ongoing compliance, which results in a lower residual risk profile. The organization's regulatory requirements, therefore, should be appropriately considered in the risk profile and IT audit universe. For example, all organizations registered with the SEC are required by the U.S. Sarbanes-Oxley Act of 2002 to report on the effectiveness of their internal controls over financial reporting. The legislation also created the U.S. Public Company Accounting Oversight Board (PCAOB) to guide public accounting firms on how to conduct an audit of internal controls over financial reporting. Other regulations include the Basel II Accord in the finance sector and a growing number of privacy and data protection laws and regulations, such as the European Union's Directive on Data Protection, U.S. Gramm-Leach-Bliley (GLBA) Act, the U.S. Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS).

6. The degree and method of outsourcing.

IT outsourcing is becoming more prevalent in many organizations due to the high cost and expertise required to deliver noncore services. (The IIA's Information Technology Outsourcing GTAG provides a detailed discussion on the types of IT outsourcing arrangements and their degree of risk.6) In terms of outsourcing, it is important for auditors to consider the different risks stemming from the

outsourcing arrangement when drafting the IT audit plan. Key factors include how management views its oversight and monitoring role, the maturity of the arrangement (e.g., transitioning versus an established working process), country-specific risks, and the completeness of the vendor's and organization's business continuity plans.

The degree of operational standardization.

Operational processes and procedures include the entire system development life cycle as well as configuration, change, incident, operations, and security management activities. Similar to the degree of centralization and the diversity of deployed technologies, the level of operational standardization can impact the reliability and integrity of the IT infrastructure and its assets. Consequently, organizations that adopt standardized processes throughout their service delivery functions increase their ability to operate as a high-performing organization.

An example of a standardized practice is ITIL, a set of concepts and techniques for managing IT infrastructures, as well as the development and installation of new computer systems and IT operations. Its books on service support and service delivery are the most widely used and understood ITIL publications. One of the primary benefits of ITIL is that it establishes a common vocabulary of defined and widely used terms. Organizations that implement ITIL concepts have claimed a higher degree of reliability and lower delivery costs.

8. **The level of reliance on technology.**

Some organizations are intensive technology users or use technology to differentiate themselves from their peers and competitors. While technology can improve overall internal controls with the use of automated application controls, strong governance and internal operational processes become more important as reliance on IT increases. In addition, as organizations depend more on the availability and integrity of IT functionality to enable business operations and meet their objectives, the significance of IT risks in the organization's overall risk profile increases. Hence, the nature and extent to which the organization relies on technology should be evident in the risk assessment used to develop the IT audit plan.

These eight IT environment factors, along with the top-down approach used to understand the organization's operations and IT infrastructure, provide auditors with the information needed to move to the next step of the audit planning process — defining the IT audit universe and performing a risk assessment.

4. Defining the IT Audit Universe

Determining what to audit is one of the most important internal audit activities, as performing the annual IT audit plan will have a profound impact on the overall success of the internal audit department. Consequently, the ultimate goal of the IT audit plan is to provide adequate coverage on the areas that have the greatest risk and where internal auditors can add the most value to the organization.

One of the first steps to an effective IT audit plan is to define the IT universe, a finite and all-encompassing collection of audit areas, organizational entities, and locations identifying business functions that could be audited to provide adequate assurance on the organization's risk management level. At this initial phase, identifying potential audit areas within the IT universe is done independently from the risk assessment process. Auditors need to be aware of what audits could be performed before they can assess and rank risks to create the annual audit plan. Defining the IT audit universe requires in-depth knowledge of the organization's objectives, business model, and the IT service support model.

4.1 Examining the Business Model

Organizations can have different operational units and support functions to accomplish its objectives, which, in turn, have business processes that link activities to achieve their goals.

Referring back to the example of companies that assemble and sell personal computers, a traditional company in this industry sector consists of several assembly plants located in different countries, sales, and marketing units, as well as different corporate management and support functions. The sales and marketing units, for instance, have established processes for accepting, fulfilling, and invoicing customer orders, while other operating units and support functions have their own processes. Underlying these processes will be critical IT applications and supporting infrastructure. Therefore, it is important for auditors to understand the company's IT environment when defining the IT universe and identifying the processes critical to the success of each unit.

Using a top-down approach to understand the organization's structure and activities can help auditors identify critical IT functionality processes that sustain the organization's operating units and support functions. However, variation in how similar business units perform their processes can add complexity to this analysis. For instance, manufacturing plants in different locations might use different procurement processes. In decentralized organizations, business units might use different applications for similar business processes, or a common application might be configured differently to the extent it functions like an entirely different application. For example, one business unit uses SAP R/3 on a UNIX and Oracle platform, while another business unit uses SAP R/3 on a Windows and SQL Server platform. Although similar, the IT support structure for these business processes is different and may require separate assurance reviews.

4.2 Role of Supporting Technologies

Identifying supporting IT infrastructure technologies can be a simple process when detecting business activities that rely on key applications. However, it is much harder to associate the use of supporting technologies, such as the company's network, e-mail application, and encryption software, to business objectives and risk. Yet, these supporting technologies exist because the business requires them, and a failure in these services and products can hinder the organization's ability to accomplish its mission. Therefore, key supporting technologies, while not directly associated with an application or business process, must be identified and represented in the universe of auditable areas.

4.3 Annual Business Plans

Another important element is to take into consideration the organization's annual business plans and strategies. Operating plans can provide auditors with information on important changes and projects that may be pursued in the upcoming year, which might require audit involvement and become subjects in the IT audit universe. Projects might be directly IT-related, such as the implementation of a new ERP system, or business projects that manage major engineering or construction initiatives. For example, energy companies form major capital projects when developing new facilities to bring oil and gas discoveries into production. These business projects can benefit from the use of critical IT components that merit IT audit attention, such as access controls over document management systems and external network connections for partners and contractors. Because companies can be partners on one project and competitors on another, it is important to limit their access to required IT resources only.

4.4 Centralized and Decentralized IT Functions

Auditors need to identify centrally managed IT functions that support the entire or a large portion of the organization. Centralized functions are good candidates for individual audits in the IT audit universe and include network design and security administration, server administration, database management, service or help desk activities, and mainframe operations. For example, the organization may have a server administration group that is responsible for all Windows servers. Because this group might use common configurations and administrative processes across the entire server population, it represents an ideal candidate for an individual IT audit that is part of the IT audit universe. The homogeneous nature of the environment also lends itself to sampling for the audit's execution.

There are several benefits to identifying centralized audit subjects. The main benefit is the effective use of limited IT audit resources, which can enable the audit team to focus on one area, use sampling techniques, and gain a large amount of coverage in a single audit. Another benefit is the transfer of internal audit efficiencies to other audits because centralized areas have already been covered and may be excluded from the scope of other audits. The benefit of referencing centralized audit coverage is particularly applicable to application auditing. For example, there could be hundreds of applications residing within a Windows server administration group environment. Since the general controls for the infrastructure are reviewed in a more centralized audit, the IT audit should be limited to application-specific technical areas rather than the entire infrastructure platform hosting the application. The organization also benefits as it is audited thoroughly only once and is not impacted when applications are reviewed individually during each business process audit.

Furthermore, organizations may centralize their IT functions differently. A common practice of many organizations is to create a single network support function that manages its network design and security administration. This network support function could be divided into firewall, router, and switch configuration activities, as well as Internet connectivity, wireless, digital voice, and external network connection management. As a result, each of these areas may be an independent audit subject in the IT universe. Furthermore, because centralized IT functions can change over time, they should be reviewed and refreshed in the audit universe at least annually.

A similar approach can be taken for decentralized IT functions, where each physical location might represent a separate audit subject. Depending on the location's size, the site's audit may review general and technical controls for each infrastructure stack layer. The review should only include the IT controls for which the local site is responsible, while controls handled by centralized IT functions should be excluded. If the site is large and supports a wide number of technologies, auditors might need to perform multiple reviews for that location as part of the IT audit universe.

4.5 IT Support Processes

Even if the organization has a decentralized IT function, it may have standardized support processes. Organizations that are striving to be high-performing organizations understand the importance of having standardized support processes across their operating units regardless of the business model. Examples of standardized support processes include service desk activities as well as change, configuration, release, incident, and problem management procedures. The service desk is generally the first point of contact for customers to register an IT service or issue resolution request, thus initiating the request's life cycle management process and triggering a

chain of events including incident, problem, change, and release management activities.

Again, one of the leading sources for IT service best practices is ITIL. Many organizations are implementing ITIL practices or other standardized processes to attain better efficiency and higher

performance in managing their IT functions. Internal audit groups should become involved in efforts to implement standardized support processes where appropriate and consider new ways to provide assurance on their effectiveness. One approach could be to review the deployment and governance of standardized processes at the enterprise level within the audit plan. These top- level reviews could assess the effectiveness of the processes themselves, the effectiveness of deployed processes, and the effectiveness of the governance model to ensure standardized support processes are used as intended. Once standardized processes are audited, site audits should concentrate on how they are followed rather than on their effectiveness.

4.6 Regulatory Compliance

Different laws and regulations around the world are mandating the use of internal controls and risk management practices and the privacy of personally identifiable information, including the Sarbanes-Oxley Act and Basel II Accord. As discussed earlier, some of these regulations mandate the protection of customer information in the credit card industry (e.g., GLBA and the PCI DSS) and the safeguarding of personal medical information (e.g., HIPAA). Although most of these regulations do not address IT controls directly, they imply the need for an adequately controlled IT environment. Therefore, these regulatory areas are potential subjects in the IT audit universe, as auditors need to determine whether the organization has rigorous processes in place and whether they are operating effectively to ensure compliance.

4.7 Define Audit Subject Areas

The way the IT environment is divided into individual audit subjects could be somewhat influenced by personal preference or staffing considerations. However, the ultimate goal is to figure out how to divide the environment in a manner that provides the most efficient and effective audits. The preceding discussions on centralized IT functions and standardized support processes stated how audit subjects can be grouped in the audit universe to define an audit approach that is more efficient. Although auditors should not be assessing business risks at this phase of the audit planning process, the goal is to have an audit plan that focuses on the highest-risk areas where auditors can add the most value.

Although there is no single right way to define IT audit subjects, there are incorrect or inappropriate ways to do this.

Pitfalls include improper sizing of subjects, basing a plan solely on staffing capabilities, and creating a focus imbalance. In addition, audit subjects should be divided into appropriately sized areas to define a reasonable allocation of audit resources. When doing so, auditors should keep in mind that defining small or large audit subject areas might hinder audit efforts. This is because a certain amount of overhead is required for each audit engagement, including administrative efforts for audit planning, management reviews, sign-offs of completed work, and reporting and communicating results. If the audit universe and plan contains numerous small audits, for example, internal auditors could spend as much time administrating the audits as performing them. Conversely, if the audit subject area is defined broadly, audits could run for an extended period of time, be disruptive to the client, or be reviewed insufficiently. Depending on the organization's culture, overly broad definitions might even result in an unplanned increase in scope (i.e., scope creep).8

Finding the right audit size depends on the organization's audit practices and culture. As a general rule for most organizations, defining audit subjects that require two to three technical auditors for a three- to four-week duration is a reasonable target, as this provides different auditor perspectives

and experiences. In addition, the three- to four-week duration is a reasonable request for most organizations.

The audit size also should be consistent with company- accepted historical audit practices. However, the IT audit universe should not be defined solely on audit staffing capability, as this might result in a focus imbalance. For instance, some IT audit functions do not have any technicians or IT professionals, but consist of business auditors who have knowledge of currently used business applications. Because these auditors tend to focus on the application layer and might ignore the underpinning infrastructure layers, it's important to have a well-balanced coverage of all layers as part of the audit.

Ideally, the internal audit function should consist of highly technical personnel and general auditors who have a good understanding of application controls. The technical auditors, for example, would help ensure the IT infrastructure has proper security controls in place and review general application controls. The proper balance of audit subjects covering all environment layers should be the cornerstone of the IT audit plan even if the IT audit constraint is an issue. If that is the case, alternative resource staffing for these audits would be required to supplement the expertise of the internal audit staff.

Auditors should consider that the audit technique used during the security review could be ineffective when used in a nonhomogeneous server environment consisting of multiple server platforms. This is because the general server administration subject area might be too large or unmanageable.

For this reason, many organizations review security based on their platform type, thus enabling a more detailed review. Unfortunately, this activity could result in redundancy as audit steps are duplicated. Hence, auditors could establish separate audit areas for each platform type and a general controls subject audit that is performed across all platforms.

A key consideration in identifying IT environment components and in grouping distinct audit subjects is management accountability. A worst-case scenario would be to define audit subjects crossing reporting lines and involving management from different reporting units, as this might create a conflict over who eventually owns the resolution of issues presented in the audit. As a result, it should be clear who will receive the audit report and who is responsible for the remediation of identified control deficiencies. Finally, the scope of each audit subject should be described clearly so that organizational accountability is determined properly.

4.8 Business Applications

CAEs need to determine which audit group will be responsible for the planning and oversight of business application audits. Depending on how the audit function operates, business applications can be included as part of the IT audit universe, business audit universe, or both. There is a growing consensus among internal audit functions that business applications should be audited with the business processes they support. This provides assurance over the entire suite of controls — automated and manual — for the processes under review, helps to minimize gaps and overlaps of audit efforts, and minimizes confusion over what was included in the scope of the engagement.

Because of their expertise, the business audit function is probably best suited to determine when applications should be reviewed. If business applications are maintained as part of the IT audit universe, the business audit universe should be linked to the IT audit universe to work together during the audit. Even if business applications are maintained separately from the IT audit universe, individual audit subjects can be created within the IT audit universe for large-scale applications that

are used by multiple functions for multiple processes, such as ERP systems. This is because it might make sense to review the application's general controls in a standalone audit rather than arbitrarily including this area in one of the many business audits.

4.9 Assessing Risk

After the IT universe is defined, a systematic and uniform assessment of risk across all subjects should be the next step in determining the annual audit plan. The next section presents risk and risk assessment fundamentals that can help CAEs and internal auditors create an effective IT audit plan.

5. Performing a Risk Assessment

The HA defines *risk* as the possibility that an event will occur that could affect the achievement of objectives, which is measured in terms of impact and likelihood.' Therefore, it is vitally important for organizations to determine the contents of their risk portfolio periodically and perform activities to manage risks to an acceptable level. As discussed earlier, the risk assessment process should not be conducted until the CAE and internal audit team understand the contents of the IT universe and how they link back to or support the organization. It is paramount — no matter the risk assessment model or approach used — for the risk assessment to determine IT environment areas that can significantly hinder the organization's achievement of objectives. In other words, the risk assessment needs to examine the infrastructure, applications, and computer operations or components that pose the greatest threat to the organization's ability to ensure system and data availability, reliability, integrity, and confidentiality.

In addition, auditors need to identify the effectiveness and usefulness of risk assessment results, which should be directly predicated on the methodology employed and its proper execution. That is, if the risk assessment's methodology input (i.e., the IT universe and its link to the business audit universe) is deficient or is applied incorrectly, it is likely that the output (i.e., risk assessment results) will be incomplete in some capacity.

5.1 Risk Assessment Process

After the CAE and internal audit team understand the organization and its use of technology, they can conduct the risk assessment. Performing this task correctly is paramount to ensuring relevant IT risks (i.e., those with the greatest likelihood of occurrence and impact to the organization) are identified and evaluated effectively and adequate mitigation measures take place. The culmination of the risk assessment process is then used by the CAE and audit team to develop the IT audit plan.

5.1.1 Identify and Understand Business Objectives

One of the foundational elements of any risk assessment methodology is gaining an understanding of the organization's business objectives and determining how IT is used to assist or support the achievement of these objectives. If business objectives are not identified, auditors need to perform this activity before performing the IT risk assessment. Business objectives may be broad and strategic in nature (e.g., become the industry leader) or more linear and tactical in nature (e.g., replace legacy IT applications with an ERP solution).

Furthermore, risk management processes should have five key objectives:

- Risks arising from business strategies and activities need to be identified and prioritized.
- Management and the board need to determine the level of risk acceptable to the organization, including the acceptance of risks designed to accomplish the organization's

strategic plans.

- Risk mitigation activities need to be designed and implemented to reduce or otherwise manage risk at levels that are acceptable to management and the board.
- Ongoing monitoring activities need to be conducted to reassess risk periodically and the effectiveness of controls to manage risk.
- The board and management need to receive periodic risk management process reports. The organization's corporate governance processes also should provide periodic communication of risks, risk strategies, and controls to stakeholders.

5.1.2 Identify and Understand IT Strategy

Once CAEs and internal auditors become familiar with the organization's objectives, they need to identify the company's overall IT strategy to understand how it aligns with the objectives identified in the prior step. Because the organization could have different forms of documentation showing the relationship between its business objectives and the IT strategic plan, CARS and internal auditors need to obtain, read, and understand these documents. Generally speaking, the IT strategic plan should link back to organizational objectives and provide clear direction as to how it links back to these objectives. In other words, the IT plan should identify tactical actions to be performed by the IT department within a defined period of time, which are designed to support the achievement of the organization's objectives.

5.1.3 IT Universe

As discussed earlier, auditors first need to inventory the key computing environment components to determine which IT areas need to be reviewed from a risk and controls perspective. While there isn't a single-best approach to perform the inventory, many organizations divide their IT universe into three major sub-categories: infrastructure, computer operations, and applications.

The infrastructure area consists of all computing components that support the flow and processing of information, such as servers, routers, bridges, mainframes, communication lines, printers, datacenters, networking equipment, antivirus software, and desktops. Computer operations, on the other hand, consist of the processes and controls that manage the computing environment. Examples include physical and logical security administration, backup and recovery, business continuity and disaster recovery planning, service-level agreements (SLAs), program change controls, and compliance with laws and regulations. Finally, applications consist of the software used by the organization to process, store, and report business transactions. Examples include ERP systems and stand-alone applications, such as Microsoft Excel or Access.

5.2 Ranking Risk

Once an inventory of the IT universe is completed, the next step is to assign a risk rating to all sub-categories — infrastructure, computer operations, and applications. These sub-categories need to be ranked based on the impact their risks will have on the organization and their likelihood of occurrence. In other words, auditors need to determine what could go wrong in each area and how the organization will be affected if controls to manage or mitigate risk are not designed and operating effectively.

In addition, auditors need to keep in mind that each risk might not be equally significant or weighed the same way across the IT audit universe. (Weight differentiates the relative importance of a risk

over the others). For example, if an area has a direct tie to the accuracy of financial reporting, it would carry a higher weight relative to an area that does not directly affect the accuracy of financial reporting. According to The Research Foundation's Assessing Risk, there are three approaches to measuring risk and impact:"

1. **Direct probability estimates and expected loss functions or the application of probabilities to asset values to determine exposure for loss.** This process is the oldest and not considered a best practice. The insurance industry still uses this method, but internal auditing does not.

2. **Risk factors or the use of observable or measurable factors to measure a specific risk or class of risks.** This process is favored for macro-risk assessments, but is not efficient or particularly effective for micro-risk assessments, except when auditable units are homogeneous throughout the audit universe as in branch, location, or plant audits.
3. **Weighted or sorted matrices or the use of threats versus component matrices to evaluate consequences and controls.** This method is superior for most micro-risk assessments.

This GTAG will focus exclusively on the weighted or sorted matrices approach to measure risk and impact. As shown in table 1, this approach uses a simplistic method to rate risk that is based on the risk's high (i.e., three), medium (i.e., two), or low (i.e., one) likelihood of occurrence.]

Likelihood Scale		
H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low probability that the risk will occur.

Table 1. Risk likelihood scale

While the likelihood of risk occurrence is relatively simple to determine, determining the impact of risk occurrence is another matter entirely. This is because there can be several different qualitative and quantitative aspects of risk impact. Furthermore, not every qualitative and quantitative aspect is treated equally (i.e., some risks are more important than others). According to Assessing Risk, three types of risk factors are commonly in use — subjective risk factors, objective or historical risk factors, and calculated risk factors.

1. **Subjective risk factors.** Measuring risk and its impact requires a combination of expertise, skills, imagination, and creativity. This emphasis on subjective measurements is borne out in practice — many auditable units change so much between audits that prior audit history is of little use. Therefore, an experienced practitioner's sound subjective judgment is just as valid as any other method.

2. **Objective or historical risk factors.** Measuring risk factor trends can be useful in organizations with stable operations. In all cases, current objective information is helpful in measuring risk.

3. **Calculated risk factors.** A subset of objective risk factor data is the class of factors calculated from historical or objective information. These are often the weakest of all factors to use because they

are derivative factors of risk that is further upstream.

Due to these risk factors, CAEs and internal auditors must design and use a risk impact model that fits their organization. The model should be similar to the one used for the enterprise wide risk assessment. However, the model's scale and rank methodology needs to be changed for each IT risk. As shown in table 2, and for the purposes of this GTAG, a simplistic ranking method that uses high, medium, and low categories is used for the impact of each component that is based on the same likelihood concepts presented in table 1.

Impact Scale (Financial)		
H	3	The potential for material impact on the organization's earnings, assets, reputation, or stakeholders is high.
M	2	The potential for material impact on the organization's earnings, assets, reputation, or stakeholders may be significant to the audit unit, but moderate in terms of the total organization.
L	1	The potential impact on the organization is minor in size or limited in scope.

Table 2. Risk impact model scale

Table 3 shows an example of a completed risk assessment that is based on the scales used for likelihood and impact across the risk categories of financial impact, quality of internal controls, changes in the audit unit, availability, integrity, and confidentiality. The score for each area is calculated by multiplying risk's likelihood and impact values across each category. For example, on the risk category for ERP application and general controls, the sum of the likelihood and impact values is 42. The same logic is used across the other risk categories for each possible audit area.

Area	Financial Impact		IT Risks										Score and Level	
			Quality of Internal Controls		Changes in Audit Unit		Availability		Integrity		Confiden-tiality			
	L	I	L	I	L	I	L	I	L	I	L	I		
ERP Application & General Controls	3	3	2	3	3	3	2	3	2	3	2	3	42	H
Treasury EFT Systems	3	3	3	3	3	3	2	2	3	2	2	2	41	H
HR/Payroll Application	3	3	3	2	3	3	2	2	2	3	2	3	40	H
Employee Benefits Apps (Outsourced)	2	3	2	2	3	3	3	2	2	3	3	3	40	H
IT Infrastructure	2	2	3	2	3	3	3	3	3	2	2	2	38	H
Process Control Systems	1	1	2	2	2	2	2	2	1	1	1	1	15	L
Database Administration and Security	2	2	2	2	2	2	3	3	2	2	2	1	27	M
UNIX Administration and Security	2	2	2	3	2	2	3	1	1	1	3	2	24	M
Corp. Privacy Compliance	2	2	3	2	3	3	2	1	2	2	3	3	34	M
Windows Server Admin and Security	2	2	1	2	2	2	2	3	3	2	2	2	26	M
Environment Reporting Systems	2	2	3	2	2	2	2	3	1	1	3	1	24	M
SOX Sustainability Review	2	2	2	2	2	2	1	1	2	2	1	2	19	L
Network Administration and Security	2	2	1	1	1	2	2	1	2	2	2	2	17	L
ITIL Deployment Practices	1	1	1	3	2	1	3	1	1	3	3	3	21	M
IT Governance Practices	1	1	2	2	1	1	3	1	1	1	1	2	12	L
Remote Connectivity	1	1	1	2	2	1	1	1	1	2	2	2	12	L
Application Program Change Control	2	3	1	3	1	1	1	1	1	3	1	2	16	L
Lowest possible score			6											
Highest possible score			54											
Mid point			30											
L = Likelihood I = Impact														

Table 3. Example of an IT risk-ranking score model

Based on this scoring approach, the lowest possible score is six and the highest possible score is 54. Table 4 shows the scoring ranges and their corresponding audit or review frequencies based on the organization's resource availability.

Level	Composite Risk Score Range	Recommended Annual Cycle
H	35–54	Every 1 to 2 years
M	20–34	Every 2 to 3 years
L	6–19	Every 3 to 5 years

Table 4. Scoring ranges and corresponding audit or review frequencies

5.3 Leading IT Governance Frameworks

Up to this point, the guide has focused on the steps necessary to define the IT audit universe and to perform a risk assessment that determines what should be audited and how often. This discussion is not based on any particular IT governance framework, such as COBIT, the ISO 27002 Standard, or ITIL. As a result, it is the CAE's responsibility to determine the components of these and other frameworks that best serve the organization. It is important to keep in mind that none of these frameworks is a "one-size-fits-all." Rather, they are frameworks organizations can use to manage and improve their IT functions. While it is not within the scope of this GTAG to provide guidance on the pros and cons of these and other IT governance models, an overview of COBIT will be provided. Since its release in 1996, COBIT has been a leading IT governance framework. Its mission is "to research, develop, publicize, and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors."11 As a framework and supporting tool set, COBIT allows organizations to bridge the gap with respect to control requirements, technical issues, and business risks, and communicate that level of control to stakeholders. COBIT also enables the development of clear IT control policies and practices. In addition, COBIT provides a set of tools CAEs and internal auditors can use to help guide the IT risk assessment process. Some of its tools are a set of clearly stated control objectives, ideas on how to test controls, and a scale for ranking the maturity of the IT control environment. The COBIT framework consists of four domains with a total of 34 IT processes: plan and organize (PO), acquire and implement (AI), deliver and support (DS), and monitor and evaluate (ME). As with any best practice control framework, auditors should proceed with caution when using this framework. CAEs and internal auditors must understand and apply the framework's concepts and guidance in their proper context. In other words, COBIT has been developed and refined over the last decade with the assistance of practitioners, academia, and different industries from around the globe. As a result, COBIT tends to have the look and feel of a framework that might work beautifully in a large organization with a sizable IT function, but may be equally challenging to work with in mid-size and small organizations. Furthermore, the CAE and internal audit team must realize that simply because the IT function does not follow or adhere to the COBIT framework, this does not mean the IT function, its processes, or data is not controlled or managed properly. At a minimum, CAEs and internal auditors can use COBIT as a helpful guide during the IT risk assessment and audit process. In a best case scenario, the CAE and internal audit team should integrate the use of COBIT under the

umbrella of risk and control-related frameworks and guidance, as well as to help the IT function with implementing part or all of the framework.

6. Formalizing the IT Audit Plan

Defining the IT audit universe and performing a risk assessment are precursor steps to selecting what to include in the IT audit plan. While everything in the IT audit universe could be reviewed on a recurring basis if the availability of resources is unlimited, this is not the reality for most internal audit functions. Consequently, CAEs must create an IT audit plan within the constraints of the audit function's operating budget and available resources.

6.1 Audit Plan Context

Figure 4 depicts the differences and challenges of moving from the risk assessment step to identifying the audits that will be included as part of the audit plan. In theory, each of these steps should be a separate and distinct effort because the objectives and focus are different. In the risk assessment, the objective is to understand risks in a relative context. Therefore, the major focus or driver of this effort is risk, while a major influencer may be resources. In defining the audit plan, the objective is to review high-risk areas through the allocation of available resources. As such, the driver is the resources and the influencer is the risks.

For most companies, these two steps are merged to some extent, as depicted in the overlap area of the two spheres representing each process in figure 4.

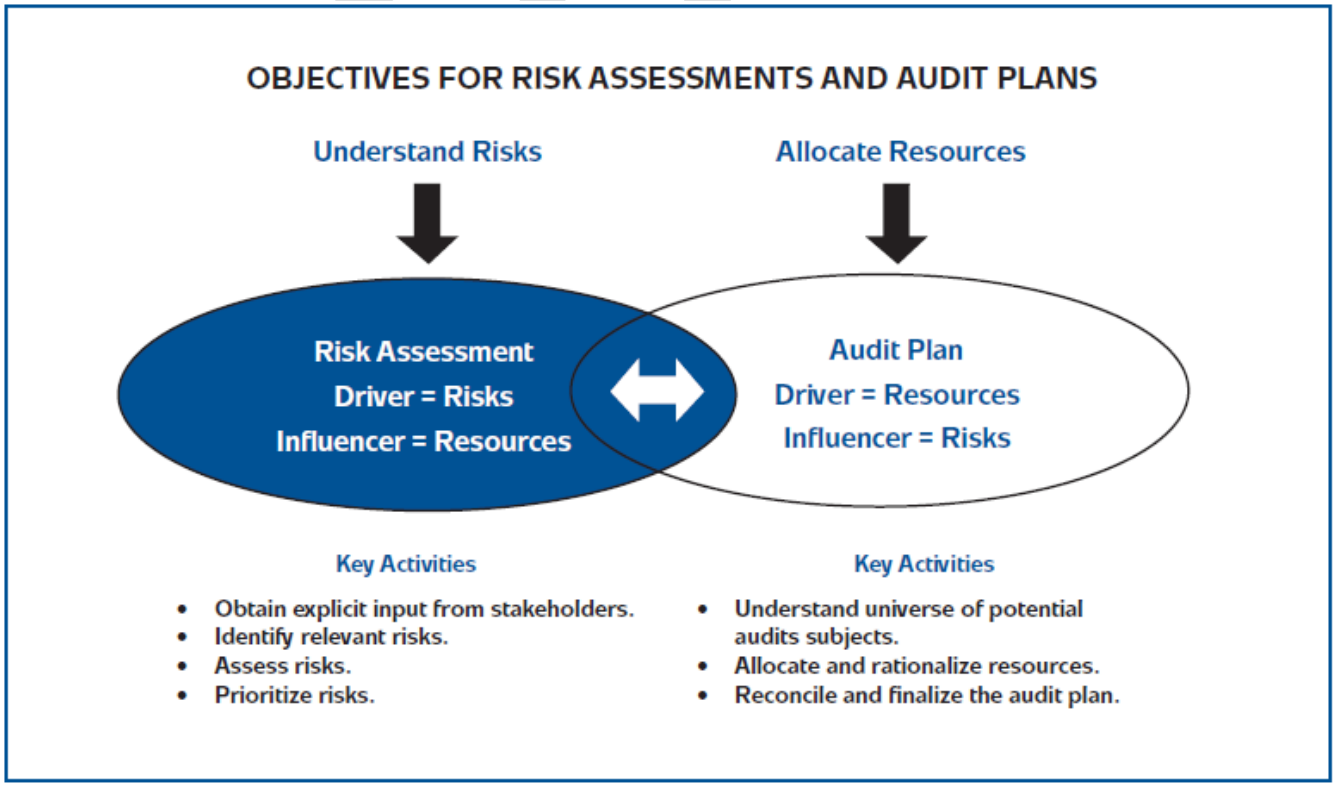


Figure 4. Objectives for risk assessment and audit plan

For example, certain risks or auditable areas may be excluded from the risk assessment based on the level of resources that may be required to execute the audit. However, it is important to perform these steps in an objective manner considering each step's stated objective and driver forces. In addition, the IT audit plan should be created as part of the internal audit function's strategic planning process. This planning process should be cyclical and can be understood under the classical management cycle of "plan, do, check, and act." Thus, while the plan is the key enabler to implement the process, it delineates how to reach audit objectives and goals. As a result, it should include a list of audit activities as well as the timing, dependencies, and resource allocation needed to reach audit goals. Certain IIA standards describe the nature of internal audit services and provide quality criteria against which the performance of these services can be measured. More specifically, the 2000 series, Performance Standards for Managing the Internal Audit Activity, are relevant to the audit planning process:

• **IIA Standard 2010: Planning.** The CAE must establish risk-based plans to determine the priorities of internal audit activities consistent with the organization's goals.

• **IIA Standard 2020: Communication and Approval.**

The CAE must should communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and board for review and approval. The CAE must also communicate the impact of resource limitations.

• **IIA Standard 2030: Resource Management.** The CAE must ensure that internal audit resources are appropriate, sufficient, and deployed effectively to achieve the approved plan.

6.2 Stakeholder Requests

Internal auditors should have ongoing discussions throughout the IT audit plan's development with key stakeholders to better understand the business and risks the organization faces. Through these discussions, insights on the business will be gathered along with concerns key stakeholders might have. This is also an opportunity to learn about special audit assurance and consulting services requests, referred to in this document as stakeholder requests. Stakeholder requests may come from the board of directors, audit committee, senior managers, and operating managers. They should be considered during the audit planning phase based on the engagement's potential to improve the overall management of risks and the organization's control environment. These requests may be specific enough to determine the required resource allocation, or the allocation may be based on previous audit work. These engagements also can include fraud investigations that come up throughout the year and requests to review service providers. (The IIA Standard 2010.C1 provides information on consulting engagements.) CAEs, therefore, should consider accepting proposed consulting engagements based on their potential to improve risk management activities and add value to and improve the organization's operations. Accepted engagements must be included in the IT audit plan.

6.3 Audit Frequency

Depending on the risk assessment's results, not all audit areas can nor should be reviewed in every audit cycle. As presented in section 5, audit frequency is based on an evaluation of the likelihood

and impact of risk occurrence in relationship to the organization's objectives. Since audits occur on a cyclical basis, multiyear audit plans are developed and presented to management and the audit committee for review and approval. The multiyear plan, usually three to five years in terms of its timeframe, is created to document what audits will be performed and when, ensure adequate audit coverage is provided over this period of time, and identify audits that may require specialized external resources or additional internal resources. In addition, most organizations create a one-year plan, as a derivative of the multiyear plan that outlines planned audit activities for the upcoming year. Auditors can use one of two strategies to arrive at the ideal frequency of planned audit activities:

- The audit frequency is established in an initial risk assessment to take place every three to five years and is proportional to the risk level.
- The audit plan is based on a continuous risk assessment without a predefined audit frequency.

Some organizations use this approach, which is especially appropriate within the context of the IT audit plan, given the higher rate of IT change as compared to changes in non-IT activities. Table 5 shows criteria that can be used to determine frequency and resource allocation based on the results of the risk assessment. This process should be understood as a cyclical, repetitive, and iterative sequence of activities, integrating a top-down approach through at least three layers:

- Layer 1: The audit universe where all the inputs are integrated.
- Layer 2: The individual business processes where engagements should be identified and preliminarily planned.
- Layer 3: The audit engagements where fine-tuning and plan optimization can be conducted.

	Priority	Frequency	Resource Allocation
H	Immediate action, usually within the first year	Annual reviews or multiple actions within the cycle	High allocation
M	Mid-term action within the audit cycle	One or several audit engagements within the cycle; could be postponed	Base allocation
L	Audit engage-ments usually not planned within the cycle	At most one audit engagement planned within the cycle	Limited allocation

Table 5. Frequency and resource allocation of audit activities

In addition to frequency, other factors should be considered when defining the audit plan:

- **Internal audit sourcing strategies.**

Different sourcing or staff augmentation strategies are common practices in the industry, including hiring internal staff, outsourcing, and co-sourcing, which should be considered during the annual planning process.

- **Estimated available IT audit resources.**

This consists of a technical skills inventory of current staff that is mapped to IT audit plan needs. The availability of resources usually is established on an annual basis and is based on the number of full-time equivalent auditors and skills required. Available audit days are the net of possible audit days minus non audit activities and exception time, such as training, vacation, and holidays.

- **Board and management requests included in the plan and related to control assurance or consulting services.**
- **The organization's regulatory and compliance requirements.**

These should be included in the audit universe and risk assessment.

- **External audits that should be synchronized with the audit plan.**

The IIA Performance Standard 2050 establishes that the CAE should share information and coordinate activities with other internal and external providers of relevant assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

- **Internal initiatives and efforts to improve the audit function.**

Any effort beyond audit engagements that represents an investment of effort should be planned, budgeted, and reflected in the audit plan. Examples include quality assurance reviews, integrated risk assessments, audit committee reporting tasks, and audit recommendation follow-ups.

- **A contingency IT audit budget and plan for reasonable coverage of unplanned situations.**

6.4 Audit Plan Principles

Internal auditors should consider linking the Audit Plan to Risk and Exposures when dentifying audit plan principles:

1. In developing the internal audit activity's audit plan, many chief audit executives find it useful to first develop or update the audit universe, i.e., a list of all the possible audits that could be performed

2. The audit universe can include components from the organization's strategic plan so that it reflects the overall business' objectives and attitude toward risk and the degree of difficulty to achieving planned objectives.

3. The CAE prepares the internal audit activity's audit plan based on the audit universe, input from senior management and the board, and an assessment of risk and exposures affecting the organization.

4. The audit universe and related audit plan are updated to reflect changes in management direction, objectives, emphasis, and focus on at least an annual basis.

5. Audit work schedules are based on, among other factors, an assessment of risk and exposures. Prioritizing is needed to make decisions for applying resources, and a variety of risk models exist to assist the CAE with that task.

6.5 The IT Audit Plan Content

The content of the IT audit plan should be a direct reflection of the risk assessment described in previous sections.

The plan also should have different types of IT audits, for example:

- Integrated business process audits.
- Audits of IT processes (e.g., IT governance and strategy audits, as well as audits of the organization's project management efforts, software development activities, policies and procedures, COBIT/ISO/ITIL processes, and information security, incident management, change management, patch management, and help desk activities).
- Business projects and IT initiative audits, including software development life cycle (SDLC) reviews.
- Application control reviews.
- Technical infrastructure audits (e.g., demand management reviews, performance reviews, database assessments, operating systems audits, and operation analyses).
- Network reviews (e.g., network architecture reviews, penetration testing, vulnerabilities assessments, and performance reviews).

To verify each audit provides appropriate coverage, auditors can incorporate the following elements as part of the audit:

- IT general controls, application controls, and infrastructure controls.
- Contributions to operational reviews, financial reviews, and compliance reviews.
- Main control objectives (i.e., segregation of duties, concentration of duties, and security, among others).
- New IT trends and their threats, innovations, and impact.
- All IT layers of the stack.

6.6 Integration of the IT Audit Plan

One key aspect of the planning process is to determine the integration level of the IT audit plan with non-IT audit activities in the audit department. As explained in section 4.7, auditors need to determine which audit group will be responsible for the planning and oversight of business application audits. This discussion could be extended to include all IT components. For instance, will the IT audit plan be presented and executed on a stand-alone basis or will IT audit subjects be integrated with business areas? Answers to these questions should be based on the internal audit department's function as well as its staff, size, geographical distribution, and management approach. A range of integration scenarios could be considered from a low integration scenario where the IT audit function is well-defined and established within the internal audit department (i.e., with their own IT audit universe and scope) to a fully integrated audit approach where all IT components are

understood under each business segment. Table 6 illustrates scenarios based on different options to integrate the IT audit plan. These scenarios are:

- **A low-integrated plan.**

This is a stand-alone IT audit plan under the responsibility of the IT audit team. A low-integrated plan is organized by IT subject areas, is generally isolated from non-IT audit activities, and includes the review of applications. Non-IT Audit activities generally do not include any of the IT components within their scope.

- **A partially integrated audit plan, which outlines IT audit engagements that are established by a core IT audit team.**

These plans provide an additional set of planned engagements, generally referred to as application reviews, which are distributed across other non-IT audit teams and coordinated with other business process reviews.

- **A highly integrated audit plan, where IT audit activities are incorporated as part of business process engagements.**

Often, IT audit activities are planned under the responsibility of a multidisciplinary team that has a balanced skill set, including IT audit expertise.

Given that a system of internal control typically includes manual and automated controls, with more reliance on application controls, the ability to scope an audit that covers all controls is essential in providing a holistic assessment of the control environment. A complete business audit, including a review of all IT components, provides the opportunity to evaluate whether there is an appropriate combination of controls to mitigate business risks.

Audit Universe	Low-integrated Audit Plan	Partially Integrated Audit Plan	Highly Integrated Audit Plan
Business Processes • Operational • Financial • Compliance	Non-IT audit	Non-IT audit	Integrated approach
Applications Systems • Application controls • IT general controls	IT audit	Integrated approach	Integrated approach
IT Infrastructure Controls • Databases • Operating systems • Network	IT audit	IT audit	Integrated approach

Table 6. IT auditing and integrated auditing

6.7 Validating the Audit Plan

Unfortunately, there is no direct test that can be performed to validate whether the right and most effective audit plan exists. Therefore, auditors need to establish criteria to evaluate the plan's effectiveness in meeting its objectives. As discussed earlier, the plan should consist of risk-based audits, mandated audit areas, and management requests for assurance and consulting services. Because one of the objectives of the planning phase is to allocate resources to areas where the department can add the most value to the organization and highest risk IT areas, auditors should determine how the plan reflects this objective. The chart in figure 5 depicts the plan's target. According to this chart, if all audit subjects and engagements are plotted based on their risk likelihood and impact, audits should be reflected in all chart quadrants. The bolded box represents the ideal selection of audits and engagements, so that the largest majority of the plan consists of audits from the highest-risk quadrant with the balance proportionally selected from medium- and low-risk quadrants. Furthermore, some of the audits in the plan should deal with compliance and mandated areas. Consequently, auditors should note that while there are valid reasons for including low-risk audits in the plan, alternative audit approaches such as control self-assessments should be considered to limit the resources required to complete the review.

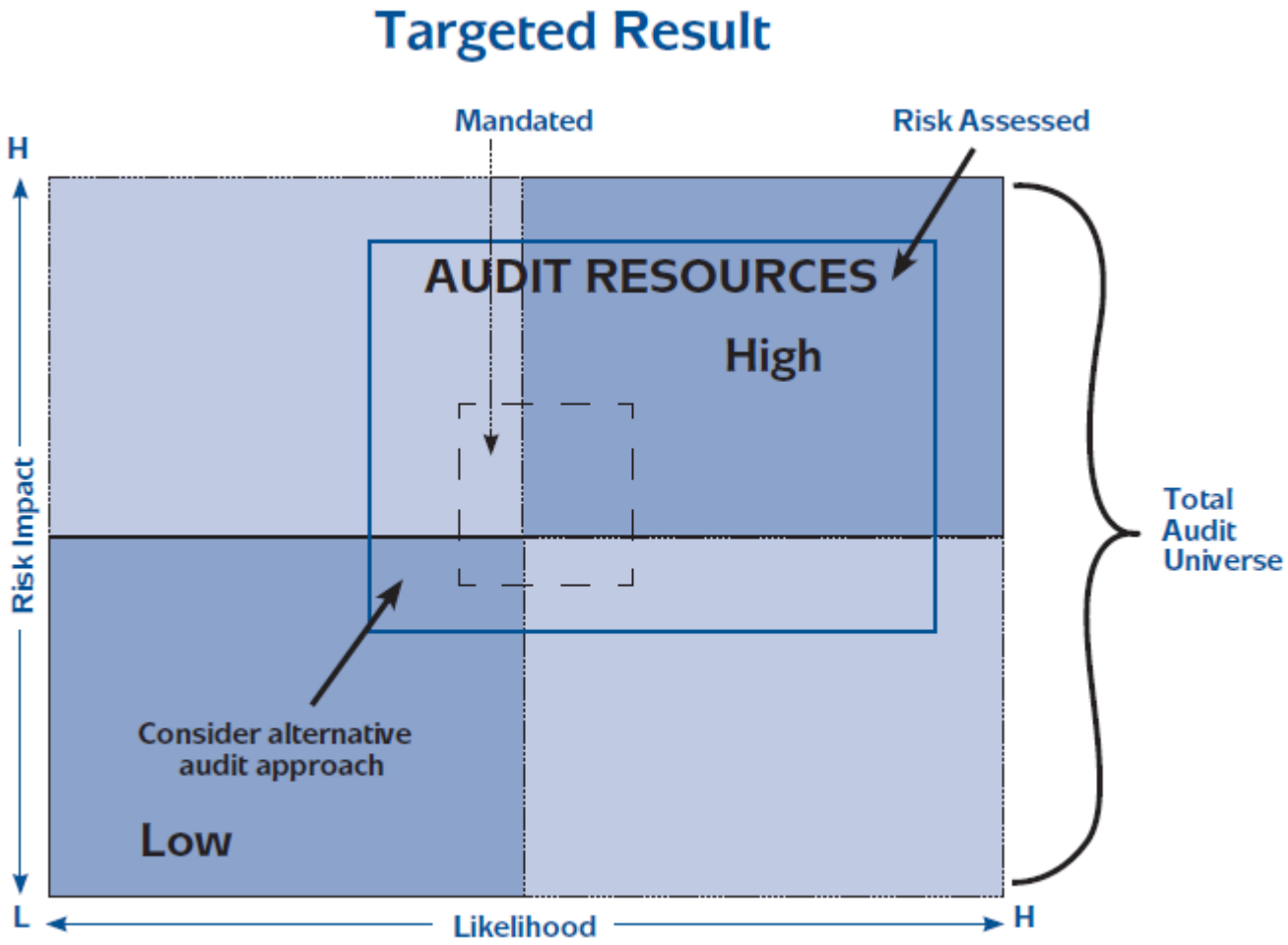


Figure 5. Chart of targeted audit results

6.8 The Dynamic Nature of the IT Audit Plan

As technology continues to change, so does the arrival of new and potential risks, vulnerabilities, and threats to the company. In addition, technological changes may prompt a new set of IT goals and objectives, which in turn leads to the creation of new IT initiatives, acquisitions, or changes to meet the organization's needs. An important point to consider when drafting the audit plan, therefore, is the organization's dynamic nature and its ongoing changes. More specifically, auditors need to consider the higher rate of IT change compared to changes in non-IT activities, the appropriate timing of a system's SDLC phases, and the results of SDLC audits.

In addition, auditors need to consider the specific source of the change. For instance, frequent changes in the IT audit plan could be the result of:

- Changes in strategic, organizational, or human resources.
- New business process initiatives involving the use of high-risk technology, such as e-commerce.
- Major changes in applications, such as the use of a new Web application version.
- Critical administration and support software packages.
- Network and infrastructure threats and vulnerabilities that lead to a reassessment of information security management activities.

As a consequence, periodic reassessments of IT audit plan priorities should be conducted and, if needed, reported to the board and senior management on a more frequent basis as compared with other more traditional and static audit topics. The IT audit function also must analyze changes in the IT audit universe and have the flexibility to adjust the plan to the new conditions. Furthermore, the plan should be reassessed periodically, and greater flexibility is needed to react to changes in the business and IT environments by adjusting the ranking and prioritization of planned audits. Finally, it is important for the plan to link each element of the IT audit universe to one of the following SDLC phases: feasibility study, analysis, design, implementation, testing, evaluation, and maintenance and production. The value added provided by an internal audit function depends highly on the quality of its recommendations and the benefit that the company obtains from their implementation.

Often there are direct benefits from addressing monetary compliance issues. However, there may be an indirect benefit to help enhance the organization's reputation, competitive advantage, maturity of business processes, and innovation.

One of the main attributes of audit recommendations that affect their value added is timing. This attribute is especially relevant during the entire life cycle of IT applications. In general, the earlier in the software's life cycle a weakness or risk is identified, the higher the added value of audit recommendations. For example, the cost of implementing a structural change to address a critical application weakness is substantially greater once the system is in production compared to addressing the same weakness at the design phase. Besides the added value stemming from audit recommendations, the internal auditor's reputation is improved in terms of his or her professionalism. The challenge for the IT audit function then becomes how to plan activities to deliver the appropriate type of audit recommendations within the optimal life cycle timeframe. As a rule, the planning strategy must be performed prior to the beginning of the entire cycle, so that appropriate activities are planned in terms of time and resources. It is critical for the IT audit plan to

balance audit activities throughout the entire life cycle, such as avoiding a concentration of audit efforts on the maintenance and production phase and having adequate coverage during the early stages. By following these recommendations, organizations will be able to move from a traditional and post-mortem planning strategy (i.e., one that is based mostly from an operational, compliance, and financial approach) to one that is more innovative, adds value, and is more consultative in nature.

6.9 Communicating, Gaining Executive Support, and Obtaining Plan Approval

As part of their goals, the internal audit department should present the audit plan to senior management and audit committee board members. In particular, resource requirements, significant interim changes, and the potential implications of resource limitations must be communicated to senior management and the board, according to IIA Standard 2020.

It is also important for the IT component of the internal audit plan or the IT audit plan to be discussed with senior management and the board as well as key IT stakeholders, such as the chief information officer, the chief technology officer, IT managers, business applications owners, and other employees with similar roles. The input received from these stakeholders is paramount to the success of the audit planning exercise and will enable CAEs and internal auditors to better understand the business environment, identify risks and concerns, and select audit areas. Furthermore, dialogue on the final plan will help to validate the stakeholders' input throughout the process and provide a preview of upcoming activities. When discussing the IT audit plan, internal auditors should do so in a manner that is supported by key IT executives, managers, and staff. Gaining the IT team's understanding, coordination, and support will make the audit process more effective and efficient. In addition, understanding the plan facilitates an open and continuing dialogue where evolving risks and changes to the operating environment can be discussed throughout the plan's life cycle and adjustments are made on an ongoing basis. Interaction with the clients when conducting the risk assessment and prior to the final plan's approval is critical to ensure the plan's overall quality.

7. Appendix: Hypothetical Company Example

The example in this chapter illustrates how to incorporate the IT audit planning elements discussed in earlier sections. Although the steps can be universally followed, the example's audit subjects and risk assessment results are generic in nature.

7.1 The Company

The hypothetical company is a publicly traded manufacturer and supplier of commodity products used as feeder stock by consumer product manufacturers in different markets around the world. The company's profile is as follow:

- US $7 billion in total assets.
- Based in the United States.
- Thirty production facilities in seven countries, including Belgium, China, Qatar, Saudi Arabia, Singapore, South Korea, and the United States.
- Six research, technology, and quality control centers located in each production facility.
- Five thousand employees worldwide.
- Five major competitors.
- Holds nearly 3,000 domestic and international patents and patent applications.
- Three major business units for manufacturing operations along product lines, centralized headquarters, and support-service organizations.
- Three major capital projects to build and expand manufacturing capacity. In addition, the company's centralized IT organization consists of four basic divisions:
- Global infrastructure:
    - Telecommunications.
    - Voice communications.
    - Networks.
    - Remote connectivity.
    - Desktop and Internet.
    - Information life cycle management.
    - Servers.

• Enterprise applications:

    - One major ERP application used throughout the company for supply chain management, financial accounting, human resources (based in the United States), sales, and distribution.
    - Also supplies SAP technical support and Advanced Business Application Programming (ABAP).

• Manufacturing Systems:

    - Responsible for systems operating at manufacturing facilities.
    - Local applications include payroll for non-U.S. sites, research and quality control databases, environmental reporting, and manufacturing process control systems.
    - Financial analysis and controls.

• Strategy and risk management:

    - Contracts, purchasing, and licensing.
    - Strategy, architecture, and standards.
    - Security services.

- IT change and governance.
- Project management office

The manufacturing facilities are the organization's lifeblood. Because they are located throughout the world and have different capacity sizes, they introduce risks that may impact business fundamentals and financials. Furthermore, although the manufacturing facilities create a somewhat decentralized business model, the organization's centralized corporate and service elements offer the opportunity for process-based audits that cross business functions. In the area of compliance, the organization is subject to U.S. and European requirements, including Sarbanes-Oxley, the European Union's Directive on Data Protection (Privacy), the U.S. Foreign Corrupt Practices Act, and other similar regulations in the locations in which it operates. According to the annual business plan, several major capital investment projects are under way that will have a great impact on the organization's future competitiveness.

Finally, the company's IT function aligns closely with its business model. The company uses a fairly homogeneous group of applications, including a standard ERP application, a global network and server infrastructure, and standard support processes for IT service delivery functions, governance, and security.

7.2 The IT Audit Plan

Based on this description, an IT audit universe can be identified that defines a holistic inventory of conceivable audit subject areas and provides management with information on the effectiveness of their control environment and operations.

As mentioned in the previous paragraphs, the centralized corporate and services elements offer the opportunity for global, process-type audit subjects. The company's centralized ERP application, global infrastructure support areas, and standard IT service delivery processes are good candidates for independent audit subjects covering large areas of IT risk.

Manufacturing facilities also are represented in the IT audit universe with subjects from locally supported applications and an underlying infrastructure (shown as facility 1–30 for simplicity in table 7). These audit subjects are likely to be aligned with business process audits in each facility. Table 7 shows what a sample universe of potential IT audit subjects might look like for the company. Each of the 30 manufacturing facilities has these and other audit subject areas.

Business Unit	Audit Subject
Corporate	Network administration and security
Corporate	Remote connectivity
Corporate	Windows Server administration and security
Corporate	UNIX administration and security
Corporate	ERP application and general controls
Corporate	Sarbanes-Oxley sustainability review
Corporate	Corporate privacy compliance
Corporate	Database administration and security
Corporate	IT governance practices
Corporate	ITIL deployment practices
Corporate	Application program change control
Business Segment 1–3	Major capital investment projects (e.g., information protection and corporate compliance)
Facility 1–30	IT infrastructure
Facility 1–30	Human resources and payroll application
Facility 1–30	Process control systems

Table 7. IT audit universe

After the IT audit universe is defined at a high level, the next step is to assess the business and IT risks on each area.

Risk categories are assessed based on their likelihood of occurrence and the impact they would have on the organization if the risk was not adequately managed. This risk approach uses relative ranking as shown in table 8. For example, a three point scale to assess likelihood and impact is used as outlined in the following description:

Likelihood Scale		
H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low probability that the risk will occur.

Impact Scale (Financial)		
H	3	There is a potential for material impact on the organization's earnings, assets, reputation, or stakeholders.
M	2	The potential impact may be significant to the audit unit, but moderate in terms of the total organization.
L	1	The potential impact on the organization is minor in size or limited in scope.

Table 8. Three-point likelihood and impact scale

To aid in the analysis, a range is selected that indicates a relative risk ranking of high, medium, and low, as follows:

Level	Composite Risk Score Range	Recommended Annual Cycle
H	35–54	Every 1 to 2 years
M	20–34	Every 2 to 3 years
L	6–19	Every 3 to 5 years

Table 9. Range of relative risk ranking

As part of the risk assessment step, auditors need to define a recommended annual cycle for audit subjects in the universe based on composite risk score ranges, where high-risk audit subjects are reviewed every one to two years, medium-risk subjects every two to three years, and low-risk subjects every three to five years. This will ensure that high-risk areas are reviewed frequently and low-risk areas are covered adequately over a five-year span. Table 10 shows an example of a completed risk assessment.

Area	Financial Impact		IT Risks										Score and Level	
			Quality of Internal Controls		Changes in Audit Unit		Availability		Integrity		Confiden-tiality			
	L	I	L	I	L	I	L	I	L	I	L	I		
ERP Application & General Controls	3	3	2	3	3	3	2	3	2	3	2	3	42	H
Treasury EFT Systems	3	3	3	3	3	3	3	2	3	2	2	1	41	H
Facility 3 – HR/Payroll Application	3	3	3	2	3	3	2	2	2	3	2	3	40	H
Employee Benefits Apps (Outsourced)	2	3	2	2	3	3	3	2	2	3	3	3	40	H
Facility 3 – IT Infrastructure	2	2	3	2	3	3	3	3	3	2	2	2	38	H
Facility 3 – Process Control Systems	3	3	3	2	3	3	3	3	2	2	2	1	39	H
UNIX Administration and Security	2	2	3	2	3	3	2	3	3	2	2	2	35	M/H
Corp. Privacy Compliance	3	1	3	3	3	3	2	1	2	1	3	3	34	M/H
Database Administration and Security	2	2	2	2	2	2	3	3	2	2	2	1	27	M
Windows Server Admin and Security	2	2	1	2	2	2	2	3	3	2	2	2	26	M
Facility 1 – IT Infrastructure	2	2	3	2	1	3	3	2	3	1	1	1	23	M
Facility 1 – Process Control Systems	2	3	3	2	2	2	3	3	1	1	1	1	27	M
Environment Reporting Systems	2	2	3	2	2	2	2	3	1	1	3	1	24	M
Facility 2 – IT Infrastructure	2	2	3	2	1	3	3	2	3	1	1	1	23	M
Major Capital Investment Projects	2	2	3	3	1	1	2	2	1	1	2	3	25	M
Application Program Change Control	2	3	2	3	1	2	2	2	1	3	1	2	23	M
SOX Sustainability Review	2	2	2	3	2	2	1	2	2	2	1	2	22	M
Network Administration and Security	2	2	2	1	2	2	2	2	2	2	2	2	22	M
Facility 2 – Process Control Systems	2	2	2	2	1	2	2	2	2	2	1	1	19	M/L
ITIL Deployment Practices	1	2	2	3	3	1	3	1	1	3	2	1	19	M/L
Facility 2 – HR/Payroll Application	1	2	1	2	2	3	2	2	3	1	1	2	19	M/L
Facility 30 – HR/Payroll Application	1	1	1	2	2	2	2	2	2	2	1	2	17	L
Facility 1 – HR/Payroll Application	1	1	1	2	2	2	2	2	2	2	1	2	17	L
Facility 30 – IT Infrastructure	1	1	3	1	1	1	2	2	2	1	1	1	12	L
Facility 30 – Process Control Systems	1	1	2	2	2	2	2	2	1	1	1	1	15	L
IT Governance Practices	1	1	2	2	1	1	3	1	1	1	1	2	12	L
Remote Connectivity	1	1	1	2	2	1	1	1	1	2	2	2	12	L

L = Likelihood
I = Impact

Table 10. Risk assessment

Once risk assessment results are available, the next step is to formalize the audit plan. As discussed in section 6, the audit plan consists of risk-driven audit projects, mandatory compliance reviews, stakeholder requests, and follow-up audits of previously identified significant issues. Because these tasks need to be completed using available internal audit resources, some risk-driven audit projects might not be incorporated in the plan. Continuing with the hypothetical company example, the board has asked the IT department to be involved in the coordination of an external infrastructure penetration test, and operating management has requested assurance that Sarbanes-Oxley management testing is sustained throughout the organization. In addition, the IT function asked the internal audit department to be involved with an ITIL deployment project to identify whether service delivery processes are effective and cover all risks. These stakeholder requests are accepted because

they fit with the mission of the internal audit department and will be added automatically to the audit plan. Furthermore, there was a significant segregation of duties issue identified in the previous year's procurement process audit, so a follow-up review will be added to the plan to ensure agreed upon remediation efforts are progressing as planned. In the compliance area, compliance with the new corporate policy on protecting personal data for privacy will be included because there are plans to transmit personal data between non-U.S. facilities and the U.S. corporate headquarters.

The company has an IT audit staff of five auditors or approximately 1,000 available days for engagements after considering exception time and training. Based on the risk assessment of available audit subjects, mandatory activities, and stakeholder requests, the most effective audit plan is shown in table 11. Several high-risk subjects were not included in the plan (e.g., treasury electronic funds transfer (EFT) systems, process control systems, and database administration and security) because they were reviewed in the last 12 months.

Engagement	Risk Level	Cycle	Audit Days Allocated
Penetration Test Coordination	*	0	40
Procurement Application Follow-up	*	0	20
ERP Application & General Controls	H	1	100
Facility 3: HR/Payroll Application	H	2	30
Employee Benefits Apps (Outsource)	H	3	100
Facility 3: IT Infrastructure	H	2	90
UNIX Administration and Security	M/H	1	90
Corp. Privacy Compliance	M/H	3	40
Windows Server Administration and Security	M	3	90
Facility 1: IT Infrastructure	M	3	90
Facility 1: Process Control Systems	M	3	90
Environment Reporting Systems	M	3	30
Major Capital Investment Projects	M	3	30
Sarbanes-Oxley Sustainability	M/*	3	120
ITIL Deployment Practices	L/*	4	40
Total			1000
* Management Request			

Table 11. The audit plan

The audit plan in table 11 represents the ideal audit plan based on the company's internal audit department and its understanding of the company's strategies and objectives, historical knowledge of the control environment, and anticipated changes in operations during the next audit period. The plan should be reviewed with senior and operations management as a follow-up discussion to the risk assessment and audit planning phases. Doing so will validate management input was considered

accurately in the process and give managers a preview of the upcoming year's IT audit plan. The review also is an appropriate time to discuss potential audit engagement dates as the company might experience blackout periods due to the audit's possible disruption of company operations. For example, planned dates for application or infrastructure upgrades should be discussed, as well as schedules of significant operational activities, such as plant shutdowns and turnarounds, that could affect the audit process. Following the plan's completion is the scheduling of audits and audit resources. In general, audits have to be staffed with appropriately skilled auditors to ensure the engagement's success. However, the audit schedule is also a good opportunity to address staff development needs through the exposure of audits that will expand and develop specific skill areas. Finally, there will be changes that might impact the audit plan and schedule due to the organization's dynamic nature. As a result, it is important to have an effective plan in place, manage the plan throughout its life cycle, and be flexible to company changes so that resources stay focused on evolving risk areas and the organization's concerns.

IT Controls

IT Controls

1. IT Controls

In this chapter we discuss the knowledge needed by members of governing bodies, executives, IT professionals, and internal auditors to address technology control issues and their impact on business. The chapter also provides information on available frameworks for assessing IT controls and describes how to establish the right framework for an organization. Our objectives are to:

- Explain IT controls from an executive perspective.
- Explain the importance of IT controls within the overall system of internal controls.
- Describe the organizational roles and responsibilities for ensuring IT controls are addressed adequately within the overall system of internal controls.
- Describe the concepts of risk inherent in the use and management of technology by any organization.
- Describe the basic knowledge and understanding of IT controls needed by the CAE to ensure effective internal audit assessments of IT controls.
- Describe the relevant elements of the IT controls assessment process as provided by the internal audit function.

1.1 Introduction to IT Controls

An IT control is a procedure or policy that provides a reasonable assurance that the information technology (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 can be categorized as either general controls (ITGC) or application controls (ITAC).

An IT general control should demonstrate that the organization has a procedure or policy in place for technology that affects the management of fundamental organizational processes such as risk management, change management, disaster recovery and security. IT application controls, which are actions that a software application does automatically, should demonstrate that software applications used for specific business processes (such as payroll) are properly maintained, are only used with proper authorization, are monitored and are creating audit trails.

IT controls are a subset of the more general term, internal controls.

IT controls do not exist in isolation. They form an interdependent continuum of protection, but they may also be subject to compromise due to a weak link. They are subject to error and management override, may range from simple to highly technical, and may exist in a dynamic environment.

IT controls have two significant elements: the automation of business controls and control of IT. Thus, IT controls support business management and governance as well as provide general and technical controls over IT infrastructures.

The internal auditor's role in IT controls begins with a sound conceptual understanding and culminates in providing the results of risk and control assessments. Internal auditing involves significant interaction with the people in positions of responsibility for controls and requires continuous learning and reassessment as new technologies emerge and the organization's opportunities, uses, dependencies, strategies, risks, and requirements change.

1.2 Understanding IT Controls

IT controls provide for assurance related to the reliability of information and information services. IT controls help mitigate the risks associated with an organization's use of technology. They range from corporate policies to their physical implementation within coded instructions; from physical access protection through the ability to trace actions and transactions to responsible individuals; and from automatic edits to reasonability analysis for large bodies of data.

You don't need to know everything about IT controls, but remember two key control concepts:

- Assurance must be provided by the IT controls within the system of internal controls. This assurance must be continuous and provide a reliable and continuous trail of evidence.
- The auditor's assurance is an independent and objective assessment of the first assurance. Auditor assurance is based on understanding, examining, and assessing the key controls related to the risks they manage, and performing sufficient testing to ensure the controls are designed appropriately and functioning effectively and continuously.

1.3 IT control Frameworks

A control framework is a data structure that organizes and categorizes an organization's internal controls, which are practices and procedures established to create business value and minimize risk. IT controls being a subset of internal controls; IT framework is designed to provide a model that corporations can use to run an efficient and well-controlled IT environment.

Many frameworks exist for categorizing IT controls and their objectives, IT control frameworks include COBIT (Control Objectives for Information and Related Technology), ISO/IEC 17799: Code of Practice for Information Security Management and ITIL (Information Technology Infrastructure Library).

But whatever the framework by any organization, it uses the applicable components of existing frameworks to categorize and assess IT controls, and to provide and document its own framework for:

- Compliance with applicable regulations and legislation.
- Consistency with the organization's goals and objectives.
- Reliable evidence (reasonable assurance) that activities comply with management's governance policies and are consistent with the organization's risk appetite.

1.4 Importance of IT Controls

Many issues drive the need for IT controls, ranging from the need to control costs and remain competitive through the need for compliance with internal and external governance. IT controls promote reliability and efficiency and allow the organization to adapt to changing risk environments. Any control that mitigates or detects fraud or cyber-attacks enhances the organization's resiliency because it helps the organization uncover the risk and manage its impact. Resiliency is a result of a strong system of internal controls because a well-controlled organization has the ability to manage challenges or disruptions seamlessly.

Key indicators of effective IT controls include:

- The ability to execute and plan new work such as IT infrastructure upgrades required to support new products and services.
- Development projects that are delivered on time and within budget, resulting in cost-effective and better product and service offerings compared to competitors.
- Ability to allocate resources predictably.
- Consistent availability and reliability of information and IT services across the organization and for customers, business partners, and other external interfaces.
- Clear communication to management of key indicators of effective controls.
- The ability to protect against new vulnerabilities and threats and to recover from any disruption of IT services quickly and efficiently.
- The efficient use of a customer support center or help desk.
- Heightened security awareness on the part of the users and a security-conscious culture throughout the organization.

1.5 IT Roles and Responsibilities

Many different roles have emerged in recent years for positions within the organization with IT control responsibilities and ownership. Each position within the governance, management, operational, and technical levels should have a clear description of its roles, responsibilities, and ownership for IT controls to ensure accountability for specific issues (e.g. CIO, CSO, IT Manager). This chapter addresses the various IT control roles and responsibilities within the organization and allocates them to specific positions within a hypothetical organizational structure.

1.6 Analyzing Risk

IT controls are selected and implemented on the basis of the risks they are designed to manage. As risks are identified, suitable risk responses are determined, ranging from doing nothing and accepting the risk as a cost of doing business to applying a wide range of specific controls, including insurance. This section explains the concepts of when to apply IT controls.

1.7 Monitoring and Techniques

The implementation of a formal control framework facilitates the process of identifying and assessing the IT controls necessary to address specific risks. A control framework is a structured way of categorizing controls to ensure the whole spectrum of control is covered adequately. The framework can be informal or formal. A formal approach will more readily satisfy the various regulatory or statutory requirements for organizations subject to them. The process of choosing or constructing a control framework should involve all positions in the organization with direct responsibility for controls. The control framework should apply to, and be used by, the whole organization — not just internal auditing.

1.8 IT Control Assessment

Assessing IT controls is a continuous process. Business processes are changing constantly as technology continues to evolve. Threats emerge as new vulnerabilities are discovered. Audit methods improve as auditors adopt an approach where IT control issues in support of the business objectives are near the top of the agenda.

Management provides IT control metrics and reporting. Auditors attest to their validity and opine on their value. The auditor should liaise with management at all levels and with the audit committee to agree on the validity and effectiveness of the metrics and assurances for reporting.

2 Assessing IT Control

When CAEs review and assess the controls over IT, they should ask:

- What do we mean by IT controls?
- Why do we need IT controls?
- Who is responsible for IT controls?
- When is it appropriate to apply IT controls?
- Where exactly are IT controls applied?
- How do we perform IT control assessments?

The audit process provides a formal structure for addressing IT controls within the overall system of internal controls. Figure 1, *The Structure of IT Auditing*, below, divides the assessment into a logical series of steps. The internal auditor's role in IT controls begins with a sound conceptual understanding and culminates in providing the results of risk and control assessments. Internal auditors interact with the people responsible for controls and must pursue continuous learning and reassessment as new technologies emerge and the organization's opportunities, uses, dependencies, strategies, risks, and requirements change.

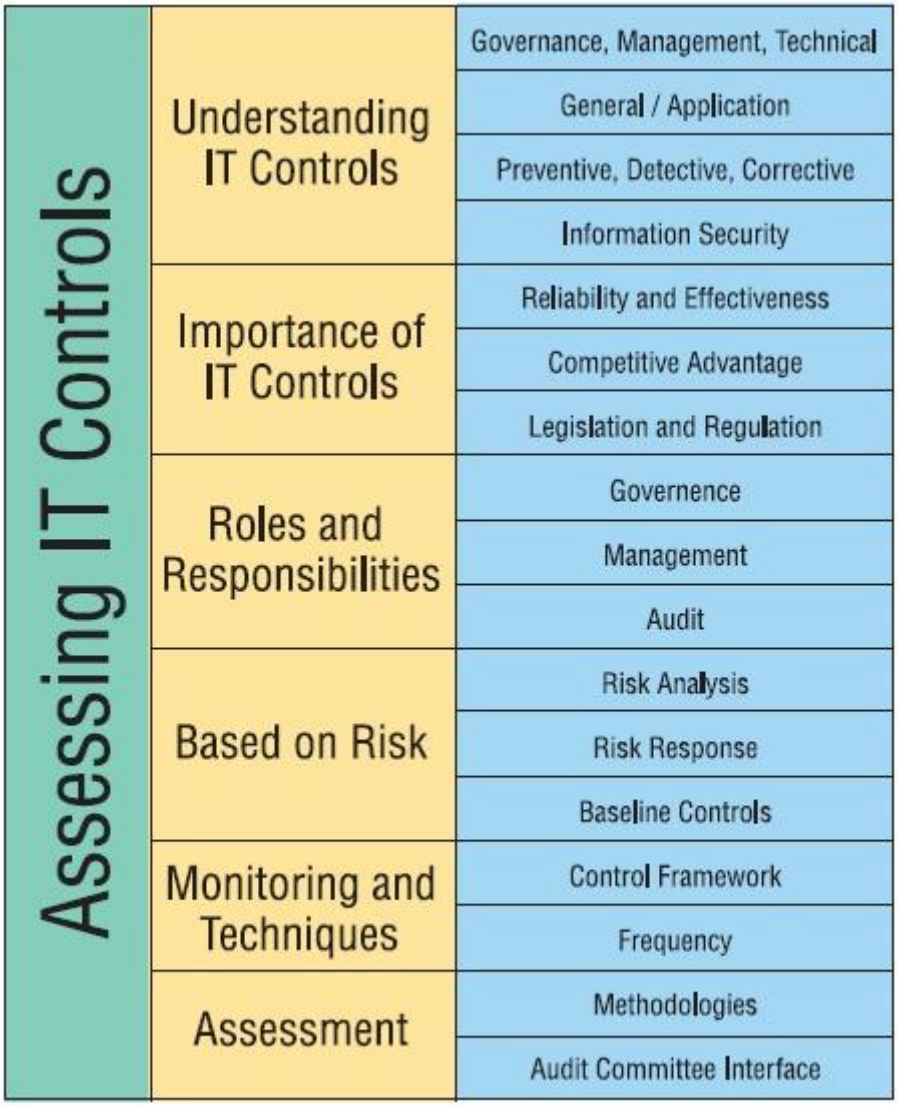


Figure 1 - The Structure of IT Auditing

3. Understanding IT Controls

As defined earlier *internal control* is a process, affected by an organization's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

IT controls encompass those processes that provide assurance for information and information services and help mitigate the risks associated with an organization's use of technology. These controls range from written corporate policies to their implementation within coded instructions; from physical access protection to the ability to trace actions and transactions to the individuals who are responsible for them; and from automatic edits to reasonability analysis for large bodies of data.

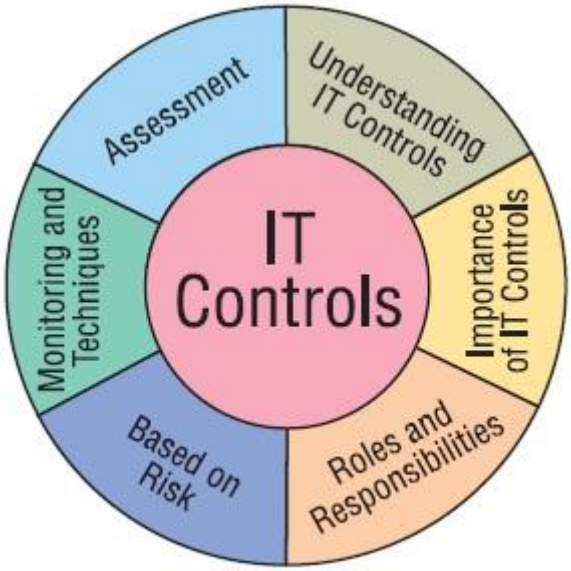


Figure 2

4 Control Classifications

Controls may be classified to help understand their purposes and where they fit into the overall system of internal controls (See Figure 3).

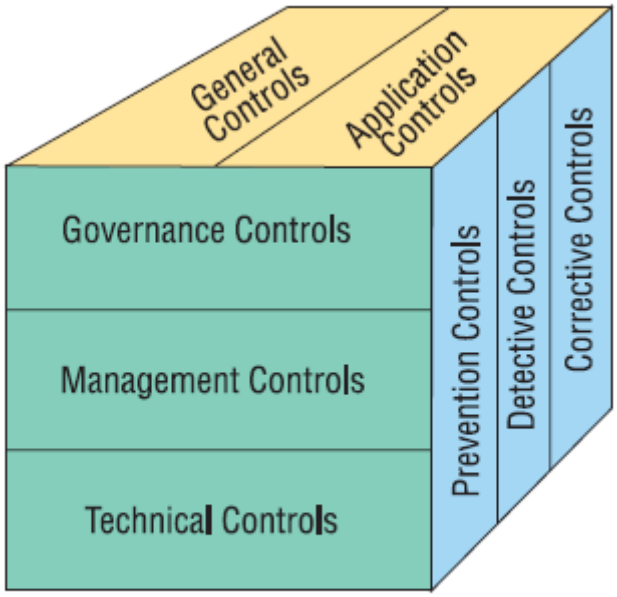


Figure 3 - Some Control Classifications

By understanding these classifications, the control analyst and auditor are better able to establish their positions in the control framework and answer key questions such as:
Are the detective controls adequate to identify errors that may get past the preventive controls? Are corrective controls sufficient to fix the errors once detected?

4.1 General Classification

A common classification of IT controls is *general* versus *application*.

4.1.1 General controls

(Also known as infrastructure controls) apply to all systems components, processes, and data for a given organization or systems environment. General controls include, but are not limited to: information security policy, administration, access, and authentication; separation of key IT functions; management of systems acquisition and implementation; change management; backup; recovery; and business continuity.

4.1.2 Application controls

Pertain to the scope of individual business processes or application systems. They include such controls as data edits, separation of business functions (e.g., transaction initiation versus authorization), balancing of processing totals, transaction logging, and error reporting. The function of a control is highly relevant to the assessment of its design and effectiveness.

4.2 Classification based on Functionality

Controls may be classified based on the functionality as *preventive*, *detective*, or *corrective*.

4.2.1 Preventive controls

Prevent errors, omissions, or security incidents from occurring. Examples include simple data-entry edits that block alphabetic characters from being entered into numeric fields, access controls that protect sensitive data or system resources from unauthorized people, and complex and dynamic technical controls such as antivirus software, firewalls, and intrusion prevention systems.

4.2.2 Detective controls

Detect errors or incidents that elude preventive controls. For example, a detective control may identify account numbers of inactive accounts or accounts that have been flagged for monitoring of suspicious activities. Detective controls can also include monitoring and analysis to uncover activities or events that exceed authorized limits or violate known patterns in data that may indicate improper manipulation. For sensitive electronic communications, detective controls can indicate that a message has been corrupted or the sender's secure identification cannot be authenticated.

4.2.3 Corrective controls

Correct errors, omissions, or incidents once they have been detected. They vary from simple correction of data-entry errors, to identifying and removing unauthorized users or software from systems or networks, to recovery from incidents, disruptions, or disasters. Generally, it is most efficient to prevent errors or detect them as close as possible to their source to simplify correction. These corrective processes also should be subject to preventive and detective controls, because they represent another opportunity for errors, omissions, or falsification. Many other control classifications described in this guide may be useful in assessing their effectiveness. For example, automated controls tend to be more reliable than manual controls, and nondiscretionary controls are more likely to be applied consistently than discretionary controls. Other control classifications include mandatory, voluntary, complementary, compensating, redundant, continuous, on-demand, and event-driven.

4.3 Classification based on group responsibilities

Another common classification of controls is by the group responsible for ensuring they are implemented and maintained properly. For the purpose of assessing roles and responsibilities, we categorizes IT controls as *governance*, *management*, and *technical*. The first two levels — governance and management — are the core focus of this course although it may also be useful to understand how higher-level controls specifically are established within the technical IT infrastructures.

4.3.1 Governance Controls

The primary responsibility for internal control resides with the board of directors in its role as keeper of the governance framework. IT control at the governance level involves ensuring that effective information management and security principles, policies, and processes are in place and performance and compliance metrics demonstrate ongoing support for that framework.

Governance controls are those mandated by, and controlled by, either the entire board of directors or a board committee in conjunction with the organization's executive management. These controls are linked with the concepts of corporate governance, which are driven both by organizational goals and strategies and by outside bodies such as regulators.

An important distinction between governance and management controls is the concept of "noses in, fingers out." The board's responsibility involves oversight rather than actually performing control activities. For example, the audit committee of the board does no auditing, but it does oversee both the internal and external auditing of the organization.

4.3. 2 Management Controls

Management responsibility for internal controls typically involves reaching into all areas of the organization with special attention to critical assets, sensitive information, and operational functions. Consequently, close collaboration among board members and executive managers is essential. Management must make sure the IT controls needed to achieve the organization's established objectives are applied and ensure reliable and continuous processing. These controls are deployed as a result of deliberate actions by management to:

- Recognize risks to the organization, its processes, and assets.
- Enact mechanisms and processes to mitigate and manage risks (protect, monitor, and measure results).

4.3.3 Technical Controls

Technical controls form the foundation that ensures the reliability of virtually every other control in the organization. For example, by protecting against unauthorized access and intrusion, they provide the basis for reliance on the integrity of information — including evidence of all changes and their authenticity. These controls are specific to the technologies in use within the organization's IT infrastructures. The ability to automate technical controls that implement and demonstrate compliance with management's intended information-based policies is a powerful resource to the organization.

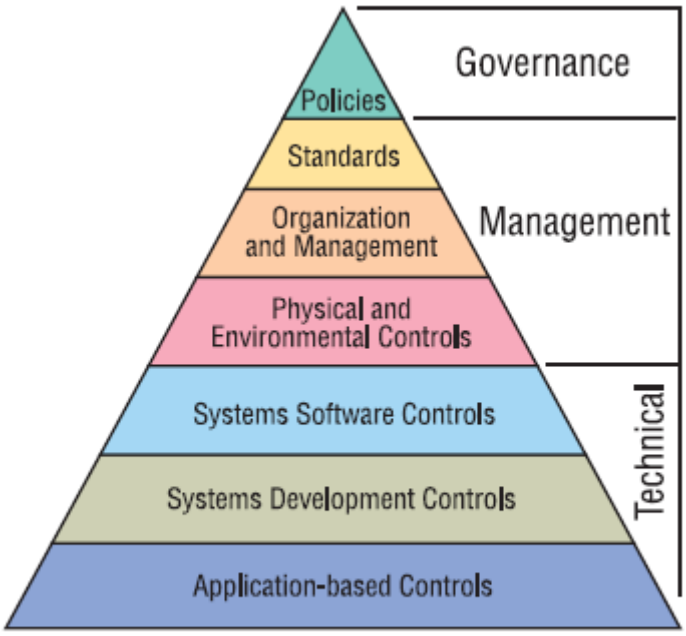


Figure 4 – IT Controls

5 IT Controls – What to Expect, (discussing group based classification of controls in detail)

Individual control mechanisms a CAE can expect to find within the organization can be defined within the hierarchy of IT controls, from the overall high-level policy statements issued by management and endorsed by the board of directors, down to the specific control mechanisms incorporated into application systems.

The hierarchy in Figure 4, *IT Controls*, represents a logical "top-down" approach, both when considering controls to implement and when determining areas on which to focus audit resources during reviews of the entire IT operating environment.

The different elements of the hierarchy are not mutually exclusive; they are all connected and can intermingle.

Many of the control types within the elements are described below.

5. 1 Policies

All organizations need to define their aims and objectives through strategic plans and policy statements. Without clear statements of policy and standards for direction, organizations can become disoriented and perform ineffectively. Organizations with clearly defined aims and objectives tend to be successful.

Because technology is vital to the operations of most organizations, clear policy statements regarding all aspects of IT should be devised and approved by management, endorsed by the board of directors, and communicated to all staff. Many different policy statements can be required, depending on the organization's size and the extent to which it deploys IT. For smaller organizations, a single policy statement may be sufficient, provided it covers all the relevant areas. Larger organizations that implement IT extensively will require more detailed and specific policies. IT policy statements include, but are not restricted to:

- A general policy on the level of security and privacy throughout the organization. This policy should be consistent with all relevant national and international legislation and should specify the level of control and security required depending on the sensitivity of the system and data processed.
- A statement on the classification of information and the rights of access at each level. The policy should also define any limitations on the use of this information by those approved for access.
- A definition of the concepts of data and systems ownership, as well as the authority necessary to originate, modify, or delete information. Without these guidelines, it is often difficult to coordinate change within large organizations, because there may not be anyone designated to have overall responsibility for the data or systems.
- A general policy that defines the extent to which users can deploy intelligent workstations to create their own applications.
- Personnel policies that define and enforce conditions for staff in sensitive areas. This includes the positive vetting of new staff prior to joining the organization, carrying out annual credit checks, and having employees sign agreements accepting

responsibility for the required levels of control, security, and confidentiality. This policy would also detail related disciplinary procedures.

- Definitions of overall business continuity planning requirements. These policies should ensure that all aspects of the business are considered in the event of a disruption or disaster — not just the IT elements.

5. 2 Standards

Standards exist to support the requirements of policies. They are intended to define ways of working that achieve the required objectives of the organization. Adopting and enforcing standards also promotes efficiency because staff are not required to reinvent the wheel every time a new business application is built or a new network is installed. Standards also enable the organization to maintain the whole IT operating environment more efficiently.

Large organizations with significant resources are in a position to devise their own standards. On the other hand, smaller organizations rarely have sufficient resources for this exercise.

As a guideline, the CAE should expect to see standards adopted for:

- **Systems Development Processe**s – When organizations develop their own applications, standards apply to the processes for designing, developing, testing, implementing, and maintaining systems and programs. If organizations outsource application development or acquire systems from vendors, the CAE should ascertain that agreements require the providers to apply standards consistent with the organization's standards, or acceptable to the organization.
- **Systems Software Configuration** – Because systems software provides a large element of control in the IT environment, standards related to secure system configurations, such as the CIS Benchmarks from the Center for Internet Security, are beginning to gain wide acceptance by leading organizations and technology providers. The way products such as operating systems, networking software, and database management systems are configured can either enhance security or create weaknesses that can be exploited.
- **Application Controls** – All applications which support business activities need to be controlled. Standards are necessary for all applications the organization develops or purchases that define the types of controls that must be present across the whole range of business activities, as well as the specific controls that should apply to sensitive processes and information.
- **Data Structures** – Having consistent data definitions across the full range of applications ensures disparate systems can access data seamlessly and security controls for private and other sensitive data can be applied uniformly.
- **Documentation** – Standards should specify the minimum level of documentation required for each application system or IT installation, as well as for different classes of applications, processes, and processing centers.

As with policies, standards should be approved by management, should be written in clear and understandable language, and should be made available to all who implement them.

5.3 Organization and Management

Organization and management plays a major role in the whole system of IT control, as it does with every aspect of an organization's operations. An appropriate organization structure allows lines of reporting and responsibility to be defined and effective control systems to be implemented.

5.3.1 Separation of Duties

Separation of duties is a vital element of many controls. An organization's structure should not allow responsibility for all aspects of processing data to rest upon one individual or department. The functions of initiating, authorizing, inputting, processing, and checking data should be separated to ensure no individual can both create an error, omission, or other irregularity and authorize it and/or obscure the evidence. Separation-of-duties controls for application systems are provided by granting access privileges only in accordance with job requirements for processing functions and accessing sensitive information.

Traditional separation of duties within the IT environment is divided between systems development and operations. Operations should be responsible for running production systems — except for change deployment — and should have little or no contact with the development process. This control includes restrictions preventing operators from accessing or modifying production programs, systems, or data. Similarly, systems development personnel should have little contact with production systems. By assigning specific roles during implementation and other change processes to both the personnel responsible for application systems and those responsible for operations, appropriate separation of duties can be enforced. In large organizations, many other functions should be considered to ensure appropriate separation of duties, and these controls can be quite detailed. For example, privileged accounts, such as the Administrator group in Windows and Super User in UNIX, can modify log entries, access any file, and in many cases act as any user or role. It is important to restrict the number of individuals with this privilege to a minimum.

Software tools are also available and should be considered to limit the power and monitor the activities of individuals with privileged accounts.

5.3.2 Financial Controls

Because organizations make considerable investments in IT, budgetary and other financial controls are necessary to ensure the technology yields the protected return on investment or proposed savings. Management processes should be in place to collect, analyze, and report information related to these issues. Unfortunately, new IT developments often suffer massive cost over-runs and fail to deliver the expected cost savings because of insufficient planning. Budgetary controls can help identify potential failings early in the process and allow management to take positive action. They may also produce historical data that organizations can use in future projects.

5.3.3 Change Management

Change management processes can be specified under organizational and management control elements. These processes should ensure that changes to the IT environment, systems software, application systems, and data are applied in a manner that enforces

appropriate division of duties; makes sure changes work as required; prevents changes from being exploited for fraudulent purposes; and reveals the true costs of inefficiencies and system outages that can be obscured by ineffective monitoring and reporting processes. Change management is one of the most sensitive areas of IT controls and can seriously impact system and service availability if not administered effectively. The IT Process Institute has published research demonstrating that effective IT change management can bring significant benefits organizations.

5.3.4 Other Management Controls

Other typical management controls include vetting procedures for new staff, performance measurement, provision of specialist training for IT staff, and disciplinary procedures. These are listed in the Information Security Program Elements in Appendix A and will be covered in greater detail in other GTAG publications.

5.4 Physical and Environmental Controls

IT equipment represents a considerable investment for many organizations. It must be protected from accidental or deliberate damage or loss. Physical and environmental controls, originally developed for large data centers that house mainframe computers, are equally important in the modern world of distributed client-server and Web-based systems. Although the equipment commonly used today is designed for ease of use in a normal office environment, its value to the business and the cost and sensitivity of applications running business processes can be significant. All equipment must be protected, including the servers and workstations that allow staff access to the applications. Some typical physical and environmental controls include:

- Locating servers in locked rooms to which access is restricted.
- Restricting server access to specific individuals.
- Providing fire detection and suppression equipment.
- Housing sensitive equipment, applications, and data away from environmental hazards such as low-lying flood plains or flammable liquid stores.

When considering physical and environmental security, it is also appropriate to consider contingency planning — also known as disaster recovery planning — which includes response to security incidents. What will the organization do if there is a fire or flood, or if any other threat manifests itself? How will the organization restore the business and related IT facilities and services to ensure normal processing continues with minimum effect on regular operations? This type of planning goes beyond merely providing for alternative IT processing power to be available and routine backup of production data; it must consider the logistics and coordination needed for the full scope of business activity. Finally, history consistently demonstrates that a disaster recovery plan that has not been tested successfully in a realistic simulation is not reliable.

5. 5 Systems Software Controls

Systems software products enable the IT equipment to be used by the application systems and users. These products include operating systems such as Windows, UNIX, and Linux; network and communications software; firewalls; antivirus products; and database management systems (DBMS) such as Oracle and DB2. Systems software can be highly complex and can apply to components and appliances within the systems and network

environment. It may be configured to accommodate highly specialized needs and normally requires a high degree of specialization to maintain it securely. Configuration techniques can control logical access to the applications, although some application systems contain their own access controls, and may provide an opening for hackers to use to break into a system. Configuration techniques also provide the means to enforce division of duties, generate specialized audit trails, and apply data integrity controls through access control lists, filters, and activity logs.

IT audit specialists are required to assess controls in this area. Small organizations are unlikely to have the resources to employ such specialists and should consider outsourcing the work. Whether IT auditors are employed or outsourced, they require a highly specific set of knowledge. Much of this knowledge can come from experience, but such knowledge must be updated constantly to remain current and useful. Certification confirms that a technical specialist has acquired a specified set of knowledge and experience and has passed a related examination. In the IT audit world, global certificates include the Qualification in Computer Auditing (QiCA), from IIA–United Kingdom and Ireland; Certified Information Systems Auditor (CISA), available through the Information Systems Audit and Control Association (ISACA); and Global Information Assurance Certification (GIAC) Systems & Network Auditor (GSNA), from the SANS Institute's GIAC program. Additional certifications address general and specialized competence in information security, network administration, and other areas closely related to IT auditing and are useful for identifying an IT auditor's potential ability.

Some key technical controls the CAE should expect to find in a well-managed IT environment include:

- Access rights allocated and controlled according to the organization's stated policy.
- Division of duties enforced through systems software and other configuration controls.
- Intrusion and vulnerability assessment, prevention, and detection in place and continuously monitored.
- Intrusion testing performed on a regular basis.
- Encryption services applied where confidentiality is a stated requirement.
- Change management processes — including patch management — in place to ensure a tightly controlled process for applying all changes and patches to software, systems, network components, and data.

5. 6 Systems Development and Acquisition Controls

Organizations rarely adopt a single methodology for all systems development projects. Methodologies are chosen to suit the particular circumstances of each project. The IT auditor should assess whether or not the organization develops or acquires application systems using a controlled method that subsequently provides effective controls over and within the applications and data they process. All computer application systems should perform only those functions the user requires in an efficient way. By examining application development procedures, the auditor can gain assurance that applications work in a controlled manner.

Some basic control issues should be evident in all systems development and acquisition work:

- User requirements should be documented, and their achievement should be measured.
- Systems design should follow a formal process to ensure that user requirements and controls are designed into the system.
- Systems development should be conducted in a structured manner to ensure that requirements and design features are incorporated into the finished product.
- Testing should ensure that individual system elements work as required, system interfaces operate as expected, users are involved in the testing process, and the intended functionality has been provided.
- Application maintenance processes should ensure that changes in application systems follow a consistent pattern of control. Change management should be subject to structured assurance validation processes.

Where systems development is outsourced, the outsourcer or provider contracts should require similar controls.
Project management techniques and controls need to be part of the development process, whether developments are performed in-house or are outsourced. Management should know projects are on time and within budget and that resources are used efficiently. Reporting processes should ensure that management completely understands the current status of development projects and does not receive any surprises when the end product is delivered.

5.7 Application-based Controls

The objective of internal controls over application systems is to ensure that:

- All input data is accurate, complete, authorized, and correct.
- All data is processed as intended.
- All data stored is accurate and complete.
- All output is accurate and complete.
- A record is maintained to track the process of data from input to storage, and to the eventual output.

Reviewing the application controls traditionally has been the “bread and butter” of the IT auditor. However, because application controls now represent a huge percentage of business controls, they should be the priority of every internal auditor. All internal auditors need to be able to evaluate a business process and understand and assess the controls provided by automated processes.

There are several types of generic controls that the CAE should expect to see in any application:

- Input Controls – These controls are used mainly to check the integrity of data entered into a business application, whether the source is input directly by staff, remotely by a business partner, or through a Web-enabled application. Input is checked to ensure that it remains within specified parameters.

- Processing Controls – These controls provide automated means to ensure processing is complete, accurate, and authorized.
- Output Controls – These controls address what is done with the data. They should compare results with the intended result and check them against the input.
- Integrity Controls – These controls can monitor data in process and/or in storage to ensure that data remains consistent and correct.
- Management Trail – Processing history controls, often referred to as an audit trail, enable management to track transactions from the source to the ultimate result and to trace backward from results to identify the transactions and events they record. These controls should be adequate to monitor the effectiveness of overall controls and identify errors as close as possible to their sources.

6 Information Security

Information security is an integral part of all IT controls. Information security applies to both infrastructure and data and is the foundation for the reliability of most other IT controls. The exceptions are controls relating to the financial aspects of IT (e.g., ROI, budgetary controls) and some project management controls.
The universally accepted elements of information security are:

- **Confidentiality** – Confidential information must only be divulged as appropriate, and must be protected from unauthorized disclosure or interception. Confidentiality includes privacy considerations.
- **Integrity** – Information integrity refers to the state of data as being correct and complete. This specifically includes the reliability of financial processing and reporting.
- **Availability** – Information must be available to the business, its customers, and partners when, where, and in the manner needed. Availability includes the ability to recover from losses, disruption, or corruption of data and IT services, as well as from a major disaster where the information was located.

6.1 Responsibilities of Groups regarding IT Security

6.1.1 Governance (Board of Directors):

- Oversee risk management and compliance programs pertaining to information security.
- Approve and adopt broad information security program principles and approve assignment of key managers responsible for information security.
- Strive to protect the interests of all stakeholders dependent on information security.
- Review information security policies regarding strategic partners and other third parties.
- Strive to ensure business continuity.
- Review provisions for internal and external audits of the information security program.
- Collaborate with management to specify the information security metrics to be reported to the board.

6.1.2 Management

- Establish information security management policies and controls and monitor compliance.
- Assign information security roles, responsibilities, and required skills, and enforce role-based information access privileges.
- Assess information risks, establish risk thresholds, and actively manage risk mitigation.
- Ensure implementation of information security requirements for strategic partners and other third parties.
- Identify and classify information assets.
- Implement and test business continuity plans.
- Approve information systems architecture during acquisition, development, operations, and maintenance.
- Protect the physical environment.
- Ensure internal and external audits of the information security program with timely follow-up.
- Collaborate with security staff to specify the information security metrics to be reported to management.

6.1.3 Technical

Establishing a complete information security program requires attention to the following technical program elements:

- User identification and authentication.
- User account management.
- User privileges.
- Configuration management.
- Event and activity logging and monitoring.
- Communications, e-mail, and remote access security.
- Malicious code protection, including viruses, worms, and trojans.
- Software change management, including patching.
- Firewalls.
- Data encryption.
- Backup and recovery.
- Incident and vulnerability detection and response.
- Collaboration with management to specify the technical metrics to be reported to management.

7 IT Controls Framework

IT controls are not automatic. For the more than 50 years organizations have used IT, controls have not always been the default condition of new systems hardware or software. The development and implementation of controls typically lag behind the recognition of vulnerabilities in systems and the threats that exploit such vulnerabilities. Further, IT controls are not defined in any widely recognized standard applicable to all systems or to the organizations that use them. Many frameworks exist for categorizing IT controls and their objectives. Each organization should use the most applicable components of these

frameworks to categorize or assess IT controls and to provide and document its own internal control framework for:

- Compliance with applicable regulations and legislation.
- Consistency with the organization's goals and objectives.
- Reliable evidence (assurance) that activities are in compliance with management's governance policies and are consistent with the organization's risk appetite.

Many issues drive the need for IT controls, including controlling costs and remaining competitive, protecting against information theft by hackers. IT controls promote reliability and efficiency and allow the organization to adapt to changing risk environments. For example, any control that mitigates or detects fraud or cyber attacks enhances the organization's resiliency by helping the organization uncover the risk and manage its impact. Resiliency is a result of a strong system of internal controls that give an organization the ability to manage disruptions seamlessly.

The need for controls is further driven by the complexity resulting from the necessity for diverse technical components to work with one another. While flexibility and adaptability of IT are crucial to meeting the changing needs of customers and business partners and responding to competitive pressures, they also add complexity to business and IT infrastructures. In addition, information security has been acknowledged as a key component of internal control with the emergence and widespread acceptance of standards such as the International Organization for Standardization Code of Practice for Information Security Management (ISO 17799).

Organizations that implement effective IT controls experience improvements in efficiencies, reliability of services, flexibility of systems, and availability of assurance evidence — all of which add value and increase stakeholder and regulator confidence in the organization. Some key indicators of effective IT controls include:

- The ability to execute planned, new work such as the IT infrastructure upgrades required to support new products and services.
- Delivery of development projects on time and within budget, resulting in cheaper and better product and service offerings when compared with competitors.
- Ability to allocate resources predictably.
- Consistent availability and reliability of information and IT services across the organization and for customers, business partners, and other external interfaces.
- Clear communication to management of effective controls.
- The ability to protect against new vulnerabilities and threats quickly and efficiently and to recover from any disruption of IT services.
- The efficient use of a customer support center or help desk.
- A security-conscious culture among end users throughout the organization.

Although the internal audit function likely will include specialist IT auditors to address IT issues in detail, the CAE also should understand IT control issues at a high level, particularly their interactions with other IT and non-IT controls. This understanding is particularly

important when discussing compliance or control deficiencies with high level managers such as the chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO), and with the various board committees. The CAE should be able to discuss relevant regulations and legislation with the audit committee, the chief legal counsel, and other relevant individuals and committees. The CAE also should understand how IT controls support reliability and effectiveness and help promote competitive advantage. Moreover, the CAE should thoroughly understand the major issues that drive the need for controls within the organization's particular sector to ensure they are considered during audit assessments. Without a thorough knowledge and understanding of IT controls, the auditor will be unable to grasp their significance or to assess them adequately as part of the overall review of internal control.

8. IT Roles in the Organizations

Many different roles have emerged in recent years for positions within the organization with responsibilities and ownership of IT controls. Each position at the governance, management, operational, and technical levels should have a clear description of its roles and responsibilities for IT controls to avoid confusion and ensure accountability for specific issues. This section addresses the various IT control roles and responsibilities within the organization and allocates them to specific positions within a hypothetical organizational structure. There is no universally applicable means of defining the organizational structure for IT control. The CAE should identify where IT control responsibilities lie and assess their appropriateness with regard to separation of duties, as well as any gaps that may exist in assigned responsibilities. Once this is done, the CAE will know whom to approach to discuss specific IT issues and where specific information can be obtained. Overall, the objectives for the use of IT within any organization are:

- To deliver reliable information efficiently and secure IT services in line with the organization's strategies, policies, external requirements, and risk appetite.
- To protect stakeholder interests.
- To enable mutually beneficial relationships with customers, business partners, and other outside parties that accomplish business objectives.
- To identify and respond to threats and potential violations of control appropriately.

Specific roles within the organization support these objectives. The position descriptions and titles will differ across different countries, industries, and organizations, and some of the roles may be merged within smaller organizations. However, some individuals within the organization must address the IT control function and interact with the CAE and internal audit staff members.

8.1 Board of Directors/Governing Body

One important role of the full board of directors is to determine and approve strategies, set objectives, and ensure that objectives are being met to support the strategies. In relation to IT, this requires:

- Awareness of the key IT topics, such as the IT and information security policies, and the concepts of risk as they relate to IT.
- Understanding of the IT strategy's infrastructure and components as well as awareness of key system development and acquisition projects and how they

support and impact overall corporate strategies, objectives, and short- and long-term budgets.
- Approval of the data classifications structure and the related access rights.

The board will establish various committees based on its relationships with the organization. The most common committees of the board are audit, compensation, and governance, but some boards have additional committees such as a risk management committee or finance committee. These committees may bear different names from those identified below, and their roles may vary. The functions, rather than the names, are important.

8.1.1 Audit Committee

The role of the audit committee encompasses oversight of financial issues, internal control assessment, risk management, and ethics. IT control is a strong element of each of these duties and calls for:

- Understanding of financial management (financial expert role) and the organization's reliance on IT for financial processing and reporting.
- Ensuring IT topics are included in the committee meeting agenda — especially CIO reporting.
- Ensuring general IT controls and controls in business application systems and processes involved in preparing financial statements are assessed and tested adequately.
- Overseeing the overall assessment of IT controls.
- Reviewing the business and control issues related to new systems development and acquisition.
- Examining internal and external audit plans and work to ensure IT topics are covered adequately.
- Reviewing the results of audit work and monitoring the resolution of issues raised.
- Understanding the IT topics that impact ethics monitoring.

8.1.2 Compensation Committee

The compensation committee has no direct relationship with IT. However, it can improve the board's oversight of IT by making IT one of the performance elements of any compensation plan it approves.

8.1.3 Governance Committee

The Governance Committee is responsible for board member selection and assessment and for leadership of the board's operations. In relation to IT, this committee should:

- Ensure that potential and current board members have a suitable IT knowledge or background.
- Assess board committees' performance in terms of their oversight of IT.
- Review any external regulatory governance assessments in relation to IT topics.
- Ensure that the board reviews IT policies periodically and that board meetings focus on IT with adequate frequency.

8.1.4 Risk Management Committee

The risk management committee is responsible for oversight of all risk analysis and assessment, risk response, and risk monitoring. Its role includes:

- Assessing the extent to which management has established effective enterprise risk management in the organization.
- Being aware of, and concurring with, the organization's risk appetite and tolerance.
- Appreciating the impact of IT-related risks.
- Reviewing the organization's risk portfolio — including IT risks — and considering it against the organization's risk appetite.
- Being apprised of the most significant IT risks and determining whether or not management's response to changes in risk and threats is appropriate.
- Monitoring and evaluating all activities performed by management to minimize all known and documented risks.

8.1.5 Finance Committee

The main role of the finance committee is to review financial statements, cash flow projections, and investment management. Members of this committee need to understand the control elements of IT that ensure the accuracy of information used to make key financing decisions and generate financial reports. They also should consider, and ask management to report on, the benefits and costs of maintaining — versus replacing — critical IT systems. Management's report should consider "soft" efficiency issues, such as gains or losses to productivity based on ease and efficiency of use; the "hard" costs of repairs and upgrades, and the potential for risk due to loss or corruption of data.

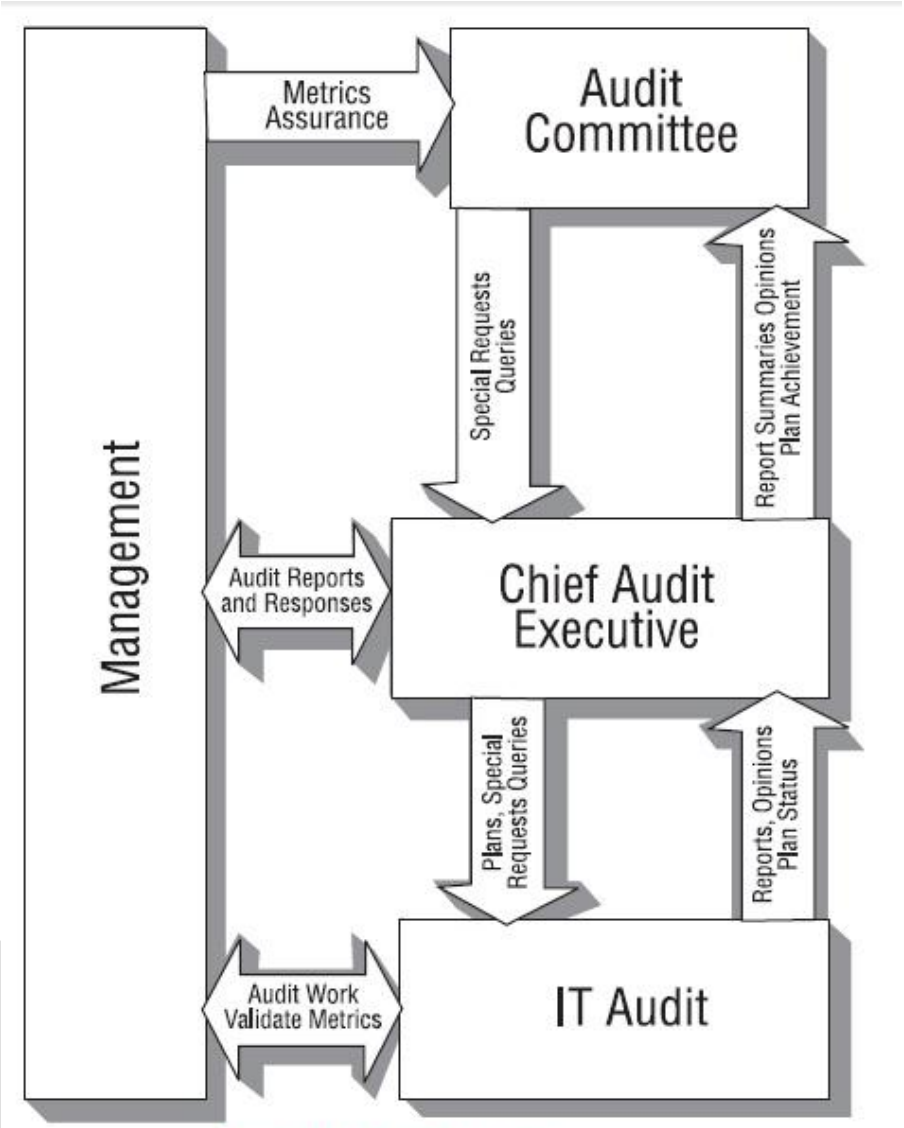
8.2 Management

Several specific roles have emerged in large organizations in relation to IT risk and control. As stated previously, small organizations might not allocate an individual for each role, although the function must still be performed. An individual may perform multiple roles, but care must be taken so that allocating these roles does not compromise the need for division of duties where roles are incompatible. Where IT is outsourced, there is still a requirement for organizations to keep many of these roles in-house to provide oversight of the outsourced functions.

8.2.1 Chief Executive Officer

The individual with overall strategic and operational control of the organization must consider IT in most aspects of the role. In particular, the CEO will:

- Define corporate objectives and performance measures in relation to IT.
- Act as custodian over the organization's critical success factors in relation to IT.
- Understand and approve the short-term and long-range strategy for IT.
- Approve IT resources for the organization, including structure and oversight/monitoring.
- Determine IT issues for periodic management, board, and staff discussion.
- Operate as the highest-level control owner, having ultimate responsibility for the success or failure of controls and for coordinating all other operational managers within their responsibilities framework who act as control owners of their particular areas.



Audit Interfaces

8.2.2 Chief Financial Officer

The CFO has overall responsibility for all financial matters in the organization and should have a strong understanding of the use of IT both to enable financial management and to support corporate objectives. This individual should have an overall understanding of:

- The total cost of ownership for IT initiatives.
- The entity's IT strategies for remaining technologically competitive.
- The technologies used to implement financial applications.
- The operation of specific financial applications.
- The limitations and benefits of IT.
- The IT control structure for general controls that apply to all business systems and data as well as controls that are specific to financial applications.

The CFO should operate as the highest-level control owner for financial systems and data.

8.2.3 Chief Information Officer

The CIO has overall responsibility for the use of IT within the organization. In relation to IT controls, the CIO should:

- Understand the business requirements that drive the need to implement IT.
- Develop IT partnerships with business management to:
  - Ensure IT strategy is aligned with the business strategy.
  - Ensure compliance.
  - Profit from process-efficiency gains.
  - Mitigate assessed risks.
- Design, implement, and maintain an IT internal control framework.
- Plan, source, and control IT resources.
- Explore, assess, select, and implement technology advances (e.g. wireless communications).
- Provide training for IT personnel to ensure that levels of knowledge and skills remain current.
- Operate as the highest-level data/system custodian and IT control owner.
- Measure the operational performance of IT in support of business objectives by:
  - Setting expectations.
  - Evaluating results.
- Developing all necessary means to verify and acknowledge that IT is providing services and support as expected by its users and final customers such as regulators and external and internal auditors.

8.2.4 Chief Security Officer

The chief security officer (CSO) is responsible for all security across the entire organization, including information security, which may be the responsibility of a chief information security officer as well.

The CSO:

- Has responsibility for documenting the enterprise security policy and for ensuring mechanisms have been established to communicate and enforce the policy.
- Has overall responsibility for logical and physical security in the organization and for all external connections to the Internet or other networks.
- Acts as a key link between the compliance, legal, CIO, and audit functions.
- Is at the forefront of implementing key compliance programs affecting IT.
- Is responsible for business continuity planning, including incident handling and disaster recovery.
- Ensures that security staff provide support for implementing controls at all levels.
- Acts as the key leader for investigating and evaluating new best practices that may be incorporated into the organization.

8.2.5 Chief Information Security Officer (CISO)

Information security is a subset of the overall security role. The CISO:

- Develops and implements the information security policy in coordination with the CSO.
- Controls and coordinates information security resources, ensuring they are allocated adequately to meet the organization's security objectives.
- Ensures alignment of information security and business objectives.

- Manages operational information risks throughout the organization.
- Oversees security within the IT organization.
- Provides education and awareness on information security issues and new best practices.
- Develops end-user policies for the usage of IT information, in conjunction with the human
- resources function.
- Coordinates information security work with the chief risk officer (CRO) and CIO.
- Advises the CEO, CRO, CIO, and board on IT risk issues.
- Acts as a key link for the CAE when internal auditing performs IT control-related audits.

8.2.6 Chief Legal Counsel (CLC)

Legal counsel may be an employee or officer of the organization or an external legal adviser. The role involves:

- Understanding and dealing with the liabilities arising out of information disclosures and providing policy level guidance to help manage risks related thereto.
- Ensuring financial reports and presentations comply with laws and regulations.
- Understanding IT legal issues and advising on legal risks related to IT.
- Managing organizational reputation in relation to legal issues, compliance, and public relations.
- Understanding fraud involving IT.
- Managing IT contractual issues.
- Understanding investigative forensics protocols regarding suspected criminal activity.

8.2.7 Chief Risk Officer

The CRO is concerned with managing risk at all levels of the organization. Because IT risks form a part of this function, the CRO will consider them, with the help of the CISO. This includes:

- Analysis and assessment of IT risk exposures, including information compromises such as loss, damage, unauthorized disclosure, and interrupted access.
- Assessment of IT events such as interruptions, disasters, and changes.
- Analysis and assessment of business risk as it is affected by IT risk.
- Monitoring, supporting, and acting as a mentor for all IT activities related to minimizing risks.

8.3 Audit

8.3.1 Internal Auditing – CAE and Audit Staff

Internal auditing is an essential part of the corporate governance process, whether or not a specific internal audit group is employed. Internal auditors need a general understanding of IT, but the level of their understanding will vary depending on the category of auditing or audit supervision they perform. The internal audit role in relation to IT involves:

- Advising the audit committee and senior management on IT internal control issues.
- Ensuring IT is included in the audit universe and annual plan (selecting topics).

- Ensuring IT risks are considered when assigning resources and priorities to audit activities.
- Defining IT resources needed by the internal audit department, including specialized training of audit staff.
- Ensuring that audit planning considers IT issues for each audit.
- Liaising with audit clients to determine what they want or need to know.
- Performing IT risk assessments.
- Determining what constitutes reliable and verifiable evidence.
- Performing IT enterprise-level controls audits.
- Performing IT general controls audits.
- Performing IT applications controls audits.
- Performing specialist technical IT controls audits.
- Making effective and efficient use of IT to assist the audit processes.
- During systems development or analysis activities, operating as experts who understand how controls can be implemented and circumvented.
- Helping to monitor and verify the proper implementation of activities that minimize all known and documented IT risks.

8.3.2 External Auditor

Independent external audits are a requirement for most organizations and normally are performed annually. Topics to be considered by the internal audit department and the audit committee include:

- The extent of the external auditor's responsibilities for understanding and evaluating the IT system and related IT controls during financial audits.
- The scope of the external auditor's responsibilities for examining the IT system and controls during any formal attestation that may be required by statute or regulation, such as internal controls over financial reporting and other regulatory requirements.

9 Analyzing Risk

9.1 Risk Determines Response

IT controls are selected and implemented on the basis of the risks they are designed to manage. As risks are identified — through experience or formal risk assessment — suitable risk responses are determined, ranging from doing nothing and accepting the risk as a cost of doing business to applying a wide range of specific controls, including insurance.

It would be a relatively straightforward task to create a list of recommended IT controls that *must* be implemented within each organization. However, each control has a specific cost that may not be justified in terms of cost effectiveness when considering the type of business done by the organization. Furthermore, no list of controls is universally applicable across all types of organizations. Although there is a lot of good advice available on the choice of suitable controls, strong judgment must be used. Controls must be appropriate for the level of risk faced by the organization.

The CAE should be able to advise the audit committee that the internal control framework is reliable and provides a level of assurance appropriate to the risk appetite of the organization. In this respect, the risk appetite of the organization is defined as:

"… the degree of risk, on a broad-based level, that a company or other organization is willing to accept in pursuit of its goals. Management considers the organization's risk appetite first in evaluating strategic alternatives, then in setting objectives aligned with the selected strategy, and in developing mechanisms to manage the related risks."

In addition, the CAE should consider risk tolerance. defined *risk tolerance* as:

"… the acceptable level of variation relative to the achievement of objectives. In setting specific risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with its risk appetite."

Thus, the CAE should consider whether or not:

- The organization's IT environment is consistent with the organization's risk appetite.
- The internal control framework is adequate to ensure that the organization's performance remains within the stated risk tolerances.

9.2 Risk Considerations in Determining the Adequacy of IT Controls

Risk management applies to the entire spectrum of activity within an organization, not just to the application of IT. IT cannot be considered in isolation, but must be treated as an integral part of all business processes. Choosing IT controls is not simply a matter of implementing those recommended as best practices. They must add value to the organization by reducing risk efficiently and increasing effectiveness. When considering the adequacy of IT controls within the organization's internal control framework, the CAE should consider the processes established by management to determine:

- The value and criticality of information.
- The organization's risk appetite and tolerance for each business function and process.
- IT risks faced by the organization and quality of service provided to its users.
- The complexity of the IT infrastructure.
- The appropriate IT controls and the benefits they provide.
- Harmful IT incidents in the past 24 months.

The frequency of risk analysis is important and is influenced greatly by technological change. In a static business and technical infrastructure environment, the risk assessment process could be as infrequent as yearly or could be performed in concert with a major implementation project.

9.2.1 The IT Infrastructure

Analyzing and assessing risk in relation to IT can be complex. The IT infrastructure consists of hardware, software, communications, applications, protocols (rules), and data, as well as their implementation within physical space, within the organizational structure, and

between the organization and its external environment. Infrastructure also includes the people interacting with the physical and logical elements of systems.

The inventory of IT infrastructure components reveals basic information about the vulnerabilities of the environment. For example, business systems and networks connected to the Internet are exposed to threats that do not exist for self-contained systems and networks. Because Internet connectivity is an essential element of most business systems and networks, organizations must make certain that their systems and network architectures include the fundamental controls that ensure basic security.

The complete inventory of the organization's IT hardware, software, network, and data components forms the foundation for assessing the vulnerabilities within the IT infrastructures that may impact internal controls. Systems architecture schematics reveal the implementation of infrastructure components and how they interconnect with other components within and outside the organization. To the information security expert, the inventory and architecture of IT infrastructure components — including the placement of security controls and technologies — reveals potential vulnerabilities. Unfortunately, information about a system or network can also reveal vulnerabilities to a potential attacker, so access to such information must be restricted to only those people who need it. A properly configured system and network environment will minimize the amount of information it provides to would-be attackers, and an environment that appears secure presents a less attractive target to most attackers.

9.2.2 IT Risks Faced by the Organization

The CAE discusses IT risk issues with the CIO and process owners to ensure that all related parties have an appropriate awareness and understanding of the technical risks faced by the organization through the use of IT and their roles in applying and maintaining effective controls.

9.2.3 Risk Appetite and Tolerance

Armed with the knowledge of IT risks, the auditor can validate the existence of effective controls to meet the established risk appetite of the organization and its risk tolerance in relation to IT. The auditor's assessment will involve discussions with many members of management and ultimately with the board. The level of detail of these discussions can be determined by the CRO with input from the CIO, CISO, CSO, CAE, and process owners. The final decision regarding risk appetite and tolerance must be made by the risk committee — with input from the audit committee — and must be endorsed by the full board. The definitions of *risk appetite* and *tolerance* must be communicated to all relevant managers for implementation.

The goal of enterprise risk management is to ensure that everyone is working with the same level and understanding of risk and that decisions made at all levels of management are consistent with the organization's risk appetite.

9.2.4 Performing Risk analysis

Performing risk analysis is not the sole preserve of either the CRO or the CAE, although both of them, or their representatives, should be involved, along with representatives from IT and the business areas. There are eight basic questions associated with the risk assessment process. The first five include:

- What are the assets at risk and the value of their confidentiality, integrity, and availability?
- What could happen to affect that information asset value adversely (threat event)?

Implicit to this question is the vulnerability analysis and mapping of vulnerabilities to threats and potentially impacted information assets.

- If a threat event happened, how bad could its impact be?
- How often might the event be expected to occur (frequency of occurrence)?
- How certain are the answers to the first four questions (uncertainty analysis)?

The next three questions apply to risk mitigation analysis:

- What can be done to reduce the risk?
- How much will it cost?
- Is it cost-efficient?

9.2.5 Value of Information

Determining the value of the information processed and stored is not an easy task due to the multidimensional nature of value. The Generally Accepted Information Security Principles, address information value within the following categories:

- Exclusive possession – cost in the event of a breach of confidentiality.
- Utility – cost in the event of a loss of integrity.
- Cost of creation/re-creation.
- Liability in the event of litigation.
- Convertibility/negotiability – represents market value.
- Operational impact of unavailability.

9.2.6 Appropriate IT Controls

Finally, appropriate IT controls must be chosen and implemented to address the risks identified. Much advice is available on this subject. The CAE and internal audit group should be involved in the process of analyzing and assessing risk. While they should operate in a manner that maintains the independence and objectivity of their function, they also must provide an opinion on the effectiveness of the internal control framework.

9.3 Risk Mitigation Strategies

When risks are identified and analyzed, it is not always appropriate to implement controls to counter them. Some risks may be minor, and it may not be cost effective to implement expensive control processes for them. In general, there are several ways to mitigate the potential impact of risks:

- **Accept the risk.** One of the primary functions of management is managing risk. Some risks are minor because their impact and probability of occurrence is low. In this

case, consciously accepting the risk as a cost of doing business is appropriate, as well as periodically reviewing the risk to ensure its impact remains low.

- **Eliminate the risk.** It is possible for a risk to be associated with the use of a particular technology, supplier, or vendor. The risk can be eliminated by replacing the technology with more robust products and by seeking more capable suppliers and vendors.

- **Share the risk.** Risk mitigation approaches can be shared with trading partners and suppliers. A good example is outsourcing infrastructure management. In such a case, the supplier mitigates the risks associated with managing the IT infrastructure by being more capable and having access to more highly skilled staff than the primary organization. Risk also may be mitigated by transferring the cost of realized risk to an insurance provider.

- **Control/mitigate the risk.** Where other options have been eliminated, suitable controls must be devised and implemented to prevent the risk from manifesting itself or to minimize its effects.

9.4 Control Characteristics to Consider

Some of the issues to be addressed during the IT control evaluation process include:

- Is the control effective?
- Does it achieve the desired result?
- Is the mix of preventive, detective, and corrective controls effective?
- Do the controls provide evidence when control parameters are exceeded or when controls fail? How is management alerted to failures, and which steps are expected to be taken?
- Is evidence retained (audit or management trail)?

9.5 Baseline IT Controls

IT controls are to be applied when mitigating the risks is the best option. While IT controls should be applied with due regard to the relevant risks, there is a basic set of controls that need to be in place to provide a fundamental level of IT hygiene. For example, the use of a firewall to control traffic between a corporate network and a public network such as the Internet, or between internal network domains, is a baseline control. The level of risk associated with the business value and sensitivity of the network traffic, the services provided, and the information stored in the infrastructure determines the extent to which firewalls restrict traffic coming into and departing from an organization's networks. Firewalls are a physical and logical manifestation of information security policy elements that dictate what is allowed into or out of an organization. IT controls most widely applicable to all IT infrastructures are known as *baseline controls*. There are many types of baseline controls.

It is not easy to define the baseline IT controls, because the general threats, such as malicious software and hacking, change and newer technologies and applications frequently are implemented across the organization.

The following questions can be considered when selecting a suitable set of baseline controls:

- Do IT policies — including for IT controls — exist?
- Have responsibilities for IT and IT controls been defined, assigned, and accepted?
- Are IT infrastructure equipment and tools logically and physically secured?
- Are access and authentication control mechanisms used?
- Is antivirus software implemented and maintained?
- Is firewall technology implemented in accordance with policy (e.g., where external connections such as the Internet exist and where separation between internal networks is needed)?
- Are external and internal vulnerability assessments completed and risks identified and appropriately resolved?
- Are change and configuration management and quality assurance processes in place?
- Are structured monitoring and service measurement processes in place?
- Are specialist IT audit skills available (either internally or outsourced)?

10 Choosing & Monitoring IT Controls

10.1 Choosing a Control Framework

The process of identifying and assessing the IT controls necessary to address specific risks is aided considerably by the organization's adoption of a formal control framework. This framework should apply to, and be used by, the whole organization — not just internal auditing. Although many frameworks exist, no single framework covers every possible business type or technology implementation.

A control framework is a structured way of categorizing controls to ensure that the whole spectrum of control is adequately covered. The framework can be informal or formal. A formal approach will satisfy the various regulatory or statutory requirements faced by many organizations more readily.

Each organization should examine existing control frameworks to determine which of them — or which parts — most closely fit its needs. The process of choosing or constructing a control framework should involve all positions in the organization with direct responsibility for controls. The CAE should be involved in the decision process because the internal audit function will assess the framework's adequacy and use it as a context for planning and performing audit work. The CAE needs an overall knowledge of IT risk issues to assess the effectiveness and appropriateness of IT controls. The CAE will base the audit plan and allocate audit resources according to the IT areas and issues that merit attention due to their inherent levels of risk. Risk analysis and assessment cannot be viewed as a one-time process, especially when applied to IT, because technology changes constantly and rapidly, as do the associated risks and threats. Categorizing IT controls according to their organizational placement, purpose, and functionality is useful in assessing their value and adequacy, as well as the adequacy of the system of internal controls. Knowledge of the range of available IT controls, the driving forces for controls, and organizational roles and responsibilities allows for comprehensive risk analysis and assessments.

In assessing control effectiveness, it is also useful to understand whether the controls are mandated or voluntary, discretionary or nondiscretionary, manual or automated, primary or secondary, and subject to management override.

Finally, the assessment of IT controls involves selecting key controls for testing, evaluating test results, and determining whether or not evidence indicates any significant control weaknesses. The checklist in Appendix H can help the CAE ensure all relevant issues have been considered when planning and directing internal audit assessments of IT controls.
Several existing frameworks and approaches can assist the CAE and other managers when determining IT control requirements. However, organizations should investigate enough frameworks to determine which one best fits their own needs and culture.

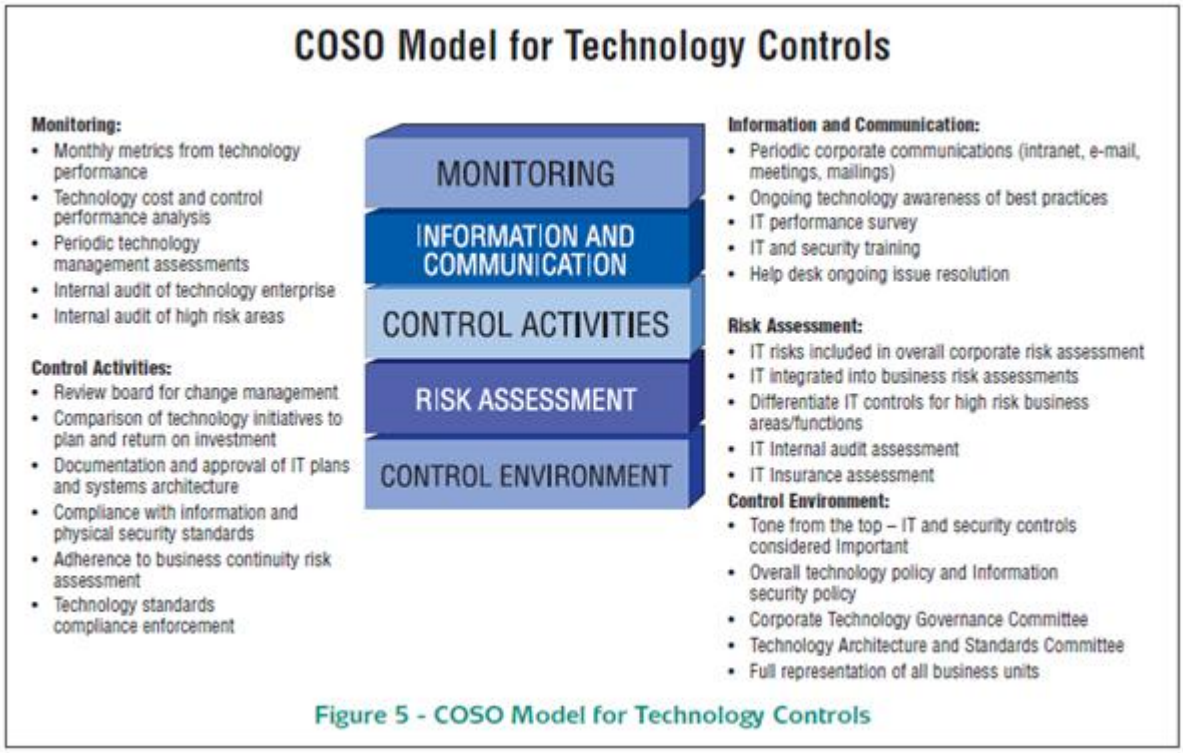


Figure 5 - COSO Model for Technology Controls

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a commonly used framework for internal controls. The COSO framework is designed to provide a model that corporations can mainly use to run an efficient and well-controlled financial environment. However, it is not specific and detailed to all areas of IT. This framework is considered to be a “suitable, recognized” framework to adopt as it covers all areas of IT
implementation, albeit at a high level of abstraction.

COSO's main components:

- Internal control environment
- Objective setting
- Event identification

- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring.

10.2 Monitoring IT Controls

Determining where to apply control monitoring and assessment and their frequency is not easy. Participation by the auditor in risk analysis exercises and implementation of a suitable control framework help ensure that the CAE has sufficient information to create a suitable audit plan to address the major IT risks.

Ultimately, management is responsible for monitoring and assessing controls. The auditor's monitoring and assessments are performed to independently attest to management's assertions regarding the adequacy of controls. Management's control monitoring and assessment activities should be planned and conducted within several categories as follows:

10.2.1 Ongoing Monitoring

- **Daily/Periodic** – Some information must be checked daily to ensure controls are working as required. Management normally performs such monitoring, which traditionally involves checking data-processing control reports to reconcile satisfactory task and job completion. Such controls, where they exist, are most often automated. The CAE will ensure such management monitoring is in place and that it is subjected to internal audit assessment.

- **Event-driven** – Discrepancies, or even frauds, may result within normal processing or in special circumstances, such as where there are large-value transactions. In many IT environments, malicious attacks are likely. Consequently, specific controls should be in place to detect and report unusual activities to an entity within the organization that is chartered specifically to investigate and determine if preventive or corrective actions should be applied. Such monitoring controls are complementary to the normal controls employed and provide assurance on the effectiveness of those controls or early warning that they may have been breached.

- **Continuous** – Technology now provides the ability to monitor and assess certain sensitive controls continuously. A good example of continuous monitoring is the use of intrusion detection software, which continually monitors network traffic for evidence that other protective controls, such as firewalls and virus protection, may have been breached.

10.2.2 Special Reviews

- **Annual (or quarterly) control assessment** –
  Although the board of directors is required to make statements regarding the effectiveness of internal controls, management actually must provide the assurances to the board, and the internal and external auditors must perform sufficient audit work to attest to these assurances.

- **Audit reviews** – A regular program of audit reviews is still necessary, despite the proliferation of new audit approaches. It is only through the formal review of infrastructure, process, and technology implementation that the CAE can assess the overall reliability and robustness of the system of internal controls. In the past, such reviews were planned on a cyclical basis. However, given the fast-changing world of IT, audit reviews should now be scheduled based on the level of risk.

11 Assessment

Assessing IT controls is an ongoing process, because business processes are constantly changing, technology continues to advance, threats evolve as new vulnerabilities emerge, and audit methods keep improving. The CAE should keep assessments of IT controls that support business objectives near the top of the audit agenda.

Assessing IT controls is not a case of determining whether best practices are employed, as controls are specific to the organization's mission, objectives, culture, deployed processes and technologies, and risks. Technology should be tailored to provide effective control, and the CAE should ensure internal auditing adopts appropriate and effective methods. Auditing IT is a continuous learning process. The CAE is rarely in a position to understand all the technologies used in his or her environment and their specific control implications. That is why properly certified and experienced IT auditors are a major asset for any internal audit function. However, the CAE should understand the overall control issues and be able to communicate them to senior management and to appropriate committees of the board of directors in a form they will understand and in a manner that will result in an appropriate response. The key to assessing IT controls effectively is communication with technical staff, management, and board members.

12 Auditor Knowledge Considerations

Proficiency of The IIA's Standards require that the internal audit activity collectively should possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities. Varying levels of IT knowledge are needed throughout the organization to provide a systematic, disciplined approach to evaluating and improving the effectiveness of risk management, control, and governance processes. Knowledge of how IT is used, the related risks, and the ability to use IT as a resource in the performance of audit work is essential for auditor effectiveness at all levels.

The IIA's International Advanced Technology Committee has identified three categories of IT knowledge for internal auditors.

12.1 Category 1 – All Auditors

Category 1 is the knowledge of IT needed by all professional auditors, from new recruits up through the CAE. Basic IT knowledge encompasses understanding concepts such as the differences in software used in applications, operating systems and systems software, and networks. It includes comprehending basic IT security and control components such as perimeter defenses, intrusion detection, authentication, and application system controls. Basic knowledge includes understanding how business controls and assurance objectives

can be impacted by vulnerabilities in business operations and the related and supporting systems, networks, and data components. It is fundamentally about ensuring that auditors have sufficient knowledge to focus on understanding IT risks without necessarily possessing significant technical knowledge.

12.2 Category 2 – Audit Supervisors

Category 2 applies to the supervisory level of auditing. In addition to having basic IT knowledge, audit supervisors must understand IT issues and elements sufficiently to address them in audit planning, testing, analysis, reporting, follow-up, and assigning auditor skills to the elements of audit projects. Essentially, the audit supervisor must:

- Understand the threats and vulnerabilities associated with automated business processes.
- Understand business controls and risk mitigation that should be provided by IT.
- Plan and supervise audit tasks to address IT-related vulnerabilities and controls, as well as the effectiveness of IT in providing controls for business applications and environments.
- Ensure the audit team has sufficient competence — including IT proficiency — for audits.
- Ensure the effective use of IT tools in audit assessments and testing.
- Approve plans and techniques for testing controls and information.
- Assess audit test results for evidence of IT vulnerabilities or control weaknesses.
- Analyze symptoms detected and relate them to causes that may have their sources in business or IT planning, execution, operations, change management, authentication, or other risk areas.
- Provide audit recommendations based on business assurance objectives appropriate to the sources of problems noted rather than simply reporting on problems or errors detected.

12.3 Category 3 – Technical IT Audit Specialists

Category 3 applies to the technical IT audit specialist. Although IT auditors may function at the supervisory level, they must understand the underlying technologies supporting business components and be familiar with the threats and vulnerabilities associated with the technologies. IT auditors also may specialize in only certain areas of technology.

Software for Business

1. Introduction

Since the aim of this course is to enable the students with enough IT knowledge that they, being a manager, take right decision about acquiring and managing the IT infrastructure that it strengthen the business processes of the company they are the part of. Information technology is a major investment for any business - and computer software is a key part of that investment. This is therefore important that the course taker is equipped with right knowledge about software types that can help their business. Software not only makes your computer hardware perform important tasks, but also helps your business work more efficiently and could even lead to new ways of working. It is therefore a crucial business asset and you should choose your software carefully so that it matches your business needs. This chapter will help you understand different types of software and how to choose the most appropriate for your business.

Business benefits of new software

Before investing in new software, you should think about what you want it to do for you. For example, you might want to:

- cut costs by automating routine tasks
- improve customer service - e.g. with an interactive online contact system for after-sales support or to check order status
- enable your employees to work more efficiently
- communicate and collaborate electronically with suppliers or partners

2. Choosing and buying software

As a manager, You should also discuss with your employees, suppliers and customers who may have ideas for improving your business processes using IT. They may also keep you up to date about new advancements in software field and you may come up with a better alternative.

There are many ways to get advice and support when choosing software, including software or business consultants - although they may be biased towards software they are familiar with software vendors - again, remember their possible bias professional and trade associations the computer press - magazines like Computer Weekly and Computing can be a good way to get information on the basic issues, so you know the right questions to ask

2.1 Acquiring Software Solution

First It is recommended to write down the objectives and potential benefits of new software, then prioritize the list to work out the best returns on investment.

2.2 Document your business

Diagrams may make documenting your business easier - for example, using boxes for processes and arrows to show documents, invoices etc, entering or leaving processes.

Documenting your business in this way will help you identify areas where new software could improve your business processes. It will also help you explain your business and its requirements to potential suppliers when buying software.

Compare your list of requirements with the information that you have about each package. Reject all packages that cannot meet your 'must have' requirements. From the remainder, select the one that delivers the greatest number of your advantageous and 'nice to have' features at a price your business can afford.

2.3 Additional costs

As well as the price of software, you should also consider support costs, future upgrade costs and the need for hardware upgrades to use your software to full effect.

Choose software that will run on your current hardware, as long as this doesn't reduce potential benefits. You should include any hardware upgrade costs in your budget.

2.4 Planning for the future

Ideally you should develop a long-term strategy, covering your future IT needs. This should take into account potential changes in customers, staffing levels and/or your products and services.

3. Types of software

There are various types of software and you need to know the differences between them.

3.1 Bespoke/Customized Software Applications

It is possible to write software specifically for your business. You can either:

- Hire a software developer and write the software in house. However, If you run a small business, writing the software yourself is unlikely to be cost-effective as you need to spend on the software development expert and lots of time.
- Have the software written by an external supplier. With specialist help, you should get the exact functionality you need. However, the price is likely to be high, and you will be tied to that supplier for future support.

Producing any bespoke software can take a long time and your staff will need to have an input in the development process. Otherwise, chances are that the software my malfunction and contains bugs.

3.2 System or application software

System software is not directly useful for business purposes but makes the computer hardware useful. An example is the Microsoft Windows operating system.

Application software is designed for a specific use - like word processing or accounts. You will need both types of software.

3.3 Packaged software

Packaged software is standardized and generally low priced. The functionality may not be exactly what you need, but it could make sense to change your business practices to suit the software rather than having software specially written.

An example of packaged software can be accounting systems like Peachtree & Quick Books.

The high volume of sales of such software usually means that you will be able to get support and training from a number of different sources.

Standard software packages are usually the best choice for small businesses.

3.4 Business Intelligence Software

Business intelligence software are a type of application software designed to retrieve, analyze and report data. The tools generally read data that have been previously stored, often, though not necessarily, in a data warehouse.

Business Intelligence software, also called BI software, is software that is designed to analyze business data to better understand an organization's strengths and weaknesses. Business intelligence software allows an organization's management to better see the relationship between different data for better decision-making and optimal deployment of resources. Business Intelligence software plays a key role in the strategic planning process of the corporation.

These systems allow a company to gather, store, access and analyze corporate data to aid in decision-making. Generally these systems will illustrate business intelligence in the areas of customer profiling, customer support, market research, market segmentation, product profitability, statistical analysis, and inventory and distribution analysis to name a few.

he types of tools that make up a business intelligence software application solution generally include tools for spreadsheets, operational dashboards, data mining, reporting, search (query), analytics processing (OLAP), content viewer, and other components of enterprise resource planning (ERP) systems. Often, business intelligence software may also integrate tools designed for specific verticals, such as retail, healthcare or education.

Other examples include accounting, collaboration, customer relationship management (CRM), management information systems (MIS), enterprise resource planning (ERP), invoicing, human resource management (HRM), content management (CM) and service desk management.

Business intelligence software applications can be deployed in a number of ways, with the following being the most common options:

- Cloud Computing (cloud) Implementation: private cloud, hybrid cloud or a public cloud.
- On-Premise Installment: deployed in-house using owned or leased equipment.
- SaaS (hosted on-demand): hosted by the application service provider (ASP).

4. Enterprise Resource Planning

Enterprise Resource Planning is the latest high end solution, information technology has lent to business application. The ERP solutions seek to streamline and integrate operation processes and information flows in the company to synergize the resources of an organization namely men, material, money and machine through information. Initially implementation of an ERP package was possible only for very large Multi National Companies and Infrastructure Companies due to high cost involved. Today many companies in India have gone in for implementation of ERP and it is expected in the near future that 60% of the companies will be implementing one or the other ERP packages since this will become a must for gaining competitive advantage.

In the present business environment, role of a Chartered Accountant is considered to be very important and inevitable. Chartered Accountants as managers, consultants, advisors or auditors play an important role in controlling, managing, and supporting the business.

As the business needs are very complex in nature, the implementation of an ERP package needs Chartered Accountants with functional skills for evaluation, Business Process Reengineering (BPR), Mapping of Business requirements, Report designing, ensuring Business controls, customization of the package for the specific requirements, Documentation etc.,

Sooner or later a Chartered Accountant without the knowledge of ERP may feel as if he is a fish out of the bowl. By this article it is attempted to highlight various aspects of ERP and specific areas of ERP that are relevant for Chartered Accountants.

4.1 Evolution of ERP

In the ever growing business environment the following demands are placed on the industry :

- Aggressive Cost control initiatives
- Need to analyze costs / revenues on a product or customer basis
- Flexibility to respond to changing business requirements
- More informed management decision making
- Changes in ways of doing business

Difficulty in getting accurate data, timely information and improper interface of the complex natured business functions have been identified as the hurdles in the growth of any business. Time and again depending upon the velocity of the growing business needs, one or the other applications and planning systems have been introduced into the business world for crossing these hurdles and for achieving the required growth. They are:

- Management Information Systems (MIS)
- Integrated Information Systems (IIS)
- Executive Information Systems (EIS)
- Corporate Information Systems (CIS)
- Enterprise Wide Systems (EWS)

- Material Resource Planning (MRP)
- Manufacturing Resource Planning (MRP II)
- Money Resource Planning (MRP III)

The latest planning tool added to the above list is Enterprise Resource Planning.

4.2 Need for ERP

Most organizations across the world have realized that in a rapidly changing environment, it is impossible to create and maintain a custom designed software package which will cater to all their requirements and also be completely up-to-date. Realizing the requirement of user organizations some of the leading software companies have designed Enterprise Resource Planning software which will offer an integrated software solution to all the functions of an organization.

4.3 Benefits of ERP

The benefits accruing to any business enterprise on account of implementing are unlimited. According to the companies like NIKE, DHL, Tektronix, Fujitsu, Millipore, Sun Microsystems, following are some of the benefits they achieved by implementing ERP packages:

- Gives Accounts Payable personnel increased control of invoicing and payment processing and thereby boosting their productivity and eliminating their reliance on computer personnel for these operations.
- Reduce paper documents by providing on-line formats for quickly entering and retrieving information.
- Improves timeliness of information by permitting, posting daily instead of monthly.
- Greater accuracy of information with detailed content, better presentation, fully satisfactory for the Auditors.
- Improved Cost Control
- Faster response and follow up on customers
- More efficient cash collection, say, material reduction in delay in payments by customers.
- Better monitoring and quicker resolution of queries.
- Enables quick response to change in business operations and market conditions.
- Helps to achieve competitive advantage by improving its business process.
- Improves supply-demand linkage with remote locations and branches in different countries.
- Provides a unified customer database usable by all applications.
- Improves International operations by supporting a variety of tax structures, invoicing schemes, multiple currencies, multiple period accounting and languages.
- Improves information access and management throughout the enterprise.
- Provides solution for problems like Y2K and Single Monitory Unit(SMU) or Euro Currency.

4.4 Features of ERP

Some of the major features of ERP and what ERP can do for the business system are as below:

- ERP facilitates company-wide Integrated Information System covering all functional areas like Manufacturing, Selling and distribution, Payables, Receivables, Inventory, Accounts, Human resources, Purchases etc.,

- ERP performs core Corporate activities and increases customer service and thereby augmenting the Corporate Image.
- ERP bridges the information gap across the organization.
- ERP provides for complete integration of Systems not only across the departments in a company but also across the companies under the same management.
- ERP is the only solution for better Project Management.
- ERP allows automatic introduction of latest technologies like Electronic Fund Transfer(EFT), Electronic Data Interchange(EDI), Internet, Intranet, Video conferencing, E-Commerce etc.
- ERP eliminates the most of the business problems like Material shortages, Productivity enhancements, Customer service, Cash Management, Inventory problems, Quality problems, Prompt delivery etc.,
- ERP not only addresses the current requirements of the company but also provides the opportunity of continually improving and refining business processes.
- ERP provides business intelligence tools like Decision Support Systems (DSS), Executive Information System (EIS), Reporting, Data Mining and Early Warning Systems (Robots) for enabling people to make better decisions and thus improve their business processes

4.5 Components of ERP

To enable the easy handling of the system the ERP has been divided into the following Core subsystems:

- Sales and Marketing
- Master Scheduling
- Material Requirement Planning
- Capacity Requirement Planning
- Bill of Materials
- Purchasing
- Shop floor control
- Accounts Payable/Receivable
- Logistics
- Asset Management
- Financial Accounting

4.6 Selection of ERP

Once the BPR is completed the next task is to evaluate and select a suitable package for implementation. Evaluation of the right ERP package is considered as more crucial step. Evaluation and selection involves:

- checking whether all functional aspects of the Business are duly covered
- checking whether all the business functions and processes are fully integrated
- checking whether all the latest IT trends are covered
- checking whether the vendor has customizing and implementing capabilities
- checking whether the business can absorb the cost
- checking whether the ROI is optimum

4.7 Suppliers of ERP

There are many numbers of ERP suppliers who are very active in the market. Some of the companies offering renowned international ERP products include:

- Baan
- CODA
- D&B
- IBM
- JD Edwards
- Marcarn
- Oracle
- Peoplesoft
- Platinum
- Ramco
- SAP
- SMI
- Software 2000

4.7 BPR and ERP

Business Process Reengineering is a pre-requisite for going ahead with a powerful planning tool, ERP. An in depth BPR study has to be done before taking up ERP. Business Process Reengineering brings out deficiencies of the existing system and attempts to maximize productivity through restructuring and re-organizing the human resources as well as divisions and departments in the organisation

Business Process Engineering evolves the following Steps:

- Study the current system
- Design and develop new systems
- Define Process, organization structure and procedure
- Develop customize the software
- Train people
- Implement new system

The principle followed for BRP may be defined as USA principle(Understand, Simplify Automate)

i.e., Understanding the existing practices, Simplifying the Processes and Automate the Process. Various tools used for this principle are charted below:

- Understand Simplify Automate
- Diagramming Eliminating EDI
- Story-boarding Combining ERP
- Brain storming Rearranging

4.9 Implementation of ERP

In case the organization decides to develop a in-house bespoke implementation of ERP, Implementing an ERP package has to be done on a phased manner. Step by step method of implementing will yield a better result than big-bang introduction. The total time required for successfully implementing an ERP package will be anything between 18 and 24 months. The normal steps involved in implementation of an ERP are as below:

- Project Planning
- Business & Operational analysis including Gap analysis
- Business Process Reengineering
- Installation and configuration
- Project team training
- Business Requirement mapping
- Module configuration
- System interfaces
- Data conversion
- Custom Documentation
- End user training
- Acceptance testing
- Post implementation/Audit support

The above steps are grouped and sub-divided into four major phases namely

1. detailed discussions,
2. Design & Customization,
3. Implementation and
4. Production.

The phases of implementation vis-a-vis their tasks and respective deliverables are as below:

4.9.1 Detailed Discussion Phase:

1. **Task**
   Project initialization, Evaluation of current processes, business practices, Set-up project organization
2. **Deliverables**
   Accepted norms and Conditions, Project Organization chart, Identity work teams

4.9.2 Design and customization Phase:

1. **Task**
   Map organization, Map business process, Define functions and processes, ERP software configuration and Build ERP system modifications.
2. **Deliverables**
   Organization structure, Design specification, Process Flow Diagrams, Function Model, Configuration recording and system modification.

4.9.3 Implementation Phase:

1. **Task**
   Create go-live plan and documentation, Integrate applications, Test the ERP customization, Train users
2. **Deliverables**
   Testing environment report, Customization Test Report and Implementation report

4.9.4 Production Phase:

1. **Task**
   Run Trial Production, Maintain Systems
2. **Deliverables**
   Reconciliation reports, Conversion Plan Execution

5. CRM

5.1 Introduction

CRM stands for Customer Relationship Management. CRM is used in an organization to manage customer relationships proficiently. It is a modified method to contact customers and to build long-term relationships with them. It stores customers' information in a database and further uses it for

their benefit. CRM helps in binding strong relationship between organization and customers. It helps in managing issues related to pre-sales, post-sales and support operations.
CRM includes adoption of IT related systems, training of employees and amendment in business processes related to customers. It is not just software but an approach to update and enhance business methods to improve customers' relationship with the organization.

Successful organizations understand that their growth is contingent upon both new and repeat business. In
order to grow as a company, you have to grow your relationships with your customers—and just like any
other relationships, they need to be nurtured. The most effective way to develop, strengthen and maintain
these relationships is through, you guessed it: CRM.

5.2 Why CRM?

CRM is about gaining and retaining customers. By leveraging a CRM system, organizations can document and react to a customer's experience based on information collected over time. Examples of the types of information that can be tracked in a CRM system include (but are not limited to) the following:

- A customer's contact information (business and personal)
- Recent customer activity (visits to your website or calls)
- Customer support issues or cases and the status of their resolutions
- Commitments that have been made to the customer
- Status of current customer orders
- Any other personal information about the customer that can strengthen your relationship (social media interactions or in-person relationship-building meetings)

This data empowers everyone in the organization with the ability to view a unique profile of every customer so that internal teams can collaborate on catering to that customer's specific needs. More than anything, customers want to feel valued and appreciated by the company in which they invest time and money. To a customer in need of support, a company that has no prior information about a customer, continuously transfers a customer to different departments, or makes the customer repeat information conveys the following message: "We don't care about you." On the other hand, if your company has information readily available, the customer is able to see the value you place on maintaining relationships.
Consider the kind of service the favorite airline would provide. For example, when you call that airline, perhaps the phone system recognizes your phone number and welcomes you by name. From there, the system might let you choose to use their automated system or simply say, "operator," to be connected to an agent immediately. "en, that agent will address you by name and already knows all your preferences, upcoming might information, or issues you may be having. By knowing you, the airline is providing a reason for you to continue doing business with them. The lesson here? Taking the time to empower your employees with tools to better know your customer can make all the difference in whether or not you gain a new customer or retain an existing customer. Customers who

feel valued are happy customers and happy customers mean repeat business—not to mention, improved bottom lines

5.3 Advantages of CRM

CRM allows you to gather and manage all your valuable customer data in a centralized location. There are many benefits to implementing a CRM system, but the top six things CRM can do for you are:

5.3.1 Creating A Standardized Process

Each of your company's departments has a unique process—not only how they work individually, but how they work together. For example, think about the various stages in a sales cycle versus how your marketing department creates campaigns targeted to prospects. Because each department relies so heavily upon each other for success, it's important to have a defined process for how your departments function individually and how they interact with one other.

A CRM system gives you the tools to manage measure and improve your processes. Creating workflow rules, for example, ensures that your sales reps follow specific stages throughout the sales cycle. A CRM system also allows you to automate the processes you have in place, from the sales stages your sales reps go through, to managing approvals, to logging all communication between reps and customers. As a result, not only are departments working smarter on their own, but departments are working smarter together.

5.3.2 No More Weekly Status Reports

One of the immediate and most visible benefits of a CRM system is the elimination of the weekly, manual status report. Salespeople who track all their opportunities in a CRM system no longer have to manually create a spreadsheet and send it as a status report to their manager at the end of the week. With a CRM system, salespeople can track their opportunities in one place, and their managers won't have to stress about compiling and organizing data from multiple documents. The more data documents you have, the more likely you are to misplace or lose that information.

A CRM system can automatically run a status report and email it to your sales manager. Management similarly has access to all the sales data online and can run its own reports without even having to wait for status updates. Minimizing the lag time between your salespeople and their managers allows your company to make the most of its efforts. Time is money, so why waste it when you could be capitalizing on your opportunities?

While a CRM does not do away with status updates, your employees no longer have to spend hours pulling all the information together. "e time your company saves eliminating disorganized reports can instead be focused on your customers. "e bottom line is that a CRM system provides better organization and better insight into the overall performance of your company.

5.3.3 Automate Your Unique Sales Process

One of the biggest objections salespeople have to adopting CRM is that they already have too many processes in place. However, any good CRM system should be flexible enough to allow sales people to seamlessly integrate their existing processes into the CRM system without additional burden.

A CRM system will automate the sales team's manual and repetitive steps, giving them more time to sell and focus on turning leads into customers. Simply put, a CRM system is positive extensions to the processes you already have in place that lets your team reach its full potential.

5.3.4 Improve Collaboration

Communication is key for each department to work efficiently with one another. Lack of collaboration on a departmental and organizational level can lead to confusion, longer sales cycles and incorrect information.

Remember that while you're tracking various documents, past or concurrent sales opportunities and other forms of data in CRM, you're collaborating with your colleagues to ensure a successful process. It is likely that you're not the only person who needs to view all of this necessary information about any given customer case.

A CRM application gives you visibility across departments, can help you track your marketing e$orts all the way through closing a deal, and can even manage post-sales support. When using CRM, your employees can more easily share information with each other, which may result in a faster sales cycle and increased revenues.

5.3.5 Greater Visibility

Without a CRM system, it is hard to have detailed sales numbers and compare them with your company's past performance. Spreadsheets only tell a small part of the story, so trying to correlate marketing activities to sales performance is even more difficult.
A CRM system should come standard with reporting capabilities. "is allows you to slice and dice historical and current customer, sales, marketing, and support information any way you want. With this detailed information, your company can determine what practices are successful and which ones need improvement.

5.3.6 A Single Place To Keep All Your Customer Data

Many of us already keep our customer contacts in some sort of system, all the way from business cards to notebooks; Post-it Notes to Excel spreadsheets; email to contact databases; and in some cases, even our memory. With these systems, there are several pitfalls. What if you lose your computer? What if your top salesperson leaves the company with his little black book? What if you forget the customer information that is so vital to your company's success?
A CRM system allows you to store your information in a third-party system. This means that if you were to lose your computer or your top sales person was to leave the company, you would not lose your information.
The information would remain in the on-site server or cloud services provided by the CRM vendor. These services mean that you can breathe easier knowing your information is always accessible when you need it.

5.4. Types of CRM

CRM can be subdivided into three segments:

5.4.1 Operational CRM

Operational CRM is responsible for automating business processes that are related to customers like marketing and sales etc. It is beneficial for any company/firm in three major areas:

5.4.1.1 Sales Force Automation (SFA)

SFA is responsible for automating all sales related processes. Its basic purpose is to improve the productivity of sales department that in turns improve company's sales process.

5.4.1.2 Customer Service and Support (CSS)

CSS is responsible for automating process related to different services like product complaints, service requests and product returns etc.

5.4.1.3 Enterprise Marketing Automation (EMA)

EMA is responsible for automation of marketing related processes. Its key role is to improve efficiency for marketing department that in turns improves company's marketing processes.

5.4.2 Analytical CRM

Analytical CRM is responsible for analyzing customers' behavior in terms of sales, marketing or any other service provided. It utilizes data warehouse to extract appropriate data regarding different customers.

5.4.3 Communication/Collaborative CRM

Communication/Collaborative CRM as the name implies, is responsible for efficient collaboration/association with the customers through e-mails, fax, phone, SMS or face to face communication.

Organizations intending to improve their customer relations, surely implement CRM for their business processes. CRM helps to gain and retain customers and provide services to them efficiently.

6. Sales Force Automation (SFA)

Sales Force Automation (SFA) is used to automate sales and sales force management functions. Sales Force Automation is a subset of customer relationship management (CRM); however, CRM does not necessarily imply automation of sales tasks.

Sales Force Automation automates the business tasks of sales, including order processing, contact management, information sharing, inventory monitoring and control, order tracking, customer management, sales forecast analysis and employee performance evaluation.

Sales Force Automation tracks customer interactions, analyzes sales forecasts and automates business tasks, such as inventory control and order processing. It also supports lead generation, contact, scheduling, performance tracking and other functions for sales and staff. Sales Force Automation functions are normally integrated with base systems that provide order, product, inventory status and other information and may be included as part of a larger CRM system.

Sales Force Automation is used primarily by sales management to monitor the performance of the sales team and individual sales representatives to boost sales. Management can quickly figure out which leads are worth pursuing, when they might close, can see and manage the sales pipeline months into the future and can separate sales performers from the un-performers in your sales force.

6.1 SFA vs. ERP

Sales Force Automation is a natural progression of Enterprise Resource Planning (ERP) software. ERP vendors have already "extended" ERP by front-ending their application suites with Sales Force Automation functionality and back-ending them with CRM applications. Sales Force Automation and CRM are both "front-office" systems, not like "back-office" functions, such as accounting. Since front-office systems influence ERP decision-making, financial system managers must understand how Sales Force Automation fits into the big picture. And as front- and back-office systems have become more integrated, Sales Force Automation has become an integral part of ERP systems.

Sales Force Automation's functionality includes integration with your current databases. Information, records and other applications can be shared with accounting, for example, and perform calculations. Sales Force Automation can go from interacting with accounts payable and receivable to Word, PIMs, and your e-mail system.

6.2 Components of SFA?

Sales Force Automation applications increase the productivity and profitability of a sales team, because they offer incredibly detailed information covering every aspect of the extended sales tree: from prospects and pipeline to opportunities and territories. This is why a subset of Sales Force Automation, **Knowledge Management**, plays such an important role in the effectiveness of a sales force. The sales force must be kept informed of any news that has a bearing on their customers. Whether it is internal or external knowledge about products, promotional campaigns, acquisitions, the stock market, or events, it must be sent to the sales team immediately. Such news can be attached to

the Sales Force Automation application as Word documents. Excel spreadsheets, customer data, and jpegs too. An email newsletter can be developed and sent to the sales team with this or other information.

Sales Force Automation includes a **contact management system** which tracks all contact that has been made with a given customer, the purpose of the contact, and any follow up that may be needed. This ensures that sales efforts are not duplicated, reducing the risk of irritating customers. \

SFA also includes a **sales lead tracking system**, which lists potential customers through paid phone lists, or customers of related products. Other elements of an SFA system can include sales forecasting, order management and product knowledge. More developed SFA systems have features where customers can actually model the product to meet their needs through online product building systems. This is becoming more and more popular in the automobile industry, where patrons can customize various features such as color and interior features such as leather vs. upholstered seats.

An integral part of any SFA system is companywide integration among different departments. If SFA systems aren't adopted and properly integrated to all departments, there might be a lack of communication which could result in different departments contacting the same customer for the same purpose. In order to mitigate this risk, SFA must be fully integrated in all departments that deal with customer service management.

Making a dynamic sales force links strategy and operational actions that can take place within a department, the SFA relies on objectives, plans, budget, and control indicators under specific conditions. In order to perform the objectives correctly, specific procedures must be implemented:

6.3 Advantages of Sale Force Automation

Sales force automation systems can also create competitive advantage:

As mentioned above, productivity can increase. Sales staff can use their time more efficiently and effectively. The sales manager can become more efficient and effective (see above). This increased productivity can create a competitive advantage in three ways: it can reduce costs, it can increase sales revenue, and it can increase market share.

Field sales staff can send their information more often. Typically information can be sent to management after each sales call, rather than daily or weekly. This provides management with current information, which they can use while it is more valuable. Management response time can be greatly reduced. The company can become more alert and agile.

These systems could increase customer satisfaction if they are used with wisdom. If the information obtained and analyzed with the system is used to create a product that matches or exceeds customer expectations, and the sales staff use the system to service customers more expertly and diligently, then customers should be more satisfied with the company. This can provide a competitive advantage because customer satisfaction leads to increased customer loyalty, reduced customer acquisition costs, reduced price elasticity of demand, and increased profit margins.

6.3.1 Managing Sales Territory

Tracking sales territory and lead routing are the bulwarks on which to build efficiency into a sales organization. Instead of using the conventional spread sheet and obsolete software it makes more sense to use a good CRM lead management to allow you to better manage leads as well as prospects from the time of initial capture till the sale is closed. CRM solutions can do this with higher efficiency and greater integrity.

- Automation of lead processing and better management of sales territory eliminates drilling for individual records and helps to save time and money as well as energy.
- Leads can be assigned on the basis of proper business rules which you have already set. This will eliminate conflict over ownership of sales territory and leads.
- Instantaneous email notifications can help the sales rep to follow up with their customers quickly and in doing so will improve service quality and ensure higher number of closed deals.

6.3.2 Managing opportunity and tracking competitors

For a company to achieve success it must manage and also take advantage of every sales opportunity that comes its way. CRM solutions can provide the company with a number of benefits including:

- Taking advantage of greater number of sales opportunities and maximizing Return on Investment by showing your company every opportunity and not having to rely solely on aggregate lists.
- Tracking competitors helps you learn which deals have been lost and which were won. This kind of intelligence will help in educating the sales force.
- Sales reps can find out about discounts and pricing rules that are specific to customers.
- Better response to a sales enquiry and better chance of driving return sales and making customers stay loyal to you.
- Keep track of progress of each customer transaction from time of first contact to the time the sales is closed.

6.3.3 Forecasting

A good CRM solution can also give your sales team more teeth by providing them with tools to help make more accurate forecasts. This allows the sales force to make:

- Calculation based forecasts based on an opportunity or quote or on existing orders.
- Override forecasting is possible where the sales force can make their own predictions.
- Booking as well as recurring revenue forecasting.

Forecasting allows the sales force to make their sales much more predictable. All that is required is to fine tune the forecasting methods to ensure that these are more accurate and relevant.

6.3.4 Managing Orders

Managing orders with the help of a CRM solution can help in streamlining the entire fulfillment procedure and it will also cut down on paperwork which in turn will give the sales force more time in which to concentrate on selling. At the same time, it also helps the customer receive their order in a

timely manner which then boosts customer satisfaction and makes them more loyal to you over the long term.

6.4 Disadvantages

The major disadvantages in Sales Force Management Systems are:

- Difficulty in adopting the system
- Too much of time spent on Data Entry
- Losing personal touch in the process of automation
- Laborious process of continuous maintenance, information updating, information cleansing and system upgradations
- Cost involved in Sales Force Automation Systems and Maintenance
- Difficulty in integration with other management information systems

6.5 Choosing Sale Force Automation

A good CRM solution must be built around the customer and the orders and must take into account:

- Reports
- Dashboards
- Customer intelligence

A good CRM solution will also allow the sales force to work their deals via a pipeline right up to the time that the sale is affected. This means that you can also get to view booked orders in the forecast and this will improve reliability and predictability as well as accuracy. The sales force will also be in a better position to turn an estimate into an order and all this can be done with a single click of the mouse button without involving any great amount of paperwork.

A good order management system will give your organization a means to access similar and latest order information. A representative from the support department will get to see the status of an order and the sales reps will know when it is time to give a follow-up call. Customers on the other hand will get to check the status of their order in a real time environment via your website or through your Customer Centre.

Outsourcing IT

1. Introduction:

Information technology (IT) outsourcing has grown in popularity as an efficient, cost-effective, and expert solution designed to meet the demands of systems implementation, maintenance, security, and operations. Access to skilled personnel, advanced technology infrastructures, flexibility, and cost savings are the driving forces behind IT outsourcing. The benefits of IT outsourcing are accompanied by the need to manage the complexities, risk, and challenges that come with it. Internal auditors, therefore, can help organizations with a comprehensive review of its outsourcing operations, identify risks, provide recommendations to better manage the risks, and also include evaluation of the outsourcing activity's compliance with applicable laws and regulations. This guide is not intended to represent all considerations that may be necessary, but a recommended set of items that should be addressed. All decisions related to IT outsourcing should be thoroughly evaluated by each organization.

Key questions to ask during audits of IT outsourcing activities include:

- Are internal auditors appropriately involved during key stages of the outsourcing lifecycle?
- Do internal auditors have sufficient outsourcing knowledge and experience to provide the right input?
- Do internal auditors understand the roles and expectations of stakeholders within the context of the organization's outsourcing initiative?
- If IT audit plans are outsourced, are created plans based on a complete, top-down, and risk-based scope of work?
- Are internal auditors able to present outsourcing recommendations in a way that managers understand to facilitate their implementation?
- Are internal auditors able to communicate outsourced IT audit findings in a way that is understood and taken seriously by the organization's board of directors?

In this chapter we discuss key considerations of the internal audit function within the context of IT outsourcing and discuss information on the types of IT outsourcing activities that may be considered, the IT outsourcing lifecycle, and how outsourcing activities should be managed by implementing well-defined plans that are supported by a companywide risk, control, compliance, and governance framework.

Key issues include:

- How do you choose the right IT outsourcing vendor? The selection of the vendor will directly determine the success of the outsourcing arrangement. This guide will provide key considerations for vendor selection.

- What are the best ways to draft and manage outsourcing contract agreements? The concept of IT outsourcing is fairly mature, thus lending itself to well-established contracting practices. This guide explores key contract components and structure.

- What practices need to be followed to ensure internal operations are transitioned as best as possible to the outsourcing party? Transition management can be a difficult process and needs precise planning and execution to succeed. This guide provides information on the transition process to help organizations have a smooth migration.
- How can organizations mitigate outsourcing risks? The impact of IT outsourcing on the organization can be dramatic. When business-critical functions are outsourced, they can have a significant impact on the organization's internal controls. This guide discusses main outsourcing risks and related recommendations.

- Which is the most effective framework for establishing outsourcing controls? When IT functions are outsourced, a number of critical controls shift to the vendor organization, both operationally and physically. However, the ultimate responsibility for achieving control objectives rests with the client. This guide discusses the frameworks available to help organizations design internal controls to better manage outsourcing activities effectively.

1.1 Need of IT Outsourcing Guidance for Internal Auditors

Although IT outsourcing is an established practice and some large organizations are already experiencing the many benefits it has to offer, IT outsourcing is still evolving. However, before hiring an IT service provider, management is faced with some critical questions that must be answered to achieve its business objectives.

Further we discuss some of the pros and cons of IT outsourcing, which, in turn, will enable organizations to make better outsourcing decisions. It is important that internal auditors understand the outsourcing expectations of stakeholders regarding the outsourced activity and align their audit objectives to those of the organization. In the context of outsourced IT operations, evaluating the effectiveness of the organization's internal risk and controls framework and the chosen service provider is critical to mitigate internal control risks during the pre-transition stage and throughout the lifespan of the outsourcing agreement.

Another key issue is the internal auditor's role in ensuring adherence to the various security and compliance standards and to what extent they can rely on the work done by independent service auditors and other specialists. In essence, this guide will provide a roadmap to navigate through the complex fabric that is IT outsourcing and will point to some emerging trends in the area.

1.2 Definition of IT Outsourcing

During the past 15 years, outsourcing has moved from an imaginative, innovative, and high-risk attempt at reducing costs to a tried and tested strategic collaboration that helps organizations derives business value. A big contributor to this change has been the success of IT outsourcing. However, one of the key challenges for organizations is their ability to balance the benefits derived from outsourcing, such as reduction in operational costs, while maintaining a healthy risk appetite.

IT outsourcing is often defined as the use of service providers or vendors to create, maintain, or reengineer a company's IT architecture and systems. Although this definition is deceptively simple, it encompasses a wide range of outsourcing activities.
Over the years, IT outsourcing has evolved significantly in terms of its format and objectives. IT outsourcing has evolved from the outsourcing of low-end, non-core, labor intensive activities for cost reduction to the offshoring of functions such as:

- Network and IT infrastructure management.
- Application development and maintenance.
- Data center management.
- Systems integration.
- Research and development (R&D).
- Product development.
- Security management.

Other outsourced services include Web site hosting, development, and maintenance, as well as Internet security and monitoring services.

Two of the biggest contributors to the success of IT outsourcing have been the use of specialized IT skills across the globe and improvements in the technology sector that have resulted in the creation of faster, cheaper, and more effective systems and services. Countries such as India, China, and the Philippines have witnessed the emergence of large-scale, specialized vendors who have invested countless resources in the development of world-class IT infrastructures and processes. These vendors have evolved to support world-class, next-generation, end-to-end products at a lower cost and faster time.

A key driver of IT outsourcing has been the heterogeneity of IT services, platforms, and programs used by many large companies today. In many of these companies, chief information officers (CIOs) are no longer leading the IT service function. Instead, they are being asked to perform more strategic functions, such as improving service and efficiency levels, reducing costs, and adding significant business value. As a result, IT outsourcing is being used to:

- Reduce internal IT workload. This enables companies to focus on critical activities, such as IT strategy development and alignment of IT goals with business strategies.
- Achieve significant improvements in process efficiency levels. Outsourcing by definition includes process reengineering, thus resulting in a more efficient and proactive IT function.
- Provide a bandwidth of IT skills that otherwise may not be easy to retain within the organization. As a result, the vendor provides a range of IT competencies and skills that can be leveraged as the backbone of the IT function.

IT outsourcing's compelling business case as a strategic collaboration process that is capable of delivering substantial benefits and reducing long-term costs has made it a popular business. Unfortunately, anticipated cost savings sometimes leads to outsourcing contracts that are initiated for the wrong reasons or with inadequate planning. Outsourcing requires establishing and maintaining a partnership in which the vendor is an integral member of the CIO's team and the organization. Such relationships build long-term confidence and trust, remain focused on the company's objectives, and create the win-win scenarios necessary to make working relationships more productive.

The risks and impacts can have a material, strategic effect on the organization. Although processes in key areas may have been outsourced, the organization may still be vulnerable to IT risks. Thus, internal auditors can help management understand and better manage these outsourcing risks. Table 1 on the following page contains a list of common outsourcing risks and their potential impacts throughout the outsourcing lifecycle.

To establish the foundation for IT outsourcing success in terms of IT spending and performance optimization, the organization's management and internal control and operations functions must be coordinated. Components such as IT governance, IT investment portfolio management, and contract management are best addressed at the global headquarters. Other components such as cultural and communications management, local IT vendor selection, monitoring of vendor performance, and local regulatory and tax issues are best managed onsite at the local office. Regardless of where each function is managed, all of these elements must be in place and well-coordinated to ensure the project's success. In essence, the strategic outsourcing of non-core IT-assisted business functions can enable organizations to focus less on day-to-day technology management and more on its core competencies and activities. However, effective IT outsourcing requires an effectively managed collaboration with the IT service provider. This is essential to help the organization achieve benefits including:

- Reduced costs.

- Increased productivity.
- Improved customer and vendor relationships.
- Enhanced technology use.
- Increased controls.
- Proper business continuity.
- Competitive advantage.
- A renewed focus on innovation and excellence.

Internal auditors can help management oversee outsourcing activities by playing a proactive role in performance and compliance monitoring and by identifying areas of improvement and recommendations that can help vendors manage IT outsourcing activities.

Risks	Impact
Strategy: Outsourcing strategy is not aligned with corporate objectives.	• The decision to outsource is the wrong one. • The contract is not set up and managed in line with corporate objectives.
Feasibility: Assumptions (e.g., payback period, customer and supply-chain impacts, and cost savings) are wrong as the result of inadequate due diligence from suppliers and the organization's failure to assess relevant risks.	• The potential for outsourcing is not explored in detail, resulting in the lack of fully derived benefits. • The contract is awarded to an inappropriate supplier. • Supplier issues are not managed efficiently and effectively because they were not anticipated properly.
Transaction: Procurement policies are not met; proper service-level agreements are not implemented; operational, human resources (HR), and regulatory implications are not considered; and contingency arrangements are not planned.	• Absence of a well-drafted agreement could lead to a situation in which the client might be unable to fall back on a legally binding document to ensure compliance by the vendor to intended contractual terms. • Potential breaches of regulatory compliance exist that lead to financial penalties and negative repercussions on the company's brand.
Transition: There is a lack of formal transition planning, failure to plan for retention of appropriate skills, and an ineffective escalation and resolution of operational IT issues.	• There is a loss of key resources during the transition period. • Operational difficulties are present. • There is a loss of customer confidence in the outsource service.
Optimization and Transformation: The outsourcing contract is not managed effectively. Therefore, outsourcing benefits and efficiencies are not realized.	• The return on investment is not what was expected or is minimal compared to the outsourcing costs. • The organization provides services that fall below established expectation levels. • There is a rise in unplanned costs
Termination and Renegotiation: There is an inadequate termination of outsourcing processes.	• The company is unable to take over the outsourced activity at a later date or to terminate or renegotiate the contract.

Table 1: Examples of IT Outsourcing Risks and Impact

2. Types of IT Outsourcing

IT outsourcing has changed over the years. From traditional outsourced services, such as application development and IT help desk activities, to high-end services, such as product development, specialized R&D, and distributed computer support, companies continued to outsource IT services as the technology market kept maturing. The most regularly outsourced IT services today include:

- Application management.
- Infrastructure management.
- Help desk services.
- Independent testing and validation services.
- Data center management.
- Systems integration.
- R&D services.
- Managed security services.

Please note that service providers and clients may use different names for the types of outsourcing activities mentioned above. Clients also may outsource one or more of the above services to one or more service providers.

2.1 APPLICATION MANAGEMENT

Application management can be in the form of application development, custom software development, software maintenance, and production support.

2.1.1 Application Development

Development of software applications or specific functionalities or modules within an application should be outsourced to third-party software development firms that have the technical expertise and knowledge to develop applications based on the specifications provided by the client. Typically, such services start with the client's request for a technical or functional specification (e.g., requests for increased system functionality, new modules, structure or workflow activities, or system capacity work), system requirement specifications (SRSs), and functional requirement specifications (FRSs). However, in some cases the service provider may need to conduct a study of the business processes and user requirements, prepare the FRSs, and validate requirements with the client.

Coding should take place after the software development lifecycle (SDLC) methodology is created as part of the service provider's quality process. In certain arrangements, SDLC steps may be specified, monitored, and managed directly by the client. The contract or work statement should be defined clearly from the beginning, as well as the final stages of the development phase for which the service provider is responsible. In most cases, the SDLC process ends with the successful completion of the client's user acceptance testing (UAT), however, the service provider may only be responsible until the unit testing is complete. The system, integration, and user testing phases are essential elements that ensure the system satisfies the client's requirements. Testing can be conducted by the client team or jointly by the client and service provider. In either case, any problems or issues noted in the testing phase are referred back to the service provider for correction Following are key aspects to consider during audits of SDLC activities:

1. The client and service provider need to agree on all SDLC activities, milestones, and deliverables. Service provider controls help to ensure that the development follows the guidelines defined by the client and service provider.
2. The client needs to sign off on technical and functional specification documents prior to the application's development. Alternatively, business requirements need to be received from

users based on the functional specifications approved by the service provider and the client's project manager.
3. Software programming should follow a defined coding standard.
4. Independent reviews need to be designed at each stage of the SDLC process, and the review process needs to be documented.
5. Test plans, test cases, and test results must be documented and shared with the client, as well as specified in the contract.
6. Logs need to document problems noted during the unit or integration testing phase, as well as issues notified by the client after the user testing phase. Logs can be used as evidence when evaluating all defects or bugs.
7. Access control and segregation should be maintained during the development, testing, and migration of codes or programs as defined by the client's security standards.
8. Intellectual property rights are defined.
9. Access to source code in the event of financial insolvency of the outsourcer is specified.

2.1.2 Custom Software Development

The purpose of custom software is to develop applications that meet specific user requirements or provide industry specific solutions. Clients usually want a specific solution that meets a specific need or requirement. This can range from a simple standalone application to an integrated enterprise system that processes transactions from varied business cycles across the organization and updates the central database. Although audits of custom software applications are similar to those of standard development processes, the following distinct activities should be considered during internal audits of the SDLC process of custom applications:

1. Clients must sign off on all business requirement specification (BRS) documents (i.e., documents that state the functional and technical specifications of the proposed solution). Otherwise, the application may not meet the customer's needs. Therefore, users need to be satisfied with and sign off on the proposed design.
2. Risk assessments and impact analyses need to evaluate the proposed solution and its capacity to meet established requirements.

2.1.3 Software Maintenance

The custom software development recommendations should be implemented during the maintenance of existing applications and during any application upgrades whether these consist of minor changes, such as creation of new fields or reports, or major changes, such as the creation of a new module. In addition to the factors listed above, internal auditors should look at the following items during the software maintenance phase:

1. The turnaround time (TAT) defined by the client for all maintenance activities.
2. The time needed to complete the system's maintenance as recorded and monitored by the client.
3. Service provider controls are in place and adhere to the TATs. This is a crucial service-level expectation because failure to establish appropriate service provider controls could lead to a maintenance problem.
4. Integration and regression testing are completed successfully for the new module or functionality, while problems are rectified to ensure the seamless integration of existing applications.

2.1.4 Production Support

Production support activities fix errors and interruptions in functioning systems (i.e., applications, mainframes, and databases) that are in production. The service provider needs to investigate the reasons for the error and interruption and fix the problem quickly. The turnaround time should be

faster than that of a maintenance service because the affected systems are live and require a quick recovery so that the organization can resume regular operations.

Key audit considerations include identifying whether:

1. Service-level expectations such as expected TATs and the quality of the service provided are defined by the client in the contract. The TAT should relate to a response (e.g., the time taken to respond to the reported problem ticket) and resolution (e.g., the time taken to resolve the reported error or issue after it is logged in by the user or the time taken to submit a problem response).
2. A trail is maintained for each response and resolution. Also, auditors need to ensure there is adequate tracking and monitoring of SLA compliance by the client. Specifically, internal auditors should look at the efficiency of the monitoring process and verify that the system's performance is measured.

2.2 INFRASTRUCTURE MANAGEMENT

Services to manage and maintain the IT infrastructure can be classified as infrastructure management. These services include managing and maintaining infrastructure performance, troubleshooting errors, maintaining databases, and backing up and restoring services. More recent and value added services under this category are the monitoring of IT infrastructure activities, performing of downtime analyses, and reporting of critical system failures and their management implications.

Key audit considerations include determining whether:

1. Requests for outsourced maintenance, production support, and infrastructure management services are formally sent to the service provider. Although a workflow-based system where job tickets issued by the client to the service provider is the most effective way to send a service request, e-mails also can be used as an alternative. Verbal requests should be noted as a procedural or control weakness.
2. Approval from the client for implementation is noted in the same job ticket or separately through a written message.
3. Service-level expectations (i.e., TATs and expected quality of the resolution) are defined by the client in the contract.
4. TATs are measured and monitored adequately to ensure the availability of the infrastructure's backbone.

2.3 HELP DESK SERVICES

Any of the maintenance services, such as troubleshooting problems, production support, and infrastructure management, can be categorized as a help desk service. Under this arrangement, the service provider's personnel support the client through various IT problems either onsite (i.e., at the client's premises) or offsite (i.e., from the service provider's premises). TATs (i.e., responses and resolutions) are then defined for each level of service.

Critical compliance with service levels consist of meeting defined TATs and the quality of the service provided. In addition, the evaluation process needs to include an evaluation of procedures that measure and compare actual performance to the expected service-level parameters. Finally, performance results should be used as one of the core criteria for ongoing vendor evaluation. Audit reviews need to determine whether periodic status reports were submitted to the client and issues and improvement action items were documented.

2.4 INDEPENDENT TESTING AND VALIDATION

Many organizations outsource the testing and validation of software developed in house or by a third party. Specialized testing of the developed system is required to monitor the system's performance and identify and correct any programming errors or problems. During the testing and validation phase, internal auditors should review that:

1. Testing parameters (i.e., the system or application to be tested; actual test parameters; and the test's duration, level, and location) were defined by the client.
2. Test specifications developed by the service provider are based on the client's requirements and are signed off on by the client.
3. Test parameters include:
    - A validation of the system's design to determine whether user requirements are outlined in the system's function specification document.
    - The system is designed with adequate load balancing capability (i.e., the system can handle the required number of simultaneous user transactions).
    - User inputs are accepted correctly, transactions are processed completely, and the desired output is obtained.
    - Application security parameters are built in to prevent common or known vulnerabilities specific to the product or platform.
4. Test cases designed to evaluate the parameters defined in point (b) above are validated by the client. Such cases also should be maintained as evidence and for future testing and reference.
5. Test results are maintained.
6. Errors, outages, and glitches (e.g., incorrect output and incomplete updates) are identified and reported in the test report.

2.5 DATA CENTER MANAGEMENT

As more IT industry sectors, vendors, and service providers came into the market, there was a shift in the outsourcing mindset. The objective of outsourcing changed from simple cost savings to providing higher levels of operational efficiency, specialized products, and dynamic growth. Vendors started offering specialized services that could be leveraged across multiple clients, regardless of the industry sector. One such example is the use of data center operations. Outsourcing of data center operations originated from the need of organizations to decrease information management costs. As a result, data centers today typically provide the following services:

- Hardware, software, and operating system planning, specification, procurement, installation, configuration, maintenance, upgrades, and management.
- Continuous monitoring of the server's performance and operational status.
- Server capacity management, including capacity planning, load balancing, tuning, and reconfiguration.
- Server application software installation and upgrades that meet release procedures agreed by the client and service provider.
- Ongoing installation and management of hardware and software.
- Security administration and data backup to ensure the security and integrity of systems and applications.
- Recovery of server systems in the event of a disaster that follows implemented TATs. During reviews of outsourced data services, auditors need to determine whether:
    i. The service provider has adequate capacity (i.e., infrastructure, financial, and technical capacity) to host outsourced services.
    ii. The service provider has segregated physically each client's data and systems to ensure their confidentiality and integrity.

iii. The service provider has adequate back up capacity to ensure the client's infrastructure and network availability.

2.6 SYSTEM INTEGRATION

In a decentralized environment, various functions are organized through disparate systems and applications that do not talk to each other. The risks of having a decentralized environment include the lack of seamless system and application updates, un-reconciled account balances, and erroneous reporting or management of information systems.

System integration services involve the development of scripts, modules, tools, or programs to integrate multiple applications and systems. This enables existing applications to communicate with one another in a seamless fashion, resulting in the presence of one consolidated system. A key limitation of systems integration is its dependency on the accuracy of existing data.

When reviewing system integration services, auditors need to determine whether:

1. Client internal assessments certify that the proposed system meets scalability, interoperability, security, and reliability requirements. Evaluation parameters should consider system interdependence, infrastructure load balancing capability, capacity planning for added infrastructure, and functional design.
2. Tools used for integration are tested separately for applicability and effectiveness.
3. Output reviews generated from the integrated system compare with desired outcomes and validate the integration's accuracy and completeness.
4. Test result reviews validate the integration's completeness and accuracy.
5. Back out procedures and conditions are defined adequately for system and integration failures.

2.7 R&D SERVICES

To stay tuned to existing market needs while continuing to build and maintain their directories and databases, many companies outsource the research and development of different technologies, solutions, processes, and systems. Outsourced research work also includes the use of third-party vendors to perform market analyses that identify the trends and responsiveness of key industry sectors for certain products.

Audits of R&D activities need to determine whether:

1. R&D outsourced activities are classified by their necessary solutions, technologies, or specific work areas.
2. A task plan was created that identifies the sources, strategies, and types of research to be performed.
3. A database or data repository is maintained that stores information collected from various sources by category or the type of task identified. Information also needs to be collated and properly fed into the database or data repository.

2.8 MANAGED SECURITY SERVICES

Recently, many organizations started outsourcing their security services. This outsourcing area also is known as managed security services (MSS) due to the activity's management of an organization's third-party security requirements. Other terms used to identify this function include Internet security services, security outsourcing, intelligence services, security consulting services, network security services, security management services, security assessment services, security consulting, and IT security services.

MSS is defined as the service that oversees an organization's security over its entire IT infrastructure, data assets, and user management activities. Depending on the client's needs, contract terms may include the use of end-to-end security architecture design and support (e.g., design consultation, implementation, security administration, and technical support) or include the management of specific security functions on a particular system (e.g., firewall monitoring, data transmission, content filtering, virus protection, and intrusion detection and response, and network vulnerability assessments).

Due to the growth of information security requirements, more organizations across the world are making security a top business priority.

To help organizations better manage their outsourced MSS, auditors need to examine the following:

1. Assessments of companywide security requirements. These requirements need to be based on the organization's type of work, country of operation, applicable security regulations, infrastructure set up, and user requirements (e.g., the system's level of access or system availability). The assessments should be conducted at least once per calendar year to validate the applicability and adequacy of established security requirements.
2. The outsourced function. The outsourced MSS needs to be commensurate to the assessment above.
3. The prototype design. This design needs to be validated before implementation and should be based on identified security requirements.
4. Post-implementation and MSS monitoring reports. These reports need to be presented to the user management team and include reports on vulnerability assessments, intrusion detection logs, and virus alerts.
5. Root-cause analyses of the reported vulnerabilities or incidents.
6. Designed mitigation procedures. These procedures should not be compromised at any point and ensure the security, confidentiality, and availability of data assets and systems.

Based on the types of activities described above, audit reviews need to further determine whether:

- The client follows a defined process to ascertain the access rights required by the service provider in the client systems.
- Access given to the service provider team is commensurate to the type of services rendered.
- Access is granted and revoked on a timely basis and is determined by the addition or removal of service provider staff, or by the expiration of time-based services.
- Periodic reviews of access rights take place to make sure rights established are valid based on the system's user requirements and lead to the removal of redundant access rights.
- The outsourcing team has adequate skills and expertise to determine the cause of errors and formulate plans to correct them.

3. Key Outsourcing Control Considerations – Client Operations

A successful outsourcing initiative requires careful consideration of several aspects before the partnership is initiated and throughout its lifecycle. Each successful initiative begins with careful consideration of the business case, which specifies the investment schedule and the expected business benefits in terms of cost reduction and maximized work efficiency over a three- to five-year period. Thus, the business case helps to establish the expected payback period. A well-constructed business case also indicates how identified benefits are to be accomplished through a careful

alignment of vendor selection, an established transition and process improvement approach, and the use of risk and security solutions.

The figure below depicts a typical outsourcing value chain. Some of the aspects are discussed in detail in the following paragraphs.

3.1 Governance Outsourcing Framework

When undertaking an IT outsourcing initiative, governance is arguably an area that organizations underestimate most frequently in terms of time and investment and the structural architecture necessary to manage accountability. Companies that commit to an IT outsourcing partnership without a strong governance capability do not have the means to properly manage the outsourced activity. A robust governance framework requires skill and expertise so that the organization can deliver the strategic, operational, and project management guidance necessary for the outsourcing activity to be effective. Because the outsourcing activity spreads across two separate organizations, the need for a clear governance structure is critical when specifying the processes, roles, responsibilities, and incentives that will form the outsourcing arrangement.

As a result, the governance structure should help the organization meet the following objectives:

- Align every IT outsourcing contract with the organization's key business objectives and the needs of primary stakeholders.
- Set up a monitoring mechanism to ensure the IT services outsourced are performed according to the client's specifications.
- Manage changes in IT projects and services across complex portfolios.
- Establish direct and visible accountability for IT performance.
- Define specific ownership of key contract terms.
- Define well-integrated IT management processes for the client and service provider.

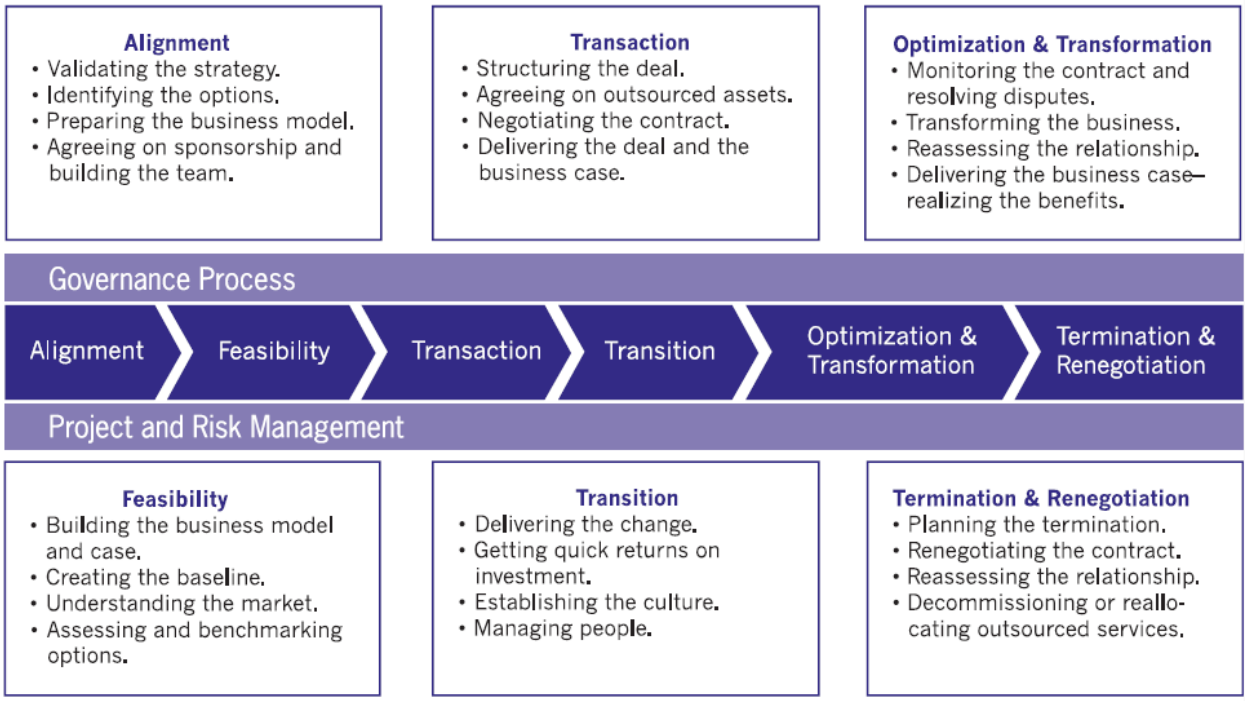


Figure 1: Typical outsourcing value chain.

Audits of governance effectiveness should evaluate risks in the client organization with regards to the objectives outlined above. Key questions auditors need to ask include:

- How transparent is the governance process?
- Do formal relationship management processes address outsourcing conflicts and build effective working relationships between contracting parties?
- Are roles, responsibilities, and delegation of authority activities defined clearly between contracting parties?
- Are communication channels established clearly?

3.2 Alignment and Feasibility

The alignment and feasibility phase deals with the formalization of the IT outsourcing strategy. During this phase, the client should prepare a business case that is based on various IT outsourcing models and an assessment of outsourcing options that is based on research and benchmarking. The outsourcing strategy chosen needs to detail the portfolio of services that will be assigned to one service provider, or to multiple service providers, and the location of these services (i.e., onsite or offsite).

The different outsourcing models usually include build-operate-transfer activities, joint ventures with service providers, or a combination of both. Key audit considerations include:

- Is the client's IT outsourcing strategy aligned with the company's overall business strategy?
- Did the client properly consider all financial, operational, and legal considerations before embarking on the IT outsourcing partnership?
- Are outsourcing assumptions validated by research or data?

3.3 Transaction

3.3.1 Vendor Selection

Vendor selection requires a comprehensive evaluation of the service provider's technical competencies and constraints and is based on the organization's outsourcing service needs. Although there is no right or wrong approach, organizations should follow the steps below as part of any vendor selection program.

Step 1: Plan and Prepare

- Establish a formal project management process that clarifies the roles and responsibilities of all the internal staff involved in the outsourcing partnership. The process also needs to be based on the type of services being outsourced and should define how authority is to be delegated.
- Create a core team to evaluate vendors and participate in negotiations. According to industry best practices, team members should represent different company segments, including IT, finance, legal, and HR, as well as management from affected business units. The CIO typically leads this team.
- Identify the roles and responsibilities of team members throughout the lifecycle of the IT outsourcing initiative.
- Detail the scope of work (i.e., application, infrastructure, and type of service) that is expected to be outsourced. This includes the creation of a milestone-based plan that discusses how and when the organization should increase or extend the scope of outsourced work.
- Create a list of parameters to be considered for vendor selection that is in line with the organization's key outsourcing requirements. Parameter considerations could include the use of global delivery centers, necessary language skills, and minimum level of IT outsourcing

experience in specific kinds of environments. List attributes may come from multiple formal and informal sources, such as referrals, market knowledge, competitor insight, and independent consultant recommendations.
- Understand legal outsourcing requirements, including compliance with different country-specific regulations, such as open market restrictions and open tendering.

Step 2: Gather Vendor-specific Data

After plans and preparations are under way, the team needs to assess the vendor's capability and operations. Depending on the criticality, value, timeliness, and scope of the contract, the assessment should be conducted through a formal request for proposal (RFP) process or by holding informal discussions with identified vendors.

Key actions to be completed when gathering vendor-specific information include:
- Gathering specific details, such as the vendor's size, stability, experience, location, infrastructure, level of process quality, and skill sets.
- Incorporating clear specification requirements into a document called the "statement of requirement" that highlights the scope of services to be outsourced, the contract's duration, expected control requirements and compliance, service-level requirements for all key processes and services, and the client's capacity requirements. The statement of requirement needs to be completed as part of the RFP process.
- Developing an exhaustive list of vendor information requirements with values attached to each parameter that can be used during the final selection round. Parameters to be used can include the vendor's:
  - Background and statement of experience.
  - Management and project management employee information. This is especially relevant for organizations that pay close attention to the vendor's technical skills.
  - Operation and risk management frameworks, including any relevant certifications, methodologies, and business continuity measures; compliance with intellectual property rights; data and sub-contracting security measures; and legal and regulatory compliance activities.
  - Project-specific approach and methodology, including the allocation of resources.
  - Client references including, information on transitioning success.

The service provider's ability to manage the transition of client services is an essential aspect that needs to be evaluated during the vendor selection stage.

Transition parameters encompass critical assessments of the robustness of the vendor's transitioning methodology for issues that include:
- All phases of the transitioning stage and incorporate best practices such as Six Sigma principles.
- Transitioning details on specific milestones, documentation, technology analysis, capacity planning, and costs.
- Available support to mitigate risk and manage productivity during the transition period.
- Onsite redundancy, reorganization, and retraining.

- Success in previous transitions, including number of transitions and whether they occurred on time and within budget.
- Robustness of support plans, such as risk, contingency, and business continuity plans.
- Quality of the transitioning team, including the team's profile and experience.

Step 3: Conduct Due Diligence

When responses to RFPs have been received, the project team should begin to analyze the submitted information against the pre-defined evaluation framework.

Action items to complete include:

- Client reference checks during the final due diligence stage. The project team must evaluate the vendor's project management competency, success rate, the quality and standard of work, adherence to contract terms, and communication process.
- Country-specific risks and information, including availability of skills, costs, political environment and stability, cultural compatibility, and accessibility.
- Site visits to evaluate the service provider's capabilities, operations, infrastructure, and local culture.

Based on each vendor's response, client reference checks, site visits, and final negotiations typically take place with a final group of two to three service providers.

Step 4: Negotiate and Close

Negotiating and closing the deal are the final steps in the vendor selection process. How to conduct this step is determined largely by the due diligence exercised in the previous steps.

Below is a description of actions organizations can take.

- Simultaneously negotiate with at least two vendors. This enables the company to compare deal prices and legal terms. Large outsourcing contracts could involve negotiations with three to four vendors.
- Involve legal and senior management staff to discuss the contract's terms and conditions. Service providers usually come prepared with a standard contract containing the partnership's terms and conditions. Most organizations discuss the contract with their legal advisors before doing so with the service provider.
- Sign the contract. Most service providers are prepared to modify the contract as needed before signing takes place.

3.3.2 Legal and Contractual Considerations When Contracting With Service Providers

IT outsourcing arrangements involve different levels of complexity, risk, and a range of legal and contractual issues. Special concerns deal with the difficulties of terminating long-term engagements and in defining responsibilities in organizations that have not worked together before, especially in an environment shaped by changing business conditions. Many senior managers will agree that part of the foundation for a successful initiative is based on the legal and contractual due diligence that takes place before the outsourcing engagement is formalized. Therefore, unless managerial outsourcing controls are supported by a well-written contract, management and operational activities may be under-supervised. This increases the likelihood that key processes, quality specifications, service delivery timing, and outcomes will be driven by or depend on the vendor.

Legal and contractual issues that should be addressed when drafting a well-written contract include:

1) Service levels and incentives.

The organization must outline minimum performance benchmarks, standards, and metrics that are most appropriate for the outsourcing objective, such as measures that are directly tied to operational indicators (i.e., service quality, system availability, and response times). If possible, it is important to avoid exclusivity or preferred provider clauses to maintain competitive pressure on the vendor.

2) Vendor personnel.
People represent a core performance driver. The client should be able to approve the selection of key vendor personnel and be in a position to define the criteria used to screen replacements. Because the loss of key personnel can affect the vendor's ability to deliver on contracted obligations, some clients insist on having approval rights over the vendor's retention and compensation strategies. This will maximize the likelihood that personnel critical to solution delivery and knowledge transfer continue to work for the vendor throughout the agreement's duration.

3) Data protection, privacy, and intellectual property.
Risk is always involved when third-party entities are given access to sensitive customer data, privileged business operation details, or intellectual property vulnerable to public or competitor disclosure. Key issues can range from requiring the vendor to maintain specified levels of security through employee awareness training and contractual obligations, such as signing a non-disclosure agreement by service delivery personnel and company indemnification by the vendor for any breaches.

4) Price protections.
Establishing price changes is one of the most important contract areas in IT outsourcing because small differences in price can affect an outsourcer's options, choices, and business objectives. Contracts should cover pricing issues such as changes in service scope, agreed pricing parameters, maintenance of preferred or "most favored customer" pricing, and procedures to accelerate the resolution of pricing disagreements.

5) Third-party assignments.
In situations where the vendor hires a third party (i.e., a sub-service provider) to deliver services, the client needs to include in the contract how service quality will be managed and any client performance risks.

6) Ownership of assets used or created by the IT outsourcing partnership.
IT outsourcing vendors sometimes require use of the organization's resources or assets to meet contractual obligations. Rules and procedures should define and create ownership rights when new value is created from an outsourcing activity. Contract terms should specify any procedures needed to minimize confusion and disagreements that can arise whenever systems, resources, and assets are shared.

7) Conflicts among different legal systems.
Contracts must be based on applicable national and local laws. Outsourcing contracts, especially those defining parameters for offshore initiatives, can become quite complex if different justice systems and legal resolution disputes are not considered at the beginning of the initiative. Key issues in this area include the use of language that clarifies potential ambiguities in contract interpretation and dispute settlements, as well as language that clearly defines procedures and processes for problem identification, discussion, escalation, resolution, and management (e.g., dispute resolution, mediation, and arbitration).

8) Contingency management and change planning.
One of the most important goals of the contract is to protect the client's ability to reshape the outsourcing contract, relationship, or operating framework so the client can adapt to changes in the business environment. Critical to any outsourcing partnership is the flexibility to accommodate unanticipated business changes, such as growth, extraordinary events, mergers, acquisitions, or sales. This flexibility needs to be stated in the contract.

9) Notice of adverse material impacts.

A well-written contract must ensure the client's right to be informed of any event that could affect the vendor's ability to meet its obligations. Receiving timely notice on impending events enables the organization to keep down contingency planning costs while maintaining a high return on investment (ROI) when unforeseen events do occur.

10) Right to audit.
Contracts need to include clauses that provide the client with well-defined rights to audit processes, controls, and results associated with the outsourced activity. This includes the use of Statement of Auditing Standard No. 70 (SAS 70) reports or a similar kind of review, as well as the audit of various regulatory compliance issues such as those associated with the U.S. Sarbanes-Oxley Act of 2002.

11) Termination.
Even IT outsourcing contracts developed under the most auspicious principles of partnership and collaboration should stipulate the conditions leading to termination. These conditions range from termination for a specific reason to termination due to a convenience factor. Contract language should define the client's rights, as well as procedures that must take place for termination and the options to purchase or license assets.

Key internal audit considerations that need to be reviewed in this stage include:

- Determining whether the vendor selection process was conducted in a fair manner.
- Examining the contract's description of aspects the client will be exposed to once the outsourcing partnership begins.
- Identifying whether a checklist exists that consists of the legal and contractual factors agreed on by the client and service provider that help to determine the vendor's compliance with each of these factors.

3.4 Transition Management

Transitioning or migration involves the transfer and ownership of knowledge to an entity with no previous experience with a given system, process, corporate culture, or industry. Although transition plans are the responsibility of the client, they usually are delegated to vendors. Migration activities typically involve two stages, planning and knowledge transfer.

3.4.1 Planning

The planning phase involves the development of a migration strategy. During the planning phase, the organization needs to include the costs and timelines for each significant milestone in the migration plan. As part of the transition strategy, the client and service provider jointly identify the most optimal migration mode (e.g., a complete transfer or all activities or a gradual rollout of functions based on a prioritization scheme). The strategy also needs to assign specific resources and budgets for each step of the migration phase.

3.4.2 Knowledge Transfer

Executing an effective knowledge transfer plan is essential for the long-term success of the outsourcing partnership. This requires that the client and service provider identify and document all the necessary information (e.g., technical, business, process, and background information) so that the transfer process has the least impact possible on the service quality of the outsourced activity.

A high-quality service provider should have a well-established process for ongoing knowledge management that does not disrupt the client's quality of service. Comprehensive and detailed documentation needs to be available so that the company can bring the activity back in-house or

transition to another service provider if necessary. This gives the client greater leverage to ensure services are delivered as stipulated in the contract. In addition, the client needs to have access to the relevant information documented during this phase. As a result, the company needs to perform periodic audits of the knowledge transfer process.

Finally, this stage may involve on-site visits by the service provider's senior project managers. Some organizations also prefer that their staff visit the service provider to set up the outsourcing process. Key personnel may include senior managers or product directors who can organize the outsourcing activity and senior engineers who can train the service provider team. The frequency and duration of visits should decrease as service operations mature and stabilize.

3.5 Change Management

The outsourcing project can disrupt the organization's operations during various stages of the outsourcing initiative. Organizations need to identify, plan for, and manage these disruptions as best as possible to reach their desired outcome.

Transitioning is one stage in which the client and service provider could experience high levels of change. During this stage, the service provider has to ensure it has the necessary experience to deal with any disruptions caused by the transition process.

The client and service provider can manage any changes that occur during the transition phase by:

- Defining key processes and control requirements. These processes and controls should cover security, business continuity planning, disaster recovery, compliance, and data protection activities.
- Identifying plan elements and their corresponding timelines.
- Describing client and service provider responsibilities during the transition phase.
- Establishing service-level requirements for all key processes and services, including service levels at various stages of the transition process.
- Specifying the different technology and connectivity adaptations needed during the transition period.
- Describing robust reporting tools, policies, and procedures to handle interfaces during and after the transitioning of reporting formats (i.e., status reports, key performance indicator (KPI) reports, hierarchy reports, and frequency reports) and escalating mechanisms to be used during the transition phase.

3.5.1 Stabilization and Monitoring

The last stage of the change management process is the stabilization of operations. This refers to the live performance of the outsourced processes under the service provider's controls. During the transition phase, certain outsourced activities may resume their normal operations within a defined timeframe. Any delays should be closely monitored because they can have a negative impact on the realization of outsourcing benefits. This also helps the organization react and respond to any issues in a proactive manner. During the monitoring phase, organizations need to ensure communication takes place between the on-site team and service provider. This is imperative for the partnership's success.

Communication should address:

- Reports on KPIs and other performance measures.
- Analysis of KPI trends and performance.
- Documentation of any performance deviations and their analysis.
- Plans that identify any resolution issues including the timeframe for each resolution.

- Communicate through the appropriate channels. This may include telephone calls, Webex or Internet based meetings, chat sessions, e-mails, and video conferences, or more formal channels, such as weekly and monthly updates or meetings.
- The responsibility of the vendor to upload any software product development information, project related documentation, and work in progress reports to the appropriate intranet site, so that clients can obtain the necessary project status information.

3.5.2 Internal Audit Considerations

Key questions internal auditors need to consider at this stage include:

- Does a formal transition management strategy exist?
- How effective is the knowledge transfer strategy in terms of its design and operating effectiveness?
- Has attrition affected the transfer phase or affected the operation of outsourced activities?
- How effective is the communication and review process?
- How effective is the change management process in terms of its design and operating effectiveness?
- Is there a process in place to ensure only approved changes are carried out by the service provider?
- Are review samples documented appropriately to demonstrate that all stages of the change management process were followed?
- Is there a formal management process? If so, did it monitor the project's progress and its benefits at the specified timelines?

3.6 Transformation and Optimization

A well-defined, yet flexible, contract is often the key to a successful IT outsourcing relationship. This contract defines the boundaries, rights, liability, and expectations of the outsourcing vendor and client and is often the only mechanism for regulating the outsourcing relationship. IT outsourcing contracts must be crafted to provide clients with tools that:

- Retain leverage and manage change.
- Manage in-scope and new services.
- Monitor and manage service quality.
- Deliver promised cost savings.
- Provide competitive price protection.
- Manage potential liability and risks without affecting the project's price.

One of the most critical outsourcing contract elements is the definition of service-level targets, which must be achieved as part of the outsourced service's delivery. It is important for the client to have a process in place that addresses how service- level parameters are to be changed, how formal reviews need to address compliance to agreed parameters, and how to evaluate any deviations.

The SLA should describe:

- The service's objectives and scope.
- Performance metrics and corresponding service levels against each metric, including:
    - Volume (i.e., the number of maintenance requests per month and lines of code).
    - Availability (i.e., availability of provided services for a specific period of time).
    - Quality (i.e., the number of production failures per month, number of missed deadlines, and number of deliverables rejected).

  - Responsiveness (i.e., the time needed to implement an enhancement or to resolve production problems).
  - Efficiency (i.e., the number of programs supported per person, rework rates, and client satisfaction surveys).
- Frequency definitions to measure performance (e.g., monthly, quarterly, etc.) and other informal contract performance reviews through regular progress meetings and reports.
- Payments based on SLA performance.
- Definition of clauses that stipulate the availability of the contract's renegotiation for non-achievement of SLAs.

As contract management increases in complexity, the role of contract manager may emerge, especially in organizations with a large number of outsourcing contracts. The contract manager can be an in-house or contracted employee and should work with the client's internal legal department to observe contract formalities. A full-time, experienced contract manager should track communications, as well as review and maintain manual and monitoring operation procedures for compliance with the contract's terms.

3.6.1 Internal Audit Considerations

A key aspect internal auditors need to examine during this stage is the SLA conformance. Auditors also need to evaluate the strength of the client's review process. Key questions to ask include:

- Are key areas defined in the SLA aligned with the benefits or process improvement parameters identified in the business case?
- Are periodic reports from the service provider based on the key areas agreed in the SLA?
- Are service provider reports independently validated for accuracy and completeness?
- Is the review of service provider reports effective? Was adequate action taken when deviations occurred?
- Are SLA term changes approved appropriately?

3.7 Project and Risk Management

Given today's regulatory landscape, compliance risk management is emerging as a top priority for many organizations, especially those in the financial services and healthcare industries. To establish an effective compliance risk management process, clients and service providers need to:

- Determine the types of compliance risks the client organization is exposed to based on the type of outsourced service.
- Identify processes that can have a material impact on compliance risk.
- Establish manual and automated process controls to ensure that all risks are mitigated.
- Define SLAs with regard to potential compliance risk exposures, which processes will be reviewed, audit responsibilities and frequency, and correctional steps.
- Implement and monitor a robust governance model for overseeing regulatory compliance.

Outsourcing risks range from incorrect vendor selection, poor contract management, transition problems, risks of organizational backlash, and security vulnerabilities. As outsourcing activities mature, organizations become more aware of and are more sensitive to these risks. The challenge, then, is to identify hidden risks and define the appropriate strategies needed to minimize their impacts. For example, a possible control risk could arise after a service provider is made responsible for the outsourced activity's success or failure. As a result, the client organization must interact closely with the outsourced teams to track, guide, and plan outsourced operations based on organizational goals and expectations.

Project tracking that is based on predefined metrics, such as quality, timelines, and resource planning enables the seamless integration of client and service provider teams, cultures, and knowledge. This may be done through:

- Status reports and meetings. Many organizations maintain joint risk logs. This helps to ensure a better transparency and visibility of issues and action plans, thereby facilitating proactive decision making.
- Reports of project milestones.
- Daily communication among team members on operational issues through telephone calls, chat sessions, video conferencing, or e-mail.
- Delivery of interim artifacts, such as program designs, codes, documentation, and test plans.
- Project portals where all documents related to the project are stored. The project portals should be accessible only to team members assigned to the project.
- Service staff traveling onsite or development team members from client organizations visiting the vendor for reviews.

Sustaining and enhancing software development quality is one of the most important objectives of organizations that outsource IT operations. To ensure quality, outsourcing processes need to be well planned, managed, and monitored. Organizations also need to establish a special quality assurance (QA) team to ensure process quality, especially in organizations engaging in specialized processes such as software development.

In addition, contracts can be used to establish risk management expectations. Although a contract is a useful statement of the parties' responsibilities, it should not be a substitute for a strong governance model to monitor, communicate, and resolve vendor disputes. Client and vendor relationships are mutually beneficial when contract terms are clear and the parties have provided a robust mechanism to manage daily activities and a procedure for dispute resolution.

3.7.1 Internal Audit Considerations

During their evaluations, internal auditors need to determine whether the service provider is in compliance with the outsourcing agreement and whether their activities are robust, transparent, and unbiased.

To this end, internal auditors need to identify:

- The presence of a well-structured business case that clearly outlines desired business outcomes.
- A well-documented statement of requirements.
- A planned, structured, and transparent vendor short list, evaluation, and selection process, with predefined criteria and objective rankings.
- A formal migration strategy and knowledge transfer process.
- Mechanisms for the arrangement's stabilization and monitoring through defined KPIs and pre-agreed communication and status monitoring channels.
- Well-defined SLAs and comprehensive flexible contracts.
- Established processes for change and risk management, as well as process quality assurance.
- Well-documented frameworks for managing business continuity processes, as well as information, network, physical, and personnel security.

For the internal auditor to determine that the outsourced activity is executed in a well-planned and controlled environment, each of the above considerations must be met fully in terms of adequate documentation and evidence of operations.

4. Service Provider Operations

As part of the IT outsourcing venture, some of the client's controls may be transferred to the service provider totally or in part. In such cases, the audit's scope extends beyond the client's operations. This section discusses key control considerations that need to be evaluated to identify the effectiveness of the service provider's internal controls.

4.1 Control Environment

An important control consideration is the evaluation of the service provider's IT control environment. The control environment sets the organization's tone, impacts user behavior, and is the foundation for other internal control components. For instance, certain aspects of a service provider's control environment may affect the services provided to the client. Control environment prerequisites include the prevalence of strong documented policies, procedures, and guidelines, as well as a clear definition of the roles and responsibilities of information systems personnel.

Another objective of this evaluation is to gain reasonable assurance regarding the strength of the service provider's IT governance structure. As a result, this evaluation should analyze the service provider's:

- Team structure and composition (i.e., does the team have the skills, competency, and experience necessary for the services provided?).
- Delivery of services according to agreed SLAs.
- Security controls for all customer information.
- Endpoint security for all networks, extranets, and intranets, as well as security controls for all Internet activities and services, Internet service providers, and Web site activities directly linked to data centers.
- Feedback received from customers.
- Customer data backups.
- Disaster recovery and business continuity plans.
- System uptime and performance.

Service organizations also are required to perform periodic risk assessments that take into consideration various factors affecting the services provided to the client. Periodic, structured risk assessments of the IT infrastructure, systems, and applications are a good indicator of the service provider's attitudes toward the IT environment from a control perspective.
Factors that should be considered while performing these risk assessments include:

- Changes in the operating environment.
- New or revamped information systems.
- Growth, including but not limited to, organizational growth and growth in services provided to clients.
- New technology.
- New business models, products, or activities.
- New accounting pronouncements.
- New personnel.

4.1.1 Information Security Policies and Procedures

Service providers normally have documented policies and procedures related to various information security (IS) functions, including:

- IT administration (i.e., IT management, records management, document management, device naming conventions, transmission control protocol/Internet protocol implementation standards, network infrastructure standards, computer and Internet use policies, and e-mail policies).

- IT asset management (i.e., IT asset standards, IT vendor selection, asset assessment, asset installation satisfaction, and media storage procedures).
- IT training and support (i.e., system administration, IT support center, IT server and network support, IT troubleshooting, and IT user and staff training plans).

Organizations may have a separate IS team that has a clearly defined organizational structure and documented roles and responsibilities. The IS team establishes detailed security policies and procedures on IT security and disaster recovery activities, such as:

- IT threat and risk assessment.
- IT security planning.
- Media storage.
- IT disaster recovery.
- Presence of computer malware.
- User access control.
- E-mail security.
- Remote access controls.
- Network security management.
- Password policies.
- Data classification guidelines.
- IT security audits.
- IT incident handling.

Service organizations should ensure that policies and procedures are formulated, developed, and documented for all key IT activities. The policies and procedures developed should be communicated clearly to the appropriate process owners and business teams. A process should exist to review the policies and procedures periodically, while required modifications should be performed based on existing business conditions.

A policies and procedures compliance process is also vital. Once outsourcing procedures are formalized, they should be reviewed periodically to ensure their compliance with established policies. A defined process also needs to be implemented to address noncompliance with policies and procedures and remediate identified issues.

4.2 Security Considerations

To obtain the desired ROI, security risks need to be managed effectively. The primary types of security risks that need to be addressed in any IT outsourcing context include:

- Information protection.
- Network security.
- Physical security.
- Personnel security.
- Logical access controls to applications.

4.2.1 Data Protection Risks

Data is an essential business component and should be treated as an important corporate asset. Information is not restricted to papers and documents; it includes data residing in services and application software, employee information, research records, price lists, and contracts. To protect data assets, companies need to:

- Identify which security risks may affect the organization.

- Establish policies and procedures addressing key areas, such as acceptable use, information classification, third-party access, data transmission and remote data access, and password and user access policies.
- Support policies with necessary guidelines, procedures, and templates.
- Obtain senior management's commitment to the information security initiative. This demonstrates the presence of a strong operational team that understands the threats posed by security issues and the organization's ability to monitor and deal with security problems and vulnerabilities.

4.2.2 Network Security

Organizations can take a number of measures to secure their networks, the place were information is stored and transmitted.

To ensure the security of their networks, the following security elements need to be included as part of the organization's data protection efforts:

- Proper documentation, design, and implementation of the network.
- Configuration of firewalls to deny access to unauthorized traffic.
- Physical and logical separation of the client network from the service provider's local area network.
- Installation of antivirus software on all servers and systems.
- Use of regular virus signature updates.
- Measures to prevent unauthorized access to the company's network or data.
- Secure connection and encryption.
- Security of network software and operating systems.
- Policies for access control and authentication.
- Remote diagnostic port protection.
- Network connection control.
- Network routing control.
- Intrusion detection systems.

4.2.3 Physical Security and Environmental Controls

Physical security refers to the means used to secure an object or location, such as company's building, work areas, systems and devices used, and documents. Depending on the type of activity outsourced, client organizations need to ensure that the service provider's documents, systems, and infrastructure are secured properly.

Many organizations are demanding higher security levels in outsourcing facilities, especially when the activity outsourced is critical for the success of the organization's operations. Key security measures include:

- Around-the-clock use of trained security guards provided by professional security agencies and
- use of physical entry controls such as:
  - Access authorization and identification mechanisms (e.g., identification cards and swipe cards).
  - Access restriction on a need-to basis to areas dedicated for client processing and service delivery. These areas should have their own dedicated workstations, computer network, and infrastructure (e.g., phone lines, file and print servers, and printers).
  - An entry and exit tracking system to ensure visitors are issued appropriate entry badges and

  - their belongings are checked.
  - Additional restricted access to server rooms and data centers.
  - A dedicated floor space monitored by closed circuit television 24 hours a day, seven days a
  - week to prevent and monitor suspicious activity on critical locations (e.g., the data center,
  - network room, building entrance, and production floors).
  - Restricted movement of media (e.g., compact disks, floppy disks, and flash drives) and papers
  - controlled though physical inspection and authorization at gate passes.
- Use of shredders located at various locations to dispose of data and documents. This helps to ensure that confidential documents and data are not stored or carried outside the building.
- Storing backup media containing critical data at on- and off-site fireproof cabinets.
- Use of fire suppression systems such as smoke detectors.

4.2.4 Personnel Security

Personnel security refers to companywide procedures to ensure that all personnel who have access to sensitive information or a particular location have the required authority and clearances. The evaluation of personnel security should consist of the following:

- Detailed background checks of potential employees that identify previous employer reference checks, criminal record checks, and educational qualifications. The background check also could verify other aspects, such as a person's social background. Although most organizations prefer to conduct employee reference checks in-house, they may be outsourced to a specialized local agency.
- Mandatory confidentiality agreements for all employees. Most outsourcing partners have a standard non-disclosure agreement, which states the penalties for a breach of contract, including termination of services.
- Use of printers and photocopies on a need-to basis. Many service providers secure their photocopiers with staff and keep track of the employees, number of pages, and information printed or photocopied.
- Logs of each employee's work and access.
- Internet access controls. Some service providers have cybercafé facilities outside of the client processing area for employee use.
- Tools that scan all internal e-mails, forbid access to external e-mails, and scan e-mails for critical words band size limits.
- Password management, including confidentiality, regular change schedules, and single user sign-on where multiple accesses are required.
- Automatic terminal identification, terminal logon procedures, and user identification and authentication.

4.2.5 Logical Access

Restricted access and application password controls are critical to prevent unauthorized access in locations where sensitive data is processed or stored. This may require restricting access to specific data elements based on a person's role and responsibilities, preventing access to other confidential data, or requiring the restriction of particular transactions to certain users.
Key logical access considerations include:

- Verifying that security requirements specified in the contract are implemented, such as regulatory specifications.
- Reporting security breaches regularly, such as invalid
- access attempts.

- Using independent tests to check that security levels cannot be breached, such as conducting penetration tests of IT networks and Web sites.
- Restricting access to sensitive data or particular transactions to key staff.
- Auditing the technology and processes used to prevent unauthorized access to the client's records in situations where a supplier provides IT operation services to several customers. This may require specialist assistance.

In addition, particular focus should be placed on logical access controls over critical applications, databases, and operating systems, such as:

- A formal process for account management (i.e., user and administrative controls for critical systems, such as operating systems, application systems, and databases).
- Audit trails to track the creation of user accounts and access authorization for user accounts.
- A formal review process for periodic user accounts on operating systems, databases, and applications that support a critical function to ensure logical access is provided to authorized users only.

Finally, the following security requirements should be considered when using Web services:

- Firewall protection with access rules and restrictions for internal network and applications accessible via the Internet by an Internet browser.
- Anti-spam software to prevent unauthorized Internet e-mail addresses or software downloads to the network.
- Installation of virus protection software to protect against and detect viruses on e-mails or Internet downloads.
- Regular updates of virus software to ensure that new viruses are detected.
- Authentication controls for applications residing outside the network (e.g., use of smart cards and digital certificates).

4.2.6 Business Continuity

Business continuity management (BCM) is an enterprise wide, risk-based approach to develop proactive measures that ensure the continuing availability of business support systems and mitigate disruptions risks. As stated in figure 2, BCM helps organizations to maximize the availability, reliability, and recoverability of business systems through the effective management of people, processes, and technology. It also enhances an organization's ability to recover from a disaster, minimize losses, and have the best level of preparedness to deal with business interruptions and restore operations. In the absence of such a plan, the organization could face long term revenue losses and loose customer confidence.

Business continuity policies and guidelines are a critical component of the outsourcing contract and should be detailed clearly in SLAs addressing:

- BCM mechanisms.
- Response times based on the outsourced process type.
- Types of audits required, as well as the audit's location, frequency, cost, person in-charge of the audit, and the information that will be shared between the parties.
- Penalties due to the inability of the service provider to resume business operations during and after a disaster as defined in the SLA.

Business Continuity Management			
Issues Addressed	Availability	Reliability	Recoverability
Solution	Enterprise High Availability	Service Level Management	Enterprise High Availability
Objective	Achieve and maintain the chosen availability level of the enterprise's IT infrastructure.	Effectively manage and control the IT infra-structure to improve the overall operational reliability.	Provides an effective plan to minimize down-time of key processes in the event of a major disruption.
Emphasis	Technology	Processes	People
Focus	Proactive and Preventive		Response and Recovery

Figure 2: Description of the BCM process.

The scope and operational aspects of the BCM typically differ based on the organization's risk appetite, the criticality of activities and projects outsourced, and the overall dependence of operations on IT. Business continuity plans should identify:

- Potential sources of disruption.
- Critical processes and applications and acceptable levels of downtime via a business impact analysis.
- Acceptable response and recovery times.
- BCM mechanisms including:
  - Storage mechanisms and locations (e.g., tapes, off-site servers, and redundant arrays of independent disks).
  - Frequency of data backups.
  - Creation of alternate sites.
  - Infrastructure availability of equipment and networks.
  - Access points into several telecommunication carriers.
- Personnel responsibilities based on the extent of the disruption and the nature of the process impacted.
- The individuals accountable for the business continuity process.
- Business continuity plan tests and maintenance activities.

As a result, the following aspects become critical during the BCM process:

- Reviews of the service provider's BCM and disaster recovery plans to ensure that disruptions in their premises, staff, or systems will not affect the client's systems adversely.
- Reviews of the service provider's BCM and disaster recovery test plans and test reports.
- An understanding of the role BCM and disaster recovery testing plays in ensuring the service provider's plans are effective for the client systems.

4.3 SDLC Controls

SDLC controls should be applied to all new applications developed or acquired by the service provider or during major enhancements and maintenance activities to existing applications. To reduce acquisition and implementation risks, organizations may use a specific system development or quality assurance process or methodology that is supported by standard software tools and IT architecture components. This process provides a structure for identifying:

- Automated solutions.
- System design and implementation activities.
- Documentation requirements.
- Testing, approvals, project management and oversight requirements.
- Project risk assessments.

Ideally, service organizations are expected to maintain evidence that demonstrates the procedures below are followed for all new developments and acquisitions, as they may have a direct impact on the delivery of client services.

Key methodology components include:

- IT project definition and project management.
- Systems analysis.
- Software design, programming, documentation, testing, releases, and updates.
- Infrastructure planning.
- Design changes during development.
- IS clearance procedures.
- Code reviews.
- Data migration procedures.
- End-user training.

4.4 Change Management Control Considerations

Application maintenance addresses ongoing change management activities and the implementation of new software releases. Appropriate system controls should exist to make sure all changes are made properly. Controls may involve the use of authorizations of change requests, reviews, approvals, documentation, and testing, as well as assessments of changes on other IT components and implementation protocols. The change management process also needs to be integrated with other IT processes, including incident management, problem management, availability management, and infrastructure change control. From an audit standpoint, the service provider must be able to provide evidence that changes are based on authorized requests only.

4.5 Human Resource Policies and Procedures

Successful outsourcing depends on technology and people. Therefore, an evaluation of the vendor's HR policies and procedures is important in the successful implementation and operating effectiveness of designed controls.

Key review considerations in this area include:

- Adoption and promotion of the company's integrity management culture, including the organization's ethics, business practices, and HR evaluations.
- Reviews of employee incentives to ensure employees are not pressured to use unethical or unfair practices to meet unrealistic performance targets, particularly for short-term results.

- Use of adequate hiring practices, such as specification of job requirements, job posting procedures, handling of employment applications, interviews, background checks, job offers, and new employee orientations.
- Capturing, analyzing, and reviewing employee turnover patterns for potential fraud or collusion.

4.6 Internal Audit Considerations

In the beginning, many organizations were reluctant to outsource their services due to fears of loosing control. Because of this, a strong outsourcing control environment is especially important on the service provider side. The control aspects discussed in this chapter need to be understood and evaluated in all third-party processes based on the kind of services being outsourced and their complexity.

The internal auditor plays a critical role in evaluating the service provider's control environment. As a result, auditors need to assess the strength of the control framework and control activities affecting the outsourced processes, as well as inform management on the effectiveness of outsourcing operations from a compliance and operations standpoint. To do so, auditors should evaluate and test the service provider's policies, procedures, guidelines, risk assessments, and SDLC control monitoring activities, as well as obtain independent information through the established communication channels. Auditors also can rely on the international standards adopted by the service provider for compliance, such as the use of SAS 70 reports, and evaluate the service provider's documentation to identify whether controls were customized to fit the client's unique environment.

5. Applicable Control Frameworks and Guidelines

When outsourcing an IT solution, companies face the risk that sensitive customer data may end up in the service provider's custody. Loss of data confidentiality and integrity, as well as unauthorized use and tampering of customer data, could lead to penalties and reputation loss. Data breaches also could result in security and privacy violations as indicated by regulations such as HIPAA, GLBA, and the EU's Data Protection Act, depending on the company's type of work and country of operations.

Although different frameworks can be adopted to oversee the effectiveness of outsourced activities, the contract remains the most important framework in reviewing a service provider's work and compliance. Below is a description of the main regulations service providers and organizations alike need to keep in mind or comply with throughout the duration of the outsourcing partnership.

a) Control Objectives for Information and Related Technology (CobiT)®

IT Governance Institute (ITGI) CobiT framework lays down a set of control objectives for effective IT governance. CobiT also helps organizations implement the necessary requirements to ensure the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of information.

CobiT IT processes are defined under four domains:

- planning and organization,
- acquisition and implementation,
- delivery and
- support, and monitoring.

Control objectives and processes are defined for each of the four domains, which can be adopted as best practices for designing an effective framework. Specifically, CobiT provides maturity models for

control over IT processes so that management can map its current control maturity levels, where it stands in relation to best-in-class organizations, and where the organization wants to be.

Maturity models describe:

- Critical success factors that define important management-oriented implementation guidelines to achieve control over and within its IT processes.
- Key goal indicators, which define measures that enable management to identify whether an IT process has achieved its business requirements.
- KPIs that serve as lead indicators on how well the IT process is enabling goals to be reached.

b) The UK Office of Government Commerce's (OGC's) IT Infrastructure Library (ITIL)

Another global framework on IT governance and management is ITIL, an IT operations and services best practice framework that helps organizations align their business and IT activities. The OGC developed ITIL in the mid-1980s for companies seeking to manage their IT environments more efficiently. One of the main reasons ITIL is used by many organizations is due to its freedom. ITIL does not mandate organizations to implement all framework specifications.

ITIL's Service Support book helps organizations define their core IT service functions. According to the book, the role of an IT service function is to offer uninterrupted and best possible services to users.

The book also defines five processes:
incident management, problem management, configuration management, change management, and release management, which describe how to manage software, hardware, and HR services efficiently and ensure continued and uninterrupted business activities.

5.3 Internal Audit Considerations

As outsourcing continues to evolve into a more global service delivery model, it is important for internal auditors to keep abreast of the control frameworks used worldwide. This allows auditors to make informed decisions on which frameworks are best suited to meet the needs of client organizations based on their type of work, the activities being outsourced, and the different kinds and levels of risks. Internal auditors also are playing a key role in the recommendation and evaluation of different IT control frameworks and the options available for deployment.

As a result, internal auditors need to assess the efficiency of the certifying organization's review processes and design an audit program that caters to the specific framework under evaluation. Audit results will help client organizations determine how much they can rely on the service provider's activities based on the certification obtained.
Factors that need to be considered when evaluating the effectiveness of the review process and certification include:

1. The reputation and competency of the organization that conducted the review and provided the certification.
2. The review's period of coverage (i.e., the review period should be current and within the client's financial period).
3. The control framework defined (i.e., the control, objectives, and control processes should cover the IT processes and operations outsourced, as well as include the controls desired by the client and mandated by regulatory requirements).
4. Review results (i.e., the efficiency of the control design in meeting the objectives and operating effectiveness of the controls over the period under review). Review results need

to note any exceptions, the risk rating of exceptions based on their impact, management's response, and the time committed by management for implementing remedial measures. For high-risk exceptions, audit reports need to document the remediation measures implemented to ensure program effectiveness.

5.4 Top 10 Questions CAEs Should Ask

1. Are the services outsourced significant to the client?
2. Does the client have a well-defined outsourcing strategy?
3. What is the governance structure relating to outsourced operations? Are roles and responsibilities clearly defined?
4. Was a detailed risk analysis performed at the time of outsourcing, and is a regular risk analysis being done?
5. Do formal contracts or SLAs exist for the outsourced activities?
6. Does the SLA clearly define KPIs for monitoring vendor performance?
7. How is compliance with the contract or SLA monitored?
8. What is the mechanism used to address noncompliance with the SLA?
9. Are the responsibilities of the ownership of data system, communication system, operating system, utility software, and application software clearly defined and agreed upon with the service provider?
10. What is the process for gaining assurance on the operating effectiveness of the internal controls on the service provider's end?

6. Recent Trends and the Future of Outsourcing

Although IT outsourcing is an established management practice, ongoing and rapid industry changes have established the presence of trends. Below are some of the most noteworthy trends in the IT outsourcing arena.

- Application development continues to be one of the most outsourced IT activities followed by application maintenance and support. This trend is expected to continue in the near future. Service providers are continuing to build their skills and capacity in this area and hold high expectations for growth in the managed services category, particularly in the areas of database management and network management.
- Mega deals in excess of US $1 billion represent a significant share of the total outsourcing contract value, which averaged US $25.3 billion per year between 2003 and 2005. However, mega deals are set to decline in the near future and will be replaced by an increase in mid and large deals in the US $100 million to US $999 million range1. This trend is expected to create increased competition in the service provider arena, as both large and mid-size players start to face direct competition from each other.
- Although there has been an increased emphasis on the outsourcing partnership model, contract term lengths are declining. Research indicates that the average length of an IT outsourcing contract declined from 6.2 years to 5.3 years from 2003 through 2005. This is attributed to negative vendor experiences from first-generation outsourcing deals that were implemented in a hurry to bring in tactical cost reductions. The trend is to give organizations flexibility and not lock them into a particular service.
- Cost savings continues to be the key driver for IT outsourcing. However, the importance of superior technical skills to improve quality is rising rapidly. This may be corroborated by a growing number of clients using outsourcing as a way to introduce innovation into their organizations. This change in relative importance may be attributed to increased consensus on real cost savings estimated between 15 and 25 percent. Outsourcing arrangements that have
- focused solely on delivering savings have failed to meet client and service provider expectations.
- Europe will continue to witness significant activity in IT outsourcing and will come close to catching up with the U.S. market share.
- Many companies are relying on pilot projects to ensure a good fit between the client organization and vendor. Pilots allow companies to review the vendor's project management process for efficiency and effectiveness. Specifically, the pilot looks at whether project execution is completed within established guidelines, deliverables are timely, and the vendor has adhered to defined quality standards. Pilot projects serve as an excellent way for organizations to check facts before making a final vendor decision.

They also let companies experience the benefits of outsourcing before jumping into a long-term relationship. Often, companies will conduct a proof of concept with various vendors to compare results and choose the best vendor.

- Multi-sourcing will be one of the most visible trends. As a result, organizations will need to develop the competencies necessary to manage a multi-vendor environment.
- IT service providers will evolve their businesses around distinct models including:
    - The global champion model. Under this model, the service provider can offer multiple service lines and solutions to large organizations.
    - The IT specialist model. Under this model, service providers focus on three to four major IT industry or cross-industry services.

- The ADM factory model. Under this model, service providers can position themselves as low-cost developers of applications and maintenance services.

Service providers will have to bring innovation into their business models by focusing on new service lines, such as infrastructure outsourcing. In addition, service providers will need to increase their knowledge domains and enhance the quality of their business environments by providing better services with better technological solutions.

Managing and auditing IT Projects

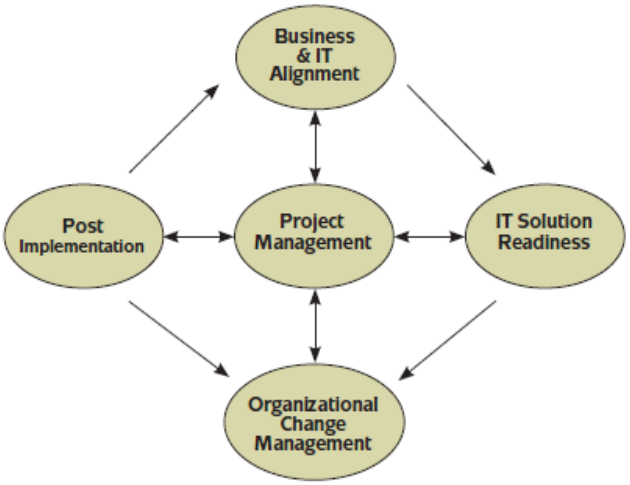
1. Introduction

Organizations invest large amounts of capital to fund the implementation of new information systems, enter new markets, develop new products, and manage alliances and acquisitions. Project teams are often created to manage such efforts. These investments don't just bring about positive change to the organization, but also present a high degree of risk. As a result, the success or failure of these investments can be critical to the strategy of an organization, as well as have an impact on the organization's efficiency and reputation.

Many projects and investments are focused around information technology (IT). In the past, studies indicate that for IT projects in particular, the failure rate can be as high as 50 percent. Project failure often comes down to two key things: too much optimism from a people aspect, or technology failures from a systems perspective. Given the level of risk that projects face, it is essential for the internal audit department to be aware of the projects taking place in the organization and to determine at what stage it should be involved in order to provide guidance on the controls aspect of the project or an independent assessment of the achievement of desired results.

Internal auditing can contribute to the success of IT projects by assessing project-related risks. Auditors can focus on areas such as security and internal controls, and they can play a role in evaluating the overall project management. By helping project teams respond to risks, internal auditing can increase the project's chance of success. Internal auditing can add value through both traditional assurance and consultative engagements.

To be successful , auditors must demonstrate to both senior management and project managers the value that an independent advisor can bring. Senior management can give auditors access to projects, but auditors can be more effective when the project managers buy into their involvement and give them greater access.



The purpose of this chapter is to provide the chief audit executive (CAE) and internal auditors with an overview of techniques for effectively engaging with project teams and project management offices (PMOs) to assess the risks related to IT projects. The field of project management is quite broad, and as such the purpose of this guide is to outline a framework for assessing project-related risks, provide examples of common project management risks, and discuss how the internal audit function can participate actively in the review of projects while maintaining its independence. The IIA's International Standards for the Professional Practice of Internal Auditing provide principle-focused guidance for performing these engagements. Within the context of this chapter we will focus on five key components of IT projects for which we recommend building an audit approach (see Figure 1):

1. Business and IT Alignment
2. Project Management
3. IT Solution Readiness
4. Organizational and Process Change Management
5. Post Implementation

Figure shows that project management is the central concept that links all of these areas. When planning the project audit approach, the auditor should consider all five of these areas to ensure that all major risks are addressed.
This guide is not intended to be a complete project risk assessment or audit guidance; rather it provides an outline of key considerations for auditing IT projects. Auditing projects is an excellent opportunity for internal auditing to provide assurance on strategic risk. A number of studies have shown that internal auditing spends a large amount of time auditing operational risk, but not enough on strategic risk. Project audits can provide an opportunity to expand the risk focus.

2. Introduction

2.1 What Exactly Is an IT Project?

The term *IT Project* is a bit of a misnomer. In reality, most system implementation or maintenance projects are increasingly complex initiatives that involve or impact more than just the IT department and, as such, should be considered as a business project as well as an IT project. In the most general sense, a project is a unique set of activities with a discreet beginning and end, undertaken to achieve a particular purpose within defined constraints of schedule, scope, and resources. It is important to note that this chapter is intended to focus on projects that include a technology-related solution; however the principles are very similar to other types of projects.

IT-related investments have been a major source of expenditure for organizations for many years. They tend to come in waves, and all organizations worldwide respond to them. Large IT projects easily can cost tens of millions of dollars. Major waves of IT system-related projects in the last 15 years include enterprise resource planning (ERP) systems, solving the Year 2000 problem, e-commerce/dot-com solutions, and customer relationship management (CRM) systems. Such projects could include building new infrastructure, new product development (commonly referred to as research and development, or R&D), and the implementation of new business processes or business transformations. In the evaluation of such projects, it is necessary to understand the key risks, and to develop a set of criteria to evaluate the project at various stages.

2.2 Understanding the Impact

Today, determination of a project's success extends beyond traditional on-time, on-budget metrics. Failed or challenged projects can have a significant impact on an organization, depending on the business need behind the project.

A few examples of possible risks include:

- Disruption of service to customers.
- Loss of competitive advantage.
- Fines from failed regulatory compliance.
- Loss of revenue.
- Negative impact on reputation.
- Delays in deploying critical strategic initiatives, products, or processes.
- Loss of expected return-on-investment.
- Loss of critical business and IT personnel.
- Facility closure or damage.
- Loss of shareholders/investors.

Many researchers and consulting firms have performed studies reporting on the fact that IT projects are regularly challenged or fail — they are over budget, behind schedule, do not achieve objectives, or are cancelled. As a result, there is no shortage of ideas, articles, and white papers on the subject.

Regardless of the interpretation of the data, there is overwhelming evidence that projects pose a significant challenge. Ultimately, management is accountable for ensuring that the project and benefit outcomes are achieved.

2.3 Examples of Failed IT Projects

Most large IT project failures will never be publicized because of the negative impact the disclosure would have on an organization's reputation and shareholders. However, the following are some examples of significant failures that have been reported.

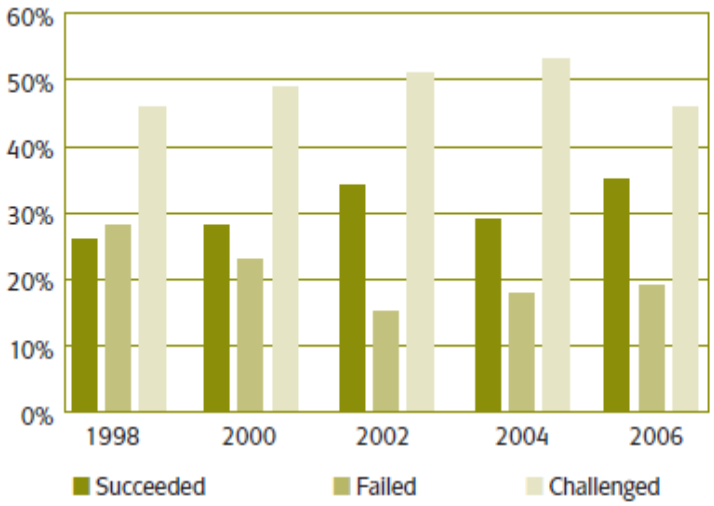
1. In August 2005, *CIO Magazine* reported that a large U.S. government agency had to scrap a US $170 million virtual case file management system development project due to schedule delays, cost overruns, and technical difficulties.

2. In 2004, one of the top telecommunications companies in the world experienced a project failure during a CRM system upgrade. The resulting problems cascaded across the IT environment and led to disruptions in wireless service to customers. The company lost many customers over the incident, and the revenue impact was estimated to be US $100 million. The stock price fell and before it could recover, the company was sold to a competitor for less than half of the original share price.

3. In 1999, one of the largest food manufacturers in the world suffered a significant ERP implementation failure, which resulted in two profit warnings in the last quarter of the year. The event led to significant product distribution problems during the critical holiday sales season. By year end, the stock price was down 27 percent, which was very poor considering a stock market boom was occurring at the time.

2.4 Historical Statistics on IT Project Success and Failure

Statistics around IT project failures have been studied consistently and reported over the last two decades by numerous analysts and consultants, including the Gartner Group, Forrester Group, The Standish Group, and KPMG. There are far too many reports and statistics to discuss here, but the CAE should be aware of the research to understand the inherent risks associated with IT projects. Auditors should investigate statistics and failures that relate to their specific organization and industry. Such statistics can be presented to management when discussing the need for project audits. The following are some examples of relevant research regarding project failures.



	1998	2000	2002	2004	2006
Succeeded	26%	28%	34%	29%	35%
Failed	28%	23%	15%	18%	19%
Challenged	46%	49%	51%	53%	46%

Table 1. CHAOS Research Study

- The 2007 CHAOS Report from The Standish Group7 provides summary results of its research studies from 1998 to 2006. The data shows that project success cannot be taken for granted. As

of 2006, 65 percent of projects either failed or were challenged, meaning that they were unable to meet all or part of their objectives, cost, or schedule goals.

- CA, Inc. sponsored an independent research group in the United Kingdom, Loudhouse, to survey 100 IT directors across the UK and Ireland. The study concluded that poor visibility into IT project status and a lack of management control over projects is costing UK companies a quarter of a billion pounds (US $350 million) each year. A third of all projects implemented each year end up over budget, with the typical over-spend between 10 percent and 20 percent of the original budget. The survey also highlighted the increased complexity of IT projects; it indicated a typical company runs 29 projects at any one time and has an average IT budget of between £1m and £5m8 (US $1.4m and US $7.03m).
- KPMG's Global IT Project Management Survey, released in 2005, found that 49 percent of survey participants had experienced at least one project failure in the previous 12 months. Further, the report revealed that 59 percent of organizations either have no process or only an informal process in place to assess whether or not a project is on track to provide the intended benefit.

These are just a few examples. While it is possible to debate the detailed accuracy of such statistics, the fact remains that the large number of project failures has been reported consistently.

2.5 Top 10 Factors for Project Success

To counter the failures many research groups provide ideas on steps to take to ensure that projects have the best chance for success. The Standish Group provides an annual report based on its research of why projects succeed. The following 10 rules for success come from the latest Standish annual project management report, "The CHAOS Report 2007."

1. **User Involvement**
   - Business and IT users are involved with key consensus-building, decision-making, and information-gathering processes.
2. **Executive Support**
   - Key executives provide alignment with business strategy, as well as financial, emotional, and conflict resolution support.
3. **Clear Business Objectives**
   - Stakeholders understand the core value of the project and how it aligns with business strategy.
4. **Agile Optimization**
   - Project uses iterative development and optimization processes to avoid unnecessary features and ensure critical features are included.
5. **Emotional Maturity**
   - Project manager directs the emotions and actions of project stakeholders and avoids ambition, arrogance, ignorance, abstinence, and fraudulence.
6. **Project Management Expertise**
   - Organization uses project managers who understand the basic skills and practices, such as certified Project Management Professional from the Project Management Institute (PMI) or the like.
7. **Financial Management**
   - Project manager is able to manage financial resources, account for project budget/costs, and demonstrate the value of the project.

8. **Skilled Resources**
   – Skilled project personnel are acquired, managed, retained, and controlled to move forward in the face of turnover and other personnel hurdles.
9. **Formal Methodology**
   – There is a predefined set of process-based techniques that provide a road map on when, how, and what events should occur in what order.
10. **Tools and Infrastructure**
   – The project infrastructure is built and managed with tools that enable management of tasks, resources, requirements, change, risks, vendors, user acceptance, and quality management.

2.6 Purpose and Benefits of Internal Audit Involvement

While all of the success factors outlined above are clearly the role of management, internal auditing can add considerable value by evaluating the effectiveness of risk management over both the IT and organizational aspects of IT-related projects. Internal auditing offers an independent approach to assessing whether an organization or function is achieving its stated objectives. Auditors analyze business processes or activities in a methodical way to highlight issues and recommend corrective actions. Given the IT-related project risks outlined above, internal auditing can bring the value of their experience and methodology to review projects in the early stages to also help increase the likelihood of success. Benefits of internal audit involvement may include:

- Providing independent ongoing advice throughout the project.
- Identifying key risks or issues early, which enables project teams to operate proactively to mitigate risks.

3. Five Key Focus Areas for Project Audits

Research has shown not only what some of the risks are, but also that early intervention is a key to success. As stated in the introduction, this GTAG focuses on five key areas of projects around which we recommend building an audit approach. The following five categories were chosen as the logical areas around which to focus based on a variety of research and the authors' past experience with using various project risk assessment methodologies.

1. Business and IT Alignment
2. Project Management
3. IT Solution Readiness
4. Organizational and Process Change Management
5. Post Implementation

The next sections provide considerations for each of the five key focus areas. (See Appendix F for a suggested list of audit questions and examples of specific risks and controls for each of these focus areas.)

3.1 Business and IT Alignment

Alignment simply means that the vision and objectives of both the business and IT are understood, are in harmony with each other, and that the project is in line with the strategy of the organization. Almost every project consists of interdependence among various levels and functions of an organization. This means that achieving and maintaining alignment is a significant challenge throughout the life of the project! Regular meetings with all stakeholders present and channels for an open flow of communication are critical, as are fully dedicated sponsors who provide the leadership, time, and energy that the project requires. Further to the sponsorship, the project team selection is equally crucial. A project team that is lacking the right experience, skill set, and

willingness to support the project is a prevalent barrier to project success. There are many aspects associated with project alignment, and for many organizations these aspects are incorporated into the business case.

3.3.1 Assessing the Business Case

For any project to get started, management needs information to determine the viability of taking what sounds like a good idea forward. Preparation of the business case is a process that is followed by a dedicated team to provide the information necessary to facilitate a decision regarding whether to proceed with the project. The ultimate decision may be taken by the project steering committee, or may be taken at a higher level in the organization. Indeed, entire audit guides have been written on the subject of reviewing
the business case. Therefore, for the purposes of this GTAG, we will focus on just a few of the common risk areas.
Key components of the business case should include:

- Benefits that are realistic, understood, and measurable.
- Environmental concerns such as the regulatory landscape, architectural compatibility, etc.
- Organizational considerations such as who should be involved from what functions.
- A clearly defined project scope.
- Project deliverables, in terms or process and functionality.
- Necessary resources, both in terms of cost and people.
- Analysis of the risks regarding the viability of partners or vendors.
- Measurement or likelihood of success.

In building the business case, it is essential to establish project sponsorship as well as project impact. At the earliest phase, project sponsors must understand the full impact of the project and to ensure all internal and external stakeholders are considered. The direct stakeholders include internal departments or functions that will use the new system, external customers or suppliers who may interact with it, and anyone else with a vested interest. It is important also to ensure that indirect stakeholders are consulted early, which could include finance, internal audit, IT security, legal, purchasing, or regulatory functions. Feedback should be received from all impacted groups — even those on which the impact may be minimal — to ensure all considerations are taken into account.
The business case should ensure that all available alternatives are considered. Typical factors include building the solution in-house or buying an external package; using internal resources versus outsourcing; and of course considering whether the project is in response to a regulatory requirement, or simply a business efficiency solution. In the analysis of alternatives, a strong business case enables management to make the most informed decision and to understand the trade-offs that must be considered. Lastly, the business case should assess the capacity of the organization to undertake the project, the priority level of the project, and whether the organization has the people with the right skill set to execute it.

3.2 Project Management

Understanding Project Management

As depicted in Figure 1, project management is central to the five focus areas. Project management, like internal auditing, is a profession with its own set of best practices, terminology, and standards. (Due to the wide availability and broad scope of guidance on project management as a profession, the appendices of this GTAG were developed to provide a summary of project management reference material, best practices, and standards.) Auditors should be careful to ensure they fully understand the risks associated with project management. Even an auditor with a strong IT and business background may find many project management best practices unfamiliar. Internal auditors

will have to invest time to study and better understand project management processes and terminology.

The following terminology is fundamental to project management:

- **Project Portfolio** – The collection of projects within an organization. Programs may include a number of projects. In order to plan, scope, and assess projects and programs, the auditors must understand the concepts of project management, project governance, and project management methodology within the context of their business and organization.
- **Project Management** – The discipline of organizing and managing resources (e.g. people and budget) so that the project is completed within defined scope, quality, time, and cost constraints.
- **Project Governance** – The overlap between projects and corporate governance, the governance of project management at the entity level. It ensures the organization undertakes the right projects, controls the project portfolio, establishes priorities, assigns authority to the correct level, and has appropriate decision-making processes in place. Good project management governance ties all of the areas illustrated in Figure 2 (on page 8) together and ensures that they have the support to operate effectively.
- **Project Management Methodologies** – Broad collections of integrated policies, standards, methodologies, life cycles, procedures, tools, techniques, stakeholders, and organizations that are used to guide the planning and execution of a project. The Standish Group points out that the methodology also includes what it calls "the other 90 percent of a project environment" (e.g., emotional attitudes, culture, stakeholder education, and nonprocess/procedure maturity of the organization).

Auditors and Project Management Methodologies

Just like it is true that no two businesses are the same, it is also true that no two project management methodologies are the same. Every organization will use a different combination of methodologies, life cycles, best practices, tools, etc. For instance, large defense contractors may use a complex methodology such as earned value management (EVM) — a project management technique for measuring project progress in an objective way by combining scope, schedule, and cost[12] — in order to support large government contracts, while a small organization may use a simple project management software package or spreadsheet just to track the project tasks and status.

Before performing any project audits, the CAE and the internal audit team should first gain an understanding of the organization's project management methodology — also known as an ecosystem or life cycle. Additionally, they must understand the best practices, risks, and controls associated with both project management and systems development. Failure to understand this relationship could result in an internal auditor not scoping IT project audits to account for the full range of possible risks.

Figure 2 shows the components that might be included in a methodology and where key controls should reside. It also highlights the interdependence between levels and functions that exist, and to what level the audit may need to go to have a complete understanding of the project magnitude. The organization's project management methodology provides the context the auditor needs to perform the audit. The methodology offers a basis for helping the auditor during the planning and execution of audits to identify key project governance groups and key project management control points, and to determine the policies, standards, and best practices against which to audit.

Table 2, Project Methodology Components and Value to Auditor, highlights the major methodology components and their value to the auditor.

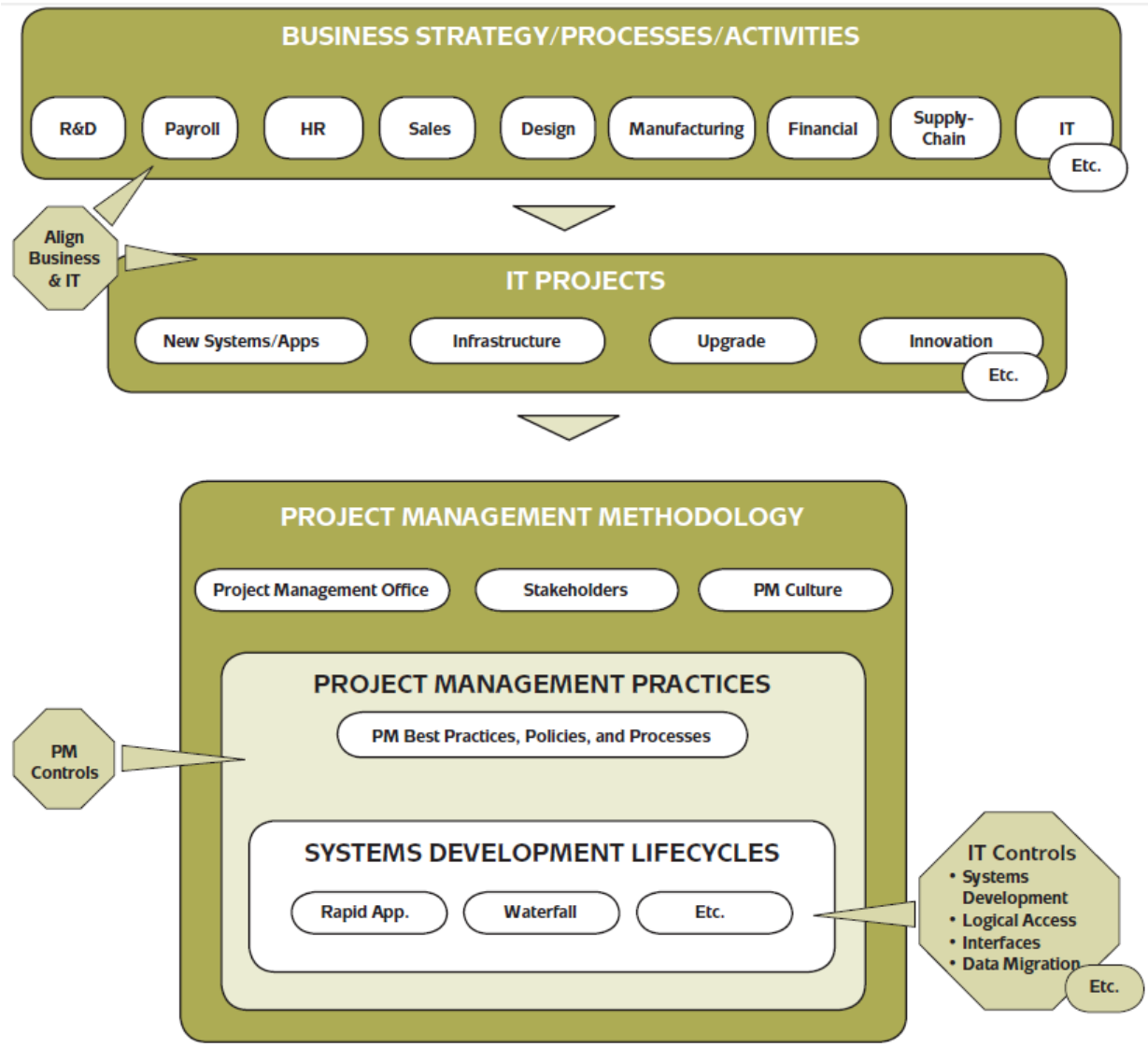


Figure 2. Project Management Methodology.

Methodology Component	Value to Auditors	Examples
Organizational		
Project Stakeholders	Provide auditors with multiple perspectives (business, IT, contractor, etc.) on the risks and issues associated with individual projects.	• Business Owner • IT Owner
Project Management Offices	Provide a centralized location to identify and review all project methodologies and associated deliverable requirements, which aids in annual audit planning and scoping, audit program development, etc.	• Strategic/Global • Single Project • Business Unit
Models and Methods		

Project Portfolio Management	Provides a centralized location to identify and review all projects, which aids in annual audit planning, audit prioritization, etc.	• Strategic/Global • Single Project
Project Management Maturity Models	Provides a "measuring stick" for planning project audits. Auditors can assess project methodologies and processes to identify gaps as a basis for improvement.	• The Portfolio, Program, and Project Management Maturity Model (P3M3) • Organizational Project Management Maturity Model (OPM3)
System Development Maturity Models	Provides a "measuring stick" for scoping and planning project audits. Auditors can assess project methodologies and processes to identify gaps for improvement.	• Capability Maturity Model Integration for Development (CMMI) • The Software Process Improvement and Capability determination (SPICE)
Software Development Life Cycle (SDLC)	Provides a basis for identifying and assessing adherence to system development processes, as well as when to use or not use a particular approach.	• Waterfall • Rapid Application Development (RAD)
Project Management Best Practice Guides	Provides a foundation for developing an audit approach and a basis for assessing organizational and project-level performance.	• Project Management Body of Knowledge (PMBOK) • Projects in Controlled Environments (PRINCE2)
Automated Tools	Enables review of audit schedules, expenditures, resource allocation, issues, etc. If portfolio management tools are used, they enable the auditor to run reports listing all projects in order to risk-prioritize projects based on budgets and schedules, and to use metrics to identify "troubled projects."	• Schedule Management • Resource Management • Issue Tracking

Project Stakeholders

Internal auditors must understand how their organization identifies and includes stakeholders in IT projects. Stakeholders are the collection of people and groups that make the project happen. Projects simply cannot succeed without the proper stakeholders working together in a well-coordinated way. Executive stakeholders must provide strategic guidance, as well as financial, political, and emotional support. Business and IT user stakeholders ensure that the requirements and final product meet the intended business need. The number and types of stakeholders vary by organization and project. (See Appendix B for a list of typical stakeholders.)

Project Management Office (PMO) and the Internal Auditor

If the organization has a PMO, this will be a key starting point for the internal auditor to understand the organization's project management culture, methodologies, standards, and processes. Many organizations implement PMOs to help govern and influence project success across an organization. According to studies by the Project Management Institute, the top reasons for implementing a PMO are to improve project success rates, standardize practices, and lower costs. Although small

organizations can manage projects effectively without a PMO, large organizations with a vast number of projects will find success unlikely without one.

Because of the critical role the PMO can play in a project management methodology, it is essential that the auditor develops and maintains a strong relationship with the PMO. PMOs may play a key role during project audits and may serve as a valuable liaison between internal auditing and project managers. Auditors can play an advisory role to the PMO by sharing their perspective on IT project risk and by setting auditing's expectations for the PMO and individual projects. IT project auditors should seek to understand the following:

- PMO's roles and functions
- Project management methodologies
- IT project cost and schedule performance data and trends
- IT project success/failure rates, statistics, metrics, and lessons learned
- Trends that are driving success or failure across all IT projects

They should also seek to obtain a listing of approved and funded IT projects annually — sorted by budget, risk, or other key factors — and a listing of major milestones and go-live dates for major system implementations.

Project Portfolio Management

Project portfolio management (PPM) refers to the collective management of projects to ensure that well-informed project investment decisions are made. Organizations use PPM to make better IT investment decisions, ensure adequate funding across business requirements, and elevate the role of IT in the organization by showing the value of all IT initiatives and projects. Internal auditors can use PPM to identify high-risk projects and the overall priorities of the organization.

Internal Auditors and Maturity Models

Generally speaking, maturity models exist to help organizations move from less mature processes to more mature processes. They help the organization identify current weaknesses and gaps in capability and identify its current level of maturity and then plot a strategy for improving to the next level of maturity. The general idea is to develop well defined, robust, and repeatable processes. There are specific maturity models for software development and project management. (See Appendix D for a summary of maturity models.)

Auditors can use maturity models as a basis for assessing an organization's project management and/or systems development processes. However, this probably only makes sense if the organization has already chosen a maturity model and is structuring its processes to be aligned with a model. If an organization plans to implement a maturity model for the first time, internal auditing could perform an initial audit against the proposed maturity standard. This would provide a baseline understanding for the organization to begin its use of the maturity model.

Auditors should view the use of maturity models by the organization as a very positive step in terms of improving the organization's IT project management approach. However, there is no requirement for an organization to use a maturity model, and many do not because of the cost and complexity.

Best Practices for IT Project Management

Best practices provide an ideal starting point for auditors to frame their risk assessment and audit approach. Best practices come from both general project management guides as well as those that are specific to IT development. Some widely accepted examples include:

- Project Management Body of Knowledge (PMBOK).[13]
- PRojects IN Controlled Environments (PRINCE2).

- Control Objectives for Information and related Technology (COBIT).[15]
- International Standards Organization (ISO) Standards.[16]

Internal auditors should not expect organizations to fully implement PMBOK, PRINCE2, COBIT, or any other large set of best practices. Rather, they should expect to see that these practices have been customized and integrated into the organization's project management methodology. Appendix E - General Project Management Best Practices gives more details on each of these best practices and frameworks.

Project Management Tools and Automation

Auditors should expect to see any number of automated tools for project management or teamwork being used on projects. Software may by used to manage entire portfolios containing hundreds of projects, and/or individual projects. Auditors may leverage these tools to obtain:

- Information on cost, schedule, and technical problems.
- Insight into project decision-making and issue-tracking.
- Information on resource utilization.

The following are some examples of project areas that may benefit from automation and tools.

Project Management

Schedule management
Cost management
Requirements management
Issue tracking
Resource management
Risk management
Quality management
Team collaboration/knowledge sharing.

Systems Development

Software defect tracking
Software testing
Source code management and version control

3.3 IT Solution Readiness

IT solutions have a natural development life cycle that includes a sequence of phases that must be followed in order to convert a management need into an IT system or application and to maintain the system in a controlled way. Typically, this sequence is referred to as a software life cycle (SLC) or software development life cycle (SDLC). (See Figure 3: Generic Software Development Life Cycle.)
Organizations may use their own software life cycle methodology for custom development or one provided by consultants or vendors for use with their products. SDLCs may vary by the type of technology being developed. They may be customized to meet any of the following development or implementation scenarios:

- Custom development using internal resources
- Custom development using fully or partly outsourced resources located on site or offsite (locally or in an offshore location)
- Vendor software packages implemented as-is with no customization
- Vendor software packages customized to meet specific requirements

Well-known types of SDLC models include Waterfall and Rapid Application Development.
Regardless, the internal auditors should expect to see some type of development life cycle and will need to determine whether it is appropriately followed. They'll then use the phases in the life cycle to determine when to perform the project audit and what controls to test.
The implementation phase of the project is often thought of as simply when the new system gets "turned on" in production; however, there are a series of critical steps and decisions that take place during the course of the project. Many project failures have been attributed to a lack of interim checkpoints, which should be established as part of the project

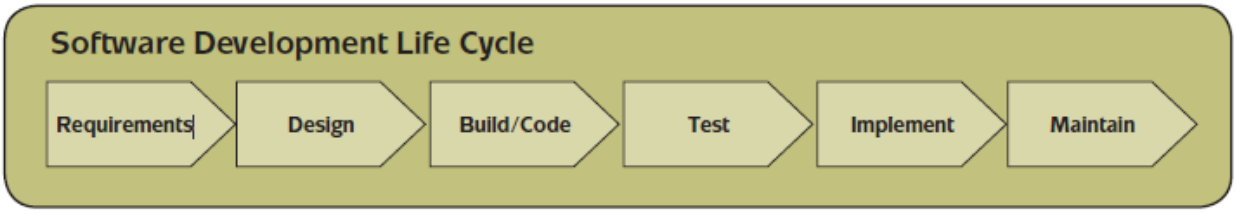


Figure 3. Generic Software Development Life Cycle

management methodology with the specific goal of the project team making a conscious decision to move forward with the project. Projects that are especially complex, such as an enterprise resource planning (ERP) system, should include specific decision points at the end of significant project milestones to ensure the project is on track.

External Consultant Assessment

During the solution or system implementation phase of the project it is quite common for the project management team to partner with an external firm or resource, especially for the implementation of a large package such as an ERP. Auditors should consider whether the viability of the external partner chosen has been reviewed especially for a project that will be lengthy. In addition, it is essential that the roles and responsibilities of all parties are well defined up front so that everyone will have a clear understanding of where accountability lies for the deliverables of the project.

Solution Design

During the solution design phase of the project, auditors should look to ensure that business requirements and both the existing and future business processes are taken into consideration. At the end of this phase, the project scope should be frozen, and all functionality should be prioritized in terms of what is required for the system launch. This prioritization is often referred to as the "must-have versus nice-to-have" decision. It's also typical during this phase for the project team to decide whether to build the solution in house or to buy an external package. Regardless of the decision made, it is imperative to ensure that both functional and security-related internal controls are considered so that they will be included in the solution up front.

Code, Build, and Data

Following the design phase, there should be a process to review the actual coding or building of the system. Within a system's life cycle, there may be many different internal rules or guidelines that the audit can follow. For example, a code development process review can be performed to determine

whether robust and secure programming methods are being followed. Following the system build, the configurations or localizations will take place, followed by the conversion and/or loading of new or legacy data. In addition, the interfaces or connectivity to other systems in the organization will be set up. The data loading consideration is one of the most critical, in particular the preparation of any master data such as employee, customer, or vendor files. While it is important to ensure that there can be continuity of legacy information, it is imperative to start with data that has been clearly identified prior to loading to the new system. In other words, if there is duplicate or old data in the old system, the data should be cleansed before doing a conversion whenever possible.

Testing and Go-live

The next key step is the testing phase. It is essential to determine whether testing includes not only the end users, but also the workflows, security, and connectivity to other systems. Once testing is complete, there should be a checkpoint to decide on the readiness for go-live, or the launch in production. The go-live should not merely be considered as an event, but rather a phase in which a transition plan is in place to transition the new system from the project team to the team that ultimately will be responsible for ongoing operation and support. In this phase it is important for the project to take into account contingency or fall-back strategies to mitigate any unforeseen issues that arise with the final implementation. During this phase of the project there is usually significant pressure to show progress and meet deadlines and, as a result, some important aspects of the detail planning may be overlooked.

3.4 Organizational and Process Change Management

For any project, organizational and process change management is often the most important element to manage and, in fact, can present the most risk to a project. The most complex scenarios include both the change of a business process and the related information systems. Good project management governance processes, as illustrated in Figure 2, enable effective change management. Change management encompasses more of the soft, or intangible, aspects of a project, including understanding the magnitude of how the project will impact the organization and how it will change the way people work. From an audit perspective, this is where the integrated audit team becomes essential to ensure operational and technical aspects are assessed, with the right level of skills from the audit team.

Managing Communication

One of the most critical aspects of change management is managing communication in a broad sense, beginning with obtaining buy-in and representation from all stakeholders, marketing the benefits or reasons for the project, and managing the expectations of end users. For example, what processes will be impacted by the new system and what impact will the changes have on vendors or customers? These points should be stated clearly at the beginning of the project and must be managed well beyond post implementation.

Organizational Readiness

Organizational readiness entails assessing changes to the organization proposed by the new project and managing the level of resistance there will be to the change. This is especially true with projects that involve centralization of processing, such as a shared service center combined with the implementation of an ERP, or with those involving outsourcing. An assessment should be made on the skill set of existing staff members compared to changing or new roles, and determine whether

processes or workflows are clearly defined, to gauge the readiness of the organization to accept the change.

Training

A key success factor for any new system implementation is ensuring that all users who will be impacted receive adequate training. The audit team should evaluate whether the training is complete, timely, and includes user guides that are not generic. In addition, training provided to the IT team and/or helpdesk personnel should be reviewed to determine whether it is adequate to support the new system.

Post launch Support

It is essential for auditors to ensure that a post go-live support plan is defined in terms of the support team organization, for both functional and technical issues. The support team should be analyzed to determine whether it is correctly sized for the go-live and post launch workload, which is usually much higher than normal. Additionally, contingency plans should be established in the event something goes wrong during the go-live period.

3.5 Post Implementation

Following the system go-live, there inevitably is a stabilization period. During this time, the users are getting acclimated to the system or new functionality, and any outstanding issues are being resolved. During this phase, there are key risks to watch for — many of which are related to change management aspects. In other words, the auditors must determine whether the new system is being used correctly and the functionality is meeting the requirements as intended. If many changes were made to the business processes along with the implementation of a new system, the stabilization period can take a relatively long time. A key consideration is to determine whether there is any prolonged resistance to change. For example, are users finding a work-around or short cuts because the new system is not as user-friendly as its predecessor? Discussions and interviews with users can be held to determine this. A post implementation review can take a couple of different approaches. More detailed information on conducting a post-implementation review can be found in Section 4.3.

4. Project Audit Planning

IT projects should be included in the annual internal audit plan using a systematic process. Figure 4: IT Project Planning Process depicts a logical workflow progression that uses a top-down approach to determine which projects to audit. It is consistent with the large audit planning process described in GTAG 11: Developing the IT Audit Plan.

Internal auditors can add considerable value by evaluating both the IT and organizational aspects of IT-related projects. Key questions the internal auditor should consider include:

- How should IT project audits be incorporated into the annual audit plan?
- What is the appropriate role for the internal auditor?
- What projects should be audited and why?
- What type of project audit should the internal auditor perform?

4.1 IT Projects and the Annual Internal Audit Plan

To include projects in the annual audit plan or audit universe, internal auditing should have access to the organization's entire list of IT or technology-related projects. Ideally, there should be a list of all projects in a centralized system where auditors can run reports based on risk factors such as the cost of the project, schedule, project risk, project duration, etc. If no such list exists, questions regarding IT or technology-related projects can be raised during annual audit planning to both IT and key business functions. In addition, the PMO can be an invaluable source of information to aid auditors as they develop the audit universe and the annual audit plan, and as they plan audits of individual projects. The internal auditors should engage with the PMO as part of scoping and planning prior to conducting IT project audits.

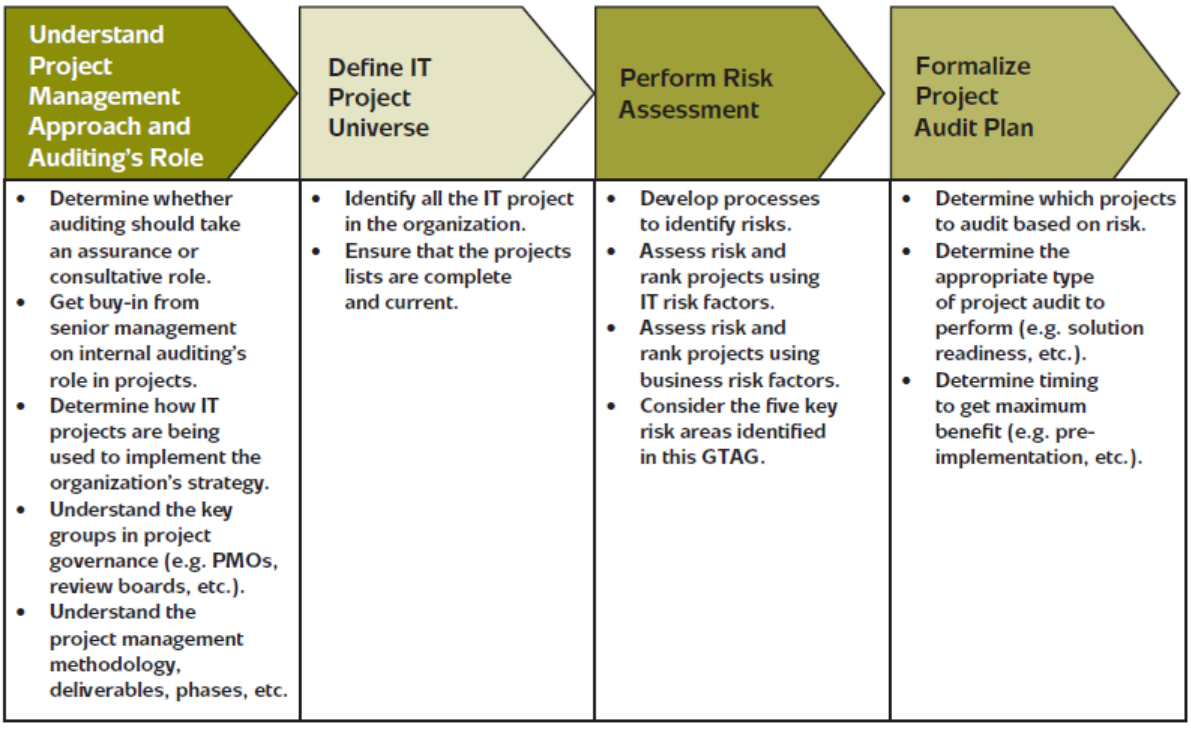


Figure 4. IT Project Planning Process, adapted from *GTAG 11: Developing the IT Audit Plan*.

The following points may be useful for auditors to consider when assessing the project risk at the organizational level and to determine how to include IT-related projects in the annual audit plan:

- A complete and accurate inventory of all projects — with enough supporting information to assess the risk at a high level — is unavailable.
- There are a large number of IT projects spread across the company.
- The organization lacks centralized methodologies and processes for project governance, including project management methodologies and system development life cycles.
- Senior management is overly confident in its ability to deliver projects effectively, yet cannot produce evidence of project inventories or centralized methods.
- Project managers and senior management believe that auditors cannot add value to projects and that project teams are too busy to deal with supporting a project audit because of lack of resources, impending deadlines, etc.

4.2 Internal Auditing's Role

When considering the internal auditor's role, a key point to keep in mind is the nature of the internal audit organization and whether the function is mandated to perform only assurance type engagements, or whether engagements that are more of an operational or consultative nature are

also permitted. The IIA's International Standards for the Professional Practice of Internal Auditing provide the necessary guidance for the internal audit function to perform these roles.

Internal auditors can add significant value to a project by engaging early and supporting the project team throughout the project life cycle. They may be asked to support the project in various capacities, ranging from consultative reviews to formal audits. This can create the potential for perceived impairment of auditor independence. The IT auditor should provide reasonable assurance that his or her interest, if any, in the IT solution will not impair the objectivity of the review, and that his or her participation is one of providing advice without being responsible for making the decision. As an additional resource, the IT auditor may also consider Information Systems Audit and Control Association's (ISACA's) Guideline G17: Effect of Non-audit Roles on the IS Auditor's Independence. The sooner the auditor engages with a project, the better. Internal audits or assessments performed during the early phases of the project can be the most valuable because they can identify issues earlier and reduce cost. When auditors find issues, their recommendation often includes the addition of automated controls or possibly design changes. It has been well established in studies of software development that software fixes and adjustments are far cheaper to address in the early project stages, such as the design phase, rather than in the later stages of the project. Finding and fixing a software problem after delivery is often 100 times more expensive than finding and fixing it during the requirements or design phases.[19] Figure 5: Relative Costs to Fix Errors Throughout Life Cycle shows the dramatic relative cost of fixing software changes throughout the life of a project. This can be a major selling point in convincing senior management to support early internal audit involvement in the project.

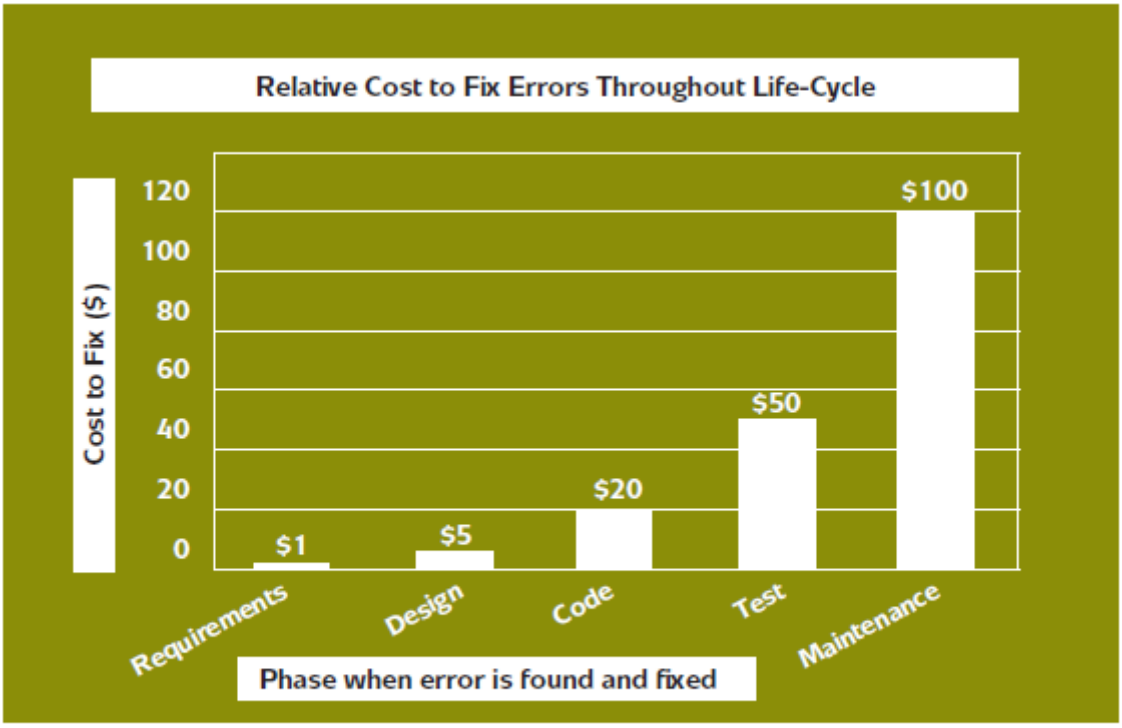


Figure 5. Relative Costs to Fix Errors Throughout Life Cycle.

4.3 Types of Project Audits

Internal auditors may perform a variety of different reviews, depending on the project risk and needs of the organization. This GTAG highlights five of the most common types of project-related audits or assessments to consider:

- Project risk assessment to gauge likelihood of success.
- Readiness assessment during key phases or pre-launch.
- Post implementation review.
- Audit of a key project phase during the life of the project.
- Overall project management methodology assessment.

The most important consideration for any type of internal audit review is staffing the engagement with the right skill set. This is where the benefits of an integrated internal audit team become very clear. Using an integrated team ensures that both the functional and technical risks of the project are included in the scope of the review. An integrated audit team should include skill sets of both a business and technical nature.

Risk Assessment

A risk assessment typically involves an overview of all project areas to identify the key risks that could impact project delivery and determine how well they are being tracked and mitigated. This type of review is also quite common if management believes the project is not progressing well, costs are exceeding the budget, or the project has already experienced delays.

Readiness Assessment

A readiness assessment is a review that takes place at a key stage of the project — usually upon completion of the business case, alignment phase, solution design phase, or pre-launch phase. The key objective for this type of review is to provide objective assurance on the completeness of each phase and to ensure management is aware of any newly identified risks or issues before moving forward to the next step.

Post-implementation Review

A post-implementation review takes place at some predetermined point after the new system has gone live. There are many different variables to consider regarding the target timing for this type of audit, including whether the system needs time to stabilize, how long the project team will be available to correct issues, vendor contractual considerations, and post launch issues raised by the users.

There are a couple of different approaches to performing a post-implementation project review. Its purpose can be to evaluate how well the project followed the organization's project methodology or SDLC, or to measure how well the new system is working. A post-implementation review likely would use an integrated audit approach because both the system and related business processes should be examined in tandem.

During the project initiation and development of the business case, many project benefits are noted. A benefits realization review is another type of post-implementation or post-project review that may be performed and would be geared toward measuring how well the project has achieved the benefits, savings, or efficiency gains it was intended to achieve. ISACA's Guideline G29: Post Implementation Review offers specific guidance on this type of review.[20]

Another approach is to audit the end results of the project back to the originally stated objectives, or to conduct an assessment of how the project went so that lessons learned can be captured for use on future projects. The audit team may also perform an end-to-end process review to include all

aspects, or functionality, of both the business processes and the new information system. However the approach is designed, it is essential to allow an adequate stabilization period following the launch.

The duration of the stabilization period should be determined up front in the project plan. In general terms, the stabilization usually takes on average three to six months depending on the complexity of the system. It's also important for the auditors to keep in mind how quickly the project team will disband, and to identify who will take over the project documentation and manage the transition into a normal maintenance or continuous improvement phase. Auditing a project after the project team moves on can be quite difficult if there isn't adequate documentation available, or to understand why some decisions were made.

Key Phase Review

A key phase review, undertaken during the course of a project, is a proactive approach often used for high-risk projects. This can include SDLC or system design reviews, or participation by the internal auditor in a "gate" or specific project phase review, for example. The key objective is usually associated with assessing how closely the project management or SDLC methodologies are followed. As indicated above, internal auditing can work with project teams to address concerns before the system is moved into the production environment, when it is still relatively inexpensive to make corrections. Through early project involvement, internal auditing can raise questions and suggestions that influence a project in either a formal or informal way.

Project Management Methodology Assessment

Auditing the overall project management methodology can identify risks and point out weaknesses in the methodology that could help the entire organization improve. For organizations that have too many projects to audit individually, this type of review utilizes a more holistic approach. In addition, by auditing the methodology, the internal auditor will be better prepared to audit individual projects because the PMO audit will provide a strong basis for understanding the organization's practices.

Possible objectives of auditing project methodologies include:

- Assessing the adequacy of project management methodologies.
- Determining whether the methodology supports the full range of IT projects in the organization, from very small to very large.
- Assessing the effectiveness of management level support provided by the PMO. (This may be articulated in a PMO charter or mission statement.)
- Determining whether the PMO policies, standards, methodologies, and processes are implemented and executed consistently across all projects in the organization.
- Assessing the ability of the PMO to add the intended level of value.
- Determining whether the PMO has a complete inventory of all projects in the organization.
- Determining whether the PPM processes are working effectively.

Project Audit Reports

The report out from the audit team following a project review can vary depending on the type of review performed, and the stage of the project at which the audit team gets involved. The IIA's International Standards for the Professional Practice of Internal Auditing 2400 series provides guidance for communicating results; however, the type of review should be carefully considered when determining what format works best within the organization. For example, if the audit team is participating throughout the life of the project, status updates or memos to the project steering

committee could be a format to consider. For a post-implementation review, especially if the full functionality of the system and underlying business processes are evaluated, the formal audit report format may be preferred.

4.4 External Auditor Considerations

Because IT and technology-related projects may have a critical impact on the organization's financial statements and operations, external auditors will want to know what major projects are underway in an organization. Specifically, they will be concerned with IT projects that could have a major impact on:

- Financial statement reporting (e.g., a new SAP general ledger system).
- Revenue generation (e.g., order processing).
- Inventory management.
- Major business or IT transformations that affect financial data or systems that produce financial data.
- Major regulatory requirements such as the U.S. Sarbanes-Oxley Act of 2002.

The CAE should engage with the external auditors to understand their perspectives on the risks associated with IT projects. A major risk for the organization is that the external auditor is unaware of major projects and highlights key control considerations of a project after the new system is already in production, when it is considerably more expensive to modify existing controls or implement new controls.

Conclusion

In conclusion, "auditors should consider projects to be opportunities to exploit their core competencies in new areas, while they help ensure the effective risk management, cost containment, and organizational success of projects," notes Richard B. Lanza in an article on technology project risks that appeared in Internal Auditor in 2002,23 which is still very relevant today. The incorporation of projects into the audit universe helps internal audit to partner with both project managers and senior management and to have a positive impact towards future project success.

Appendix A – Project Management

A.1 Project Management Methodologies

An IT project management methodology is like a toolkit for project teams. A good methodology explains the relationships among all the relevant project management and organizational processes. It is a comprehensive structure of repeatable processes that provides a road map on when, how, and what events should occur in what order. For IT projects, it is based on a combination of project management and system development best practices. Typically, it is composed of interrelated phases, activities, and tasks that are supported by documented milestones, guidelines, techniques/methods, templates, samples, and roles and responsibilities.

A methodology is necessary to:

- Provide a standard, repeatable model approach that can be used to deliver a project.
- Promote the use of best practices that will increase a project's probability of success.

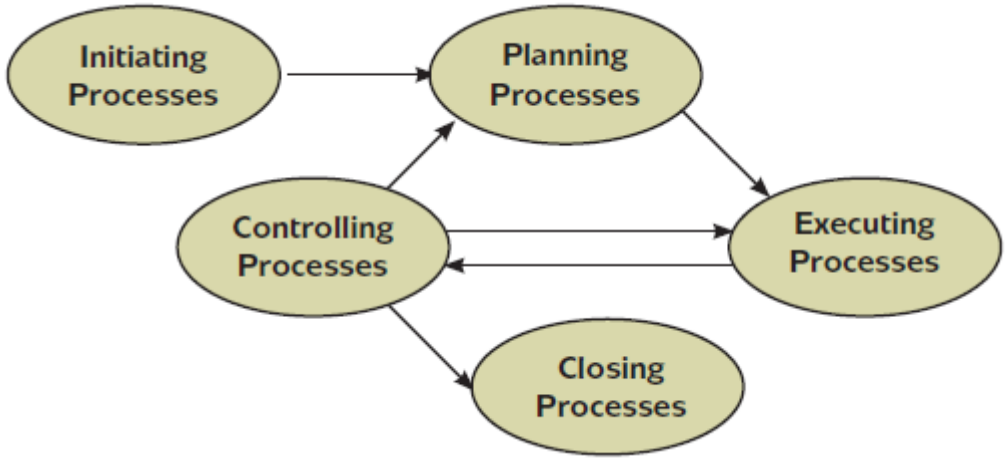
- Define what is happening so that it can be improved. (According to the Software Engineering Institute (SEI), a process has to be defined before it can be improved or made repeatable.)
- Increase the chances of project success and reduce known risk areas.
- Provide a structure for project managers to manage their projects.
- Ensure best practices are systematically deployed across projects.
- Provide a structure for assessing the effectiveness of project outcomes and updating the methodology with those lessons learned.

- Provide a structure for consistently monitoring project performance against a consistent set of deliverable requirements and performance metrics. Types of components typically found in a methodology include:
  - **Frameworks –** composed of phases, activities, and tasks.
  - **Guidelines –** define the activities required to generate deliverables.
  - **Techniques/Methods –** provide guidance on how to perform activities.
  - **Templates** and **Samples –** make it easier to apply recommended techniques.
  - **Roles –** communicate who is responsible for what.
  - **Project Plans –** lists the activities at both high and detail level for the project.

A.2 Project Management Life Cycle

According to the Project Management Institute, there are five phases in a project life cycle. The phases are linked by the outcomes they produce — the outcome of one is the input to another.

1. Initiating – Authorizing the project.
2. Planning – Defining and refining objectives and selecting the best of the alternative courses of action to attain the objectives that the project or phase was undertaken to address.
3. Executing – Coordinating people and other resources to carry out the plan.
4. Controlling – Ensuring that the project objectives are met by monitoring and measuring progress regularly to identify variances from the plan so that corrective action can be taken when necessary.
5. Closing – Formalizing acceptance of the project or phase and bringing it to an orderly end.



Stakeholder	Responsibility
Steering Committee (Executive or Technical)	Executive leaders (business and IT) who influence guiding principles, strategy, and major decisions
Sponsor	Person who provides the financial resources or endorsement of the project

Project Manager	Person with overall project responsibility and clear lines of authority and accountability
User (Business, IT, etc.)	Those who use the outcome from the project
Project Team	The team that performs day-to-day work on the project, a mix of IT and business people
Influencers	Those not directly related to the use of the project, but due to their position, can have negative or positive influence
Project Management Office	The office that provides project managers or other team members, which may have direct or indirect responsibility for the outcome of the project
Compliance Review Boards	The team that assesses special compliance or policy requirements such as the U.S. Sarbanes-Oxley Act of 2002, local laws, etc.
IT Security	Those who ensure that the final system is designed with the IT security features to meet organizational security policies or best practices
IT Architecture Board	The team that ensures that the system will be compatible with existing or future infrastructure
Consultants and Vendors	Development consultants or the applicable system vendors (e.g., SAP, Peoplesoft, etc.)
Auditors (Finance, IT, External, and Internal)	Those who perform audits and provide auditor perspective on risk
Procurement	Those who buy project materials and labor

The following table is a suggested list of audit questions that can be used in the assessment of the five key focus areas that have been highlighted throughout this GTAG. These questions have been adapted from a Lafarge internal audit work program.

Business Case and Alignment		
Area		**Criteria**
1 — Business Case- Investment / Benefit Realization		
1.1	Business case management	There is an agreed-upon business case for the project.
		It is updated, and includes lower levels of details as information becomes available.
		Realistic assumptions are being made about costs and benefits.
		Assumptions are documented and agreed-upon
		Assumptions are actively proven or disproved as the project progresses, and appropriate action is taken as a result.
1.2	Project costs	The project management team is confident in the estimates.
		A standard estimating model is used for all common pieces of work.
		It is clear who needs to agree with and understand the model
		Extra budget has been allocated to speed up or fast-track development projects to allow for testing out the approach, environment, etc
		Estimates are included in the budget for both staff and nonstaff costs (hardware / software external/internal resources, developments,

		end-to-end testing, quality assurance, benefits realization follow-up, vendor costs, operational costs, etc.).
		There is a definition of what contingency is to be used. If an issue arises, there is a plan for how it will be addressed.
		The estimates have been reviewed by a qualified third party.
1.3	History	Changes in project costs have been made since the original business case.
		Changes have been made, if so, understand why.
1.4	Timing of costs	The estimated timing of costs is appropriate. Understand if it is possible to postpone some costs.
		Timing of costs has been changed, if so, understand why.
1.5	Type of benefits	Types of benefits (e.g., cost reduction, increased revenue, qualitative) are clearly articulated.
		The realization of benefits is dependent on external factors.
		How dependencies should be approached is defined.
		The benefits are aligned with the current scope of the project.
1.6	Realization of benefits	It is clear how benefits will be measured (e.g., direct bottom line cost reduction, staff reduction or cost reallocation).
		The responsibility for achievement of benefits is clearly defined in terms of who will do what.
		The owners have approved the benefits as reasonable and achievable.
1.7	Realization of benefits	It is clear how benefits will be measured (e.g., direct bottom line cost reduction, staff reduction or cost reallocation).
2 — Project Plan and Approach		
2.1	Objective and scope	The scope of the project is clearly defined, and it includes sufficient level of detail.
		There is an up-to-date and communicated project charter.
		There is a common understanding of scope by both the business and the project.
		There is an agreed-upon procedure for changing the scope, which was designed at the outset of the project.
2.2	Estimates, timeline, and scope	The current estimates are clearly communicated to the project group, sponsor, steering group, and project office.
		Understand if estimates have changed over time, and why.

		The project has been reevaluated based on business case updates.
2.3	Organization	Each role in the project is defined.
		The project organization is defined.
		Everyone on the project knows and understands his or her role.
		Understand if there are any incentives attached to project success and the impact.
2.4	Deliverables	The content and structure of each deliverable of the phases are documented.
		The purpose of the deliverables are clearly understood and documented.
		All project signatories are aware of the required deliverables sign-off.
		The format of the deliverables been discussed and agreed-upon with the signatories.
		Appropriate experts have reviewed key deliverables.
2.5	Dependencies	Tasks outside the project are clearly documented and understood. The plans for these tasks have been developed and agreed-upon.
		Checkpoints are defined in advance, along with what will be produced.
		The planning assumptions are understood, documented, and agreed-upon.
2.6	Time plan and activities	There is an overall project plan that links together all the sub-project plans.
		Every stream within the project has a detailed plan with visible milestones. Check if this only applies to critical areas.
		Each area has a clear view of the end result and what is required to get there.
		The main pieces of work have been identified and the relationship between them is documented.
		Each piece of work has a clear focus and owner.
		All inter-project and external dependencies have been identified and due dates and owners are defined.
		There is a fast track or pilot project to prove the methodology, deliverables, environment, etc.
		The pilot project run is small, discrete, and representative.
		The owners of the pieces of work have agreed to the plans.
		The planned days/weeks allow for holidays/training.
		The plan reflects learning curves/knowledge transfer.
		The plan allows for schedule contingency between each main piece of work as well as at the end of each phase.
		The plan includes sufficient lead-time for phase set-up tasks (e.g., environment, standards, and procedures.).
		Appropriate reviews and sign-off time is incorporated into the plan.
3 — Project Communication and Coordination		
3.1	Communication and change management	Everyone knows why we are doing this and the timeline of events.
		Everyone knows how it will affect him or her.
3.2	Organization	Each role in the organization is defined.
		Everyone knows how his or her role relates to the process on the

		whole.
3.3	Dependencies	All inter-department and external dependencies have been identified.
		Management is releasing the necessary resources to work on the project.
		Management is willing to halt other projects/areas of work if they conflict.
3.4	Shared Programs	The project has sponsors or representatives from each affected area.
3.5	Current status	Understand the current status of the project with regard to time, cost, and scope, and whether there are any deviations from the project definition.
		Understand the key concerns with respect to status.
		Understand why any deviations have occurred.
		Reasons behind deviations were identified as risks before they occurred.
		Corrective actions have been taken to address deviations, risks, and issues.
3.6	Work plan	The work plan has been updated regularly.
		The project estimates are accurate and key milestones have been met on time.
		Key tasks to be completed are identified, and the critical path or must-have list for go-live has been identified.
		A plan to handle overruns if expected has been developed.
3.7	Risk handling	A risk assessment has been performed, documented, and communicated.
		It includes mitigation actions / contingency plans and those accountable.
		The risks are understood by the business.
		The risks and actions to mitigate them are proactively managed.
		Risks are reviewed regularly with the business.
		Issues have a clear owner for resolution.
3.8	Dependencies on other project/areas	The plan incorporates a mechanism for the coordination of changes resulting from other business/systems projects.
		Service level agreements have been specified for support areas.
IT Solution and Change Management		
Area		**Criteria**
4 — Process Design		
4.1	Business scope	Scope — in terms of business units, locations, and business rules — is defined and validated.
4.2	Process and supporting design	The process design is documented through business scenarios and business process design documents.
		Business scenarios are documented, tested successfully, and signed off by business representatives.
5 — Configuration and Developments		
5.1	Translation	All screens and customizing is documented.
5.2	Configuration	Configuration of critical tables are reviewed for completeness, and fully documented.
5.3	Programs	Functional design is complete, up to date, and agreed-upon with

		business representatives.
		Technical design is complete, according to specifications, and successfully unit-tested, and acceptance is tested by the project team.
		Specific programs are developed according to standards.
		Specific programs are unit tested.
		Programs are migrated to production platform or environment.
5.4	Interfaces	Functional designs for interfaces are complete, up-to-date, and agreed to.
		Technical designs for interfaces are complete and up-to-date.
		Reports are developed according to design, successfully unit-tested, and accepted by the project team.
		Interfaces are tested “end-to-end” with the production platform.
		The functional error-handling process is defined, developed, and tested.
		There are no outstanding “urgent” or “high” issues with interfaces.
6 — User Acceptance Tests		
6.1	User acceptance tests	All business scenarios are successfully executed and signed-off. All user acceptance tests are complete and scripts signed-off.
		There is adequate business involvement to ensure realistic testing.
6.2	Issues list	All functional gaps noted in the issues list are closed and resolutions are agreed.
6.3	Batch schedule	Daily, weekly, monthly, quarterly, and annual batch schedules are designed and validated with project and technical teams.
		Job failure instructions, from a functional perspective, are defined (e.g., skip job, rerun next day or hold schedule).
6.4	Issues remaining at go-live	Functional team leads have agreed with key business representatives which issues will not be fixed until after go-live, and work-arounds if necessary are defined.
		Where required, workarounds have been defined and communicated to the training and help desk/support groups.
There are no outstanding “urgent” or “high” issues with the data load.		
7.4	Go-live plan	The go-live plan is developed and communicated to all impacted project and business personnel.
		The legacy batch schedule is ready.
		Legacy access profiles are amended to ensure users do not continue to use legacy systems by mistake.
		Timing and participants of go/no-go meetings are agreed-upon.
		Fallback plans are developed and agreed-upon.
7.5	Reconciliation	Financial balances reconcile to legacy systems. Balances are loaded and can be reconciled to legacy systems.
		Procedures are in place to explain or fix discrepancies.
8 — Technical Infrastructure		
8.1	User interface	All user locations are identified.
		The user interface is installed and has been checked on each PC.
		Logon procedures are checked.
		All update procedures are documented and communicated.
8.2	Printers	All printer locations are identified, and printers are set up and tested.

		All printers are established in the different systems.
		All printers can print from the different systems.
8.3	Electronic output	All fax and other electronic output formats are agreed-upon and tested.
		A production test is completed to outside fax line and electronic data interchange (EDI) recipients.
8.4	Batch schedule	Nightly and monthly batch schedules are checked.
		All server/directory destinations for interfaces are set up to point to production systems.
		There are no outstanding “urgent” or “high” issues.
8.5	Error handling procedures	Procedures for checking that errors are logged (batch interface) are in place.
		Batch interruption re-start procedures are agreed-upon and tested.
		Procedures for communicating errors to the business are agreed-upon.
8.6	Communication links	All communication links (e.g., LAN, WAN) are tested.
		Bandwidth supports peak data volumes.
		Fallback procedures are in place and tested.
8.7	System sizing	All infrastructure components that form part of the overall technical architecture is sized and tuned to accommodate peak activity and predicted growth rate.
		Hardware, software, and applications are tuned for go-live.
8.8	Performance tests	Performance tests have been conducted, and performance is acceptable for key business processes.
8.9	System performance	Post go-live, online, and batch system performance monitoring and tuning procedures are in place.
8.10	Disaster recovery	Procedures are in place for downtime, and a disaster recovery plan is in place.
		Procedures successfully tested.
8.11	Online system availability and maintenance slots	Online system availability and maintenance slots are agreed-upon with the business.
8.12	Security profiles	Security profiles are defined and implemented for IT support staff.
		The production environment is secured.
8.13	Interfaces	The interface technical set up is complete and tested.

Business and User Readiness		
Area		**Criteria**
9 — Business Simulation		
9.1	Preparation	All business scenarios are written (capitalize on user acceptance testing).
		The technical environment is ready.
		All necessary data are converted in the simulation environment.
		Users and profiles are ready.
9.2	Completion	All business scenarios with “urgent” or “high” issues are successfully executed.
		There is adequate business involvement to ensure realistic testing.
10 — Data Maintenance Post Go-live		

10.1	User ownership	Data types are inventoried and owners agreed-upon.
		The actual persons who will perform maintenance are appointed and trained.
10.2	Data maintenance	Procedures exist for each type of add/update.
		Procedures cover updating of any related trans-codification tables.
		Procedures have been communicated to all impacted users.
11 — Roles and profiles		
11.1	User profiles	Profile design is agreed-upon by the project team and business representatives.
		Profiles are developed and tested successfully.
		There are no outstanding “urgent” or “high” issues with profiles.
11.2	Business risks	Key business risks are identified and covered through systems features or procedures.
		There are no outstanding “high” issues.
11.3	System user access	All profiles are developed and tested for production and non-production environments.
		The business signs off on who receives what access.
		The business controls approval on segregation of duties.
		All user profiles are set up, including conversion and support roles.
11.4	Profile maintenance	Procedures for maintaining profiles after go-live are developed, approved, and distributed to impacted personnel.
12 — User Readiness and Training		
12.1	User impact	All users understand how their job will be impacted by the solution.
		All affected users have received job change information.
12.2	User training and competence	All affected users have attended training.
		Trainees have demonstrated competence in using the solution through the completion of training exercises.
		Extra coaching and support is scheduled for those users post go-live.
12.3	Interface errors	Users responsible for correcting interface errors have been identified and have been trained on the procedures.
12.4	Support tools	Users have access to support tools
12.5	New codes and form layouts	Customers/suppliers are informed of all new codes, form layouts, etc.
Implement - Transition - Post Implementation		
Area		**Criteria**
13 — Resource Staffing and Key Roles		
13.1	Competence requirements and fulfillment	The required skills are understood, documented, and updated.
		The required skills are covered by people assigned to the project.
		The project is competing with other projects/initiatives for key competencies/resources. If so, understand the impact.
		There is a training program to build skills that are missing.
13.2	Competence localization	Key resources have been localized in the project premises, and/or the project team members are all located together.
13.3	Resource mix	The project has sufficient full-time resources.
		The internal vs. external resource mix is clear. There is a clear process for knowledge transfer if the external support is high.
		Agreements have been put in place for external resources (e.g.,

		time and materials, or pay for realized benefits).
13.4	Staffing of key roles	The staffing of all areas receives sufficient priority — or is the skilled staff located in one key area?
		Knowledgeable resources are best placed to maximize their contribution to the project.
		The following roles are filled with staff with the right skills: technical architect, data architect, business architect, functional architect, and conversion/migration architect.
14 — Implementation Into Business Areas		
14.1	Roles projects/business areas	The business area understands their role in each phase of the project, and is prepared for the implementation.
		Each business area has a dedicated resource to work with the project.
		The decision-making process is clearly defined.
		The business area understands their role in the decision-making process.
14.2	Plans and resources	There are plans and resources for training, roll-out, follow-up, and sign-off.
15 — Implementation into IT Production and Maintenance		
15.1	IT production	There is a plan for transferring knowledge.
		The production team has agreed to a deployment plan.
		There are plans to ensure capacity.
15.2	IT maintenance	There is a plan for transferring knowledge.
		Maintenance has agreed to a deployment plan.
		There are plans to ensure capacity.
15.3	Implementation	The conversion dates been changed. If so, why?
16 — Transition to Support		
16.1	Support strategy	The overall support strategy is agreed-upon.
		The first-level support members are identified and trained on the required tools.
		The second-level support members are identified and trained on the required tools.
16.2	Change requests and fix procedures	The process for assessing and implementing change requests is agreed-upon and communicated (e.g., impact analysis, funding).
		The process for applying fixes and change requests is agreed-upon and communicated.
16.3	Support processes and contacts	Support numbers and guidelines for what information needs to be recorded if a problem is found have been communicated to users.
		The business is aware of on-site support contacts.
16.4	System usage, control measures, and review meetings	System usage measures (i.e., the system is being used, and it's working) are defined and agreed. Procedures are in place for capturing and reporting information.
		Daily post go-live review meetings are arranged.
17 — Business Continuation Plans		
17.1	Business continuation plans	Business continuation plans, in the event of loss of system, are developed and agreed-upon with project and business groups.
		Fallback plans are established to address procedures to take when the system becomes available again, to ensure items are not processed twice and financials are updated.

		Any required manual forms/other systems are in place to support fallbacks.
		The process for triggering fallback plans (i.e., who decides and who communicates) is defined and agreed-upon.