GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Management of IT Auditing

2nd Edition

The Institute of
Internal Auditors

Global Technology Audit Guide (GTAG®) 4
Management of IT Auditing
2nd Edition

January 2013

GTAG — Table of Contents

1. Executive Summary

IT has a pervasive impact on the internal audit function. As new risks emerge, new procedures are required to manage these risks adequately. The process for executing IT audit work is, in general, no different from the process for executing any other audit work. The auditor plans the audit, identifies and documents relevant controls, tests the design and operating effectiveness of the controls, concludes, and reports. The chief audit executives (CAEs) regularly report to key stakeholders such as the board, executive management, regulators, external auditors, and the chief information officer (CIO) on the results of IT audit work. This guide is to help the CAE plan and manage IT audit work more effectively and efficiently and covers how to:

> **Determine where IT audit resources are needed.** Which parts of the internal audit plan will require IT audit specialists? The CAE should be able to measure planned use of IT auditors against the guidelines presented here to help ensure the scope is adequate. IT audit resources are typically scarce, and IT audit demands are substantial. Defining IT audit needs helps the CAE understand how to build effective IT coverage into the internal audit plan. Regardless of the size of the internal audit workgroup, the concepts of having the right skills for the particular audit work prevail, and these can be insourced or outsourced depending on organizational capabilities.
>
> **Evaluate IT-related risk.** IT risks continue to change as technology evolves. Some of these risks are related to the technology itself and some to the manner in which the business uses IT. This guide helps the CAE understand how to identify and quantify IT-related risks. Doing so will help ensure that IT audit resources are focused on the areas that deliver the greatest value to the organization.
>
> **Execute IT audit work.** The proliferation and complexity of IT increases the need for appropriate IT audit procedures that can be integrated into routine operational and process audits to address specific risks identified during audit planning. Auditing by checklist or by inquiry is insufficient.

In addition, the guide provides assistance for the CAE around required skill sets IT auditors should possess to bring sufficient knowledge and expertise to the audit function, tools to assist the auditor in performing IT-related testing, and specific reporting expectations. The focus of this guide is on providing pragmatic information in plain English, with specific recommendations that a CAE can implement immediately. Consideration is given to providing criteria that a CAE can use to evaluate the maturity of IT audit capabilities and ensure the internal auditing team is performing to a high standard.

2. Introduction

The risks organizations face, the types of audits that should be performed, how to prioritize the audit universe, and how to deliver insightful findings are all issues that challenge CAEs. This Global Technology Audit Guide (GTAG) is designed for CAEs and internal audit management responsible for overseeing IT-specific audits, as well as IT testing integrated into other audits performed.

The purpose of the guide is to help sort through strategic issues regarding planning, performing, and reporting on IT audit work. Consideration is given to the fundamentals as well as emerging issues. An annual risk assessment performed to develop the audit plan that does not address IT risks would be regarded as deficient (see Standards 1210.A3, 1220.A2, and 2110.A2). Three issues should be considered by internal audit:

- A high percentage of key internal controls relied upon by the organization are likely to be technology driven. Example: Organizational policy states that before any payment is made to a vendor, a three-way match is performed. A three-way match is a comparison of a purchase order, delivery docket, and invoice. Historically, a clerk physically matched pieces of paper, then stapled and filed them. Now, all matches may be performed within the organization's enterprise resource planning (ERP) system. The system automatically performs the match based on pre-configured rules and tolerance levels and automatically posts variances to defined variance accounts. To audit that control effectively, an auditor may need to access the ERP systems' applicable configuration settings and evaluate the rules and settings, which requires a certain level of technical skills that not all audit professionals may possess.
- Organizations need to understand strategic risks introduced by complex IT environments. The adoption of IT as a business facilitator will change an organization's strategic risks. The organization needs to understand this change and take appropriate action to manage such risks.
- IT general and application controls should be developed to adequately manage IT risks. Effective IT controls are needed to protect an organization's operations and ensure competitive readiness is not impacted; systems that do not perform as expected are likely to cause significant reputational damage. Example: Consider the automated process described above, where a sales order comes in via a website and is directly transmitted through the ERP system to the warehouse floor. Now consider what happens when a customer accidentally orders 100 pallets instead of 100 units. If the organization has fully optimized its processes with an ERP system, it is possible that the system will check inventory, note that 100 pallets are not available, update the production schedule to produce 100 pallets, and automatically send off purchase orders for raw materials via electronic data interchange (EDI). Without proper preventive controls, this error would likely not get detected until the customer received the goods.

One issue that often comes up is understanding how IT controls relate to financial reporting, fraud, operations, compliance, and other key issues. This is considered relatively easy to grasp when you are evaluating controls within an application system (e.g., the three-way match settings discussed earlier). However, it is much more difficult when evaluating supporting technologies that can have a far greater impact on the organization than IT controls specific to a single application or process.

For example, assume that an organization creates electronic payments that it sends to its vendors. These payments are routed electronically to bank accounts based on Society for Worldwide Interbank Financial Telecommunication (SWIFT) routing numbers for each vendor account. All Automated Clearing House (ACH) numbers are stored somewhere in a table in the organization's database system. A database administrator, anyone with the right access to the database, or individuals without approved access who have technical skills to improperly access the database could change every entry in that table to his or her own bank account ACH routing number. The next time an electronic payment run is performed, the funds would be deposited into the perpetrator's bank account. This would completely circumvent all security, control, and audit trail mechanisms that exist within the business process and the business application.

In the above scenario, it is easy to see how a control deficiency at the database level could have a far greater impact than a deficiency with the three-way match settings. As part of the annual risk assessment performed, the likelihood and potential impacts of risks associated with the IT environment should be carefully evaluated.

3. Business Strategy, Processes, and Projects

Business strategy is a critical driver in identifying the audit universe and it is vital for the organization to consider in risk assessment. Business strategy articulates the objectives of the organization and the methods to be used to achieve them. It is important for the CAE and the internal audit management team to understand the business strategy, and technology's role in the organization and the effect each has on the other. One of the tools the CAE can use in assessing the business strategy of an organization and its influence on IT audit work is *GTAG 11: Developing the IT Audit Plan*. It provides the CAE with information on understanding the organization's IT environment in a business context.

The IT components listed in section 4 provide tools necessary to map the organization's operations to the IT infrastructure, and define IT aspects of other areas identified in the audit universe necessary to perform the risk assessment.

As the CAE maps the organization's operations and IT infrastructure, the impact of various IT and operational relationships in the organization will become apparent. Extended mapping could identify critical areas such as infrastructure, applications, processes, and relationships (both internal and external) that may be subject to risks not previously identified. This mapping process will assist the CAE in assessing IT risk and risk tolerances within the organization, and provide insights into potential unidentified risks, which should be communicated to senior and IT management.

Typically, IT projects utilize specialist resources from internal audit to provide assurance over project milestones. The CAE should assess the level of skills and knowledge required to perform IT audit work and assign appropriate resources. In some cases, external subject matter expertise is needed to properly staff such engagements. Necessary steps are discussed in more detail in *GTAG 12: Auditing IT Projects*.

4. Technology Infrastructure and Processes

Defining IT

One of the initial challenges a CAE faces when determining the involvement of IT audit resources is identifying IT usage. Are the telephone and voice mail systems part of IT? Should facilities access and identification requirements and physical security systems be included? What if they are outsourced to the property management company? These are some of the issues that need to be addressed when determining how to allocate IT audit resources.

IT means different things to different organizations. Two organizations in the same industry may have radically different IT environments. To further complicate matters, within a single organization controls may be centralized, decentralized, or a mixed mode. Mobile computing, social networking, and cloud computing are extending the boundaries further away from central control, and introducing unique risks and considerations. Unfortunately, IT is not clearly or universally defined.

This section will help CAEs address how to think about IT within an organization. Some components are integrated with manual processes and procedures, and some may be considered stand-alone. IT risks exist in each component of the organization, and they vary greatly. Hacking the corporate website and diverting an electronic payment run, for example, are very different risks to the organization.

Consider Each Layer

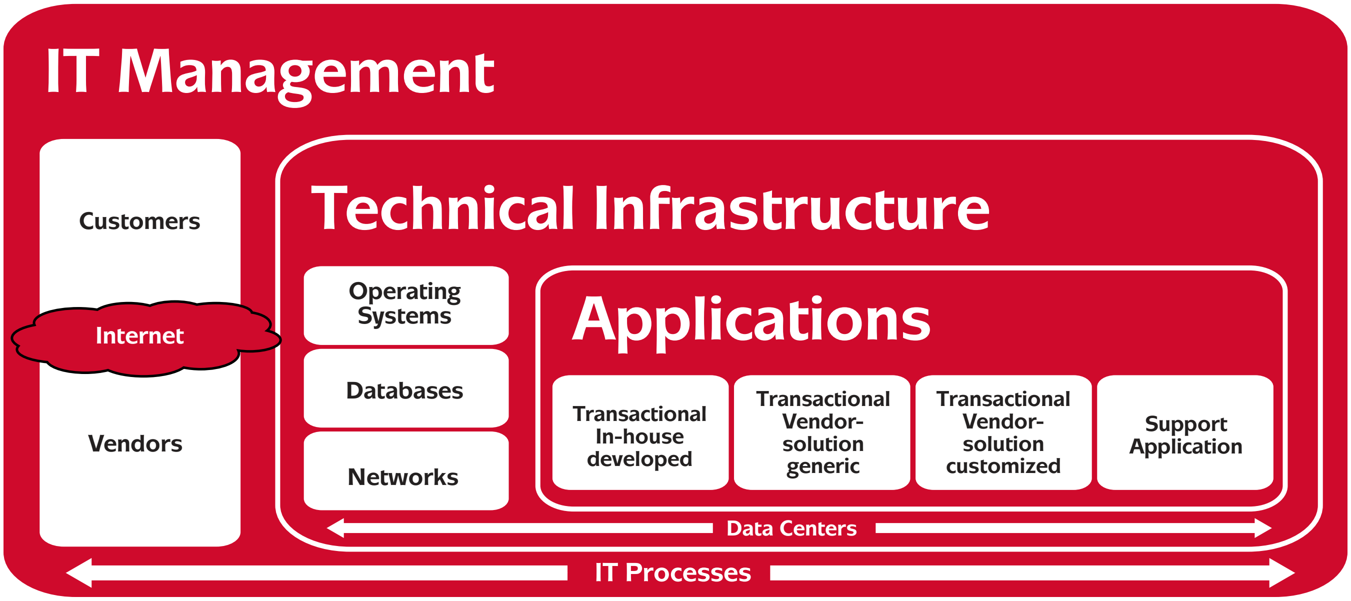
For an internal audit to be effective, the risks of each IT layer need to be considered and prioritized, and audit resources should be allocated to each layer according to those risks. If the IT component of the audit plan does not include audits of each of the layers, the audit plan taken as a whole may not address the organization's IT-related risk adequately.

In some cases, it may be appropriate to consider all the layers over a period of time (i.e., over multiple years on a rotational basis) rather than covering all layers within a single year. Rotational plans that extend beyond three years could be inadequate due to the high rate of change in the IT environment.

How many resources should be allocated to each layer? Where should they be allocated? Answers to these challenging questions are natural outcomes of the risk assessment processes, combined with the auditor's judgment and strategic analysis. Regardless of the specific resource allocation, all IT layers should be considered.

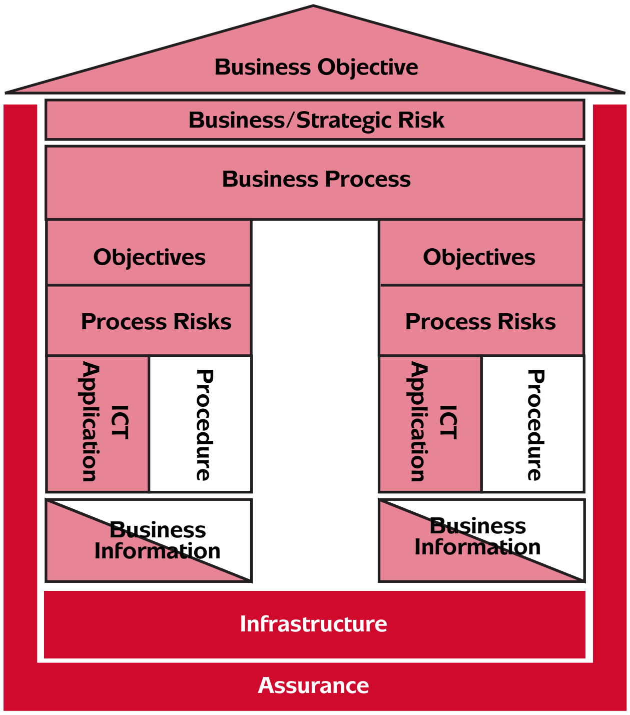
What Are the Layers?

Below is a graphic depiction of IT within an organization. Each organization is different, but this picture will help identify the critical IT processes in most organizations. Other IT architecture models can be considered and are referenced in Appendix A.



ICT is an acronym that stands for Information Communications Technology. The key layers to consider are:

- IT management.
- Technical infrastructure.
- Applications.
- External connections.



Note that this graphic does not define the categories of the audit plan. When specific IT audit work is planned, it may be organized into categories based on the organization's processes, or by a standardized framework. This graphic is designed to help think about how IT relates to the organization and to assure audit resources are allocated to each layer. Organizing specific audits is left to the judgment of the CAE.

IT Management

IT management comprises the set of people, policies, procedures, and processes that manage IT services and facilities. The integrity of processing and data is highly contingent on the specific tasks administrative personnel perform on a regular basis. Therefore, this component includes system monitoring, programming, planning, vendor management, problem and incident management, change management, IT project management, disaster recovery, security management, IT governance, etc.

These functions are business processes and will have a similar audit approach. The auditor is looking at people and tasks rather than a technical system setting. In some cases the management processes address technical facilities and the audit will include both the facilities and the management process. Some of the controls over these processes may be quite technical and may require specialist skills, but the skills of any experienced internal auditor will be largely sufficient.

Technical Infrastructure

This layer essentially refers to the technology that underlies, supports, and enables primary business applications. In general, this includes:

Operating Systems – The set of programs that tell the computer systems how to function. Examples include Z/OS, UNIX, Windows, and OS/400. All programs and files are managed by the operating system. Actions performed at the operating system level generally bypass most security and controls that exist at the process level.

Files and Databases – All electronic business data, critical or otherwise, are held in files, which may form part of a database somewhere in the environment. Databases (which may be a single file or a group of files) comprise tables containing data, relationships between data items, and indexes to the data items. The flexibility of database structures means they are used for most business processing and reporting applications. Examples include Oracle, MS SQL Server, and DB2. Actions performed at the database level also tend to bypass most controls that exist at the process level.

Networks – For data to flow through an organization, it must have a method of traveling, whether across a wire, a fiber optic cable, or wireless system. The network consists of: physical components such as cables; devices that manage the movement of network traffic such as switches, routers, or firewalls; and programs that control the movement of data. The integrity of the network plays an important role in ensuring the completeness and accuracy of the organization's business data. For example, if a warehouse worker preparing to ship a product scans it with a barcode scanner, how does that transaction get recorded on the general ledger? Answer: It travels across the network and is processed. But what if it does not travel across the network? What if it is changed along the way, or disappears altogether? How would the organization know?

Data Centers – Computer equipment is housed within data centers and server rooms, which provide the physical infrastructure, physical security, and environmental controls required to safeguard technical infrastructure and applications.

Technical infrastructure audits focus on review of technical configuration settings in combination with their associated management processes.

Applications

Business applications are programs that perform specific tasks related to business operations. They are an integral part of the business process and cannot be considered separately from the processes they support. Applications, generally, can be classified into two categories:

Transactional applications consist primarily of software that processes and records business transactions. Examples include sales order processing, general ledger recording, and warehouse management.

Support applications are specialized software programs that facilitate business activities but generally do not process transactions. Examples include data warehouses, email programs, fax software, business intelligence software, document imaging software, and design software.

The bulk of IT audit attention will be oriented toward transactional applications. However, some support applications, such as those that support external reporting or applications that control machinery, may be high risk as well.

Internal audit needs to continuously assess the organization's emerging risks and identify the required audit response. The specialist knowledge required for some aspects of IT may make this a complex process.

External Connections

The corporate network does not operate in isolation. It is almost certainly connected to many other external networks. The Internet is the one that most readily comes to mind, but many times auditors make the mistake of stopping there.

In fact, it is highly likely that the corporate network is connected to many other networks (including cloud computing and software as a service providers). For example: Does the organization do business through EDI? If so, the corporate network is probably connected to an EDI provider network, or perhaps directly connected to the network of a trading partner. Does the organization use any third-party warehouse providers? If so, the two networks are probably linked together. The risks associated with other corporate networks and the controls that can be applied differ from those that may apply to Internet connections.

As organizations continue to automate key processes, more access to the corporate network is granted to outsiders, often via the Internet. Consider, for example, the ability to look up the account status of a credit card or the shipping status of a package. Customers who perform those activities are likely entering those organizations' internal networks via the Internet.

The issue is that external networks are not under the control of the organization and therefore should not be trusted. All communication to and from external networks should be tightly controlled and monitored to the extent required by the level of risk to the organization. It can be challenging to define IT audit procedures to address this risk, because the organization can only audit what it can control. Thus, it is critical to audit the entry and exit points, at a minimum.

5. Risk-based Approach

A risk-based approach applies to all activities of internal audit management including building and maintaining the audit program and staffing and executing IT audit work. This section will concentrate on the IT portion of the risk assessment.

The internal audit portion of the assessment of IT-related risks identifies IT-specific audit work with the highest potential value in the relevant time period, to be evaluated for inclusion in the audit plan. There is no need for a distinct methodology for addressing IT-related risks. Using the same methodology for all risk types is important to ensure that there is one consistent internal audit risk assessment process that is used across the internal audit function.

Risk is usually expressed as a combination of the consequence of an event and the probability of that consequence occurring. It often is difficult to calculate risk exactly, especially when considering very unlikely event chains. Both factors should be used for the risk assessment. and information from statistics and error logs can give good input for these assessments. In some cases it is sufficient to consider the consequences (e.g., the loss of a data center) — without needing to know either the event paths that might bring it about or the likelihood of occurrence — to know that the risk needs attention.

Often, it will be possible to define general risk terms that apply to all types of IT audit work but with different manifestations. Generally applicable measures for the potential exposure could be size and business criticality. For example, the number of business applications a data center supports could describe its business criticality (possibly weighted for importance), and the number of servers it hosts could possibly characterize its size. The size of a project, on the other hand, could be measured with its budget, and its business criticality with the number of entities that the resulting application will support. The number of incidents that are known to have occurred, or the organization's past success with projects could measure the likelihood of occurrence.

In addition to the collection of data, another important source for assessment of IT-related risk is performing interviews with important stakeholders such as IT management, business management, and experts. Interviews can help to quantify risks that are difficult to measure directly.

It is critical to consider the high rate of change in technology and society's use of it. This requires frequent updates of any risk assessment. A vivid example of this is the rapid growth in importance of privacy issues driven by the availability and usage of social networking. For a more detailed description, please refer to The IIA's Practice Guide, Auditing Privacy Risks.

Finally, for a more detailed description of the assessment of IT-related risks, please refer to GTAG *11: Developing the IT Audit Plan*.

6. Audit Universe

To form a basis for the allocation and budgeting of IT audit resources and to ensure the coverage required to provide reasonable assurance over IT-related risks, the audit universe should identify those reviews that involve IT and may require IT audit specialist skills.

There should not be a separate IT audit universe. IT audit work should be embedded within the overall audit universe, because there are strong interdependencies between IT and the business processes it supports. For example, IT business applications will typically be in the overall audit universe as part of a business process. The audit universe should be structured in a way that allows for grouping by audit types and therefore allows the identification of reviews requiring IT specialization (e.g., audit of IT applications and IT processes).

For the grouping/structuring processes, one generally relies on the structure used by IT management. This can usually be found in the IT strategy. Ideally, this structure is based on widely used frameworks like COBIT, ITIL, COSO (for details, see section 8), and others.

In a complex organization, an overly detailed audit universe could easily contain thousands of IT-related elements. Such an audit universe is difficult to manage because of the effort it takes to produce it, keep it up to date, and perform a risk assessment on all elements. If, on the other hand, the IT-related elements are too general, then it probably will not be a sufficient basis for the creation of the audit plan.

Some important principles that should be followed when developing the IT components of the audit universe include:

- Ensure completeness by including all relevant objects, including those that might not be obvious (e.g., outsourced activities like offshore service providers, business related elements with strong IT relevance, and strongly automated business processes).
- In the update process, put particular emphasis on new and emerging topics. Current examples are cloud computing, social media, or use of mobile devices.
- The audit universe should not be kept secret but shared with relevant partners (e.g., IT and other management) to encourage input and suggestions for improvement.

For more detailed information, please refer to *GTAG 11: Developing the IT Audit Plan*.

7. Competencies and Skills

A recurring theme in many organizations is the gap between the use and dependence of IT systems and the resources used to identify and manage the risks created by these technologies. It is therefore vital that the internal audit function gives due consideration to information systems when evaluating governance, risk management, and control processes.

One of the key components for a CAE to address these risks is to ensure necessary competence in the audit team. This is supported by the International Professional Practices Framework's (IPPF) Code of Ethics that requires internal auditors to engage only in those services for which they have the necessary knowledge, skills, and experience; and Standard 1210: Proficiency, requiring internal auditors to possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. It is the internal audit activity collectively that should possess or obtain the knowledge, skills, and other competencies needed. The IIA provides an integrated competency framework to help identify the necessary competencies to maintain the internal audit activity.

The CAE should obtain competent advice and assistance if the internal audit department lacks the knowledge, skills, or other competencies needed to perform all or part of an IT audit. The resources assigned to execute planned audits play a critical role. For example, the skill set needed to audit a firewall configuration is vastly different from the skills needed to audit accounts payable configuration tables in a database. It is critical to match the skills needed to perform a particular audit with the appropriate auditor. Directionally, the CAE needs to understand that no auditor will be able to do all IT audit work and that an audit function in many cases will need to have some auditors more aligned with applications and others more aligned with infrastructure technologies.

Consequently, a CAE who has a good understanding of the audit universe, the risks created by the use of technology, and the current IT audit skill set on staff should be able to focus his or her recruiting and training efforts accordingly. If the required IT skills and competencies are not available or a decision is made not to develop or hire staff with these skills, the CAE may seek an external service provider to support or complement the internal staff (i.e., outsourcing or cosourcing)[1].

To fulfill the CAE's IT-related responsibilities, there are some key questions the CAE should consider as part of managing competencies and skills for the auditors:

- Are all the organization's IT components included as part of the planning process and have the high-risk areas been identified?
- Is there an overview of the different skill sets needed to audit the organization's IT use and what type of skills does the CAE already possess in his or her audit department?
- Does the audit department have a policy for how to address knowledge gaps (e.g., recruitment, outsourcing, or cosourcing)?
- Do the IT auditors have the required formal education, certifications, and experience? If not, does the department have a plan to address the gap?
- Does the internal audit department offer adequate training for the auditors so that they are knowledgeable about the organization's use of technology, the related risks, and how to effectively perform audits?

[1] For details, please refer to the Practice Advisory 1210.A1-1: Obtaining External Service Providers to Support or Complement the Internal Audit Activity.

8. Executing IT Audit Work

The process for executing IT audit work is, in general, no different than the process for executing any other audit work. The auditor plans the audit, identifies and documents relevant controls, tests the design and operating effectiveness of the controls, concludes, and reports. Because most CAEs are familiar with this overall process, it will not be covered in detail in this GTAG. However, there are some issues related to IT audit work that the CAE needs to be aware of and manage.

Collaboration Between IT Auditors and Other Auditors

Internal audit should strive for a holistic view in its audit execution. There are IT domains that will probably be audited exclusively by specialist IT auditors (primarily IT infrastructure-oriented topics such as data centers, networks, or IT processes such as user help desk), but for reviews of applications, the most value comes from auditing whole value chains including both business and IT. In such types of audits, the focus should be on business objectives and all risks (including IT-related risks) should be evaluated from this perspective. This can be a challenge but also strongly rewarding as it recognizes the dependency of business on IT. As an example, if IT audit work shows that there is no disaster recovery plan in place, IT auditors and operational auditors can work together to describe the impact of the expected downtime in the emergency case on the business (e.g., reduced production level, delays in paying employee salaries, inability to sell any goods). For a mature internal audit organization, it is irrelevant who has the lead on specific audits in such a situation. The focus should be on collaboration to deliver the optimal audit result.

Frameworks and Standards

One challenge auditors face when executing IT audit work is knowing what to audit against. Most organizations have not fully developed IT control baselines for all applications and technologies. The rapid evolution of technology could likely render any baselines useless after a short period of time.

A CAE should be able to start with a set of IT control objectives and, although it would not provide 100 percent specificity to that particular environment, select an appropriate framework.

COSO and COBIT

Where can a CAE find a comprehensive set of IT control objectives? COSO's *Internal Control–Integrated Framework* and *Enterprise Risk Management–Integrated Framework* are frequently referenced sources of information, but are not focused on IT. A COSO-based control environment should be augmented with more detailed IT control objectives to assess the IT control environment effectively. A number of options are available for this.

A widely used IT governance and control framework is the Information Systems Audit and Control Association (ISACA) *Control Objectives for Information and Related Technology* (COBIT), which was originally published in 1994. Version 5.0 of COBIT was released in 2012. COBIT is not intended to compete with COSO or other frameworks, but it can be used to complement them by augmenting the others with more robust IT-specific control objectives.

Policies, Standards, and Procedures

A framework such as COBIT offers a generally accepted set of IT control objectives that helps management to conceptualize an approach for measuring and managing IT risk. Management would generally use such a framework to guide the development of a comprehensive set of IT policies, standards, and procedures. An overview of relevant sources for policies, standards, and procedures can be found in Appendix A.

9. Reporting

CAEs regularly report to key stakeholders such as the board[2], executive management, regulators, external auditors, or the CIO on the results of IT audit work in the same way as other assurance work. For further guidance about how to interact with key stakeholders, please see The IIA's Practice Guide, Interaction with the Board.

As with most audit reports, readers of reports addressing IT audit work can be management several levels above those actually being interviewed or executing the controls. Audit reports should convey the most important information precisely and clearly, so observations or issues are understood and responsible management can react to it. A well-executed good audit is a waste of time and money if management does not implement effective action plans to address the issues and related risks identified. Management generally does not want to read about the audit process that was followed to deduce that something was wrong. They want to know what was wrong, the potential consequence, and what needs to be done about it.

The internal audit function should strive for a holistic view in its reporting. Because most organizations are totally dependent on IT systems, reporting on the risk and controls in an organization's IT environment should be part of a CAE's approach to providing assurance. While there are IT processes and IT infrastructure that can be audited in isolation (and perhaps should be for efficiency reasons), in general, most value comes from auditing whole value chains (including both business and IT). In such types of audits, there can be much greater focus on business risk, which is more easily communicated to management than IT-related risk. IT-related risk ultimately results in business risk; however, the link is not always so clear.

So, from a reporting point of view, what IT audit work should be performed as part of internal audit's assurance? Should an audit of wireless networks be performed; an audit of network architecture and design; or a review of the electronic design application? If the audits are broken up in this fashion, there is a risk that the reporting of audit findings will be related only to details of each individual piece of technology. For some audiences this may be the right thing to do, the board or executive management may not care or understand much about detailed technical issues. They usually want IT audit findings to be tied to business issues. Therefore, the IT audit work should integrate with the process/operational/financial auditors and the procedures they are performing. This will particularly be the case in environments with large integrated ERP applications, where a high number of key process controls are contained within the systems. Remember though, that in some cases auditing will be difficult for central infrastructure components like data centers or wireless networks so it will make sense to perform those audits on individual components. However, risks identified during the audit still need to be translated into business language and business risks.

Reports should be written with the expectation that the audience is knowledgeable but may lack specific experience in the audited area and should not hide the message in verbiage or technical terms. The CAE's goal is to present a clear, understandable, and balanced message.

[2] The term *board* is used as defined in the *Standards* glossary: "The highest level of governing body charged with the responsibility to direct and/or oversee the activities and management of the organization. Typically, this includes an independent group of directors (e.g., a board of directors, a supervisory board, or a board of governors or trustees). If such a group does not exist, the 'board' may refer to the head of the organization. 'Board' may refer to an audit committee to which the governing body has delegated certain functions."

10. Audit Tools

CAEs should look for opportunities to use tools and/or techniques to increase the efficiency and effectiveness of the audit. In general, audit tools require an investment, so the CAE should carefully consider the cost/benefits of any solution prior to investing in the tool. Audit tools can be divided into two general categories: audit facilitators (not described here), which help support the overall management of the audit (e.g., an electronic workpaper management tool); and testing tools, which automate the performance of audit tests (e.g., data analysis tools and CAATS).

IT Testing Tools

Testing tools can automate time-consuming audit tasks, such as reviewing large populations of data. Also, using a tool to perform audit procedures helps establish consistency. For example, if a tool is used to assess server security configuration, all servers tested with that tool will be assessed along the same baselines. Performing these procedures manually allows for a degree of interpretation on the part of the auditor. Lastly, the use of tools enables auditors to test an entire population of data, rather than just a sample of transactions. This provides for a much higher degree of audit assurance.

CAEs should be aware that when acquiring IT audit tools, the same considerations apply as when selecting any business tool (e.g., functionality, support).

Security Analysis Tools

These are a broad set of tools that can review a large population of devices and/or users and identify security exposures. There are many different types of security analysis tools, the most prevalent being network analysis tools:

Network Analysis Tools – These tools consist of software programs that can be run on a network and gather information about the network. Hackers would typically use one of these tools on the front end of an attack to determine what the network looked like. IT auditors can use these tools for a variety of audit procedures, including:

- Verifying the accuracy of network diagrams by mapping the corporate network.
- Identifying key network devices that may warrant additional audit attention.
- Gathering information about what traffic is permitted across a network (which would directly support the IT risk assessment process).

Vulnerability Assessment Tools

Most technologies have a number of standard vulnerabilities, such as the existence of default IDs and passwords or default settings when the technology is installed out of the box. These assessment tools provide for an automated method of checking for standard vulnerabilities.

Such tools can be used for firewalls, servers, networks, and operating systems. Many provide for plug-and-go usage; the auditor plugs in a range of what he or she wants the tool to search for and the tool collates a report of all vulnerabilities identified in that range.

These tools are important for an auditor to run for several reasons, not the least of which is that these are the types of tools a hacker would use to mount an attack against the organization. It is important to note that some of these tools are potentially dangerous to run because they can impact the integrity of the systems they are scanning. The auditor should review the planned usage of any of these tools with the security officer and coordinate the testing with IT management to ensure the timing of testing will not impact production processing. In some cases, the security officer or systems administrators may already be running some of these tools on a regular basis as part of the systems management processes. If so, the results may be able to be leveraged to support IT audit work, if properly designed and executed.

Application Security Analysis Tools

Many large integrated applications have vendor supplied application security analysis tools that analyze user security against preconfigured rules. These tools also may evaluate segregation of duties within the application. The CAE should be aware that most of these tools come with a set of preconfigured rules or vendor-touted "best practices."

11. Conclusion

As new technology-related risks emerge, new procedures are required to manage these risks adequately. There is no question that over the past 15 years, technology has changed the nature of the internal audit function. The risks organizations face, the types of audits that should be performed, how to prioritize the audit universe, and how to deliver insightful findings to boards and senior management are all issues that CAEs should address.

Business strategy guides the identification of the audit universe and risk assessment, determines what is important to boards and management, and what from the current operations is likely to change. It is therefore important for the CAE to understand both the business strategy and IT's role in the organization and the impacts they have on each other.

When the CAE maps the organization's operations and IT infrastructure, he or she is in a unique position to see the impact of various technology and operational relationships in the organization. IT projects are often key elements in driving change in organizations and they often are the mechanism used by management to implement business strategy.

The initial challenges a CAE faces when developing the IT components of the audit plan is identifying the IT activity within the organization. Recognizing that there is a high amount of diversity in IT environments, a CAE can approach the definition of IT by thinking about it in components. While each component is different, each is important. Using a risk-based approach is a general concept that applies to almost all activities of internal audit. The audit universe should embed IT considerations, because there are strong interdependencies between IT and the business.

For a CAE, one of the key components to address these risks is to ensure necessary competence in the audit team. Additionally, CAEs should look for opportunities to use tools and/or techniques to increase the efficiency and effectiveness of the audit. Like any business tool, audit tools require an investment in time and resources, so the CAE should carefully consider the cost/benefits of any solution prior to investing in the tool.

Finally, the process for executing an audit that includes IT risks is, in general, no different than the process for executing any other audit. The auditor plans the audit, identifies and documents relevant controls, tests the design and operating effectiveness of the controls, concludes, and reports. Similarly, CAEs regularly report to key stakeholders such as the board, executive management, regulators, external auditors, or the CIO on the results of IT audit work in the same way as with other assurance engagements.

12. Authors and Reviewers

Authors*:*

Stephen Coates, CIA, CGAP, CISA
Max Haege
Rune Johannessen, CIA, CCSA, CRMA, CISA
Jacques Lourens, CIA, CISA, CGEIT, CRISC
Cesar L. Martinez, CIA, CGAP

Reviewers:

Steve Hunt, CIA, CRMA, CISA, CGEIT
Steve Jameson, CIA, CCSA, CFSA, CRMA

Appendix A: Sources for Standards

Some standards for consideration are:

ISO 27001– The International Organization for Standardization (ISO) published this internationally recognized generic information security standard, which began as a British Standard (BS7799), and evolved into an ISO standard known as ISO 27001. It contains generally accepted best practices on information security management and is useful as a baseline for IT auditors to audit against.
http://www.iso.org

Capability Maturity Model Integration (CMMI) – Carnegie Mellon University's Software Engineering Institute (SEI) has developed the concept of Capability Maturity Models (CMMs) for various processes within an organization, primarily related to the deployment of software. The most recent approach is CMMI.
http://www.sei.cmu.edu

United States Computer Security Resource Center – A division of the National Institute of Standards and Technology (NIST), the United States Computer Security Resource Center provides a comprehensive series of publications that offer detailed information on information security control topics. Sample publications include "Guidelines for Securing Wireless Local Area Networks (WLANs)" and "Guidelines on Security and Privacy in Public Cloud Computing." These standards provide best practices that can be used across all industries.
http://csrc.nist.gov

SysAdmin, Audit, Network, Security (SANS) Institute – One of the most trusted sources for information security education and training in the world, the SANS Institute publishes numerous documents on various aspects of security for various technologies. SANS publications provide a number of specific requirements that an IT auditor can audit against.
http://www.sans.org

The IT Infrastructure Library (ITIL) – ITIL is the most widely accepted approach to IT service management in the world. ITIL provides a cohesive set of best practices, drawn from the public and private sectors internationally.
http://www.itil-officialsite.com

Vendor-specific Standards – Many technology vendors issue security and control guidelines for the technology they produce. SAP, for example, issues a security guide that provides detailed recommendations for securing and controlling the SAP ERP application. These vendor-released standards often do not take security and control considerations to the same level that perhaps a NIST publication might, but they provide a good start. CAEs should check with the vendors of mission-critical systems to see if specific standards are available. In many cases, the vendor may not have released anything, but the user group associated with that technology has (e.g., the different SAP Users' Groups).

Appendix B: IT Architecture Models

Some IT Architecture models and references for consideration are:

The Abu Dhabi IT Architecture & Standards Framework – Based on an eight-layer framework, this covers all aspects of an IT environment and includes: Business, Access & Presentation, Application, Data, Integration, Infrastructure, Security, and Operations.
http://adsic.abudhabi.ae

AndroMDA – Modern enterprise applications are built using several components connected to one another, each providing a specific functionality. Components that perform similar functions are generally grouped into layers. These layers are further organized as a stack where components in a higher layer use the services of components in a lower layer. A component in a given layer will generally use the functionality of other components in its own layer or the layers below it.
http://www.andromda.org

TOGAF® – An Open Group Standard is a proven enterprise architecture methodology and framework used by the world's leading organizations to improve business efficiency.
http://www.opengroup.org

GTAG®

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance.

Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

IIA®

The Institute of
Internal Auditors

www.globaliia.org

130091