IT Governance and Strategy

Practical guidance for managers on how to prepare for successful audits
Research Sponsors

Symantec

Tripwire
About the IT Compliance Institute

The IT Compliance Institute (ITCi) strives to be a global authority on the role of technology in business governance and regulatory compliance. Through comprehensive education, research, and analysis related to emerging government statutes and affected business and technology practices, we help organizations overcome the challenges posed by today’s regulatory environment and find new ways to turn compliance efforts into capital opportunities.

ITCi’s primary goal is to be a useful and trusted resource for Information Technology professionals seeking to help businesses meet privacy, security, financial accountability, and other regulatory requirements. Targeted at CIOs, CTOs, compliance managers, and information technology professionals, ITCi focuses on regional- and vertical-specific information that promotes awareness and propagates best practices within the IT community.

For more information, please visit: www.itc institute.com

Comments and suggestions to improve the IT Audit Checklists are always encouraged. Please send your recommendations to editor@itc institute.com.

Table of Contents

2 Executive Overview

3 Introduction to IT Governance and Strategy

4 What Is IT Governance?

6 What Are the Benefits of Sound IT Governance?

7 The Auditor’s Perspective on IT Governance and Strategy

7 Why Audit?

7 Who Is Responsible for IT Governance?

10 Management’s Role in the Audit Process

11 What Auditors Want to See

12 Auditors Like...

12 Auditors Don’t Like...

12 How Companies Help (or Hinder) Auditors

13 Who Should Talk to the Auditors?

14 IT Governance and Strategy Audit Checklist

14 Audit Planning

14 Audit Testing

15 Processes

15 Steps

16 Controls for IT Governance and Strategy

19 Audit Reporting

20 Preparing for an Audit

21 Communicating with Auditors

22 Appendix—Other Resources
Executive Overview

What Is the IT Audit Checklist Series?
The IT Ci IT Audit Checklists are a series of topical papers that provide practical guidance for IT, compliance, and business managers on preparing for successful internal audits of various aspects of their operations. In addition to helping managers understand what auditors look for and why, the IT Audit Checklists can also help managers complete proactive self assessments of their operations, thereby identifying opportunities for system and process improvements that can be performed in advance of an audit.

What Is This Paper About?
This paper, “IT Audit Checklist: IT Governance and Strategy,” supports an internal audit of the organization’s IT leadership and high-level planning resources, systems, and processes. The paper includes guidance on assessing the completeness, effectiveness, and sustainability of existing IT governance and strategy; guidance on supporting effective IT leadership; and information on ensuring continual improvement of governance efforts. The paper is intended to help IT, compliance, business, and audit managers prepare for an audit of high-level processes and resources and to provide concrete tools managers can use to ensure that the audit experience and results are as beneficial as possible to both IT leaders and the company as a whole.

Paper Contents
According to the IT Governance Institute (ITGI), “IT governance is the responsibility of the Board of Directors and Executive Management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategy and objectives.”1 This IT Audit Checklist focuses on measurable IT practices that strategically address the growing complexity and risk engendered in IT operations. In addition to providing general insight into audit goals and processes, the paper suggests specific control objectives drawn from regulatory and best-practices documents.

While other papers in IT Ci’s Audit Checklist series offer specific guidance on IT functional realms, such as information security, this paper explores IT objectives and practices that allow executives and leaders to form appropriate governance plans, strategies, purchase decisions, and policies that not only meet compliance goals, but enable enterprise risk management and support competitive business efforts, as well. Generally, IT governance controls include, but are not limited to do:

- Leadership and operational structures
- Measurement and management of IT resources
- IT architectures and models
- Investment management

Audits and reviews of these control areas advance the goal of IT oversight and promote continuous improvement and success of technology-enabled business processes and IT systems and functions. In designing and meeting corporate objectives, neither auditing nor IT can afford to be a black box. Both functions must cooperate to recognize their common goals of reducing corporate risk, improving IT and business processes, and supporting ethical, profitable corporate performance.

Additional resources that complement the content of this paper are provided in the appendix.

Introduction to IT Governance and Strategy

IT has always played an ambiguous role in business success. Is it a mechanism or driving force? Does it define or merely facilitate business processes? Does it warrant top-level consideration at all? The answers to these questions have traditionally depended on corporate philosophy and how well IT was integrated into business goals and strategies.

But if IT’s role in business gain is ill defined, its culpability in business loss is well recognized. Information systems and processes represent the beating heart of corporate communications, accounting, manufacturing, supply chain management, and other critical business processes. In many companies, management has learned the hard way that failure of IT is tantamount to business failure; thus, IT has earned its own audit discipline. In a business climate where risk commands almost as much managerial mindshare as profit and growth did just five years ago, internal audits cannot ignore—and, in fact, must constantly strive to better understand—IT’s business role and risk factors.

Prior to the spectacular collapse of Enron, WorldCom, Tyco, and other corporations between 2001 and 2003, financial auditing was relatively perfunctory. Before the 2001 terrorist attacks in the US, customer recognition was merely good business practice. And prior to the ChoicePoint security breach in 2004, privacy laws were relatively scarce. But these and other corporate scandals and catastrophes loosed a deluge of preventive laws, including Sarbanes-Oxley (SOX), US-state and to international data protection acts, and the USA Patriot Act (USAPA). Collectively, these new rules have changed risk management from a by-product of compliance to a core requirement.

SOX in particular has revolutionized IT auditing. In preparing for their initial audits, corporate executives found they couldn’t certify the integrity of financial information without understanding the applications and systems that stored financial data. SOX’s auditing oversight board, the PCAOB, explicitly recognized this dependency with more than 20 references to information technology in its primary guidance, “Auditing Standard No. 2.”2 Auditors questioned. Few companies could adequately answer. By 2003, it was apparent that almost everyone—from CFOs to regulators and even financial auditors—had underestimated how much financial management relied on IT underpinnings. In 2004, it became clear that financial auditors lacked the technical knowledge necessary to perform effective IT audits. In 2005, the Information Systems Audit Control Association (ISACA) reported that the number of people applying to take its Certified Information Systems Auditor (CISA) exam doubled from the previous year.

But, as companies and auditors continue to learn, the challenges of IT auditing go beyond technical competency. Misalignment of communications between auditing, business management, and IT management plagues many companies. Definition of internal systems and controls continues to be a substantial capital and resource cost. And appropriate scoping of audits according to control impact and risk relevance is an issue endemic to both financial and IT audits, but particularly acute for IT management, which often oversees several thousand (or more) policies and processes.


www.ITCinstitute.com
As companies have recognized their reliance on IT and the need for appropriate IT oversight, the internal audit function has increased the frequency and comprehensiveness of its assessments. Regulatory guidance to improve the risk relevance of audits has also helped to align audit-management communications. Neither auditing nor IT can afford to operate as a black box. Both must cooperate to recognize their common goals of identifying and reducing risk, improving processes, and supporting ethical, profitable corporate performance.

Successful IT governance audits require definition and balance. Auditors must help management understand compliance scope, but management is responsible for defining the risks and risk materiality that ultimately determine audit scope. Management must work with auditors to identify risk existence, materiality, and potential remediation. Auditors should also help management understand how to demonstrate seemingly intangible concepts such as leadership and responsibility in terms of concrete policies and processes. And management must help auditors understand controls and assess their effectiveness.

What Is IT Governance?

According to the IT Governance Institute (ITGI), “IT governance is the responsibility of the Board of Directors and Executive Management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization’s IT sustains and extends the organization’s strategy and objectives.”

Whereas corporate governance encompasses all organizational assets and processes, IT governance focuses chiefly on the IT organization. IT managers are answerable to the board for risks and audit findings associated with their organization. However, as an integrated component of corporate governance, IT management cannot ignore the bigger picture. It must consider not only IT goals and responsibilities, but technology’s integrated role in corporate processes.

With this big picture in mind, IT governance and strategy encompasses the core definitions, structures, and processes that shape all IT efforts and systems. Auditable functions of IT governance include:

1. Definition of what the IT organization is and does, including values and goals
2. IT risk definition and management
3. Definition of roles and responsibilities, including leadership structures
4. Strategic planning, monitoring, and continual improvement
5. Oversight of standards, policies, and procedures
6. Oversight of technical foundations, such as IT infrastructure, architectures, a semantic baseline or glossary, and data management
7. Asset management, including staff, systems, media, networks, and content
8. Resource planning
9. Investment management

Every IT practice, program, and procedure is guided by these functions. Information security, business continuity, records management, and all other strategic initiatives live and die by their effectiveness.

In general, governance principles, whether in IT or business, are somewhat canonical. However, corporate governance guidance issued by international organizations can provide a foundation for IT governance

---

principles. Over the past five years, governance research groups and standards bodies have increasingly updated their guidance with deference to IT. And IT-specific frameworks and guidance have been developed independently and as a complement to existing corporate governance documents.

- “The Principles of Corporate Governance,” issued by the Organisation for Economic Co-operation and Development (OECD)⁴. Although designed for public-company oversight, the principles can be broadly applied to non-public companies and internal organizations. In December 2006, the OECD also issued an audit guide, “Methodology for Assessing the Implementation of the OECD Principles on Corporate Governance,” an assessment framework with governance principles.

- The UK Financial Reporting Council’s “Internal Control: Revised Guidance for Directors on the Combined Code,” conventionally called the Turnbull Guidance, offers a more specific approach to maintaining and reviewing a system of internal control.

- “Enterprise Risk Management—Integrated Framework,” commonly called “COSO,” after its publisher, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)⁵ is similar in outlook and focus to the Turnbull Guidance, but includes a more robust and explicit internal control framework. COSO is recognized by the US SEC and PCAOB as an approved control framework for SOX.

- “Organizational Governance: Guidance for Internal Auditors,” a position paper from the Institute for Internal Auditors (IIA), ties corporate governance principles to audit goals and roles. Much of the content can be used as a model for IT governance and auditing.

- CobiT, published by the Information Systems Audit and Control Association (ISACA), is widely considered the leading framework for IT controls.⁶ CobiT 4.0 covers 34 high-level objectives, comprising 215 control objectives in four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring and evaluation. ISACA also publishes correlative audit guidelines, management guidelines, and an implementation toolset.

CobiT is perhaps the most widely used IT control framework, since it spans the gamut of IT; offers mappings to other governance standards; and is supported by many published materials, education, and a vast user community.

Adoption of CobiT as a primary best-practices standard is also facilitated by several mapping documents that can help IT managers align their processes, governance, and regulatory response. ISACA’s supporting document IT Control Objectives for Sarbanes-Oxley, 2nd Edition contains a general map of CobiT processes to PCAOB Auditing Standard No. 2. In May 2006, ISACA issued CobiT Mapping, Overview of International IT Guidance, 2nd Edition, which provides a general comparison of COSO and CobiT frameworks.

In January 2007 ISACA also published a map of CobiT and the IT Infrastructure Library (ITIL) from the UK Office of Government Commerce. By aligning the two UK documents, it is possible to map COSO to ITIL at a high level, and therewith compile a framework that aligns enterprise risk management principles with IT controls and, finally, fairly narrowly defined IT services. Links to each of these documents is included in the appendix of this paper.

---

⁴ Citations and links for the resources mentioned in this section are included in Appendix A

⁵ Since the passage of SOX, Turnbull and COSO have emerged as the major pillars of compliance and risk management. From an IT perspective, COSO is more accessible than Turnbull, since it is more widely documented and has been approximately mapped to an IT control framework, Control Objectives for Information and related Technology (CobiT), published by the Information Systems Audit and Control Association (ISACA).

⁶ Although COSO is officially endorsed for SOX compliance, CobiT has received no official endorsement.
While most companies had IT governance processes and some controls in place long before they were required by SOX and other regulations, the adoption of frameworks to organize and round out governance and control efforts is a governance best practice. Frameworks such as CobiT provide a comprehensive overview of control objectives against which to standardize and align IT governance and auditing efforts.

What Are the Benefits of Sound IT Governance?

Sound IT governance addresses the growing complexity and threat that are the hallmarks of IT operations. Compared to just a few years ago, business processes are more complicated; technology is more powerful, functional, and ubiquitous; and attacks on corporate systems, from within and without, are more frequent and sophisticated.

In general, IT governance ensures that the company’s technology assets and the information they contain are known, available, credible, and protected. Since legislation seeks the same goals, good IT governance must be aligned with regulatory compliance. Beyond that, however, the business benefits of sound IT governance and strategy include:

1. Better alignment between business and IT strategy
2. More informed, practical decisions about technology investments
3. Greater agility in meeting shifting business demands, and a stronger foundation for innovation
4. Better measurement and control of costs related to information systems and their protection
5. Lower risk of non-compliance with regulatory requirements
6. Lower risk of serious business disruption from events
7. More healthy organizational relationships and reputation with directors, business staff, customers, and partner organizations

Recognizing the ROI of IT governance is an important step in meeting governance goals. Many governance controls such as network mapping, master data management, and asset inventories, have substantial costs. While good IT governance might be touted as its own reward, the ability to tie its concrete costs to equally concrete returns is itself a good IT governance practice.
The Auditor’s Perspective on IT Governance and Strategy

Why Audit?

Audits are opportunities for companies to improve, based on auditor analysis and advice. To preserve the integrity and authority of audits, auditors maintain a delicate distinction between offering advice and making decisions.

For each organization, the scope of auditor responsibility should be documented in the company’s internal audit charter and be approved by the audit committee. Because every organization has different goals and objectives—and certainly different issues and challenges—there is no one-size-fits-all audit process, nor one audit approach, that fits all situations.

Historically, corporate governance has focused primarily on broad topics of leadership, management, ethics, and reporting. IT governance audits encompass many of the same issues and can include business plans, documentation and measurement of objectives, organizational reporting structures, contract management, and industrial and regulatory monitoring. It also has a significant technology component. For example:

- Does the organization have an information architecture model?
- Do hardware and software acquisition plans exist?
- How is e-content (including intranets, Web sites, blogs, and wikis) managed?
- How are investments and development projects evaluated and do they meet business requirements?
- How does the IT organization ensure system continuity in case of disruptive contingencies?

Who Is Responsible for IT Governance?

The board of directors, IT executives, business executives, and internal auditors all have significant roles in IT governance assurance and the auditing of IT governance and strategies. The big question for many companies is how these stakeholders should work together to ensure that everything that should be done to protect sensitive information is being done—and that the company’s information assets are protected appropriately.

1. The board of directors must provide oversight at a level above IT executives. The directors’ role in IT governance is to ask executives the right questions

---

and encourage the right results. Directors must set an appropriate tone at the top, making executive management aware of their oversight and ensuring they have adequate information to make intelligent decisions about IT strategy and direction. To this end, many boards establish IT committees, which include representatives from both IT and business organizations. The board also has a role in setting the IT governance culture, which includes organizational values and attitudes.

According to ITGI, boards should guide IT management to deliver measurable value by: 1) delivering solutions and services with the appropriate quality, on time and on budget, 2) enhancing reputation, product leadership and cost-efficiency, and 3) providing customer trust and competitive time-to-market.\(^8\)

2. **IT executives** work with the board to define IT identity characteristics. These can include the IT organization’s business plan and/or model, expectations and commitments, and vision. Chief information officers (CIOs) and chief security officers (CSOs) should understand the business organization well enough to bridge the gap between IT and senior business managers or the board.

IT executives look both into and outward from their organization to assess the impact on IT of industry norms and trends, regulatory changes, contractual obligations, even environmental threats. Internally, executives ensure that objectives and strategies are supported and understood across the organization. Finally, by subjecting IT processes, resources, and leadership to audit and board review, IT executives advance the goal of corporate oversight and promote its continuous improvement and success.

3. **IT managers** marshal many of the requirements of IT governance, ensuring internal compliance with leadership mandates and drafting policies and procedures that support strategic goals. IT managers are also the eyes and ears of the IT organization. They are responsible for reporting up to executive management. And, when controls fail, IT managers are generally responsible for drafting remediation plans that meet governance requirements.

4. **Business executives** must have some insight into and influence on IT governance and programs, since business managers are ultimately accountable for the results of the business processes enabled by IT systems. Managers should review IT strategy to ensure it is appropriate, despite ever-changing risks and business requirements. This is, in fact, a form of auditing IT governance. And managers who own business-unit information must also help define their IT requirements based on business objectives, the significance of the information involved, legal requirements, and the seriousness of risks associated with data integrity and security. Especially if the IT organization reports to the CEO or other business leader, that office is responsible for providing resources and organizational structure to support IT strategy.

5. **Internal auditors** provide strategic, operational, and tactical value to IT leaders. For example, the internal auditing function:

- Informs the board and IT executives as to whether business and IT staff understand the importance of governance objectives and strategy. Auditors can tell IT leaders whether staff is adhering to IT policies, whether key information assets and systems are sufficiently secure, whether business continuity programs are sufficient, whether governance efforts continually strengthen IT performance, whether resources are sufficient, and whether policies are reasonable. In brief, internal audits assess the state

\[^8\] Board briefing on IT Governance, p 17 (2003). IT Governance Institute. [http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance26964_Board_Briefing_final.pdf](http://www.isaca.org/Content/ContentGroups/ITGI3/Resources1/Board_Briefing_on_IT_Governance26964_Board_Briefing_final.pdf)
of the IT governance environment and recommend improvements.

- Independently validates that the organization’s governance and strategy are proactive and effective against fraud, information security threats, and business disruption. To provide this level of assurance, internal auditors may compare current organizational practices with industry practices and regulatory guidelines.

In addition, the auditing function should complement, but never replace, management’s responsibility to ensure IT security controls are operating effectively. To fulfill an audit’s potential, internal auditors need to: 1) know what they are doing (have the knowledge and skills to perform appropriate audits); 2) understand both technical and the business environments; 3) know what to ask for from the board, executives, and managers; and 4) complete regular and ongoing training to stay on top of new guidance and standards of practice.

Of course, auditing provides only a reasonable level of assurance. Auditors cannot provide an insurance policy against any fault or deficiency, particularly in regard to activities that cannot be totally controlled, such as collusion and management override.

---

**IT GOVERNANCE AND STRATEGY RESPONSIBILITIES**

**BOARD OF DIRECTORS**
- Provide oversight: ask the right questions, encourage the right results
- Set IT strategy and direction with executive input
- Define IT governance culture

**IT EXECUTIVES**
- Work with board to define IT business plan/model
- Assess impact on IT from internal and external factors, including industry trends, regulations, contracts, etc.
- Ensure objectives and strategies are supported and understood across the organization
- Subject IT processes, resources, and leadership to audit and review to promote continuous improvement and success

**IT MANAGERS**
- Ensure internal compliance with leadership mandates via policies and procedures
- Report to executives regarding success/failure of implementation of strategic goals
- Draft and implement remediation plans to meet governance requirements

**BUSINESS EXECUTIVES**
- Understand, review, and help define IT strategy to ensure it supports business requirements
- Provided resources and organizational structure to support IT strategy

**INTERNAL AUDITORS**
- Assess the state of IT governance environment and recommend improvements
- Validate governance and strategy efforts and compare current practices to industry standards
- Recommend improvements
Management’s Role in the Audit Process

An internal audit engagement typically has three phases: planning, testing, and reporting. Management has an important role in each phase:

- **During planning**, management should first focus on the audit plan (the auditor’s “road map”) and ensure that managers understand and are in general agreement with the audit purpose, focus, and approach. An open, positive discussion with the audit team regarding these defining factors helps management and the audit team communicate their expectations up front. Audit planning should focus on critical or sensitive risks, but all risks should be considered. To this end, active involvement by management in audit planning is vital to the overall success of an internal audit.

Management should also discuss the evaluation criteria auditors will use in assessing IT governance. Finally, managers and auditors should broadly discuss audit testing, although auditors must have the authority and discretion to select tests they deem appropriate.

- **During testing**, management facilitates auditors’ access to relevant people and systems. Management confirms the audit results, not re-performing the actual tests, but verifying processes and data in order to gain confidence in the audit findings. Where management has deployed alternative or compensating controls, it should show how the controls are adequate to satisfy control objectives. Auditors should assess compensating controls according to whether they address identified risk. Adhering too rigidly to a control “checklist” or prefabricated audit framework can introduce unnecessary cost and delay into the audit process and ultimately undermine the audit’s goals.

The audit team leader and senior executives of the areas being audited should meet regularly throughout the audit process—usually weekly and at least once a month—to discuss audit progress, identified issues, and potential actions.

An open, transparent dialogue between senior members of both management and the audit team can avert many misunderstandings and resolve disputed findings before they find their way into an audit report. The audit team should communicate critical findings to management as early as possible, even outside of the established meeting schedule. These findings may also be reviewed during regular meetings, but prompt notice is necessary and usually appreciated.

- **During reporting**, management receives and reviews the findings of auditors, plans and develops corrective actions, and implements change.

Although most internal audits begin with this cycle, auditing is often an ongoing, non-linear process. As PCAOB Auditing Standard No. 4 indicates, the discovery of a material weakness is just the first step in many communications that auditors and management might have about a particular control. In addition, many companies are moving towards continuous audits through which automated control monitoring and reporting test control effectiveness on an ongoing basis.

---

What Auditors Want to See

Audits exist to assess how well a business unit or program meets the performance goals of the organization, as dictated through policy by the CEO, CFO, board, and investors. Accordingly, the managerial goal in auditing is not simply to “make auditors happy,” but to demonstrate how well operations, controls, and results meet the needs of the business. During audit planning, managers help auditors to design an audit process that truly reflects business strategies and goals. Thus, the managerial response to auditors throughout the audit process—planning, testing, and reporting—is for the benefit of the business, not its auditors.

Auditors exist to provide the board and senior management with an objective, independent assessment of a business unit or program (such as information security), including what they see as key opportunities for improvement. To prepare their opinions and conclusions, auditors need to review and assess evidence of sound IT governance. If auditors can demonstrate performance, verify the efficacy of policy and policy adherence, and show that accountability has been established and is working, they should produce a positive audit report.

Accordingly, auditors and managers should work to help each other reach common goals—auditors striving to earnestly, honestly, and completely assess program effectiveness, and management working to help auditors make valid assessments. In that vein, there are some typical program characteristics and managerial processes that auditors do and don’t like to see. As in all aspects of audit and risk management programs, auditor likes and dislikes vary by company; however, the following list itemizes typical indicators of good and bad audits.

Managers and auditors should work together throughout the audit process to ensure that auditors pursue appropriate goals and have proper insight into IT and business processes. Good communication throughout the audit process helps ensure that audit findings are relevant and can be used to benefit the company.
Auditors Like...

- Good governance characteristics, such as an ethical culture, atmosphere of open dialog, and absence of fear as a motivator
- Organized, clear, and up-to-date documentation
- Regular managerial analysis of operating results
- Management actions based on facts and actual results
- Documentation of the chain of command and roles and responsibilities, such as up-to-date organization charts and the related job descriptions
- Timely investigation and clearance of reconciliation items within key accounts
- Supervisory review of critical performance reports
- Consistent understanding and use of policy and procedures, from senior management through frontline staff, with no substantial misunderstandings
- Good management practices—planning, direction, monitoring, reporting, etc.
- A balance of short- and long-term focus, for both objectives and results
- Staff development, in terms of knowledge, skills, productivity, and other metrics
- An engaged workforce and management team

How Companies Help (or Hinder) Auditors

- (Not) having requested documentation available at the prearranged time
- (Not) meeting deadlines and (not) providing needed documentation
- (Not) communicating at an appropriate managerial level
- (Not) having administrative support when it’s needed
- (Not) forecasting audit requirements and (not) responding dispassionately to auditor requests
- (Not) providing accurate documentation
- (Not) informing relevant staff about the audit and its goals
- (Not) having an audit charter for the internal audit function

Auditors Don’t Like ...

- Interviewing defensive or uninformed executives
- Wading through piles of disorganized documentation
- Managers who can’t or won’t comprehend the level of risk they are incurring
- The opposite of the “like” items listed above
Who Should Talk to the Auditors?

An efficient audit process depends on effective communication between auditors, managers, and workers. Management and auditors should strive to balance efficiency (having a minimal number of staff dealing directly with the auditors) with the need for “open access” to management and staff by the audit team (when needed).\(^\text{10}\) Obviously, it is impractical and unproductive for both teams to put too many staff in front of auditors. Instead, management should:

- Provide knowledge of operations through several informed “point” people to interact with auditors. A “short list” of interviewees within the program area being audited can more quickly answer auditor queries and provide better continuity of audit support.
- Allow ready access to all management and staff, if required by the audit team to gain a clearer picture of overall operations.
- Work with the audit team to draw up a staff interview schedule as part of the planning effort. Update the schedule as necessary during the audit fieldwork phase, if circumstances change.

In many situations, a single point of contact for each audited program provides the vast majority of documentation to the audit team. The role of that individual—and, indeed, for all auditor contacts—is to ensure that the audit team receives accurate and adequate information for the task. Auditors still use their professional judgment to determine if and when additional sources of information (other staff interviews) are required. The audit team also conducts a variety of audit tests, if necessary, to confirm their audit analysis.

\(^{10}\) The audit team is always expected to ensure all their interactions (with all staff) are professional and result in a minimal disruption.
An audit’s goals, scope, and purpose determine appropriate audit procedures and questions. An audit of information security should determine that key risks to the organization are being controlled, that key controls are operating effectively and consistently, and that management and staff have the ability to recognize and respond to new threats and risks as they arise.

The following checklist generally describes IT governance audit steps that management might follow in preparation for and during an audit. The list does not attempt to itemize every possible information security objective, but rather to provide general guidance on defensible controls and a logical control hierarchy.

Audit Planning

During the audit planning phase the audit team determines the scope of the audit and develops an initial draft of the internal audit plan. Other planning steps include:

- Managers of the information security program and other appropriate executives meet with the audit team to review audit program steps and define key players and necessary resources
- Management collects program documentation in preparation for audit
- Management supports a preliminary survey of the information security program (by the internal audit team)
- The audit team drafts the internal audit program plan
- Management and board members provide feedback on the draft plan

Audit Testing

Management has a responsibility to ensure that audit testing is productive. The audit team performs tests to independently assess the existence and effectiveness of the IT governance program. Although the audit team ultimately determines the nature of these tests and the extent of testing, such as documentation and sample sizes, management should engage auditors in discussions about their testing methods and goals.

In tone, management should try to strike a balance, neither entirely deferring to the audit team nor micromanaging the internal audit efforts. The key is to provide productive input on the evaluation methodology before audit management signs off on it.

As the testing phase winds up, the audit team prepares summaries of its key findings. IT executive and managers should be prepared to provide feedback and comments on audit summaries, prior to the more final, formal audit report.

Proactive communication, candor from all parties, and thorough documentation can prevent many surprises and conflicts that might otherwise arise during the testing phase; however, managers might still disagree from time to time with audit results. Management should strive to provide solid evidence—not just argument—that supports its contrasting position. Facts are the most successful tool for swaying an adverse opinion before the audit report is finalized.

Since the audit report often forms the basis of future security focus and investment, management should ensure that every audit point raised—and its related recommendation—is relevant and valid. Likewise, every action plan proposed by managers or auditors should be achievable, appropriate, cost effective, and able to produce lasting effect.
Audit Testing Processes

The following processes should be repeated for each audit cycle:

- Managers and auditors complete a “kick-off” meeting
- Managers support auditors’ high-level assessment of the information security program with interviews and documentation of:
  - Scope and strategy, including how thoroughly the program addresses potential risks and compares with industry best practices
  - Structure and resources, reflecting managerial commitment to effective information security management and the program’s robustness relative to the potential impact of adverse events
  - Management of policies and related procedural documentation
  - Communication of program policies and expectations to stakeholders
  - Impact of program efforts on organizational culture
  - Internal enforcement processes and consistency
  - Ongoing improvement efforts
- Managers support more detailed audit analysis of the information security program
- Auditors evaluate design adequacy
- Auditors evaluate control effectiveness

Audit Testing Steps

The following activities may be repeated in each of the aforementioned audit processes:

- Auditors evaluate information on information security processes and procedures
- Managers assist auditors with walkthroughs of selected processes and control documentation
- Auditors evaluate the design adequacy of the information security program; the ease, reliability, and timeliness of access to such information by key decision makers; and the operational consistency with which such information is generated
- Auditors assess information security performance metrics: existence, usefulness, application, monitoring, and responses to deviation
- Auditors evaluate whether risk management controls are sufficiently preventive, as well as detective
- Auditors define tests to confirm the operational effectiveness of information security activities. Tests might include management and staff interviews, documentation and report review, data analysis, and result sampling for recent initiatives.
- Managers provide requested data, documentation, and observations
- Auditors identify and recommend opportunities for improvement of information security activities
- Managers and auditors complete an exit meeting to discuss audit findings, auditor recommendations, and managerial response
Controls for IT Governance and Strategy

In general, auditors look at three types of controls: management, operational, and technical. Within these categories, auditors may review the controls listed in this section (and potentially others, depending on the audit’s purpose and focus).

The actual IT governance and strategy controls to be audited are determined during the audit planning phase. Controls are assessed during the audit testing phase. Management should determine which controls are appropriate for each organizational environment, based on the corporate risk profile, and compare the list to the controls in this section, which reflect audit best practices and government guidance on IT governance and strategy. In the following section, controls reflect COSO, Turnbull Guidance, “Enhancing Corporate Governance in Banking Organisations” from The Bank for International Settlements (BIS), and other referents noted in this paper.

Management Controls

Management controls to ensure well-run and effective IT governance:

- **Roles and responsibilities**
  - Roles, responsibilities, and relationships of C-level officers (CIO, CTO, CSO, etc.), executives, and management are defined, documented, communicated, and understood
  - Roles and responsibilities are aligned with the execution and continuous improvement of short- and long-term plans
  - An IT organization chart exists and includes management and reporting structures
  - Accountability for policies and procedures is documented and acknowledged by management and staff
- **External influences**
  - IT leaders understand and monitor regulatory definitions and requirements
  - IT leaders track industry processes and norms
- **Planning**
  - The IT organization maintains short- and long-term plans. Short-term plans execute the long-term plans
  - Plans state objectives and performance metrics
  - Plans indicate appropriate budget, timelines, and staff allocations
  - Plans are evaluated by stakeholders for appropriateness and execution
  - Strategic plans and changes to long-range plans are communicated to stakeholders
  - Executive management is involved in critical decisions regarding information security, records management, operational management, business continuity, and other IT regimes

- **IT responsibilities and objectives**
  - A business model exists for the IT organization
  - Management sets an appropriate “tone at the top” for IT activities, policies, and processes
  - IT’s organizational commitments and expectations are documented and communicated
  - The IT organization adheres to corporate values
  - The IT organization enforces a code of conduct
Management Controls (cont.)

☐ IT investment management¹¹
  - IT management identifies business needs for new projects
  - IT management evaluates new project proposals against IT and business objectives
  - IT management tracks assets associated with new projects
  - IT managers monitor project performance
  - IT evaluates proposed new projects with deference to the entire project portfolio
  - IT performs investment reviews and analysis to assess project performance versus expectations
  - IT documents project selection criteria
  - IT documents authority and alignment of managers responsible for project selection and oversight
  - IT performs post-implementation reviews and evaluates stakeholder feedback
  - IT management annually reviews project portfolios and identifies opportunities for improvement
  - IT plans and documents system and technology succession
  - IT benchmarks the investment process
  - IT uses investment benchmarking to reduce risk associated with strategic business change

☐ Resource management
  - An IT budget is maintained. IT leadership is accountable to corporate management for budget adherence
  - IT sets appropriate budgets for projects
  - Appropriate staff, systems, and processes are dedicated to the IT governance effort

☐ Monitoring and reporting
  - Management monitors and measures organizational performance
  - Management reviews short- and long-terms plans compared to performance
  - Reporting policies and mechanisms are well defined and understood
  - Management receives and reviews project standards
  - IT executives review key IT controls for financial reporting, transaction processing, electronic messaging, data and database management, information protection, and e-content management
  - Contingency and failure reporting policies exist, escalation processes are documented, and policies and processes are communicated and understood
  - Performance metrics are established and regularly measured against objectives
  - Staff performance appraisals are completed regularly

Management Controls (cont.)

- Continuous improvement
  - Plans and timelines exist to remediate identified IT governance control weaknesses
  - Plans exist to standardize systems, policies, and processes across operations
  - Management directs plan improvement based on monitoring results
  - Management attempts to streamline redundant, incompatible, and overly complex processes
  - Management ensures existence and adequacy of training programs

Operational controls

Operational controls to ensure the effective performance of the IT governance program:

- Controls exist to meet compliance requirements
  - Management sets levels and assurance metrics for information security
  - Management is rapidly notified of security breaches

- Management tracks contractual definitions and requirements

- IT maintains an inventory of technology assets, including functions and relation to business processes. Assets include hardware, software, storage media, networks, and electronic content.

- The IT organization has a standardized semantic baseline (glossary) for the development of policies and procedures

Technical controls

Technical controls to ensure that IT governance is effective and efficient:

- The IT infrastructure is mapped and inventoried; infrastructure management documents are regularly updated and reviewed

- Data management and data stewardship policies and procedures are documented and enforced

- Management sets project scope and requirements prior to project start

- An enterprise architecture model exists and is enforced

- Management ensures that appropriate technical controls exist and are effective for major compliance practice areas, including data protection, content management and e-discovery, and electronic messaging (e-mail, instant messaging, blogs, etc.)

- Management sets and enforces strategic data-management best practices, including policies for data dictionaries, master data management, and data integrity and quality controls

- IT automates controls in order to reduce resource requirements and ensure consistency and quality of results

---

12 For a control-by-control comparison of regulatory indications for IT leadership, see the ITCI Unified Compliance Project, Leadership and High Level Objectives IT Impact Matrix. http://www.itcinstitute.com/ucp/lhlo
Audit reporting

During the reporting phase, management and the board of directors receive formal feedback from the audit team. This knowledge transfer should be an open and transparent process.

Almost every audit identifies opportunities for improvement. The primary goal of management and auditors should be to address critical issues first, followed by important issues. Both management and auditors should work to ensure that, whatever action plans they set, the goals are achievable and beneficial to the organization.

During the reporting phase, management must determine which corrective actions it will implement and when, based on audit findings. Managers will provide oversight and support to ensure the timely resolution of found issues. Although the audit team may make recommendations based on its assessments of risks and consequences, it cannot make or dictate managerial decisions.

The following are typical steps an audit team takes to confirm and release the audit results.  

- Auditors debrief management, formally discussing significant audit findings and conclusions before they issue the final audit report
- Managers receive a written draft report from auditors
  - The report communicates audit results clearly and precisely
  - Results are presented in an unbiased tone, noting where management has taken actions to correct deficiencies and acknowledging good performance
- Management and auditors discuss the draft report
- Management provides feedback on the draft report
- Auditors review managerial comments and action plan(s)
- Auditors finalize and distribute the final audit report
- Auditors close out the internal audit project and plan any necessary follow-up efforts regarding management’s action plans

Auditors might also choose to disclose some audit findings that management might be able to use to improve governance efficiency and effectiveness, but that do not warrant inclusion in the formal report. This type of communication should be documented, if only as a note in audit findings that the topic has been discussed.

---

13 In organizations with established internal audit functions, there may be standard operating procedures (SOP) for audit reporting (and other audit activities). If so, these audit SOPs should be reviewed by management.
Preparing for an Audit

A well-managed IT governance program includes robust plans, procedures, goals, objectives, trained staff, performance reporting, and ongoing improvement efforts. The internal audit team looks for evidence that the business unit and governance program is well organized and well managed. The security program must also specifically and traceably mitigate risks related to key business objectives. Managerial preparation should mainly be routine, day-to-day practices.

Management’s ultimate goal in the audit process is not to make auditors happy, but rather to demonstrate that IT governance meets the demands of the CEO, board of directors, regulators, and investors. Likewise, auditors’ requests should align with these overarching needs; that is, to support responsible program performance within a sound, ethical business environment.

While the audit is in the planning phase, management should proactively work with the audit team to “educate” the auditors. As a rule, managers should provide constructive input on the evaluation methodology before audit management approves it. Expectations are a two-way street: management must help auditors ensure that audit expectations are aligned and that participants understand each other.

Prior to the audit, managers should collect the information and documentation necessary to demonstrate how well they manage their operations in concert with the overall organizational business objectives. They should be prepared to provide auditors with evidence of well-managed security efforts and results. This might include documentation of security plans, supporting budgets, policy and procedure manuals, assignments of responsibilities (such as up-to-date job descriptions), results reporting and other trending information, and finally, any other relevant guidance (to management and staff) that demonstrates a “well-run” and well-performing program.

In selecting documentation, management should not overload the audit team with information, but provide genuine insight into how IT governance works and how well it performs.

Other steps management should take prior to the audit:

- Learn early and contribute often to the internal audit goals, objectives, purpose, approach, and procedures (audit tests). In particular, setting an appropriate purpose and the audit approach are the two most important elements of every successful audit.

- Discuss with audit management the evaluation criteria and standards and how the audit will actually be conducted, in order to ensure that you’ll receive a quality audit. Ask whether they audit in accordance with international standards for the professional practice of internal auditing.

- Learn who is on the audit team and their qualifications, talents, and motivations. The audit team exists to help make your operations more efficient and effective, but they are also individuals with strengths and weaknesses common to many employees. It pays to know the experience of your auditors, whether they’re rookies or veterans (and perhaps to push for the latter). Showing an interest in their work can also influence and increase the benefits from the audit—within reason. At the end of the day, auditors still need to be independent and objective.

Throughout its discussion with the audit team prior to the audit, management should try to strike a balance between influence and deference. Managers should neither yield entirely to the audit team nor micromanage its efforts.
Communicating with Auditors

Like any interaction between people, but particularly in the work environment, a professional and trusting relationship is a strong precursor to successful collaboration.

When managers interact with the auditors in a professional manner, they tell the audit team that its function is respected and supported. Likewise, lackadaisical efforts by managers and staff reflect poorly on the business unit or process, its capabilities, and its performance. Managers should also expect professional interaction from the audit team and push back whenever they see an exception to this practice.

To contribute to a successful and accurate audit report, managers should be receptive to auditor observations and the audit team’s recommendations. Managers should also be firm when discussing anything they see as incorrect, in order to ensure there are no misunderstandings.

Finally, always remember: managers, not auditors, are responsible for defining and implementing solutions to issues found in the audit. Thus, it is in everyone’s best interest to have a cooperative, collaborative audit process that respects the independence and discretion of all participants. Auditors should listen to management. And for its part, management should encourage staff to be open and honest with auditors.
APPENDIX:
IT Governance, Strategy, and Audit Resources


Symantec
Define, Control, and Govern is Symantec’s approach to IT policy governance. Our approach reduces the cost and complexity of achieving and sustaining compliance with IT governance frameworks, best practices, and corporate and regulatory mandates. Only Symantec can help you simplify compliance management and ensure ongoing enforcement of IT policies across your organization through a single view of multiple standards, comprehensive IT controls coverage, and real-time intelligence.

For more information please visit www.symantec.com/compliance

Tripwire
Tripwire is the leading provider of configuration audit and control solutions to over 5,500 enterprises worldwide, enabling IT to control risk and increase operational efficiency. Tripwire’s advanced configuration control solutions detect and analyze all change activity across the IT infrastructure to identify and resolve unauthorized changes, policy discrepancies, configuration drift, and security violations. Leading global enterprises rely on Tripwire to strengthen their compliance, security and governance, to reduce unplanned work, increase availability, and accelerate success with CMDB initiatives.

For more information please visit www.tripwire.com
ABOUT THE AUTHORS

Dan Swanson, CMA, CIA, CISA, CISSP, CAP

Dan Swanson is a 24-year internal audit veteran who was most recently director of professional practices at the Institute of Internal Auditors. Prior to his work with the IIA, Swanson was an independent management consultant for over 10 years. Swanson has completed internal audit projects for more than 30 different organizations, spending almost 10 years in government auditing at the federal, provincial, and municipal levels, and the rest in the private sector, mainly in the financial services, transportation, and health sectors. The author of more than 75 articles on internal auditing and other management topics, Swanson is currently a freelance writer and independent management consultant. Swanson recently led the writing of the OCEG internal audit guide for use in audits of compliance and ethics programs (http://www.oceg.org) and participated in the COSO small business task force efforts to provide guidance for smaller public companies regarding internal control over financial reporting (http://www.coso.org). Swanson is a regular columnist for ComplianceWeek and also writes the ITCi “Auditor Answers” column.

Cass Brewer

Cass Brewer is the editorial and research director for the IT Compliance Institute (ITCi, www.itcinstitute.com), an independent research and media firm committed to advancing IT’s leadership role in corporate compliance, risk management, and governance. Brewer directs ITCi’s editorial, analytical, and educational initiatives and is the chief contact for the institute’s member community of more than 8,000 business managers, regulators, auditors, consultants, and solution providers from countries and companies around the world. Over the past 13 years, Brewer has issued more than 100 articles, presentations, and white papers on IT and data management topics, and has provided strategic advice and editorial direction for hundreds of additional publications and events. Since 2002 she has focused exclusively on IT compliance issues, leading ITCi’s research and analytical efforts and presenting at live events, including the “Sustainable Sarbanes-Oxley Compliance” Webinar for AIIM in 2005 and the “Measuring and Monitoring Risks and Responsibilities” session for the National Compliance Conference in Warsaw, November 2006.

If you have ideas for improving ITCi's IT Audit Checklists, please write editor@itcinstitute.com.

Legal Disclaimer

When assessing any legal matter, do not rely solely on materials published by third parties, including the content in this paper, without additionally seeking legal counsel familiar with your situation and requirements. The information contained in this IT Audit Checklist is provided for informational and educational purposes and does not constitute legal or other professional advice. Furthermore, any applicability of any legal principles discussed in this paper will depend on factors specific to your company, situation, and location. Consult your corporate legal staff or other appropriate professionals for specific questions or concerns related to your corporate governance and compliance obligations.

ITCi makes every effort to ensure the correctness of the information we provide, to continually update our publications, and to emend errors and outdated facts as they come to our attention. We cannot, however, guarantee the accuracy of the content in this paper, since laws change rapidly and applicability varies by reader.

The information in this publication is provided on an “as is” basis without warranties of any kind, either expressed or implied. The IT Compliance Institute disclaims any and all liability that could arise directly or indirectly from the reference, use, or application of information contained in this publication. ITCi specifically disclaims any liability, whether based in contract, tort, strict liability, or otherwise, for any direct, indirect, incidental, consequential, punitive or special damages arising out of or in any way connected with access to or use of the information in this paper.

ITCi does not undertake continuous reviews of the Web sites and other resources referenced in this paper. We are not responsible for the content published by other organizations. Such references are for your convenience only.
IT Compliance Conference

WASHINGTON, DC, MAY 2–4, 2007

www.ITCiInstitute.com/dc07

ITCi invites you to be a part of the IT Compliance Conference (ITCC), the only education and networking event dedicated to helping professionals like you solve the complex challenges of information systems management for corporate governance, risk control, and compliance.

You’ll Learn

• Practical ways to reduce compliance costs in existing programs
• How to build consensus among change-resistant stakeholders
• Data management principles for efficient enterprise compliance
• How to benefit from difficult conversations with IT auditors

Hot Topics

• Leadership strategies for stronger IT decisions
• End-to-end identity and access management
• The impact of SEC and PCAOB guidance on SOX compliance
• Case studies on enterprise content management and securing mobile devices

Who Should Attend

• CIOs/CTOs
• Chief compliance officers
• Chief security officers
• IT directors and managers
• Compliance managers
• CFOs/financial officers