GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

IPPF – Practice Guide

Information Security Governance

The Institute of Internal Auditors

About IPPF

The International Professional Practices Framework (IPPF) is the conceptual framework that organizes authoritative guidance promulgated by The Institute of Internal Auditors. IPPF guidance includes:

Mandatory Guidance

Conformance with the principles set forth in mandatory guidance is required and essential for the professional practice of internal auditing. Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The three mandatory elements of the IPPF are the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing (Standards)*.

Element	Definition
Definition	The Definition of Internal Auditing states the fundamental purpose, nature, and scope of internal auditing.
Code of Ethics	The Code of Ethics states the principles and expectations governing behavior of individuals and organizations in the conduct of internal auditing. It describes the minimum requirements for conduct and behavioral expectations rather than specific activities.
International Standards	*Standards* are principle-focused and provide a framework for performing and promoting internal auditing. The *Standards* are mandatory requirements consisting of: • Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance. The requirements are internationally applicable at organizational and individual levels. • Interpretations, which clarify terms or concepts within the statements. It is necessary to consider both the statements and their interpretations to understand and apply the *Standards* correctly. The *Standards* employ terms that have been given specific meanings that are included in the Glossary.

Strongly Recommended Guidance

Strongly recommended guidance is endorsed by The IIA through a formal approval processes. It describes practices for effective implementation of The IIA's Definition of Internal Auditing, Code of Ethics, and *Standards*. The three strongly recommended elements of the IPPF are Position Papers, Practice Advisories, and Practice Guides.

Element	Definition
Position Papers	Position Papers assist a wide range of interested parties, including those not in the internal audit profession, in understanding significant governance, risk, or control issues and delineating related roles and responsibilities of internal auditing.
Practice Advisories	Practice Advisories assist internal auditors in applying the Definition of Internal Auditing, the Code of Ethics, and the *Standards* and promoting good practices. Practice Advisories address internal auditing's approach, methodologies, and consideration but not detail processes or procedures. They include practices relating to: international, country, or industry-specific issues; specific types of engagements; and legal or regulatory issues.
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.

This GTAG is a Practice Guide under IPPF.

For other authoritative guidance materials, please visit www.theiia.org/guidance/.

Global Technology Audit Guide (GTAG®) 15
Information Security Governance

Authors:

Paul Love, CISSP, CISA, CISM

James Reinhard, CIA, CISA

A.J. Schwab, CISA

George Spafford, CISA

June 2010

GTAG — Table of Contents

1. Executive Summary

Multiple definitions of *information security governance (ISG)* exist across organizations and standard-setting bodies. Common ISG themes include:

- Promoting good information security (IS) practices with clear direction and understanding at all levels.
- Controlling IS risks associated with the business.
- Creating an overall IS activity that reflects the organization's needs and risk appetite levels.

One way to depict ISG is demonstrated in Figure 1 (Page 2). IS is an important part of the enterprise's overall governance and is placed in the middle of IT governance, IT operations (i.e., current state of IT), and IT projects (i.e., future state of IT). Figure 1 represents a traditional model for IS in many organizations. The trend of the IS field is for ISG to have a role in IT and within the organization. IS always will have a special relationship with IT because of the amount of data that information systems have as well as the impact of losing that information as opposed to paper-based business processes. While the information both processes hold is important to the IS practitioner, in terms of sheer impact, the IT loss would be dramatically more significant. There are no right or wrong governance models; each organization is different as is its needs and risk tolerance.

Boards of directors and executive management must support the ISG structure. The board provides overall strategic guidance to management who must carry out the board's directives through day-to-day management and strategic initiative alignment. Effective and efficient IS requires both governance and management actions.

To improve corporate governance, the board should establish oversight of business/organizational risks including IS as part of the charter of the board's risk committee or another committee under the board's purview. The internal audit activity (IAA) should support the designated board committee by assuring relevant policies, procedures, and practices pertaining to IS are in place and operating effectively.

The chief audit executive (CAE) has responsibility within an organization to provide assurance over the management of major risks, including IS risks. Information is a significant component of most organizations' competitive strategy either by the direct collection, management, and interpretation of business information or the retention of information for day-to-day business processing. Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated. If an organization depends on the faith and trust of its customers, a minor breach can shake customer confidence to the point of loss of business. IS typically is not a reason that customers choose to create or renew a business relationship with an organization, but failing to meet customer expectations for IS controls can cause a current customer to not renew a business relationship or deter a potential customer from forging a new relationship.

The IAA should support the ISG process to the extent allowed by its charter and The IIA's International Professional Practices Framework (IPPF). This participation will likely include activities such as:

- Assessing the degree to which governance activities and standards are consistent with the IAA's understanding of the organization's risk appetite.
- Consulting engagements as allowed by the audit charter and approved by the board.
- Ongoing dialogue with the ISG activity to ensure that substantial organizational and risk changes are being addressed in a timely manner.
- Performing formal audits of the ISG activity that are consistent with *The IIA's International Standards for the Professional Practice of Internal Auditing (Standards)* Standard 2110.A2: "The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.[1]"

Audits of ISG primarily should focus on the organization's implementation of ISG practices, which include clearly defined policies, roles and responsibilities, risk appetite alignment, effective communication, tone at the top, and clear accountability.

This Global Technology Audit Guide (GTAG) will provide a thought process to determine what matters to the organization. This GTAG also will assist the CAE in incorporating an audit of ISG into the audit plan focusing on whether the organization's ISG activity delivers the correct behaviors, practices, and execution of IS.

Core objectives of this GTAG include:

1. Define ISG.
2. Help internal auditors understand the right questions to ask and know what documentation is required.
3. Describe the IAA's role in ISG.

[1] These preliminary discussions may seem familiar to readers of *GTAG-9: Identity and Access Management*, which recommends that, "Prior to conducting an IAM [identity and access management] audit, auditors need to understand the organization's existing IAM structure, such as the company's business architecture and IAM policies, as well as the laws, regulations, and mandates for which compliance is necessary." A key distinction between IAM and ISG is that governance is inherently a strategic activity where access and identity management is largely operational/tactical in nature.

2. Introduction

2.1. What is Information Security Governance?

The IIA's IPPF provides the following definition of Information Technology (IT) Governance:

Information Technology Governance consists of leadership, organizational structures, and processes that ensure the enterprise's information technology sustains and supports the organization's strategies and objectives.

The IPPF does not provide a specific definition for ISG. However, one way to depict ISG is demonstrated in Figure 1 (below). IS is an important part of the enterprise's overall governance, IT operations (i.e., current state of IT), and IT projects (i.e., future state of IT). (Note: The authors are not suggesting that IT is the only area where ISG should be practiced, but in terms of impact of control failure, it should be one of the first areas of focus.)

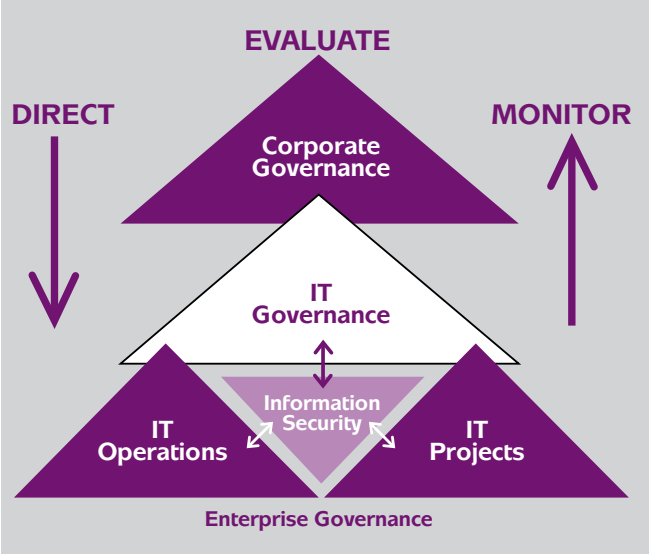


Figure 1. Information Security Governance Triangle

The term ISG can be widely interpreted. Various security organizations and standard-setting bodies have their own definitions and guidance surrounding ISG[2]. Common ISG themes among these security organizations and standard-setting bodies include promoting good IS practices with clear direction and understanding from the top down, controlling security risks associated with the business, and sustaining an overall IS activity that reflects the organization's needs and risk appetite levels. An organization develops a framework and reporting structure to address ISG and while formalized documented policies may exist, reporting lines to the organization's defined governance bodies can be formal or informal. The importance of the informal reporting lines should not be underestimated because many activities in an organization occur outside the formal structures.

IT management literature commonly commingles the concepts of governance and management to the detriment of both because roles and responsibilities are no longer clear. Governance typically has a board that is responsible for setting the organization's strategy and goals. As part of this, the board focuses on strategy, risk management, and leadership. Oversight of management and direction of the organization are central to governance.

In contrast, management is tasked with using resources, including financial and labor, to accomplish and safeguard stated objectives in the identified timeframe. The board does not manage the day-to-day activities of management but strives to ensure that the desires of investors and other key stakeholders are met. For example, pressures from investors to improve quarterly earnings can cause the board to be at odds with management. The segregation of duties between the board and management provides a key control to safeguard the goal of maximizing return on shareholder equity and balancing it with indentifying and managing risks.

The Information Security Practical Guidance on How to Prepare for Successful Audits, from the IT Compliance Institute, provides some clarification of the board's and executive management's roles in ISG. The document states that the board should "provide oversight at a level above other business managers. The board members' role in information security is to ask managers the right questions and encourage the right results." The document notes that the board must provide the appropriate tone at the top for IS. Conversely, the document states "executive management must provide leadership to ensure that information security efforts are supported and understood across the organization, demonstrating by example that mandate of security policies." Figure 2 (Page 3) is reprinted from the IT Compliance Institute's guidance and further outlines the roles of the board and executive management, as well as presents the roles of line managers and internal auditors. (Note: Additionally, the authors of this GTAG would add "establish the risk appetite" as part of the board of directors' roles in Figure 2.) Figure 3 (Page 4), taken from *GTAG-1: Information Technology*

[2] Examples include the Information Security Forum's *The Standard of Good Practice for Information Security*; Australian Standard (AS) 11770.1-2003, Information Technology — Security Techniques — Key Management; the Software Engineering Institute's *Governing for Enterprise Security Implementation Guide*; the National Institutes of Standards and Technology's *Program Review for Information Security Management Assistance (PRISMA)*; and Information Security Management Series (ISO 27000) published jointly by the International Organization for Standards and the International Electrotechnical Commission.

Information Security Responsibilities	
Board of Directors	• Provide oversight. • Communicate business imperative. • Establish and oversee security policy. • Define corporate security culture.
Executive Management	• Provides leadership. • Ensures IS efforts are supported and understood across the organization. • Dedicates sufficient resources to be effective. • Advances the goal of security oversight and promote continuous improvement and success.
Staff and Line-of-Business Managers	• Contribute to design and implementation of IS activities. • Review and monitor security controls. • Define security requirements.
Internal Auditors	• Assess information control environments, including understanding, adoption, and effectiveness. • Validate IS efforts and compare current practices to industry standards • Recommend improvements.

Figure 2. Information Security Responsibilities[3]

Controls, further describes a typical structure of a public company's board, standing committees, and specific executive management roles (e.g., CEO, CFO, CIO) that could be part of any organization's ISG program.

In regards to IS, it must be recognized as a key risk management activity. "Security is a state of being free from doubt or danger. Information security involves protection of information assets (whether in digital, physical, or human form) and information systems from damage, misuse, or attack (whether in storage, processing, or transit), resulting in information being stable, reliable, and free of failure."[4]

Effective IS requires both governance and management actions. The board needs IS to help mitigate and report on confidentiality, integrity, and availability risks to the organization's goals. To improve corporate governance, the board would typically establish oversight of IS as part of the charter of the board's risk committee or another committee within the board's structure. If the business units and the IT services that create and store data do not provide the degree of confidentiality, integrity, and availability expected by stakeholders, customers, or regulating entities, then unacceptable risks likely will exist. In most cases, the lowest common threshold is always compliance with the law, which will help the IS practitioners understand the lower bar that should never be breached. The internal auditor should confirm that relevant policies, procedures, and practices pertaining to IS are in place.

Management will then create an IS organizational structure[5] and budget that are commensurate with the direction set forth by the risk committee, or other such forum, and the board. In absence of specific direction, management should understand the compliance aspects and use that as the minimum threshold to fill any vacuums that may exist with guidance from the top. Audits provide assurance that management has implemented and is sustaining both an effective IS activity and overall compliance with IS policies.

2.2. What is Effective Information Security Governance?

An effective ISG program:

- Involves appropriate organizational personnel.
- Defines a governance framework or methodology.

[3] Excerpt from the IT Compliance Institute's *Information Security Practical Guidance on How to Prepare for Successful Audits*. www.t2pa.com/analysis-a-advice/library/179-it-audit-check-list-information-security

[4] Bihari, Endre. Information Security Definitions, 2003. www.perfres.net

[5] This can include a separate IS activity as well as embedding IS responsibilities into existing roles as long as accountability is clear. The structure is organizational-dependent.

Description of Various Board Standing Committees and Executive Management	
Audit Committee	The role of the audit committee encompasses oversight of financial issues, internal control assessment, risk management, and ethics.
Governance Committee	The governance committee is responsible for board member selection and assessment and for leadership of the board's operations.
Risk Management Committee	The risk management committee is responsible for oversight of all risk analysis and assessment, risk response, and risk monitoring.
Finance Committee	The main role of the finance committee is to review financial statements, cash flow projections, and investment management. Members of this committee need to understand the control elements of IT that ensure the accuracy of information used to make key financing decisions and generate financial reports.
Chief Executive Officer (CEO)	The CEO has overall strategic and operational control of the organization and must consider IT in most aspects of the role.
Chief Financial Officer (CFO)	The CFO has overall responsibility for all financial matters in the organization and should have a strong understanding of the use of IT to enable financial management and to support corporate objectives.
Chief Information Officer (CIO)	The CIO has overall responsibility for the use of IT within the organization.
Chief Security Officer (CSO)	The CSO is responsible for all security across the entire organization, including IS, which also may be the responsibility of a chief information security officer (CISO). Additionally, as discussed in *GTAG-6: Managing and Auditing IT Vulnerabilities*, the CISO supports activities such as effective vulnerability management and helping to align technical risks with business risks.
Chief Legal Counsel (CLC)	The CLC may be an employee, an officer of the organization, or an external legal adviser.
Chief Risk Officer (CRO)	The CRO is concerned with managing risk at all levels of the organization. Because IT risks form a part of this function, the CRO will consider them with the help of the CISO.

Figure 3. Roles of the Governance Bodies and Functions[6]

- Enables uniform risk measurement across the organization.
- Produces quantifiable, meaningful deliverables.
- Reflects business priorities, organizational risk appetites, and changing levels of risk.

The ISG activity needs to involve appropriate organizational personnel.

This personnel includes the board (as discussed in section 2.1) and executive management from whom internal auditors must elicit commitment and financial and political support. The IS department will provide standards/baseline tools and processes to support the execution of the IS activity. Privacy, compliance, legal, and IT functions should participate in this program to ensure that information assets are adequately indentified and managed according to relevant outside expectations (e.g., current and future customers, regulators, stakeholders, and others who are relevant to the organization's long-term, strategic goals). Finally, the human resources function should assist in communicating uniform standards to all employees and in providing uniform guidance in disciplinary activity associated with violation of the IS mandates. Without the appropriate support of these

[6] *GTAG-1: Information Technology Controls*

groups, the ISG activity may devolve into IS management and become an operational/tactical, rather than strategic, activity.

The ISG activity defines an appropriate framework or methodology to guide its activities.

Examples of governance frameworks can be found in *GTAG-11: Developing the IT Audit Plan* or the IT Governance Institute's *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*. These frameworks help ensure that the organization operates within a structured, consistent, objective, and effective manner that can be easily explained to stakeholders, regulatory agencies, service providers, and other outside parties. Well-planned frameworks also can guide future business changes and activities by ensuring that proposed activities are considered according to the same criteria as existing activities. Using a framework allows an organization to benefit from leading practices developed over time.

Uniform IS risk evaluations are also an element of effective ISG.

Like all business activities, IS activities must be prioritized. Deploying uniform risk measurement tools across the organization helps ensure that the areas of highest IS risk can be clearly identified. Risk evaluation tools should establish thresholds to distinguish inherent risk across the environment. An organization may, for example, choose to leave systems as-is (i.e., accept risk) if acceptable thresholds have not been exceeded. This can begin as a simple assessment of risk at a very high level, such as a simple document outlining the high-level risks. (Note: It is expected that these tools will evolve, but the authors have seen very complicated, quantitative methods used to implement a risk evaluation process that never bears any value due to the sheer number of risks any organization takes in its day-to-day activities.) It is crucial that management provide the appropriate time and resources to allow the activity to develop naturally throughout the organization.

The ISG activity should yield quantifiable and measurable deliverables.[7]

Qualitative data can be useful in management activities, but quantitative data offers improved tracking and trending capabilities that are not available through qualitative measures. Quantitative measures could include the number of policies and standards delivered, the number of significant security events occurring, and results of corporate security training programs. This does not mean that qualitative results have no value; qualitative data without appropriate quantitative supporting data diminishes the perceived value of the information provided. A mixture of quantitative and qualitative measures taken together provide the insight into the IS activity of which management needs to make appropriate decisions. However, a successful ISG activity should be driven by fact-based, objective metrics with appropriate risk analysis performed by IS professionals who understand the organization.

The ISG activity should adapt its priorities based on legal, regulatory, and business changes, and deploy policies and standards that reflect the organization's risk appetite and are practical, reasonable, and enforceable.

Successful businesses are rarely static. They face changing external conditions such as competition, regulation, evolving business models, and changes in supply chains. The ISG team needs to understand and support these activities. As an example, if the organization expands to add a new business activity, the impact must be fully considered. Does it introduce new regulations? Does it introduce new inherent risks? Does it alter the state of existing business functions? The ISG activity also should reflect ongoing changes within established businesses. Legacy business activities are also subject to emerging regulations and emerging threats. If the organization does not adapt its governance and management activities to reflect these changes, it may not survive. As noted in *GTAG-11: Developing the IT Audit Plan*, 36 percent of internal auditors now re-perform their risk assessments more than once per year. This reflects how rapidly changes in risk can occur.[8]

2.3. What is Efficient Information Security Governance?

An efficient ISG activity will reflect the concept of proportionality by:

- Encouraging a tiered structure of internal control.
- Adjusting reporting based on the level of management involved.
- Allow for properly approved deviations to policies and standards.

An efficient ISG activity encourages proportional control.

This means providing greater control for higher impact activities and more valuable assets. It also encourages less control

[7] Examples of deliverables and metrics can be found in the National Institute of Standards and Technology's *The Performance Measurement Guide for Information Security* (Special Publication 800-55 Revision 1).

[8] IPPF Standard 2010: Planning — "The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals." IPPF Standard 2010.A1 — "The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually."

for lower risk activities and less valuable assets. Unless compelled by regulation or external certification authorities, an organization would not typically spend money to further control low-risk activities.

Proportional control should be observed in the design of reporting.

Reporting on the state of IS within the organization should vary depending on the organizational levels involved. IS violations will probably occur routinely in any sizeable organization. The types of infractions will vary from less threatening (e.g., improper use of a single letter) to very threatening (e.g., loss of protected customer data through electronic breach). Executive management should be substantially involved in major security events, but likely will only be aware of more routine security violations through the trending of aggregate statistics. Mid-level management or line management may, however, be substantially involved in these more routine events to identify trends.

An efficient ISG activity is adaptable enough to handle systems that cannot cost-effectively or technically conform to policies and standards.

When controls cannot be cost-effectively implemented and alternate solutions are not available, an efficient governance structure provides a structured mechanism for deviating from policies and standards. This mechanism will typically include formal risk acceptance with documentation that records the analysis that has been performed to demonstrate that management has acted in an informed manner; which is prudent and appropriate in proportion to the business value to be received. This also will include re-evaluation of deviations on a regular basis to ensure the deviation from policy is still appropriate and warranted or if the factors within the organization have increased to warrant revocation of the deviation (e.g., aggregated risk has increased, cost of control has decreased, new control option exists).

2.4. Why Should the CAE Be Concerned About Information Security Governance?

Information is a significant component of most organizations' competitive strategy whether it is strategic business plans or customers' personally identifiable information (PII). The loss of this information could have a significant detrimental impact on the organization. As mentioned previously, for most organizations, IS is generally not a reason why one organization is chosen over another, but the loss of information can have significant impact on current and future business opportunities. In addition to direct loss, there are issues around the loss of integrity/fidelity of information, especially when it comes to financial reporting, thefts of money, or disruption of service. Some of the more obvious consequences of failing to ensure that management is keeping its responsibilities regarding IS in context with organizational needs are:

- *Regulatory actions*. Many organizations handle some form of PII, Protected Health Information (PHI), or other regulated information (e.g., prerelease information) for their customers or employees. In many jurisdictions, this type of information is heavily regulated. In addition to the well-known PII issues, the loss of data or compromised data integrity could present a serious problem in the confidence of the financial statements or other issues. Noncompliance has multiple penalties that may detrimentally affect the organization.
- *Reputational damage*. Organizations that have significant IS breaches often face a negative reaction from their customers.
- *Competitive advantage*. The compromise of competitive strategies, pricing, customer and partner information, and other key corporate information can jeopardize an organization's ability to compete against other organizations that do not have compromises.
- *Contractual noncompliance*. Contracts increasingly contain stipulations for the protection of information. A breach could result in the loss of key contracts, and customers, as well as civil suits.
- *Inaccurate or incomplete data*. Organizations must provide, store, and retain accurate and complete information. Inaccurate or incomplete information may result from simple errors to outright fraud. Regardless of the cause, governance efforts should include information integrity.
- *Fraud*. Failure to implement adequate IS will increase the likelihood of successful fraud against the organization.

Beyond the items listed, the CAE has a responsibility to the board of directors to provide assurance on the effective and efficient achievement of ISG objectives, as well as help the board ensure that the IT activity can execute its fiduciary duties to stakeholders. For these reasons, the IS activity must be a consideration in the execution of the IAA's mandate.

3. The Internal Audit Activity's Role in Information Security Governance

As noted in IPPF Standard 2130.A1:

The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- *Reliability and integrity of financial and operational information.*
- *Effectiveness and efficiency of operations.*
- *Safeguarding of assets.*
- *Compliance with laws, regulations, and contracts.*

Also, as noted in IPPF Standard 2110.A2:

The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.

The CAE must include these expectations in planning ISG audits. Reliability and integrity, safeguarding, and compliance are typically associated with IS management, but effectiveness and efficiency should be factored into the risk appetite of the board as well as allow the IAA to determine whether governance activities result in properly controlled, under-controlled, or over-controlled systems and workflows. Properly controlled systems are both effective and efficient in providing reliability, safeguarding, and compliance. Under-controlled systems may be efficient but also may be less effective — especially during periods of volatility. Over-controlled systems, or those with more controls than warranted by the associated potential loss, may be more effective, but not as efficient. The IAA needs to ensure that the ISG activity is both effective and efficient in addressing confidentiality, integrity, availability safeguarding, and compliance. However, the effectiveness of a control is always the most important consideration.

3.1. The Internal Audit Activity's Responsibilities Related to Information Security Governance

While the IAA cannot establish organizational structures, approve methodologies, or write policies, it can challenge them and should support the ISG activity to the extent allowed by the internal audit charter and the IPPF. This participation will likely include activities such as:

- Assessing the degree to which governance activities and standards are consistent with the IAA's understanding of the organization's risk appetite.
- Consulting engagements as allowed by the internal audit charter and approved by the board.
- Ongoing dialogue with the ISG activity to ensure that substantial organizational and risk changes are being addressed in a timely manner.
- Formal audits of the ISG activity consistent with IIA Standard 2110.A2.

3.2. Auditor Background and Experience Level

To perform an effective audit of an ISG activity, one must be an experienced auditor with an understanding of ISG concepts. Instead of a checklist approach, an ISG audit will require the auditor to interpret and understand the organization's ISG activities. The CAE should ensure the IAA possesses the resources and competencies necessary to evaluate IS and associated risk, including both internal and external risk exposures and those relating to the organization's relationships with outside entities. The CAE may need to rely on staff that has experience working with security and executive management. In small audit functions, the CAE may be actively involved in this process. The staff should have an understanding of the existing governance structure and possess adequate relationship management skills to form effective working relationships with the security management leadership and governance structure.

3.3. Audits of Information Security Governance

An audit of the ISG activity could take several forms:

- The most basic ISG engagement would be to benchmark the ISG activity against independent standards.[9] This level of review provides some assurance on how comprehensively management has defined an ISG framework but does not actually test how strictly implemented processes conform to the framework. A benchmarking engagement could provide an effective starting point in a multiyear audit plan because it allows management time to address design flaws in the governance structure before additional audit testing occurs. This approach can also help the CAE to ensure that IAA resources are being efficiently managed because conformance testing will not occur until the IAA has reasonable assurance that the program meets basic expectations.
- Once the CAE is sufficiently satisfied with the design of the ISG activity, audit testing should focus on the degree to which the program has been executed. This type of auditing could include reviews of management

[9] The internal auditor also may want to verify whether management is benchmarking and, if so, consider the benchmarking activities.

reporting, approval and documentation of exceptions, consistency of risk assessments, effective use of metrics, timely updates based on emerging business needs and external changes, review of minutes of board and committee meetings, business strategies and plans, business changes, and interviews with management members.

- Finally, the IAA ultimately should examine the degree to which other auditable entities provide adequate ongoing support to the ISG activity. This likely will involve specific test steps in other audits such as assessing whether possible security events are properly documented, escalated, responded to, and managed by support teams and reviews of IS risk in each of the strategic business processes. While this could be construed as auditing IS activities instead of governance, observing the degree to which organizations, and their departments or functions, understand and conform to the expectations established by the governance process is imperative to understanding true ISG effectiveness. For example, if the help desk under-reports 50 percent of improper use activities, the organization as a whole will dramatically underestimate its true risk profile and may ultimately fail to achieve key business objectives as a result.

4. Auditing Information Security Governance

4.1. Auditing Information Security Governance – Planning

To effectively and efficiently audit an ISG activity, an audit plan — which will test the aspects identified as most important by the IAA with input from the audit committee and management — must be created and maintained. To do this, the IAA must consider an organization's structure, purpose and objectives, lines of communication, risk appetite, level of integration with other business units, and external pressures.

4.1.1. Understand the Information Security Governance Organizational Structure

The first step is to assess the organizational structure in support of the IS activity. Care must be taken to understand the formal reporting structure as the IS activity typically will need to be high enough within the organizational hierarchy to exert influence and avoid conflicts of interest. For example, the head of IS may report to the CIO, CFO, or the enterprise-level CSO, thus reducing any potential conflicts of interest when functioning within lower levels of the organization.

The IS activity likely will have formal reporting lines to key stakeholders per organizational policies. This includes the board and/or committees, corporate counsel, regulatory compliance, and so on. Ideally, these structures should be formally documented. The internal auditor should collect information on both the formal and informal reporting structures to understand the political nuances and organizational priority that management has placed on the activity.

An additional dimension to assess is the level of depth and breadth in the governance structure and the level of resilience the organization appears to have should key persons in the governance structure be unavailable. For example, what would happen to IS if the CIO or CSO were to be dismissed? How would the governance structure react and what would be the impact?

This evidence can be collected by requesting organizational charts, job descriptions, and corporate IS policies, as well as interviews with C-level executives and the heads of the audit and risk committees.

Questions to ask:

1. Who is formally responsible for IS?
2. Where is he or she located within the organizational diagram?
3. To whom does this person formally report?
4. To whom does this person have a dotted line responsibility?
5. Are there any committee functions, boards, or other groups that IS staff regularly reports to either on an informational basis or a more formal steering function?
6. What is the career level of the person in charge of IS? Is this an officer-level position or a managerial position? Does this individual have other roles?
7. Are roles and responsibilities, accountability, and performance for all IS responsibilities formally defined?
8. How are conflicts of interest avoided?
9. Is the CSO driving the IS activity or mostly reporting compliance?
10. Does an IS forum exist? If so, what is its role?

4.1.2. Understand the Purpose and Objectives of Each Component of the Environment

Once the governance structure is understood, documents that support management's assertions need to be collected and evaluated. The intent is to validate that discussions are occurring in a manner commensurate with the desires of the board and executive management.

Examples of documentation to collect include IS policies, charters, objectives, relevant job descriptions, minutes of governance or board meetings where security governance is discussed, incident response evidence handling documentation, retention policies, process narratives, training materials, etc.

Questions to ask:

1. Are roles and responsibilities for the IS activity formally defined?
2. How are business unit and/or individual performance objectives tied to IS objectives? Do they support the IS activity?
3. Does each component of the ISG structure have sufficient capital and operating expense budgets to support IS efforts?
4. Are procedures in place to oversee IS incidents including public and investor relations and coordination with law enforcement?
5. Are IS policies supported by written standards? Are the standards supported by written procedures?[10]

4.1.3. Understand the Documented Communication That Occurs Among Reporting Lines

Policies, standards, and procedures should outline information exchanges that should transpire between the IS department and other groups, such as the audit committee. An internal auditor should collect data to assess whether the exchanges are taking place as intended and that there are not unintended obstacles — political, technical, etc. For example, if the organization is a highly structured, regimented organization, does the CSO have appropriate access

[10] The auditor should see a clear link between the IS policies, standards, and procedures where the policies drive the standards.

to the decision makers? The policies and procedures should identify criteria for escalation in the event of certain situations such as unavailability of staff and abnormal business conditions.

Whenever possible, feedback loops should be formally identified and documented. Instead of the IS activity sending reports with no return communication, there ideally should be a dialogue wherein the receiver acknowledges receipt and addresses any questions. This helps reinforce accountability for IS activities.

Questions to ask:

1. What information exchanges are formally defined?
2. Are they sufficient?
3. Are they taking place according to schedule?
4. Does the IS activity get effective/meaningful feedback from the groups it works with?
5. What is the escalation path that IS news/alerts must follow?

4.1.4. Understand the Organization's Risk Appetite

If possible, the internal auditor needs to interview the board to understand its risk appetite. This relates to the level of risk that the board deems acceptable in terms of the organization and should be reflected in the organization's culture and management's level of risk appetite. Additionally, the internal auditor may find other corroborative evidence that reflects the organization's risk appetite by reviewing written policies covering risk, circumstances which need to be escalated to the board, and incidents that should be reported to the executive level.

Some boards are very risk averse and tend to be conservative in the creation and protection of value. Other boards may accept high levels of risk in the pursuit of larger returns. An understanding of the board's perspectives on risk will set the broad context for ISG.

The internal auditor needs to understand the materiality threshold that warrants engaging the board. Additionally, broad guidelines around types of incidents for engaging the board should be established. Organizational policies should identify these incidents, as well as the correct escalation paths, communication plans, and so on.

Questions to ask:

1. Under what circumstances does the board need to be engaged?
2. What is the organization's materiality threshold?
3. What are the IS risks that the board would deem unacceptable?
4. How often is this criteria reviewed?

4.1.5. Understand Integration of Information Security Governance Within the Organization

The IS activity is best enacted through integration with an organization's other business units. In other words, the IS activity in isolation cannot secure an organization. It must work with management, development, project management, server engineering, network and desktop engineering, release management, business continuity, business process owners, and other groups to help them achieve their objectives. These objectives must include the security of information commensurate with management's intent as codified in policies.

An internal auditor can review and use the organizational chart and interview business units to determine whether the IS activity has met with each business unit to establish mutual integration requirements both for the unit and for IS. Policies should set the review cycle and meeting minutes or other summary reports should exist to establish the go-forward plans.

Questions to ask:

1. Is IS a consideration in other business units' strategy, processes, and procedures? Has the IS activity added value?
2. Is IS a consideration in the organization's IT strategy?
3. Is there a formal meeting schedule?
4. What are the meeting agenda items? Are actions taken, or do issues lack progress?

4.1.6. Understand External Influences That Could Affect the Information Security Governance Structure

As the risk environment changes, so too should the controls, processes, and structure. Such external influences include:

- *Regulatory changes*. There are laws and data privacy regulations that require an organization to comply with certain mandates that may, or may not, align with the organization's short-term objectives. Noncompliance may result in fines, civil suits, and damage to the brand.
- *Evolving industry standards*. There are multiple industry forces, such as Payment Card Industry Data Security Standards (PCI-DSS) or BITS Product Certification (formerly Banking Industry Technology Secretariat), requiring compliance to conduct business with critical partners. Understanding these needs and the risks of not complying must be taken into consideration to avoid detrimental impact.
- *Legal developments*. There are risks that arise from contracts as well as from the legal environment. For example, the payment card industry has contractual requirements that organizations processing credit cards must follow. In addition, organizations need to understand the legal environment to avoid civil suits relating to negligence and other potential issues.
- *Dynamic market forces*. There are risks that arise from the direction of the market. For example, the movement to electronic commerce creates security risks for organizations to mitigate.

Questions to ask:

1. What regulations, laws, and contractual requirements apply to the organization?
2. How often, and when, were regulations last reviewed to understand IS requirements? Is the legal department involved in the review, or is interpretation left to non-legal staff?
3. Is there an internal or external regulatory compliance group, and when did the IS activity last meet with them?
4. What regulations are costly and operationally inefficient?
5. What contracts have IS components?
6. When did the IS activity last review contractual requirements with legal counsel?
7. Does legal counsel consult with the IS activity to assess requirements during the contract process?
8. What legal contracts are most burdensome, and why?
9. When did the IS activity last review the legal environment with legal counsel?
10. What legal environment issues affect ISG and why?
11. When did the IS activity last meet with marketing and strategy groups to understand what is happening in the market?
12. What market forces affect ISG and why?

4.2. Auditing Information Security Governance – Testing

Based on what the internal auditors learned from reviewing the organization's documentation, they should confirm and validate their understanding with key people within the ISG structure. This validation will help auditors identify whether the organization's documentation is factual and whether stakeholders' perceptions are correct.

4.2.1. Confirm Stakeholder Concerns

The internal auditor needs to confirm — with all identified persons, activities, or committees within the ISG structure — what is important to protect. Once confirmed, the internal auditor can then determine whether all parts of the governance structure are aligned.

As previously mentioned, the internal auditor should first confirm high-level concerns with the organization's governing board. Then, the internal auditor should proceed down the ISG structure. Inquiries should specifically address what each person, activity, or committee is worried about as it relates to the business and ISG. Figure 4 (right) presents suggested questions to confirm concerns.

Questions to Confirm Concerns

- Are there any questions regarding the regulatory requirements of the organization's industry? Are you satisfied with the types of communication you are receiving about the organization's regulatory compliance?
- What are our risk appetite levels? What is our priority: confidentiality, integrity, or availability? If all three are important, which is the priority when all three are a consideration? How much confidentiality do you want (e.g., a high assurance of zero records lost, which is expensive)?
- Is there something of which we need to be aware to avoid negligence (e.g., lack of compliance due to insufficient protection of consumers' information)?
- Are there trends in our industry of which we should be aware? What level of assurance are our competitors seeking? What has happened within our industry that warrants a reaction? Are there industry best practices, recommended guidelines, or regulatory requirements to which we need to adhere (e.g., BITS, PCI-DSS)?
- Is the board satisfied with the way management is assessing and reporting on risk? If not, what information does it need to be successful in assessing the direction of the IS activity? Are there practices that board members or management have seen elsewhere that might be worth introducing into this organization?
- Is there any other reason we should be concerned (e.g., strategic direction)?

Figure 4. Questions to Confirm Concerns

Responses can vary based on the organization and will include both internal and external business concerns. Examples of concerns could include profit, brand protection, liability, intellectual property, or regulatory compliance. Responses also could be organization- or industry-specific. For example, a charitable organization may be more interested in investment risk than profits. Responses also may include discussions of external relations and regulatory compliance, including concern of external reputational risk.

Based on this inquiry process, the internal auditor will develop a situational awareness of the ISG structure. Next, the internal auditor will need to determine whether responses align with the governance structure including its charters, objectives, policies, and other supporting documentation. The internal auditor should then compare responses to the reporting structure and related supporting documentation, as well as identify areas where alignment does or does not occur.

The resultant picture will allow the internal auditor to summarize and make appropriate recommendations regarding the ISG structure. Variances may occur between what is documented and what actually is occurring. These differences could be the result of formal practices that are too cumbersome or have not been modified as the organization changes. The organization itself will usually adapt and create new practices that may not be documented but may be more efficient and effective in achieving the same objectives as stated by the current formal written documents. The internal auditor needs to evaluate each of these variances to verify that current practice achieves the organizational objectives and are in fact operating more efficiently and effectively. If current processes deviate from documented expectations, the auditor must determine whether the differences are intended to circumvent that governance structure or whether documentation is simply out of date.

4.2.2. Confirm Reporting and Communication Lines

Information and communication is one of the components of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model. Communication and reporting relationships within the organization should be formally defined and processes — that allow for effective communication up and down the chain of command — within the organization should exist. These processes should include procedures for identifying, capturing, and reporting pertinent information related to IS within a defined time frame that allows users within the ISG activity to respond and carry out their responsibilities.

The internal auditor needs to confirm whether these formal reporting and communication relationships occur as identified in the organization's documentation and are effective. Confirmation can occur through inquiry and review of documentation. The internal auditor could use the information and communication component of the COSO model as he or she reviews and evaluates the organization's formal communication and reporting relationships.

When reviewing the formal reporting relationships, the internal auditor must be cognizant of other communication lines that are not documented as part of the formal ISG structure because informal communication lines could be a sign of ineffective reporting and communication. These communication lines may develop over time from perceived inefficient formal reporting lines or communication methods, relationships among various individuals within the ISG structure, or political perceptions.

Organizations could be overburdened with formally defined reporting and communication requirements such as requiring minutes of every committee that meets or requiring documentation for all communications in a specified manner. Users could get bogged down or frustrated with having to communicate through an entire chain of command for some small item when calling someone is more efficient. These examples provide users within a governance structure the opportunity to establish informal communication channels that allow them, within their perception, to be more efficient and effective than if they followed formal processes. Control breakdowns may result if formal reporting and communication processes are not followed. Therefore, the internal auditor needs to be aware of these and should consider potential opportunities for business improvements by incorporating some of the informal processes into the formal structure or helping reestablish situational awareness of what is lost when formal processes are not followed.

Sometimes as relationships become established within an organization's formal reporting process, requirements break down as casual conversation takes its place. Also, individuals within the chain of command may become more familiar with each other and therefore circumvent formal reporting lines to speed up the communication efforts. As the internal auditor becomes aware of these situations, opportunities to remind individuals of why formal communication processes exist may become necessary as not following procedures could result in breakdowns in internal controls.

The internal auditor also must be keenly aware of organizational politics. Formal processes attempt to dissuade use of political perceptions by requiring specific reporting and communications to occur within a defined chain of command. Politics in any organization are inevitable, but formal processes should help ensure that political pressure or perceptions are minimized.

Deviations from formal communication and reporting lines are areas the internal auditor can use to provide feedback as opportunities for business improvement. Evaluation and consideration of alternatives will allow the internal auditor to complete his or her evaluation and provide appropriate recommendations.

4.2.3. Confirm Key Performance Indicators and Their Use

Key performance indicators (KPIs) are a form of reporting that organizations can use to monitor IS. KPIs relate to the COSO model's Information and Communication component where data is collected and disseminated based on formal reporting lines. Managers then use the reported results for timely follow-up activities.

KPIs are useful to the organization to show how facets of an activity or process are working. KPIs can be used to measure a number of items, such as efficiency and effectiveness, compliance, and organizational performance. The organization should define the ranges of acceptable and unacceptable key results (e.g., the minimum and maximum performance measures for each of the chosen indicators that are considered acceptable). Once KPIs are established and data is collected, an evaluation should occur and the organization should decide how the results are to be used.

The National Institutes of Standards and Technology's (NIST's) *Performance Measurement Guide for Information Security* (Special Publication 800-55 Revision 1) discusses a collection of three types of measures:

- Implementation measures to ascertain the execution of a security policy.
- Effectiveness/efficiency measures to gauge the results of security delivery service.
- Impact measures to weigh business or mission consequences of security events.

The guidance further clarifies these measurement categories and provides examples of each.

Auditors could perform a review of the above NIST guidance prior to commencing a review of the ISG activity specific to KPIs. Internal auditors could use the guidance as a basis to evaluate whether the KPIs are comprehensive. Consideration of the previously collected organizational information will assist the internal auditor in assessing whether the KPIs are relevant.

To evaluate the KPIs, the internal auditor needs to understand them and their intent. Some questions the internal auditor should consider include:

- What is being measured? Why, and how?
- Given the organization and what is being measured, do the KPIs make sense?
- Are the KPIs driving desired behavior?
- Does a feedback loop, which provides input for continuous improvement, exist?

If the internal auditor concludes that the KPIs are valid, then he or she should use these to assess the effectiveness of the IS activity and its governance structure. Additionally, this process may allow the internal auditor to obtain a better understanding of the effectiveness of the organization's information and communication systems. The internal auditor also may want to understand the manner in which the data is accumulated for the KPIs, the how and to whom they are reported, and what management does with the final results.

By obtaining an understanding of the validity of the KPIs, the resulting manager follow-up, and improvement efforts, the internal auditor will have a better picture of the overall effectiveness of the ISG activity.

4.2.4. Confirm Alignment of Supporting Documentation With Governance Structure

By this time in the review, the internal auditor should have a fairly good understanding of the organization's ISG activity and related supporting documentation. Based on interviews and other testing evidence, the auditor also should be able to identify where the documentation differs from actual practice. In addition, the internal auditor should identify and further explain the variance between what is stated and what actually is performed. Some items for the internal auditor to consider include:

- Does actual practice provide better controls or a more efficient and effective process than what is documented?
- Why do differences exist?
- What really is the best practice to use — what is documented or what is currently in practice?

The internal auditor's recommendations will depend on the overall controls within the governance structure and how each variance from the documented process affects the structure. In the end, the final documentation should align with the agreed practices.

4.2.5. Confirm Alignment of Risk Appetite

The IIA's *Standards* define *risk appetite* as the level of risk that an organization is willing to accept. The internal auditor needs to confirm that all the facets of the governance structure, including regulatory and contractual areas of integration, align with the organization's acceptable risk appetite. As discussed in section 4.2.4, the supporting documentation should also align with the organization's risk appetite. Additionally, as should be noted in the organization's policy, the board needs to be engaged at the appropriate level in overseeing and defining the organization's risk appetite, which should be defined at the board level and flow from the top to the bottom of the organization. The board also should make formal statements that may not be specific to ISG but do reflect the organization's overall risk appetite.

In some organizations, a statement of risk appetite may not exist. In this case, the internal auditor will need to glean this information from corroborative evidence or through direct inquiry of the board. In practice, the internal auditor should understand the organization's risk appetite as knowledge of this subject usually is required to complete the annual risk assessment or the organization's enterprise risk management activities. If not formally defined, the internal auditor may wish to suggest that the board formally defines a statement of risk appetite.

Specific risk tolerance levels may be defined by management at specific levels within the ISG activity. All risk tolerance levels defined by management should align with the organization's risk appetite. In some organizations, the board and executive management could have the same tolerance level, but other management levels may have increased risk tolerances. Variances can occur, but overall, the internal auditor should ensure that specific defined risk tolerances are within the parameters defined by the board's risk appetite.

If the internal auditor concludes that the organization's risk tolerances as defined by management are not aligned, then he or she should consider appropriate suggestions. Additionally, prior to making recommendations, the internal auditor should consider all corroborative evidence.

4.3. Auditing Information Security Governance – Analyzing

After confirming the alignment of the organization's risk appetite, the internal auditor should begin the analysis phase — where all of the information is gathered together and tied via themes — so he or she can draw a conclusion about whether the program is effective. During this phase, one question the internal auditor must consider is: "How does my organization match up against the recommended practices the authors provide?"

4.3.1. Accountability

The internal auditor will need to analyze the data and determine whether the governance process creates and supports accountability. To obtain reasonable assurance that the ISG activity creates and supports accountability, the internal auditor needs to identify whether the evidence demonstrates the following:

- First, the organization's risk appetite and executive management's directives should have been effectively translated into policies, procedures, and standards. If policies do not align with the stated goals of the board and executive management, holding people accountable for understanding and following these policies will not achieve the desired result. The internal auditor should note that this is a critical step in the analysis phase. If employees are consistently taking the wrong actions, this may result in a high level of conformity, but it will not yield effective long-term governance.
- Second, upon determining that management's directives have been effectively translated into policies, standards, and procedures, the internal auditor must determine whether accountability for significant processes is established and supported. Accountability can be established but not supported, which still results in an ineffective governance structure. This state is sometimes described as having accountability, but not authority, for an activity. An example of unsupported accountability would be declaring that the CISO will ensure that all systems receive security patches in a timely fashion. This statement establishes clear accountability. If, however, the CISO lacks enforcement capability, then the organization has created accountability without authority. Alternatively, if the organization states that the CISO will work with system owners to ensure that all patches are applied within a certain timeframe and also entrusts the CISO with sufficient authority to shut down or logically isolate any nonconforming systems, then the internal auditor may be able to state and conclude that assignments of accountability and authority are sufficiently matched.
- Third, the internal auditor should identify whether ownership is clearly assigned based on position/role in the organization. Policies, procedures, and standards should assign responsibility for an activity to a single individual rather than a group of people. That individual may work with a larger group to execute his or her assigned work, but based on an assigned role, the individual should still be responsible for ensuring that a specific ISG activity is actually taking place.
- Fourth, the internal auditor must evaluate situations in which there are broad assignments of accountability. Many general policies and standards stipulate that all users are accountable for an activity. Examples include safeguarding assigned credentials (e.g., username and password), protecting customer data, and using business assets appropriately. Yet, these statements do not produce real accountability if the users lack sufficient training to reasonably comply with the expectations or if enforcement of the standards is inconsistent across the organization. Policies and standards must be supported through sufficient training and be applied consistently.
- Fifth, the internal auditor needs to identify whether there are appropriate consequences for failure to conform to policies, standards, and procedures that reflect management's directives.

The current state of an organization's IS activity should be measured for good or recommended practices. One method is to evaluate the program against independent standards that are relevant to IS. In fact, The IIA's IPPF states: "In planning the engagement, internal auditors must consider … the adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model." The scoping decisions made in section 4.1.1. of this document are relevant here. The nature of the organization and its industry will dictate the degree to which recommended practices may be relevant or even required. An organization in a highly regulated industry may need to continuously demonstrate compliance with one or more externally recommended frameworks to show due diligence. An organization may feel compelled to demonstrate compliance to maintain a competitive advantage. Other organizations may not require demonstrable adherence to externally recommended practices. Auditor judgment will be important in completing this step. If the audit process has demonstrated good alignment between business realities, industry standards, the board's expectations, and management's behaviors, a strict comparison with recommended practices may be unnecessary.

4.3.2. Design Effectiveness

Leveraging the information gathered in section 4.2., the internal auditor must now deliver an opinion on how effectively the ISG activity has been designed. If the analysis in section 4.3.1. concluded that there was insufficient accountability or authority at one or more levels, it is unlikely that the governance process can sustain effective performance. The organization that is following an incomplete framework will deliver unpredictable results over time. While testing may indicate that the overall framework is still effective at the time of the actual evaluation, the internal auditor should highlight this situation for attention because a lack of sustainability represents a control deficiency in the activity's design.

If there is sufficient accountability and authority, and the program reflects industry, board, and management expectations, the internal auditor likely will deliver an opinion that the ISG activity is effectively designed. The internal auditor may then proceed in assessing whether the activity is effectively implemented.

4.3.3. Information Security Program Effectiveness

At this stage of the evaluation, internal auditors have enough information to determine whether there is an ISG activity designed to support the organization's objectives and have identified whether sufficient accountability and authority have been assigned to enable the program. Even if all of these conditions hold, the program may still fail to achieve its stated objectives. The internal auditor must now examine the evidence (e.g., documentation, organization, and structure) generated by the ongoing execution of the ISG activity and decide — based on available evidence — how completely the deployed activity achieves its design potential. An effective ISG activity will show evidence of proper communication and training, maintenance of policies and standards, ongoing reporting of program results through metrics and qualitative comments, escalation of security- or risk-related events to a proper level of management, and appropriate responses when management's directives are unintentionally or intentionally circumvented. Additional details for each of these items include:

- Policies and standards must be maintained to remain effective and to appropriately reflect management's intent. The internal auditor should find some evidence that policies and standards are periodically reviewed. Reviews should be documented and provide independent validations as needed. For example, standards on information asset classification should be reviewed by people with sufficient expertise to confirm that the organization is updating its standards to reflect changing external requirements.
- Proper communication and training is necessary to effectively implement and maintain an ISG activity. This communication and training will vary depending on the audience, but it is necessary at all levels of the organization from the board of directors to end users, suppliers, and vendors. The internal auditor should be able to identify that some IS expectations are communicated at each level of the organization and to third parties that interact with the organization's information resources. For executives, this communication may be a brief discussion. For IT administrators, the training programs may be very involved. For vendors and suppliers, expectations may be identified and communicated contractually.
- The ISG activity must have some associated reporting. The level of formality associated with this activity will vary depending on the size, needs, and complexity of the organization. Although the number of metrics will vary depending on the organization, this reporting likely will include formal metrics (e.g., KPIs). This reporting process also should provide a mechanism for reporting on qualitative feedback. Key themes from a regulatory examination are an example of important qualitative feedback that does not conform to a simple mathematical formula like KPIs.
- The ISG activity also should demonstrate that security- and risk-related items are highlighted to a sufficient level of management to ensure effective responses. Significant items, such as suspected loss of trade secrets and exporting illegal software (e.g., encryption algorithms), may immediately be escalated to key executives while more benign items, such as personal use of an e-mail system, might be handled by line management. The governance process should demonstrate some overall reporting and tracking of these items to ensure that trends in IS can be detected and addressed early. This response process also may entail specific predefined responses to user activities. This may result in additional training, for example, when minor policy violations occur and disciplinary activity when major policy violations occur.

4.3.4. Efficiency

An important question that the internal auditor will face when analyzing any KPI is whether the reporting is sufficient to support ongoing gains in efficiency. Without sufficient reporting, the organization can never achieve ongoing process improvement. As an example, the organization may want to evaluate whether a two-hour, Web-based security course is as effective as a legacy four-hour classroom course. Without effective metrics, the organization probably will struggle to compare the relative effectiveness of the new course. With effective metrics, the organization may roll out the new course to selected sites or business units and compare security-related incidents among those receiving the legacy course and those receiving the new course. If the new course

yields comparable results, the organization can easily switch to the less time-intensive, lower-cost option and be reasonably sure that its security posture has not been negatively impacted. Even without the support of metrics that enable the organization to optimize its ISG activity, the activity may still be effective. Throughout this process, the internal auditor also should consider efficiency. As noted previously, the process can be effective but not efficient. Some examples of this behavior would include:

- *Excessive documentation of policies, standards, and procedures.* If the audit activity finds a 15-page procedure written about how to enroll in online security training courses, the organization has likely created too much documentation.
- *Excessive sign-offs or approvals.* If the organization requires CFO and CIO approval to enable a new user account for anything except the most sensitive systems, it has not improved security.
- *Excessive escalation of security issues.* If the CIO is notified each time that someone scans the perimeter firewall, security concerns are being inappropriately escalated.

4.3.5. Resource Levels

Given the understanding of the ISG activity, do the resources required align with the delivery of the service activity?

As with any other function, the ISG activity needs to be supported with adequate staffing. This GTAG previously discussed accountability and authority as critical enablers. Even with accountability and authority, it is possible to fail in delivering good governance because of insufficient personnel to ensure delivery. Because of the far-reaching nature of ISG, delivering good governance requires sustained support throughout the organization. As mentioned in section 4.1., governance may require support from a number of organization groups such as legal and human resources. If resources from any of these groups are not available, this dramatically impairs the long-term sustainability of ISG activities. Ensuring that proper staffing is maintained may require the person charged with managing ISG to periodically report to the board or other executive level management about the composition of the team, both in terms of key positions, the qualifications of the people in those positions, and the tenure of each person in a key position.

4.3.6. Value Added

What benefits are derived from the governance structure? If internal auditors have made it this far in the analysis and have confidence in the ISG activity, then they can assume that the organization will consistently codify the regulatory/legal needs and executive management's directives into actionable policies, standards, and procedures. Internal auditors also can conclude that these results are generally applied and understood across the organization. The net benefit of these activities results from a low probability of unacceptable loss associated with a security event. Because these concerns may create operational, regulatory, or reputational damage to the organization, management can take comfort in knowing that proactive efforts have dramatically decreased the chance that a major loss will occur and long-term strategies are likely to succeed without IS-related problems.

In any organization, a process must provide some benefit to the organization and the more value added, the better it enhances the organization. Are there value added benefits that could be obtained from the governance process? Can organizations improve on these benefits to obtain more value? Certainly, this is always possible. As previously mentioned, one possible improvement would be to measure the activity to see if it can be streamlined to deliver the same results. The example cited was replacing classroom training with streaming content to determine whether the end results are comparable. Another possible ongoing improvement is to use the organization's security for competitive advantage. As previously noted, strong IS should yield reductions in the number and severity of security-related incidents. The organization should carefully consider whether this can be translated into competitive advantage. For example, if the organization is providing online transaction processing, does the ISG activity provide sufficient confidence that the organization can contractually commit to higher availability targets than its competitors? This could yield competitive differentiation in the marketplace. If the organization is transferring risk through insurance, can it use the demonstrable outcomes of the ISG activities to negotiate lower insurance premiums?

Following the steps in this section, the internal auditor can begin to evaluate the effectiveness of the ISG activity.

4.3.7. Continuous Improvement

The design of the ISG activity should be reviewed periodically to verify that the organization's needs continue to be met. The prior discussion has largely focused on the execution against the current design, but efforts must be made to keep the design relevant. As the risk environment and organization change, so too must its IS activity. The internal auditor should verify that the board and management review the risk appetite, risk tolerance, and policies and procedures at least once a year according to a set schedule or after a major change (e.g., new regulations or key management changes) to the organization.

Questions to ask:

1. Is there a formal schedule identified to review the ISG activity?
2. Is there a document that identifies who will conduct the review, how it will be conducted, and how results will be communicated and acted upon, if necessary?
3. Have reviews been conducted according to schedule? Are the previous meetings' minutes formally retained and reviewed during subsequent meetings?

4. If corrective actions were identified as required, were outcomes of the reviews acted upon in a timely manner?
5. If formal meetings are infrequent, are committed activities tracked and reported against between formal meetings?

5. Conclusion/Summary

The internal auditor can help an organization understand the risks and options to create an effective ISG activity. Executive and line management throughout the organization must be held accountable for appropriately managing the risks associated with IS and ensuring that the tone at the top actively supports IS, as well as provides an important message for the entire organization to act appropriately and do the right things.

ISG provides the organization with a framework for making appropriate risk mitigation decisions and building the organization's ability to protect and react to external and internal threats. The ISG activity enables the organization to continuously build upon its security program through continuous feedback from the lowest line manager to the board.

The organization's ISG activity should be designed to maintain and grow the organization's security program. Effective and efficient ISG practices must include clearly defined roles and responsibilities, alignment of risk appetite with strategic IT objectives, effective communications and reporting, and maintaining accountability through value-added monitoring systems.

6. Appendix – Sample Audit Questions/Topics

6.1. Is the organization's risk appetite well defined and understood?

Every organization has a risk appetite whether defined or undefined. Sustainable performance requires a defined risk appetite that reflects the input of all key stakeholders and the industry, as well as supports regulatory expectations.

- Discuss risk and risk appetite with the board, executive management, and middle management. Is it consistently defined and understood at all levels? Is common terminology used to discuss risk?
- Is there evidence that risk is a component when making strategic decisions? Is risk included in discussions of new business ventures, strategic shifts in priorities, changes in the regulatory environment, and in planning and managing key initiatives?

6.2. Is there a defined, effective information security governance process?

An effective ISG activity builds upon risk management activities. It should support the evaluation of risk and control activities designed to mitigate or accept risk. It also should adapt to strategic shifts in business and regulatory climates.

- Discuss the risk management process with appropriate levels of management.
- Evaluate internally developed and deployed risk management frameworks against available industry guidance if it exists. Identify whether major gaps exist.
- Document recent significant changes in business and regulatory environments and discuss with appropriate levels of management to identify whether these are changed risk evaluations or ongoing management activities.

6.3. Is there effective organizational support for the information security governance activity?

Once the organization has defined and understood its risk appetite and identified common methods for defining and measuring risk, it still must provide sufficient training to encourage appropriate ongoing effectiveness.

- Identify whether roles and responsibilities are properly defined for supporting ISG. Review deliverables for key participants in the governance activity to ensure that supporting activities are occurring. Are those responsible for updating policies, standards, and procedures doing so? Are those responsible for monitoring the risk environment communicating to all affected stakeholders doing so? Are those responsible for delivering training doing so? Are employees given sufficient time and organizational support to complete required training courses? If specialist knowledge is required, is the organization hiring people with sufficient skills or purchasing expertise from external consultants?

6.4. Does the organization monitor the ongoing health of the information security governance activity?

Similar to any process supported by people, the process will drift away from its original goals and purpose over time. The process needs to be continuously monitored so that substantial shifts can be addressed in a timely manner.

- Is there effective reporting for the ISG activity? Is the reporting and feedback mechanism formal and highly structured or something less structured? Evaluate whether the level of formality is appropriate to the organization's size, complexity, and business activities.
- Are there defined, tracked, and reported metrics that can measure ISG? Are thresholds defined that identify when corrective action should be taken in response to changes in these metrics?
- Are people held accountable for performing activities that support governance? If training is not delivered in a timely fashion, does the organization take corrective action in response to this? If policies, standards, and procedures are not renewed in a timely manner, what is the organization's response?

6.5. Has the organization taken steps to improve its governance over time?

- Does it measure itself against external benchmarks?
- Does it use metrics data to drive sustained improvements?
- Does it look for inefficiencies in control and take action to streamline controls?

7. References

- *2007 Global State of Information Security Study*, PricewaterhouseCoopers.
- Bihari, Endre. Information Security Definitions. www.perfres.net
- *Building an Information Technology Security Awareness and Training Program* (Special Publication 800-50), National Institutes of Standards and Technology (NIST), Gaithersburg, Md., USA, 2003.
- *Corporate Governance of Information Technology* (ISO/IEC 38500:2008), International Organization for Standardization, 2008.
- *Enterprise Risk Management — Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission, 2004.
- *Governing for Enterprise Security (GES) Implementation Guide*, Software Engineering Institute, 2007.
- *GTAG-1: Information Technology Controls*, The Institute of Internal Auditors, Altamonte Springs, Fla., USA, 2005.
- *GTAG-9: Identity and Access Management*, The Institute of Internal Auditors, Altamonte Springs, Fla., USA, 2007.
- *GTAG-11: Developing the IT Audit Plan*, The Institute of Internal Auditors, Altamonte Springs, Fla., USA, 2008.
- *GTAG-12: Auditing IT Projects*, The Institute of Internal Auditors, Altamonte Springs, Fla., USA, 2009.
- *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (Special Publication 800-84), National Institutes of Standards and Technology (NIST), Gaithersburg, Md., USA, 2006.
- Guide to the Assessment of IT Risk (GAIT) Series, The Institute of Internal Auditors, Altamonte Springs, Fla., USA.
- *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd Edition, IT Governance Institute, Rolling Meadows, Ill., USA, 2006.
- *Information Security Governance: Guidance for Information Security Managers*, IT Governance Institute, Rolling Meadows, Ill., USA, 2008.
- *Information Security Oversight: A 2007 Survey Report*, National Association of Corporate Directors and KPMG's Audit Committee Institute.
- *Information Security Practical Guidance on How to Prepare for Successful Audits*, IT Compliance Institute, 2006. www.t2pa.com/analysis-a-advice/library/179-it-audit-check-list-information-security
- *Information Security Standards* (ISO/IEC 27000:2009), International Organization for Standardization, 2009.
- *Information Technology — Security Techniques — Key Management*, Australian Standard 11770.1—2003, Standards Australia International, Sydney, Australia, 2003.
- *Internal Control — Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission, 1992.
- The International Professional Practices Framework, The Institute of Internal Auditors, Altamonte Springs, Fla., USA, 2009.
- *An Introduction to Computer Security: The NIST Handbook* (Special Publication 800-12), Chapter 2: Elements of Computer Security, The National Institutes of Standards and Technology (NIST), Gaithersburg, Md., USA, 1995.
- The IT Service Management Forum. www.itSMFi.org
- *Performance Measurement Guide for Information Security* (Special Publication 800-55 Revision 1), National Institutes of Standards and Technology (NIST), Gaithersburg, Md., USA, 2008.
- *Program Review for Information Security Management Assistance* (PRISMA), National Institutes of Standards and Technology (NIST), Gaithersburg, Md., USA, 2007.
- *The Standards of Good Practice for Information Security*, Information Security Forum, 2007.

8. Authors and Reviewers

Authors:

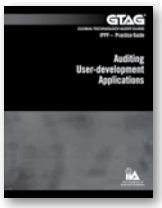
- Paul Love, CISSP, CISA
- James Reinhard, CIA, CISA
- A.J. Schwab, CISA,
- George Spafford, CISA

Reviewers:

The IIA thanks the following individuals and groups who provided valuable comments to this guide:

- AICPA – American Institute of Certified Public Accountants
- Douglas J. Anderson, CIA
- David F. Bentley
- Lily Bi, CIA, CGEIT, CISA
- Lawrence P. Brown, CIA, CISA
- Jeanot de Boer
- Lisa K. Hirtzinger, CIA, CCSA
- Steven Hunt, CIA, CISA, CGEIT
- The Institute of Internal Auditors – South Africa
- The Institute of Internal Auditors – UK & Ireland
- Rune Johannessen, CIA, CCSA, CISA
- David S. Lione, CISA
- Steve Mar, CFSA
- Cesar L. Martinez, CIA, CGAP
- Professional Practices Advisory Council:
  - Advanced Technology Committee
  - Board of Regents
  - Committee on Quality
  - Ethics Committee
  - Internal Audit Standards Board
  - Professional Issues Committee
- Sajay Rai
- R. Vittal Raj, CIA
- Ross A. Richards
- Stig J. Sunde, CIA, CGAP
- Dan Swanson, CIA, CISA, CISSP
- Johannes Tekle, CIA, CFSA
- Archie R. Thomas, CIA
- David Williams, CISA
- Tom Wilson, MIIA
- Karine F. Wegrzynowicz, CIA, CISA

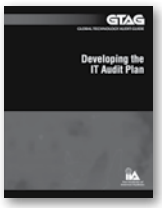
Written in straightforward business language to address timely issues related to IT management, control, and security, the GTAG series serves as a ready resource for CAEs on different technology-associated risks and recommended practices.



AUDITING USER-DEVELOPED APPLICATIONS (UDAs) addresses risks associated with UDAs, provides direction on how to scope an internal audit of UDAs, and includes sample internal audit programs. Because management relies on UDAs, they should be a consideration to incorporate into the audit plan.

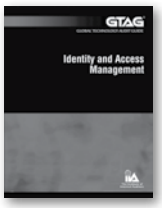
FRAUD PREVENTION AND DETECTION IN AN AUTOMATED WORLD addresses IT-related fraud risks and risk assessments and how the use of technology can help internal auditors and other key stakeholders within the organization address fraud and fraud risks.

AUDITING IT PROJECTS provides an overview of techniques for effectively engaging with project teams and management to assess the risks related to IT projects.

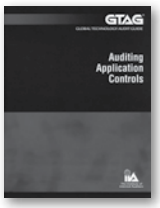


DEVELOPING THE IT AUDIT PLAN provides step-by-step guidance on how to develop an IT audit plan from understanding the business, defining the IT audit universe, and performing a risk assessment to formalizing the IT audit plan.

BUSINESS CONTINUITY MANAGEMENT defines business continuity management (BCM), discusses business risk, and includes a detailed discussion of BCM program requirements.



IDENTITY AND ACCESS MANAGEMENT covers key concepts surrounding identity and access management (IAM), risks associated with IAM process, detailed guidance on how to audit IAM processes, and a sample checklist for auditors.



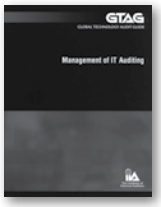
AUDITING APPLICATION CONTROLS addresses the concept of application control and its relationship with general controls, as well as how to scope a risk-based application control review.

Global Technology Audit Guide (GTAG)

INFORMATION TECHNOLOGY OUTSOURCING discusses how to choose the right IT outsourcing vendor and key outsourcing control considerations from the client's and service provider's operation.

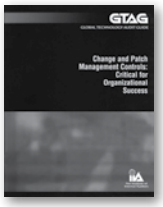
MANAGING AND AUDITING IT VULNERABILITIES discusses, among other topics, the vulnerability management life cycle, the scope of a vulnerability management audit, and metrics to measure vulnerability management practices.

MANAGING AND AUDITING PRIVACY RISKS discusses global privacy principles and frameworks, privacy risk models and controls, the role of internal auditors, top 10 privacy questions to ask during the course of the audit, and more.

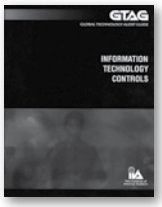


MANAGEMENT OF IT AUDITING discusses IT-related risks and defines the IT audit universe, as well as how to execute and manage the IT audit process.

CONTINUOUS AUDITING addresses the role of continuous auditing in today's internal audit environment; the relationship of continuous auditing, continuous monitoring, and continuous assurance; and the application and implementation of continuous auditing.



CHANGE AND PATCH MANAGEMENT CONTROLS describes sources of change and their likely impact on business objectives, as well as how change and patch management controls help manage IT risks and costs and what works and doesn't work in practice.



INFORMATION TECHNOLOGY CONTROLS topics discusses IT control concepts, the importance of IT controls, the organizational roles and responsibilities for ensuring effective IT controls, and risk analysis and monitoring techniques.

GTAG®

Information Security Governance

Information is a significant component of most organizations' competitive strategy either by the direct collection, management, and interpretation of business information or the retention of information for day-to-day business processing. Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated.

This Global Technology Audit Guide (GTAG) will provide a thought process to assist the chief audit executive (CAE) in incorporating an audit of information security governance (ISG) into the audit plan, focusing on whether the organization's ISG activity delivers the correct behaviors, practices, and execution of IS.

This GTAG will assist efforts to:

1. Define ISG.
2. Help internal auditors understand the right questions to ask and know what documentation is required.
3. Describe the internal audit activity's (IAA) role in ISG.

We'd like your feedback! Visit the GTAG page under www.theiia.org/gtags to rate it and submit your comments.

The Institute of Internal Auditors

www.theiia.org

53000

9 780894 136870

Order Number: 1073
ISBN: 978-0-89413-687-0
Member Price: $25.00
Nonmember Price: $30.00

IPPF ALIGNED
International Professional Practices Framework