The Institute of Internal Auditors

Richard F. Chambers
Certified Internal Auditor
Qualification in Internal Audit Leadership
Certified Government Auditing Professional
Certification in Control Self-Assessment
Certification in Risk Management Assurance
President and Chief Executive Officer

T: +1-407-937-1200
E-mail: richard.f.chambers@theiia.org

January 16, 2017

Secretary, Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Response emailed to: regs.comments@federalreserve.gov

RE: Enhanced Cyber Risk Management Standards
Docket No. R-1550, RIN 7100-AE61

Dear Sir/Madam:

On behalf of the more than 65,000 U.S. members of The Institute of Internal Auditors (IIA), I am pleased to provide a response to the joint advance notice of proposed rulemaking, Enhanced Cyber Risk Management, issued by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation.

The IIA has a longstanding position that the presence of an effective internal audit function makes an unequivocal statement about the way an organization's leadership views strong and effective risk management, internal control, and corporate governance. As a result, we believe that the internal audit function would be well-positioned to provide assurance under the areas being considered in the proposed standards, as demonstrated by high-performing internal audit functions in the financial industry that already incorporate cyber risk management assessments in their overall audit plans. One of the main functions of internal audit is the evaluation of the corporate and IT governance structures and practices within an organization, in conformance with "IIA Standard 2110 – Governance":

The internal audit activity must assess and make the appropriate recommendations to improve the organization's governance processed for:

- Making strategic and operational decisions.
- Overseeing risk management and controls.
- Promoting appropriate ethics and values within the organization.

Global Headquarters
1035 Greenwood Blvd, Suite 401
Lake Mary, FL 32746 USA
T: +1-407-937-1100
F: +1-407-937-1101
www.theiia.org

- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communication information among, the board, external and internal auditors, other assurance providers, and management.

2110.A2 – The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

The evaluation of effective governance includes the assessment of key components, such as leadership, organizational structure, policies, processes, risks, and controls as described in The IIA's Global Technology Audit Guide (GTAG), **"Auditing IT Governance,"** issued in July 2012 (copy attached).

Due to the dynamic nature of cyber risks, as well as the varied size and industry role of certain covered entities, any standards resulting from the new rulemaking should permit flexibility for developing frameworks that would allow allocation of resources to effectively address areas of higher risk (Question 2). In addition, as the enhanced cyber risk management standards will apply to key vendors to financial institutions, The IIA recommends consideration for a new type of generally accepted, service provider cyber risk management reporting, as this would greatly reduce the burden on these vendors of having multiple clients conduct individual assessments (Question 4).

The IIA supports the requirement that covered entities structure cyber risk management into the Three Lines of Defense model. The participation of business units, and risk management in the implementation of cyber risk initiatives, is critical because IT management must have a clear understanding of the organization's objectives, risk profile, business processes, and dependencies on third parties to develop and implement the necessary controls to address cyber risks.

Internal audit as the third line of defense can evaluate the effectiveness of risk management, internal controls, and corporate and IT governance, and provide advice to the board to better manage an organization's IT environment within its risk appetite and tolerance.

Conformance with the following IIA standards currently prepare an internal audit function to discharge the responsibilities described in the proposed standards (effectively monitor, measure, manage and report on cyber risk):

1110 – Organizational Independence
1111 – Direct Interaction with the Board
2000 – Managing the Internal Audit Activity
2130 – Control
2420 – Quality of Communications
2440 – Disseminating Results

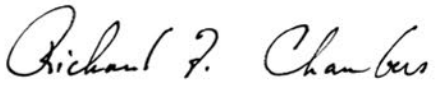
Reports on cyber risks, threats and vulnerabilities should include expert interpretation of the data so as to provide meaningful analysis for the board and executive management to make effective decisions. Internal audit can provide assurance reports on the effectiveness of the cyber risk framework, including vulnerabilities, and controls. However, mandating specific reporting frequency may be inefficient, as the board and executive management should be kept informed, as necessary,

when there is a significant weakness or cyber incident. The IIA recommends that the board and executive management work with internal audit to determine the nature of reports based on the current level of risk. Over time, the appropriateness of the report details can be reviewed and adjusted periodically by the board and executive management. (Question 15).

The IIA is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in New York in 1941, The IIA today serves more than 185,000 members from more than 170 countries and territories. The association's global headquarters are based in Lake Mary, Fla.

We appreciate the opportunity to provide our response to this joint advance notice of proposed rulemaking. If you have any questions about our response or would like to discuss further, please contact Kathy Anderson, The IIA's Managing Director of North American Advocacy. Ms. Anderson can be reached at Kathy.anderson@theiia.org or 1-407-937-1291.

Sincerely,



Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
President & Chief Executive Officer

Attachment: Global Technology Audit Guide *"Auditing IT Governance"*

cc: Cassian Jae, Director, Financial Services Audit Center
Brad Jones, Director, Government Relations

GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Auditing IT Governance

The Institute of Internal Auditors

Global Technology Audit Guide (GTAG®) 17
Auditing IT Governance

July 2012

GTAG — Table of Contents

EXECUTIVE SUMMARY 1

1. INTRODUCTION 2

2. IT GOVERNANCE RISKS 7

3. ALIGNING THE ORGANIZATION AND IT — Key Considerations 12

4. THE ROLE OF INTERNAL AUDIT IN IT GOVERNANCE 15

CONCLUSION 18

AUTHORS AND REVIEWERS 18

APPENDIX — IT Governance Risk Assessment/Engagement Planning Considerations 19

Executive Summary

As defined by The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF), *governance* is "the combination of processes and structures implemented by the board[1] to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives." The internal audit activity is uniquely positioned and staffed within an organization to make significant contributions toward achievement of these objectives by providing assurance and consulting services related to organizational governance. While effort is generally focused on the delivery of governance services, the IT component, in many cases, continues to be lacking or ignored. Combined with the continued increase in the speed of technological advancement, IT proliferation, and organizational dependence on IT, it is clear why the internal audit activity should address this inherently high-risk area. To this end, an interpretation of IIA Standard 2110: Governance states, *"the internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives."*

While IT supports the financial and human capital governance areas, it plays a much more significant role with respect to organizational information. The information and technological components of an organization are among its most important assets. A lack of appropriate governance over information stored, processed, or produced by IT systems can have a significant negative impact on an organization, ranging from fines and penalties to damaged reputation that can take time, energy, and money to rebuild. In many organizations, there is a disconnect between senior management and IT due to the view that IT exists solely to deliver day-to-day IT services.

Research[2] shows that proper alignment of organizational objectives and IT result in as much as a 20 percent higher return on investment[3] (ROI). Alignment of organizational objectives and IT is more about governance and less about technology. Governance assures alternatives are evaluated, execution is appropriately directed, and performance is monitored, and these same concepts apply to IT governance.

To support the heightened importance of IT governance and the mandatory nature of the *International Standards for the Professional Practice of Internal Auditing* (*Standards*), this GTAG provides internal auditors with the foundational knowledge necessary to fulfill their responsibilities in providing both assurance and consulting services, applicable in the public and private sector. Some of the key areas of IT governance internal auditors should address are:

- Chief IT Officer (e.g. Chief Information Officer; Chief Technology Officer; Chief Information Security Officer) related roles and responsibilities.
- Accountability and decision-making.
- IT performance monitoring and reporting metrics, including financial management of IT operations and projects.
- CxO[4] level of understanding of how IT supports and enables the achievement of the organization's strategy and objectives.
- Alignment between IT and the organization.
- IT governance risks and controls.

Additionally, internal auditors face the challenge of assisting and educating the board and management team on the role(s) of the internal audit activity within governance processes and how to maximize the value to the organization.

This GTAG covers aspects of governance that should be in place to ensure IT supports the strategies and objectives of the organization. It also describes elements of effective governance and performance frameworks such as balanced scorecards, maturity models, and quality systems. This guidance describes example controls that address IT governance risks, audit planning, verification, testing, and reporting actions useful in the development of practical audit programs. Finally, this GTAG provides guidelines to facilitate audits of IT governance by providing direction on how to scope the engagement, define audit objectives, and evaluate related risks and controls.

IT governance is defined by the IPPF as: "IT governance consists of the leadership, organizational structures, and processes that ensure that the enterprise's [IT] supports the organization's strategies and objectives."

1 The term *board* is used in this GTAG as defined in the *Standards* glossary: "a board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report."

2 Source: Accenture, ISACA/IT Governance Institute, Peter Weill, and Jeanne Ross.

3 ROI: A performance measure used to evaluate the efficiency of an investment or to compare the efficiency of a number of different investments. To calculate ROI, the benefit (return) of an investment is divided by the cost of the investment; the result is expressed as a percentage or a ratio.

4 CxO denotes different Chief Officers. C-suite is a term used for chief officers or executive/top/senior management. Though different titles are used in the public sector, the topic covered in this GTAG is applicable to both public and private sector.

1. Introduction

The purpose of this guide is to increase the internal auditor's awareness and understanding of IT governance and provide guidance on how to address governance as part of internal audit engagements required by Standard 2110.

1.1 What is IT Governance?

IT governance involves managing IT operations and IT projects to ensure alignment between these activities and the needs of the organization defined in the strategic plan. Proper alignment between IT and the organization means: 1) organization management understands the potential and limitations of IT; 2) the IT function understands the objectives and corresponding needs of the organization; and 3) this understanding is applied and monitored throughout the organization via an appropriate governance structure and accountability. Understanding the value and the cost of IT is important for the board and senior and IT management. Successful alignment between the organization and IT occurs when goals and objectives of the organization are aligned with the needs of the organization, and IT is able to meet those needs in collaboration with management.

1.2 IIA Standards

Standard 2110 states, "the internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management."

While several IIA standards have components related to the internal auditor's role with respect to IT, no other standard is as clear as Standard 2110.A2, which states,

"the internal audit activity must assess whether the [IT] governance of the organization supports the organization's strategies and objectives."

IT governance includes processes and combinations of controls that help organizations better manage their IT environments and balance their overall IT risk profile and organizational objectives within risk appetite and tolerance levels. IT governance helps to increase an organization's ability to achieve its overall goals and objectives. The internal audit activity should evaluate the IT governance structure and ability to deliver results for the organization and make recommendations for improving the efficiency and effectiveness of the IT function.

1.3 IT Governance — Roles and Global Standards

The board and senior management should play critical roles in directing, evaluating, and monitoring IT (see Figure 1: IT Governance Roles, Standards, and Frameworks below). Effectiveness of the IT governance structure and processes are directly dependent upon the level of involvement of the board and senior management. Figure 1 provides examples of frameworks and standards relevant to governance levels, from corporate governance standards, to IT governance standards, and more operational IT management standards. Different levels of the framework require different tools, techniques, and standards addressing specific needs of an effective IT governance structure.

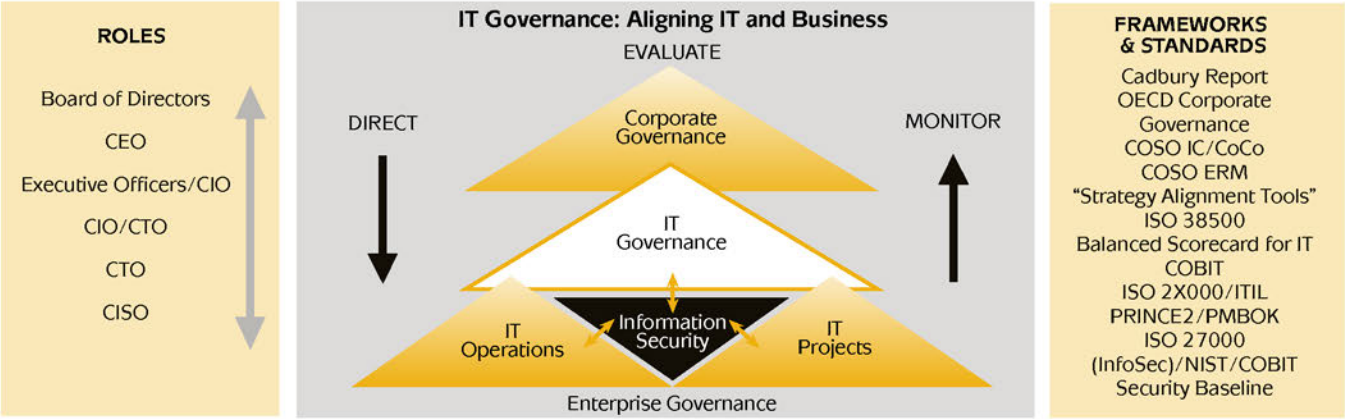


Figure 1: IT Governance Roles, Standards, and Frameworks[5]

5 CIO: Chief Information Officer; CTO: Chief Technology Officer; CISO: Chief Information Security Officer

1.4 IT Governance — Characteristics & Risks

IT governance consists of the organizational structure, leadership, and processes that ensure IT support of the organization's strategies and objectives. Figure 2: IT Governance Five Components shows the five important components of effective IT governance. The five components are:

- Organization and Governance Structures.
- Executive Leadership and Support.
- Strategic and Operational Planning.
- Service Delivery and Measurement.
- IT Organization and Risk Management.

The board and executive management evaluate alternatives, provide direction, and monitor achievement of the organization's strategies and objectives.

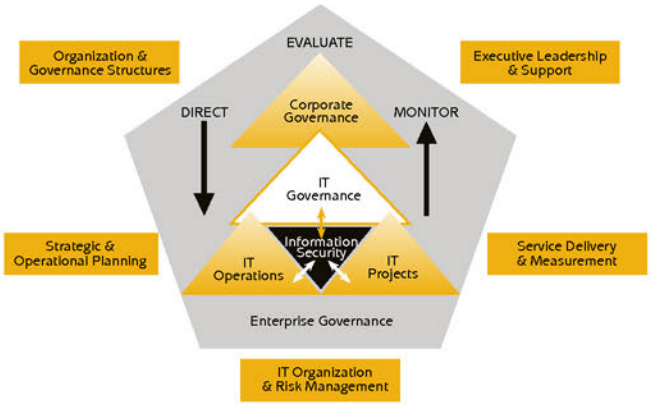


Figure 2: IT Governance Five Components

Organization and Governance Structures

Clear organizational structures, the operational nature of their components, how they communicate with each other, and the accountability protocols are important for the IT function to provide the required types and levels of service, based on investments in IT, for the enterprise to achieve its objectives. In addition, the governance structure should be aligned with the organizational structure. For example, if strategic management is centralized within headquarters, the governance structure should be centralized as well. However, if the organization is decentralized and divisions operate more independently or autonomously, the governance structure also should be decentralized. The IT enterprise architecture should mirror the organizational structures to enable better alignment and meet the organization's needs. The board and senior management should engage IT and the CIO in the strategic decisions about governance, enabling IT to add value in key decisions.

Existing organization and governance structures provide a good indication of whether IT supports and helps enable the organization in achieving its strategic objectives. The following questions will help the internal auditor gain an understanding of the degree or presence of IT governance:

1. Is there a CIO in place, and is he or she a member of the senior management team?
2. Are the structure of the organization and its operational components clearly organized such that the IT function can efficiently and effectively help enable the achievement of the organization's objectives?
3. What decision bodies are in place to enable alignment of organization needs with IT services and do they have adequate empowerment and accountability?
4. Are organizational needs and IT service requirements defined in strategic and tactical plans, and monitored? Do the CIO and senior management meet and discuss progress on plans on a regular basis?
5. Are roles and responsibilities clearly defined and communicated, and are organization leaders empowered and held accountable for results?

Executive Leadership and Support

An important requirement to enable and sustain alignment between IT and organization objectives is the tone at the top and executive leadership. The board, CEO, CIO, and other senior management team members should set a clear vision for the organization understanding and communicating how IT supports and enables the enterprise to achieve its objectives, which in turn enables a more effective ROI on IT spending. With clear alignment of IT to the organization's strategy, executive leadership will view and support IT as a strategic enabler and not just another cost to the organization. This vision should be documented in the form of a strategic plan that defines IT dependencies. This strategic plan is driven by the board and top management.

It is important to determine the effectiveness of the tone at the top, how the tone is communicated to all levels within the organization, and how that message impacts the IT function. The following questions will help the internal auditor gain an understanding of the degree to which the IT function is integrated into the organization:

1. Does senior management have clearly defined and communicated roles and responsibilities for the IT function with respect to the organizational achievement of strategic and tactical goals?
2. Are the roles and responsibilities of the CIO clearly defined and communicated?

3. Does the organization recognize in its strategy that the IT function is a significant contributor in enabling the achievement of goals, as well as supporting the organization on a day-to-day basis?
4. Is the CIO a member of the senior management team? Does the CIO meet with the board and the senior management team on a regular basis to discuss IT service delivery related to strategic and tactical plans?
5. Does IT have adequate funding to meet the organization's needs?

Strategic and Operational Planning

An important component of effective IT governance should be reflected in the form of a strategic plan. This strategic plan should define organizational dependencies of IT and the IT function's role and responsibilities in achieving the objectives set forth in the plan. The CIO, in turn, should create a tactical operating plan that is aligned with the strategic plan of the organization. This operating plan provides the mechanism for how the IT function is measured in terms of supporting and enabling the achievement of goals defined within the strategic plan. The lack of proper definition and identification of IT goals within the strategic plan may be an indication of improper alignment between the organization's goals and IT's goals. This omission could increase the risk that the organization will not achieve its goals in an efficient and cost-effective manner. Scorecards or similar management tools can be used to monitor IT's efforts toward the achievement of objectives noted in the strategic plan. IT should be measured on how it contributes to the achievement of strategic goals of the organization.

Strategic performance management is an integral component of effective IT governance, enabling proper mechanisms to govern the needs of the organization and IT service delivery. The internal auditor can gain an understanding of how well strategic performance management has been implemented by senior management by asking the following questions:

1. Do the board and senior management view IT as a strategic organizational partner?
2. Does the strategic plan of the organization include how IT is required to support and enable value creation?
3. Is the strategic plan supported by individual tactical operating plans that take into account IT requirements and deliverables?
4. Are key performance indicators (KPIs) used by senior management to measure and monitor the effectiveness of the IT function?
5. Are strategic IT investment decisions based on accurate cost benefit analyses and evaluated after implementation to determine whether the projected ROI has been realized? Are lessons learned factored into future IT investment decisions?
6. Is the IT organization structured effectively relative to the size and composition of the organization?
7. Are the CIO and IT leadership qualified and experienced?

Service Delivery and Measurement

Proactively managing IT spending and measuring the resulting value increases the likelihood of greater ROI from IT investments. A financial model should be part of performance management used by the organization, which should include IT metrics. One important aspect of performance management is the extraction and measurement of the right data. The measurement of financial data requires the right information at the appropriate level of detail. An effective performance management framework that captures the right quantitative and qualitative data to enable proactive measurement, analysis, and transparency further assures sound IT governance. These metrics will normally include measurements of services delivered to users/customers and technical and non-technical user satisfaction.

IT-related financial metrics play an important role in measuring strategic, operational, and technical results. Outcomes enabled by IT should be measured to show the value contribution at the strategic and tactical levels. These measurements allow IT management to understand how it is performing relative to the strategic plan, and to better understand how to more effectively manage the cost of IT service delivery by organizational unit, line of business, etc.

Service delivery metrics include financial management. This is an important component of controlling and monitoring IT costs/benefit measurement. Answers to the following questions can indicate how well financial management of IT is functioning:

1. Do the board and senior management have a clear understanding of IT costs and how they contribute to the achievement of organization strategic objectives?
2. Do leaders of the organization measure IT value and deliverables? How?
3. How do IT costs compare to other comparable organizations?
4. Is CIO performance measured by financial and nonfinancial data?

5. What sourcing arrangements are in place, and how are these measured and monitored?

IT Organization and Risk Management

How are IT risks and resources managed (both human and technical)? The success of IT is heavily dependent upon direction provided by the board, CEO, and other members of senior management. This direction is built into and communicated through the organization's strategic plan and structure.

Although components of IT are technical in nature, the measurement of IT governance is less technical. Internal auditors can gain a high-level understanding of the IT governance environment by asking the following questions:

1. To what degree are organizational processes automated?
2. How complex is the IT infrastructure and how many applications are in use?
3. Are data standardized and easily shared across applications (and the IT infrastructure)?
4. Are there standard IT hardware, software, and service procurement policies, procedures, and controls in place?
5. How mature are IT management processes and are recognized frameworks used (e.g., COBIT IT Governance Framework, ITIL IT Service Management framework, ISO 20000?
6. How are risks managed in relation to meeting organization needs, security, and compliance requirements?
7. What is the strategic importance of IT?

Responses to these key questions provide the internal auditor with a foundation on which to build and to understand how best to scope and execute an IT governance audit.

IT Governance — Characteristics and Benefits

IT governance can influence and impact the entire organization.

- **Enhancing the Relationship Between the Organization and IT** — IT governance structures and processes provide mechanisms to link the use of IT to the overall strategies and goals of the organization. The relationship between the organization and IT helps ensure limited resources are focused on doing the right things at the right time. Communication between IT and the organization should be free flowing and informative, providing insight into what IT is delivering to assist in the achievement of organization goals, and the status of those efforts. Internal audit should review the alignment and determine whether strong portfolio management processes exist, allowing the organization and IT to collaborate on resource priorities, initiatives, and overall investment decisions.
- **Enterprise Risk Management of the Organization and IT** — Risk management is a key component of an effective IT governance structure within an organization. IT governance helps ensure close linkage to an organization's risk management activities, including enterprise risk management (ERM). IT governance should be an integral part of overall corporate risk management efforts so that appropriate techniques are incorporated into IT activities, including communication of status to key stakeholders. Internal audit should review the risk management activities being utilized by the organization and determine whether adequate linkage exists between IT risk management and corporate risk activities such that appropriate attention is being given to the IT risk profile. *The Risk IT Practitioner Guide* developed by the IT Governance Institute (ITGI) provides a framework for identifying and assessing IT risks while also providing direct linkage to ISACA's COBIT framework.
- **Visibility Into IT Management's Ability to Achieve its Objectives** — IT organizations should define their strategies and tactics to support the organization by ensuring day-to-day IT operations are delivered efficiently and without compromise. Metrics and goals are established to help IT perform on a tactical basis and also to guide the efforts of personnel to improve maturity of practices. The results will enable the IT function to execute its strategy and achieve its objectives established with the approval of organization leaders. Internal audit can determine whether the linkage of IT metrics and objectives aligns with the organization's goals, adequately measure progress being made on approved initiatives, and express an opinion on whether the metrics are relevant and useful. Additionally, internal audit can help validate that metrics are being measured correctly and represent realistic views of IT operations and governance on a tactical and strategic basis.
- **IT Governance Improves the Adaptability of IT to Changes in the Organization and the IT Environment** — IT governance provides a foundation for IT to better manage its responsibilities and support of the organization through defined processes and roles/responsibilities of IT personnel. By having such formality in place, IT has the ability to better identify potential anomalies on a daily and trending basis, leading to root cause identification. Additionally, IT can thus adapt more easily to ad hoc requests for new or enhanced organizational capabilities. Internal audit

can evaluate such data sources as helpdesk and problem management to evaluate how IT is addressing known issues. Internal audit can also review IT portfolio management processes to understand how needs are prioritized and whether flexibility exists to reprioritize needs based on changing priorities of the organization.

As internal audit activities evaluate the IT governance structure and practices within an organization, several key components that lead to effective IT governance can be evaluated.

- **Leadership.** Evaluate the relationship between IT objectives and the current/strategic needs of the organization and the ability of IT leadership to effectively communicate this relationship to IT and organizational personnel. Assess the involvement of IT leadership in the development and ongoing execution of the organization's strategic goals. Determine how IT will be measured in helping the organization achieve these goals. Review how roles and responsibilities are assigned within the IT organization and how they are executed. Review the role of senior management and the board in helping establish and maintain strong IT governance.
- **Organizational structure.** Review how organization management and IT personnel are interacting and communicating current and future needs across the organization. This should include the existence of necessary roles and reporting relationships to allow IT to meet the needs of the organization, while providing the opportunity to have requirements addressed via formal evaluation and prioritization. In addition, how IT mirrors the organization structure in its enterprise architecture should also be included.
- **Processes.** Evaluate IT process activities and the controls in place to mitigate risks to the organization and whether they provide the necessary assurance regarding processes and underlying systems. What processes are used by the IT organization to support the IT environment and consistent delivery of expected services?
- **Risks.** Review the processes used by the IT organization to identify, assess, and monitor/mitigate risks within the IT environment. Additionally, determine the accountability that personnel have within risk management and how well these expectations are being met.
- **Controls.** Assess key controls that are defined by IT to manage its activities and the support of the overall organization. Ownership, documentation, and reporting of self-validation aspects should be reviewed by the internal audit activity. Additionally, the control set should be robust enough to address identified risks based on the organization's risk appetite and tolerance levels, as well as any compliance requirements.
- **Performance measurement/monitoring.** Evaluate the framework and systems in place to measure and monitor organizational outcomes where support from IT plays an important part in the internal outputs in IT operations and developments.

2. IT Governance Risks

A survey on IT governance performed by ITGI[6] revealed, from a strategic perspective, that high-performing organizations have more effective IT governance programs and processes in place when the IT function and the organization are aligned. More specifically, the survey results noted the following key findings and conclusions that should be addressed by organizations to strengthen IT governance:

- Ownership of IT accountability and IT governance.
- The CIO reporting line should be as direct as possible to senior management.
- More attention should be paid to the potential innovation IT can offer.
- Enterprise wide IT value measurements should be in place.

As noted in Sections 1 and 2, alignment between IT and the mission of the organization should exist within the five key components that are indicative of effective IT governance. This alignment requires effective strategic management and organization structures that appropriately allow IT to ensure the activities of the IT function support the organization's objectives. Financial and performance management provide the tools to direct, manage, and monitor IT activities to ensure the organization's objectives are achieved.

Organization structure should be addressed together with technological architecture considerations. The latter requires large investments that may lead an organization in a direction that is too costly to change and may not adequately support the needs of the organization. Discussion of cost benefit analyses should take place at the board level, as well as within the senior management team, to ensure alignment between the organization and IT. All of these critical elements begin with leadership. The senior management team and other key members of management set the tone and provide clear direction on how IT and the organization should be aligned for optimal achievement of strategic objectives and ROI. This requires senior management to understand IT, its characteristics, and inherent risks.

6 Global Status Report on the Governance of Enterprise IT (2011), Unlocking Value: An Executive Primer on the Critical Role of IT Governance (2008), and Understanding How Business Goals Drive IT Goals Executive Briefing (2008), published by ISACA and ITGI.

The following section provides more information on the five components of IT governance and gives insight into some of the ways the organization and IT can be misaligned and the resulting risks.

2.1 Organization and Governance Structures

Clear organizational structures and accountability are paramount for IT to deliver value and enable the organization to meet its strategic objectives. Since the ROI in IT is generally long-term in nature and the impact is felt for some time, it is important that a clear organization structure is established and that the IT function is aligned within it. The role of the IT function should be clearly defined within the strategic plan, and management should be empowered to make the necessary decisions and be held accountable for results.

Organization — Operating Model

With a centralized operating model, standards and processes can be more easily enforced across organizational units. From the IT perspective, components such as infrastructure and applications — including supporting standards and procedures — can be uniformly applied. In addition, it is important that the board and senior management assure the CIO understands how the organization structure works and its inherent risks to apply the most appropriate investment solutions for IT infrastructure and applications investments.

A decentralized organizational structure reduces the possibility of scalability because this normally means that operating units (different legal or geographical entities) are allowed to have different IT infrastructures and applications, which often reduces the possibilities of leveraging IT investments and sharing information and standards across the enterprise. However, there may be valid reasons for operating in a decentralized manner that do not inherently have a negative impact on organizational or IT governance or investments.

Governance — Accountability

One aspect of successful IT governance is accountability of organizational leaders. Organization structures should include clear lines of reporting and role responsibilities. The strategic goals and objectives of the organization should be driven to operational objectives and targets, and responsibility for objective achievement should be placed on unit leaders, which promotes clear accountability, especially if linked to performance monitoring. Unit leaders should be empowered to manage resources within their area of responsibility, enabling them to manage toward expected performance targets.

Operations versus Projects

The interaction between organization units and IT should occur formally and informally. From a formal perspective, regular communication should occur through a committee consisting of leaders from organization units and IT. As part of this structure, organization unit leaders meet with the CIO and other IT function leaders to determine the most effective methods for supporting and further enabling the achievement of each unit leader's objectives. When significant changes to the IT environment are required, the efforts will normally be organized as a project with a separate project committee reporting to senior management (see *GTAG 12: Auditing IT Projects*).

Outsourcing IT Services

Many organizations today outsource part or all of their IT function to service providers. While there are many benefits to these arrangements, they are not without risk when it comes to the strategic use of IT. Managing a sourcing partner requires an appropriate structure, which not only monitors performance, but also includes leaders within the organization who have the appropriate level of authority to hold the providers accountable. Some of the tools used to manage and monitor IT service providers are performance targets, service level agreements (SLAs), and scorecards. It is important to understand and remember that senior management cannot abdicate its ultimate responsibility for IT service delivery just because it has been outsourced. The table below lists some of the indicators of possible misalignment between the organization and IT.

Organization and Governance Structures	Consequences of Misalignment (Risks)
Lack of empowerment or accountability	Creates leadership void and potential lost opportunities
Unclear IT and operational organizational structures	Promotes resource mismanagement and conflicting activities Possible misalignment with resources and operational objectives
Unclear communication channels between IT leaders and organizational unit leaders	Lack of an effective planning and monitoring system

2.2 Executive Leadership and Support

Investments in IT can be large in relation to an organization's overall budget and require cost benefit analysis and ROI calculations as a basis for the board and senior management to make the best decisions possible. To reduce the risks resulting from unsound IT investment decisions, organization leaders should understand important characteristics of IT. The IT architecture of an organization is a direct reflection of its mission, vision, and the strategy.

The table below lists some of the indicators of possible disconnects between the organization and IT with respect to leadership and knowledge. For the CIO to make appropriate investments in IT, he or she relies very heavily on the vision, mission, and associated strategy of the organization. Collectively, these provide the direction on where to focus IT investment dollars. The lack of a clear vision, mission, and strategic plan for the organization and the role of IT can result in ineffective use of IT capital and other resources, thereby reducing the organization's ability to achieve its goals.

Executive Leadership and Support	Consequences of Misalignment (Risks)
Lack of clear entity wide vision by senior management and IT senior management	Inability to meet the organizational mission
Senior management not appropriately involved in the IT decision-making process	Allows for misdirection of resources Lack of oversight and improper delegation of authority
Lack of core organizational focus by IT senior management	IT is unable to focus efforts or identify inefficient use of resources
Senior management and unit leaders lack a true understanding of IT	Possibility of missed opportunities and lower return on IT investments
The strategic importance of IT is not assessed	Misunderstanding of what role IT plays in the organization

2.3 Strategic and Operational Planning

IT governance relates to the achievement of organizational objectives (outcomes), whereas IT management is focused on operational aspects and ensuring IT services are delivered timely with a high degree of quality, the outputs of which are measured in more technical terms. In a model IT governance structure, the IT function is measured not just on its performance related to operational/tactical plans, but on its impact on the achievement of organizational objectives documented in the strategic plan.

Strategic Metrics for IT Projects

For IT projects, there should be metrics in place to measure IT project effectiveness in terms of timeliness of delivery, budget vs. actual spending, and whether the solutions delivered contributed to the achievement of organizational objectives as noted in their cost benefit analysis (see *GTAG 12: Auditing IT* Projects for more details). Cost benefit analysis for each potential IT investment should include ROI analysis, transformation costs, and benefits. It also is important to note the distinction between output and outcome and measure each. While output metrics might be useful and possibly the only means of measurement, the internal auditor should analyze these in relation to actual outcomes. In addition, performance-based agreements and incentives should be reviewed to ensure the organization is exercising intended governance. Post-implementation reviews are a useful tool for learning and increasing knowledge of what works and what does not.

Strategic Metrics for IT Operations

Metrics should be in place to measure the effectiveness of the day-to-day operational aspects of the IT function. From an internal perspective, IT management will require more technical metrics such as system uptime/downtime, helpdesk ticket open-to-closed ratio, peak usage time periods, capacity, and utilization. To enable easier measurement of IT's impact on the achievement of strategic organization goals, it could be helpful to break down these goals into lower level operational component objectives and use various metrics such as SLAs and operations level agreements (OLAs). The table below provides some indications of misalignment between the organization and IT. A clear strategy that includes IT, with appropriate performance indicators, is one of the keys to effective IT governance.

Strategic and Operational Planning	Consequences of Misalignment (Risks)
Organizational strategy does not address IT	Strategic IT objectives will not be achieved
Organizational improvements via IT resources are not evaluated	Potential for inefficiencies within the organization
Unclear sourcing strategies and lack of SLAs	Failure to meet organizational requirements
Lack of empowerment or accountability for results	Creates leadership void and potential lost opportunities
Ineffective IT financial management	Misuse of IT financial resources

2.4 Service Delivery and Measurement

Effective management of IT costs increases the likelihood of obtaining value from IT operations while ensuring budgeted dollars are spent appropriately. IT financial metrics play an important role on strategic, operational, and technical levels. IT deliverables should be measured to show the value contribution and to understand and manage the costs of IT services at the organization unit level. It is also important to note that IT financial metrics work hand-in-hand with strategic and performance management metrics. Service delivery includes more than financial metrics, but ensuring return on IT investments will require a focus on financial metrics.

One important aspect of financial management is the ability to extract the right information as well as measure the components correctly. For effective analysis of financial metrics, the details should be available.

The table below provides some indicators of misalignment of IT and the organization from a financial management perspective.

Service Delivery and Measurement	Consequences of Misalignment (Risks)
Costs are higher than comparable entities	Inefficiencies are the norm and not the exception
No drill-down capabilities to lower-level metrics as needed	Not able to achieve organizational mission
IT costs are not known or detailed enough	Returns on IT investments are not monitored Lack of decision-making information
Do not track the value delivered by IT initiatives	Lack of accurate financial data
No meaningful metrics or too many metrics	Inability to achieve financial and management goals
No accountability	Unable to enforce accountability for initiatives or outcomes
IT senior-level compensation not linked to organizational outcomes	Misalignment between organizational outcomes with strategic objectives
No measure of technical/operational and financial performance in IT	Lack of alignment with goals and strategic mission

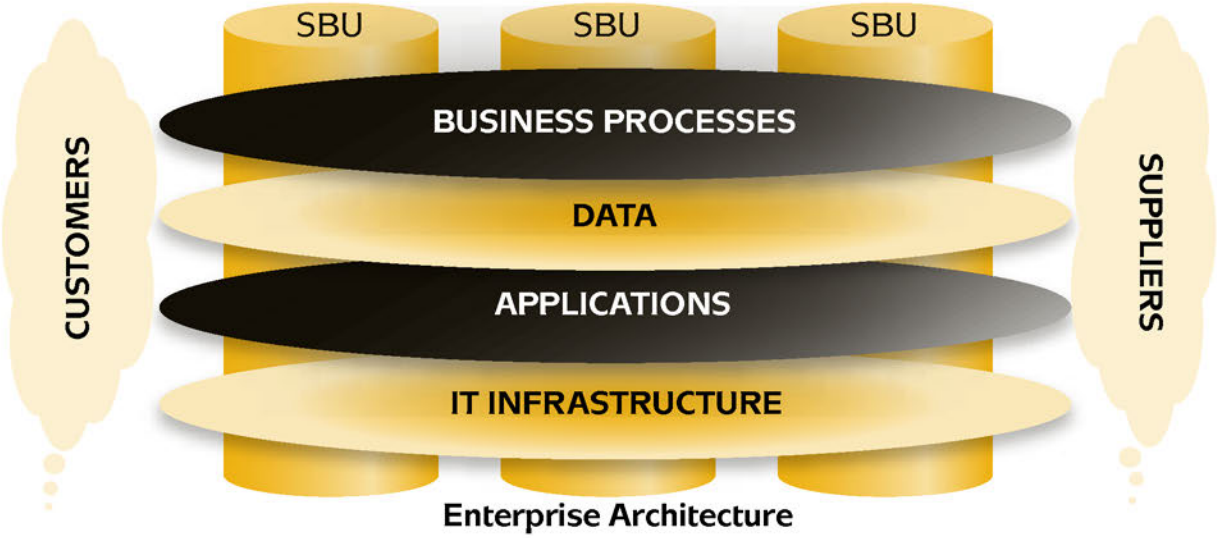
2.5 IT Organization and Risk Management

Information and the technical components of the IT environment should be very well organized to include methodologies and related standards for technology selection, acquisition, and implementation. However, the ultimate success of the IT function and its efforts is predicated upon the direction provided by the board and senior management in the form of a strategic plan and properly designed organizational structures.

Enterprise Architecture

The technical enterprise architecture should be developed based on the operating model of the organization and aligned with the organization's strategy. A centralized operating model may be beneficial in that it enables IT to have a more homogeneous infrastructure and fewer applications supporting organizational processes across the enterprise. This also facilitates easier sharing and standardization of information and should enable better and more complete reports across areas for monitoring and decision-making purposes. An organization undergoing change or with ambitious targets to grow will require strong interaction with IT to develop appropriate technical enterprise architecture to support and enable the changes and the growth.

When the organization delivers uniform services and products to customers, a more centralized governed organization and operating model would be expected. If the opposite is the case, there may be good reasons for it without compromising the effectiveness of IT governance.



In a decentralized operating model, the strategic business units (SBU) are allowed to operate more independently and autonomously, with their own IT budgets and using different applications and IT infrastructure. As a result, the organization will likely not be successful in effectively deploying a single set of IT standards across the enterprise with regard to applications, IT infrastructure, processes, and procedures. Scalability becomes less possible, but there may be valid reasons for the decentralized structure that actually provide IT investment ROI in the aggregate.

Information Security Management

Appropriate information security management depends on the organizational operating model. In a centralized command structure, information security policies and procedures are easier to implement across the whole organization, while a decentralized structure will require a different approach. No matter the operating model, information security risk appetite and risk tolerance levels also play a role, as well as technical differences between the various IT environments and their components.

For IT management to have an appropriate and effective information security management program, it should first identify and understand the areas of greatest inherent risk. Through the execution of a risk assessment and various methods and techniques of risk response, IT management should manage and mitigate these risks to a level of acceptable residual risk.

It is important to note that without the appropriate risk assessment, IT management could very likely have unknown vulnerabilities to vital IT assets including, but not limited to, infrastructure and information. Furthermore, it is crucial that IT management respond to the findings related to the risk assessment. If IT management fails to do so, risks will likely not be adequately managed and IT governance programs and processes will be compromised.

The table below lists some indications that IT governance is likely not in place or not operating effectively due to misalignment between the organization and IT with respect to information and technology components. An overly complex IT infrastructure, relatively high number of applications, and lack of standards are signs of such misalignment.

IT Organization and Risk Management	Consequences of Misalignment (Risks)
IT infrastructure and applications are too complex, not mature, or unverified	Possibility of losing corporate knowledge Lack of efficacy or efficiency in using new technologies
No standard for technology selection	Potential for design inefficiencies and lack of viable benchmarking options
Organizational processes are not integrated or automated	Misalignment of key controls
Systems are not standardized	Inefficiencies are not mitigated
Data are not shared	Duplication of effort
Data are not standardized	Not able to incorporate efficiencies into key IT processes

3. Aligning the Organization and IT — Key Considerations

Section 2 provided insight into risks that may result due to inadequate alignment between the organization and IT. This section discusses how to align the organization and IT.

Internal Audit and IT Governance Alignment Optimization

The process of moving from an ineffective IT governance position to a more effective or optimal model is one of continuous improvement, and there is no one-size-fits-all solution or paradigm for any organization. The process of optimization is not accomplished overnight. Achieving optimal alignment between the organization and IT can be difficult if the board and senior management do not understand the basic relationship of IT governance to the overall concept of corporate governance. The board and senior management also should understand some basic aspects of the IT controls within the organization. IT controls are those that support management and governance as well as provide general and technical controls over IT infrastructure such as applications, information, and people.

For the internal auditor to assist an organization with the alignment between the organization and IT and strengthen IT governance, he or she should begin the process by evaluating the organization's current state as compared to the IT governance components introduced in Section 1.

Strong IT-organizational alignment is a critical IT governance factor driving productivity gains, which includes the following general factors for effective IT governance:

- Effective IT financial management.
- Improvements that can be achieved through IT.
- Return on IT investments.
- Organizational value delivered by IT initiatives.
- Senior management compensation linked to the outcomes.

Effective IT governance occurs when senior management plays an essential role throughout the IT investment lifecycle and accountability for results is enforced. Top management enforces this accountability by being actively involved in relevant decision making, metrics, and implementation of such which are driven from the top down to stakeholders. Research also points out that the most successful decision makers focus on a set of five to seven critical metrics, with drill-down capabilities to lower-level metrics as needed.

The figure introduced in Section 1 illustrates the roles, frameworks, and standards that are most relevant at different levels of the IT governance framework. As stated throughout this GTAG, IT governance is more about governance and less about technology, but the board and senior management should understand IT and its impact on the organization well enough such that alignment between IT and the organization occurs and IT is governed appropriately.

The previous sections introduced some of the concepts necessary to understand the context, objectives, and organizational risks related to IT governance. In this section, the CAE, internal auditors, and functions responsible for internal controls within an organization are provided with examples of key controls and formal and informal mechanisms that an organization should have in place to mitigate risks related to IT governance.

Soft (informal) controls usually address intangible objectives such as competence, values, openness, leadership, and expectations. Hard controls, or formal controls, refer to the set of documented or tangible control tools used by an organization such as policies and procedures, organizational structures, reporting mechanisms, and established internal review processes.

Understanding the difference between soft and hard controls can help internal auditors realize the multidimensional set of mechanisms needed to address the complexity of IT governance. There are at least three different governance components to be effectively managed: people, processes, and technology. In this sense, an appropriate IT governance framework should include a top-down set of both hard and soft controls to ensure these three components are managed effectively. In addition, specific efficiency and effectiveness tests are necessary for each one of the key IT governance controls, which provide internal auditors the information to evaluate an organization's technology governing processes.

Maturity Model

In conjunction with a designated framework to migrate toward effective, more optimal IT governance, the CAE may use a maturity model[7] for comparison purposes to communicate to the board and senior management the current status of the IT governance environment.

Once an assessment of an organization's IT governance maturity level has been performed and documented, senior management, with support and direction from the board,

7 COBIT Process Assessment Model (PAM) Using COBIT 4.1, 2011, ISACA.

can begin to modify and/or implement practices, policies, and procedures that will assist the organization with IT governance optimization.

Due to the complexity of IT governance, the CAE and the internal audit team are in a position to provide value-add insights to the board and senior management about areas that may not be of significant priority to some decision makers. The CAE can provide an overview of how some of the organization's existing board and senior management tools can be improved relative to IT governance. As previously noted, IT governance should be based on sound and effective practices and recognized frameworks. The use of these IT governance practices should involve controls that assist the organization in meeting its strategic objectives. The following section provides some additional points on some of these controls. Of particular importance is the understanding and use of the IT Governance control point framework presented in Table 1: IT Governance Control Points. This framework may be used as a method to communicate and understand the roles and relationships that exist within an IT governance structure at strategic and tactical levels.

3.1 IT Governance Controls

Effective IT governance includes controls that ensure organizational strategies and objectives are met. To properly govern IT, and to some extent the knowledge capital of the organization, the IT governance process includes a set of hard and soft controls that should collectively govern people, processes, and technology.

Governance is about evaluating alternatives, providing direction, monitoring, and following up on execution.

The set of controls can be conceptualized as an integrated multiple-dimensional grid as reflected in Table 1 below.

Table 1: IT Governance Control Points

		PEOPLE	PROCESSES			TECHNOLOGY
		Human Capital	**Organizational Bodies**	**Organizational Roles**	**Organizational Tools**	**Technologies and Tools**
IT Governance	**Strategic Level**	• Corporate culture • Values • Beliefs • Behaviors	• Board	• Senior executives • CEO, chief financial officer, vice presidents, chief operating officer, chief information officer	• IT strategy • IT policies • Information architecture • Information security architecture	• Organizational plans • Corporate IT balanced scorecard • Service level oversight
IT Management	**Tactical Level**	• Skill set • Sourcing Strategies	• IT steering committee • Other collective IT tactical bodies	• Chief information officer • Chief applications officer • Program/ Project management officer • Managers	• IT standards and policies • Security baselines • Project management methods • Services level management	• Multiple departmental IT balanced scorecard • Project metrics • Application systems metrics • Service level agreements
	Day-to-Day Operations	• Training • Awareness • Compliance • Continuous improvement	• Other collective management bodies		• IT projects and initiatives • IT procedures and guidelines • Tasks and initiatives • Services level monitoring	• Operation dashboards • Network and infrastructure monitoring tools • Project monitoring • Application systems monitoring

Ethics and Values Set by the Tone at the Top

IT governance exists in the context of the organization's overall control environment. The King III Report on Corporate Governance (2009) provides a greater degree of understanding and awareness of the responsibilities of the use of IT, introducing, in particular, an emphasis on ethical governance of IT:

"5.1.3. The board should ensure promotion of an ethical IT governance culture and awareness of a common IT language."

Furthermore, in its introduction, King III states:
"In exercising their duty of care, [board] directors should ensure that prudent and reasonable steps have been taken in regard to IT governance."

IT Standards, Policies, and Procedures

From a tactical perspective, the internal auditor should consider how tools such as IT standards and policies and security baselines are used, which are usually managed and approved by non-IT managers and the CIO or equivalent that are accountable for their implementation. Meanwhile, organizational IT plans, IT strategies, IT policies, and architectures should be considered or approved by the CIO or equivalent, who should have final responsibility for these organizational tools.

Performance Management and Reporting

IT governance stakeholders should have a consistent and meaningful understanding of the organization's IT goals and initiatives to oversee, monitor, manage, and assure the expected outcomes. Techniques and tools such as the balanced scorecard could help to address that need.

Internal audit should be in a position to provide assurance and advice on governance structures and processes to board and senior management. As the CAE is in a unique position of understanding the relationships in the IT governance environment, he or she also should be aware of emerging issues that should be communicated to those responsible for IT governance. To deliver the appropriate consulting services, the CAE should use strategic development techniques that assist the organization with focusing on the big picture. Furthermore, the organization's senior management governance committee or similar group should ensure:

- Current and potential IT governance committee members have appropriate IT knowledge or IT background.
- Committee's performance of IT oversight is monitored.
- The committee stays abreast of external regulatory governance issues that may impact the organization.
- The IT governance committee reviews IT policies on a periodic basis.
- Regular IT governance committee meetings are conducted.

4. The Role of Internal Audit in IT Governance

The primary responsibility for IT governance lies with board and senior level management. The internal audit activity is responsible for assessing whether the organization's IT governance supports the organization's strategies and objectives as outlined under Standard 2110.

Performance Versus Compliance

Internal auditors conduct both performance audits and compliance audits. While compliance audits are generally focused on adherence to external regulatory requirements and related internal policies and procedures, performance audits require more analysis and evaluation as to what drives performance in the organization to develop an effective audit program. Assessing the effectiveness and efficiency of an organization is in a way more demanding, but is required to be able to determine whether IT governance of the organization sustains and supports the organization's strategies and objectives.

When performing an IT governance audit, the internal audit activity should ensure independence is maintained and objective assurance is provided to the board as to IT governance effectiveness. Even before the audit commences, internal auditors should ensure they possess the knowledge, skills, and other competencies to perform the audit.

In scoping and executing an IT governance audit, the internal audit engagement team should:

- Determine whether the IT function aligns with and understands the organization's objectives and strategies.
- Determine the effectiveness of IT resource and performance management.
- Assess risks that may adversely affect the IT environment.

Developing the IT Governance Audit Plan

Internal audit should follow established performance standards as outlined in the 2200 series of standards that cover engagement planning. Standard 2200: Engagement Planning states, "*Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations.*" In addition, as part of the IT governance engagement planning exercise, consideration should also be given to the 2200 series Practice Advisories as they offer further detailed guidance. These tools are designed to provide the practitioner with a conceptual framework for understanding and executing the IT governance audit plan. CAEs should use professional judgment in developing their own IT governance audit engagement plan and should be receptive to the uniqueness of their organization's control environment, strategies, and objectives.

The information that follows provides the internal auditor with guidance on areas of focus for each of the five IT governance components first presented in the Introduction.

Organization and Governance Structures

While the internal audit activity cannot establish organizational structures, approve methodologies, or write policies, it should review them for completeness, accuracy, and relevancy while supporting the IT governance activity to the extent allowed by the internal audit charter and the IPPF. This participation will likely include activities such as:

- Reviewing the organizational structure to identify whether there is a CIO in place, and whether this person is a member of the senior management team.
- Assessing the degree to which governance activities and standards are consistent with the internal audit activity's understanding of the organization's risk appetite.
- Consulting engagements as allowed by the internal audit charter and approved by the board.
- Ongoing dialogues with the IT governance activity to ensure that substantial organizational and risk changes are being addressed in a timely manner.
- Formal audits of the IT governance activity consistent with IIA Standard 2110.

Executive Leadership and Support

As noted throughout this GTAG, the effectiveness of leadership in creating and communicating the right tone at the top culture or mindset is paramount to an effective governance program. Furthermore, it is of vital importance that the board and senior management ensure the IT function is aligned with, and a part of, the strategic plan of the organization. From an audit perspective, as noted in the interpretation of 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."*

Reliability, integrity, efficiency, effectiveness, safeguarding, and compliance are typically associated with IT management and related controls and the requisite audit skills within the internal audit activity. However, to perform an effective audit of governance-related activities, one should be a very experienced internal auditor with an in-depth understanding of controls and governance concepts. With respect to an audit of IT governance, it will require the internal auditor to interpret and understand the organization's IT governance activities. The CAE should ensure the internal audit activity possesses the resources and competencies necessary to evaluate the IT governance program and associated risk, including both internal and external risk exposures and those relating to the organization's relationships with outside entities as required by Standard 2130. The CAE may rely on staff that has experience working with IT security and executive management but may not have experience with, or knowledge of, IT governance concepts. In addition, internal audit staff should have an understanding of the existing governance structure and possess adequate relationship management skills to form effective working relationships with security management leadership and within the governance structures. In small audit functions, the CAE may be actively involved in the delivery of an IT governance audit, or the IT governance audit may be co-sourced or outsourced to a third party provider.

Strategic and Operational Planning

Strategic and performance (tactical) IT management and related measurement are key components of an effective IT governance program. As noted in Standard 2110.A2:

"The internal audit activity must assess whether the [IT] governance of the organization supports the organization's strategies and objectives."

The internal audit activity should, in line with Standard 2110, conduct governance-related audits, including assessing whether IT governance sustains and supports the organization's strategies and objectives. The internal auditor may find that an IT governance program is not in place or in other cases may find ones in place that are adequately designed and controlled or under- or over-controlled. While each organization's IT governance program is different, each one should have sufficient performance components that tell management whether IT is being governed adequately such that strategic goals are being achieved.

Service Delivery and Measurement

Auditing the financial management components of an IT governance program may vary from one organization to another due to direction of the board and senior management, pressures and conditions within industry, and competition. In any event, financial management is an important part of controlling and monitoring costs and benefit realization from IT.

Internal audit, at a minimum, should have an understanding of how well IT financial management has been designed and deployed by senior management. Internal audit should begin by gaining an understanding of IT financial management policies by asking:

- Do the board and senior management have a true understanding of IT costs and how they contribute to the achievement of strategic goals and objectives of the organization, outcomes, and both top and bottom line?
- Do organizational unit leaders measure IT deliverables and value received? How?
- How do IT costs compare to other organizations of similar size and within the same industry?
- Are financial analyses performed as a part of cost benefit studies for larger IT investments?
- Are organizational unit leaders and the CIO measured on both financial and nonfinancial performance?

As stated in the section on risks of misalignment, one important aspect of financial management is the ability to extract the right information, as well as measure the right things.

For effective analysis of the financial data, details should be available. Building a performance framework for both financial and nonfinancial measures is one of the keys for effective IT governance.

IT Organization and Risk Management

When focusing on the information and technology components of IT governance, the audit activities performed would likely first focus on a more general review of the IT governance structures and processes. This assurance engagement provides the internal audit activity with an understanding of the IT governance program, related policies, and procedures. In addition, the engagement could also involve a comparison of the program against independent standards. The internal auditor also may want to verify whether management is performing its own benchmarking and, if so, review these benchmarking activities. This level of review provides some assurance on the nature of the IT governance program, but may not reveal conformity with IT governance frameworks. A benchmarking engagement also could provide an effective starting point in a multiyear audit plan because it allows management time to address design gaps in the governance structure before additional reviews are performed. This

approach can help the CAE to ensure that internal audit resources are being efficiently managed because conformance testing will likely not occur until the audit activity has reasonable assurance that the program meets basic expectations.

Once internal audit is sufficiently satisfied with the design of IT governance, audit testing should focus on the degree to which the program is operating consistent with Standard 2110. This type of an audit could include reviews of:

- Management reporting.
- Exceptions approvals and documentation.
- Risk assessments consistency.
- Effective use of metrics.
- Timely updates based on emerging organizational needs and external changes.
- Board and committee meetings minutes.
- Strategies and plans.
- Organizational changes and interviews with management members.

Finally, the internal audit activity should examine the degree to which other auditable entities provide ongoing support to the IT governance program. This likely will involve specific test steps used in other audits such as assessing whether possible security events are documented, escalated, responded to, and managed by support teams and reviews of IT risk in each of the strategic processes. While this could be construed as auditing IT 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 program is imperative to understanding true IT governance 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 organizational objectives as a result.

Upon completion of an IT governance audit, the CAE should communicate the results to the board and senior management and follow established performance standards as outlined in Standard 2400: Communicating Results.

"Communications must include the engagement objectives and scope as well as applicable conclusions, recommendations, and action plans."

In auditing IT governance, the internal audit activity may encounter IT governance issues that require varying degrees of communication given the level of risk within the organization. Given the uniqueness of different organizations and the industries and countries in which they operate, the internal audit activity should follow the guidance in Standard 2400 as a framework for reference when determining the communication method.

It is recommended that the internal audit activity review the guidance in the following standards for further discussion and clarification on the subject of communicating to the board/management:

- Standard 2410: Criteria for Communicating.
- Standard 2420: Quality of Communications.

Conclusion

This GTAG is intended to act as a tool and provide a high-level method internal auditors can use when conducting an audit of IT governance. This guide is based on global practices and research on the mechanisms and characteristics necessary to enable optimal return on IT investments while supporting the strategies and objectives of the organization. As each organization has different structures and practices, internal auditors should tailor the audit program as appropriate within this GTAG for each audit client.

The five components of effective IT governance are a result of global practices and research. They cover governance structures, roles and responsibilities, and activities dealing with strategic and operational planning, implementation, and monitoring of delivering on the plans, including ensuring aligning organizational needs and IT enterprise architecture to support and meet those needs. Both performance and risk management form an integral part of these activities, where the board and executive management evaluate alternatives, give directions, and monitor and follow up on directions given.

Authors and Reviewers

Authors:

Stig J. Sunde, CIA, CISA, CGAP, CRISC
Cesar L. Martinez, CIA, CGAP
Fernando Nikitin, CIA, CCSA, CRMA, CISA, CGEIT, CISM, CRISC, CISSP
Steve Hunt, CIA, CRMA, CISA, CGEIT, CRISC, CBM

Reviewers:

Steven E. Jameson, CIA, CCSA, CFSA, CRMA, CPA, CFE, CBA, CGMA

Appendix — IT Governance Risk Assessment/ Engagement Planning Considerations

From a risk assessment perspective, the following questions can be used to help determine if an audit of IT governance should be built into the audit plan. From an engagement planning perspective, these questions also can be used as a guide to help scope the IT governance audit.

ORGANIZATION & GOVERNANCE STRUCTURES	ASSESSMENT—Y/N, COMMENTS
Is there a lack of empowerment or accountability for organizational results?	
Are IT and operational organizational structures clearly defined?	
Are communication channels between IT leaders and organization leaders clearly defined?	
EXECUTIVE LEADERSHIP & SUPPORT	
Is there a clear entity wide vision?	
Are executives actively involved in the decision making processes related to IT?	
Does core organization have a clear focus (a clear strategy which is communicated)?	
Does CEO (and Strategic Business Unit heads) have a clear understanding of IT?	
STRATEGIC & OPERATIONAL PLANNING	
Does the organizational strategy address IT? Is there an IT strategy?	
Are organizational improvements through IT resources evaluated?	
Are the sourcing strategies clear and supported by SLAs?	
Is empowerment or accountability for organizational results clear?	
Is the IT financial management effective and supporting decision makers?	
SERVICE DELIVERY & MEASUREMENT	
Are costs higher than comparable entities?	
Are there drill-down capabilities to lower-level metrics as needed?	
Are the IT costs known or detailed enough?	
Is it possible to track the organizational value delivered by IT initiatives?	
Are there meaningful metrics or too many metrics?	
Is the accountability clearly defined?	
Is IT senior-level compensation linked to organizational outcomes (not output alone)?	
Are there measures of technical/operational and financial performance in IT?	
IT ORGANIZATION & RISK MANAGEMENT	
Are IT infrastructure and applications too complex?	
Is there a standard for technology choices?	
Are organizational processes integrated or automated?	
Are systems standardized?	
Is data shared?	
Is data standardized?	
Is core organizational focus lacking (thus difficult for IT to focus)?	

GTAG®

About the Institute

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

About Practice Guides

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

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

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

Disclaimer

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

Copyright

Copyright © 2012 The Institute of Internal Auditors.
For permission to reproduce, please contact The IIA at guidance@theiia.org.

The Institute of Internal Auditors

www.globaliia.org