IPPF

International Professional Practices Framework

Supplemental Guidance

GTAG®

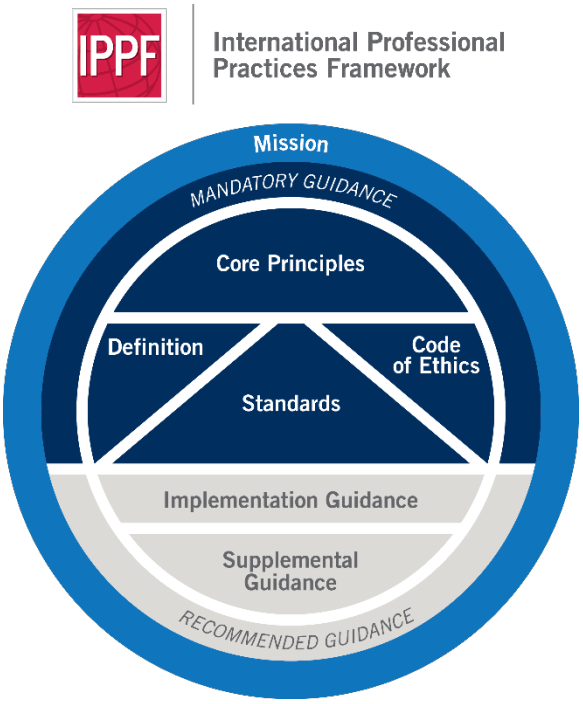
Global Technology Audit Guide

# Auditing IT Governance

The Institute of Internal Auditors | Global

# About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA. A trustworthy, global, guidance-setting body, The IIA provides internal audit professionals worldwide with authoritative guidance organized in the IPPF as Mandatory Guidance and Recommended Guidance.




Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- *International Standards for the Professional Practice of Internal Auditing*.

## About Supplemental Guidance

Supplemental Guidance is part of the IPPF and provides additional recommended, nonmandatory guidance for conducting internal audit activities. While supporting the *Standards*, Supplemental Guidance is intended to address topical areas, as well as sector-specific issues, in greater procedural detail than the *Standards* or Implementation Guides. Supplemental Guidance is endorsed by The IIA through formal review and approval processes.

### Practice Guides

Practice Guides are a type of Supplemental Guidance that provide detailed step-by-step approaches, featuring processes, procedures, tools, and programs, as well as examples of deliverables.

Practice Guides are intended to support internal auditors. Practice Guides are also available to support:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.globaliia.org/standards-guidance.

# Table of Contents


Executive Summary ..... 4

Introduction ..... 5

IT Governance Overview ..... 6

- Business Significance ..... 8
- Key Risks ..... 10
- IT Governance Components ..... 10
- The Role of Internal Audit in IT Governance ..... 12
  - Proficiency ..... 13

Engagement Planning ..... 14

- 1. Understand the context and purpose of the engagement. ..... 15
- 2. Gather information ..... 16
  - 2.1 Obtain and Document Information ..... 17
  - 2.2 Interviewing Relevant Stakeholders ..... 18
- 3. Conduct a preliminary risk assessment. ..... 18
- 4. Form engagement objectives. ..... 19
  - 4.1 Consulting Engagement Objectives ..... 21
- 5. Establish engagement scope. ..... 21
- 6. Allocate resources. ..... 22
- 7. Document the plan. ..... 23

Reporting the Engagement Results ..... 23

Appendix A. Relevant IIA Standards and Guidance ..... 24

Appendix B. Glossary ..... 25

Appendix C. IT Governance Internal Controls Questionnaire ..... 27

Appendix D. Risk and Controls Matrix for IT Governance ..... 30

Appendix E. Additional Resources ..... 38

Acknowledgements ..... 39

# Executive Summary

Taking a strategic approach to implementing information technology (IT) governance helps organizations address the speed of technological advancements, IT services proliferation, and the greater dependency on IT to meet organizational objectives. Effective IT governance contributes to control efficiency and effectiveness, and allows the organization's investment in IT to realize both financial and nonfinancial benefits. Often when controls are poorly designed or deficient, a root cause is weak or ineffective IT governance.

> Alignment of organizational objectives and IT is more about governance and less about technology. Governance assures alternatives are evaluated, execution is appropriately directed, and risk and performance are monitored.

IT governance is directly related to organizational oversight of IT assets and risks, making it a shared responsibility of senior management[1] and the board. Senior management carries out the day-to-day direction that tactically aligns with the overall strategic guidance of the board to ensure the effective, efficient, and acceptable use of IT resources. The primary outcomes of effective IT governance include:

- IT strategies are aligned with organizational objectives.
- Risks are identified and managed properly.
- IT investments are optimized to deliver value to the organization.
- IT performance is defined, measured, and reported using meaningful metrics.
- IT resources are managed effectively.

Absent or poor IT governance can have significant negative impacts on an organization, both financially and reputationally. Recovery from such impacts requires time, energy, and money. In many organizations, there is a disconnect between senior management and IT due to the old belief that IT exists solely to deliver day-to-day IT services. In reality IT is critical in the development of competitive advantage and to support the achievement of the organization's goals and strategic objectives.

The internal audit activity is uniquely positioned and staffed within an organization to assess whether the information technology governance of the organization supports the organization's strategies and objectives and to make recommendations as needed (Implementation Standard 2110.A2).

As the second edition of "Auditing IT Governance," this GTAG has been updated to reflect the 2017 International Professional Practices Framework and to be more directly practical to internal auditors.

---

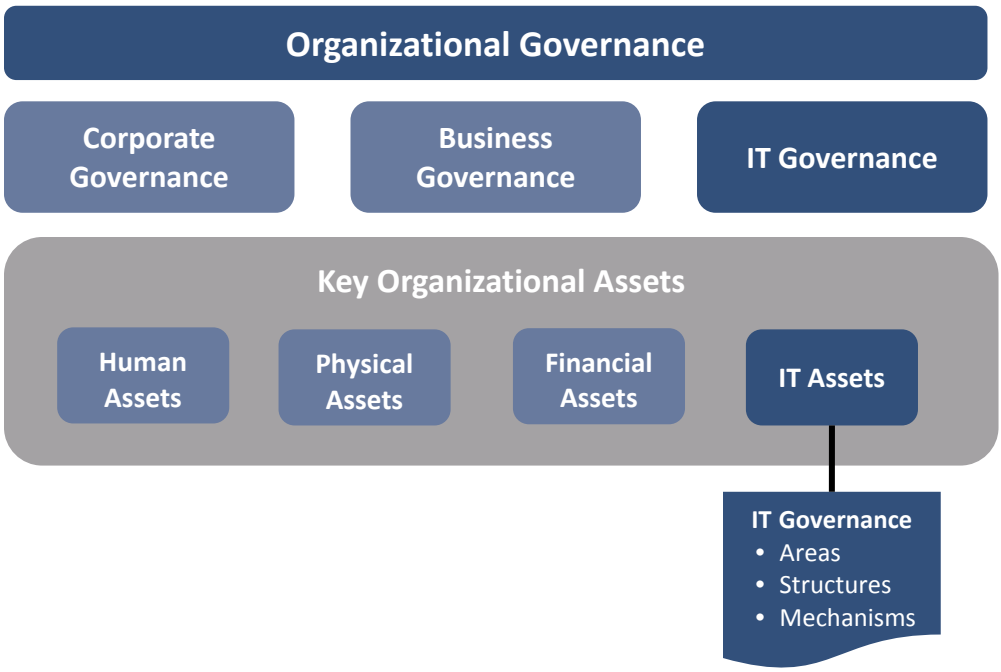
[1] Senior management usually includes the chief executive officer (CEO), chief financial officer (CFO), chief operations officer (COO), chief marketing officer (CMO).

# Introduction

The highest level of governance is organizational governance, which is defined by the *International Standards for the Professional Practice of Internal Auditing* as "the combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives."

IT governance is a subdiscipline of organizational governance consisting of the leadership, organizational structures, policies, and processes that ensure that the organization's information technology supports its strategies and objectives. IT governance supports the organization's regulatory, legal, environmental, and operational requirements to enable the achievement of strategic plans and aspirations. Other subdisciplines include corporate governance responsible for conformance processes and business governance responsible for performance processes. Figure 1 shows the relationship between organizational governance and IT governance.

**Figure 1: Organizational Governance and IT Governance Relationship**




Source: Adapted from Institut de la Gouvernance des Systèmes d'Information, *Place of IT Governance in the Enterprise Governance*, (Paris: CIGREF, 2005.), 6-7, http://cigref.typepad.fr/itgifrance/2006/04/place_of_it_gov.html.

The objective of this guidance is to assist internal auditors in providing assurance services over IT governance. The guide provides a high-level description of IT governance processes, practices, and terminology to help internal auditors attain an understanding of the concept of governance and the characteristics of good governance processes.

This edition provides tools and techniques to help internal auditors build a work program and perform engagements involving IT governance.

# IT Governance Overview

Implementing IT governance is an imperative part of organizational strategies because it is fundamentally concerned with goals that ensure that IT delivers value to the business in a controlled and effective manner. A typical IT governance framework would focus on five key areas:

- Strategic alignment – IT governance provides strategic direction of IT and the alignment of IT and the business with respect to services and projects, business objectives, up-to-date IT strategy, linkage between business objectives, and IT initiatives.
- Risk management – IT governance can help determine what processes are in place to ensure that risks have been adequately addressed. Additionally, it can ensure that enterprise risk management includes risk aspects of IT investments, defined responsibilities for risk management, defines a common risk analysis methodology, and define strategies for addressing risks, continuous monitoring of threats, occurrence, and impact in a holistic manner.
- Value delivery – IT governance helps IT and the business to create a partnership designed to drive maximum business value from IT. The business is enabled to oversee the delivery of value by IT, and measure return on investments (ROI), IT tactical plan execution, and clear benefits for each level of the organization. For example, system uptime (infrastructure strategy), degree of automation in the software development (SDLC) strategy, productivity (operational strategy), and ultimately revenue (IT financial strategy).
- Performance measurement – IT governance provides the mechanisms to verify strategic compliance (i.e., achievement of strategic IT objectives), measure IT performance, and its contribution to the bottom line (i.e., delivery of promised business functionality). Further metrics include continuous monitoring and reporting, follow-up policies, root cause analysis and problem management, benchmarking against industry practices, and proven standards or frameworks.
- Resource management – IT governance provides high-level direction for sourcing and use of IT resources to: oversee the aggregate funding of IT at the enterprise level; and ensure there is an adequate IT capability and infrastructure to support current and expected future business requirements, sourcing strategies, human management practices, user manuals, segregation of duties, time reporting, infrastructure life cycle management, service level agreements, and acceptable usage policies.

Some of the challenges that IT governance can help organizations address include:

- The increasing complexity of IT environments.
- A growing dependency on data to make business decisions.
- The proliferation of mobile devices.
- The need to exchange information with customers, service providers, and business partners.
- The increasing risk of cyberattacks.
- An increase in laws and regulations related to data protection.

In the IT governance conceptual framework, senior management and the board are responsible for establishing the organization's IT objectives in alignment with the overall business strategy; defining IT strategies to achieve business objectives; and establishing IT governance policies, organizational structures, and processes to manage the risks to accomplishing those objectives.

IT management is responsible for the day-to-day activities of an organization: planning, executing, and monitoring the use of IT resources to ensure the achievement of the strategies and policies established by the board.

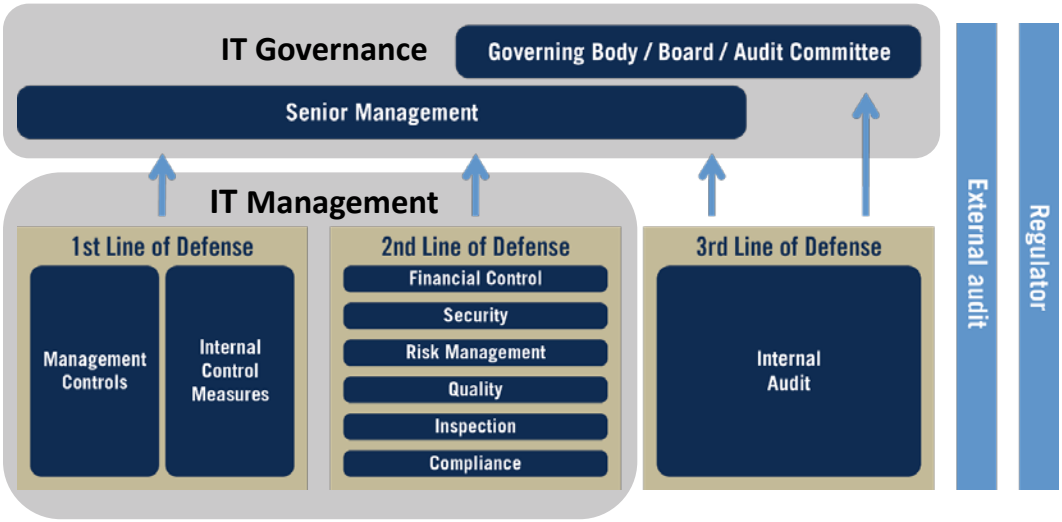
The role of internal audit in IT governance has become increasingly important in the wake of global financial crises and high-profile information security breaches. According to survey results published in The IIA's CBOK® report, Promoting and Supporting Effective Organizational Governance, internal audit is well positioned to promote and support organizational governance and thus help achieve a balance between value creation and value preservation.

Internal audit's role includes the responsibility to assess and make recommendations to improve the organization's governance processes (Standard 2110 – Governance) to help prevent governance failures and improve strategic performance as part of the third line of defense.

In the Three Lines of Defense model, operational management (including IT) represents the first line of defense and is responsible for the implementation and maintenance of processes and controls to manage risks. Compliance functions and risk management represent the second line of defense and are responsible for monitoring risks across the organization. Internal audit represents the third line of defense and is responsible for providing independent assurance that risk management and controls are operating effectively, and advise senior management and the board when deficiencies are identified.

Figure 2 shows the responsibilities for the Three Lines of Defense model as it relates to IT governance.

**Figure 2: Three Lines of Defense in Reference to IT Governance**




Source: Adapted from "IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control" (Altamonte Springs, Fla. USA: The Institute of Internal Auditors, 2013).

There are many internationally recognized IT governance frameworks that can be used to supplement this guidance. Frameworks such as ITIL®, COBIT®, ISO/IEC 38500, King III, and King IV reports cover in more detail the processes and mechanisms needed to develop, implement, evaluate, and improve an IT governance program. This guide is focused on the processes and mechanisms that internal audit can use to assess whether the IT governance program supports the organization's strategies and objectives in conformance with Implementation Standard 2110.A2.

## Business Significance

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 a damaged reputation that can take time, energy, and money to rebuild. Simply put, IT governance can influence and impact the entire organization, not only IT.

Greater dependency on systems and information means that organizations have to invest greater resources to improve and maintain their IT environments. These are expected to help manage risk, improve operations, and create value by delivering services that help achieve financial and nonfinancial organizational objectives.

The main focus of IT governance is on creating alignment between organizational priorities and IT objectives to ensure that IT efforts concentrate on processes or projects that support strategic goals. Successful alignment between the organization and IT occurs when senior management and the board understand the value of IT as a strategic partner, and recognize IT's role in supporting the bottom line.

Proper alignment between the organization and IT means:

- Senior management and the board understand the potential and limitations of IT.
- IT senior management understands the objectives and corresponding needs of the organization.
- This understanding is applied and monitored throughout the organization via an appropriate governance and accountability structure.

A robust IT governance framework provides several benefits, including:

- Competitive advantage.
- Improved speed to market.
- Effective information security and compliance.
- Process automation and innovation.
- More informed decision making.
- Better understanding of root causes related to problems leading to continuous process improvement.

Activities that are in the IT governance scope include:[2]

- Align IT investments and priorities with business objectives.
- Manage, evaluate, prioritize, fund, measure, and monitor requests for IT services, and the resulting work and deliverables, in a more consistent and repeatable manner that optimizes returns to the business.
- Maintain responsible utilization of resources and assets.
- Establish and clarify accountability and decision rights – clearly defined roles and authority.
- Ensure that IT delivers on its plans, budgets, and commitments.
- Manage major risks, threats, change, and contingencies proactively.
- Improve IT organizational performance, compliance, maturity, staff development, and outsourcing initiatives.
- Champion innovation within IT and the entire organization.

[2] Gad J. Selig, *Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management*, (Zaltbommel, NL: Van Haren Publishing, 2008), 9-10.

## Key Risks

Just as the benefits of IT governance can help an organization achieve financial and nonfinancial objectives, improve operations, and control risk, the negative impacts can be detrimental to the entire organization.

Emphasis on technical or financial aspects of IT instead of emphasis on the organizational context of using IT as a business enabler usually results in negative outcomes, poor return on IT investments, or failure to demonstrate the benefits created through IT investments.

Other examples of negative impacts include:

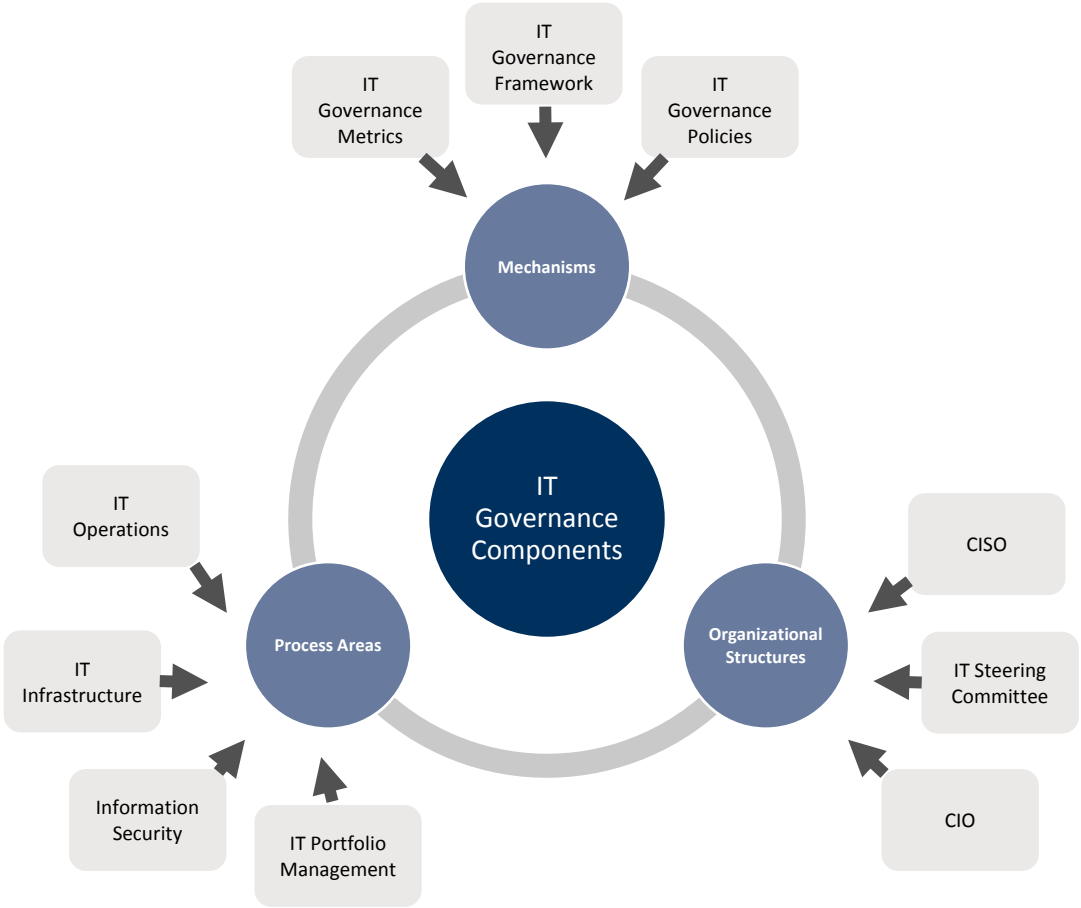
- Financial losses due to business disruption.
- Higher costs to run business operations.
- Poor quality or failure to meet new customer expectations and unsatisfied customers.
- Core business processes are negatively impacted by poor delivery of IT services.
- Unidentified risks and threats expose the entire organization to security breaches.
- Penalties resulting from failing to meet regulatory requirements.

## IT Governance Components

Implementation and maintenance of an IT governance program depends on components that can help senior management and the board direct, monitor, and measure IT performance. As shown in **Figure 3**, the key components of effective IT governance have been grouped into three categories:

- *Process Areas* – Include all IT processes implemented to provide services to the organization (for example, change management, information security management, software development, and project management).
- *Organizational Structures* – Include the 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 (**Figure 4**).
- *Mechanisms* – Include standards, policies, and frameworks implemented to direct, monitor, and measure IT performance. The IT governance framework should determine which processes must be in place to ensure that risks have been satisfactorily identified, assessed, and either addressed or accepted in accordance with the organization's risk appetite and tolerance.

## Figure 3: IT Governance Components




## Figure 4: Examples of Organizational Structures

| Governance Body | Members | Scope |
|---|---|---|
| IT governance board | CEO, CFO, CIO, CAE* | Business and IT strategy and investment plans. |
| IT steering committee | IT senior management, business unit owners | IT strategic alignment. |
| IT portfolio office | IT program managers, business program/project managers, IT project managers | IT project metrics, monitoring, and reporting. |
| IT architecture office | CIO, CISO, COO, IT infrastructure managers | IT architecture design. |
| Technology council | CIO, CTO, business unit owners | Evaluate technology opportunities. |
| Cybersecurity and data protection council | CIO, CTO, CISO, CRO, CFO, COO, CAE* business unit owners | Evaluate organizational risk and strategies to protect the organization's information assets. |

* Note: The CAE participates in the governance board as a nonvoting advisor on risk and controls.

## The Role of Internal Audit in IT Governance

IT governance is a management responsibility, internal audit should remain independent, but this can provide an excellent position to influence and recommend change.

It is imperative that audits of IT governance be divided into both assurance and consulting activities depending on the robustness of the IT governance system in place. Independence should not inhibit provision of advice, so long as management takes full responsibility and accountability for implementation and operation of controls.

Any type of audit can assess if business owners are following policies and demonstrate adequate protection of assets by working with IT to identify risk and controls.

Governance processes are considered during the internal audit activity's risk assessment and audit plan development. The CAE typically identifies the organization's higher-risk governance processes, which are addressed through assurance and consulting projects described in the final audit plan. In addition, Implementation Guide 2110 specifically identifies the internal audit activity's responsibility for assessing and making appropriate recommendations to improve the organization's governance processes for:

Factors that can help strengthen IT governance:

- Clear IT ownership and accountability.
- CIO reporting line to senior management.
- The innovation value that IT can offer is recognized.
- IT performance is monitored and measured.

- Making strategic and operational decisions.
- Overseeing risk management and control.
- 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, other assurance providers, and management.

Internal audits of IT governance should focus on the organization's implementation of governance practices, which include clearly defined policies, roles, and responsibilities, risk appetite alignment, effective communication, tone at the top, management of IT value, and clear accountability. Internal audit assessments will likely include activities such as:

- Assessing the degree to which governance activities and standards are consistent with the internal audit activity's understanding of the organization's risk appetite.
- Conducting consulting engagements as allowed by the audit charter and approved by the board.

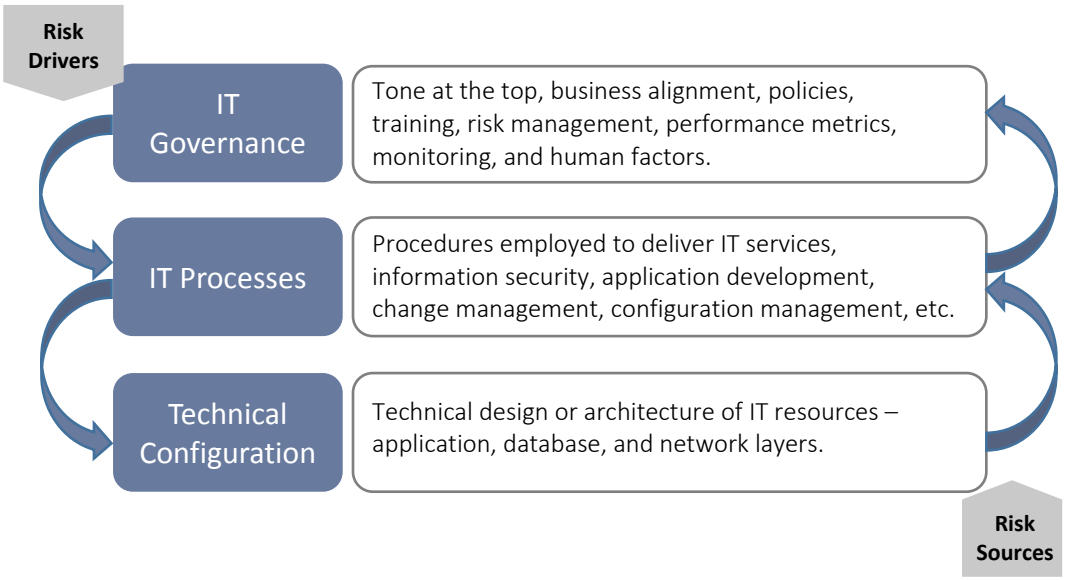
- Ongoing dialogue with the IT governance body to ensure that substantial organizational and risk changes are being addressed in a timely manner.

When reviewing governance, internal audit must do more than just identify problems. They need to identify root causes and make constructive recommendations when weaknesses in IT controls are identified; for example, poor or weak firewall configuration. In this particular case, a root cause evaluation can include different layers of control to identify the source of the problem.

Figure 5 shows a root cause analysis framework showing three layers of control that can be used for the evaluation of IT weaknesses. Starting at the technical layer, go up to the process layer and ask if there were any process breakdowns that caused the weak firewall configuration (e.g., lack of oversight or monitoring, or inadequate separation of duties).

From the process layer, go up one more layer to IT governance and ask if the organization has effective IT governance practices such as risk assessment and policy development, maintenance, and training regarding firewalls.

**Figure 5: IT Risk – Root Cause Analysis Framework**




The internal audit activity adds value when it identifies root causes and ensures the creation of constructive action plans in cooperation with management to address the issue.

## *Proficiency*

As noted in Implementation Standard 2130.A1, assessing IT governance may involve assurance and/or consulting services to evaluate the adequacy and effectiveness of controls in responding to risks

While it might seem that auditing IT governance requires extensive IT experience, the strategic aspects of IT governance can be part of any operational engagement.

Engagement planning generally includes the following steps:

- Understand the context and purpose of the engagement.
- Gather information to understand the area or process under review.
- Conduct a preliminary risk assessment of the area or process under review.
- Form engagement objectives.
- Establish engagement scope.
- Allocate resources.
- Document the plan.

For detailed instructions on how to plan and scope an audit engagement see The IIA Practice Guide "Engagement Planning: Establishing Objectives and Scope."

within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

## Engagement Planning

According to Standard 2200 – Engagement Planning, internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement. This section is intended to help the internal auditor determine the key areas that should be included in an IT governance engagement, the type of documents that can be requested, questions that can be included in interviews, and evidence documentation that should be obtained. The examples provided are not exhaustive.

One of the most important things an internal audit activity must determine in planning the engagement is whether the organization has a unified and cohesive governance structure in place, including policies, processes, and tools to consistently manage the environment and control the risks related to IT.

It may be difficult to audit the entire IT governance program; instead the scope of the audit engagement can be defined using criteria that meets a specific objective. For example, the scope can be defined by organizational units, locations, strategic objective, or by any other criteria that is meaningful to the organization.

## 1. Understand the context and purpose of the engagement.

The chief audit executive (CAE) and internal auditors should start by attaining a clear understanding of the concept of governance and the characteristics of typical governance processes. They should also consider the formal definition of governance, as it appears in the glossary of the *International Standards for the Professional Practice of Internal Auditing*, and become familiar with globally accepted governance frameworks and models (e.g., The Committee of Sponsoring Organizations of the Treadway Commission's frameworks [COSO] or the International Standards Organization [ISO] 31000, and 38500).

Governance frameworks, models, and requirements vary according to organization type and regulatory jurisdictions. How an organization designs and practices the principles of effective governance also depends on factors such as its size, complexity, life cycle, maturity, stakeholder structure, and the legal requirements to which the organization is subject. Internal audit's approach to assessing governance and making recommendations to management will vary based on the framework or model the organization uses.

Internal audit must first ask what framework the organization is using to drive IT governance. If the organization has not implemented a framework, internal audit can offer to perform a consulting engagement to help management map existing controls and practices to an agreed to framework.

Next, the CAE contemplates whether the current internal audit plan encompasses the organization's governance processes and addresses their associated risks. Governance does not exist as a set of independent processes and structures. Rather, governance, risk management, and control are interrelated. For example, effective governance activities consider risk when setting strategy. Equally, risk management relies on effective governance (e.g., tone at the top; risk appetite, tolerance, and

### Good IT Governance at a Glance

- Existing organization and governance structures provide a good indication of whether IT supports and helps enable the organization in achieving its strategic objectives.
- 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 IT.
- Service delivery metrics, including financial management, are important components of controlling and monitoring IT cost/benefit measurement.
- 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.

culture; and the oversight of risk management). Likewise, effective governance relies on internal controls and communication to the board about the effectiveness of those controls.

According to Implementation Guide 2110 – Governance, "the CAE may review board and committee charters, as well as meeting agendas and minutes, to gain insight into the role the board plays in the organization's governance, especially regarding strategic and operational decision making. The CAE may also speak with others in key governance roles (e.g., chairman of the board, top elected or appointed official in a governmental entity, chief ethics officer, human resources officer, independent external auditor, chief compliance officer, chief risk officer) to gain a clearer understanding of the organization-specific processes and assurance activities already in place. If the organization is regulated, the CAE may want to review any governance concerns identified by regulators.

An understanding of governance is the foundation for a discussion with the board and senior management about what constitutes governance, so that an appropriate internal audit plan and approach can be executed."

## 2. Gather information

It is important that internal auditors document the information gathered while developing the plan, in accordance with Standard 2200 – Engagement Planning. It is helpful to note that this process is not always a sequential number of steps. Rather, it is an ongoing process that must be updated throughout the engagement planning as new information is obtained through the review of prior assessments (e.g., risk assessments, and reports by assurance and consulting service providers), understanding and mapping process flows and controls, or interviewing relevant stakeholders.

Implementation Guide 2110 indicates that, usually, a single audit of governance is not attempted. Rather, the internal audit activity's assessment of governance processes is likely to be based on information obtained from numerous audit assignments over time.

If an overall governance assessment is appropriate, it would take into account:

- The results of internal audits of the specific governance processes identified above.
- Governance issues arising from audits that are not specifically focused on governance, such as:
    - Strategic planning.
    - Operational efficiency and effectiveness.
    - Internal control over financial reporting.
    - Risks associated with IT, fraud, and other areas.
    - Compliance with applicable laws and regulations.
- The results of risk assessments.

- The results of management assessments (e.g., compliance inspections, quality audits, and control self-assessments).
- The work of external assurance providers (e.g., legal investigators, government auditor general offices, and public accounting firms) and regulators.
- The work of internal assurance providers, or second line of defense functions (e.g., health and safety, compliance, and quality).
- Other information on governance issues, such as adverse incidents indicating an opportunity to improve governance processes.

### *2.1 Obtain and Document Information*

Obtaining a thorough understanding of the organization and IT governance enables internal auditors to conduct a preliminary assessment of the relevant risks, as required by Standard 2210.A1. Sources of information include documentation and interviews with stakeholders.

At a minimum, at the end of this step the engagement plan should contain:

- Objectives of the area under review.
- Strategies used to achieve those objectives.
- Risks to achieving those objectives.
- Processes and key controls.
- IT and other systems relevant to the area or process under review.
- Sources and reliability of data into and out of the area or process under review.

Examples of documentation the internal auditor can request to plan the IT governance internal audit engagement include:

- Past audit reports.
- Strategic plans (organization's mission and vision).
- Organizational governance framework.
- IT governance framework.
- Information security policy.
- IT architecture policies.
- Organizational charts.
- The organization's strategy and goals.
- Enterprise risk management (ERM) reports.
- IT performance reports.
- Governance meeting minutes.
- Board and committee meeting minutes.

- Management reports.
- Exceptions approvals and documentation.

### *2.2 Interviewing Relevant Stakeholders*

Interviewing relevant stakeholders is a critical step that helps internal auditors better understand the objectives, design, operations, and control environment of the area or process under review. Often, organizational charts can assist internal auditors in identifying relevant stakeholders.

Interviews with departmental heads may reveal what processes led to strategic and operational decisions, gauge whether the organization's efforts result in sufficient awareness of its ethical stand, and whether employees have a clear understanding of their responsibilities over risk and control processes and the impact to the organization.

Appendix C provides an internal controls questionnaire that can help internal auditors develop a high-level understanding of the existing IT governance environment, and determine how to best scope, plan, and execute an audit engagement.

Example of Interview Questions:

- Does the board understand the organization's dependency on IT? How is that understanding reflected in the strategic plan?
- Do you have a clear definition of your role in IT governance? How do you know that you are meeting expectations?
- What decision-making bodies do you consult when making IT-related decisions?
- What policies exists and how are they disseminated by the different governance committees and subcommittees?
- How does the organization measure value?

In addition, internal auditors may brainstorm with individual personnel or in selected groups to identify relevant risks. For this purpose, auditors may ask, "What would keep the business objectives from being met?" Additionally, to identify inherent risks, internal auditors may ask, "What could go wrong if no controls were in place?"

## 3. Conduct a preliminary risk assessment.

Due to time and resource constraints, not all risks can be reviewed during an engagement. Therefore, internal auditors must conduct a preliminary risk assessment and prioritize risks according to significance, which is measured as a combination of risk factors.

One effective way to perform and document a preliminary engagement-level risk assessment is to create a chart showing the relevant risks and controls, such as a risk and control matrix. A risk and control matrix is a tool commonly used by internal auditors to identify, organize, and assess the risks that may impact the business objectives of the area under review, as well as any mitigating controls.

**Figure 6** shows an example of a risk and control matrix created using risks identified through risk scenarios. In this matrix, the impact and likelihood ratings are not included but would be added as risks are assessed.

See The IIA's Practice Guide "Engagement Planning: Establishing Objectives and Scope" for detailed instructions on developing:

- Risk scenarios.
- Risk and control matrix.
- Risk prioritization maps (i.e., heat maps).

**Figure 6: Risk and Control Matrix for IT Governance**

| Risk Scenario | Risk | Control |
|---|---|---|
| In a decentralized operating model, the strategic business units (SBUs) are allowed to operate more independently and autonomously, with their own IT budgets and using different applications and IT infrastructure. | The organization will likely not be successful in effectively deploying a single set of IT standards across the organization with regard to applications, IT infrastructure, processes, and procedures. | The IT enterprise architecture should mirror the organizational structure to enable better alignment and meet the organization's needs.<br>The development of the IT governance structure should be based on current and anticipated IT architecture designs. |
| The organization does not include risk management as part of project management practices. | Projects can fail due to poor planning to address risks. | There is a process in place to assess, address, and communicate IT risks to key stakeholders and executive management during the project, change, and release management processes. |

Appendix D provides a risk and control matrix for IT governance. This matrix is provided as an example and should be customized to meet the specific needs of the organization under review.

## 4. Form engagement objectives.

Once internal auditors have completed the preliminary risk assessment and identified the significant risks to evaluate during the engagement, they can form the engagement objectives. The engagement objectives articulate what the engagement is specifically attempting to accomplish; therefore, the objectives should have a clear purpose, be concise, and be linked to the risk assessment (Standard 2210.A1).

The engagement objectives for IT governance can be related to compliance with external and internal IT governance requirements, or operational performance of the IT governance processes,

and can be defined in different ways. For example, the objectives can be defined as part of the annual audit plan, or as a result of ERM results, past audit findings, regulatory requirements, or by specific assurance needs from the board or audit committee.

Internal auditors must also identify adequate criteria to evaluate the governance, risk management, and controls of the area or process under review and determine whether the business objectives and goals have been accomplished. Identifying such criteria ensures that assurance engagement objectives are measurable, practical, and aligned with the objectives of both the organization and the area or process under review.

According to Standard 2210.A3, internal auditors must use the criteria already established by management and/or the board, if such criteria exist. If no criteria are in place, internal auditors must identify appropriate criteria through discussion with management and the board. Internal auditors should also consider seeking input from subject matter experts to help develop relevant criteria.

Examples of criteria include:

- Existing key performance indicators.
- Targets set during strategic planning.
- The degree of compliance with area or process policies and procedures, external laws, and regulations, and/or contracts.
- Industry standards or benchmarks.

To avoid misinterpretation or challenge by any personnel responsible for the area or process under review, the evaluation criteria should be relevant, reliable, and documented. Adequate, appropriate criteria will provide a reference for internal auditors to evaluate evidence, understand findings, and assess the adequacy of the controls in the area or process under review. The criteria, or lack thereof, should be compared to industry benchmarks, trends, and forecasts, as well as the organization's policies and procedures.

The following are examples of how assurance engagement objectives could be formulated for the IT governance engagement.

The internal audit activity will provide assurance that:

- IT governance activities and standards are consistent with the internal audit activity's understanding of the organization's risk appetite.
- The IT governance body is addressing substantial organizational and risk changes in a timely manner.
- The linkage of IT metrics and objectives aligns with the organization's goals.
- Metrics are being properly implemented to provide realistic views of IT operations and governance on a tactical and strategic basis.

### *4.1 Consulting Engagement Objectives*

Internal auditors can act in a number of different capacities to assess and recommend ways to improve governance practices. They may provide independent, objective assessments of the design and effectiveness of governance processes within the organization. In addition to — or instead of — providing assurance, internal auditors may elect to provide consulting services.

This may be a preferred approach, particularly when known issues exist or the governance process is immature. Whether providing assurance or consulting services, the CAE may decide to use continuous monitoring methods, such as assigning internal auditors to observe meetings of governance-related bodies and advise them on an ongoing basis, as indicated in Implementation Guide 2110.

Due to consulting services being advisory in nature, the expectations and objectives are determined either by, or in conjunction with, the engagement client. Thus, consulting engagement planning typically occurs after the engagement objectives and scope have already been determined. Therefore, internal auditors may not need to complete a preliminary risk assessment, as they would when planning an assurance engagement. However, Standard 2201.C1 requires internal auditors to establish an understanding with the consulting engagement client about the objectives, scope, responsibilities, and other expectations. For significant engagements, this understanding must be documented.

Additionally, internal auditors must address governance, risk management, and control processes to the extent agreed upon with the consulting engagement client (Standard 2210.C1). Although the consulting engagement purpose and expectations are directed by the engagement client, internal auditors must ensure the engagement objectives are consistent with the organization's values, strategies, and strategic objectives (Standard 2210.C2).

A benchmarking engagement 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.

An objective for an IT governance consulting engagement could be:

- The internal audit activity will advise on the effectiveness of existing organizational structures supporting IT governance core activities.
- The internal audit activity will advise on the effectiveness of existing governance controls over change and patch management.

## 5. Establish engagement scope.

Once the risk-based objectives have been formed, the scope of the audit engagement can be determined. Because an engagement generally cannot cover everything, internal auditors must determine what will and will not be included. The engagement scope sets the boundaries of the

engagement and outlines what will be included in the review. Internal auditors must carefully consider the boundaries of the engagement to ensure that the scope will be sufficient to achieve the objectives of the engagement (Standard 2220 – Engagement Scope).

The scope may define such elements as the specific processes and/or areas, geographic locations, and time period (e.g., point in time, fiscal quarter, or calendar year) that will be covered by the engagement, given the available resources. Internal auditors must carefully consider the breadth of the scope to ensure it enables timely identification of reliable, relevant, and useful information to accomplish the identified engagement objectives (Standard 2210 – Engagement Objectives and Standard 2310 – Identifying Information).

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

- Determine whether the IT function aligns with and understands the organization's objectives and strategies.
- Review the organizational structure to identify whether there is a CIO in place, and whether this person is a member of the senior management team.
- Assess the degree to which governance activities and standards are consistent with the internal audit activity's understanding of the organization's risk appetite.
- Determine the effectiveness of IT resource and performance management.
- Assess risks that may adversely affect the IT environment.

## 6. Allocate resources.

After establishing the engagement objectives and scope, internal auditors must determine appropriate and sufficient resources to achieve the engagement objectives, as required by Standard 2230 – Engagement Resource Allocation. The interpretation of Standard 2230 clarifies that *appropriate* refers to the mix of knowledge, skills, and other competencies needed to perform the engagement, and *sufficient* refers to the quantity of resources needed to accomplish the engagement with due professional care.

Resources are allocated to the engagement based on the following:

- The knowledge internal auditors acquire during engagement planning.
- The nature and complexity of the engagement.
- Time constraints and/or the number of hours budgeted for the engagement.
- The knowledge, skills, and experience of available resources.

Internal auditors should consider whether external resources (e.g., specialists or supplemental resources) or technology will be necessary when the internal audit activity does not have appropriate or sufficient resources.

### 7. Document the plan.

During planning, internal auditors document information in engagement workpapers. This information becomes part of the engagement work program that must be established to achieve the engagement objectives, as required by Standard 2240 – Engagement Work Program.

The process of establishing the engagement objectives and scope may produce any or all of the following workpapers:

- Process map.
- Summary of interviews and brainstorming sessions.
- Preliminary risk assessment (e.g., risk and control matrix and heat map).
- Rationale for decisions regarding which risks to include in the engagement.
- Criteria that will be used to evaluate the area or process under review (required for assurance engagements, according to Implementation Standard 2210.A3).

Refer to The IIA Practice Guide "Audit Reports: Communicating Assurance Engagement Results" for detailed guidance on how to prepare an internal audit report.

## Reporting the Engagement Results

The style and format of reporting engagement results varies across organizations and should take into account laws and regulations, organizational culture and communication policies, and the expectations of senior management and the board or equivalent governing body.

Because IT governance is a strategic element of an organization's entire governance structure, it is important for the CAE to communicate with senior management, the board, and the Audit Committee the results from IT governance audits so together they may address any apparent weaknesses as they work to carry out their individual responsibilities. Standard 2060 – Reporting to Senior Management and the Board states it is the CAE's responsibility to include significant risk and control issues, including governance issues, that require the attention of those bodies. IT governance is key to an entire organization's structure and strategy, and those charged with responsibility for decision making at the highest levels must be informed as they consider the strategic impact IT governance has organizationwide.

IT governance supports the organization's regulatory, legal, environmental, and operational requirements to enable the achievement of strategic plans and aspirations, so it is imperative that senior management, the board, and the Audit Committee are apprised on a timely basis of the results of IT governance audits.

# Appendix A. Relevant IIA Standards and Guidance

The following IIA standards, guidance, and other resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

| Standards |
| --- |
| 1210 – Proficiency |
| 2000 — Managing the Internal Audit Activity |
| 2060 – Reporting to Senior Management and the Board |
| 2110 — Governance |
| 2120 – Risk Management |
| 2130 – Control |
| 2200 – Engagement Planning |
| 2201 – Planning Considerations |
| 2210 – Engagement Objectives |
| 2220 – Engagement Scope |
| 2230 – Engagement Resource Allocation |
| 2240 – Engagement Work Program |
| **Guidance** |
| Practice Guide, "Audit Reports: Communicating Assurance Engagement Results," 2016. |
| Practice Guide, "Engagement Planning: Establishing Objectives and Scope," 2017. |
| Practice Guide "Engagement Planning: Assessing Fraud Risks," 2017. |
| **Other IIA Resources** |
| Position Paper "The Three Lines of Defense in Effective Risk Management and Control," 2013. |
| CBOK Report, "Promoting and Supporting Organizational Governance: Internal Audit's Role," 2016. |

# Appendix B. Glossary

Terms identified with an asterisk (*) are taken from the "Glossary" of The IIA's *International Professional Practices Framework®* (*IPPF®*), 2017 edition.

**Assurance Services* –** An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.

**Board*** – The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, "board" in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

**Chief Audit Executive*** – Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

**Compliance*–** Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

**Consulting Services* –** Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

**Control Processes*** – The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

**Governance*** – The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

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

**Internal Audit Activity*** – A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

**Management** – To exercise control and supervision within the authority and accountability established by governance. The term management is often used as a collective term for those with responsibility for controlling an organization or parts of an organization.[3]

**Risk*** – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

**Risk Appetite*** – The level of risk that an organization is willing to accept.

**Senior Management** – Group of persons who have authority delegated from the governing body for implementation of strategies and policies to fulfill the purpose of the organization. This group can include roles which report to the governing body or the head of the organization or have overall accountability for major reporting functions, for example Chief Executive Officers (CEOs), Heads of Government Organizations, Chief Information Officers (CIOs), and similar roles.[4]

**Significance* –** The relative importance of a matter within the context in which it is being considered, including quantitative and qualitative factors, such as magnitude, nature, effect, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

**Standard*** – A professional pronouncement promulgated by the International Internal Audit Standards Board that delineates the requirements for performing a broad range of internal audit activities, and for evaluating internal audit performance.

---

[3] ISO/IEC 38500:2015, Information Technology – Governance of IT for the Organization, https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en.

[4] Ibid 5.

# Appendix C. IT Governance Internal Controls Questionnaire

The following questionnaire has been developed to help internal auditors evaluate the current IT governance state as part of the engagement planning phase.

## Organization and Governance Structures

The following questions will help the internal auditor gain an understanding of the degree or presence of IT governance:

| Question | Assessment/Comments |
|---|---|
| Is there a CIO in place, and is this function a member of the senior management team? | |
| 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? | |
| Are decision-making bodies in place to enable alignment of organizational needs with IT services and do they have adequate empowerment and accountability? | |
| 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? | |
| Are roles and responsibilities clearly defined and communicated, and are organization leaders empowered and held accountable for results? | |

## Executive Leadership and Support

The following questions will help the internal auditor gain an understanding of the degree to which the IT function is integrated into the organization:

| Question | Assessment/Comments |
|---|---|
| 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? | |
| Are the roles and responsibilities of the CIO clearly defined and communicated? | |
| 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? | |
| 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? | |
| Does IT have adequate funding to meet the organization's needs? | |

## Strategic and Operational Planning

The internal auditor can gain an understanding of how well strategic performance management has been implemented by senior management by asking the following questions:

| Question | Assessment/Comments |
|---|---|
| Do the board and senior management view IT as a strategic organizational partner? | |
| Does the strategic plan of the organization include how IT is required to support and enable value creation? | |
| Is the strategic plan supported by individual tactical operating plans that take into account IT requirements and deliverables? | |
| Are key performance indicators (KPIs) used by senior management to measure and monitor the effectiveness of the IT function? | |
| 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? | |
| Is the IT organization structured effectively relative to the size and composition of the organization? | |
| Are the CIO and IT leadership qualified and experienced? | |

## Service Delivery and Measurement

The internal auditor can gain an understanding of how well financial management of IT is functioning by asking the following questions:

| Question | Assessment/Comments |
|---|---|
| Do the board and senior management have a clear understanding of IT costs and how they contribute to the achievement of the organization's strategic objectives? | |
| Do leaders of the organization measure IT value and deliverables? If so, how? | |
| How do IT costs compare to other comparable organizations? | |
| Is CIO performance measured by financial and nonfinancial data? | |
| Are there sourcing arrangements in place? If yes, are they measured and monitored? | |

## IT Organization and Risk Management

Internal auditors can gain a high-level understanding of the IT governance environment by asking the following questions:

| Question | Assessment/Comments |
|---|---|
| To what degree are organizational processes automated? | |
| How complex is the IT infrastructure and how many applications are in use? | |
| Are data standardized and easily shared across applications (and the IT infrastructure)? | |
| Are there standard IT hardware, software, and service procurement policies, procedures, and controls in place? | |
| How mature are IT management processes and are recognized frameworks used (e.g., COBIT, ITIL, ISO)? | |
| How are risks managed in relation to meeting organizational needs, security, and compliance requirements? | |
| What is the strategic importance of IT? | |

# Appendix D. Risk and Controls Matrix for IT Governance

This appendix provides examples of business objectives, risks, and controls to help internal auditors start developing the audit work program.

## Organization and Governance Structures

| Control Objective: Organizational structures should include clear lines of reporting and role responsibilities. | |
|---|---|
| **Risk** | **Control** |
| Accountability is not clearly defined, resulting in lack of transparency of IT costs, processes, projects, and services. | The strategic goals and objectives of the organization should drive operational objectives and targets, and responsibility for objective achievement should be placed on unit leaders to promote clear accountability. |
| Lack of empowerment or accountability resulting in potential lost opportunities for innovation and collaboration. | IT and business unit leaders should be empowered to manage resources within their area of responsibility, enabling them to manage toward expected performance targets. |
| Unclear strategic alignment and understanding between the organization and IT functions, resulting in reduced contribution to stakeholder returns. | Creating multidisciplinary organizational structures allows representation of the different interests within the organization, including internal audit, which represents the interests of the entire organization. |
| Senior management and the board do not understand the basic relationship of IT and business objectives, which can result in ineffective allocation of resources to strategic initiatives and/or poor understanding of overall IT costs and their input to ROI cases. | Roles and responsibilities should provide mechanisms to link the use of IT to the overall strategies and goals of the organization. |

| Control Objective: Organizational structures include the operational nature of their components and communication protocols. | |
|---|---|
| **Risk** | **Control** |
| Unclear communication channels between IT and organizational unit leaders, resulting in an ineffective planning and monitoring system. | To ensure consistency throughout the organization, ongoing effective communication regarding IT governance should be maintained across all units and functions.<br><br>A proper communication plan should include the aspect and metrics to be informed, preparers and receivers, frequency, and escalation procedures. |

| Control Objective: IT personnel is capable of allocating resources to meet business objectives. | |
|---|---|
| **Risk** | **Control** |
| Unclear IT roles and responsibilities resulting in misalignment of resources and operational objectives. | Processes, roles, and responsibilities of IT personnel are defined, documented, and communicated. |
| Irresponsible utilization of IT resources and assets due to the absence of consistent and repeatable IT processes. | Processes are documented and evaluated periodically to ensure they are consistent and repeatable. |

## Organization and Governance Structures

| Control Objective: The organization and IT collaborate on resource priorities, initiatives, and overall investment decisions. | |
|---|---|
| **Risk** | **Control** |
| IT senior management is not included in the decision process to align IT and the organization's objectives, resulting in IT's inability to support decisions or adjust to changing priorities in a timely manner. | Senior management and the board should engage IT in strategic decisions about governance, enabling IT to add value in key decisions. |
| Lack of or poor IT portfolio management processes may result in poor prioritization of IT investments. | A strong portfolio management process exists, allowing the organization and IT to collaborate on resource priorities, initiatives, and overall investment decisions. |
| Misalignment between IT resources and operational objectives resulting in external and internal stakeholder dissatisfaction with the way the organization operates and financial results (government, regulators, society in general, shareholders, board, business partners, customers, suppliers, consultants, employees, and external auditors). | 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. |
| **Control Objective: The IT governance structure is defined in alignment with the IT architecture (for example, if the strategic management is centralized within headquarters, the governance structure should be centralized as well).** | |
| **Risk** | **Control** |
| Inadequate enterprise architecture can result in unnecessary investment in redundant or incompatible technologies. | The IT enterprise architecture should mirror the organizational structure to enable better alignment and meet the organization's needs. |
| Misalignment between the IT governance structure and the IT architecture can result in processes that do not support the organization's needs and can be too costly to modify. | The development of the IT governance structure should be based on current and anticipated IT architecture designs. |

## Executive Leadership and Support

| Control Objective: The vision, mission, and associated strategy of the organization collectively provide the direction for IT investment. | |
|---|---|
| **Risk** | **Control** |
| 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 needed to fulfill the organization's strategic goals. | The organizational vision is the basis for defining frameworks, processes, activities, roles, and relationships. This vision should be documented in the form of a strategic plan that defines IT dependencies. |
| A clear relationship between IT project performance indicators and organizational objectives does not exist. | Organizational and IT goals and metrics are aligned. |
| Senior management is not appropriately involved in the IT decision-making process, which can result in misdirection of IT resources. | Roles are established, communicated, and accepted explicitly for investment decision making, program sponsorship, program management, project management, service delivery, and associated support roles. |
| Lack of definition of the value and cost of IT in terms of impact to the organization's goals and objectives can result in poor ability of IT to achieve its goals and objectives, as well as the overall organization's strategic goals and objectives. | Formal training should be provided to information owners and administrators. This training should be mandatory during the employee onboarding process, and periodic briefing sessions should be developed to explain any changes to policy and how it affects working practices. |

| Control Objective: IT budget is communicated to senior management. | |
|---|---|
| **Risk** | **Control** |
| Senior management is unaware of IT funding and its implications to the enterprise's resources. | Budgets are updated and communicated periodically. |

| Control Objective: Budgets are controlled and monitored. | |
|---|---|
| **Risk** | **Control** |
| IT budgets are reallocated to nonstrategic projects without proper review and approval. | IT financial planning practices are reviewed regularly, and there is assurance that resources are reallocated when the proper documentation and approval are provided. |
| IT expenditures are not aligned with business objectives, which may result in resource allocation to noncritical objectives. | Require management to provide a cost benefit analysis and ROI calculations of potential IT investments as a basis for the board and senior management to make the best decisions possible. |

| Control Objective: Organizational leadership understands the investments that have been made in IT. | |
|---|---|
| **Risk** | **Control** |
| Senior management and unit leaders lack a true understanding of IT, which can result in missed opportunities or lower ROI. | To reduce the likelihood of unsound IT investment decisions, organization leaders should understand important characteristics of IT.<br><br>To this end, the CIO is invited to board meetings to discuss IT-related risk and opportunities. |
| Lack of core organizational focus by IT senior management could mean that IT is unable to focus efforts or identify inefficient use of resources. | Senior management and the board should have a clear understanding of core objectives and strategies. |

## Executive Leadership and Support

| Control Objective: IT initiatives are properly aligned with organizational objectives. | |
|---|---|
| **Risk** | **Control** |
| The strategic importance of IT is not assessed, resulting in misunderstanding of the role IT plays in the organization. | IT and organizational leaders meet on a periodic basis to review the current and upcoming IT initiatives to reassess alignment with organizational objectives (i.e., assess business case documentation validity). |
| Inadequate IT capability and/or allocation of resources to deliver required service can result in technology benefits not being achieved, resulting in lost opportunities; inability to achieve IT and organizational goals. | |
| IT resources remain allocated to objectives that are not critical. | |
| **Control Objective: IT governance helps champion innovation within IT and the entire organization.** | |
| **Risk** | **Control** |
| Lack of executive leadership commitment can lead to inadequate championing of innovation within the IT function and throughout the organization. | Leadership commitment is proven by initiatives supporting the IT strategy. |

## Strategic and Operational Planning

| Control Objective: IT and business strategies are aligned. | |
|---|---|
| **Risk** | **Control** |
| Unclear strategic alignment and understanding between the organization and IT functions can lead to:<br>▪ Reduced contribution to stakeholder returns.<br>▪ Ineffective allocation of resources to strategic initiatives.<br>▪ Lack of transparency of IT costs, processes, projects, and services.<br>▪ Poor understanding of overall IT costs and their input to ROI cases. | Accountabilities and practices are documented in governance frameworks.<br>The CIO attends executive board meetings, and IT's contribution to enterprise goals is discussed. |
| Unclear and/or inadequate organizational structures can lead to:<br>▪ Resource mismanagement and conflicting activities.<br>▪ Misalignment with resources and operational objectives.<br>▪ External and internal stakeholder dissatisfaction with the way the organization operates. | The governance framework is organized by processes and includes information about process activities, owners, and areas of improvement. |
| Unclear communication channels between IT and organizational unit leaders can lead to ineffective planning and monitoring practices. | The strategic organization should include communication protocols to ensure that IT and the organization maintain an open dialogue. |

| Control Objective: The organization has defined roles that include accountability, authority levels, and decision rights. | |
|---|---|
| **Risk** | **Control** |
| Irresponsible utilization of IT resources and assets due to the absence of consistent and repeatable IT processes. | Formal job descriptions and reporting relationships have been created and communicated for all IT positions. Processes are properly documented, published, and employees know how to find them. |
| IT investments and priorities are not aligned with business objectives. | The IT strategy is documented and updated frequently to incorporate feedback from stakeholders. |

| Control Objective: IT resources dedicate more time to tasks related to strategic objectives. | |
|---|---|
| **Risk** | **Control** |
| Inadequate allocation of resources to deliver IT critical services can result in technology benefits not achieved, lost opportunities, or complete inability to achieve organizational goals. | IT resources (employees, applications, hardware) have been allocated to support organizational objectives. |

## Service Delivery and Measurement

| Control Objective: IT delivers on its plans, budgets, and commitments. | |
|---|---|
| **Risk** | **Control** |
| Core business processes are negatively impacted by poor delivery of IT services. | Processes are in place to review key performance metrics and correct items falling below reasonable levels. |
| **Control Objective: IT department reports performance metrics to key stakeholders.** | |
| **Risk** | **Control** |
| Senior management and the board do not have a clear awareness of IT performance based on quantifiable data. | A proper communication plan should include the aspect and metrics to be informed, preparers and receivers, frequency, and escalation procedures. |
| Strategic objective achievement is not monitored and reported. | Strategic objectives are achieved rather than changed or not met. |
| Performance management activities do not include third-party metrics. | Performance management activities consider both internal and third-party IT activities. |
| No drill-down capabilities to lower-level metrics as needed can result in:<br>▪ IT investment ROI not monitored.<br>▪ Lack of decision-making information.<br>▪ Costs higher than comparable entities. | Financial reporting should be defined with sufficient detail to allow drill-down and cost analysis capabilities. |
| Lack of accurate financial data can result in value delivered by IT not tracked properly. | Financial data related to IT investments is captured and reported to stakeholders. |
| **Control Objective: IT performance reported in IT and business terms.** | |
| **Risk** | **Control** |
| IT reports are prepared using IT jargon. | IT performance reports must be structured in ways that are easy to understand by IT and non-IT stakeholders. |
| **Control Objective: Metrics based on changing business needs.** | |
| **Risk** | **Control** |
| Unclear performance indicators fail to provide an accurate state of IT initiatives. | Performance indicators are defined, including metrics and benchmarks. |

## IT Organization and Risk Management

| Control Objective: The level of IT-related risk that the enterprise is willing to take to meet its objectives is defined (risk appetite). | |
|---|---|
| **Risk** | **Control** |
| IT risk exceeds the organization's risk appetite. | The organization provides oversight of IT risk management and control activities. |
| IT risk exceeds the organization's risk tolerance. | Risk assessments and risk scenarios are updated frequently and the results are properly communicated. |
| IT risk is not integrated into the enterprise risk management (ERM) system. | The organization's risk management strategy includes IT-related risks. |
| Risk and control information is not communicated to the appropriate areas of the organization, which can result in decisions outside the organization's risk tolerance. | There is a process in place to assess, address, and communicate IT risks to key stakeholders and executive management during the project, change, and release management processes. |
| **Control Objective: A business continuity and disaster recovery plan exists and is tested on a periodic basis.** | |
| **Risk** | **Control** |
| Organization experiences significant information security breaches, resulting in negative customer reaction and damage to the organization's public reputation. | The organization has implemented a process to manage major risks, threats, changes, and contingencies proactively. |
| **Control Objective: IT projects are delivered on time and on budget.** | |
| **Risk** | **Control Objectives** |
| Project management processes do not include risk assessments. | A risk management plan exists and risk management activities are incorporated into project, change, and release management processes. |
| **Control Objective: The IT risk profile is updated frequently.** | |
| **Risk** | **Control** |
| IT risk profile is not managed properly, resulting in risks not addressed or risk taken above tolerance limits. | The IT risk profile is updated as part of ERM good practices. |

## IT Organization and Risk Management

| Control Objective: Asset classification determines what level of control is required over its handling and use. | |
|---|---|
| **Risk** | **Control** |
| Personal staff or customer data may be released or accessible to unauthorized internal or external parties. | The details of the classification, use, origin, and location should be entered into an information asset register. This should be performed by IT administrators. |
| The asset register is not updated to reflect new risks, threats, or vulnerabilities. | Processes to maintain the register will need to be developed and implemented to continuously identify the areas of greatest risk. |

| Control Objective: The organization's incentive plans are designed executed to prevent or detect unacceptable behavior. | |
|---|---|
| **Risk** | **Control** |
| Inconsistent performance management and accountability can result in actions that do not support strategic objectives. | The organization has implemented policies and processes related to staff compensation, objective setting, and performance evaluation. |
| Unacceptable behavior or excessive risk-taking is not detected. | Associated measurements (e.g., key performance indicators) and incentive plans (e.g., bonuses) are appropriately designed and executed to prevent or detect unacceptable behavior or excessive risk-taking and to support actions aligned with the organization's strategic objectives. |

# Appendix E. Additional Resources

The Committee on the Financial Aspects of Corporate Governance, *Financial Aspects of Corporate Governance* (The Cadbury Report), 1992. http://www.ecgi.org/codes/documents/cadbury.pdf.

*COBIT* is a framework for the governance of enterprise IT published by ISACA in 2012. www.isaca.org/cobit/pages/default.aspx.

Institute of IT Governance (Institut de la Gouvernance des Systemes d'Information), *The place of IT Governance in the Enterprise Governance: Balancing Performance and Conformance*, 2005, offers a general framework for IT governance and its place inside the global enterprise governance.
http://cigref.typepad.fr/itgifrance/files/place_IT_governance_in_enterprise_governance.pdf

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 38500:2015, *Governance of IT for the Organization*, 2015 version is a framework for corporate governance of IT and is a key input to other frameworks such as ITIL and COBIT. https://www.iso.org/standard/62816.html.

IT Infrastructure Library (ITIL) is a framework developed by the United Kingdom's Cabinet Office as a library of best practice processes for IT service management. https://www.itil-itsm-world.com/index.htm.

The Institute of Directors in Southern Africa (IoDSA), *King Report on Corporate Governance* and *King Code of Corporate Governance* (King III) was compiled by the King Committee in response to the emergence of the South African companies Act 71 of 2008. A new King IV was published on Nov. 1, 2016. http://www.iodsa.co.za/?kingIII.

National Computing Centre, IT Governance: Developing a successful governance strategy, NACD 2005.

NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, NIST 2011.

Organisation for Economic Co-operation and Development (OECD), G20/*OECD Principles of Corporate Governance, 2015 version.*

Selig, Gad J. *Implementing IT Governance: A Practical Guide to Global Best Practices in IT Management*. Zaltbommel, NL: Van Haren Publishing, 2008.

# Acknowledgements


## Guidance Development Team

Himi Tina Kim CIA, CGAP, CRMA, United States (Chairman)

Avin Mansookram, South Africa (Project Lead)

Kenneth Drinkard, United States

Sajay Rai, United States

Terence Washington, CIA, CRMA, United States

## Global Guidance Contributors

Harun Abdul Haqq, CIA, CISA, CFE, Trinidad and Tobago

Graciela Braga, CGEIT, CSX (F), Argentina

Jason Brucker, CISA, CGEIT, United States

Elastos Chimwanda, CIA, CISA, Zimbabwe

Jamie DuBray, CIA, CRMA, CISA, CGEIT, CISSP, United States

Ulrich Hahn, CIA, CGAP, CRMA, CISA, Germany

Nigel James, CISA, United States

Stephen Stanbury, CIA, CRMA, CFE, United Kingdom

## IIA Global Standards and Guidance

Eva Sweet, CISA, CISM, IT and PS Director (Project Lead)

Lisa Hirtzinger, CIA, QIAL, CCSA, CRMA, Vice President

Debi Roth, CIA, Managing Director

Lauressa Nelson, Technical Writer

Michael Citro, Technical Writer

*The IIA would like to thank the following oversight bodies for their support: Information Technology Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and International Professional Practices Framework Oversight Council.*

## About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 190,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

## Disclaimer

The IIA publishes this document for informational and educational purposes and, as such, is only intended to be used as a guide. This guidance material is not intended to provide definitive answers to specific individual circumstances. 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© 2018 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact guidance@theiia.org.

January 2018

The Institute of Internal Auditors | Global

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101
www.theiia.org