Auditing IT Governance and IT Management

3rd Edition

Global Practice Guide

Aligns with the Global Internal Audit Standards

The Institute of Internal Auditors

GLOBAL TECHNOLOGY AUDIT GUIDE

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

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

Global Guidance Council Reviewers (3rd edition)

Augusto Cuenca, CIA, Paraguay

Mark Sullivan, CIA, QIAL, United Kingdom

International Internal Audit Standards Board Reviewers (3rd edition)

Marthin Johann Grobler, CIA, CRMA, South Africa

James A. Rose, CIA, CRMA, United States

IIA Standards and Guidance

Benito Ybarra, CIA, CFE, CISA, CCEP, Executive Vice President

Katleen Seeuws, CIA, CGAP, CRMA, CFE, CISA, Vice President

George Barham, CIA, CRMA, CISA, Director (Project Lead)

The IIA thanks the following oversight bodies for their support: Global Guidance Council, International Internal Audit Standards Board, and the International Professional Practices Framework Oversight Council.

About the IPPF

International Professional Practices Framework® (IPPF)

A framework provides a structural blueprint and coherent system that facilitate the consistent development, interpretation, and application of a body of knowledge useful to a discipline or profession. The International Professional Practices Framework® (IPPF)® organizes the authoritative body of knowledge, promulgated by The Institute of Internal Auditors, for the professional practice of internal auditing. The IPPF includes Global Internal Audit Standards™, Topical Requirements, and Global Guidance.

The IPPF addresses current internal audit practices while enabling practitioners and stakeholders globally to be flexible and responsive to the ongoing needs for high-quality internal auditing in diverse environments and organizations of different purposes, sizes, and structures.

Global Guidance

Global Guidance supports the Standards by providing nonmandatory information, advice, and best practices for performing internal audit services. It is endorsed by The IIA through formal review and approval processes.

Global Guidance provides detailed approaches, step-by-step processes, and examples on subjects including:

- Assurance and advisory services.
- Engagement planning, performance, and communication.
- Financial services.
- Fraud and other pervasive risks.
- Strategy and management of the internal audit function.
- Public sector.
- Sustainability.
- Global Technology Audit Guides® (GTAG®) provide auditors with the knowledge to perform assurance and advisory services related to an organization's information technology and information security risks and controls.

Global Guidance is available as a benefit of membership in The IIA.

Contents

Executive Summary

Taking a strategic approach to implementing information technology (IT) governance and IT management helps organizations address the speed of technological advancements, the proliferation of IT services, and an increasing need to use IT to meet organizational objectives. Effective IT governance and IT management contribute to control efficiency and effectiveness and allow an organization's investment in IT to realize financial and nonfinancial benefits. When controls are poorly designed or not established, weak or ineffective IT governance or IT management is often a root cause.

Note

Alignment of organizational objectives and IT is more about governance and management and less about technology. Governance assures alternatives are evaluated, execution is appropriately directed, and risk and performance are monitored. Management is focused on monitoring the daily performance of IT processes that support the organization.

The Global Internal Audit Standards define governance 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 directly related to board oversight of IT assets and risks.

The primary outcomes of effective IT governance include:

- IT strategies are aligned with organizational objectives.
- A risk management process is established to identify, manage, and monitor IT threats promptly.
- IT investments and resources are optimized to deliver value to the organization.
- Metrics are established to monitor and report on IT performance.

ISACA defines management as "the planning, building, running, and monitoring of activities in alignment with the direction set by the governance body to achieve the enterprise objectives."[1] IT management carries out the processes and daily supervision that tactically align with the board's overall strategic guidance to ensure the organization's IT resources are used effectively, efficiently, and acceptably.

Outcomes of effective IT management include ensuring:

1. "Glossary," ISACA, accessed August 1, 2025, https://www.isaca.org/resources/glossary#glossm.

- IT performance is defined, measured, and reported using meaningful metrics.
- Risks are identified and managed properly, including communication with the board.
- IT resources are managed effectively and efficiently.

Absent or poor IT governance or IT management can have significant negative impacts on an organization, both financially and reputationally. Recovery from such impacts requires resources, such as time, effort, and money. IT is critical to the organization's development of competitive advantage and its achievement of goals and strategic objectives.

The internal audit function should be uniquely positioned and staffed to assess whether the organization's IT governance and IT management support its strategies and objectives and to make necessary recommendations (Standards 9.1 Understanding Governance, Risk Management, and Control Processes and 14.4 Recommendations and Action Plans).

In its third edition, this GTAG aligns with the 2024 International Professional Practices Framework, including the Global Internal Audit Standards™ and Topical Requirements.

Introduction

The Global Internal Audit Standards define **governance** 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, a subdiscipline of organizational governance, focuses on establishing structures, policies, processes, and frameworks to ensure that the organization's information technology supports its strategies and objectives. IT governance supports the organization's **compliance** and operational requirements, enabling it to achieve its strategic plans and aspirations.

IT management supports the achievement of organizational objectives. It is the responsibility of **senior management**, which the Standards define as "The highest level of executive management of an organization that is ultimately accountable to the board for executing the organization's strategic decisions, typically a group of persons that includes the chief executive officer or head of the organization."

Note

Terms in **bold** are defined in the glossary in Appendix B.

The Global Internal Audit Standards use certain terms as defined in the glossary. To understand and implement the Standards correctly, it is necessary to understand and adopt the specific meanings and usage of the terms as described in the glossary.

The Standards use the word "must" in the Requirements sections and the words "should" and "may" to specify common and preferred practices in the Considerations for Implementation sections.

This guidance aims to assist internal auditors in providing **assurance** or **advisory services** on IT governance and IT management. It provides a high-level description of relevant processes, practices, and terminology to help internal auditors understand the concepts of governance and management functions and the characteristics of good governance and management processes. The guide focuses on the processes and mechanisms that internal auditors can use to assess whether the IT governance and IT management programs support the organization's strategies and objectives, supporting conformance with Standard 9.1 Understanding Governance, Risk Management, and Control Processes.

In addition, this guidance may be supplemented by internationally recognized frameworks that detail the processes and mechanisms needed to develop, implement, evaluate, and improve IT governance and IT management programs. Examples of such frameworks appear in Figure 1.

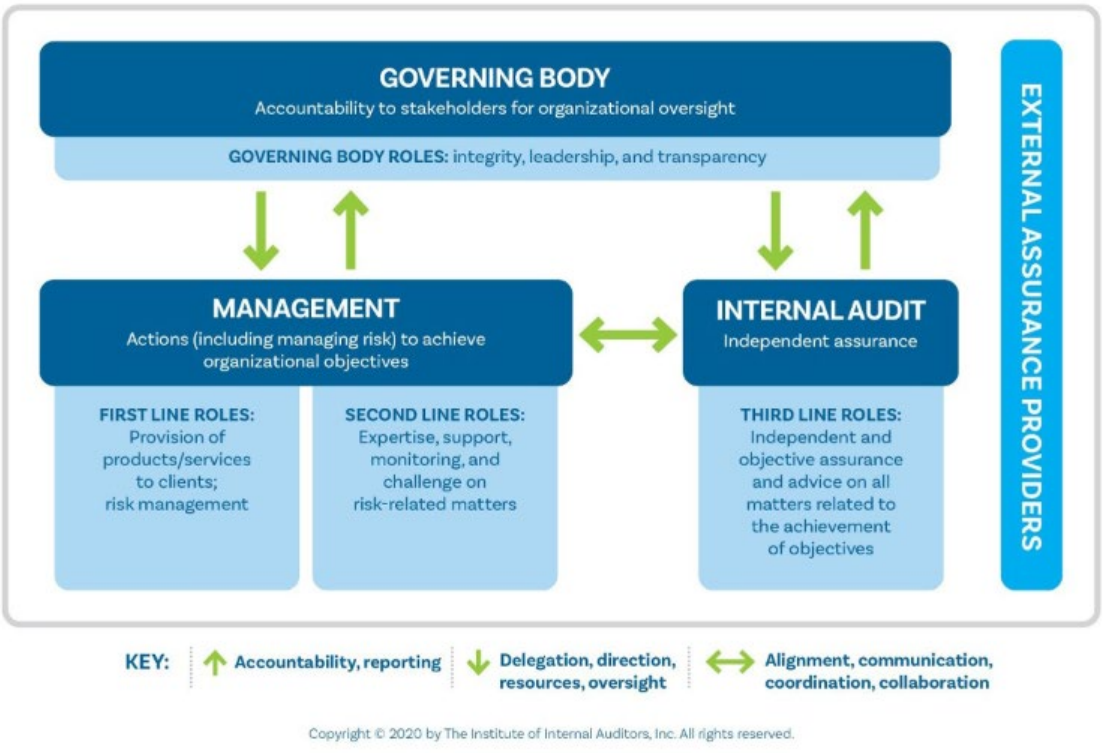
Figure 1. IT Frameworks

IT Governance Frameworks	IT Management Frameworks
• *COBIT® 2019 Framework: Governance and Management Objectives.* • *ISO/IEC 38500:2024 – Governance of IT for the Organization.* • *King IV Report on Corporate Governance for South Africa 2016.*	• *Information Technology Infrastructure Library (ITIL® 4).* • *ISO/IEC 27001:2022 – Information Security Management Systems.* • *CIS Critical Security Controls Version 8.1.*

The Three Lines Model

While the board and senior management both have vital responsibilities regarding IT performance, it is important to distinguish between them since they have separate roles in supporting **stakeholder** IT expectations. "The IIA's Three Lines Model: An Update of the Three Lines of Defense" states, "Stakeholders entrust organizational oversight to a governing body,[2] which in turn delegates resources and authority to management to take appropriate actions, including managing **risk**." Figure 2 depicts the relationships in the model.

Figure 2. The IIA's Three Lines Model



While governance, **risk management**, and **control processes** are interrelated, it is important that roles and responsibilities are clearly defined. For example, the board is responsible for effective

2. The meaning of the term "governing body" in the Three Lines Model parallels that of the term "board" in the Global Internal Audit Standards. Thus, the terms can be considered synonyms.

governance activities, such as considering risks when setting strategy. Risk management, a second-line responsibility maintained by management, supports effective governance by providing risk considerations that are used to formulate strategic direction. Likewise, effective governance oversight relies on independent **assurance** provided by the **internal audit function** in its third line role, such as assessing the effectiveness of internal **controls**. Timely and ongoing communication between the board, senior management, and the internal audit function is vital.

IT Governance Overview

IT governance is crucial for ensuring IT services deliver value to the organization in a controlled and effective way, thus supporting the organization's ability to achieve strategic goals. The board (or governing body) is 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.

Key governance areas include:

- **Strategic alignment –** IT governance directs the IT strategy and IT's alignment with the organization's services, projects, objectives, strategy, and the linkage between business objectives and IT initiatives.

  Additional details are available in ISACA's *COBIT 2019 Framework: Governance and Management Objectives,* Objective EDM 01 Ensured Governance Framework Setting and Maintenance.

- **Risk oversight –** IT governance oversees the processes in place to ensure that risks have been identified and adequately mitigated by management. Additionally, IT governance can ensure that enterprise risk management includes:
  - Risk aspects of investments within the IT portfolio.
  - Defined responsibilities for risk management.
  - A common risk analysis methodology.
  - Strategies for holistically addressing risks including continuously monitoring threats, occurrences, and **impacts**.

  Additional details are available within ISACA's *COBIT 2019 Framework,* Objective EDM 03 Ensured Risk Optimization.

- **Enabling value delivery –** IT governance helps the organization and its IT function collaborate, promoting maximum IT value. The board enables management to oversee IT's delivery of value, measure return on investments, execute an IT tactical plan, and report on the benefits achieved at each level of the organization. Examples of IT benefits include establishing direction and monitoring system uptime (infrastructure strategy), automating the software development strategy, increasing productivity (operational strategy), and increasing revenue (IT financial strategy).

Additional details are available within ISACA's *COBIT 2019 Framework,* Objective EDM 02 Ensured Benefits Delivery.

- **Performance oversight –** IT governance monitors strategic compliance (for example, the achievement of strategic IT objectives), IT performance, and IT's contribution to the bottom line (such as the delivery of promised business functionality). IT governance determines which key performance indicators should be established and tracked by management.

  Additional details are available within ISACA's *COBIT 2019 Framework,* Objective EDM 05 Ensured Benefits Delivery.

- **Resource oversight –** IT governance provides strategic direction for sourcing and using IT resources. Such strategic direction includes overseeing the aggregate funding of IT at the enterprise level and ensuring IT capabilities and infrastructure can support current and expected future business requirements. IT resources are commonly known as the "IT portfolio" and include the assets (hardware and software), services, projects, and vendors needed to deliver both short- and long-term technology solutions to the organization.

  Additional details are available within ISACA's *COBIT 2019 Framework,* Objective EDM 02 Ensured Benefits Delivery.

IT Management Overview

IT management is responsible for an organization's daily activities: planning, executing, and monitoring the use of IT resources to ensure the achievement of the strategies and policies established by the board. IT management should communicate with the board regularly (for example, quarterly) to provide the timely and relevant information necessary to enable effective governance.

The IIA's Three Lines Model states, "Management's responsibility to achieve organizational objectives comprises both first- and second-line roles. First-line roles are most directly aligned with the delivery of products and/or services to clients of the organization and include the roles of support functions. Second-line roles assist with managing risk."

Key areas of management include:

- **Operational management –** IBM defines IT operations as "the process of implementing, managing, delivering, and supporting IT services to meet the business needs of internal and external users."[3] IT management plays a critical role in ensuring that the organization is supported from a technology standpoint and has the critical services that are necessary to keep all functions running properly. IT project management is an important

3. "What is IT operations," IBM, October 8, 2021, https://www.ibm.com/think/topics/it-operations.

aspect of operational management, as it ensures that significant hardware or software installations or upgrades are deployed effectively.

Additional details are available within ISACA's *COBIT 2019 Framework,* Objectives APO 01 Managed I&T Management Framework, APO 02 Managed Strategy, and DSS 01 Managed Operations.

- **Risk management** — Risk management, or **enterprise risk management**, is a second-line function that broadly focuses on risks that affect the entire organization, including covering compliance with laws, regulations, and other external requirements. Additionally, IT risk management is a vital component of enterprise risk management. Management may use a framework to support their efforts.

  Examples include *NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, *COBIT 2019 Framework*, and COSO's *Enterprise Risk Management—Integrating with Strategy and Performance*.

- **Control processes** — While enterprise risk management is defined as a second-line function, it is important to note that managing daily risks is a first-line function, because the first line is responsible for ensuring that the **control processes** are established and operating effectively.

  Additional details are provided within ISACA's *COBIT 2019 Framework*, MEA 02 Managed System of Internal Control, MEA 03 Managed Compliance with External Requirements, APO 12 Managed Risk, and DSS 06 Managed Business Process Controls.

- **Performance measurement and monitoring** — IT management works closely with IT governance to understand the board's expectations for using performance measures or key performance indicators to track the achievement of strategic IT objectives and to measure IT performance. Additional metrics include continuous monitoring and reporting, follow-up policies, **root cause** analysis, problem management, and benchmarking against industry practices and proven standards or frameworks.

  Additional details are provided within ISACA's *COBIT 2019 Framework*, MEA 01 Managed Performance and Conformance Monitoring.

- **Resource management** — IT management is responsible for managing IT resources to support organizational technology requirements, sourcing strategies, human resource management, user manuals, segregation of duties, time reporting, infrastructure life cycle management, service level agreements, and acceptable usage policies.

  ISACA's *COBIT 2019 Framework* provides additional details within Objectives APO 05 Managed Portfolio, APO 06 Managed Budget and Costs, BAI 01 Managed Programs, BAI 09 Managed Assets, and BAI 11 Managed Projects.

Together, IT governance and IT management can help organizations address challenges, including:

- 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 continuing elevated risk of cyberattacks[4].
- An increase in laws and regulations related to data privacy and protection.
- An increase in the adoption and use of artificial intelligence.
- The need to strengthen organizational resilience.

In the Three Lines Model, operational management (including IT) is the first line and is responsible for implementing and maintaining processes and controls to mitigate risks. Compliance functions and risk management are the second line, and they are responsible for monitoring risks across the organization.

Good IT Governance and IT Management at a Glance

- Governance structure focuses primarily on whether IT supports and helps enable the organization to achieve its strategic objectives.
- The tone at the top (from the board and senior management) is communicated effectively to all levels within the organization, supporting effective IT governance and IT management.
- Service delivery metrics, including financial management, are used to measure, monitor, and control IT's costs and benefits.
- Performance monitoring, including periodic reporting to the board, is an integral component, enabling proper mechanisms to manage the needs of the organization and IT service delivery.

Business Significance

The information and technological components of an organization are among its most important assets. A lack of appropriate governance and management 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. Other possible negative outcomes from a lack of appropriate governance and management could include financial losses, loss of the confidence of investors and other stakeholders, job losses, and regulatory fines. Simply put, IT governance and IT management can influence and impact not just IT but the entire organization.

4. The Internal Audit Foundation's *2025 Global Risk in Focus* report that indicates that cybersecurity continues to be the leading risk on a globally. https://www.theiia.org/en/internal-audit-foundation/latest-research-and-products/risk-in-focus/.

Greater dependency on systems and information means that organizations are investing greater resources to improve and maintain their IT environments. The resources 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 strategic: aligning IT goals and objectives with organizational priorities to ensure that IT efforts concentrate on processes and projects that support the organization's strategic goals. IT management's focus is on the operational performance and delivery of IT services and resources to support the numerous processes that rely on technology. Successful alignment between the organization and IT occurs when the board and senior management understand IT's value as a strategic partner and recognize its role in supporting the achievement of strategic and operational goals.

Effective IT governance and IT management provide 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, allowing continuous process improvement.

Proper Alignment

Proper alignment between the organization and IT means:

- The board and senior management understand IT's capabilities and limitations.
- IT senior management understands the organization's objectives and corresponding needs.
- The organization's structures of governance, management, and accountability reflect and monitor this understanding.

Activities that are within the scope of IT governance and IT management include:[5]

- Aligning IT investments and priorities with business objectives.
- Managing, evaluating, prioritizing, funding, measuring, and monitoring requests for and outcomes of IT services in a more consistent and repeatable manner that optimizes returns to the business.
- Responsibly using resources and assets.
- Establishing and clearly defining roles, accountability, and authority (decision rights).
- Ensuring that IT delivers on its plans and commitments within its budget.

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

- Managing major risks, threats, changes, and contingencies proactively.
- Improving IT organizational performance, compliance, maturity, staff development, and **outsourcing** initiatives.
- Promoting innovation within IT and the entire organization.

Key Risks

Just as the benefits of effective IT governance and IT management can help an organization achieve financial and nonfinancial objectives, improve operations, and control risk, poor IT governance and IT management can negatively affect the entire organization.

Emphasizing IT's technical and financial aspects instead of its role as a business enabler usually results in negative outcomes, such as a poor return on IT investments or a failure to demonstrate the benefits they generate.

Other examples of negative impacts include:

- Financial losses due to business disruption.
- Higher costs to run business operations.
- Unsatisfied customers.
- Poorly delivered IT services resulting in unsupported core business processes.
- Unidentified risks and threats that leave the organization vulnerable to security breaches.
- Penalties resulting from failing to meet regulatory requirements.

The Internal Audit Function's Role

The internal audit function, as the third line, is responsible for providing independent assurance that risk management and controls operate effectively and for informing senior management and the board when deficiencies are identified. This responsibility includes the **chief audit executive** promptly communicating any identified "themes related to the organization's governance, risk management, and control processes…, along with insights, advice, and/or conclusions, to the board and senior management," as described in Standard 11.3 Communicating Results.

The responsibility is also reflected in Standard 14.4 Recommendations and Action Plans, which requires internal auditors to "determine whether to develop recommendations, request action plans from management, or collaborate with management to agree on actions to…enhance or improve the **activity under review**." Additionally, Standard 14.5 Engagement Conclusions states, "Assurance **engagement conclusions** must include the internal auditors' judgment regarding the effectiveness of the governance, risk management, and/or control processes of the activity under review, including an acknowledgment of when processes are effective."

The internal audit function may provide both assurance and advisory services related to IT governance and IT management. The services provided depend on the **engagement objectives** and scope (Standard 13.3 Engagement Objectives and Scope). As described in Principle 2 Maintain Objectivity of the GIAS, "Internal auditors must maintain professional **objectivity** when performing all aspects of internal audit services. Professional objectivity requires internal auditors to apply an impartial and unbiased mindset and make judgments based on balanced assessments of all relevant circumstances. Internal auditors must be aware of and manage potential biases."

Governance and management processes are considered during the internal audit function's engagement **risk assessment** and when determining the objectives and scope of the engagement (Standards 13.2 Engagement Risk Assessment and 13.3). The chief audit executive must consider the organizationwide risk assessment on which the **internal audit plan** was based (Standard 9.4 Internal Audit Plan).

Assurance engagements of IT governance and IT management should focus on the organization's implementation of governance and management practices.

Internal audit services will likely include activities such as:

- Determining whether the organization's policies, roles, responsibilities, and accountabilities are clearly defined.
- Assessing whether the tone at the top and communication are effective,
- Determining how IT value is managed.
- Assessing the degree to which governance and management activities and standards are consistent with the internal audit function's understanding of the organization's **risk appetite**.
- Conducting advisory services as allowed by the **internal audit charter** and approved by the board.
- Ongoing dialogue with those responsible for IT governance and IT senior management (including enterprise risk management) to ensure that substantial changes in the organization and the risks to which it is exposed are addressed in a timely manner.

When reviewing governance and management, the internal audit function must do more than just identify issues. The function must collaborate with management to identify **root causes** and make constructive recommendations when weaknesses in IT controls are identified. For example, if a firewall configuration is poor or weak, different layers of controls may be evaluated to identify the root cause of the problem (Standards 11.3 Communicating Results and 14.3 Evaluation of Findings).

The internal audit function adds value when it identifies root causes and cooperates with management to ensure constructive action plans are created to address the issue (Standards 14.4 Recommendations and Action Plans and 15.1 Final Engagement Communication).

Assessing IT governance and IT management may involve assurance and/or advisory services to evaluate how the organization identifies and assesses significant risks and selects appropriate control processes. This includes understanding how the organization identifies and manages the following key risk areas:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws and/or regulations.

Strengthening Governance and Management

Factors that can help strengthen IT governance and IT management:

- Clear IT ownership and accountability.
- The chief information officer having a reporting line to both senior management and the board.
- Recognition of IT's potential innovation value.
- Monitoring and measurement of IT performance and its contribution to the organization's ability to achieve its objectives.

Plan Engagements Effectively

Internal auditors must develop and document a work program for each engagement (Standards 13.3 Engagement Objectives and Scope and 13.6 Work Program). During planning, internal auditors must consider the organization's strategies, objectives, and risks relevant to the engagement (Standard 13.2 Engagement Risk Assessment). This section is intended to help the internal auditor determine the key areas that should be included in an IT governance and IT management engagement, the type of documents that may be requested, questions that may be included in interviews, and evidence documentation that should be obtained. The examples provided are not exhaustive.

When planning the engagement, internal auditors should determine whether the organization has unified and cohesive governance and management structures in place, including formal reporting lines, policies, processes, and tools to consistently manage the environment and control IT-related risks.

It may be difficult to assess the entirety of IT governance and IT management programs; instead, the scope of a single engagement may meet a specific objective. For example, the scope may be defined by organizational units, locations, a strategic objective, or any other **criteria** that are meaningful to the organization.

Understand the Engagement's Context and Purpose

The chief audit executive and internal auditors should clearly understand the concepts and characteristics of typical governance and management processes, as described briefly in the introduction and detailed in The IIA's Global Internal Audit Standards and Three Lines Model and other governance and risk management frameworks. The chief audit executive contemplates whether the current internal audit engagements encompass the organization's governance and management processes and address their associated risks. Governance exists as an independent function from management, as described in The IIA's Three Lines Model.

How an organization designs and practices the principles of effective governance and management depends on factors such as its type, size, complexity, life cycle, maturity, stakeholder structure, and the legal and regulatory requirements to which the organization is subject. The internal audit function's approach to assessing governance and making recommendations should vary based on the framework or model the organization uses. Internal auditors should first identify the framework(s) the organization uses to drive effective IT governance and IT management, since this could provide the most relevant criteria for the engagement (Standard 13.4 Evaluation Criteria). If the organization has not implemented a

framework, internal auditors can offer to perform an advisory engagement to help management map existing controls and practices to an agreed-upon framework.

The "Considerations for Implementation" section of Standard 9.1 Understanding Governance, Risk Management, and Control Processes states, "The chief audit executive may review board and committee charters and agendas and minutes from their meetings to gain additional insight into the role the board plays in the organization's governance, especially regarding strategic and operational decision-making."

The section also advises the chief audit executive to gather risk information by reviewing "recently completed risk assessments and related communications issued by senior and operational management, those charged with risk management, external auditors, regulators, and other internal and external providers of **assurance services**."

The chief audit executive may also speak with others in key governance and management roles (such as chairman of the board, audit committee chair, top elected or appointed official in a governmental entity, chief ethics officer, human resources officer, independent external auditor, chief compliance officer, chief risk officer, or others) to gain a clearer understanding of the organization-specific processes and assurance activities already in place. If the organization is regulated, the chief audit executive may want to review any governance or management concerns identified by regulators.

An understanding of both IT governance and IT management processes provides the foundation for a discussion with the board and senior management about what constitutes governance versus management, so that an appropriate internal audit plan and approach can be implemented.

Gather Information

Obtaining a thorough understanding of the organization, IT governance, and IT management enables internal auditors to conduct a preliminary assessment of the relevant risks, as required by Standard 13.2 Engagement Risk Assessment. Sources of information include documentation and interviews with stakeholders.

It is helpful to note that this process is not always a sequential, linear progression 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 (such as risk assessments and reports by assurance and advisory service providers), understanding and mapping process flows and controls, and interviewing relevant stakeholders.

Examples of documentation internal auditors may request to plan the engagement include:

- Past audit reports.
- Strategic plans (organization's mission, vision, strategy, and goals).
- Organizational governance framework.

- IT governance framework.
- Information security policy.
- IT architecture policies.
- Organizational charts.
- Enterprise risk management reports.
- Board and audit committee meeting minutes.
- Management reports, such as IT performance reports
- Approvals and documentation of exceptions.

Document Information in the Engagement Work Program

It is important that internal auditors document the information gathered while developing the plan, in accordance with Standards 13.6 Work Program and 14.1 Gathering Information for Analyses and Evaluation. At the end of engagement planning, the **engagement work program** should document:

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

Additionally, the work program must identify:

- Criteria to be used to evaluate each objective.
- Tasks to achieve the engagement objectives.
- Methodologies, including the analytical procedures to be used, and the tools to perform the tasks.
- Internal auditors assigned to perform each task.

Interview Relevant Stakeholders

Interviewing relevant stakeholders is a critical step that helps internal auditors better understand the objectives, design, operations, and control environment of the activity 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. These interviews can also help auditors gauge whether the organization's efforts result

in sufficient awareness of its ethical expectations and whether employees have a clear understanding of their responsibilities regarding risk and control processes and the impacts of those processes on the organization.

Examples of interview questions include:

- Does the board understand the organization's IT needs? How is that understanding reflected in the strategic plan? How does management provide periodic updates to the board regarding its performance and achievement of strategic goals?
- Do you have a clear definition of your role in IT governance or IT management? How do you know that you are meeting expectations?
- Which decision-makers do you consult when making IT-related decisions?
- What policies exist, and how are they disseminated?
- How does the organization measure value?

In addition, internal auditors may brainstorm with personnel individually or in 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?"

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 (Standard 13.2 Engagement Risk Assessment).

IIA Audit Tool

The IIA's **"**Enterprise and Business Process Risks Tool**"** provides a practical approach to identifying, assessing, managing, and monitoring risks. It features a comprehensive user guide and customizable companion Excel workbook.

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

Figure 3 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.

Figure 3. Risk and Control Matrix for IT Governance and IT Management

Risk Scenario	Risk	Control
In a decentralized operating model, the strategic business units are allowed to operate more independently, have their own IT budgets, and use different applications and IT infrastructure.	The organization is unlikely to succeed in effectively deploying a single set of IT standards related to its 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. The development of the IT governance structure should be based on current and anticipated designs of IT architecture.
The organization does not include IT risk management as part of project management practices.	Projects can fail due to poor planning to address IT 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.

Establish Engagement Objectives

Once internal auditors have completed the preliminary risk assessment and identified the significant risks to evaluate during the engagement, they can establish the engagement objectives (Standard 13.3 Engagement Objectives and Scope). The engagement objectives articulate what the engagement is specifically attempting to accomplish; therefore, they should have a clear purpose, be concise, and be linked to the risk assessment (Standard 13.2 Engagement Risk Assessment).

The engagement objectives for IT governance or IT management may be related to compliance with external and internal requirements or the operational performance of the IT processes. Engagement objectives may be established in various ways. For example, the objectives can be defined as part of the audit plan (Standard 9.4 Internal Audit Plan); in relation to the results of enterprise risk management, past audit **findings**, or regulatory requirements; or based on specific board requests for assurance (Standard 11.1 Building Relationships and Communicating with Stakeholders).

The following are examples of how objectives might be formulated for an IT governance and IT management assurance engagement.

The internal audit function will provide assurance that:

- IT governance and IT management activities and standards are consistent with the internal audit function's understanding of the organization's risk appetite.
- The enterprise risk management process addresses substantial IT risks by identifying and escalating threats in a timely manner, including communicating with the board about them.
- The linkage between IT metrics and objectives aligns with the organization's goals.
- IT management properly monitors metrics to provide realistic views of IT operations and communicates with the board about the performance relative to goals and objectives.

Advisory Engagement Objectives

When the organization's IT governance or IT management processes are known to be immature or have existing issues, advisory services related to the design and effectiveness of these processes may be more appropriate than assurance services. For advisory services, the expectations and objectives may be determined either by or in conjunction with the party requesting the services. Thus, advisory 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 4.2 Due Professional Care and Standard 13.3 Engagement Objectives and Scope still apply to advisory engagements.

A benchmarking engagement could provide an effective starting point in a multi-year audit plan because it allows time to address design gaps in the governance or management structure before additional reviews are performed.

An example of an objective for an advisory engagement on IT governance could be:

- The internal audit function will advise on the effectiveness of existing organizational structures supporting IT governance core activities.

An example of an objective for an advisory engagement on IT management could be:

- The internal audit function will advise on the design of existing management controls over change and patch management.

Establish Engagement Scope

Once the risk-based objectives have been formed, the scope of the assurance 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 13.3 Engagement Objectives and Scope).

The scope may define elements such as the specific processes and/or areas, geographic locations, and time period (such as point in time, fiscal quarter, or calendar year) that the engagement will cover, given the available resources. Internal auditors must carefully consider the breadth of the scope to ensure it enables the timely identification of reliable, relevant, and useful information to accomplish the identified engagement objectives (Standard 14.1 Gathering Information for Analyses and Evaluation).

In scoping and performing an IT governance or IT management engagement, internal auditors should:

- Determine whether the IT function aligns with and understands the organization's objectives and strategies.

- Review the organizational structure to identify whether a chief information officer is in place, and whether that role is considered part of the senior management team.
- Assess the degree to which IT governance or IT management activities and standards are consistent with the internal audit function's understanding of the organization's risk appetite.
- Determine the effectiveness of the management of IT resources and related performance.
- Assess risks that may adversely affect the IT environment.

Identify Evaluation Criteria

Internal auditors must also identify the most relevant criteria to evaluate the aspects of the activity under review defined in the engagement objectives and scope (Standard 13.4 Evaluation Criteria). Adequate criteria are relevant, aligned with the objectives of the organization and the activity under review, and produce reliable comparisons.

Standard 13.4 states, "Internal auditors must assess the extent to which the board and senior management have established adequate criteria to determine whether the activity under review has accomplished its objectives and goals. If such criteria are adequate, internal auditors must use them for the evaluation. If the criteria are inadequate, internal auditors must identify appropriate criteria through discussion with the board and/or senior management." Internal auditors may also consider seeking input from subject matter experts or assurance providers to help develop relevant criteria (Standard 9.5 Coordination and Reliance).

Examples of criteria include:

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

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

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 13.5 Engagement Resources, which states that "Internal auditors must consider whether the available financial, human, and technological resources are appropriate and sufficient to achieve the engagement objectives."

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 competencies of available staff resources.

Internal auditors should consider whether external human resources (for example, specialists or supplemental resources) or technological resources will be necessary when the internal audit function does not have appropriate or sufficient resources.

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 13.6 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 (such as a risk and control matrix or heat map).
- Rationale for decisions regarding which risks to include in the engagement.
- Criteria that will be used to evaluate the activity under review (required for assurance engagements, according to Standard 13.4 Evaluation Criteria).

Communicate Engagement Results

The style and format for communicating the **engagement results** vary across organizations and should consider laws and regulations, organizational culture and communication policies, and the expectations of the board and senior management.

It is important for the chief audit executive to communicate promptly and regularly with the board and senior management about the results from engagements that assess IT governance and IT management because these IT functions support the organization's compliance with legal/regulatory, environmental, and operational requirements, ultimately facilitating performance and enabling the achievement of strategic plans.

Together, the board and senior management can address any weaknesses identified. Standards 8.1 Board Interaction, 11.3 Communicating Results, 11.5 Communicating the Acceptance of Risks, and 15.1 Final Engagement Communication discuss the communication of significant risk and control issues, including governance and management issues. IT governance and IT management are both key to the structure, strategy, and performance of organizational governance. Those charged with responsibility for decision-making at the highest levels must be informed as they consider the strategic impact of IT governance and IT management organizationwide.

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced in this guide.

Standards
Standard 4.2 Due Professional Care
Standard 8.1 Board Interaction
Standard 9.1 Understanding Governance, Risk Management, and Control Processes
Standard 9.4 Internal Audit Plan
Standard 9.5 Coordination and Reliance
Standard 11.1 Building Relationships and Communicating with Stakeholders
Standard 11.3 Communicating Results
Standard 11.5 Communicating the Acceptance of Risks
Standard 13.2 Engagement Risk Assessment
Standard 13.3 Engagement Objectives and Scope
Standard 13.4 Evaluation Criteria
Standard 13.5 Engagement Resources
Standard 13.6 Work Program
Standard 14.1 Gathering Information for Analyses and Evaluation
Standard 14.3 Evaluation of Findings
Standard 14.4 Recommendations and Action Plans
Standard 14.5 Engagement Conclusions
Standard 15.1 Final Engagement Communication
Other IIA Resources
IIA Audit Tool "Enterprise and Business Process Risks: User Guide and Workbook"
IIA Position Paper *The IIA's Three Lines Model: An Update of the Three Lines of Defense*
Internal Audit Foundation *Global Risk in Focus 2025: Hot Topics for Internal Auditors*

Appendix B. Glossary

Definitions are taken from the "Glossary" within The IIA's publication, Global Internal Audit Standards, 2024 Edition, unless otherwise noted.

activity under review – The subject of an internal audit engagement. Examples include an area, entity, operation, function, process, or system.

advisory services – Services through which internal auditors provide advice to an organization's stakeholders without providing assurance or taking on management responsibilities. The nature and scope of advisory services are subject to agreement with relevant stakeholders. Examples include advising on the design and implementation of new policies, processes, systems, and products; providing forensic services; providing training; and facilitating discussions about risks and controls. "Advisory services" are also known as "consulting services."

assurance – Statement intended to increase the level of stakeholders' confidence about an organization's governance, risk management, and control processes over an issue, condition, subject matter, or activity under review when compared to established criteria.

assurance services – Services through which internal auditors perform objective assessments to provide assurance. Examples of assurance services include compliance, financial, operational or performance, and technology engagements. Internal auditors may provide limited or reasonable assurance, depending on the nature, timing, and extent of procedures performed.

board – Highest-level body charged with governance, such as:

- A board of directors.
- An audit committee.
- A board of governors or trustees.
- A group of elected officials or political appointees.
- Another body that has authority over the relevant governance functions.

In an organization that has more than one governing body, "board" refers to the body or bodies authorized to provide the internal audit function with the appropriate authority, role, and responsibilities.

If none of the above exists, "board" should be read as referring to the group or person that acts as the organization's highest-level governing body. Examples include the head of the organization and senior management.

chief audit executive — The leadership role responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services in accordance with Global Internal Audit Standards. The specific job title and/or responsibilities may vary across organizations.

compliance – Adherence to laws, regulations, contracts, policies, procedures, and other requirements.

control – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved.

control processes – The policies, procedures, and activities designed and operated to manage risks to be within the level of an organization's risk tolerance.

criteria – In an engagement, specifications of the desired state of the activity under review (also called "evaluation criteria").

engagement – A specific internal audit assignment or project that includes multiple tasks or activities designed to accomplish a specific set of related objectives.

engagement conclusion — 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.

engagement objectives – Statements that articulate the purpose of an engagement and describe the specific goals to be achieved.

engagement planning – Process during which internal auditors gather information, assess and prioritize risks relevant to the activity under review, establish engagement objectives and scope, identify evaluation criteria, and create a work program for an engagement.

engagement results – The findings and conclusion of an engagement. Engagement results may also include recommendations and/or action plans.

engagement work program – A document that identifies the tasks to be performed to achieve the engagement objectives, the methodology and tools necessary, and the internal auditors assigned to perform the tasks. The work program is based on information obtained during engagement planning.

finding – In an engagement, the determination that a gap exists between the evaluation criteria and the condition of the activity under review. Other terms, such as "observations," may be used.

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.

impact – The result or effect of an event. The event may have a positive or negative effect on the organization's strategy or business objectives.

inherent risk – The combination of internal and external risk factors that exists in the absence of any management actions.

internal audit charter – A formal document that includes the internal audit function's mandate, organizational position, reporting relationships, scope of work, types of services, and other specifications.

internal audit function - A professional individual or group responsible for providing an organization with assurance and advisory services.

internal audit plan – A document, developed by the chief audit executive, that identifies the engagements and other internal audit services anticipated to be provided during a given period. The plan should be risk-based and dynamic, reflecting timely adjustments in response to changes affecting the organization.

likelihood – The probability that a given event will occur.

objectivity – An unbiased mental attitude that allows internal auditors to make professional judgments, fulfill their responsibilities, and achieve the Purpose of Internal Auditing without compromise.

outsourcing – Contracting with an independent external provider of internal audit services. Fully outsourcing a function refers to contracting the entire internal audit function, and partially outsourcing (also called "cosourcing") indicates that only a portion of the services are outsourced.

risk – The positive or negative effect of uncertainty on objectives.

risk and control matrix – A tool that facilitates the performance of internal auditing. It typically links business objectives, risks, control processes, and key information to support the internal audit process.

risk appetite – The types and amount of risk that an organization is willing to accept in the pursuit of its strategies and objectives.

risk assessment – The identification and analysis of risks relevant to the achievement of an organization's objectives. The significance of risks is typically assessed in terms of impact and likelihood.

risk management – A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

root cause – Core issue or underlying reason for the difference between the criteria and the condition of an activity under review.

senior management – The highest level of executive management of an organization that is ultimately accountable to the board for executing the organization's strategic decisions, typically a group of persons that includes the chief executive officer or head of the organization.

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, relevance, and impact. Professional judgment assists internal auditors when evaluating the significance of matters within the context of the relevant objectives.

stakeholder – A party with a direct or indirect interest in an organization's activities and outcomes. Stakeholders may include the board, management, employees, customers, vendors, shareholders, regulatory agencies, financial institutions, external auditors, the public, and others.

workpapers – Documentation of the internal audit work done when planning and performing engagements. The documentation provides supporting information for engagement findings and conclusions.

Appendix C. References and Additional Reading

References

Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management—Integrating with Strategy and Performance*. 2017.

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

ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. ISACA, 2018. https://www.isaca.org/resources/cobit.

ISO and IEC. *ISO/IEC 38500: 2024 — Information Technology: Governance of IT for the Organization*. ISO, 2024. https://www.iso.org/standard/81684.html.

National Institute of Standards and Technology (NIST), Joint Task Force. *NIST Special Publication 800-37, Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. NIST, 2018. https://doi.org/10.6028/NIST.SP.800-37r2.

Additional Reading

Axelos. *IT Infrastructure Library (ITIL) 4* practice guides. Axelos, 2019. https://www.axelos.com/resource-hub/practice/readers-manual-itil-4-practice-guide.

Center for Internet Security (CIS). *CIS Critical Security Controls Version 8.1*. Center for Internet Security, 2024. https://www.cisecurity.org/controls/v8-1.

Committee on the Financial Aspects of Corporate Governance. *The Financial Aspects of Corporate Governance*. Gee Publishing, 1992. https://www.ecgi.global/sites/default/files/codes/documents/cadbury.pdf.

Institute of Directors South Africa. *King IV Report on Corporate Governance for South Africa 2016*. IoDSA, 2016. https://www.iodsa.co.za/page/king-iv.

Institute of IT Governance. *Place of IT Governance in the Enterprise Governance: Balancing Performance and Conformance*. CIGREF and AFAI, 2006. https://cigref.typepad.fr/itgifrance/files/place_IT_governance_in_enterprise_governance.pdf.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy

Protection: Information Security Management Systems — Requirements. ISO, 2022. https://www.iso.org/standard/27001.

Organisation for Economic Co-operation and Development (OECD). *G20/OECD Principles of Corporate Governance*. OECD Publishing, 2023. https://doi.org/10.1787/ed750b30-en.

Appendix D. Mapping to Frameworks

IT governance and IT management subcategories can be mapped to these framework resources.

IT Governance Area	Framework Reference
Strategic Alignment	COBIT 2019: EDM 01
Risk Oversight	COBIT 2019: EDM 03
Enabling Value Delivery	COBIT 2019: EDM 02
Performance Oversight	COBIT 2019: EDM 05
Resource Oversight	COBIT 2019: EDM 02
IT Management Area	**Framework Reference**
Operational Management	COBIT 2019 APO 01, APO 02, DSS 01
Risk Management	COBIT 2019 COSO's Enterprise Risk Management NIST SP88-37 Rev. 2
Control Processes	COBIT 2019 MEA 02, MEA03, APO 12, DSS 06
Performance Measurement and Monitoring	COBIT 2019 MEA 01
Resource Management	COBIT 2019 APO 05, APO 06, BAI 01, BAI 09, BAI 11

About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 265,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer

Copyright

August 2025 (This version supersedes “Auditing IT Governance,” published in 2018.)

The Institute of
Internal Auditors

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