Sadržaj

Executive Summary

Assessing organizational governance in the public sector requires a firm understanding of the characteristics, structure, and accountability processes prevalent in international, national, regional, and local governments. At the same time, governance structures and processes must be customized according to the organization's complexity and political, cultural, economic, and regulatory environments. Regardless of the nature of the organization, a principles-based approach to assessing organizational governance will help auditors provide assurance that the public is being well-served.

Responsibilities for governance are shared among the board, senior management, and the audit function. The board bears primary responsibility for organizational governance and often delegates implementation responsibilities to senior management. The chief executive also sets the tone at the top, establishing a foundation for good governance. Audit functions provide public sector organizations with assurance and advisory services by monitoring and reporting on the effectiveness of governance processes.

Auditors should prepare for the assessment process by developing a deep understanding of the organization's governance context, including identifying key stakeholders and their governance requirements. After the context has been defined, major steps in the assessment process include gathering documents, reviewing processes and structures, establishing an assessment criteria and maturity model, developing an audit plan, and finally, planning and completing engagements.

Performing the assessment will require auditors to gather evidence from and consider processes and structures related to:

- The board and audit committee.
- Strategy.
- Enterprise risk management.
- Ethics.
- Compliance.
- Organizational accountability.
- Monitoring.
- IT governance.

Public sector governance audits are often high-profile, sensitive in nature, and a matter of public record. Adequate staffing, appropriate supervision, and quality assurance are critical throughout the process.

Introduction

In 2012, The IIA released Assessing Organizational Governance in the Private Sector, a practice guide designed to provide chief audit executives (CAEs) in the private sector with direction on how to assess and make recommendations for improving governance. This public sector-focused practice guide:

- Adapts Assessing Organizational Governance in the Private Sector to suit the unique needs of the public sector.
- Is designed to help public sector boards, audit committees, CAEs, and audit staffs assess governance.
- Is intended to be fully applicable to government and all publicly controlled or publicly funded agencies, enterprises, and other entities that deliver public programs, goods, or services.

The public sector organization's board is responsible for governance oversight. The CEO is responsible for non-board governance processes. An effective audit function that is independent, objective, and proficient; uses sound assurance processes and practices; and conforms to the *International Standards for the Professional Practice of Internal Auditing* (*Standards*), is qualified to assess governance and provide assurance on governance effectiveness to the board.

A Principles-based Approach

Public sector governance should be customized to align with the organization's complexity and geographic, political, cultural, economic, and regulatory environments. To address a wide spectrum of needs, this practice guide provides guidance that focuses on universal good principles of governance.

> *"Because governments throughout the world are structured differently – with different and possibly overlapping mandates and jurisdictions – no single governance model applies to public sector organizations. Nevertheless, certain governance principles are common across the public sector. Common principles of corporate governance encompass the policies, processes, and structures used by an organization to direct and control its activities, to achieve its objectives, and to protect the interests of its diverse stakeholder groups in an ethical manner."*[1]

Taking a principles-based approach, audit functions can assess governance across different systems of government including international governments, national and state governments, government agencies, state-owned enterprises, and municipalities. Boards, audit committees, CAEs, and audit staffs may need to supplement this guidance with additional, in-depth or rules-based guidance in specific areas applicable to their organizations and jurisdictions.

Business Significance and Related Risks

Governance is the processes and structures implemented by the board to inform, direct, manage, and monitor the organization's activities toward achieving its objectives. Strong governance systems increase the likelihood that organizations will meet their objectives and stakeholder expectations. The organization faces risks to achieving effective governance, and the board is responsible for implementing governance processes and structures. While the board remains accountable for governance, it may delegate certain governance responsibilities to management. Board-level governance risks are outlined in the Appendix.

Related IIA Standards and Guidance

The International Professional Practices Framework (IPPF) outlines the following *Standards* pertaining to governance.

Standard 2110: Governance

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

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

2110-A1

The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.

2110-A2

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

Related IPPF practice advisories and practice guides providing additional guidance on governance include:

Practice Advisories

- PA 2110-1: Governance: Definition
- PA 2110-2: Governance: Relationship With Risk and Control
- PA 2110-3: Governance Assessments

[1] Supplemental Guidance: The Role of Auditing in Public Sector Governance, The IIA, 2012.

Practice Guides

- Auditing Executive Compensation and Benefits
- Assessing Organizational Governance in the Private Sector
- Evaluating Corporate Social Responsibility/Sustainable Development
- Evaluating Ethics-related Programs and Activities
- *Global Technology Audit Guide (GTAG)4: Management of IT Auditing, 2nd Edition*
- *GTAG 15: Information Security Governance*
- *GTAG 17: Auditing IT Governance*

Standard 2120: Risk Management

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

Related IPPF practice advisories, practice guides, and a position paper providing additional guidance on risk management include:

Practice Advisories

- PA 2120-1: Assessing the Adequacy of Risk Management Processes
- PA 2120-2: Managing the Risk of the Internal Audit Activity

Practice Guides

- Internal Auditing and Fraud
- *GTAG 10: Business Continuity Management*
- *GTAG 13: Fraud Prevention and Detection in an Automated World*

Position Paper

- The Role of Internal Auditing in Enterprise-wide Risk Management

Standard 2130: Control

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

Related IPPF practice advisories and practice guides providing additional guidance on control include:

Practice Advisories

- PA 2130-1: Assessing the Adequacy of Control Processes
- PA 2130.A1-1: Information Reliability and Integrity
- PA 2130.A1-2: Evaluating an Organization's Privacy Framework

Practice Guides

- *GTAG 1: Information Technology Risks and Controls, 2nd Edition*
- *GTAG 2: Change and Patch Management Controls: Critical for Organizational Success, 2nd Edition*
- *GTAG 8: Auditing Application Controls*
- *GTAG 9: Identity and Access Management*
- *GTAG 12: Auditing IT Projects*
- *GTAG 14: Auditing User-developed Applications*
- The Guide to the Assessment of IT Risk (GAIT) Methodology
- GAIT for IT General Control Deficiency Assessment
- Auditing External Business Relationships
- Auditing Privacy Risks, 2nd Edition

Other IIA Guidance

- Supplemental Guidance: Public Sector Definition
- Standard 1300: Quality Assurance and Improvement Program
- Standard 1312: External Assessments
- Standard 2400: Communicating Results
- Practice Advisory 2400-1: Legal Considerations in Communicating Results

Definitions of Key Concepts

This practice guide uses the following definitions for governance and governance-related terms:

Control — Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives will be achieved (*Standards*).

Governance involves the set of relationships among the organization's stakeholders, interest groups, citizens, board, and management. These relationships are framed by laws, rules, and requirements, and provide the structure through which the objectives of the organization are set, the strategies to achieve those objectives are defined, operating plans are prepared, performance is monitored, and information is communicated transparently among the parties.[2]

Public Sector — In general terms, the public sector consists of governments and all publicly controlled or publicly funded agencies, enterprises, and other entities that deliver public programs, goods, or services. Public sector governance includes two domains: public governance and organizational governance.

Public governance refers to preconditions to run (govern) a jurisdiction — processes and structures necessary to ensure that the government can stay in power until the end of its mandate, implement public policies, have smooth relationships with legislative and judiciary powers, and pass on administration to the next government.

Organizational governance is derived from the corporate governance experience and deals with the specific organizations that comprise the public sector. Organizational governance addresses how organizations should be structured to mitigate or eliminate conflicts of interest between their personnel and the citizens that the organizations represent.

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 (*Standards*).

Public Sector Characteristics

Public and private sector organizations differ considerably with regard to governance. Generally, public sector governance is more rigid and under greater regulatory burden. Table 1 outlines the major differences.

Table 1: Public vs. Private Sector Organizational Characteristics

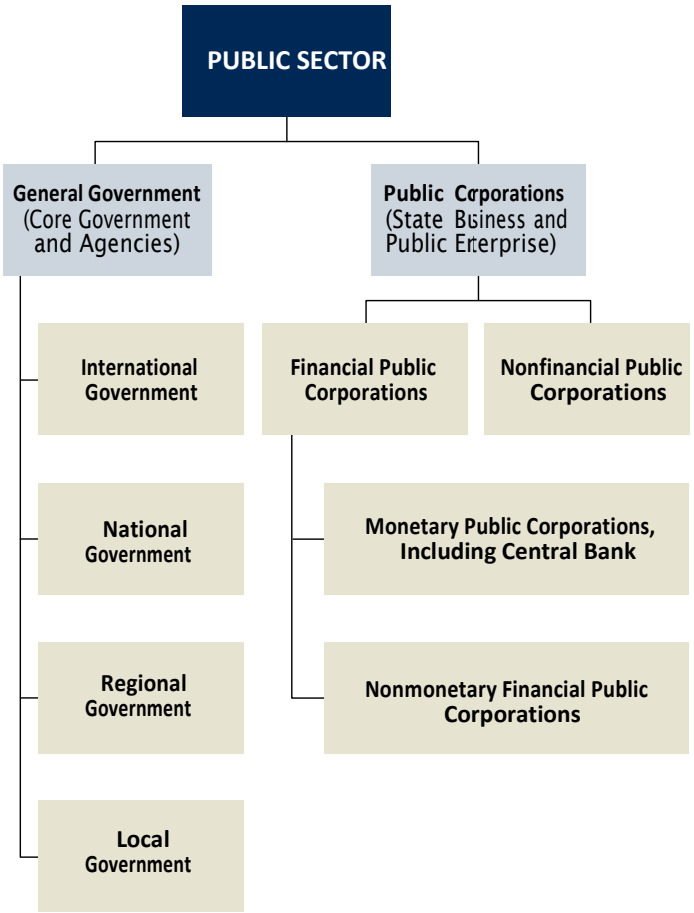
ORGANIZATIONAL CHARACTERISTIC	PUBLIC SECTOR	PRIVATE SECTOR
Main Organizational Purpose	Protect/Serve Public Interest	Maximize Shareholder Value
Creation	Law	Incorporation Acts
Governance Structure	Governing Board/Audit Committee/Senior Official	Shareholders/Board of Directors/Audit Committee
Finance	Taxes/Revenues	Ownership/Debt/Revenues
Operational Rules	Formal/Rigid/Law	Formal/Flexible/Informal
Accountability	Citizenry/Legislature	Shareholders/Stakeholders/Regulators
Outside Communication	Open/Public	Present/Potential Shareholders, Stakeholders, and Regulators
Control Systems	Rigid	Flexible

[2] For a more detailed discussion of governance context in the public sector, see The IIA's The Role of Auditing in Public Sector Governance and the International Federation of Accountants' (IFAC's) *Governance in the Public Sector: A Governing Body Perspective.*

Public Sector Structure

The public sector structure includes the general government (core government and agencies), and public corporations (state businesses and enterprises). This practice guide is intended to be fully applicable to general government public sector entities. Public corporations' objectives and conformations lie somewhere between the public and private sectors. Therefore, auditors in public corporations should refer to this practice guide in conjunction with the practice guide, Assessing Organizational Governance in the Private Sector, to potentially develop a hybrid approach for assessing governance. Figure 1 depicts a representative public sector structure.

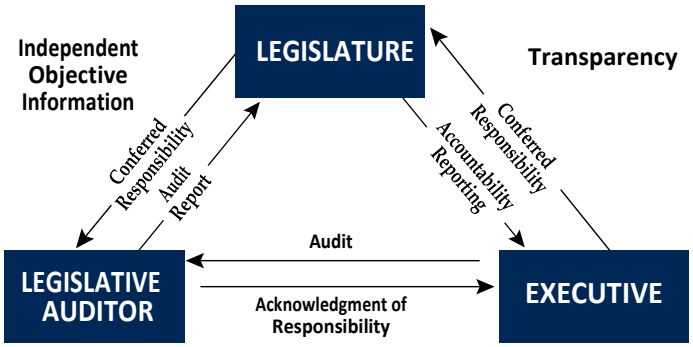
Figure 1– Public Sector Structure



Public Sector Accountability

Assessing governance structure and practices requires an understanding of public sector accountability. Public sector accountability is summarized in Figure 2.

Figure 2– Example of Overall Accountability Process in the Public Sector[3]



In democratic governments, the executive function is responsible for planning, directing, and controlling daily operations, while the legislature is responsible for authorizing the executive budget and government expenditures. The legislative auditor audits and reports on the performance of the executive branch.

In many national governments, legislative auditors are established as supreme audit institutions (i.e., independent government external auditors). In regional and local governments, auditors may play a dual role — helping to improve the government (i.e., an audit function role), and providing the legislature with timely and relevant reports for control purposes (i.e., an external assurance provider role).

In this particular accountability environment, it is important that public sector auditors recognize the importance of effective communication channels with legislative external assurance providers. Management-approved communication between audit function and external assurance providers helps to ensure public accountability. The audit committee is one of the main mechanisms to help facilitate this communication.

[3] Office of the Auditor General of Canada training material. Reproduced with the permission of the Minister of Public Works and Government Services, 2014.

The Public Sector Governance Roles and Responsibilities

The Board

The board is the focal point for effective organizational governance. It is the link between the stakeholders and the organization's executive management, and it bears primary responsibility for governance. The board:

- Sets the organization's strategic objectives and provides the leadership to put them into effect.
- Directs and provides oversight of the executive leader and senior management.
- Establishes appropriate risk levels.
- Approves and monitors entitywide ethics, operational, and compliance standards and policies.
- Institutes effective control systems.
- Provides transparent, complete, clear, and timely communication to stakeholders.

The board's actions are subject to laws, regulations, and the needs of stakeholders. The board typically delegates significant authority for the day-to-day operations to an executive leader (CEO) and the executive leadership team. To be effective, the board should be independent, engaged, and committed.

Management

The organization's executive leadership and senior management are accountable to the board. Top management is ultimately responsible for implementing the organization's governance system, as directed by the board. The CEO sets the tone at the top for the integrity, ethics, and conduct that will contribute to an effective governance environment. This tone is imparted to the executive leadership team, which in turn cascades organizationwide. The CEO and executive management should "walk the walk" to ensure that a positive governance culture exists throughout the enterprise. In addition, executive leadership and senior management should ensure that governance policies, procedures, and programs exist and are followed, and that there is compliance with applicable laws, regulations, and codes.

Audit Function

Public sector audit functions can provide their organizations with governance assurance and advisory services. The audit function charter should state that the audit function's scope includes all governance activities and processes. However, this does not mean that auditors are required to perform audits of all governance activities and processes. The audit function should be positioned appropriately within the organization and staffed with proficient professionals.

The audit function can play numerous roles in assessing and contributing to the improvement of organizational governance. For example, auditors can:

- Provide advice on ways to improve the organization's governance practices if they are not mature.
- Contribute to the organization's governance structure through internal audits, even if those audits are not focused specifically on governance.
- Act as facilitators, assisting the board in governance self-assessments.
- Observe and either informally or formally assess governance, risk, and control structural design and operational effectiveness, while not being directly responsible for them.

The appropriate role for the audit function and the resource commitment to each of these roles depends largely on the maturity of the governance system and the organization's size and complexity. The CAE should discuss and reach an agreement with the board on the audit function's role in assessing organizational governance.

The focus of the remainder of this practice guide is on providing formal assessments of organizational governance. Recognizing that there could be sensitivities to assessing and reporting on some board- and executive-level governance activities, board-level support and, if needed, sponsorship for assessments should be obtained as part of the periodic audit planning process.

Considerations by Specific Governance Process or Structure

Board and Audit Committee

The board should be satisfied that there is an effective governance system in place. To that end, it should ensure that it is fulfilling all of its governance responsibilities, the right governance processes are in place within the organization and operating effectively, and transparent communication exists between the organization and its stakeholders. The board should discuss the state of the organization's governance system and seek input from the three levels of assurance providers: operating or line management, organizationwide functions, and independent activities such as the audit function. The board should sponsor periodic evaluations and continuous improvement of governance practices. This can be done through self-assessments and obtaining assistance from the audit function or external assurance providers. A highly competent and well-positioned audit function can assist with a board's self-assessment and can provide reliable assurance on the organization's internal governance practices.

The exact role of the board is determined by the powers, duties, and responsibilities delegated to it or conferred upon it by applicable law and is typically specified in the organization's articles, bylaws, charters, rules, or other similar documents. Usually, the organization's legal documents specify the number of members of the board, how they are to be chosen, the frequency and mode of meeting, and how decisions are to be made. The bylaws primarily contain what is prescribed in legislation. Moreover, the organization's legal documents specify the roles and responsibilities of the board, senior management, and other organizational bodies and functions.

The audit committee is an important governance tool to help the board discharge its responsibility for establishing and monitoring an adequate governance system within the organization. Audit committees can be seen as complementary vehicles that can improve communication and coordination between top management — including the governing board — and the audit function, which is primarily responsible for assessing the organization's internal control, risk management, and governance structures.

The main desirable characteristics of an effective audit committee are the independence and competence of its members. These features empower audit committee members to seek explanations and information about crucial issues related to accountability and operational and financial performance. The audit committee can help ensure that accepted internal audit recommendations are followed up and taken into serious consideration by senior management.

Leading practice guides for audit committees usually address these areas: mandate, composition, independence, members' capability requirements, and reporting. Some of these best practices include:

- An oversight mandate should be set out in a written charter. At a minimum, the audit committee oversight mandate should encompass areas such as values and ethics, governance arrangements, risk management, management control framework, audit activities and other external assurance providers, financial statements, and public accountability reporting.
- The composition of public sector audit committees varies, but a minimum requirement of three members is considered a general rule.

- Independence requirements are usually considered to be met when most of an audit committee's members come from outside the government.
- Capability requirements include, among other things, inquisitiveness, outspokenness, courage, sound judgment, objectivity and integrity, a healthy constructive skepticism, a high level of ethics, and strong communications skills. Financial, control framework, governance, and management expertise also are highly desirable, if not necessary.

In assessing audit committee performance, government auditors should focus on a three-pillar framework:

- Assessing compliance with charter obligations. Does the audit committee discharge its responsibilities as stated in the charter?
- Assessing the participation of audit committee members. Is there a formal and effective assessment of each member's performance and contribution to the audit committee?
- Assessing value-added activities pursued and outcomes achieved. Does the audit committee add value to the organization by facilitating well-informed and effective decision-making, promoting and monitoring an ethical culture, implementing an effective system of risk oversight and management, implementing an effective and efficient internal control system, promoting effective communication with internal and external auditors and responding appropriately to matters they raise, and promoting high-quality internal and external reporting of financial and nonfinancial information?

Strategy

Strategic planning is an organization's process for defining strategies for achieving its objectives, as well as making decisions on allocating resources to pursue its strategies. Simply put, strategic planning outlines where an organization is going over the next few years and how the entity proposes to get there.

Strategies can exist at different levels of an organization. They start at the overall organizational level and cascade down.

Organizational Strategy — The highest level strategy, organizational strategy is concerned with the overall purpose and scope of the organization to meet stakeholder expectations. This is the most critical level because it is heavily influenced by stakeholder budgetary allocation and acts to guide strategic decision-making throughout the organization.

Subsidiary Strategies — Strategies that are concerned with how the organization will successfully operate in particular areas. Subsidiary strategies involve decisions about choice of services to be delivered, meeting community needs, influencing political agendas, and exploiting or creating new opportunities.

Operational Strategies — At the operating level, strategies are focused on how each activity or function will deliver organizational and subsidiary strategies. Compared to organizational and subsidiary strategies, operational strategies are much more detailed and focused on resources, processes, people, etc. All material discrete activities and functions should have operational strategies.

What are some conditions of satisfaction that can be used to evaluate strategies? Strategies should:

- Be developed through a disciplined process and supported by the best available information.
- Be commonly understood by organizational personnel.
- Serve as a platform for all major decisions.
- Enhance stakeholder value.
- Align with other strategies, both top-down and across the organization.
- Be clearly reflected in objectives, structures, and operations at all levels.

- Enable alignment of measurement and rewards.
- Eliminate redundancies.
- Be documented.
- Manage/maintain risks within risk tolerance limits.
- Allow risk expectations to be well understood by stakeholders such as regulators, interest groups, citizens, rating agencies, and capital markets.

In performing an assurance engagement, the audit function should assess whether each of the above conditions are present. The assessment is generally not intended to directly question the strategies themselves, but rather, to assess the strategic-planning process and how well the strategies have been communicated and adopted throughout the organization.

Enterprise Risk Management (ERM)

Generally, the board will delegate the operation of the risk management process to the organization's executive leadership team. Structures may vary depending on the size, complexity, and maturity of the organization, and its commitment to risk management. For example, in a small organization with risk-conscious managers and a high degree of communication about risks, there may be no need for a formal structure. In a large organization, the structure may consist of a single individual with a staff that owns the identification, assessment, and monitoring processes and coordinates, along with top and middle management, risk management activities. Some organizations have assigned specific risk management activities to the audit function. The IIA position paper, The Role of Internal Auditing in Enterprise-wide Risk Management, provides guidance on permitted roles, roles that may be appropriate with safeguards, and prohibited roles. Of great importance is ownership of risks. Regardless of the roles an audit function may play, it should not own any risks other than risk within the audit activity.

There are several risk management frameworks or standards to choose from in establishing the criteria upon which to base the assessment. Two of the most widely used are ISO 31000, Risk Management–Principles and Guidelines and COSO's Enterprise Risk Management–Integrated Framework.

For guidance on assessing risk management, see The IIA practice guide, Assessing the Adequacy of Risk Management Using ISO 31000.[4] That practice guide presents three potential approaches:

- **Process elements —** Are all the elements of a sound risk management process in place?
- **Key principles —** Does the risk management process satisfy a minimum set of principles?
- **Maturity model —** How mature are the elements of the risk management process? The practice guide includes a basic risk maturity model.

The auditor should look at the qualitative aspects of risk management and formal processes. For example, the quality of the risk policy or risk universe is as important as having one in place.

Ethics

Senior management members have primary responsibility for promoting strong ethics. The tone at the top, as indicated by their actions, as well as by their formal and informal communications, is critical. These actions include their own behavior and how they respond when key employees such as other executives or "the best salesman," behave unethically. Operating managers set the tone in their own areas, which may or may not be consistent with that of the organization as a whole.

Ethical standards in areas such as gift giving differ culturally. Global organizations should decide whether and how much to adapt their global standards to the local culture, while being fully cognizant of all applicable laws and regulations, and make this clear to all concerned.

[4] See "Additional Resources" for a link to this guidance.

The audit function should promote ethical behavior and may function in roles such as chief ethics officer, compliance officer, or member of an ethics council, as long as such a role does not compromise the audit function's independence. For more guidance on this matter, refer to the IIA position paper: The Three Lines of Defense in Effective Risk Management and Control.

Standard 2110.A1 states: "The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities." Evaluating the design might require developing and agreeing with management on criteria, perhaps by research and benchmarking similar programs. Evaluating the implementation will be similar to doing so for other activities. Evaluating whether the programs are having the desired effect requires an evaluation of the ethical climate itself.

Evaluating the ethical climate is sensitive and can be highly subjective. To succeed, auditors should:

- Get sponsorship and agreement on the evaluation methods from the board and senior management. To the extent possible, get buy-in from those who might be subject to criticism as a result of the review.
- Consider using a maturity model for the evaluation, because no ethical climate is completely good or bad.
- Consider using self-assessment methods such as surveys or workshops, in which employees evaluate the climate they work within and the ethical behavior of management and other employees. Whenever possible, validate the results of these methods with more tangible evidence. If they cannot be validated, make this clear in reporting, and work with management to determine the reasons for employees' perceptions of the climate.

Like other governance activities, ethics can be assessed as part of a comprehensive review of governance, as a standalone project that contributes to the overall governance assessment, or integrated into audits that focus more directly on business operations or support activities.

Compliance

Compliance and ethics are closely related and are sometimes evaluated together. The preceding section on ethics applies to compliance as well. This section presents additional considerations.

The term "compliance," particularly when referring to a compliance function, normally refers to compliance with laws and regulations, rather than compliance with internal policies and procedures. Audit functions should consider the need for technical assistance — for example, from the organization's legal department or an outside third party — when evaluating legal and regulatory compliance.

The compliance function, if one exists, might be the subject of an audit. However, the scope should go beyond the activities of the function itself. The effectiveness of the function is determined by the awareness of, and commitment to, compliance by employees whose work could be noncompliant. If the CAE is responsible for the compliance function, this audit should be strongly considered as a candidate for outsourcing to an external assurance provider.

If there is no designated compliance function, auditors should determine and assess the methods by which the organization fosters compliance knowledge and commitment in its employees.

Organizational Accountability

The organization's board and management derive their authority from its key stakeholders. Accountability is imperative to make executive management and staff answerable for their behavior and responsive to the organization's key stakeholders. This may be achieved differently in different countries or political structures, depending on the history, cultural milieu, and value systems involved.

The mechanisms used may vary from audit covenants at one level to broadly elected legislatures or more narrowly conceived consultative committees at another.

Accountability also means establishing criteria to measure the performance of the board and management, and oversight mechanisms to ensure that the standards are met. The litmus test is the process by which the stakeholders can act to address inappropriate actions and reward exemplary performance. This can be a sensitive area for internal audit to review and underscores the importance of the appropriate level of support and sponsorship.

When assessing accountability, the audit function should consider:

- The organization's legal or legislative appointment, legal structures, and applicable laws and regulations.
- Formal and comprehensive "delegated authorities" and "powers reserved."
- Documented acknowledgement of their accountabilities by key personnel.
- Processes to monitor accountabilities and corrective actions taken when accountabilities are not met.

Monitoring

There are several different monitoring and measurement systems in use today. Regardless of the nature, size, type, form, or specialization, organizations tend to be interested in the same general aspects of performance: financial, client, internal services operations, societal, special interest groups, employee, leadership, and stakeholder satisfaction.

By definition, the purpose of monitoring is to provide the board and management with early indications of progress being made, or not made, in achieving the organization's objectives. Monitoring enables and assists the board and management in making timely decisions. Also, monitoring provides a means for holding people accountable and enables the organization to continually improve performance.

Monitoring should be based on an analysis and prioritization of risks to achieving organizational objectives and the means by which those risks are mitigated. Monitoring efforts over process-level risks should include considerations for:

- Relevance.
- Reliability.
- Adaptability to address new or changing risks.
- Accuracy.
- Objectivity.
- Completeness.
- Cost-effectiveness.
- Timeliness.
- Usefulness.
- Communication and reporting content.

IT Governance

According to the *Standards*, IT governance consists of leadership, organizational structures, and processes that ensure that the enterprise's IT supports the organization's strategies and objectives.

IT governance is an extension of organizational governance. As with all governance, there is no one-size-fits-all solution. Effective IT governance should be a cohesive and integrated process aligned with the business, compatible with the management decision-making style and culture, and perceived by business management to be providing value. The board has oversight responsibility for IT governance. The CAE should ensure that IT governance is included in the annual program of audits.

Several widely recognized IT governance frameworks may be used in establishing the criteria for assessing IT governance. These include:

- ISO 38500, Corporate Governance of Information

Technology. This international standard is applicable to all types and sizes of organizations. It is built around six principles: responsibility, strategy, acquisition, performance, conformance, and human behavior.

- COBIT 5. The fifth edition focuses on governance activities that operate at the board and executive level. It is organized in three domains aligned with ISO 38500: evaluate, direct, and monitor.
- GTAGs are IPPF practice guides that provide detailed guidance for conducting audit activities.[5] Written in clear and concise business language, GTAGs provide guidance for the more detailed parts of an IT governance review.
- IT Infrastructure Library (ITIL) is a worldwide de facto standard for service management and contains broad, publicly available professional documentation on how to plan, deliver, and support IT service features. Some of the core publications are: Service Strategy, Service Design, Service Transition, and Service Operation.

Assessing Organizational Governance

The starting point for audit function's assessment is to gain an understanding of the organizational context for governance. Efforts to understand the context include identifying the key stakeholders and their requirements, and determining how the organization defines governance. The CAE should work with the board, the audit committee, and the executive management team, as appropriate, to determine how governance should be defined for audit purposes. After the context has been defined, major steps or phases of the Organizational Governance Assessment Process outlined in Figure 3 should be followed.

Gather Governance Documents

Governance should be tailored to comply with mandatory requirements and best fit the organization's risk profile. Records that document governance requirements and the organization's processes and structures to meet those requirements include:

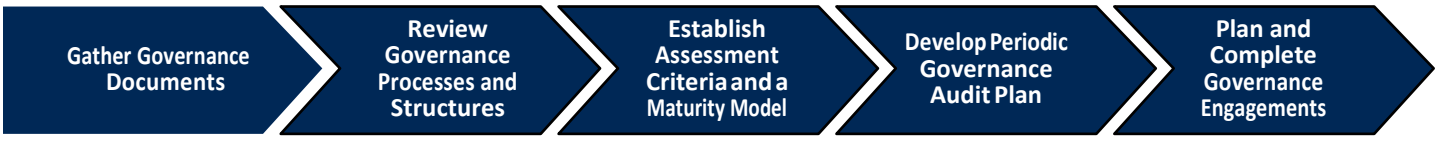
- Laws and regulations — These tend to establish minimum governance requirements.
- Organizational policies, procedures, bylaws, and operating agreements.
- Governance codes or preferred practices promulgated by an influential body related to the governance of the organization. These codes can be mandatory, strongly recommended, or optional.

Other resources useful in identifying governance processes and structures include any documented evidence of customs, behaviors, and stakeholder expectations that exist in the organization's operating environment. If governance documentation is inadequate, the board should be notified and given an initial opportunity to strengthen governance.

Review Governance Processes and Structures

Governance processes and structures should be reviewed as part of the assessment process and on a regular basis. Auditors should keep in mind that there is no one-size-fits-all governance framework or model. By design, the organization's governance processes and structures should respond to the requirements identified in the preceding section.

Figure 3 – Organizational Governance Assessment Process



[5] See "Additional Resources" for a link to this guidance.

Governance processes and structures may come under the purview of the board or management, depending on the nuances of the organization, the particular process or structure, and the level of the process or structure. The following generic, yet comprehensive, list of governance processes and structures can help audit functions ensure that they include all relevant activities in their governance review. Governance processes and structures listed are grouped at the board level and within the organizational (non-board) level, and include both quantitative (e.g., compliance metrics), and qualitative (e.g., tone-at-top) measures. Together, board and organizational processes and structures form a governance umbrella over the organization's operations.

Board-level Governance Processes and Structures

- Board and committee structure, charters, roles and responsibilities, processes, and reporting.
- Board and committee activities — calendars, meeting agendas, meeting papers, minutes and reports of meetings, follow-up actions, and self-assessments of board and committees' governance practices.
- Board and committee composition, including selection, induction, ongoing education and training, remuneration, and protection of members.
- Board and committee oversight areas, including objective-setting, strategies, structures, operating plans, budgets and capital allocation, CEO, ERM, ethics and integrity, delegated authorities, performance measurement and results, compensation and rewards, policies and procedures, compliance, decision-making, stakeholder communication such as financial reporting and disclosures, reputation, unpredictable events, and other organizational governance practices.
- Assurance practices, including external, financial, regulatory, and the audit function.
- Additional practices generally retained by the board, which may include:
  - › Selecting, monitoring, evaluating, compensating, and retaining the CEO and other key members of senior management.[6]
  - › Providing strategic guidance to the CEO and senior management.
  - › Reviewing and approving objectives and important organizational plans and actions.
  - › Making decisions on major transactions (transformational transactions) before submission to stakeholders for approval.[7]
  - › Reviewing and approving major changes in accounting and audit principles and practices.[8]
  - › Declaring dividends and approving share-repurchase programs.[9]
  - › Resolving cross-organizational issues.

Organization-level Governance Processes and Structures

- Setting objectives.
- Developing strategies, operating plans and budgets, organizational structures, and management committees.
- Assigning authority and responsibilities organization-wide.
- Defining behaviors, codes of ethics, and conduct, including conflict of interest, fair dealing, protection and appropriate use of assets, insider dealings, violation reporting (hot lines), and disciplinary actions.
- ERM to include internal control, fraud risk management, and IT governance.
- Compliance with laws, regulations, and mandatory and optional codes, where adopted.
- Monitoring and performance measurement.

[6] In some jurisdictions, compensation and retention of public sector top management is not at the discretion of the board.
[7] This type of process approval is more familiar to state-owned enterprises.
[8] This is one of the main audit committee attributes.
[9] Only applicable to state-owned enterprises.

- Ensuring effectiveness of assurance providers within the organization, particularly operational management that serves as the first line of defense for a sound system of internal controls and enterprisewide activities, such as risk management and compliance, which serve as a second line of defense.
- Communication up, down, and across the organization.
- Processes that ensure effective communication with stakeholders, interest groups, and citizens.
- Capital acquisition and allocation.[10]
- Capabilities — people selection, development, and retention.
- Transformational transactions.
- Cross-organization issues.
- Organizational responsibility and sustainability.
- Evaluation and rewards, and salary and incentive compensation.
- Organizational processes for assessing the performance and independence of external assurance providers, including the nature and extent of nonaudit services obtained.[11]

The audit function itself is a key governance tool. Its effectiveness in providing assurance to stakeholders is critical to effective governance. The board and the audit committee should look to the CAE for periodic reports on the internal audit activity's quality assurance and improvement program and ensure that the program provides for an independent assessment at least every five years, as mandated by Standard 1312: External Assessments. The CAE should ensure that the reports of independent assessors are provided to the board. In addition, the board should draw its own conclusions on the effectiveness of the audit function.

Establish Assessment Criteria and a Governance Maturity Model

Governance maturity models may be used to identify, define, and evaluate assessment criteria gleaned from the review of governance records, processes, and structures. To develop an organization-specific maturity model, the CAE should review available models for the organization's country, sector, and industry, and consider the governance documents and issues specific to the organization. A draft maturity model should be discussed and agreed on with senior management and the board, including the audit committee.

In addition to establishing relevant and reliable criteria to measure governance effectiveness, maturity models can be used to:

- Evaluate governance effectiveness.
- Develop plans for improving the organization's governance structures, processes, and arrangements, either taken as a whole or by individual governance process (e.g., ERM, compliance, and internal audit). These plans are particularly useful when varying levels of maturity exist or are desired among different processes.
- Track improvement progress.
- Benchmark governance best practices.
- Map governance activities to those responsible for their design and operating effectiveness.

Audit activities should conclude this phase of the assessment process by validating its understanding of governance processes, structures, and assessment criteria with the board and related committees.

[10] More applicable to, but not limited to, state-owned enterprises.
[11] More applicable to state-owned enterprises, which, in most jurisdictions, have their financial statements audited by private sector independent auditors. In most jurisdictions, government organizations other than state-owned enterprises have their financial accounts and operations audited by supreme audit institutions, which generally have functional and administrative independence protected by law.

Develop a Periodic Governance Audit Plan

The CAE should use a risk-based approach in defining the scope of the governance assessment or assessments. It is important to consider the nature of the organization (i.e., system of government, international government organizations, national and state government organizations, agencies, state-owned enterprises, and municipalities) and the context within which it operates. The risks to achievement of organizational objectives for which comprehensive governance processes and structures should be in place will be greatest in large, complex, highly regulated organizations and organizations in multiple jurisdictions.

Developing a periodic governance audit plan requires:

- Discussion of any special circumstances with the board.
- Consideration for relationships among governance, risk management, and control.
- Selection of an audit approach.
- Consideration for reliance on other assurance providers.

Discussion of any special circumstances with the board will provide general board and audit committee insights to help frame the overall audit plan. The sections below detail additional information on governance/risk/control relationships, audit plan approach, and reliance on other assurance providers.

Governance, Risk Management, and Control Relationships

A periodic plan for auditing governance should consider the relationships among governance, risk management, and internal controls. As outlined in PA 2110-2: Governance: Relationship With Risk and Control:

- Effective governance activities consider risk when setting strategy. Conversely, risk management relies on effective governance (e.g., tone at the top, risk appetite and tolerance, risk culture, and the oversight of risk management).
- Effective governance relies on internal controls and communication to the board on the effectiveness of those controls.
- Control and risk also are related. Control is defined as "any action taken by management, the board, and other parties to manage risk and increase the likelihood that established goals will be achieved."

Audit Plan Approach

Governance/risk/control relationships and the nature of the organization's governance process and structures will help the CAE to determine the best approach to developing the audit plan. The best approach may be one or a combination of the following approaches:

- Audits of specific governance processes and structures such as those listed in the Review Governance Processes and Structures section on page12.
- A single audit including all processes and structures that focus specifically on governance. This approach might be most practical in small organizations or as a high-level review to determine whether additional processes and structures are needed and whether the existing processes and structures, taken together, give the board all the information it needs to fulfill its governance responsibilities.
- Incorporating governance in audits that focus more directly on operations or support activities. In this approach, a component of each audit would include the interface of the governance processes and structures with the audited operation or activity. Governance audit work at the operations and support activity levels will provide detailed information to internal audit about how well governance is understood and practiced throughout the organization. Over time, and if desired by the board, the audit function may be able to assess the state of governance within the organization as a whole, using this work as a basis for that opinion.

The CAE should discuss and agree with the board on which approach or combination of approaches will be most effective for the organization. To implement the selected approach, the CAE should review the audit universe and modify it as necessary to ensure that governance processes and structures are included, for example:

- If the decision is to audit specific governance processes and structures, these processes and structures should be identified and included as auditable entities in the audit universe.
- If the decision is to perform a single audit including all processes and structures that focus specifically on governance, these processes and structures will become an auditable entity.
- If the decision is to include governance in audits that focus more directly on business operations or support activities, modifying the audit universe will be more difficult. Ideally, the CAE will identify the governance processes and structures within each auditable entity and include them when assessing risk for each entity. This might not be feasible, though, because identifying those processes and structures might be a major project in itself. In this case, it might be more practical to require the audit teams to identify and evaluate those processes and structures during the audits they perform. Auditors will have to add time for this additional work to each audit. After some time — perhaps a year — auditors will know enough about the organization's governance that identifying governance processes and structures in entities not yet audited will not be a major project.

With the universe defined, auditors should use a risk-based approach to identify the audits to be carried out over the planning horizon. Audit functions should ensure that a balance of units are selected for review with regard to governance, risk management, and control. Doing so allows the auditors to consider the holistic, organic view of governance, risk management, and control.

The CAE should obtain board input to ensure that the highest risk non-board governance processes and structures are included in the internal audit plans. Many boards categorize organizational risks into strategic, operational, reporting, and compliance categories. The CAE should work with the organization's risk management professionals to identify possible discussion points with the board.

The CAE also should determine the board's expectations for audit function governance assessment deliverables. Examples of potential deliverables include:

- An overall opinion on the effectiveness of governance processes and structures.
- Opinions on the effectiveness of specific governance attributes.
- Reports with recommendations for improvement that do not include an opinion.

The board might prefer assessments based on a maturity model, with the maturity of each governance attribute measured against specific criteria. The board can then compare the actual and desired levels of maturity for each attribute, identify strengths and gaps, and get a more complete and balanced picture of the ethical climate than an audit opinion provides.

Some of the planned audits may be sensitive. It is important that the audit plan is reviewed with the board in detail and its sponsorship is clearly established.

Reliance on Other Assurance Providers

Special consideration should be given relative to governance audits including coordination with the external assurance providers.[12]

During the planning process, the CAE should determine what reliance the audit function can place on other assurance providers. Internal assurance providers include functions such as risk management, compliance, quality assurance, environmental auditors, health and safety auditors,

[12] See Practice Advisory 2050-1: Coordination and The IIA Practice Guide, Reliance by Internal Audit on Other Assurance Providers.

and government auditors. The criteria for reliance include:

- Organizational independence.
- Individual objectivity.
- Competence (e.g., technical knowledge, experience, professional or industry certification, and continuing professional education).
- Documentation of work.
- Engagement supervision.
- Quality of written reports delivered to management.
- Issues and action plans identified.
- Communication of results to the appropriate level of the organization.
- Issue closure process.
- Issue closure escalation process to the appropriate level of the organization.
- Risk-based considerations in the annual planning process.

To confirm reliance, the audit function might:

- Review some of the assurance provider's engagement work.
- Re-perform a sample of the work.
- Perform one or more combined assessments with the assurance provider.

The annual plans prepared by other assurance providers where reliance is anticipated should be provided to internal audit early in the audit planning cycle. The plans should include scope, objectives, timing, and locations/areas to be assessed. Ideally, these plans should be risk-based using a common language — the one the audit function uses. Copies of relevant assurance-provider performance reviews should be provided to the audit function.

Boards with mature governance practices are beginning to ask for more and better coordination and integration of internal assurance services. The audit function should be instrumental in forming an integrated or combined internal assurance-provider process.

External assurance providers such as external auditors, third-party assurance providers, and regulatory examiners will give the board, executive management, and stakeholders' additional comfort on aspects of the organization's performance and compliance. The CAE should consider the nature, scope, and timing of external assurance providers' work.

Plan and Complete Governance Engagements

Note: This section deals primarily with governance activities within the organization. Some leading internal audit activities also provide assurance on board governance activities. Guidance on assessing board governance is included in the Appendix.

Due to the uniqueness of each organization's governance processes and structures, planning a governance engagement may be difficult and require significant judgment by the auditor. Each engagement should include an evaluation of the design of the process or activity and sufficient testing to draw a conclusion on operating effectiveness.

Some specific areas to consider at the engagement level include:

- Process objectives — goals and purpose of the process or activities within the scope of the engagement.
- Risks — risks to the achievement of those objectives identified in setting strategy.
- Structures — organizational units, processes, policies, and procedures that support the achievement of objectives and are documented, communicated, and understood.
- Accountabilities — clearly defined roles, responsibilities, and accountabilities.

- Compliance with legal and regulatory requirements.
- People — adequate staffing, training, and development.
- Communicating results.
- Monitoring improvement action progress.

Planning the Engagement

Planning the engagement encompasses setting engagement objectives, identifying governance process objectives and risks, legal involvement, and engagement staffing. The audit plan should include the program of audits to be completed, timelines, and the resources needed.

Setting Engagement Objectives

Engagement objectives should align with the audit plan, reflect the purpose for performing the engagement, and identify the engagement deliverables. Simply put, engagement objectives state what the audit will provide. Engagement objectives should be formally established and communicated in an engagement memo or terms of reference. Objectives should clearly state the specific assurance to be provided. Examples include:

- Assess compliance with required governance activities.
- Evaluate risk management activities at the subsidiary level.
- Provide assurance on how well the organization's strategies have been communicated and adopted organizationwide.
- Evaluate the design, implementation, and effectiveness of the organization's ethics program and related activities.
- Assess how well authorities have been delegated, acknowledged, and followed throughout the organization.

Identify Governance Activity (Process) Objectives and Analyze Associated Risks

Understanding governance activity or process objectives enables the auditor to identify and analyze associated risks and controls. The overall objective of organizational governance in the public sector is to best serve and protect the public interest and ensure appropriate management accountability and communication to its key stakeholders.

There may be different types of objectives for each specific governance activity, process, or structure. Generally, objectives can be categorized as strategic, operational, reporting, and compliance. The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Enterprise Risk Management–Integrated Framework can provide useful guidance in identifying and understanding governance objectives. The COSO framework has been adapted by audit organizations to provide more direct applicability to public sector entities.[13]

Legal Involvement

Often, auditing requires an interpretation of laws and regulations. Except for those with law degrees, auditors generally do not have the legal background to adequately interpret the more complex legal implications affecting organizational governance. The CAE or supervisor of the engagement should involve the organization's legal department or General Counsel to provide the necessary advice. When the area of audit focus is assessment of the organization's legal activity, the CAE should consider use of outside counsel and obtain agreement from the board.

Engagement Staffing

Staffing requirements are shaped by the engagement's scope and objectives. While high-profile governance audits often require individuals with advanced knowledge, skills, competencies, and experience, the CAE is often challenged with resource constraints. The CAE should identify the knowledge, skills, competencies, and experience needed for the engagement and assign staff mem-

[13] The U.S. Government Accountability Office and the International Organization of Supreme Audit Institutions are among the organizations that have issued comprehensive COSO adaptations.

bers who best fit the requirements. Where important gaps exist, the CAE should consider just-in-time training, guest auditors, or third-party providers. When using a third-party source for staffing, the CAE should ensure that guest auditors and third-party providers are independent and objective.

Performing the Engagement

Sources of Evidence

In providing assurance, auditors normally use a two-step approach: Review the design and test the operating effectiveness of key processes and structures. Audit functions should gather sufficient, relevant, and reliable information in carrying out the work and formulating conclusions and recommendations. Evidence should be gathered from a variety of sources, as recommended in Table 2.

Note: Many types of evidence may be relevant to one or more processes or structures.

Table 2: Governance Assurance Engagement

PROCESS OR STRUCTURE	EVIDENCE TO CONSIDER
Board and Audit Committee	· Legal documents establishing the organization (e.g., articles of formation, bylaws). · Legal and regulatory requirements with which the board should comply (e.g., acts, statutes, and rules). · Briefing papers including pre-meeting materials and presentations. · Meeting minutes and actions taken. · Charters including those of any committees of the board. · Board member profiles. · Self-assessments. · Regulatory actions/sanctions. · Orientation and training materials. · External reports to independent auditors, regulators, rating agencies, etc. · External reporting process documentation that evidences legal involvement. · News sources for any relevant press regarding the organization.

PROCESS OR STRUCTURE	EVIDENCE TO CONSIDER
Strategy	· Current list of the organization's objectives, standards, and strategies. · Communication protocols. · Details on alignment throughout the organization. · Process to update and re-communicate. · Evidence of board approval from meeting minutes or correspondence directly from the board. · Details showing the allocation of resources to execute strategies approved by the board. · Documented responsibility for strategy implementation. · Risk policy and procedures approved by the board that include risk process, risk universe with common risk descriptions, risk tolerance levels, risk assessment and reporting process, and risk ownership. · Details of function/department/unit/individual objectives and their alignment to organizational goals. · Performance or reward systems that encourage personnel to achieve organizational goals that are aligned with stakeholder expectations.
ERM	· Clearly defined objectives to enable the identification and assessment of risks related to objectives. · Formal processes/procedures to identify risks to the achievement of objectives across the entity. · Formal processes/procedures to analyze risks as a basis for determining how risks should be managed. · Formal processes/procedures to identify and assess changes in external and internal environments that could significantly impact the achievement of objectives. · Formal processes/procedures to consider the potential for fraud in assessing risks to the achievement of objectives.
Ethics	· Ethics and integrity policy — adoption, communication, affirmation, and training. · Mission, vision, and values established and communicated. · Whistleblower hotline established and communicated, its level of awareness and use, and the organization's response. · Organizational personnel surveys confirming individual awareness and understanding. · Organizational personnel surveys confirming that executive leadership displays a values-based culture and philosophy. · New employee training and orientation that include values, culture, and philosophy. · Communication/training exists on ethics and values in "gray areas."

PROCESS OR STRUCTURE	EVIDENCE TO CONSIDER
Compliance (organizationwide)	· Articles of formation (incorporation), bylaws, operating agreements, etc. · Policies that include purpose, roles and responsibilities, audience, scope, definitions, authorities, effective dates, implementation dates and procedures, authorities and administration, measurement, and validation. · Information and communication security/privacy policies and procedures. · Standards that articulate the level of performance expected (e.g., zero defects or tolerance, Six Sigma). · Mandatory governance requirements adopted with appropriate structures and incumbents in place at C-suite level. · Detailed process and accountability in place to keep current on governance requirements. · Governance committee charters that include purpose, scope authority, roles and responsibilities, and membership. These should be published, widely known, readily accessible, and periodically reviewed and updated as necessary. · Governance committee meeting minutes, actions taken, and reporting. · Examples of governance committees in large organizations include governance, strategy, risk, audit, control, compliance, disclosure, finance, and IT governance/risk. · For large and more complex organizations, governance structures and organization charts that cascade throughout the organization, are fully staffed, and have clear reporting relationships. · Details on governance processes where there is shared accountability, particularly in organizations that use matrices management. · Process details for addressing or approving deviations to policies, standards, and procedures. · Financial reports. · Regulatory actions. · Internal measurement results such as balanced scorecards. · Civil actions. · Press releases about the organization — what others are saying about the organization. · Analysis, particularly external, comparing actual results to objectives and expectations, both short and long term. · External reports along with documentation evidencing conformance with established procedures.

PROCESS OR STRUCTURE	EVIDENCE TO CONSIDER
Compliance (level below organizationwide structures)	· Documentation that identifies all organizational activities, operations, departments, functions, and processes. · Documented maps for each process showing inputs, activities, tasks, steps in the process, and outputs. Mapping also should include references such as objectives, citizen conditions of satisfaction, ownership, procedures to update when necessary, and procedures to make available to those with the need. · Documentation for all aspects of transformational transactions and existing process change management. · Details on mandatory/required reporting to external parties.
Organizational Accountability	· Job descriptions for all organization personnel that contain responsibilities, authorities, reporting relationships, and education. · Professional development program/process that applies to all personnel. · Leadership development program/process. · Individual training records that include skills assessments, development plans, and training completed. · Organizationwide training on ethics, integrity, and values. · Personnel surveys that provide insights into how people view the organization's commitment to people, their capabilities, accountabilities, behavior, training, and education. · Detailed, board-approved delegated authorities with processes for personnel acknowledgement, periodic review, validation, and remediation when authorities are breached. · Disclosure committee charter, roles, responsibilities, and meeting minutes.

PROCESS OR STRUCTURE	EVIDENCE TO CONSIDER
Monitoring	· Documented organizational performance measurement system that illustrates the system and describes the required information, form of the reports, reporting periods and due dates, and safeguards that ensure accuracy and completeness. · Copies of actual reports. · Personnel and customer surveys: processes, questions, frequency, audiences, results, responses, and status of improvement actions. · Monitoring systems over and above performance measurement systems that should specify what and when to monitor, responsibility, results, and improvement action plans and status. · Internal communication systems up, down, and across the organization. · Details on assurance mechanisms that include charters, scope, plans, and reports. · Benchmarking process and results. · Information "asset" management process/program. · Due diligence evidence/documentation on assessment of third-party governance practices. · External reports with comparisons to relevant internal reports covering governance practices. · Surveys and results regarding personnel perceptions of the quality of information and communication.
IT Governance (where applicable)	· IT governance/risk/control program and processes. · Defined information security policies, procedures, and practices.

Workpaper Documentation

Due to the sensitivity of some governance audit work, special handling may be needed for access and storage of related audit workpapers. Audit workpapers are the property of the organization. The files are under the control of the audit function and are accessible only to authorized personnel and citizens or others granted the right by legal jurisdiction. Management review may be granted to substantiate or explain audit findings or to use audit documentation for other purposes.

Communicating Outcomes and Results

Audit functions should communicate engagement outcomes and results consistent with Standard 2400 and Practice Advisory 2400-1.[14] Due to potential sensitivity, the audit function should consider obtaining the general counsel's advice on communicating results and retaining related workpapers before starting the engagement. Reporting may be formal or informal, with consideration for which method will stimulate corrective action without resulting in unintended negative repercussions. Even if reporting is informal, audit functions must follow the *Standards* in communicating the audit results and in monitoring improvement action progress.

The CAE may be asked to facilitate self-assessments of the board or its committees. The results, including any action plans, should be documented so that the board can monitor their progress. The method for documenting and communicating results will be at the board's discretion. The CAE should agree with the board and executive management on dissemination of all governance-related reports.

Monitoring Improvement Action Progress

The CAE should work with the audit committee to establish a system to monitor the progress of improvement actions communicated to management and the board. Due to the importance of governance activities and board and CEO responsibilities for effective governance, the system should include:

- The time frame within which the improvement action will be completed, including key milestone dates.
- Ongoing evaluation of governance activity owners' responses.
- Audit functions validation or follow-up audit of the improvement action.
- An escalation process for unsatisfactory response to include the assumption of risk for a delayed or incomplete improvement action.

Engagement Administration

Governance audits can become high profile because they are generally public record. If the audit function is to have a key role in assessing governance, its overall effectiveness in providing assurance to stakeholders is critical. The CAE should ensure that governance engagements are adequately staffed, appropriately supervised, and subject to the audit function quality assurance and improvement process, consistent with the *Standards*.

The board, through its audit committee, should look to the CAE for periodic reports on the audit activity's quality assurance and improvement program and ensure that the program provides for an independent assessment at least every five years. The CAE also should ensure that these reports are provided. In addition, the board should draw its own conclusions on the effectiveness of the audit function.

[14] See "Additional Resources" for a link to IIA guidance, Transparency of the Internal Audit Report in the Public Sector.

Additional Resources

IIA Guidance

GTAG 17: Auditing IT Governance
https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG17.aspx

Practice Advisory 2050-1: Coordination
https://global.theiia.org/standards-guidance/Member%20Documents/PA_2050-1.pdf

Practice Advisory 2110-2: Governance: Relationship With Risk and Control
https://global.theiia.org/standards-guidance/Member%20Documents/PA_2110-2.pdf

Practice Advisory 2120-3: Internal Audit Coverage of Risks to Achieving Strategic Objectives
https://global.theiia.org/standards-guidance/Member%20Documents/PA_2120-3.pdf

Practice Guide: Assessing the Adequacy of Risk Management Using ISO 31000
https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Assessing-the-Adequacy-of-Risk-Management-Practice-Guide.aspx

Practice Guide: Coordinating Risk Management and Assurance
https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Coordinating-Risk-Management-and-Assurance-Practice-Guide.aspx

Practice Guide: Evaluating Ethics-related Programs and Activities
https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Evaluating-Ethics-related-Programs-and-Activities-Practice-Guide.aspx

Practice Guide: Reliance by Internal Audit on Other Assurance Providers
https://global.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/Reliance-by-Internal-Audit-on-Other-Assurance-Providers-Practice%20Guide.aspx

Public Sector Definition
https://global.theiia.org/standards-guidance/leading-practices/Pages/Public-Sector-Definition.aspx

The Role of Auditing in Public Sector Governance
https://global.theiia.org/standards-guidance/leading-practices/Pages/the-role-of-auditing-in-public-sector-governance.aspx

Transparency of the Internal Audit Report in the Public Sector
https://global.theiia.org/standards-guidance/leading-practices/Pages/Transparency-of-the-Internal-Audit-Report-in-the-Public-Sector.aspx

Non-IIA Guidance

Board Briefing on IT Governance, 2nd Edition. IT Governance Institute.

Enhancing Board Oversight by Avoiding and Challenging Traps and Biases in Professional Judgment (2012). COSO.

Enterprise Risk Management–Integrated Framework (2004). COSO.

Internal Control–Integrated Framework (2013). COSO.

Principles of Good Governance. Professional Risk Managers' International Association, September 2009.

Appendix — Board Risks, Control Objectives, and Practices

The overall objective of organizational governance is to inform, direct, manage, and monitor an organization's activities toward achieving its objectives. On behalf of the organization's key stakeholders, the board is the focal point for ensuring effective governance.

The following table describes examples of risks that boards may encounter as well as control objectives and practices that can be used to manage them.

RISKS/EVENTS	CONTROL OBJECTIVES	PRACTICES
Board members do not have the required organization, industry, technical, IT, or other knowledge and experience.	To fulfill board roles and responsibilities completely, accurately, and timely.	There is a sufficient number of outside, independent members of the board as required by organizational need and applicable laws. The sufficient number of members and expertise needed for the board is defined by formal, specific criteria. Practices are in place to ensure the right mix of expertise, skills, and diversity is represented on the board at all times. Backgrounds of potential board members are thoroughly reviewed and validated. Term limits are strictly enforced to ensure a regular infusion of new individuals who bring needed competencies, provide fresh thinking, and keep governance connected to the stakeholders.
Members do not understand the role or responsibilities of the board.		Orientation, onboarding, and continuous training is conducted to ensure all members understand their role and responsibilities.
Failure of board members to adequately fulfill their roles and responsibilities.		The board charter, policies, roles and responsibilities, and procedures are documented and made available. Updates are made timely. Changes are communicated adequately. Board members periodically visit the organization and meet with key leaders.

RISKS/EVENTS	CONTROL OBJECTIVES	PRACTICES
Failure of the board to meet legal requirements.	To meet legal requirements of the board.	All legal requirements are identified, communicated, and made available to board members. Requirements are continuously monitored. Updates are communicated timely and adequately.
Failure of individual board members to exercise appropriate due diligence.	To ensure all board policies, procedures, and legal requirements are followed.	A parliamentarian is assigned to monitor and advise on board processes, procedures, and legal requirements. An agenda is followed and minutes are kept for all meetings. Action dockets or similar methods are used to track assignments and deadlines. Calendars are maintained to keep board members informed of meetings and important deadlines. Individual evaluations and board assessments are conducted at least annually to identify improvements and if any board members' terms have ended and/or need to be rotated off the board.
Insufficient challenge and skeptical inquiry is provided by board members.	To ensure all board members' concerns are identified and addressed.	*Robert's Rules of Order*[15] procedures are followed in board meetings, which are the standards for board rules of order. Sufficient time is allocated in all agendas for open discussion and debate. The chairman of the board position is held by an outside, independent member with extensive experience on other boards. This is considered a best practice and is mandated by law in some jurisdictions because such a person is less likely to be influenced by relationships with, and the personal interests of, management, and may be more effective in challenging executive actions. The board interacts regularly with the internal and external auditors, at times outside the presence of management, to ensure they are allowed to carry out their mandate in an unrestricted manner. A sufficient number of nonexecutive directors on the board are attending board meetings.

[14] Originally titled *Pocket Manual of Rules of Order for Deliberative Assemblies*, written by Henry Martyn Robert in 1876. See http://www.robertsrules.com/ for latest edition.

RISKS/EVENTS	CONTROL OBJECTIVES	PRACTICES
Unknown or unanticipated vulnerabilities.	To ensure board members understand the risks to the organization's objectives and the related vulnerabilities of the organization.	Risk assessments conducted by the organization's chief risk officer — if one exists — management, internal audit, or external parties (e.g., external auditors, regulators) are provided to board members as they become available. Board members conduct their own risk assessments at least annually to include scanning the environment for unanticipated events that may harm the organization's reputation.
Decisions are made or actions are taken based on unreliable, incomplete, or untimely information.	To ensure the board has reliable, complete, and timely information.	All necessary information (e.g., background, financial impact, risks, and benefits) is provided to board members in a consistent format with sufficient time for thorough review before decisions are made. Sufficient time is allowed for debate before decisions are made.
Failure to meet stakeholder expectations.	To ensure primary stakeholder needs are known by all board members.	Primary stakeholders are identified and allowed to vote on board membership. Surveys are conducted periodically to identify primary stakeholder needs. Primary stakeholders are allowed to attend meetings and ask questions at appropriate times during the meeting.
Failure to appropriately inform key stakeholders.	To ensure that all mandatory and optional information is communicated accurately and timely to key stakeholders (including regulatory agencies).	The board reviews and approves all information, reports, and filings before release of information to key stakeholders.
Organizational governance structures, processes, and practices are ineffective or lack sustainability.	Ensure an appropriate organizational governance framework is in place and operating effectively.	Board oversight and monitoring of key organizational activities such as objective setting, strategies, structures, operating plans and budgets, operating performance, and results. A succession-planning process exists for the organization's CEO and other key leadership positions. The board reviews and approves the organization's code of conduct, ethical culture, policies, and procedures.

Author, Contributors, and Reviewer

Author

Gualter Portella, CIA, CCSA, CGAP, CRMA

Contributors

Scott Cohen, CIA, CCSA, CGAP, CRMA
Oliver Dieterle, CIA, CGAP, CRMA
Dr. Tea Enting-Beijering
Greg Hollyman, CIA, CCSA, CFSA, CGAP, CRMA
Kenneth J. Mory, CIA, CRMA
Christie J. O'Loughlin, CGAP, CRMA
Gloria Spelman, CGAP
Mmathabo Sukati, CIA, CCSA

Reviewer

Bruce Turner CGAP, CRMA, CISA, CFE, CFIIA

About the Institute

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

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes. For other authoritative guidance materials provided by The IIA, please visit our website at https://globaliia.org/standards-guidance.

Disclaimer

Copyright

The Institute of Internal Auditors | Global

GLOBAL HEADQUARTERS
247 Maitland Ave.
Altamonte Springs, FL 32701 USA

T: +1-407-937-1111
F: +1-407-937-1101
W: www.globaliia.org

140454