– Practice Guide

ASSESSING ORGANIZATIONAL GOVERNANCE IN THE PRIVATE SECTOR

JULY 2012

The Institute of Internal Auditors | Global

Table of Contents

Executive Summary

In today's political and business environment, there is increasing focus on governance, risk management, and control. Strong governance systems are needed to better ensure that organizations will meet their objectives and stakeholder expectations. Stakeholders expect boards[1] and management to accept responsibility and implement appropriate governance practices. The board is the focal point for governance practices and in fulfilling its oversight responsibilities will look to the internal audit activity to provide it with assessments on the organization's governance practices. This Practice Guide provides the chief audit executive (CAE) specifically in the private sector with direction on how to assess and make appropriate recommendations for improving governance processes.

This Practice Guide includes the following sections and an appendix:

Understanding the Context of and Defining Organizational Governance

Organizational governance involves the set of relationships among the organization's stakeholders, board, and organizational management.

There are a number of authoritative definitions put forth by professional groups, regulators, academia, et al. These definitions are all very similar. The one used in this practice guide comes from The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* (*Standards*). Regardless of the governance definition used, there are common themes that are included in this section.

The Role of Internal Audit in Providing Assurance and Consulting Services

The internal audit charter should state that the scope of work includes all governance activities and processes. This does not mean, however, that internal auditors are required to perform audits of all governance activities and processes. There are several roles internal audit can play in assessing and contributing to the improvement of organizational governance practices. Although internal audit can play various roles, this Practice Guide deals only with providing formal assessments of organizational governance.

Identifying and Analyzing Relevant Governance Processes/Practices and the Assessment Criteria to Use

There is no "one size fits all" governance model. Governance structures and practices should be individually tailored to the organization. There may be legal and regulatory requirements, mandatory and optional practices prescribed by country governance codes, various organizations promoting governance principles, and practices common to the environments that the organization and its peers operate in. Guidance on IT governance is provided because of the reliance most organizations place on IT and the pervasive governance practices that should span the technology spectrum.

Developing the Periodic Plan for Auditing Governance

The range of activities, depth of review, and time period to include in the assessment should be established and agreed on with the board. All governance activities, both board and nonboard, should be considered.

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

In the process of setting the scope, the CAE will assess the relative risk of governance processes, evaluate the audit approach — assurance vs. consulting — and identify the various stakeholder expectations in setting the assessment objectives.

In developing a periodic program of governance audits, CAEs will need to consider how many audits to do and how governance assessments are woven into nongovernance-specific audits, a reliance that may be placed on other organization functions, external audit, and governance over IT.

Planning and Completing the Governance Engagements

Individual engagements flow from the annual program of audits. At the engagement level, staffing the project with the right skills competencies and experience is critical. Because many organizations are subject to regulations addressing required governance practices, the CAE should forge a strong working relationship with and involve the organization's general counsel (internal or external).

Considerations by Specific Governance Activity

With the variety of organizational operating environments globally, this Practice Guide provides aspects of important governance processes the internal auditor in the private sector should consider while developing his/her audit program(s). There is specific guidance to consider in facilitating board assessments and evaluating the organization's strategy process, ethical environment, risk management process, compliance function, monitoring activities, and IT governance.

Appendix — Board Activities/Processes and Risks

The overall objective of organizational governance is to inform, direct, manage, and monitor an organization's activities toward achievement of its objectives. On behalf of the organization's key stakeholders, the board is the focal point for ensuring effective governance. The board faces risks to achieving effective governance. However, there are a number of practices that when implemented effectively will mitigate the risks they face.

Introduction

The internal audit activity helps an organization achieve its objectives by bringing a systematic and disciplined approach to evaluating and improving the effectiveness of governance, risk management, and control processes. This practice guide discusses important areas for consideration in assessing the organization's governance practices. By their very nature, practice guides provide information on how to conduct internal audit activities. This Practice Guide should be used in conjunction with the *Standards* and practice advisories in the International Professional Practices Framework (IPPF), specifically Standard 2110: Governance and Practice Advisories, 2110.1: Governance: Definition; 2110.2: Governance: Relationship with Risk and Control; and 2110.3: Governance: Assessments. In addition, due to the relationships between governance, risk management, and control, the *Standards* addressing those specific governance activities (Standard 2120: Risk Management and Standard 2130: Control), along with supporting practice advisories and practice guides, should be referenced.

The type of organization, its size, complexity, and geographic location(s) will drive the shape of the governance requirements and practices. For that reason, this Practice Guide will provide guidance on how to assess organizational governance in the private sector. This Practice Guide will not provide a framework or audit program, as those are best designed specifically for the organization in the environment in which it operates.

The organization's board has responsibility for the governance system. The CEO owns the governance processes

within the organization (non-board processes). Many governance practices are performed by the board and executive management, which makes assessment a sensitive matter. An effective internal audit activity that is independent, objective, and capable, uses sound assurance processes and practices, and conforms to the *Standards* is qualified to audit the governance process and provide assurance to the board and management on governance effectiveness.

1.0 Understanding the Context of and Defining Organizational Governance

Organizational governance involves the set of relationships among the organization's stakeholders, board, and organization management. These relationships are framed by 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.

The term governance has a range of definitions depending on a variety of environmental, structural, and cultural circumstances and legal frameworks. The *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."

Globally, there are a variety of governance models that have been published by other organizations, including legal and regulatory bodies. For example, the Organisation for Economic Co-operation and Development (OECD) defines governance as "a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance provides the structure through which the objectives of the company are set and the means of attaining those objectives and monitoring performance are determined." The Australian Securities Exchange Corporate Governance Council defines governance as "the system by which companies are directed and managed. It influences how the objectives of the company are set and achieved, how risk is monitored and assessed, and how performance is optimized." In most instances, there is an indication that governance is a process or system and is not static. What distinguishes the approach in the *Standards* is the specific emphasis on the board and its governance activities.

The frameworks and requirements for governance vary according to organization type and regulatory jurisdictions. Examples include publicly traded companies, not-for-profit organizations, associations, government or quasi-government entities, agencies, academic institutions, private companies, commissions, and stock exchanges.

The board is the focal point for effective organizational governance. It is the link between the stakeholders and the organization's executive management. To be effective, the board should be independent, engaged, and committed. The board bears primary responsibility for the governance of its organization. The board establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the organization. The board directs and provides oversight of the executive leader and senior management in setting strategic objectives, establishing appropriate risk levels, instituting effective control systems, tracking performance, and providing transparent, complete, clear, and timely communication to stakeholders.

Other board responsibilities include setting the organization's strategic objectives and providing the leadership to put them into effect, supervising the management of the business, and reporting to the stockholders on their stewardship. The board's actions are subject to laws, regulations, and the needs of the stakeholders. The board typically delegates significant authority for the day-to-day operations to an executive leader (CEO) and his/her executive officer team.

The organization's executive leadership and senior management are accountable to the board. The CEO is ultimately responsible for implementing the organization's governance system. The CEO sets the "tone at the top" for the integrity, ethics, and conduct that will contribute to an effective governance environment. He/she imparts this tone to his/her executive leadership team, which in turn cascades organizationwide. The CEO and executive management should do more than just "talk the talk." They are on the organization's stage and 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 the appropriate laws, regulations, and codes.

The starting point for internal audit in providing assurance is to gain an understanding of the context within which its organization operates, identify the key stakeholders and their requirements, and determine how the organization defines governance. The CAE should work with the board and the executive management team, as appropriate, to determine how governance should be defined for audit purposes.

2.0 The Role of Internal Audit in Providing Assurance and Consulting Services

The internal audit charter should state that the scope of work includes all governance activities and processes. This does not mean, however, that internal auditors are required to perform audits of all governance activities and processes. There are a number of roles internal audit can play in assessing and contributing to the improvement of organizational governance practices.

- 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 not focused on governance as an audit topic.
- Act as facilitators, assisting the board in self-assessments of governance practices.
- Observe and formally assess governance, risk, and control structural design and operational effectiveness while not being directly responsible, if positioned properly within the organization and staffed with capable professionals.

The appropriate role for internal audit and the resource commitment to each of these approaches will depend largely on the maturity of the organization's governance structures and the organization's size and complexity. The CAE should discuss and reach an agreement with the board on internal audit's role in assessing organizational governance.

Although internal audit can play various roles, this Practice Guide deals only with providing formal assessments of organizational governance. The various ways to assess organizational governance are discussed in Section 4, Developing the Periodic Plan for Auditing Governance. Recognizing that there could be sensitivities to assessing and reporting on some board- and executive-level governance activities, board-level sponsorship for the assessments should be obtained as part of this periodic audit planning process.

3.0 Identifying and Analyzing Relevant Governance Processes/Practices and the Assessment Criteria to Use

The next phase in providing formal assessments of organizational governance is to identify all relevant governance processes/practices. This is followed by reviewing the processes to identify process objectives and related risks. The next step in this phase is to establish assessment criteria and, finally, validate the understanding obtained with the board and organization's executive management. As you perform these steps, you may find that the governance process documentation is not adequate. If this condition exists, it should be reported to the board as an initial opportunity to strengthen governance practices.

3.1 Sources for Governance Processes/Practices

Governance practices should be tailored to comply with mandatory requirements and best fit the organization's risk profile.

The legal jurisdictions in which the organization operates promulgate those laws and regulations deemed to be in the best interest of good governance. These tend to form the minimum requirements. Examples are the U.S. Foreign Corrupt Practices Act (FCPA), Security Laws, and the U.S. Sarbanes–Oxley Act of 2002; Ontario, Canada, Bill 198; Canada's Competitions Act; the German Corporate Governance Code; the Australian Corporate Reporting and Disclosure Law – CLERP9; France's Financial Security Law; Italy's L262/2005; South Africa's Companies Act 2008; and South Africa's King III Report.

The legal and regulatory requirements that apply to your organization should be used in conjunction with applicable requirements stemming from self-regulated organizations (SRO). An SRO is an organization having certain limited regulatory authority over its members. It can be a market mechanism or industry or profession specific. One of the largest global types of SROs is a stock exchange. Stock exchanges include in their regulations specific governance practices that listed companies should adhere to. There are more than 50 major stock exchanges.

The Articles of Association, or similar documents (e.g., Acts and Regulations for some government organizations), establish and define the purpose of the organization. Bylaws, policies, or operating agreements also may be created. The latter are rules for conduct of the organization. They are the "game plan" on how the organization is to be run and operated. Bylaws, policies, and operating agreements also set out the rights and powers of the stakeholders, board members, and officers within the organization. These are, in effect, a contract among members, and should be formally adopted and/or amended. The bylaws should be reviewed regularly.

Generally speaking, an organizational governance code is a set of principles, standards, and/or preferred practices that are promulgated by an influential body relating to governance of the organization. These codes can be mandatory, strongly recommended, or optional. Some codes are linked to stock exchange listing requirements.

The OECD[2] has published a set of governance principles that while non-binding provide common elements of good governance practices and guidance on implementation. The principles tend to focus on publicly traded corporations but are useful in comparing and improving governance practices in any organization.

Other sources useful in identifying governance practices include the customs, behaviors, and stakeholder expectations that exist in the organization's operating environment.

3.2 Review the Documented Governance Processes

Concurrent with identifying the governance requirements from Section 3.1, internal audit should obtain and review the governance documentation that exists. Keeping in mind that there is no "one-size-fits-all" governance framework or model, the actual governance processes and activities will vary. By design, the organization's governance processes should respond to the requirements identified in the preceding section.

To further ensure that all governance processes and activities have been considered, the following is provided as a generic yet comprehensive list of governance processes that should be evident in the organization's formal and informal governance practices. Governance practices

[2] OECD Countries:
Australia, Austria, Belgium, Canada, Chile, The Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, The Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States. The Council of the European Commission also takes part in the work of OECD.

are grouped at the board level and within the organization (non-board). Together, they form the governance umbrella over the organization's operations.

Board Governance Practices

- 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 committee governance practices.
- Board composition, including selection, induction, ongoing education and training, remuneration, and protection of board members.
- Board and committee oversight including objective setting, strategies, structures, operating plans and budgets, capital acquisition and allocation, CEO, enterprise risk management (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 internal audit.
- 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.
  - 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.
  - Reviewing and approving major changes in accounting and auditing principles and practices.
  - Declaring dividends and approving share repurchase programs.
  - Resolving cross-organizational issues.

Organization Governance Practices

- Setting objectives.
- Developing strategies, operating plans and budgets, organizational structures, and management committees.
- Assignment of authority and responsibilities organization-wide.
- Defining behaviors, codes of ethics, and conduct including conflict of interest, fair dealing, protection and proper 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 codes both mandatory and optional where adopted.
- Monitoring and performance measurement.
- 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 enterprise-wide activities like risk management and compliance that serve as a second line of defense).
- Communication up, down, and across the organization.
- Processes that ensure effective communication with shareholders and stakeholders.
- Capital acquisition and allocation.
- Capabilities — people selection, development, retention, and succession planning.
- Transformational transactions.
- Cross-organization issues.
- Organization responsibility and sustainability.

- Evaluation and rewards, both salary and incentive compensation.
- Organizational processes for assessing performance and independence of external auditors, including the nature and extent of non-audit services obtained.

Internal audit is itself a key governance activity. Its effectiveness in providing assurance to stakeholders is critical to effective governance. The board 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 per Standard 1312: External Assesments. The CAE should ensure that the reports of independent assessors are provided to the board. In addition, the board will draw its own conclusions on the effectiveness of the internal audit activity.

3.3 Establish the Assessment Criteria

Laws, regulations, and, potentially, governance codes provide the basis for the organization's mandatory governance practices. There also are qualitative aspects of an organization's governance practices that should be made a part of the assessment criteria. One assessment tool that may be considered is a governance maturity model. There are governance maturity models available; however, we do not provide one here because the governance attributes and criteria will vary depending on the organization's context. To develop an organization-specific maturity model, the CAE should review any available models for the organization's country and industry and take into consideration the governance documents and issues specific to the organization. A draft maturity model should then be discussed and agreed on with senior management and the board.

Once finalized, a maturity model can be used to evaluate and improve the organization's governance structures, processes, and arrangements either taken as a whole or by individual governance process — ERM, compliance, internal audit, and so on — particularly, when some governance processes may have greater desired maturity than others. Use of maturity models also provides a good facility for tracking improvement progress. The maturity model will provide the methodology for establishing the criteria needed to provide relevant and reliable information on the existing governance process effectiveness. In addition, it can be used for benchmarking practices that the board would expect to have as a minimum acceptable level.

3.4 Validate Understanding and Agree on the Assessment Criteria

The board and board-level committees have responsibility for board-level governance practices and oversight responsibility for the governance practices within the organization. The CEO has overall responsibility for governance practices within the organization and may delegate certain governance responsibilities to others in the organization. Internal audit should map the governance responsibilities to those responsible for their design and operating effectiveness.

After completing Sections 3.1, 3.2, and 3.3, internal audit should validate its understandings with the governance process owners, senior management, and the CEO. Internal audit should conclude this phase of the assessment process by further validating its understanding of the governance practices with the board and related committees. The assessment criteria should be agreed to as well.

4.0 Developing the Periodic Plan for Auditing Governance

The definition of governance in the *Standards* emphasizes the board and its governance activities. This includes evaluating board effectiveness. It also includes providing the board with timely and relevant information regarding the governance process, including the non-board activities through which governance is realized.

In addition, as discussed in Practice Advisory 2110-2, the relationships among governance, risk management, and internal controls should be considered:

- 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, as 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."

Due to these interrelationships and depending on the nature of the organization's governance structures and processes, the most appropriate way to audit governance might be one or a combination of the following:

- Audits of specific governance practices such as those listed in Section 3.2: Review the Documented Governance Processes.
- A single audit including all processes that focus specifically on governance.
  - This approach might be practical only in small organizations or as a high-level review to determine whether additional processes are needed and whether the existing processes, taken together, give the board all the information it needs to fulfill its governance responsibilities.
- Including governance in audits that focus more directly on business operations or support activities.
  - In this approach, a component of those audits would include the interface of the governance processes with those operations and activities. Governance audit work at the operations and support activity level will provide detailed information to internal audit on how well governance practices are understood and practiced throughout the organization. Over time and if desired by the board, the internal audit activity may be able to provide assessments on 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, taking into account the considerations that follow in this section.

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.

If the decision is to audit specific governance processes, these processes should be identified and included as auditable entities in the audit universe.

If the decision is to perform a single audit including all processes that focus specifically on governance, this 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. A certain amount of time will have to be added to each audit for this additional work. After some period of time — perhaps a year — enough will be known 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, a risk-based approach should be employed to identify the audits to be carried out over

the planning horizon. The audit activity should ensure that there is a balance of units selected for review in the three areas of interest to internal audit due to their interrelation — governance, risk management, and control. Doing so allows the audit activity to take into consideration the holistic organic view of governance and its effects on risk management practices and internal controls and vice versa. At the organizational level, board input should be obtained on the level of relative risk of each of the governance processes such that the highest risk organization governance processes are included in the internal audit plans. Many boards categorize organizational risks into strategic, operational, financial, and compliance. Risk-savvy boards expand the categories to include intangibles such as assets, reputation, social responsibility, and unpredictable events. The CAE should work with the organization's risk management professionals in listing possibilities for discussion with the board.

The CAE should also determine the board's expectations for internal audit's governance assessment deliverables. For example, does the board want an overall opinion on the effectiveness of all governance practices, an overall opinion on those governance practices that exist within the organization, opinions of the effectiveness of specific elements, or 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 be clearly established.

While this section deals primarily with governance activities within the organization, some leading internal audit activities also give assurance on board governance activities. The appendix includes risk considerations for a number of these activities.

4.1 Risk Assessment

As stated above, 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., publicly traded and privately held, large and small, local and global, for profit and not-for-profit, simple and complex, highly regulated and non-regulated) and the context within which it operates. The risks to achievement of organizational objectives for which comprehensive governance processes should be in place will be greatest in large, complex, highly regulated organizations and organizations in multiple jurisdictions.

4.2 Special Circumstances

The key elements in developing the audit plan are applicable for all types of organizations. Special circumstances may exist for some organizations. The CAE should review organization bylaws, articles, board and board committee charters, and the organization's operating environment, and discuss any special circumstances with the board. The board's insights from these discussions will help frame the overall audit plan. Special considerations may apply in certain non-profit and government contractor activities.

4.3 Reliance on Other Assurance Providers

Special consideration should be given relative to governance audits including coordination with the external auditors.

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

- Organizational independence.
- Individual objectivity.
- Competence (e.g., technical knowledge, experience, professional or industry certification, and continuing professional development).
- 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 appropriate level in organization.
- Risk-based considerations in the annual planning process.

To confirm reliance, internal audit might:

- Review some of the assurance provider engagement work.
- Reperform 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, and timing and locations/areas to be assessed. Ideally, these plans should be risk based using a common language — the one internal audit employs. Copies of relevant reports from these assurance provider reviews should be provided to internal audit.

Boards of organizations with mature governance practices are beginning to ask for more and better coordination and integration of the assurance services. Internal audit 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 provide the board, executive management, and stakeholders additional comfort on aspects of the organization's performance. In establishing the governance assessment approach, the CAE should consider the nature, scope, and timing of external assurance providers' work. Practice Advisory 2050-1: Coordination and The IIA's Practice Guide, Reliance by Internal Audit on Other Assurance Providers, provides guidance on coordinating work with external auditors.

4.4 Communicating Activities among the Board and External and Internal Auditors

Key communication points occur during the annual planning process, providing status on plan completion, reporting of results, and follow-ups on management improvement actions. The CAE should have practices in place with the board and the external auditors to facilitate these communications. Form, content, and timing (scheduling) should be established in advance generally using a 12- to 15-month window.

Communication is a two-way street. The CAE should set internal audit expectations with the board and external auditors to ensure receipt of relevant information that would guide and shape internal audit governance assessment work.

5.0 Planning and Completing Governance Engagements

How an organization designs and practices effective governance will vary. Therefore, establishing objectives and criteria upon which to base the assessment is difficult. There are common themes, but there are often no common practices. As a result, assessing the adequacy of governance activities will require significant judgment by the auditor. For each engagement, the assessment should include an evaluation of the design of the process or activity and include sufficient testing to draw a conclusion on operating effectiveness.

Some specific areas to consider at the engagement level include:

- Process objectives — goals, purpose, and objectives of the process or activities within the scope of the engagement.
- Risks — risks that exist to achievement of those goals and objectives identified in setting strategy.
- Structures — structures (organizational units, processes, policies, and procedures) that support achievement of objectives and are documented, communicated, and understood.
- Accountabilities — clearly defined roles, responsibilities, and accountabilities.
- Required legal and regulatory requirements conformance.
- People — adequate staffing, training, and development.
- Communicating results.
- Monitoring improvement action progress.

5.1 Planning

Setting the Engagement Objectives

Engagement objectives reflect the purpose for performing the engagement and the deliverables that are to come from the work. Simply stated, engagement objectives state what the audit will provide. While the objectives should have been developed during the periodic audit planning process, the objectives should be formally established and communicated in an engagement memo or Terms of Reference. These objectives can be stated in a variety of ways depending on the nature and scope of the assurance engagement. Regardless of the wording used, the 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 organization-wide.
- 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.

Identifying Governance Activity (Process) Objectives and Analyzing Associated Risks

Governance activity or process objectives are important to understand and will enable the internal auditor to identify and analyze the associated risks and controls. The overall objective of organizational governance is to enhance organizational value and ensure proper management accountability and communication to its key stakeholders.

For each specific governance activity or process, there may be different types of objectives. Generally, objectives can be categorized as: strategic, operational, compliance, and reporting. These are described in The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) *Enterprise Risk Management–Integrated Framework* and can provide useful guidance in identifying and understanding relevant objectives for the specific governance activity or process to be reviewed.

Section 3 introduces general governance practices grouped at the board level and within the organization. Together these activities constitute the governance umbrella over the organization's operations. The appendix provides examples of governance activity objectives and risks at the board level while Section 6 provides similar information for the key governance processes within the organization.

Legal Involvement

Oftentimes the internal auditor will be challenged to interpret application of laws and regulations. Except for

those with law degrees, internal auditors generally do not have the legal background to adequately interpret the more complex legal implications affecting organizational governance. When faced with this situation, the CAE or supervisor of the engagement should involve the legal department or the organization's legal counsel in providing the necessary legal advice. When the area of audit focus is assessment of the organization's legal activity, the CAE should consider use of outside counsel. The CAE should obtain agreement from the board on this.

Engagement Staffing

The nature of the engagement — scope and objectives — will shape the knowledge, skills, competencies, and experience needed to successfully c omplete the engagement. The CAE should identify the knowledge, skills, competencies, and experience needed for the engagement and assign staff that best fits these requirements. Where important gaps exist, the CAE should consider just-in-time training, guest auditors, or a consultant to fill the gaps.

The audit plan should include the program of audits to be completed, the timing of those audits, and the resources needed. CAEs are often challenged with limitations or constraints on resources. Governance audits are high profile, and staffing them often requires individuals with advanced knowledge, skills, competencies, and experience. When using a third-party source for staffing, the CAE should ensure that the staff is both independent and objective.

5.2 Performing the engagement

Sources of Evidence

In providing assurance, internal auditors normally use a two-step approach: review the design and test the operating effectiveness of key activities. The internal auditor should gather sufficient, relevant, and reliable information in carrying out the work and formulating conclusions and recommendations. There are a number of sources to consider in gathering the evidence.

ATTRIBUTE	EVIDENCE TO CONSIDER
Role of the Board	• Legal documents establishing the organization (Articles of "formation," bylaws, etc.). • Legal and regulatory requirements with which the board should comply (acts, statutes, rules, etc.). • 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 include independent auditors, regulators, rating agencies, etc. (for the organization's "watchdogs"). • News sources for any relevant press regarding the organization.

ATTRIBUTE	EVIDENCE TO CONSIDER
Values, Culture, Philosophy	• Ethics and integrity policy – adopted, communicated, affirmation, training. • Mission, vision, values established and communicated. • Whistleblower hotline established, communicated, level of awareness and use, organization response. • Organization personnel surveys confirming individual awareness and understanding. • Organization personnel surveys confirming executive/leadership displays a values culture and philosophy. • New employee training and orientation includes values, culture, and philosophy. • Communication/training exists on ethics and values in "gray areas."
Structures, Arrangements (includes legal documents, policies, standards, charters, etc.)	• 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 (to name a few topics that should be included). • Standards that articulate the "to what level" of performance is to be expected (i.e., 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 and are published, widely known and readily accessible, periodically reviewed and updated as necessary. • Governance committee meeting minutes, actions taken, and reporting. • Examples of governance committees that larger organizations may have include governance, strategy, risk, audit, control, compliance, disclosure, finance, and IT governance/risk. • For larger and more complex organizations, governance structures and organization charts that cascade throughout the organization fully staffed with clear reporting relationships. • Details on governance processes where there is shared accountability, particularly in organizations that use matrix management. • Process details for addressing or approving deviations to policies, standards, and procedures.
Process, Procedures, Process Management (level below organization-wide structures)	• Documentation that identifies all organizational activities, operations, departments, functions, and/or processes. • Documented maps for each process showing inputs, activities, tasks, steps in the process, and outputs. Mapping also should include such references as objectives, customer 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.

ATTRIBUTE	EVIDENCE TO CONSIDER
Goals, Objectives, Strategies, Plans, Risk, Controls	• Current list of organization's goals, objectives, standards, and strategies. • Communication protocols. • Details on alignment throughout 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 goals and objectives and their alignment to the organizational ones. • Performance or reward systems that encourage personnel to achieve organizational goals that are aligned with stakeholder expectations.
People, Capabilities, Accountabilities, Behaviors, Training, Education,	• Job descriptions for all organization personnel that contain position description, responsibilities, authorities, reporting relationships, and education. • Development program/process that applies to all personnel. • Leadership development program/process. • Individual training records that include skills assessments, development plans, and training completed. • Organization-wide training on ethics, integrity, and values. • Succession plans. • Personnel surveys that provide insights into how people view the organization's commitment to people, their capabilities, accountabilities, behaviors, training, and education. • Detailed, board-approved delegated authorities, personnel acknowledgement, periodically reviewed, validations, and remediation process where authorities are breached.

ATTRIBUTE	EVIDENCE TO CONSIDER
Metrics, Measurement, Monitoring (Oversight)	• Documented organizational performance measurement system that illustrates the system and includes description of required information, the form of the reports, reporting periods and due dates, safeguards that ensure accuracy, and completeness. • Copies of actual reports. • Personnel and customer surveys: processes, questions, frequency, audiences, results, responses, and status on 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. • Details on assurance mechanisms that would include: charters, scope, plans, reports, etc. • Benchmarking process and results. • Due diligence evidence/documentation on assessment of third-party governance practices. • External reports with comparisons to relevant internal reports covering governance practices.
Communicate, Inform, Transparency	• External reporting process documentation that evidences legal involvement. • Details on mandatory/required reporting to external parties. • External reports along with documentation evidencing conformance to established procedures. • Disclosure committee charter, roles, responsibilities, meeting minutes. • Internal communication systems up, down, and across the organization. • Surveys/survey questions and results regarding personnel perceptions on quality of information and communication. • Information and communication security/privacy policies, procedures. • Information "asset" management process/program. • Feedback from recipients on quality of communication.
Results, Stakeholder Expectations, Compliance, Objectives	• Financial reports both external and internal. • Regulatory actions. • Internal measurement results such as balanced scorecards. • Civil actions. • Organization news and blogs — what others are saying about the organization. • Analysis, particularly external, comparing actual results to objectives and expectations, both short and longer term.
Automation (Where applicable)	• IT governance/risk/control program and processes. • Defined information security policies, procedures, and practices.

Workpaper Documentation

Because of the sensitivity of some governance audit work, there may be a need for special handling of access and storage of related audit workpapers. Audit workpapers are the property of the organization. The files are under the control of the internal audit activity and are accessible only to authorized personnel. Management review may be granted to substantiate or explain audit findings or to use audit documentation for other business purposes. Where the audit work is completed at the request of the organization's legal counsel, the access and storage of the workpapers may require legal direction. Regardless, the CAE should approve all requests for access to audit workpapers.

5.3 Communicating Outcomes and Results

Internal audit should communicate engagement outcomes and results. Agreement should be reached with the organization's board and executive management on dissemination of all governance-related reports. General counsel's advice should be obtained on the communication of results and retention of related workpapers.

Communicating results should be consistent with Standard 2400: Communicating Results and the related practice advisories and practice guides.

The CAE may be asked to facilitate self-assessments of the board or its committees. The results, including action plans, if any, should be documented so the board can monitor progress. The method for documenting and communicating results will be at the discretion of the board. Options range from a written report to a brief slide presentation.

Assessments of some management governance activities might have legally sensitive results. This possibility should be considered before the assessment begins. It might be prudent to work with the organization's general counsel and do the assessment and related reporting under legal privilege.

If the assessment yields legally or politically sensitive results that were not anticipated, reporting may be formal or informal. Consideration should be given as to which method will get corrective action taken without resulting in unintended negative repercussions. Even if reporting is informal, internal audit must follow the *Standards* in communicating the audit results and in monitoring improvement action progress.

5.4 Monitoring Improvement Action Progress

The CAE should establish a system to monitor the progress on 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 be rigorous. The system should include:

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

5.5 Engagement Administration

Supervision/Quality

Governance audits are high profile and carry with them higher audit risk. The CAE should ensure that these engagements are adequately staffed, properly supervised, and subject to the internal audit quality assurance and improvement process.

If the internal audit activity is to have a key role in assessing governance, its overall effectiveness in providing assurance to stakeholders is critical. The board 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. The CAE should ensure that these reports are provided. In addition, the board will draw its own conclusions on the effectiveness of the internal audit activity.

6.0 Considerations by Specific Governance Activity

6.1 Board

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 communications exist between the organization and its stakeholders. The board should discuss the state of the organization's governance system. It should seek input from the three levels of assurance providers — operating or line management, enterprise-wide functions, and independent activities such as internal audit — and use external assurance providers to validate the three levels' representations and opinions. The board should sponsor periodic evaluations and continuous improvement of governance practices. This can be done through self-assessments and obtaining assistance from the organization's internal audit activity and external assurance service providers. A highly competent and a well-positioned internal audit activity 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 are typically specified in the organization's articles, bylaws, charters, or 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. The organization's legal documents further specify the roles and responsibilities of the board, senior management, and other corporate bodies and functions.

6.2 Strategy

Strategic planning is an organization's process of defining its strategies for achieving its goals and objectives, and making decisions on allocating its resources to pursue its strategies, including its capital and people. Simply put, strategic planning outlines where an organization is going over the next few years and how it is going to get there.

Strategies can exist at different levels in an organization. It starts at the overall organizational level and cascades down through the organization.

> Organization Strategy — At the highest level, it is concerned with the overall purpose and scope of the organization to meet stakeholder expectations. This is the most critical level since it is heavily influenced by stakeholder investment and acts to guide strategic decision-making throughout the organization.
>
> Subsidiary Strategies — These strategies are concerned more with how the organization will successfully operate in a particular "market." It involves strategic decisions about choice of products, meeting needs of customers, gaining competitive advantage, and exploiting or creating new opportunities.
>
> Operational Strategy — At the operating level, these strategies are focused on how each activity or function of the organization will deliver the organization and subsidiary strategies. Operational strategies are much more detailed and key in on resources, processes, people, etc. All discrete activities and/or functions should have operational strategies.

What are some conditions of satisfaction that can be used in evaluating 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, 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, regulators, rating agencies, and capital markets.

The assurance that internal audit provides should align to the above conditions of satisfaction. The assessment is generally not intended to directly question the strategies themselves, but rather the strategic planning process and how well the strategies have been communicated through the organization and adopted at the various levels.

6.3 Enterprise Risk Management

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 — chief risk officer (CRO) — or a CRO with a staff that owns the process and coordinates and project manages risk management activities. Some organizations have assigned specific risk management activities to internal audit. The IIA issued a position paper in 2009 on "The Role of Internal Auditing in Enterprise-wide Risk Management." This position paper 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 internal audit may play, it should not own any risks other than the internal audit risk.

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 The IIA's Practice Guide, Assessing the Adequacy of Risk Management Using ISO 31000. This 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? This Practice Guide includes a basic risk maturity model.

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

6.4 Ethics

Senior management members have primary responsibility for promoting strong ethics. Most important though is the tone at the top they set by their actions and informal

communications. These actions include their own behavior and how they respond when key employees (e.g., 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 are different in some countries than others. Global organizations should decide whether and how much to adapt their global standards to the local culture and make this clear to all concerned.

Internal audit should promote ethical behavior and may play a formal role such as chief ethics officer, compliance officer, or member of an ethics council, as long as such a role does not compromise internal audit's independence.

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 the *effectiveness* (i.e., whether they 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, internal auditors should:

- Get sponsorship and agreement on the evaluation methods from the board and/or 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/or 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' perception of the climate.

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

6.5 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. Internal auditors 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. The scope, however, 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 outsourced to an external provider.

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

6.6 Organizational Accountability

The organization's board and management derive their authorities from the organization's 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 employed 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 board and management, as well as 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 very sensitive area for internal audit to touch upon and underscores the importance of sponsorship.

When assessing accountability, internal audit 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 by key personnel of their accountabilities.
- Processes to monitor accountabilities and corrective actions taken when accountabilities are not met.

6.7 Monitoring

There are a number of 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, customer, internal business operations, employee, leadership, and society and shareholder/stakeholder satisfaction.

By definition, the purpose of monitoring is to provide the board and management with early indications of progress being made in achieving the organization's objectives. Monitoring enables and assists the board and management in making timely decisions. Also, monitoring provides the means for holding people accountable and enables the organization to continually improve performance.

Monitoring should be based on an analysis and prioritization of the risks to achieving organizational objectives and the means by which those risks are mitigated. The monitoring process level risks to consider may include:

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

6.8 IT Governance

The *Standards* Glossary provides the following definition of IT governance: "Consists of leadership, organizational structures, and processes that ensure the enterprise's [IT] supports the organization's strategies and objectives."

IT governance is an extension of the organization's 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 as providing value. The board has oversight responsibility for IT governance. The CAE should ensure that these governance practices are included in the annual program of audits.

There are several widely recognized IT governance frameworks that may be used in establishing the criteria for assessing the part of governance related to IT. 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 – Control Objectives for Information and Related Technology. 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.

Global Technology Audit Guides (GTAGs) are International Professional Practices Framework Practice Guides that provide detailed guidance for conducting internal audit activities. The GTAGs are written in very clear, concise, easy to understand business language. They provide guidance for the more detailed parts of an IT governance review.

Appendix — Board Risks, Control Objectives, Practices

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

Following are examples of risks that can be encountered by boards and controls 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 the board's role and responsibilities in a complete, accurate, and timely manner.	There is a sufficient number of outside, independent members of the board as required by organization need and applicable laws.
		The sufficient number of members and expertise needed for the board is defined in 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.		An orientation and on-boarding 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 readily available. • Updates are made timely. • Changes are adequately communicated.
		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 readily available to board members. • Requirements are continuousLY monitored. • Updates are communicated timely and adequately.
Failure of individual board members to exercise proper due diligence.	To ensure all board policies, procedures, and legal requirements are followed.	A parliamentarian is assigned to monitor and advise on board processes and 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 necessary member terminations.

RISKS/EVENTS	CONTROL OBJECTIVES	PRACTICES
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* procedures are followed in all board meetings.
		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 management actions.
		The board regularly interacts with the internal auditors and the external auditors, at times outside the presence of management, to ensure they are allowed to carry out their mandate in an unrestricted manner.
		There are a sufficient number of nonexecutive directors on the board and attending board meetings.
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, rating agencies) 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 be harmful to the organization's reputation.

RISKS/EVENTS	CONTROL OBJECTIVES	PRACTICES
Decisions are made or actions 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 prior to decisions.
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 to identify primary stakeholder needs on a periodic basis. Primary stakeholders are allowed to attend meetings and ask questions at appropriate times during the meeting.
Failure to properly inform key stakeholders.	To ensure that all mandatory and optional information is communicated accurately and timely to key stakeholders (includes regulatory agencies).	Board reviews and approves all information, reports, and filings prior to release of information to key stakeholders.
Organizational governance structures/ processes/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. Board review and approval of organization code of conduct, ethical culture, policies, and procedures.

Authors and Reviewers

Authors:

Dean Bahrman, CIA

Amipal Manchanda

James Roth, Ph.D., CIA, CCSA, CRMA

Maria Mendes, CIA, CCSA

Reviewers:

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

James Rose, CIA, CRMA, CPA, CISA, CISSP

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

120606