



International Professional
Practices Framework

Implementation Guide 2110

Standard 2110 – Governance

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

- Making strategic and operational decisions.
- Overseeing risk management and control.
- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

Revised *Standards*, Effective 1 January 2017

Getting Started

To fulfill this standard, the chief audit executive (CAE) and internal auditors start by attaining a clear understanding of the concept of governance and the characteristics of typical governance processes. They should also consider the formal definition of governance, as it appears in the glossary of the *International Standards for the Professional Practice of Internal Auditing*, and

become familiar with globally accepted governance frameworks and models (e.g., The Committee of Sponsoring Organizations of the Treadway Commission's frameworks or ISO 31000).

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

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

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

An understanding of governance is the foundation for a discussion with the board and senior management about:

- The definition of governance and the nature of governance processes within the organization.
- The requirements of Standard 2110.
- The internal audit activity's role.
- Any changes to the internal audit activity's approach and plan that may improve its conformance with the standard.

This discussion will help ensure agreement and an alignment of expectations with the board and senior management about what constitutes governance, so that an appropriate internal audit plan and approach can be executed.

Considerations for Implementation

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

- **Making strategic and operational decisions** – To evaluate an organization's governance processes for making strategic and operational decisions, the internal audit activity may review past audit reports as well as board meeting minutes, the board policy manual, or related governance documents, which can help provide an understanding of how such decisions are discussed and ultimately made. This review typically reveals whether established, consistent decision-making processes have been developed. In addition, interviews with departmental heads may reveal what processes led to strategic and operational decisions.
- **Overseeing risk management and control** – To determine how an organization provides oversight of its risk management and control activities, the internal audit activity typically reviews the process for conducting the annual risk assessment. The internal audit activity may also review minutes from meetings wherein risk management strategy was discussed, as well as previously conducted risk assessments, and may interview key risk management personnel such as compliance, risk, and finance officers. The information obtained can be compared to benchmarking and industry trends to ensure all relevant risks have been considered.
- **Promoting appropriate ethics and values within the organization** – To assess how an organization promotes ethics and values, both internally and among its external business partners, the internal audit activity reviews the organization's related objectives, programs, and activities. These could include mission and value statements, a code of conduct, hiring and training processes, an anti-fraud and whistleblowing policy, and a hotline and investigation process. Surveys and interviews may be used to gauge whether the organization's efforts result in sufficient

awareness of its ethical standards and values.

- **Ensuring effective organizational performance management and accountability** – To evaluate how an organization ensures effective performance management and accountability, the internal audit activity could review the organization's policies and processes related to staff compensation, objective setting, and performance evaluation. The internal audit activity may also review associated measurements (e.g., key performance indicators) and incentive plans (e.g., bonuses) to determine whether they are appropriately designed and executed to prevent or detect unacceptable behavior or excessive risk-taking and to support actions aligned with the organization's strategic objectives.
- **Communicating risk and control information to appropriate areas of the organization** – To appraise how well an organization communicates risk and control information to appropriate areas, the internal audit activity could access internal reports, newsletters, relevant memos and emails, and staff meeting minutes to determine whether information regarding risks and controls is complete, accurate, and distributed timely. Surveys and interviews could be used to gauge employees' understanding of their responsibilities over risk and control processes and the impact to the organization if those responsibilities are not fulfilled. Typically, during assurance and advisory engagements, the internal audit activity also evaluates how the area under review communicates risk and control information.
- **Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management** – To assess an organization's ability to coordinate activities and communicate information among the various parties, the internal audit activity could identify the meetings that include these groups (e.g., board, audit committee, and finance committee) and determine how frequently they occur. Members of the internal audit activity may attend the meetings as participants or observers, and they may review the meeting minutes, work plans, and reports distributed among the groups to learn how these parties coordinate activities and communicate with each other.

Internal auditors can act in a number of different capacities to assess and recommend ways to improve governance practices. They may provide independent, objective assessments of the design and effectiveness of governance processes within the organization. In addition to — or instead of — providing assurance, internal auditors may elect to provide consulting services. This may be a preferred approach, particularly when known issues exist or the governance process is immature. Whether providing consulting or assurance services, the CAE may

decide to use continuous monitoring methods, such as assigning internal auditors to observe meetings of governance-related bodies and advise them on an ongoing basis. Usually, a single audit of governance is not attempted. Rather, the internal audit activity's assessment of governance processes is likely to be based on information obtained from numerous audit assignments over time.

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

- The results of audits of the specific governance processes identified above.
- Governance issues arising from audits that are not specifically focused on governance, such as:
 - Strategic planning.
 - Risk management processes.
 - Operational efficiency and effectiveness.
 - Internal control over financial reporting.
 - Risks associated with IT, fraud, and other areas.
 - Compliance with applicable laws and regulations.
- The results of management assessments (e.g., compliance inspections, quality audits, control self-assessments).
- The work of external assurance providers (e.g., legal investigators, government auditor general offices, and public accounting firms) and regulators.
- The work of internal assurance providers, or second line of defense functions (e.g., health and safety, compliance, and quality).
- Other information on governance issues, such as adverse incidents indicating an opportunity to improve governance processes.

During the planning, evaluating, and reporting phases, internal auditors consider the potential nature and ramifications of the results and ensure appropriate communications with the board and senior management.

Considerations for Demonstrating Conformance

Conformance with Standard 2110 may be documented through separate internal audit reports on individual governance processes or an overall report on governance that includes assurance-based assessments and recommendations from consulting services.

Documentation may also include the minutes of a board meeting during which the CAE

discussed the internal audit activity's overall assessment of governance practices. Board meeting materials may provide evidence that the board was appropriately informed about compensation and incentive packages and that it monitored the performance of senior level executives. Statements of acknowledgment, signed by staff and business partners, demonstrate the organization's efforts to promote awareness of its ethics and values.

About The IIA

The Institute of Internal Auditors (The IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 180,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla. For more information, visit www.globaliia.org or www.theiia.org.

About Implementation Guidance

Implementation Guidance, as part of The IIA's International Professional Practices Framework® (IPPF®), provides recommended (non-mandatory) guidance for the internal audit profession. It is designed to assist both internal auditors and internal audit activities to enhance their ability to achieve conformance with the *International Standards for the Professional Practice of Internal Auditing (Standards)*.

Implementation Guides assist internal auditors in applying the *Standards*. They collectively address internal audit's approach, methodologies, and consideration, but do not detail processes or procedures.

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

Disclaimer

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

Copyright

Copyright® 2016 The Institute of Internal Auditors. For permission to reproduce, please contact guidance@theiia.org.