



International Professional
Practices Framework

Implementation Guide 2100

Standard 2100 – Nature of Work

The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

Revised *Standards*, Effective 1 January 2017

Getting Started

Conforming with Standard 2100 requires a thorough understanding of the concepts of governance, risk management, and control, as defined in the *International Standards for the Professional Practice of Internal Auditing*, as well as the individual standards that apply specifically to these concepts: Standard 2110 – Governance, Standard 2120 – Risk Management, and Standard 2130 – Control. It is also important for the internal audit activity to have an understanding of organizational objectives.

Once this understanding has been achieved, the chief audit executive (CAE) usually interviews senior management and the board to understand the roles and responsibilities of each stakeholder with respect to governance, risk management, and control. Typically, the board is

responsible for guiding the governance process, and senior management is accountable for leading risk management and control processes.

Internal auditors need to understand the business to perform meaningful evaluations and may use established governance, risk management, and control frameworks as a guide in their evaluation. In addition, internal auditors may use their knowledge, experience, and best practices to proactively highlight observed weaknesses and make recommendations for improvement.

To assist the internal audit activity in its understanding of the business strategies and risks, the CAE will typically review board and committee charters, meeting agendas and minutes, and the organization's strategic plan. The CAE will also review the organization's mission, key objectives, critical risks, and the key controls used to mitigate such risks to an acceptable level. During this review, the internal audit activity may gain insight into the definitions, frameworks, models, and processes of governance, risk management, and control used by the organization. It may also be helpful for internal auditors to understand the key organizational roles related to the three processes, which may include the chairman of the board, CEO, and other chief officers (e.g., finance, ethics, risk, compliance, human resources, IT), as well as others.

For more information on governance, risk management, and control, please see the implementation guides for standards 2110, 2120, and 2130.

Considerations for Implementation

To start implementing this standard, the CAE typically discusses with the board and senior management the requirements of the standard, roles and responsibilities, and the best strategies for the internal audit activity to evaluate and contribute to governance, risk management, and control efficiently and effectively.

The CAE may document in the internal audit charter any expectations related to the roles, responsibilities, and accountabilities of the board, senior management, and the internal audit activity. This is intended to safeguard the internal audit activity's independence by affirming that senior management and the board are responsible and accountable for governance, risk management, and control, while the internal audit activity is responsible for providing objective

assurance and consulting activities related to the three processes.

To devise an appropriate strategy for assessing the organization's governance, risk management, and control processes, the CAE typically considers the level of maturity of the three processes as well as the organization's culture and the seniority of the individuals who maintain responsibility for the processes. Then, the CAE assesses the risks associated with the three processes. The CAE may use established frameworks adopted by senior management (e.g., The Committee of Sponsoring Organizations of the Treadway Commission's internal control and enterprise risk management frameworks, the King Report on Corporate Governance, or ISO 31000) to guide the assessment. During the assessment, the CAE documents and discusses with senior management any relevant observations and conclusions. The CAE also makes recommendations to strengthen the processes and may escalate significant observations to the board.

If an established framework has not been adopted to guide the organization's governance, risk management, and control processes, the CAE may consider recommending an appropriate framework to guide senior management in their pursuit of enhancing these processes.

Considerations for Demonstrating Conformance

Documentation that may demonstrate conformance with the standard includes the internal audit charter, which documents the internal audit activity's roles and responsibilities related to governance, risk management, and control. Additionally, conformance may be evidenced by the internal audit plan or minutes of meetings in which the elements of the standard were discussed among the CAE, board, and senior management. Engagement plans may demonstrate the internal audit activity's disciplined, systematic, and risk-based approach, and engagement reports may demonstrate the outcome of relevant, value-added results.

Additional evidence of conformance is described in the implementation guides for standards 2110, 2120, and 2130.

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.