International Professional Practices Framework

Implementation Guide 2120

Standard 2120 – Risk Management

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

Interpretation:

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- *Organizational objectives support and align with the organization's mission.*
- *Significant risks are identified and assessed.*
- *Appropriate risk responses are selected that align risks with the organization's risk appetite.*
- *Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.*

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

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 risk appetite, as well as the organization's business missions and objectives. It is also important to attain a complete understanding of the organization's business strategies and the risks identified by management.

Risks may be financial, operational, legal/regulatory, or strategic in nature. The *International Standards for the Professional Practice of Internal Auditing* glossary definition of risk management should be considered, along with risk management frameworks and models published globally. Additionally, Implementation Guide 2100 – Nature of Work may be helpful to attain the foundation necessary to implement Standard 2120.

As this standard tasks the internal audit activity with evaluating the effectiveness of risk management processes, internal auditors will generally attain an understanding of the organization's current risk management environment and the corrective actions in place to address prior risks. It is important to know how the organization identifies, assesses, and provides oversight for risks before internal auditors start to implement Standard 2120.

In its risk assessment, the internal audit activity would consider the organization's size, complexity, life cycle, maturity, stakeholder structure, and legal and competitive environment. Recent changes in the organization's environment (e.g., new regulations, new management staff, new organization structure, new processes, and new products) may have introduced new risks. The CAE may also review the maturity of the organization's risk management practices and determine to what extent the internal audit activity will rely on management's assessment of risk.

Finally, the internal audit activity should have in place an established process for planning, auditing, and reporting risk management issues. Internal auditors will also evaluate risk management during assurance and advisory reviews related to a specific area or process.

Considerations for Implementation

Through the implementation of Standard 2120, the CAE and the entire internal audit activity will ultimately demonstrate their understanding of the organization's risk management

processes and look for opportunities for improvement. Through conversations with senior management and the board, the CAE would consider the risk appetite, risk tolerance, and risk culture of the organization. The internal audit activity should alert management to new risks, as well as risks that have not been adequately mitigated, and provide recommendations and action plans for an appropriate risk response (e.g., accept, pursue, transfer, mitigate, or avoid). Additionally, the internal audit activity should obtain sufficient information to evaluate the effectiveness of the organization's risk management processes.

By reviewing the organization's strategic plan, business plan, and policies, and having discussions with the board and senior management, the CAE can gain insight to assess whether the organization's strategic objectives support and align with its mission, vision, and risk appetite. Interviews with mid-level management may provide additional insight into the alignment of the organization's mission, objectives, and risk appetite at the business-unit level.

Internal auditors should thoroughly explore how the organization identifies and addresses risks and how it determines which risks are acceptable. The internal audit activity will typically evaluate the responsibilities and risk-related processes of the board and those in key risk management roles. To accomplish this, internal auditors may review recently completed risk assessments and related reports issued by senior management, external auditors, regulators, and other sources.

Additionally, the internal audit activity typically conducts its own risk assessments. Discussions with management and the board and a review of the organization's policies and meeting minutes will generally reveal the organization's risk appetite, allowing the CAE and the internal audit activity to align their recommended risk responses. The internal audit activity may consider using an established risk management or control framework (e.g., The Committee of Sponsoring Organizations of the Treadway Commission's frameworks or ISO 31000) to assist in risk identification. To remain current on potential risk exposures and opportunities, the internal audit activity may also research new developments and trends related to the organization's industry, as well as processes that can be used to monitor, assess, and respond to such risks and opportunities.

By taking these steps, internal auditors may independently perform gap analyses to determine whether significant risks are being identified and assessed adequately, and the internal audit activity will be positioned to evaluate management's risk assessment process. When reviewing the risk management process, it is important for internal auditors to identify and discuss the

risks and corresponding responses that have been chosen. For example, management may choose to accept risk, and the CAE would need to determine whether the decision is appropriate, according to the organization's risk appetite or risk management strategy. If the CAE concludes that management has accepted a level of risk that may be unacceptable to the organization, the CAE must discuss the matter with senior management and may need to communicate the matter to the board, in accordance with Standard 2600 – Communicating the Acceptance of Risks. In cases where management chooses to employ a risk mitigation strategy in response to identified risks, the internal audit activity may evaluate the adequacy and timeliness of remedial actions taken, if necessary. This can be achieved via reviewing the control designs and testing the controls and monitoring procedures.

To assess whether relevant risk information is captured and communicated timely across the organization, internal auditors may interview staff at various levels and determine whether the organization's objectives, significant risks, and risk appetite are articulated sufficiently and understood throughout the organization. Typically, the internal audit activity also evaluates the adequacy and timeliness of management's reporting of risk management results. The internal audit activity may review board minutes to determine whether the most significant risks are communicated timely to the board and whether the board is acting to ensure that management is responding appropriately.

Finally, the internal audit activity should take the necessary steps to ensure that it is managing its own risks, such as audit failure, false assurance, and reputation risks. Likewise, all corrective actions should be monitored.

Considerations for Demonstrating Conformance

Documents that may demonstrate conformance with Standard 2120 include the internal audit charter, which documents the internal audit activity's roles and responsibilities related to risk management, and the internal audit plan. Additionally, conformance may be evidenced by minutes of meetings in which the elements of the standard — such as the internal audit activity's risk management recommendations — were discussed among the CAE, the board, and senior management, or meetings between the internal audit activity and relevant committees, task forces, and key senior management.

Risk assessments performed by the internal audit activity and action plans for addressing risks generally demonstrate both the evaluation and improvement of risk management processes, respectively.

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

Copyright