International Professional Practices Framework

Implementation Guide 2600

Standard 2600 – Communicating the Acceptance of Risks

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

Interpretation:

The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk.

Revised Standards, Effective 1 January 2017

Getting Started

To be successful in implementing this standard, the chief audit executive (CAE) must first understand the organization's view of and tolerance for various types of organizational risks. Organizations vary by how much and what types of risk they consider acceptable. For example, some organizations may accept higher levels of financial risk – taking actions such as expanding into a new geography with an unstable government; or making a material investment in an exciting new product that has a relatively small probability of success, but high reward if successful. Other organizations are more averse to such financial risks, avoiding such situations. Further, organizations consider different factors in determining the level of

acceptable risk; for example, the potential impact and likelihood of the risk event, the vulnerability of the organization, and the length of time it takes management to resolve an unacceptable risk.

If the organization has a formal risk management policy, which may include a risk acceptance process, it is important that the CAE and the internal audit activity understand it.

As required by Standard 2500, the CAE also must establish and maintain a system for monitoring the disposition of the results of internal audits.

It is also helpful for the CAE to know how higher risk issues are typically communicated within the organization. Existing policies may define a preferred communication approach; for example, an organization's risk management policy may discuss timeliness, hierarchy of reporting, and similar considerations.

Considerations for Implementation

In monitoring the disposition of results and associated corrective actions, the CAE may become aware of high risk observations that are not timely corrected or may represent more risk than the organization would normally tolerate and are therefore unacceptable to the organization.

However, the ongoing monitoring process is not the only way a CAE identifies unacceptable risk. An effective CAE employs several ways to stay abreast of organizational risks. For example, the CAE may receive information from members of the internal audit activity regarding significant risks they have identified during their assurance or consulting engagements. Or the organization may employ an enterprise risk management (ERM) process to identify and monitor significant risks, and the CAE may be involved with that process. Further, by building and maintaining a collaborative, communicative network with management, the CAE may become aware of an emerging risk area in the organization. CAEs also strive to keep up with industry trends and regulatory changes to help them recognize potential and emerging risks.

Regardless of how the unacceptable risk is identified, if the CAE recognizes the risk as being at such a high level that the organization would normally not tolerate it, and if the CAE believes that the risk is not being mitigated to an acceptable level, then he or she is required to communicate this situation to senior management. Prior to such a communication, the CAE typically discusses the issue with the members of management responsible for the risk area, to share concerns, understand management's perspective, and reach an agreed path to resolve

the risk. However, if such an agreement isn't reached, then the CAE must escalate the concern to senior management. And, after a similar discussion with senior management, if the risk remains unresolved, then the CAE must communicate the issue to the board. It is then the board's decision how to address the concern with management.

The CAE uses judgment to determine how best and how quickly to communicate such matters to whom, based on the issue's nature, urgency, potential ramifications, and any policies that may be in place. For example, should the general counsel be consulted, such as when a law or regulation may have been violated? And should the risk be communicated in private to a senior executive or in a cross-functional meeting with many subject matter specialists in attendance?

This standard applies to highly significant risks that the CAE judges to be beyond the organization's tolerance level. These may include:

- Those that may harm the organization's reputation.
- Those that could harm people.
- Those that would result in significant regulatory fines, limitations on business conduct, or other financial or contractual penalties.
- Material misstatements.
- Fraud or other illegal acts.
- Significant impediments to achieving strategic objectives.

Considerations for Demonstrating Conformance

Evidence of conformance could be found in minutes of meetings where a significant risk issue was discussed with the executive management team, the board, or a risk committee. If the CAE communicates the unacceptable risk situation through one-on-one meetings or during a private session, a memo to file can be used to document the steps taken to alert management and the board. Also, an indirect indication of conformance is a policy in the internal audit manual that describes the requirements of this standard and the organization's reporting process.

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