TONE at the TOP®

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 127 | February 2025

A New Tool to Monitor Established Risks

This month, The IIA released the first in a series of new requirements that will support internal auditors' efforts to better address hot-topic areas. The newest component of The IIA's International Professional Practices Framework (IPPF), the Topical Requirements will ensure all internal audit functions, no matter their size, ownership structure, or location, apply the same audit methodology when assessing the effectiveness of governance, risk management, and controls of a particular topical area.

The Topical Requirements establish a baseline that elevates the work of the internal audit function and the value of the information and insights it provides the board and organization. This Tone will examine the Topical Requirements and what they mean to board members and their organizations.

Pervasive, High-risk Concerns

Internal auditors provide independent, objective assurance and advice to enhance processes and decision-making to maximize value. To ensure auditors have the knowledge and skills required to meet organizations' needs, The IIA regularly enhances and updates its Standards and guidance. Introduction of the Topical Requirements is part of the IPPF evolution project that also includes new Global Internal Audit Standards^{TM} introduced last year, as well as other global guidance.

Topical Requirements are intended for "frequently audited global topics that are typically higher risk and pervasive in nature." Topical Requirements will address mature risk areas and provide guidance based on established best practices. One requirement, on cybersecurity, was released earlier this month, and seven others are in development.

Planned Topical Requirements

Topical Requirements expected to be released in the next few years include:

Cybersecurity	Anti-corruption/bribery
Third-party	People management
Culture	Fraud risk management
Business resilience	Sustainability/ESG

Cybersecurity was given priority as the first Topical Requirement because of organizations' deep dependence on the internet in most or all their activities and due to the need to protect their web-based perimeter.

Internal auditors are well aware of the threat cybersecurity issues pose. In the most recent global IIA Risk in Focus report, internal audit leaders not only cite cybersecurity as the highest risk currently and in the year ahead, but also say they expect it to remain the greatest threat for their organizations over the next three years.

Respondents also are concerned about a related topic, digital disruption, including risks associated with artificial intelligence (AI), generative AI (GenAI), and other emerging technologies. They place digital disruption in the lower end of their top five risks currently and within the coming year, but they move it up to the No. 2 risk when looking ahead over the next three years. While GenAI can enhance threat detection and vulnerabilities, it can also make it easier for bad actors to develop more sophisticated and effective attacks.

Using the Topical Requirements

The Topical Requirements formalize how internal auditors address prevalent risk areas. The requirements:

- Establish a baseline for internal audit functions to use in their efforts to mitigate risk at the organization.
- Are required for relevant assurance services and recommended for consideration for advisory services.
- Require the applicability of a Topical Requirement be determined by a risk-based audit plan. Noting that assessing risk is an important part of the chief audit executive's planning, they call for that determination to be made based on an assessment of the organization's strategies, objectives, and risks.
- Establish a globally consistent approach to auditing within each topic area, which will improve the reliability of internal audit services and results.
- Provide relevant criteria for performing cybersecurity assurance services.
- Are to be applied at the entity or organizational level in areas that have an impact across the organization.
- Identify the pervasive risks that should at least be on an organization's radar.
- Add value by ensuring appropriate cyber risk coverage and consistency.
- Aren't meant to cover all aspects to be considered in an assurance engagement. Rather, they set minimum requirements for a consistent, reliable assessment of the topic.

The requirements are designed to allow internal auditors to use them judiciously. To understand how the requirements can be put to work, consider a situation in which cybersecurity has been identified as a pervasive or extensive risk for the organization during the internal audit planning process, and an audit of the subject will be performed. That is clearly a case in which the Topical Requirement must be applied, but not all cases will be as clear.

Take for example, an internal audit team performing an accounts payable audit that learns about cyber-related risks associated with a web-based purchase order request process. Even if cybersecurity was not identified as an overall organizational risk in the audit plan, internal audit would still apply the Topical Requirement, but more narrowly. The team might spend more time on the cybersecurity controls piece of the audit than on the governance or risk management side. The internal auditors would document their rationale for limiting the engagement to a specific piece.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 255,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit **theiia.org.**

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

Complimentary Subscriptions

Visit **theiia.org/Tone** to sign up for your complimentary subscription.

Reader Feedback

Send questions/comments to **Tone@theiia.org.**

Cybersecurity Governance, Risk Management, and Controls

As noted, the Topical Requirements will cover the governance, risk management, and controls of each topic area. Under the governance umbrella, internal auditors must assess whether the organization's governance processes adequately address cybersecurity. Cybersecurity governance defines related objectives and strategies that advance the company's goals, policies and procedures.

The communication section of the requirement covers what types of materials the board receives on cybersecurity strategy, risk, objectives, and controls, and considers whether strategic initiatives support cybersecurity. This section also covers the policies and procedures and roles and responsibilities created to achieve cybersecurity goals, engagement with stakeholders, and resource requirements to meet cybersecurity goals.

The cybersecurity risk management section establishes the need for a process to identify, analyze, manage, and monitor cyber threats, including a process to quickly escalate recognition of cyber risks. The main goal is to ensure cybersecurity risk management is a priority from an enterprise risk management standpoint.

The cybersecurity controls are processes that are evaluated periodically to mitigate cyber risks. The seven control processes cover important, baseline aspects that internal auditors must evaluate when performing a cybersecurity audit.

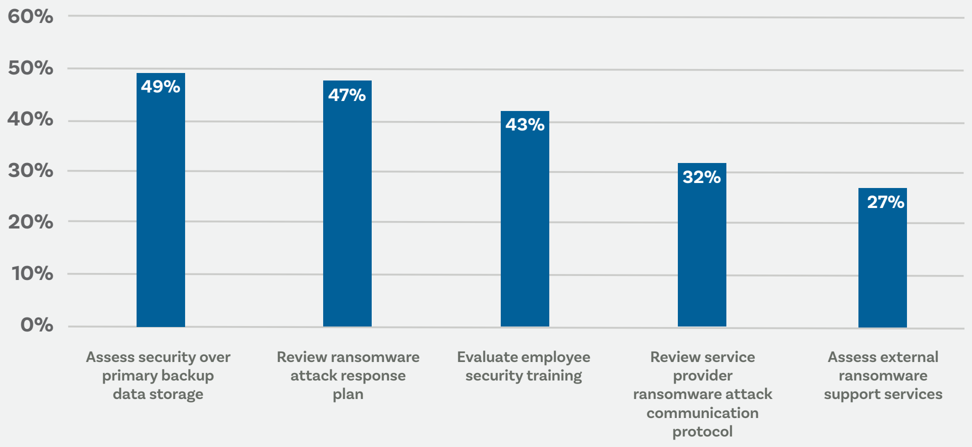
Addressing Common and Evolving Risks

Given their deep and holistic knowledge, internal auditors are uniquely qualified to recognize certain risks that are more likely to impact the organization. The chart "Internal Audit's Involvement in Cybersecurity" shows many of the areas internal audit is already involved in providing assurance and information.

Developed by a global group of internal audit leaders and other experts from a variety of sectors, the Topical Requirements will advance the work of the internal audit profession, enabling auditors to better address common and evolving risks.

Internal Audit's Involvement in Cybersecurity

"The practice of internal audit teams independently assessing information security, either internally or with the help of a third party, has remained consistent year over year," according to consulting and recruiting firm Jefferson Wells. However, the chart below, showing the percentage of companies that use internal audit teams for certain cybersecurity-related engagements, indicates that many organizations aren't taking full advantage of the information and advice that internal audit can provide.

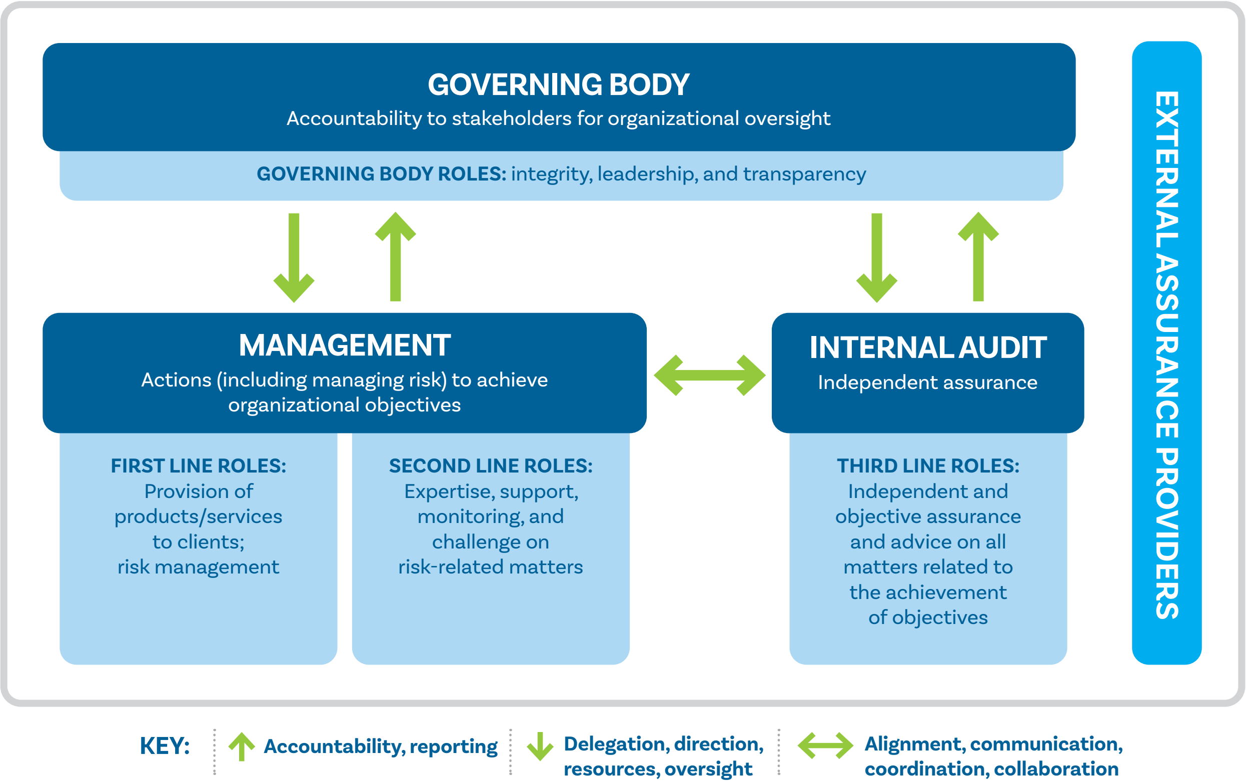


Source: 2024 Internal Audit Priorities Annual Survey, Jefferson Wells.

Topical Requirements Link to the Three Lines Model

The IIA used the Three Lines Model in developing the Topical Requirements. The governance and oversight elements of the requirements relate to the organization's governing body, the risk management element to the second line, the controls and control processes to the first line, and the internal audit function, as the third line, provides independent assurance.

The IIA's Three Lines Model



GOVERNING BODY
Accountability to stakeholders for organizational oversight

GOVERNING BODY ROLES: integrity, leadership, and transparency

MANAGEMENT
Actions (including managing risk) to achieve organizational objectives

FIRST LINE ROLES:
Provision of products/services to clients; risk management

SECOND LINE ROLES:
Expertise, support, monitoring, and challenge on risk-related matters

INTERNAL AUDIT
Independent assurance

THIRD LINE ROLES:
Independent and objective assurance and advice on all matters related to the achievement of objectives

EXTERNAL ASSURANCE PROVIDERS

KEY: ↑ **Accountability, reporting** | ↓ **Delegation, direction, resources, oversight** | ↔ **Alignment, communication, coordination, collaboration**

QUESTIONS FOR BOARD MEMBERS TO ASK

1. What are our greatest vulnerabilities?

2. Which types of cyberattacks might the organization suffer?

3. What types of adversaries might be behind them?

4. What would the adversary be seeking to accomplish — business disruption, theft of data or business information assets, collect a ransom, or some other purpose?

5. How would they carry out an attack?

6. How will we know that an attack has occurred? Are we prepared to make an immediate response?

7. Are we making the best use of the assurance and advice internal audit can offer to address cybersecurity risks?

8. Are we using AI to assist with cybersecurity? If so, in what ways? If not, have we considered the use of AI?