TONE at the TOP

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

Issue 135 | June 2026

Organizational Resilience: A Critical Board Priority

The range of new and developing organizational risks seems to expand every day, creating a constant stream of new challenges. Just a few of the issues that have grown in intensity and impact in recent years are:

- Cybersecurity concerns.
- Geopolitical uncertainty.
- New and rapidly changing economic risks.
- Fast-paced technological developments that offer both risk and opportunity.
- Regulatory and compliance risks.
- Supply chain disruptions.

It is no surprise, then, that business resilience is considered one of the greatest risks organizations are facing, according to the Internal Audit Foundation's 2026 Risk in Focus Global Survey. It was chosen by 47% of internal auditors, behind cybersecurity in first place and digital disruption (including artificial intelligence) in second. In addition, 53% of internal auditors chose business resilience as one of the top three issues on which internal audit spends the most time and effort.

Because of the importance of this topic, The Institute of Internal Auditors has released baseline requirements for its members in an Organizational Resilience Topical Requirement. Compliance with Topical Requirements is mandatory for assurance services and recommended for advisory services. Boards should be aware of this Topical Requirement, not only because it offers valuable direction to internal auditors, but also because it addresses how internal auditors should evaluate governance of organizational resilience.

Risk as a Constant

In ISO 22316:2017 Security and Resilience, the International Organization for Standardization defines organizational resilience as the "ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper."

Organizational resilience means being agile and prepared. It involves identifying risks early and taking quick action to prevent or address them. In severe situations, it also means having disaster recovery plans in place to reduce or contain damage.

According to the Organizational Resilience Topical Requirement User Guide, "In practical terms, resilient organizations are better positioned to survive unexpected challenges and evolve and thrive when faced with them."

While executives might have once seen challenges — including tariffs, protectionism, regulatory fragmentation, cyber threats, and geopolitical conflict — as temporary occurrences, they now see them as "enduring features of the operating environment," according to Top 5 Corporate Governance Priorities for 2026, a report posted by The Conference Board on the Harvard Law School Forum on Corporate Governance. As a result, boards must reconsider former approaches that handled external risk as a periodic review item rather than a standing strategic issue.

"For boards, this environment calls for greater discipline in how resilience is built into governance rather than reliance on ad hoc responses to disruption," according to The Conference Board.

Organizations must build resilience into every function — strategic, operational, technological, human, social, and financial — the Topical Requirement's User Guide notes. At the same time, related strategy decisions may encompass areas throughout the organization, including business continuity, disaster recovery, critical function matrices, succession plans, and recovery tests.

Use Case 1: Part of the Plan

The internal audit function of a public sector entity responsible for a central wholesale market is conducting its annual risk-based planning process. The function has determined that exposure to logistical disruptions, public health events, and critical infrastructure dependencies are threats to essential market operations. Based on this assessment, internal auditors apply the Organizational Resilience Topical Requirement.

To assess governance in this situation, internal auditors review board minutes, strategic plans, and budget documentation to determine whether there are formal, monitored resilience-related objectives. Specifically, internal audit evaluates whether management reports periodically to the governing body on critical vulnerabilities, such as transportation dependencies, infrastructure constraints, and health-related risks. In the absence of a resilience strategy document, internal auditors assess if resilience factors are consistently embedded across operational and strategic documentation.

Use Case 2: A Step Further

At a global professional services firm, internal auditors are performing an engagement on governance and enterprise risk management. They spot vulnerabilities caused by decentralized decision making, reliance on key local leadership, and regulatory exposure in a variety of jurisdictions. They determine that it is appropriate to apply the Organizational Resilience Topical Requirement to the engagement.

In evaluating governance, internal auditors review global policies, board reporting materials, and crisis management protocols to determine whether the company has an effective plan for sustaining operations during regulatory changes, significant turnover of critical personnel, or reputational events in one jurisdiction that may have a broader impact. They also determine whether the board receives consolidated reporting on critical risks across jurisdictions and whether accountability for resilience oversight is clearly defined.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 265,000 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.**

Key Considerations for Governance

The Topical Requirement directs internal auditors to evaluate several key considerations in terms of the governance of organizational resilience, including:

- Is there a formal organizational strategy developed by management that the board has adopted and oversees? Does it cover the operational, technological, and financial elements required to manage change and continue operations? Do resilience objectives align with the organization's overall approach to risk management?
- Does the board periodically review updates from those leading the resilience effort on the achievement of objectives? Items in the review may include risk tolerance triggers, key performance indicators, and other observations or trends. The goal here is to ensure resilience is embedded into strategic oversight, long-term planning processes, succession planning, and the organization's culture, and reflected in the resource and budgetary considerations required to support critical business activities.
- Are there policies and procedures for critical operational, technological, and financial processes that are regularly reviewed, tested, and updated as needed to strengthen the control environment?
- Is there an incident command structure that oversees and supports organizational resilience objectives? Does it include decision-making hierarchies, communication and escalation protocols, and roles and responsibilities?
- Is there a process to periodically validate the competencies needed for resilience success and to reassess the competencies of people in critical resilience roles? The process may encompass identifying relevant training programs and evidence of succession planning for key resilience roles.
- Is there a process to ensure that all relevant internal and external stakeholders are identified, prioritized, and engaged in setting up information and reporting structures intended to achieve organizational resilience objectives? Potential stakeholders include senior management, operations, risk management, IT, supply chain/procurement, facilities, human resources, finance, legal, assurance providers (including internal audit), compliance, public relations, critical vendors, customers, regulators, and others.

The Organizational Resilience Topical Requirement is not necessarily used in every engagement. Internal auditors will use it, for example, when organizational resilience is the subject of an engagement, a topic identified for further consideration during an engagement, or the theme of an engagement not in the audit plan (see Use Cases throughout).

Turn to Internal Audit

Organizational resilience has become a core governance priority, requiring boards to look beyond immediate pressures and prepare their organizations for lasting uncertainty. As an online article posted by the National Association of Corporate Directors notes, "It is becoming difficult for boards and management teams to anticipate and articulate expectations for both the near term and long term." In this environment, directors need reliable insight, independent assurance, and practical guidance to navigate emerging risks and shifting stakeholder expectations.

Internal audit is uniquely positioned to provide that support. As boards and audit committees expand their oversight beyond financial reporting to include cybersecurity, business resilience, enterprise risk management, and AI, internal audit can offer a comprehensive view of organizational preparedness, risk exposure, and control effectiveness.

As highlighted in the Public Company Series: Board Structure and Composition, boards should clearly communicate their expectations of internal audit and leverage its work to gain valuable insight while easing oversight demands on the audit committee. By strengthening this partnership, boards can move from reacting to disruption to building resilience as a sustained organizational capability.

Use Case 3: A Special Request

After a hurricane causes damage nearby, a board member of an entity responsible for critical national infrastructure asks internal audit to add an organizational resilience engagement to its audit plan to examine the organization's exposure to operational interruptions, reliance on specialized contractors, regulatory obligations, and severe environmental events.

To assess governance, internal auditors review the board-approved strategic plan and related documentation to assess whether long-term planning formally considers continuity of critical services. The internal auditors assess whether the board periodically reviews key indicators related to operational availability, maintenance of critical assets, and financial contingency planning, including insurance coverage and reserve allocations.