Organizational Resilience

Topical Requirement

The Institute of
Internal Auditors

Organizational Resilience Topical Requirement

The IIA's International Professional Practices Framework® comprises Global Internal Audit Standards™, Topical Requirements, and Global Guidance. Topical Requirements are mandatory and must be used in conjunction with the Standards, which provide the authoritative basis for the required practices.

Topical Requirements provide clear expectations for internal auditors by setting a minimum baseline for auditing specified risk areas. The organization's risk profile may require internal auditors to consider additional aspects of the topic, including local regulations.

Conformance with Topical Requirements will increase the consistency with which internal audit services are performed and improve the quality and reliability of internal audit services and results. Ultimately, Topical Requirements elevate the internal audit profession.

Internal auditors must apply Topical Requirements in conformance with the Global Internal Audit Standards. Conformance with Topical Requirements is mandatory for assurance services and recommended for advisory services.

The Topical Requirement is applicable when the topic is one of the following:

- The subject of an engagement in the internal audit plan.
- Identified while performing an engagement.
- The subject of a requested engagement that was not on the original internal audit plan.

Not all individual requirements may apply to every engagement, and some may be fulfilled through other approaches. If a requirement is excluded or superseded by other regulatory or contractual requirements or addressed through implementation of procedures in conformance with the Global Internal Audit Standards, the rationale must be documented and retained. Conformance will be evaluated during quality assessments.

For more information, see the Organizational Resilience Topical Requirement User Guide.

Organizational Resilience

Organizational resilience is defined by the International Organization for Standardization as the "ability of an organization to absorb and adapt in a changing environment" (ISO 22316:2017). While this definition establishes a clear aspiration, in practice, organizations vary widely in how they anticipate, respond to, adapt to, and recover from change and disruption. Because organizational resilience spans strategic, operational, technological, human, social, and financial dimensions, some organizations can absorb change effectively, whereas others struggle to do so or may choose different approaches in the face of uncertainty.

Organizational resilience is an umbrella term that addresses risks that may significantly disrupt or impair an organization's ability to deliver its core products and services, maintain stakeholder trust, or fulfill its strategic objectives. These risks may result from sudden-onset events (such as natural disasters, cyberattacks, and geopolitical conflict), prolonged environmental pressures (such as resource scarcity and public health crises), or shifts in the external context (such as technological disruption, regulatory changes, and reputational erosion).

These risks also may be gradual changes or slow-building pressures that, over time, compromise an organization's stability and ability to adapt. Incremental risks like these can be routinely overlooked. Resilient organizations anticipate and adapt to both sudden and subtle risks to be successful.

Inherent risk factors that elevate the threat to resilience include highly complex operations, globalized supply chains, centralized infrastructure or data systems, limited workforce availability, volatile market conditions, and strong dependence on critical third parties or geographic locations. Organizations in high-reliability sectors or those operating under intense regulatory scrutiny may also face risks that are inherently higher due to public impact and compliance obligations.

Organizational resilience focuses on managing risks before, during, and after disruption. Internal auditors commonly assess information technology (IT) processes and controls around business continuity and disaster recovery. A business continuity plan details the steps an organization takes to maintain critical functions and return to normal operational functions when a disaster occurs. A disaster recovery plan describes how organizations will restore their IT systems, critical data, and operations after a disruptive event to resume normal business operations.

Organizational resilience, which includes both of these plans, requires strategic planning, enterprise risk management, effective leadership and culture, and organizationwide control processes. Having strong control processes for organizational resilience not only enables organizations to continuously anticipate, prepare for, respond to, and adapt to change, but also allows them to survive and thrive.

Evaluating and Assessing Organizational Resilience Governance, Risk Management, and Control Processes

This Topical Requirement provides a consistent, comprehensive approach to assessing the design and implementation of organizational resilience governance, risk management, and control processes. The requirements represent a minimum baseline for assessing organizational resilience.

Governance

Requirements

Internal auditors must assess the following aspects of the governance of organizational resilience:

A. A formal organizational strategy that addresses resilience is established by management, adopted and overseen by the board, and includes the operational, technological, and financial elements required to manage change and continue operations. The resilience objectives align with the organization's overall approach to risk management.

B. Updates on the achievement of the resilience objectives are periodically communicated to the board for review. This ensures resilience is embedded into strategic oversight, long-term planning processes, succession planning, and the organization's culture, including in the resource and budgetary considerations required to support critical business activities.

C. Policies and procedures for critical operational, technological, and financial processes are established and periodically reviewed, tested, and updated as needed to strengthen the control environment.

D. An incident command structure is established and used to oversee and support organizational resilience objectives. It includes decision-making hierarchies, communication and escalation protocols, and leadership and operational roles and responsibilities.

E. A process is established to periodically validate the competencies required for resilience success and reassess the competencies of the individuals filling critical roles in resilience processes.

F. A process is established to ensure all relevant internal and external stakeholders are identified, prioritized, and engaged in setting up information and reporting structures for the achievement of organizational resilience objectives. Stakeholders may 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.

Risk Management

Requirements

Internal auditors must assess the following aspects of the risk management of organizational resilience:

A. Risks related to organizational resilience are periodically identified, assessed, and managed across the organization. Resilience risks are mapped to the organization's strategic objectives. The resilience risk management process includes evaluating key processes.

B. Accountability and responsibility for organizational resilience risk management are clearly defined. A designated individual or team is assigned to regularly monitor and report on the management of organizational resilience risks, including the resources necessary for risk mitigation and the identification of emerging threats to organizational resilience.

C. A process is established to monitor organizational resilience risk (emerging or previously identified) levels and quickly escalate those that reach a level considered unacceptable as defined by the organization's established risk management guidelines and risk tolerance or applicable legal and regulatory requirements. The impacts of organizational resilience risk are considered.

D. Management has implemented and periodically tests a process to respond to and recover from occurrences of crises, disruptions, and emergencies. The incident response and recovery process includes detection, prioritization, containment, recovery, and post-incident analysis. The incident response approach includes scenario analyses and periodic stress testing against a range of disruptive events.

Control Processes

Requirements

Internal auditors must assess the following aspects of the control processes related to organizational resilience:

A. A process is in place to identify critical third-party providers (suppliers and vendors) and determine the minimum inventory levels required to sustain essential operations. The process also involves keeping an up-to-date list of alternative suppliers.

B. Data critical for operations is identified and classified. Data classification includes identifying where the data resides, who requires access to it, how it is accessed, and whether it is backed up and recoverable during an emergency.

C. Critical IT controls and continuous monitoring are established to mitigate information security risks (including cyber-related risks) and ensure sensitive data is protected during crises, disruptions, and emergencies. The controls and continuous monitoring include real-time threat intelligence and restricting access to authorized users only.

D. Critical IT assets are inventoried. Assets include the hardware, software, and services required to support operations during crises, disruptions, and emergencies.

E. Business continuity and disaster recovery plans are established and include defined roles for assigned personnel and recovery teams. The plans are tested periodically (for example, a “tabletop exercise”), and the results of testing, including improvement opportunities, are reported to the board and senior management.

F. A process is established to modify the working environment during crises, disruptions, and emergencies.

G. A process is established to continuously monitor and report emerging threats and vulnerabilities that could affect organizational resilience. The process is used to identify, prioritize, and implement opportunities to improve organizational resilience operations, including systems for whistleblowing or gathering risk intelligence.

H. A process is established to educate and train personnel regarding organizational resilience, ensuring they are aware of the policies and procedures to follow and actions to take when crises, disruptions, and emergencies occur. The process includes training exercises in which disruptive scenarios are simulated.

I. A process is established to ensure the necessary operational, human, technological, and financial resources are budgeted and available during crises, disruptions, and emergencies. Financial resources necessary to support organizational resilience are periodically analyzed and communicated to the board.

J. A process is established for reviewing crises, disruptions, and emergencies after they occur and analyzing post-incident reviews through a lessons-learned process, including integrating the lessons into future organizational resilience planning.

About The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) is an 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.

Copyright

April 2026

The Institute of Internal Auditors

Global Headquarters
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-1101