# Public Consultation Draft
# 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.

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:

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

Evidence that each requirement in the Topical Requirement was assessed for applicability must be documented and retained. All individual requirements may not apply in every engagement; if requirements are excluded, a rationale must be documented and retained. Conformance with the Topical Requirement is mandatory and will be evaluated during quality assessments.

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

## Organizational Resilience

Organizational resilience is defined as the "ability of an organization to absorb and adapt in a changing environment," in ISO 22316:2017, *Security and resilience – Organizational resilience – Principles and attributes*, issued by the International Organization for Standardization. Organizational resilience is a broad topic, covering important strategic, operational, technological, human, social, and financial elements. Organizational resilience 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 high operational complexity, 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.

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 return to normal operational functions when a disaster occurs. A disaster recovery plan describes how organizations will protect their IT systems and critical data during an interruption. Organizational resilience also 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 resilience strategy is established and documented by the board, featuring objectives that align with and support the organization's mission and vision. The strategy addresses the operational, technological, and financial elements required to withstand and continue operations amid crises, disruptions, and emergencies and how to subsequently recover and adapt. The strategy aligns with the organization's overall approach to risk management and is periodically tested and updated.

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

C. Critical operational, technological, and financial processes related to organizational resilience have been identified. Policies and procedures for critical processes have been established and are reviewed periodically and updated as needed to strengthen the control environment.

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

E. A process is established to periodically reassess the competencies of the individuals filling critical roles in resilience processes. A succession plan exists and identifies key positions and potential candidates for replacement.

F. A process is established to engage relevant internal and external stakeholders in identifying, analyzing, and responding to existing vulnerabilities and emerging threats that could affect the achievement of organizational resilience objectives. Stakeholders may include senior management, operations, risk management, IT, supply chain/procurement, facilities, human resources, finance, legal, 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. The organization's risk assessment and risk management processes include identifying, analyzing, mitigating, and monitoring threats that could disrupt operations. The risk management strategy for organizational resilience is communicated across the organization and reviewed periodically.

B. Risks related to organizational resilience are periodically assessed and managed across the organization. Risk assessment and management may include the following areas: operations, enterprise risk management, IT, supply chain/procurement, facilities, human resources, finance, legal, compliance, regulatory, public relations, critical vendors, reputation, emerging risks, and others.

C. Accountability and responsibility for organizational resilience risk management are established. An individual or team is identified to periodically monitor and report how organizational resilience risks are being managed, including the resources required to mitigate risks and identify emerging organizational resilience threats.

D. 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 financial and nonfinancial impacts of organizational resilience risk are considered.

E. 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, containment, recovery, and post-incident analysis. The incident response approach includes scenario analyses and periodic stress testing against a range of plausible disruptive events. Results of these exercises are reviewed by the board and senior management, with improvement actions tracked and reported periodically. The recommendations are actionable with clear ownership and timelines.

### *CONTROLS*

**Requirements:**

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

A. A process is established to identify critical third-party providers (suppliers and vendors) and minimum inventory levels needed to continue vital operations. The process includes maintaining a 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 able to be recovered 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. They include the hardware, software, and services required to support operations during crises, disruptions, and emergencies.

E. Business continuity and disaster recovery plans are established. The plans 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. Modifications may include using alternative workplace locations, such as working from home or setting up a temporary office in a timely and efficient manner.

G. A process is established to continuously monitor and report emerging threats and vulnerabilities related to organizational resilience and to identify, prioritize, and implement opportunities to improve organizational resilience operations. The process may include 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 human, technological, and financial resources are budgeted and available during crises, disruptions, and emergencies. The process may include preapproved funding.

J. Financial resources necessary to support organizational resilience are periodically analyzed and communicated to the board. The analysis includes assessing liquidity, insurance coverage, and contingency funding arrangements.

K. 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 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 www.theiia.org.

## Copyright



September 2025