Draft

The Institute of
Internal Auditors

Organizational Resilience Topical Requirement User Guide

Overview of Topical Requirements

Topical Requirements are an essential component of the International Professional Practices Framework® along with the Global Internal Audit Standards™ and Global Guidance. The Institute The Institute of Internal Auditors requires the Topical Requirements to be used in conjunction with the Global Internal Audit Standards, which provide the authoritative basis of the required practices. References to the Standards appear throughout this guide as a source of more detailed information.

Topical Requirements formalize how internal auditors address prevalent risk areas to promote quality and consistency within the profession. Topical Requirements establish a baseline and provide relevant criteria for performing assurance services related to the subject of a Topical Requirement (Standard 13.4 Evaluation Criteria). Conformance with Topical Requirements is mandatory for assurance services and recommended for evaluation during advisory services. Topical Requirements are not intended to cover all potential aspects that should be considered when performing assurance engagements; rather, they are intended to provide a minimum set of requirements to enable a consistent, reliable assessment of the topic.

Topical Requirements clearly link to The IIA's Three Lines Model and the Global Internal Audit Standards. Governance, risk management, and control processes are the main components of Topical Requirements aligning with Standard 9.1 Understanding Governance, Risk Management, and Control Processes. In reference to the Three Lines Model, governance links to the board/governing body, risk management links to the second line, and controls or control processes link to the first line. While management is represented in both the first and second lines, the internal audit function is depicted in the third line as an independent and objective assurance provider, reporting to the board/governing body (Principle 8 Overseen by the Board).

Applicability, Risk, and Professional Judgment

Topical Requirements must be followed when internal audit functions perform assurance engagements on subjects for which a Topical Requirement exists or when aspects of the Topical Requirement are identified within other assurance engagements.

As described in the Standards, assessing risk is an important part of the chief audit executive's planning. Determining the assurance engagements to include in the internal audit plan requires assessing the organization's strategies, objectives, and risks at least annually (Standard 9.4 Internal Audit Plan). When planning individual assurance engagements, internal auditors must assess risks relevant to the engagement (Standard 13.2 Engagement Risk Assessment).

When the subject of a Topical Requirement is identified during the risk-based internal audit planning process and is included in the audit plan, then the requirements outlined in the Topical Requirement must be used to assess the topic within the applicable engagements. In addition, when internal auditors perform an engagement (either included or not included in the plan) and elements of a Topical Requirement emerge, the Topical Requirement must be assessed for applicability as part of the engagement. Lastly, if an engagement is requested that was not originally in the plan and includes the topic, the Topical Requirement must be assessed for applicability.

Professional judgment plays a key role in the application of the Topical Requirement. Risk assessments drive chief audit executives' decisions about which engagements to include in the internal audit plan (Standard 9.4 Internal Audit Plan). Additionally, internal auditors use professional judgment to determine what aspects will be covered within each engagement (Standards 13.3 Engagement Objectives and Scope, 13.4 Evaluation Criteria, and 13.6 Work Program). Appendix A "Practical Application Examples" describes how internal auditors determine whether the Topical Requirement applies.

Evidence that each requirement in the Topical Requirement was assessed for applicability must be retained, including a rationale explaining the exclusion of any requirements. Conformance with the Topical Requirement must be documented using auditors' professional judgment as described in Standard 14.6 Engagement Documentation.

While the Organizational Resilience Topical Requirement provides a baseline of control processes to consider, organizations that evaluate the risk topic as very high may need to assess additional aspects.

If a chief audit executive determines that the internal audit function does not have the required knowledge to perform audit engagements on a Topical Requirement subject, the engagement work may be outsourced (Standards 3.1 Competency, 7.2 Chief Audit Executive Qualifications,10.2 Human Resources Management). Even then, outsourcing does not release the internal audit function from its responsibility for conforming with the Topical Requirements. The chief audit executive retains the ultimate responsibility for ensuring conformance. In addition, if the chief audit executive determines internal audit resources are insufficient, the chief audit executive must inform the board about the impact of insufficient resources and how any resource shortfalls will be addressed (Standard 8.2 Resources).

Performance, Documentation, and Reporting

When applying Topical Requirements, internal auditors also must conform with the Standards, conducting their work in alignment with Domain V: Performing Internal Audit Services. The standards in Domain V describe planning engagements (Principle 13 Plan Engagements Effectively), conducting engagements (Principle 14 Conduct Engagement Work), and communicating engagement results (Principle 15 Communicate Engagement Results and Monitor Action Plans).

Coverage of the Topical Requirement can be documented in either the internal audit plan or the engagement workpapers based on auditors' professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. Evidence that the Topical Requirement was assessed for applicability must be retained, including a rationale explaining any exclusions.

The optional tool in Appendix C can be used as a reference and to document internal auditors' work.

Quality Assurance

The Standards require the chief audit executive to develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the internal audit function (Standard 8.3 Quality). The results must be communicated to the board and senior management.

Communications must report on the internal audit function’s conformance with the Standards and achievement of performance objectives.

Conformance with Topical Requirements will be evaluated in quality assessments. To prepare for a quality review, internal auditors may use the tool provided in Appendix C.

Organizational Resilience

Organizational resilience refers to an organization’s capacity to withstand and adapt to change, especially during times of disruption. According to the ISO 22316 framework from the International Organization for Standardization (ISO), it is defined as the “ability of an organization to absorb and adapt in a changing environment.” In practical terms, resilient organizations are better positioned to survive unexpected challenges and evolve and thrive when faced with them.

Numerous disruptions may prevent an organization from achieving its strategic goals and objectives, including, but not limited to:

- Natural disasters, such as earthquakes, fires, flooding, hurricanes, tsunamis, tropical storms, and other extreme weather events.
- Cyberattacks, such as ransomware, malware, denial of service, data breaches, insider threats, and other malicious actions intended to harm an organization or impede it from conducting operations.
- Geopolitical conflicts, such as economic sanctions, tariffs, terrorism, war, and other conflicts between nations.
- Environmental pressures, such as resource scarcity, public health crises, sustainability factors, or climate change.
- Shifting external factors, such as evolving technology (including artificial intelligence), changes in compliance (legal, regulatory, and financial reporting), employment levels, consumer demand, and reputation.
- Financial challenges, such as inflation or deflation, interest rates, currency exchange rates, and prevailing market conditions, such as recession or economic expansion.
- Operational challenges, such as complex processes, high reliance upon third parties, geographic location, cultural challenges, limited workforce availability, and ineffective leadership or risk management.
- Supply chain issues, such as the inability to source raw materials, lack of diverse suppliers, and volatile commodity pricing.
- Internal events, such as key employee turnover and operational errors.

While the nature of the disruptive event may vary, the organization should have a well-defined resilience strategy and formalized processes to continuously anticipate, prepare for, respond to, and adapt to change.

Requirements of the Organizational Resilience Topical Requirement include:

- **Governance** – clearly defined baseline resilience objectives and strategies that support achievement of the organization’s mission and vision.

- **Risk management** – processes to identify, analyze, manage, and monitor resilience threats, including a process to escalate resilience incidents promptly.
- **Controls** – management-established, periodically evaluated control processes to mitigate resilience risks.

Considerations

Internal auditors may use the following considerations to aid their assessment of the requirements in the Organizational Resilience Topical Requirement. The lettering of each consideration below is cross-referenced to its corresponding requirement in the Topical Requirement. These considerations are illustrative but not mandatory. Internal auditors should rely on professional judgment when determining what to include in their assessments.

For public sector internal audit engagements, it is accepted that internal auditors' scoping as defined by legislation and government structure may restrict some of this work. Internal auditors in the public sector should document such scope limitations as part of their risk assessment process to clearly communicate the tailored scope of their review.

Governance Considerations

To assess how the governance processes are applied to resilience objectives, internal auditors may review evidence of:

A. A formalized, documented, and periodically tested resilience strategy that is formally communicated to all personnel and closely aligns with and supports the organization's mission, vision, culture, and risk management approach. The resilience strategic plan objectives are approved by the board and periodically reviewed. The plan may include operational, technological, and financial elements, such as:

    - Operational – resilience coordination across the organization; resilience risk assessment processes; business continuity planning including periodic testing and reporting; crisis management; workforce adaptability (such as remote-surge capacity, minimum on-site staffing, and cross-training coverage for critical roles) and succession planning for vital personnel; supply chain resilience; and establishment of key performance indicators (KPIs).
    - Technological – information technology infrastructure requirements; identification of critical data (data classification); data backups; cybersecurity hardening and threat monitoring; maintenance of critical technology assets; and defined recovery point objective (RPO) and recovery time objective (RTO) for critical data (validated through restore testing).
    - Financial – budgeted funds allocated to resilience; cash reserves to maintain operations during disruption; financial reporting processes to accurately capture transactions related to disruption; insurance policies to mitigate disruption risks; and availability of credit lines for emergency borrowing.

B. Periodic (such as monthly or quarterly) resilience updates to the board by the person or team that leads organizational resilience, which may include defined risk tolerance triggers, KPIs, or other information to indicate observations or trends. Updates communicate the status of organizational resilience strategy objectives, including strategic oversight, monitoring, and long-term planning. Reporting may include monitoring results on the:

- Achievement of strategic resilience objectives and challenges that may impede achievement.
- Budgetary needs to support resilience goals and objectives, such as technology asset requirements.
- Status of resilience risks, including any significant changes in the resilience risk environment that would impact established risk tolerance levels.
- Effectiveness of resilience internal controls, including remediation progress.
- KPIs to measure resilience success.
- Human resources needed to hire, train, and develop personnel with resilience responsibilities.
- Results of resilience strategy testing along with improvement recommendations.

C. Policies, procedures, and other relevant documentation used to manage operational, technological, and financial resilience processes, including:

- How critical resilience processes are identified and periodically analyzed to determine if the processes continue to accurately reflect the most vital processes.
- Policies are reviewed and updated at least annually (or more frequently based on a higher risk level), and more frequently as required for emerging resilience risks or based on lessons learned from testing or actual disruptive events.
- A review process on the sufficiency of policies and procedures to support resilience operations.
- If resilience processes and internal controls are strengthened by the use of widely adopted frameworks for related processes, such as risk management, information technology, or governance. Examples that may be beneficial to consider include organizations such as NIST, COSO, or ISO, specifically ISO 22300 series (22316 or 22336).

D. An established and documented incident command structure that describes leadership roles and responsibilities related to achieving resilience objectives. Evidence of established decision-making hierarchies, such as personnel responsible for making resilience-related decisions during disruption or the approvals required for operational decisions, such as the disbursement of funds or the ability to legally contract the services of a third party to assist the organization during disruption. Other considerations include documented escalation paths and temporary decision-making authorities during disruption, including financial delegation and third-party contracting thresholds.

E. An established process to periodically (such as annually or semi-annually) assess the knowledge, skills, and abilities of the individuals responsible for operating and managing organizational resilience processes. The process may include identification of training programs, such as live or virtual learning, conferences, on-demand courses, or professional certifications. Evidence of succession planning to identify key resilience roles, including scenario testing to identify activities that can only be performed by one person or a limited number of individuals. The qualifications for replacements are outlined.

F. An established process to identify and engage relevant internal and external stakeholders to identify and respond to existing vulnerabilities and emerging threats that could affect the achievement of organizational resilience objectives. Evidence of stakeholder participation in discussions of resilience vulnerabilities. Evidence may be emails, meeting minutes, or reports, including indications of the use of enterprisewide metrics to measure and monitor resilience effectiveness.

Risk Management Considerations

To assess how risk management processes are applied to organizational resilience objectives, internal auditors may review evidence that:

A. The organization's risk assessment and risk management processes include identifying organizational resilience risks and are performed on a continuous basis, with results communicated across the organization. The processes include identifying, analyzing, mitigating, and monitoring resilience threats that could disrupt business operations, including how threats and vulnerabilities are:

- Initially identified and reported.
- Analyzed to evaluate the risk of achieving organizational objectives.
- Mitigated, including action plans to reduce risk to an acceptable level.
- Monitored, including a plan for ongoing reporting until threats are fully resolved.

B. Organizational resilience risk management is conducted across the organization and documented as to how risks were identified, ranked, monitored, and managed. Documentation exists through reports, emails, or meeting minutes indicating the areas of the business participating. Risk factors such as impact, likelihood, velocity, and other aspects may be included. Highly correlated or interdependent risk factors may be analyzed to determine the cumulative impact of multiple risk exposures. The risk assessment may include the evaluation of the layers of critical asset protection and resources to prevent a single point of failure. The risk assessment may be updated by incorporating lessons learned from actual crises, disruptions, and the results of tests and scenarios. The organization should prioritize the areas that pose the highest risk based on the potential impact and likelihood from its business impact analysis.

C. The organization has assigned and periodically reviews accountability and responsibility to an individual or team to monitor and report on resilience risks. The individual or team comprises qualified individuals who have experience in managing resilience, ideally within the organization's industry (such as health care, financial services, public sector). The individual or team participates in periodic training to ensure they are aware of emerging resilience risk trends.

D. The organization has established a process to monitor organizational resilience risks (emerging or previously identified) and quickly escalate those that reach a level considered unacceptable as defined by the organization's established risk management guidelines and risk tolerance, or by applicable legal and regulatory requirements. Impacts on organizational resilience risk from financial and nonfinancial measures are considered. Examples of financial measures include revenue, expenses, profitability, cash flow, debt, stock price, and overall value. Examples of nonfinancial measures include brand reputation, customer satisfaction, environmental implications, and personnel turnover. The process includes:

- Initial identification of risk and timely escalation.
- Analysis to evaluate the risk and how it could prevent the achievement of organizational objectives.
- Proposed and agreed upon risk mitigation action plans, including how to reduce risk to an acceptable level in a timely manner. Action plans are based on the overall enterprise risk management strategy. The proposal should include necessary risk mitigation resources, such as financial, personnel hours, and additional technology and software needed to increase capabilities.
- Ongoing risk monitoring and reporting on key risk indicators until threats are fully resolved.

E. The organization has implemented a process to respond to and recover from crises, disruptions, emergencies, or other incidents. The process is fully tested periodically, such as quarterly or annually, and may include more frequent partial testing, such as monthly or quarterly. Critical services may require more frequent testing. The incident response and recovery process includes:

- Detection – Continuous monitoring for cyber events may include the use of an intrusion detection system, threat intelligence, or security information and event management (SIEM). The SIEM may include the use of artificial intelligence to strengthen the process. For natural disasters or facility failures, the organization has established a communication network (such as alert protocols or notifications) for timely awareness and information sharing. For all events, the organization has defined a process to notify applicable emergency responders and legal authorities. Events should be prioritized based on criticality.
- Response and Containment – To prevent further damage during cyber events, the organization has implemented a process to isolate compromised assets, such as re-routing network traffic or limiting user access during an event. For physical events, the organization has implemented a process to physically isolate disruptive events to limit the impact, including relocating employees to an alternate location.
- Recovery – For cyber- or IT-related events, the organization has established procedures to prioritize recovery of critical assets that are needed to resume operations (such as restoring data from backups or bringing servers back online). Other non-IT resources that are required to resume operations should also be prioritized for recovery. This may include planning gradual return for key personnel or core functions.
- Post-incident analysis – The organization analyzes events to determine:
    - Root causes of disruptive events.
    - Effectiveness of actions taken.

- Improvements required to strengthen resilience processes, such as updating policies, procedures, risks, or strategy among others.

The response and recovery processes should be tested for their rigor and effectiveness through tabletop exercises, simulations, and drills covering critical services/functions and their dependencies. The testing may be aligned with organizational risk tolerance levels. The incident response approach includes scenario analyses and periodic stress testing against a range of plausible disruptive events. These events can be from internal or external incidents. Results of these exercises may be reviewed by the board and senior management, with improvement actions tracked and reported periodically. Recommendations should be actionable, with clear ownership and timelines.

Control Process Considerations

To assess how control processes are applied to organizational resilience objectives, internal auditors may review evidence that:

A. A process is in place to identify and assess critical third-party providers (suppliers and vendors) and minimum inventory levels needed to continue vital operations. The assessment may consider third-party resilience and business continuity and include risk ratings for each vendor. In addition to reviewing vendors before entering into a formal agreement, the organization may review vendors periodically to continually evaluate risk ratings. The organization should maintain a listing of potential replacement vendors in the event a vendor relationship ends.

B. Management has performed a data classification exercise, in particular identifying critical data that is required to recover from disruptive events and maintain operations. The organization has implemented effective internal controls to protect critical data, such as limiting access to authorized personnel and ensuring critical data is backed up and can be recovered timely.

C. Management has established critical IT controls and continuous monitoring processes to mitigate information security risks (including cyber-related risks) and ensure sensitive data is protected during disruptive events. Encryption should be used to protect sensitive data. Continuous monitoring and real-time threat intelligence provide alerts to management and issues are resolved timely. Widely adopted control frameworks, such as NIST, COBIT, ISO, and others, may be used.

D. The organization has inventoried critical IT assets, including hardware, software, and services required to support operations during crises, disruptions, and emergencies. IT assets that are more difficult to acquire quickly are identified as high priority.

E. A business continuity plan and a disaster recovery plan are established and identify personnel for recovery teams, which are based on business impact analysis. The plans are tested periodically (such as quarterly or annually) through tabletop exercises or stress testing, where disruptions simulate real emergencies and include testing of communication protocols with both internal and external stakeholders. The results of testing, including improvement opportunities, are reported to the board and senior management.

F. A process is in place to support the organization in modifying working environments during disruptive events. Modifications may include using alternative workplace locations, such as working from home or setting up a temporary office in a timely and efficient manner. The organization may use hybrid or remote working options to replace on-site work. Other aspects may include protocols on mobilization and reallocation of resources, ranging from IT resources, human resources, and others, in a timely and efficient manner.

G. A process is in place 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. Monitoring activities may include key risk indicators (KRIs), risk dashboards, or risk horizon scanning exercises. The organization may provide updates to all employees regarding emerging threats to raise the level of awareness, including mitigation measures or controls. All whistleblower activity is logged, analyzed, resolved timely, and communicated to senior management. Ongoing monitoring may be necessary to resolve issues, which will require additional reporting.

H. A process is in place to educate and train personnel on organizational resilience policies and procedures to follow when crises, disruptions, and emergencies occur. The process includes training exercises that simulate disruptive scenarios. Training should be conducted periodically, such as quarterly or annually. Critical services may need to be tested more frequently.

I. A process is in place to ensure the necessary human, technological, and financial resources are budgeted and available during crises, disruptions, and emergencies. The process may include preapproval of funding. Management may need to periodically, such as quarterly or annually, review resources to ensure they are adequate based on perceived risk levels. Critical services may need to be tested more frequently.

J. Management has identified and analyzed financial resources necessary to support organizational resilience and communicated the needs to the board. The analysis includes assessing liquidity, insurance coverage, and contingency funding arrangements. Financial resource requirements should be planned based on factors such as the organization’s size, complexity, industry, and risk profile.

K. A process is in place for reviewing crises, disruptions, and emergencies after they occur and analyzing post-incident reviews through a lessons-learned process. The reviews should be documented in formal reporting and the lessons learned integrated into future resilience planning.

Appendix A. Practical Application Examples

The IIA's "Topical Requirements Application Guidance" provides practical advice on navigating mandatory requirements, addressing limitations, and identifying critical risk thresholds. In addition to the application guide, the following examples describe scenarios in which the Organizational Resilience Topical Requirement would be applicable.

Example 1: Organizational resilience is identified for an internal audit engagement included in the internal audit plan.

When the internal audit function completes its risk-based planning process and includes one or more engagements on organizational resilience in the internal audit plan, the Topical Requirement is mandated when conducting such engagements. Conformance may be achieved by including the requirements across one or more engagements in the internal audit plan.

Organizational resilience is a broad topic, and not every requirement in the Topical Requirement may apply in every engagement. When internal auditors apply professional judgment and determine that one or more requirements of the Organizational Resilience Topical Requirement are not applicable and therefore should be excluded from an engagement, internal auditors must document and retain the rationale for excluding those requirements. For example, the rationale for excluding some requirements could be that the internal audit function performs various organizational resilience engagements on a rotational basis or has determined that the risk's significance in the engagement is low.

Example 2: Organizational resilience risks are identified during an audit engagement that is not focused on organizational resilience.

Internal auditors may identify resilience risks while assessing a process not directly related to resilience. For example, internal auditors may be assessing the human resource processes (such as hiring and retaining personnel) in an engagement not focused on organizational resilience and do not identify resilience risks as within the scope when planning the engagement. However, after performing the initial walkthrough, internal auditors determine that such risks should be in scope; for example, they identify succession planning risks related to how the organization retains personnel (Standard 13.2 Engagement Risk Assessment).

Once relevant risks have been identified, internal auditors must review the Organizational Resilience Topical Requirement and determine which requirements are applicable. In this example, they might only focus on requirement E in Governance and exclude the other risk management and control requirements. They must document in the engagement workpapers the rationale for excluding the other requirements of the Organizational Resilience Topical Requirement and retain the documentation.

Example 3: An organizational resilience engagement that was not originally included in the internal audit plan is requested.

Stakeholders such as the board, management, or a regulator may ask internal auditors to perform resilience assessments outside the original audit plan. For example, when organizations are the target of a cyberattack, the board may request an internal audit engagement to assess resilience controls to evaluate how well the organization is prepared to recover from a cyberattack. The Topical Requirement is applicable, the requirements must be assessed, and any exclusions documented.

Appendix B. Mapping to Frameworks

The organization may have its own organizational efforts, using frameworks such as those from ISO. Internal auditors may have already developed audit programs and testing procedures based on these frameworks. Internal auditors should reconcile their intended organizational resilience control testing to the Topical Requirement to ensure adequate coverage. The chart below maps the Organizational Resilience Topical Requirement to the ISO 22336 Framework. Additional framework references are listed in Appendix D.

Governance Requirements	ISO 22336 Framework
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.	4.1; 6.1; 6.2; 7.1; 8.4; 8.5; 9.1; 9.5
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.	6.4; 8.6; 10.2
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.	4.2; 6.3; 8.3; 8.4; 9.4
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.	5.4
E. A process exists 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.	9.6
F. A process is in place 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, information technology (IT), supply chain/procurement, facilities, human resources, finance, legal, compliance, public relations, critical vendors, customers, regulators, and others.	9.2; 9.5

Risk Management Requirements	ISO 22336 Framework
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.	7.5; 9.2; 9.3
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.	4.4; 5; 7.3; 7.4; 7.6
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.	4.3; 8.2; 9.6
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.	7.2; 7.6; 10.1
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.	7.2; 7.6; 7.8

Control Process Requirements	ISO 22336 Framework
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.	7.7
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.	6.1
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-	7.5

	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.	9.2
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.	8.6; 9.6; 10.3
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.	9.3
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.	7.6
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.	10.2; 10.3
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.	9.6
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.	6.4; 7.6
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.	10.2; 10.3

Appendix C. Optional Documentation Tool

Internal auditors are expected to exercise professional judgment in determining the applicability of the requirements based on the risk assessment and appropriately document the exclusions of certain requirements. The Topical Requirement can be documented in the internal audit plan or in the engagement workpapers based on the auditor's professional judgment. One or more internal audit engagements may cover the requirements. In addition, not all requirements may be applicable. This printable form provides one option for documenting conformance with the Organizational Resilience Topical Requirement, but its use is not mandatory

Organizational Resilience - Governance

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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 exists 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 in place 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, information technology (IT), supply chain/procurement, facilities, human resources, finance, legal, compliance, public relations, critical vendors, customers, regulators, and others.		

Organizational Resilience – Risk Management

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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.		

Organizational Resilience – Control Processes

Requirement	Executed Coverage or Rationale for Exclusion	Documentation Reference
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. 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.		

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.		

Appendix D. Expanded Mapping to Other Frameworks

Area	ISO Reference	Scope/Clause headings
Governance	ISO 22316:2017	Policy and strategy; leadership commitment; shared vision; culture; communication; continual improvement.
Risk management	ISO 31000:2018	Scope/context/criteria; risk assessment; treatment; monitoring; communication.
Business continuity/disaster recovery foundations	ISO 22301: 2019; ISO/TS 22317:2021	BCMS context, leadership, planning, operation; BIA activities and outputs.
Supply chain resilience	ISO/TS 22318:2021	Supplier dependency analysis; continuity strategies; alternates; assurance requirements.
Information and communication technology readiness	ISO/IEC 27031	ICT continuity; recovery objectives; testing and improvement; BCMS alignment.

About The Institute of Internal Auditors

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 www.theiia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

October 2025