Resilienz von Organisationen

Topical Requirement

User Guide

The Institute of Internal Auditors

Übersetzung durch DIIR Deutsches Institut für Interne Revision e.V.

Inhalt

Überblick über die Topical Requirements

Die Topical Requirements sind ein wesentlicher Bestandteil der Internationalen Grundlagen für die berufliche Praxis (International Professional Practices Framework®), zusammen mit den Global Internal Audit Standards™ und Global Guidance. Das Institute of Internal Auditors fordert, dass die Topical Requirements in Verbindung mit den Standards angewendet werden, die die maßgebliche Grundlage für die geforderten Praktiken darstellen. Dieses Dokument enthält Referenzierungen zu den Standards als Quelle für ausführlichere Informationen.

Die Topical Requirements formalisieren die Art und Weise, wie Interne Revisorinnen und Revisoren allgegenwärtige Risikobereiche angehen, um die Qualität und Konsistenz innerhalb des Berufsstandes zu fördern. Das Mandat der Internen Revision definiert klar den Umfang und die Arten der von der Internen Revision erbrachten Leistungen, darunter auch die Berücksichtigung der Topical Requirements (Standard 6.1 „Mandat der Internen Revision“). Topical Requirements bilden eine Grundlage und liefern relevante Kriterien für die Durchführung von Prüfungsleistungen, die sich auf den Gegenstand eines Topical Requirement beziehen (Standard 13.4 „Bewertungskriterien“). Die Einhaltung der Topical Requirements ist für Prüfungsleistungen verbindlich und wird für die Bewertung bei Beratungsleistungen empfohlen. Es ist nicht die Absicht der Topical Requirements, alle potenziellen Aspekte abzudecken, die bei der Durchführung von Prüfungsaufträgen zu berücksichtigen sind. Sie sollen vielmehr einen Mindestsatz an Anforderungen bereitstellen, um eine konsistente, zuverlässige Beurteilung des Themas zu ermöglichen.

Die Topical Requirements sind klar mit dem Drei-Linien-Modell des IIA und den Global Internal Audit Standards verlinkt. Governance, Risikomanagement und Kontrollprozesse sind, in Übereinstimmung mit Standard 9.1 „Verstehen von Governance-, Risikomanagement- und Kontrollprozessen“, die Hauptbestandteile der Topical Requirements. In Verbindung mit dem Drei-Linien-Modell beziehen sich Governance auf Leitungs- und Überwachungsorgane, Risikomanagement auf die zweite Linie und Kontrollen oder Kontrollprozesse auf die erste Linie. Das Management ist sowohl in der ersten als auch in der zweiten Linie vertreten. Die Interne Revision stellt als unabhängiger und objektiver Assurance Provider, der den Leitungs- und Überwachungsorganen Bericht erstattet, die dritte Linie dar (Prinzip 8 „Aufsicht durch das Leitungs- und Überwachungsorgan").

Anwendbarkeit, Risiko und professionelles Urteilsvermögen

Topical Requirements müssen befolgt werden, wenn Interne Revisionen Prüfungsaufträge zu Themen durchführen, für die es ein Topical Requirement gibt, oder wenn Aspekte des Topical Requirement in anderen Prüfungsaufträgen identifiziert werden.

Wie in den Standards beschrieben, ist die Risikobeurteilung ein wichtiger Teil der Planung durch die Revisionsleitung. Die Festlegung der in den Revisionsplan aufzunehmenden Prüfungsaufträge erfordert eine mindestens jährliche Beurteilung der Strategien, Ziele und Risiken der Organisation (Standard 9.4 „Revisionsplan“). Bei der Planung einzelner Prüfungsaufträge müssen die Internen Revisorinnen und Revisoren die für den Auftrag relevanten Risiken beurteilen (Standard 13.2 „Risikobeurteilung zu einem Auftrag“).

Wenn der Gegenstand eines Topical Requirement während des risikobasierten Planungsprozesses der Internen Revision identifiziert und in den Revisionsplan aufgenommen wird, müssen die im Topical Requirement dargelegten Anforderungen zur Beurteilung des Themas im Rahmen der betroffenen

Aufträge angewendet werden. Zusätzlich muss das Topical Requirement im Rahmen eines Auftrags auf seine Anwendbarkeit hin beurteilt werden, wenn die Interne Revision einen (im Plan enthaltenen oder nicht im Plan enthaltenen) Auftrag durchführt und Elemente des Topical Requirement identifiziert werden. Außerdem muss das Topical Requirement auf seine Anwendbarkeit hin beurteilt werden, wenn ein Auftrag erteilt wird, der ursprünglich nicht im Plan vorgesehen war und das Thema umfasst. (Siehe Standard 9.4 zu Änderungen des Revisionsplans.)

Bei der Anwendung des Topical Requirement spielt die professionelle Beurteilung eine wichtige Rolle. Risikobeurteilungen sind die Grundlage für Entscheidungen von Revisionsleitungen, welche Aufträge in den Revisionsplan aufgenommen werden sollen (Standard 9.4). Darüber hinaus nutzen Interne Revisorinnen und Revisoren ihre professionelle Beurteilung, um zu entscheiden, welche Aspekte im Rahmen der einzelnen Aufträge abgedeckt werden sollen (Standards 13.3 „Auftragsziele und Auftragsumfang“, 13.4 „Bewertungskriterien“ und 13.6 „Arbeitsprogramm“), und um die Ressourcen zu identifizieren, die notwendig sind, um die Auftragsziele zu erreichen (Standard 13.5 „Auftragsressourcen“). In Anhang A „Anwendungsszenarien“, wird beschrieben, wie Interne Revisorinnen und Revisoren das Topical Requirement anwenden.

Nicht alle einzelnen Anforderungen treffen auf jeden Auftrag zu. Einige können durch andere Ansätze erfüllt werden. Wenn eine Anforderung wegen anderer gesetzlicher oder vertraglicher Anforderungen ausgeklammert oder ersetzt wird, oder wenn es durch die Umsetzung von Verfahren in Übereinstimmung mit den Global Internal Audit Standards erfüllt wird, muss die Begründung dafür dokumentiert und aufbewahrt werden. Die Einhaltung wird im Rahmen von Qualitätsbeurteilungen beurteilt.

Die Einhaltung des Topical Requirement muss unter Nutzung des professionellen Urteils der Prüferinnen und Prüfer dokumentiert werden, wie in Standard 14.6 „Auftragsdokumentation“ beschrieben.

Das Topical Requirement „Resilienz von Organisationen“ liefert eine Grundlage für die zu berücksichtigenden Kontrollprozesse. Aber Organisationen, die dieses Risikothema als sehr hoch einschätzen, müssen möglicherweise zusätzliche Aspekte beurteilen.

Wenn die Revisionsleitung feststellt, dass die Interne Revision nicht die erforderlichen Kenntnisse für die Durchführung von Revisionsaufträgen zu einem Thema der Topical Requirements besitzt, kann der Auftrag an einen externen Dienstleister vergeben werden (Standards 3.1 „Kompetenz“, 7.2 „Qualifikation der Revisionsleitung“, 10.2 „Management personeller Ressourcen“). Für die Revisionsleitung kann das Internal Auditing Competency Framework™ des IIA eine hilfreiche Ressource sein. Die Standards gelten für jede Einzelperson oder Funktion, die Leistungen der Internen Revision erbringt, unabhängig davon, ob eine Organisation Interne Revisorinnen und Revisoren direkt beschäftigt, sie über einen externen Dienstleister beauftragt oder beides. Die Verantwortung für die Einhaltung der Anforderungen verbleibt bei der Revisionsleitung. Stellt die Revisionsleitung fest, dass die Ressourcen der Internen Revision nicht ausreichen, muss sie das Leitungs- und Überwachungsorgan über die Auswirkungen der unzureichenden Ressourcen informieren und darlegen, wie mit etwaigen Ressourcenmängeln umgegangen werden soll (Standard 8.2 „Ressourcen“).

Durchführung, Dokumentation und Berichterstattung

Bei der Anwendung der Topical Requirements müssen Interne Revisorinnen und Revisoren auch die Standards einhalten und ihre Tätigkeiten im Einklang mit Domain V („Erbringung von Revisionsleistungen“) durchführen. Die Standards in Domain V beschreiben die Planung von Aufträgen (Prinzip 13 „Plane Aufträge wirksam“), die Durchführung von Aufträgen (Prinzip 14 „Führe die Auftragsarbeiten aus“) und die Kommunikation von Auftragsergebnissen (Prinzip 15 „Kommuniziere Auftragsergebnisse und überwache Maßnahmenpläne“).

Topical Requirements sind entwickelt worden, um konsistente und qualitativ hochwertige Revisionspraktiken zu unterstützen. Sie sind in Verbindung mit den geltenden lokalen Gesetzen, Vorschriften, aufsichtsrechtlichen Erwartungen und anderen fachlich anerkannten Rahmenwerken anzuwenden, die zusätzliche oder spezifischere Anforderungen auferlegen können. Interne Revisorinnen und Revisoren haben möglicherweise bereits Arbeitsprogramme und Prüfungsverfahren auf der Grundlage dieser Vorschriften und Rahmenwerke entwickelt. Sie sollten ihre geplanten Prüfungshandlungen zur Resilienz von Organisationen und alle zuverlässigen Prüfungshandlungen anderer interner und externer Assurance Provider (Standard 9.5 „Koordination und Vertrauen“) mit den Topical Requirements abgleichen, um eine angemessene Abdeckung sicherzustellen.

Die Abdeckung des Topical Requirement kann auf Grundlage der professionellen Beurteilung der Prüferinnen und Prüfer entweder im Revisionsplan oder in den Arbeitspapieren des Auftrags dokumentiert werden. Die Anforderungen können von einem oder mehreren Revisionsaufträgen abgedeckt werden. Darüber hinaus sind möglicherweise nicht alle Anforderungen anwendbar. Der Nachweis, dass das Topical Requirement auf seine Anwendbarkeit hin geprüft wurde, muss, einschließlich einer Begründung für etwaige Ausschlüsse, aufbewahrt werden.

Das optionale Tool in Anhang D kann als Referenz und zur Dokumentation der Tätigkeiten der Internen Revisorinnen und Revisoren verwendet werden.

Qualitätsprüfung

Die Standards verlangen, dass die Revisionsleitung ein Programm zur Qualitätssicherung und Verbesserung entwickelt, umsetzt und aufrechterhält, das alle Aspekte der Internen Revision abdeckt (Standards 8.3 „Qualität“, 8.4 „Externe Qualitätsbeurteilung“, 12.1 „Interne Qualitätsbeurteilung“). Die Ergebnisse sind der Geschäftsleitung und dem Überwachungsorgan mitzuteilen. In der Kommunikation muss über die Einhaltung der Standards durch die Interne Revision und die Erreichung der Leistungsziele berichtet werden.

Die Einhaltung der Topical Requirements sollte in der Beaufsichtigung auf Auftragsebene (Standard 12.3 „Überwachung und Verbesserung der Leistung bei der Durchführung von Aufträgen“) berücksichtigt werden und wird im Rahmen von Qualitätsbeurteilungen beurteilt. Zur Vorbereitung auf eine Qualitätsprüfung können Interne Revisorinnen und Revisoren das Tool in Anhang D verwenden.

Resilienz von Organisationen

Resilienz von Organisationen bezieht sich auf die Fähigkeit einer Organisation, Veränderungen standzuhalten und sich daran anzupassen, insbesondere in Zeiten von Disruptionen. Gemäß dem ISO 22316 Rahmenwerk der International Organization for Standardization ist sie definiert als „die Fähigkeit einer Organisation, sich an ein sich veränderndes Umfeld anzupassen“. Diese Definition gibt ein klares Ziel vor, aber es gibt in der Praxis große Unterschiede in der Art und Weise, wie Organisationen Veränderungen und Störungen antizipieren, auf sie reagieren, sich anpassen und sich davon erholen. Da die Resilienz von Organisationen strategische, betriebliche, technologische, menschliche, soziale und finanzielle Dimensionen umfasst, können einige Organisationen Veränderungen wirksam auffangen, während andere damit Schwierigkeiten haben oder angesichts der Unsicherheit andere Ansätze wählen.

In der Praxis sind resiliente Organisationen besser in der Lage, unerwartete Herausforderungen zu überstehen und sich weiterzuentwickeln, wenn sie mit ihnen konfrontiert werden.

Zahlreiche Disruptionen können eine Organisation daran hindern, ihre strategischen Ziele zu erreichen, unter anderem:

- Naturkatastrophen, wie Erdbeben, Brände, Überschwemmungen, Wirbelstürme, Tsunamis, Tropenstürme und andere extreme Wetterereignisse.
- Cyberangriffe wie Ransomware, Malware, Denial-of-Service-Angriffe, Datenschutzverletzungen, Insider-Bedrohungen und andere böswillige Handlungen, die darauf abzielen, einer Organisation zu schaden oder sie an der Ausübung ihrer Aktivitäten zu hindern.
- Geopolitische Konflikte, wie Wirtschaftssanktionen, Zölle, Terrorismus, Krieg und andere Konflikte zwischen Nationen.
- Umweltbelastungen wie Ressourcenknappheit, Gesundheitskrisen, Nachhaltigkeitsfaktoren oder Klimawandel.
- Sich verändernde externe Faktoren, wie sich entwickelnde Technologien (einschließlich künstlicher Intelligenz), Änderungen bei der Einhaltung von Vorschriften (gesetzliche, regulatorische und bezüglich der Finanzberichterstattung), Beschäftigungsniveau, Verbrauchernachfrage und Reputation.
- Finanzielle Herausforderungen, wie Inflation oder Deflation, Zinssätze, Wechselkurse und vorherrschende Marktbedingungen, wie Rezession oder Wirtschaftswachstum.
- Operative Herausforderungen wie komplexe Prozesse, hohe Abhängigkeit von Drittparteien, geografische Lage, kulturelle Herausforderungen, begrenzte Verfügbarkeit von Arbeitskräften und unwirksames Führen oder Risikomanagement.
- Probleme in der Lieferkette, z. B. die Unfähigkeit, Rohstoffe zu beschaffen, ein Mangel an verschiedenen Lieferanten und schwankende Rohstoffpreise.
- Interne Ereignisse, wie z. B. die Fluktuation von Mitarbeitern in Schlüsselpositionen und betriebliche Fehler.

Die Art des disruptiven Ereignisses kann variieren, aber die Organisation sollte über eine klar definierte Resilienzstrategie und formalisierte Prozesse verfügen, um Veränderungen kontinuierlich zu antizipieren, sich darauf vorzubereiten, darauf zu reagieren und sich an sie anzupassen. Resilienz von Organisationen ist ein Oberbegriff. Die Strategie kann je nach Organisation verschiedene Komponenten umfassen, wie z. B. Business Continuity, Disaster Recovery, Matrizen für kritische Funktionen, Nachfolgepläne und Wiederanlauftests.

Zu den Anforderungen des Topical Requirement „Resilienz von Organisationen“ gehören:

- **Governance** – Klar definierte grundlegende Resilienzziele und -strategien, die das Erreichen der Mission und der Vision der Organisation unterstützen.
- **Risikomanagement** – Prozesse zur Identifizierung, Analyse, Bewältigung und Überwachung von Bedrohungen der Resilienz, einschließlich eines Prozesses zur unverzüglichen Eskalation von resilienzbezogenen Vorfällen.
- **Kontrollen** – Vom Management festgelegte, regelmäßig bewertete Kontrollprozesse zur Bewältigung von Resilienzrisiken.

Überlegungen

Interne Revisorinnen und Revisoren können die folgenden Überlegungen zur Unterstützung ihrer Beurteilung der Anforderungen im Topical Requirement „Resilienz von Organisationen“ heranziehen. Die Buchstaben der einzelnen Überlegungen verweisen auf die entsprechenden Anforderungen im Topical Requirement. Diese Überlegungen dienen der Veranschaulichung und sind nicht verbindlich. Interne Revisorinnen und Revisoren sollten sich auf ihr professionelles Urteil verlassen, wenn sie entscheiden, was sie in ihre Beurteilungen einbeziehen.

Einschränkungen bei Aufträgen der Internen Revision im öffentlichen Sektor aufgrund von Gesetzgebung, Regierungsstruktur oder politischem Umfeld werden als potenzielle Hindernisse für die Bearbeitung bestimmter Aspekte dieser Tätigkeit anerkannt. Interne Revisorinnen und Revisoren im öffentlichen Sektor sollten solche Umfangsbeschränkungen als Teil ihrer Risikobeurteilung dokumentieren und ihr professionelles Urteilsvermögen einsetzen, um den maßgeschneiderten Umfang ihrer Prüfung klar zu definieren und zu kommunizieren.

Überlegungen zur Governance

Zur Beurteilung, wie die Governance-Prozesse auf die Resilienzziele angewendet werden, können Interne Revisorinnen und Revisoren folgende Nachweise überprüfen:

A. Eine dokumentierte, vom Management festgelegte und von Geschäftsleitung bzw. Überwachungsorgan überwachte Resilienzstrategie. Sie wird allen Mitarbeitern formell mitgeteilt und ist eng mit der Mission, der Vision, der Kultur und dem Risikomanagementansatz der Organisation abgestimmt und unterstützt diese. Die Ziele des strategischen Resilienzplans werden von Geschäftsleitung bzw. Überwachungsorgan genehmigt, stimmen mit dem Gesamtkonzept der Organisation für das Risikomanagement überein und werden in regelmäßigen Abständen getestet und überprüft. Der Plan kann operative, technologische und finanzielle Elemente enthalten, wie z. B.:

   - Operativ – Koordinierung der Resilienz im gesamten Unternehmen; Resilienz-Risikobeurteilungsprozesse; Business Continuity Planung mit regelmäßigen Tests und Berichten; Krisenmanagement; Anpassungsfähigkeit der Belegschaft (z. B. Fernüberwachungskapazitäten, Mindestbesetzung vor Ort und Cross-Training zur Abdeckung kritischer Funktionen); Nachfolgeplanung für wichtige Mitarbeiter; Resilienz der Lieferkette; Festlegung wichtiger Leistungsindikatoren (KPIs); Awareness-Schulungen für Mitglieder von Geschäftsleitung bzw. Überwachungsorgan.
   - Technologisch – Anforderungen an die IT-Infrastruktur; Identifizierung kritischer Daten (Datenklassifizierung); Datensicherungen; Härtung der Cybersicherheit und Überwachung von Bedrohungen; Wartung kritischer technologischer Anlagen; definierte Wiederherstellungspunktziele (RPO) und Wiederherstellungszeitziele (RTO) für kritische Daten (validiert durch Wiederherstellungstests).

- Finanziell – Für die Resilienz vorgesehene Mittel; Bargeldreserven zur Aufrechterhaltung des Betriebs während einer Disruption; Prozesse für die Finanzberichterstattung zur genauen Erfassung von Transaktionen im Zusammenhang mit einer Disruption; Versicherungspolicen zur Abmilderung von Disruptionsrisiken; Verfügbarkeit von Kreditlinien für die Aufnahme von Notkrediten.

B. Regelmäßige (z. B. monatliche oder vierteljährliche) Aktualisierungen bezüglich der Resilienz werden der Geschäftsleitung bzw. dem Überwachungsorgan von der Person oder dem Team, das für die Resilienz der Organisation führend ist, zur Verfügung gestellt. Diese können die definierten Risikotoleranzauslöser, KPIs oder andere Informationen enthalten, um Beobachtungen oder Trends aufzuzeigen. Aktualisierungen kommunizieren den Status der strategischen Resilienzziele der Organisation, einschließlich der strategischen Aufsicht, Überwachung und langfristigen Planung. Die Berichterstattung kann die folgenden Ergebnisse der Überwachung enthalten:

   - Erreichen der strategischen Resilienzziele und Herausforderungen, die ihnen entgegenstehen könnten.
   - Budgeterfordernisse zur Unterstützung von Resilienzzielen und -vorgaben, wie z. B. der Bedarf an technologischen Ressourcen.
   - Status der Resilienzrisiken, einschließlich wesentlicher Veränderungen im Umfeld der Resilienzrisiken, die sich auf die festgelegten Risikotoleranzwerte auswirken würden.
   - Wirksamkeit der internen Kontrollen bezüglich Resilienz, einschließlich der Fortschritte bei der Behebung.
   - KPIs zur Messung von Resilienzerfolgen.
   - Personalressourcen, die für die Einstellung, Schulung und Entwicklung von Personal mit Resilienzaufgaben erforderlich sind.

C. Richtlinien, Verfahren und andere relevante Unterlagen, die zum Management der operativen, technischen und finanziellen Resilienz verwendet werden, einschließlich:

   - Wie kritische Resilienzprozesse identifiziert und regelmäßig analysiert werden, um festzustellen, ob sie weiterhin die wichtigsten Prozesse genau widerspiegeln.
   - Die Richtlinien werden mindestens einmal jährlich (oder häufiger, je nach Risikoniveau) überprüft und aktualisiert. Bei neu auftretenden Risiken oder auf der Grundlage von Erkenntnissen aus Tests oder tatsächlichen Disruptionen werden sie bei Bedarf häufiger aktualisiert.
   - Ein Prozess zur Überprüfung der Angemessenheit von Richtlinien und Verfahren zur Unterstützung von Resilienzmaßnahmen.
   - Wenn die Resilienzprozesse und internen Kontrollen gestärkt werden, indem verbreitete Rahmenwerke für verwandte Prozesse, wie Risikomanagement, IT oder Governance, verwendet werden. Beispiele, die in Betracht gezogen werden können, stammen von Organisationen wie NIST, COSO oder ISO, insbesondere die Serie ISO 22300 (22316 oder 22336).

D. Eine etablierte und dokumentierte Struktur der Einsatzleitung, die die Führungsrollen und Verantwortlichkeiten in Bezug auf die Erreichung der Resilienzziele beschreibt. Nachweis etablierter Entscheidungshierarchien, wie z. B. das Personal, das während einer Disruption für resilienzbezogene Entscheidungen zuständig ist, und die erforderlichen Genehmigungen für operative Entscheidungen, wie z. B. die Auszahlung von Geldern oder die Möglichkeit, rechtmäßig einen Vertrag mit einer Drittpartei zur Unterstützung der Organisation während

einer Disruption abzuschließen. Zu den weiteren Überlegungen gehören dokumentierte Eskalationspfade und vorübergehende Entscheidungsbefugnisse während einer Disruption, einschließlich finanzieller Delegierung und Schwellenwerte für die Auftragsvergabe an Drittparteien.

E. Ein etablierter Prozess zur regelmäßigen (z. B. jährlichen oder halbjährlichen) Beurteilung der Kenntnisse, Fähigkeiten und Fertigkeiten der Personen, die für den Betrieb und das Management der Resilienzprozesse der Organisation verantwortlich sind. Der Prozess kann die Identifizierung von Schulungsprogrammen beinhalten, wie Live- oder virtuelles Lernen, Konferenzen, On-Demand-Kurse oder berufliche Zertifizierungen. Nachweis einer Nachfolgeplanung zur Ermittlung von Schlüsselrollen für die Resilienz, einschließlich Szenariotests zur Ermittlung von Tätigkeiten, die nur von einer Person oder einer begrenzten Anzahl von Personen ausgeführt werden können. Die Qualifikationen für die Ersetzungen werden dargelegt.

F. Ein etablierter Prozess, um relevante interne und externe Stakeholder zu identifizieren, zu priorisieren und gegebenenfalls in den Aufbau von Informations- und Berichtsstrukturen einzubinden, um bestehende Schwachstellen und neu auftretende Bedrohungen, die das Erreichen der Resilienzziele der Organisation beeinträchtigen könnten, zu identifizieren und darauf zu reagieren. Nachweise für die Beteiligung von Stakeholdern an Diskussionen über Schwachstellen der Resilienz. Der Nachweis kann in Form von E-Mails, Sitzungsprotokollen oder Berichten erbracht werden, einschließlich Hinweisen auf die Verwendung von unternehmensweiten Kennzahlen zur Messung und Überwachung der Wirksamkeit der Resilienz.

Überlegungen zum Risikomanagement

Um zu beurteilen, wie die Risikomanagementprozesse auf die Resilienzziele der Organisation angewandt werden, können Interne Revisorinnen und Revisoren Nachweise für Folgendes überprüfen:

A. Die Risikobeurteilungs- und Risikomanagementprozesse der Organisation umfassen die Identifizierung von Risiken für die Resilienz der Organisation und werden kontinuierlich durchgeführt und dokumentiert, wobei die Ergebnisse in der gesamten Organisation kommuniziert werden. Der Prozess des Resilienz-Risikomanagements umfasst die Bewertung von Schlüsselprozessen wie Betrieb, unternehmensweites Risikomanagement, IT, Lieferkette/Beschaffung, Facility Management, Personal, Finanzen, Recht, Compliance, Regulatorik, Öffentlichkeitsarbeit, kritische Lieferanten, Reputation, neu aufkommende Risiken und andere. Neben der Ermittlung von Resilienzrisiken umfassen die Prozesse auch die Beurteilung, dass Bedrohungen und Schwachstellen, die den Geschäftsbetrieb stören könnten:

   - Initial identifiziert und gemeldet werden.
   - Analysiert werden, um das Risiko für das Erreichen der Organisationsziele zu bewerten.
   - Gemindert werden, einschließlich Maßnahmenpläne zur Reduktion des Risikos auf ein akzeptables Niveau.
   - Überwacht werden, einschließlich eines Plans für die laufende Berichterstattung, bis die Bedrohungen vollständig beseitigt sind.

Zusätzliche Nachweise können sein:

- Dokumentation in Form von Berichten, E-Mails oder Sitzungsprotokollen, aus denen hervorgeht, welche Geschäftsbereiche beteiligt sind. Risikofaktoren wie Auswirkungen, Wahrscheinlichkeit, Geschwindigkeit und andere Aspekte können einbezogen werden.
- Stark korrelierte oder voneinander abhängige Risikofaktoren werden analysiert, um die kumulativen Auswirkungen mehrerer Risikopositionen zu ermitteln.
- Die Risikobeurteilung umfasst die Bewertung der Schutzschichten für kritische Anlagen und der Ressourcen zur Vermeidung eines einzelnen Ausfallpunkts.
- Die Risikobeurteilung wird aktualisiert, indem Erkenntnisse aus tatsächlichen Krisen und Disruptionen sowie die Ergebnisse von Tests und Szenarien einbezogen werden.
- Die Organisation setzt Prioritäten für die Bereiche, die das höchste Risiko darstellen, basierend auf den potenziellen Auswirkungen und der Wahrscheinlichkeiten, die sich aus der Business Impact Analyse ergeben.

B. Die Organisation hat einer Person oder einem Team die Verantwortlichkeit und die Verantwortung für die Überwachung und Berichterstattung über Resilienzrisiken übertragen und überprüft diese regelmäßig. Dafür stehen qualifizierte Personen mit Erfahrung im Resilienzmanagement, idealerweise in der Branche der Organisation (z. B. Gesundheitswesen, Finanzdienstleistungen oder öffentlicher Sektor) zur Verfügung. Die Person oder das Team nimmt regelmäßig an Schulungen teil, um sich über neue Trends im Bereich der Resilienzrisiken zu informieren.

C. Die Organisation hat einen Prozess zur Überwachung von (neu auftretenden oder bereits identifizierten) Resilienzrisiken der Organisation und zur raschen Eskalation solcher Risiken eingeführt, die gemäß den festgelegten Risikomanagementrichtlinien und der Risikotoleranz der Organisation oder gemäß den geltenden rechtlichen oder regulatorischen Anforderungen ein als inakzeptabel erachtetes Niveau erreichen. Die Auswirkungen auf das Resilienzrisiko der Organisation, einschließlich finanzieller und nicht-finanzieller Maßnahmen, werden berücksichtigt. Beispiele für finanzielle Kennzahlen sind Einnahmen, Ausgaben, Rentabilität, Cashflow, Schulden, Aktienkurs und Gesamtwert. Beispiele für nicht-finanzielle Kennzahlen sind Reputation der Marke, Kundenzufriedenheit, Umweltauswirkungen und Personalfluktuation. Der Prozess umfasst:

- Erste Identifizierung von Risiken und rechtzeitige Eskalation.
- Analyse zur Bewertung des Risikos und der Art und Weise, wie es das Erreichen der Organisationsziele verhindern könnte.
- Vorgeschlagene und vereinbarte Maßnahmenpläne zur Risikominderung, einschließlich der Frage, wie das Risiko rechtzeitig auf ein akzeptables Niveau reduziert werden kann. Die Maßnahmenpläne basieren auf der umfassenden unternehmensweiten Strategie für das Risikomanagement. Der Vorschlag sollte die notwendigen Ressourcen zur Risikominderung enthalten, z. B. finanzielle Mittel, Personalstunden und zusätzliche Technologie und Software, die zur Steigerung der Fähigkeiten benötigt werden.
- Laufende Risikoüberwachung und Berichterstattung über die wichtigsten Risikoindikatoren, bis die Bedrohungen vollständig beseitigt sind.

D. Die Organisation hat ein Verfahren eingeführt, um auf Krisen, Disruptionen, Notlagen oder andere Vorfälle zu reagieren und sich davon zu erholen. Der Prozess wird in regelmäßigen Abständen, z. B. vierteljährlich oder jährlich, vollständig getestet und kann auch häufigere Teiltests, z. B. monatlich, umfassen. Kritische Dienste erfordern möglicherweise häufigere

Tests. Der Prozess der Reaktion auf einen Vorfall und der Wiederherstellung kann Folgendes umfassen:

- Erkennung – kontinuierliche Überwachung auf Cyber-Ereignisse. Dazu kann der Einsatz eines Intrusion Detection Systems, von Threat Intelligence oder Security Information and Event Management (SIEM) gehören. Das SIEM kann künstliche Intelligenz einsetzen, um den Prozess zu stärken. Für den Fall von Naturkatastrophen oder Anlagenausfällen hat die Organisation ein Kommunikationsnetz eingerichtet (z. B. Warnprotokolle oder Benachrichtigungen), um rechtzeitig auf die Situation aufmerksam zu machen und Informationen weiterzugeben. Für alle Ereignisse hat die Organisation ein Verfahren zur Benachrichtigung der zuständigen Notrufzentralen und Behörden festgelegt. Die Ereignisse sollten nach ihrer Kritikalität priorisiert werden.
- Reaktion und Eindämmung – der Ansatz zur Reaktion auf Vorfälle umfasst Szenarioanalysen und regelmäßige Stresstests für eine Reihe von disruptiven Vorfällen. Um weitere Schäden bei Cyber-Ereignissen zu verhindern, hat die Organisation beispielsweise ein Verfahren zur Isolierung der gefährdeten Anlagen eingeführt, wie die Umleitung des Netzwerkverkehrs oder die Einschränkung des Benutzerzugriffs während eines Ereignisses. Für physische Ereignisse hat die Organisation ein Verfahren zur physischen Isolierung disruptiver Vorfälle eingeführt, um die Auswirkungen zu begrenzen, einschließlich der Verlegung von Mitarbeitern an einen anderen Ort.
- Wiederherstellung – für cyber- oder IT-bedingte Ereignisse hat die Organisation Verfahren zur Priorisierung der Wiederherstellung kritischer Assets festgelegt, die für die Wiederaufnahme des Betriebs erforderlich sind (z. B. Wiederherstellung von Daten aus Backups oder Wiederherstellung des Betriebs von Servern). Auch andere Nicht-IT-Ressourcen, die für die Wiederaufnahme des Betriebs erforderlich sind, sollten für die Wiederherstellung priorisiert werden. Dazu kann die Planung einer schrittweisen Rückkehr von Schlüsselpersonal oder Kernfunktionen gehören.
- Analyse nach einem Vorfall – die Organisation analysiert die Ereignisse, um Folgendes festzustellen:
  - Grundursachen von Disruptionen.
  - Wirksamkeit der ergriffenen Maßnahmen.
  - Erforderliche Verbesserungen zur Stärkung der Resilienzprozesse, wie z. B. die Aktualisierung von Richtlinien, Verfahren, Risiken oder Strategien.

Der Reaktions- und Wiederherstellungsprozess, der durch Tabletop-Übungen, Simulationen und Drills, die kritische Dienste/Funktionen und deren Abhängigkeiten abdecken, auf Stringenz und Wirksamkeit getestet wird, kann an die Risikotoleranz der Organisation angepasst werden. Bei diesen Ereignissen kann es sich um interne oder externe Vorfälle handeln. Die Ergebnisse dieser Übungen können von Geschäftsleitung bzw. Überwachungsorgan überprüft werden, wobei die Verbesserungsmaßnahmen nachverfolgt und regelmäßig berichtet werden. Die Empfehlungen sollten umsetzbar sein, mit klaren Verantwortlichkeiten und Zeitvorgaben.

Überlegungen zum Kontrollprozess

Um zu beurteilen, wie die Kontrollprozesse auf die Resilienzziele der Organisation angewandt werden, können Interne Revisorinnen und Revisoren Nachweise für Folgendes überprüfen:

A. Es gibt einen Prozess zur Identifizierung und Beurteilung kritischer Drittparteien (Lieferanten und Anbieter) und der Mindestbestände, die für die Aufrechterhaltung des Betriebs erforderlich sind. Die Beurteilung kann die Resilienz und die Geschäftskontinuität von

Drittparteien berücksichtigen und Risikoratings für jeden Anbieter enthalten. Neben der Überprüfung der Anbieter vor dem Abschluss einer formellen Vereinbarung kann die Organisation die Anbieter auch regelmäßig überprüfen, um die Risikoeinstufung kontinuierlich zu bewerten. Die Organisation unterhält eine Liste mit potenziellen Ersatzlieferanten für den Fall, dass eine Lieferantenbeziehung endet.

B. Das Management hat eine Datenklassifizierung vorgenommen und dabei insbesondere die kritischen Daten ermittelt, die für die Wiederherstellung nach Disruptionen und die Aufrechterhaltung des Betriebs erforderlich sind. Die Organisation hat wirksame interne Kontrollen eingeführt, um kritische Daten zu schützen, einschließlich der Beschränkung des Zugriffs auf befugtes Personal und der Sicherstellung, dass kritische Daten gesichert werden und rechtzeitig wiederherstellbar sind.

C. Das Management hat kritische IT-Kontrollen und kontinuierliche Überwachungsprozesse eingeführt, um Informationssicherheitsrisiken (einschließlich Cyberrisiken) zu mindern und den Schutz sensibler Daten bei Disruptionen zu gewährleisten. Verschlüsselung schützt sensible Daten. Continuous Monitoring und Echtzeit-Bedrohungsdaten versorgen das Management mit Warnungen, und Probleme werden zeitnah behoben. Weithin anerkannte Kontrollrahmenwerke von Organisationen wie NIST, COSO, ISO und anderen können verwendet werden.

D. Die Organisation hat eine Bestandsaufnahme kritischer IT-Ressourcen durchgeführt, einschließlich Hardware, Software und Services, die zur Unterstützung des Betriebs in Krisen, Disruptionen und Notfällen erforderlich sind. IT-Ressourcen, deren schnelle Beschaffung schwieriger ist, werden als vorrangig eingestuft.

E. Ein Business Continuity Plan und ein Disaster Recovery Plan werden erstellt. Dort wird basierend auf einer Business Impact Analyse Personal für Wiederherstellungsteams bestimmt. Die Pläne werden in regelmäßigen Abständen, z. B. vierteljährlich oder jährlich, im Rahmen von Tabletop-Übungen oder Stresstests getestet, bei denen Disruptionen in realen Notfällen simuliert und Kommunikationsprotokolle mit internen und externen Beteiligten getestet werden. Die Ergebnisse der Tests, einschließlich der Verbesserungsmöglichkeiten, werden der Geschäftsleitung bzw. dem Überwachungsorgan mitgeteilt.

F. Es wird ein Verfahren zur Änderung des Arbeitsumfelds bei Disruptionen eingeführt. Zu den Anpassungen kann auch die Nutzung alternativer Arbeitsplätze gehören, z. B. die Arbeit von zu Hause aus oder die rechtzeitige und effiziente Einrichtung eines vorübergehenden Büros. Die Organisation kann hybride Arbeitsformen oder Remote Work nutzen, um Tätigkeiten vor Ort zu ersetzen. Weitere Aspekte können Verfahren für die rechtzeitige und effiziente Mobilisierung und Neuzuweisung von Ressourcen, einschließlich IT- und Personalressourcen, umfassen.

G. Es gibt einen Prozess zur kontinuierlichen Überwachung und Meldung neu auftretender Bedrohungen und Schwachstellen im Zusammenhang mit der Resilienz der Organisation sowie zur Ermittlung, Priorisierung und Umsetzung von Möglichkeiten zur Verbesserung der Resilienz. Zu den Überwachungsmaßnahmen können wichtige Risikoindikatoren (KRIs), Risiko-Dashboards und Risiko-Horizontscans gehören. Die Organisation kann alle Mitarbeiter über neu auftretende Bedrohungen auf dem Laufenden halten, um sie zu sensibilisieren, und ihnen Maßnahmen zur Abschwächung der Bedrohungen oder Kontrollen anbieten. Alle Whistleblower-Aktivitäten werden protokolliert, analysiert, zeitnah gelöst und an die Geschäftsleitung kommunizierzt. Zur Lösung von Problemen kann eine laufende Überwachung erforderlich sein, die eine zusätzliche Berichterstattung erfordert.

H. Es gibt ein Verfahren zur Schulung und Ausbildung des Personals in Bezug auf die Resilienz der Organisation und die Verfahren, die bei Krisen, Disruptionen und Notfällen zu befolgen sind. Dazu gehören auch Übungen, in denen disruptive Szenarien simuliert werden. Die Schulungen werden in regelmäßigen Abständen durchgeführt, beispielsweise vierteljährlich oder jährlich. Kritische Dienste müssen möglicherweise häufiger getestet werden.

I. Es gibt einen Prozess, mit dem sichergestellt wird, dass die erforderlichen operativen, personellen, technologischen und finanziellen Ressourcen eingeplant und in Krisen, Disruptionen und Notfällen verfügbar sind. Das Management überprüft regelmäßig, z. B. vierteljährlich oder jährlich, ob die Ressourcen auf der Grundlage der wahrgenommenen Risiken angemessen sind, und teilt der Geschäftsleitung bzw. dem Überwachungsorgan den Bedarf mit. Kritische Dienste müssen möglicherweise häufiger getestet werden. Die Analyse umfasst eine Beurteilung der Liquidität, des Versicherungsschutzes und der Finanzierungsvereinbarungen für unvorhergesehene Ereignisse. Der Bedarf an finanziellen Ressourcen wird auf der Grundlage von Faktoren wie Größe, Komplexität, Branche und Risikoprofil der Organisation geplant. Der Prozess kann eine Vorabgenehmigung der Finanzierung vorsehen.

J. Es gibt ein Verfahren zur Überprüfung von Krisen, Disruptionen und Notfällen nach deren Eintreten und zur Analyse der Erkenntnisse, die nach einem Vorfall gemacht wurden. Die Überprüfungen sollten in einem formellen Bericht dokumentiert werden und die gewonnenen Erkenntnisse sollten in die künftige Resilienzplanung einbezogen werden.

Anhang A. Anwendungsszenarien

Die folgenden Szenarien beschreiben, wann das Topical Requirement „Resilienz von Organisationen“ anwendbar ist. Darüber hinaus bietet das Dokument „Topical Requirements Anwendungsleitfaden” des IIA praktische Ratschläge zum Umgang mit verbindlichen Anforderungen, zum Umgang mit Einschränkungen und zur Ermittlung kritischer Risikoschwellen.

Szenario 1: Resilienz der Organisation wird als Untersuchungsgegenstand für einen Auftrag der Internen Revision, der im Revisionsplan enthalten ist, ermittelt.

Wenn die Interne Revision ihren risikobasierten Planungsprozess abschließt und einen oder mehrere Aufträge zur Resilienz der Organisation in ihren Revisionsplan aufnimmt, muss das Topical Requirement bei der Durchführung solcher Aufträge angewendet werden. Die Einhaltung kann dadurch erreicht werden, dass die Anforderungen in einen oder mehrere Aufträge im Revisionsplan aufgenommen werden.

Resilienz der Organisation ist ein weit gefasstes Thema, und nicht jede Anforderung im Topical Requirement trifft auf jeden Auftrag zu. Wenn Interne Revisorinnen und Revisoren nach ihrem professionellen Urteil zu dem Schluss kommen, dass eine oder mehrere Anforderungen des Topical Requirements „Resilienz von Organisationen“ nicht anwendbar sind und daher von einem Auftrag ausgeschlossen werden sollten, müssen sie die Gründe für den Ausschluss dieser Anforderungen dokumentieren und aufbewahren. Der Grund für den Ausschluss einiger Anforderungen könnte beispielsweise darin liegen, dass die Interne Revision turnusmäßig verschiedene Prüfungen zur Resilienz der Organisation durchführt oder festgestellt hat, dass die Bedeutung des Risikos für den Auftrag gering ist.

Szenario 2: Resilienzrisiken der Organisation werden bei einem Revisionsauftrag ermittelt, der nicht auf die Resilienz der Organisation ausgerichtet ist.

Interne Revisorinnen und Revisoren können bei der Beurteilung eines Prozesses, der nicht direkt mit Resilienz zu tun hat, Resilienzrisiken identifizieren. So kann es beispielsweise vorkommen, dass Interne Revisorinnen und Revisoren die Personalprozesse (z. B. Einstellung und Bindung von Mitarbeitern) im Rahmen eines Auftrags beurteilen, der nicht auf die Resilienz der Organisation ausgerichtet ist, und dass sie bei der Planung des Auftrags die Resilienzrisiken nicht als Teil des Umfangs identifizieren. Nach der ersten Durchsicht stellen sie jedoch fest, dass diese Risiken in den Umfang fallen. So ermitteln sie beispielsweise Risiken bei der Nachfolgeplanung im Zusammenhang mit der Art und Weise, wie die Organisation Personal an sich bindet (Standard 13.2 „Risikobeurteilung zu einem Auftrag“).

Sobald die relevanten Risiken identifiziert sind, müssen sie das Topical Requirement „Resilienz von Organisationen“ überprüfen und bestimmen, welche Anforderungen anwendbar sind. In diesem Beispiel könnten sie sich nur auf die Anforderung E im Bereich Governance konzentrieren und die anderen Risikomanagement- und Kontrollanforderungen ausklammern. Sie müssen in den Auftragspapieren die Gründe für den Ausschluss der anderen Anforderungen des Topical Requirements „Resilienz von Organisationen“ dokumentieren und die Dokumentation aufbewahren.

Szenario 3: Es wird ein Auftrag zur Resilienz der Organisation angefordert, der ursprünglich nicht im Revisionsplan enthalten war.

Stakeholder wie die Geschäftsleitung bzw. das Überwachungsorgan, das Management oder eine Aufsichtsbehörde können die Interne Revision bitten, außerhalb des ursprünglichen Revisionsplans Beurteilungen der Resilienz durchzuführen. Wenn Organisationen beispielsweise Ziel eines Cyberangriffs sind, kann die Geschäftsleitung bzw. das Überwachungsorgan einen Auftrag der Internen Revision zur Beurteilung von Resilienzkontrollen anfordern, um zu bewerten, wie gut die Organisation auf die Wiederherstellung nach einem Cyberangriff vorbereitet ist. Das Topical Requirement ist anwendbar, die Anforderungen müssen beurteilt und etwaige Ausschlüsse müssen dokumentiert werden (Standard 9.4 „Revisionsplan“).

Anhang B. Beispiele für Revisionsaufträge auf der Grundlage von Anwendungsszenarien

Szenario 1: Das Thema ist ein Auftrag im Revisionsplan.

Öffentliche Einrichtung, die für einen zentralen Großhandelsmarkt zuständig ist

Während ihres jährlichen risikobasierten Planungsprozesses identifiziert die Interne Revision die Kontinuität der wesentlichen Marktoperationen als einen Bereich mit hohem Risiko, da sie logistischen Disruptionen, Ereignissen im Bereich der öffentlichen Gesundheit und Abhängigkeiten von kritischen Infrastrukturen ausgesetzt ist. Basierend auf dieser Beurteilung stellen die Internen Revisorinnen und Revisoren fest, dass das Topical Requirement „Resilienz von Organisationen" auf den geplanten Auftrag anwendbar ist.

Um die Governance zu beurteilen, überprüfen die Internen Revisorinnen und Revisoren die Protokolle der Geschäftsleitung bzw. des Überwachungsorgans, die Strategiepläne und die Budgetunterlagen, um festzustellen, ob resilienzbezogene Ziele formell festgelegt sind und überwacht werden. Sie bewerten, ob das Management dem Leitungsgremium regelmäßig über kritische Schwachstellen wie Transportabhängigkeiten, Infrastrukturbeschränkungen und Gesundheitsrisiken Bericht erstattet. Wenn es kein einheitliches Dokument zur Resilienzstrategie gibt, beurteilen die Internen Revisorinnen und Revisoren, ob die Elemente der Resilienz in den operativen und strategischen Unterlagen konsistent verankert sind.

Aus der Perspektive des Risikomanagements untersuchen die Internen Revisorinnen und Revisoren das Risikoregister der Organisation und befragen das operative Management, um zu bestätigen, dass Risiken, die die Kontinuität der Versorgung beeinträchtigen können, identifiziert, beurteilt und verantwortlichen Personen zugewiesen sind. Sie prüfen, ob bei früheren Ereignissen Eskalationsmechanismen wie vorübergehende Schließungen oder Zugangsbeschränkungen aktiviert wurden, und stellen fest, ob die Reaktionsmaßnahmen mit den festgelegten Risikotoleranzparametern übereinstimmen.

Zu den Kontrollverfahren gehören die Überprüfung der Vorkehrungen für die Betriebskontinuität, die Inspektion der Nachweise für die regelmäßigen Übungen und die Prüfung der Unterlagen über die Koordinierung mit den Behörden bei disruptiven Vorfällen. Interne Revisorinnen und Revisoren überprüfen auch die Berichte nach Vorfällen, um festzustellen, ob die daraus gezogenen Erkenntnisse in aktualisierte Prozesse eingeflossen sind. Wenn bestimmte Anforderungen des Topical Requirements aufgrund gesetzlicher oder struktureller Zwänge nicht anwendbar sind, dokumentieren die Internen Revisorinnen und Revisoren die Gründe für den Ausschluss in Übereinstimmung mit den Standards.

Szenario 2: Das Thema wird bei der Durchführung eines Auftrags identifiziert.

Global aufgestelltes Beratungsunternehmen

Während einer Prüfung, die sich auf Governance und unternehmensweites Risikomanagement konzentriert, stellen Interne Revisorinnen und Revisoren Schwachstellen fest, die mit der dezentralisierten Entscheidungsfindung, der Abhängigkeit von wichtigen lokalen Führungskräften und

der Regulierung in verschiedenen Ländern zusammenhängen. Auf der Grundlage dieser Beobachtungen stellen die Internen Revisorinnen und Revisoren fest, dass bestimmte Elemente des Topical Requirements „Resilienz von Organisationen“ auf den Auftrag zutreffen.

Um die Governance zu beurteilen, überprüfen die Internen Revisorinnen und Revisoren globale Richtlinien, Unterlagen zur Berichterstattung an die Geschäftsleitung bzw. das Überwachungsorgan und Protokolle zum Krisenmanagement, um festzustellen, ob die Organisation festgelegt hat, wie der Betrieb im Falle von Änderungen an Regulierungen, eines erheblichen Wechsels wichtiger Mitarbeiter oder von Reputationsereignissen in einem Land, die sich breiter auswirken können, aufrechterhalten wird. Sie bewerten, ob das Leitungsgremium eine konsolidierte Berichterstattung über kritische Risiken in allen Jurisdiktionen erhält und ob die Verantwortlichkeit für die Überwachung der Widerstandsfähigkeit klar definiert ist.

Aus der Perspektive des Risikomanagements untersuchen die Internen Revisorinnen und Revisoren den Rahmen für das unternehmensweite Risiko, um festzustellen, ob die Risiken im Zusammenhang mit der Abhängigkeit von Schlüsselpersonen, der Einhaltung grenzüberschreitender gesetzlicher Vorschriften und der Reputationsgefährdung mit den strategischen Zielen des Unternehmens in Einklang stehen. Sie führen Stichprobentests ausgewählter Vorfälle durch, um festzustellen, ob lokale Ereignisse in angemessener Weise an die globale Führung eskaliert wurden und ob Reaktionsentscheidungen innerhalb definierter Autoritätsebenen getroffen wurden.

Zu den kontrollbezogenen Verfahren gehören die Überprüfung von Regelungen zur Geschäftskontinuität in verschiedenen Ländern, die Untersuchung, ob kritische Funktionen angemessen abgedeckt sind und ob Ersatzpersonal oder ordnungsgemäß strukturierte Nachfolgeprozesse für den Fall der Fälle vorhanden sind, sowie die Beurteilung der Angemessenheit der technologischen Infrastruktur zur Unterstützung koordinierter Remote-Aktivitäten. Die Internen Revisorinnen und Revisoren überprüfen auch die Dokumentation der Analysen nach den Ereignissen, um zu bestätigen, dass Abhilfemaßnahmen durchgeführt wurden. Wenn nur bestimmte Anforderungen des Topical Requirements anwendbar sind, dokumentieren die Internen Revisorinnen und Revisoren die Grundlage für die Einbeziehung oder den Ausschluss.

Szenario 3: Das Thema ist Gegenstand eines angefragten Auftrags.

Verantwortliche Einheit für kritische nationale Infrastrukturen

Ein zerstörerischer Wirbelsturm in einer benachbarten Jurisdiktion veranlasst ein Vorstandsmitglied, die Interne Revision zu bitten, ihren Revisionsplan um eine Prüfung der Resilienz der Organisation zu erweitern, um die Exposition der Organisation durch Betriebsunterbrechungen, die Abhängigkeit von spezialisierten Auftragnehmern, gesetzliche Verpflichtungen und schwere Umweltereignisse zu bestätigen. In diesem Fall wird das Topical Requirement „Resilienz von Organisationen“ umfassend angewendet.

Zur Beurteilung der Governance überprüfen die Internen Revisorinnen und Revisoren den vom Vorstand genehmigten Strategieplan und die zugehörige Dokumentation, um zu bestätigen, dass die Kontinuität kritischer Dienste formell in die langfristige Planung einbezogen ist. Sie prüfen die Berichterstattung an den Vorstand, um festzustellen, ob Schlüsselindikatoren in Bezug auf die betriebliche Verfügbarkeit, die Instandhaltung kritischer Anlagen und die finanzielle Notfallplanung, einschließlich Versicherungsschutz und Rücklagenbildung, regelmäßig überprüft werden.

Aus der Perspektive des Risikomanagements bewerten die Internen Revisorinnen und Revisoren, wie Risiken im Zusammenhang mit Infrastrukturstörungen, der Konzentration von Auftragnehmern, der Einhaltung von Vorschriften und der Umweltbelastung im Rahmen des Risikomanagements des

Unternehmens ermittelt, beurteilt und überwacht werden. Sie überprüfen, ob die Verantwortlichkeit für die Überwachung dieser Risiken klar definiert ist und ob bei früheren Betriebsunterbrechungen Eskalationsprotokolle befolgt wurden, einschließlich der Koordinierung mit Regulierungs- und Notfallbehörden.

Zu den Kontrolltests gehören die Überprüfung des Vorhandenseins von Business Continuity und Disaster Recovery Plänen und deren regelmäßige Überprüfung, die Durchsicht von Bestandsverzeichnissen kritischer Vermögenswerte, die Prüfung vertraglicher Vereinbarungen mit alternativen Anbietern und die Beurteilung von Unterlagen zur Analyse nach einem Vorfall, um festzustellen, ob Abhilfemaßnahmen nachverfolgt und umgesetzt wurden. Wenn bestimmte Anforderungen aufgrund von Rechtsvorschriften nicht anwendbar sind, dokumentieren die Internen Revisorinnen und Revisoren die Begründung gemäß den Standards.

Anhang C. Abbildung auf Rahmenwerke

Die Organisation kann ihre eigenen organisatorischen Anstrengungen unternehmen und dabei Rahmenwerke, wie die der ISO, verwenden. Interne Revisorinnen und Revisoren haben möglicherweise bereits Arbeitsprogramme und Testverfahren auf der Grundlage dieser Rahmenwerke entwickelt. Interne Revisorinnen und Revisoren sollten ihre beabsichtigte Prüfung der Resilienz der Organisation mit dem Topical Requirement abgleichen, um eine angemessene Abdeckung sicherzustellen (Standard 13.4 „Bewertungskriterien“). Die folgende Gegenüberstellung ordnet das Topical Requirement „Resilienz von Organisationen“ dem ISO 22336 Rahmenwerk zu. Weitere Referenzrahmenwerke sind in Anhang E aufgeführt.

Anforderungen an die Governance		ISO 22336 Rahmenwerk
A.	Eine formelle Strategie der Organisation, die sich mit der Resilienz befasst, wird von der Geschäftsleitung festgelegt und vom Überwachungsorgan angenommen und überwacht. Sie umfasst die operativen, technologischen und finanziellen Elemente, die zur Bewältigung von Veränderungen und zur Fortführung des Betriebs erforderlich sind. Die Resilienzziele stehen im Einklang mit dem Gesamtkonzept der Organisation für das Risikomanagement.	4.1; 6.1; 6.2; 7.1; 8.4; 8.5; 9.1; 9.5
B.	Geschäftsleitung bzw. Überwachungsorgan werden regelmäßig über den Stand der Erreichung der Resilienzziele unterrichtet. Dadurch wird sichergestellt, dass die Resilienz in die strategische Beaufsichtigung, die langfristigen Planungsprozesse, die Nachfolgeplanung und die Organisationskultur eingebettet ist, einschließlich der Ressourcen- und Budgetüberlegungen, die zur Unterstützung kritischer Geschäftsaktivitäten erforderlich sind.	6.4; 8.6; 10.2
C.	Richtlinien und Verfahren für kritische operative, technologische und finanzielle Prozesse werden festgelegt und regelmäßig überprüft, getestet und bei Bedarf aktualisiert, um das Kontrollumfeld zu stärken.	4.2; 6.3; 8.3; 8.4; 9.4
D.	Zur Überwachung und Unterstützung der Resilienzziele der Organisation wird eine Einsatzleitstruktur eingerichtet und genutzt. Dazu gehören Entscheidungshierarchien, Kommunikations- und Eskalationsprotokolle sowie Aufgaben und Verantwortlichkeiten in Führung und Betrieb.	5.4
E.	Es wird ein Prozess eingerichtet, um die für den Erfolg der Resilienz erforderlichen Kompetenzen regelmäßig zu validieren und die Kompetenzen der Personen, die kritische Aufgaben in Resilienzprozessen einnehmen, neu zu beurteilen.	9.6
F.	Es wird ein Prozess eingerichtet, der sicherstellt, dass alle relevanten internen und externen Stakeholder identifiziert, priorisiert und in die Einrichtung von Informations- und Berichtsstrukturen zur Erreichung der Resilienzziele der Organisation einbezogen werden. Zu den Stakeholdern gehören u. a. Geschäftsleitung, Betrieb, Risikomanagement, IT, Lieferkette/Beschaffung, Facility Management, Personalabteilung, Finanzabteilung, Rechtsabteilung, Assurance Provider (einschließlich Interne Revision), Compliance-Abteilung, Öffentlichkeitsarbeit, wichtige Lieferanten, Kunden und Aufsichtsbehörden.	9.2; 9.5

Anforderungen an das Risikomanagement	ISO 22336 Rahmenwerk
A. Risiken im Zusammenhang mit der Resilienz der Organisation werden regelmäßig identifiziert, beurteilt und in der gesamten Organisation gesteuert. Die Resilienzrisiken werden den strategischen Zielen der Organisation zugeordnet. Der Prozess des Resilienz-Risikomanagements umfasst die Bewertung von Schlüsselprozessen.	4.4; 5; 7.3; 7.4; 7.5, 7.6, 9.2, 9.3
B. Die Verantwortlichkeiten und Zuständigkeiten für das Resilienz-Risikomanagement der Organisation sind klar definiert. Eine benannte Person oder ein benanntes Team wird damit beauftragt, das Management der Resilienzrisiken der Organisation regelmäßig zu überwachen und darüber Bericht zu erstatten, einschließlich der für die Risikominderung erforderlichen Ressourcen und der Identifizierung neuer Bedrohungen für die Resilienz der Organisation.	4.3; 8.2; 9.6
C. Es wird ein Prozess eingerichtet, um das Ausmaß der (neu entstehenden oder bereits identifizierten) Resilienzrisiken der Organisation zu überwachen und solche Risiken schnell zu eskalieren, die ein Ausmaß erreichen, das gemäß den festgelegten Risikomanagementrichtlinien und der Risikotoleranz der Organisation oder den geltenden rechtlichen oder regulatorischen Anforderungen als inakzeptabel gilt. Die Auswirkungen des Resilienzrisikos der Organisation werden berücksichtigt.	7.2; 7.6; 10.1
D. Das Management hat einen Prozess eingerichtet und testet ihn regelmäßig, um auf Krisen, Disruptionen und Notfälle zu reagieren und sich davon zu erholen. Der Prozess der Reaktion auf Vorfälle und der Wiederherstellung umfasst die Erkennung, Priorisierung, Eindämmung, Wiederherstellung und Analyse nach dem Vorfall. Der Ansatz zur Reaktion auf Vorfälle umfasst Szenarioanalysen und regelmäßige Stresstests für eine Reihe von Störfällen.	7.2; 7.6; 7.8

Anforderungen an den Kontrollprozess	ISO 22336 Rahmenwerk
A. Es wurde ein Prozess eingerichtet, um kritische Drittparteien (Lieferanten und Anbieter) zu identifizieren und die Mindestbestände zu bestimmen, die zur Aufrechterhaltung der wesentlichen Abläufe erforderlich sind. Dazu gehört auch das Führen einer aktuellen Liste alternativer Lieferanten.	7.7
B. Für den Betrieb kritische Daten werden identifiziert und klassifiziert. Bei der Datenklassifizierung wird ermittelt, wo sich die Daten befinden, wer Zugang zu ihnen benötigt, wie auf sie zugegriffen wird und ob sie gesichert sind und im Notfall wiederhergestellt werden können.	6.1
C. Kritische IT-Kontrollen und Continuous Monitoring wurden eingeführt, um die Risiken für die Informationssicherheit (einschließlich cyberbezogener Risiken) zu mindern und den Schutz sensibler Daten in Krisen, Disruptionen und Notfällen zu gewährleisten. Zu den Kontrollen und dem Continuous Monitoring gehören Echtzeit-Bedrohungsdaten und die Beschränkung des Zugangs auf autorisierte Benutzer.	7.5
D. Kritische IT-Assets sind inventarisiert. Zu diesen Assets gehören Hardware, Software und Dienstleistungen, die zur Unterstützung des Betriebs bei Krisen, Disruptionen und Notfällen erforderlich sind.	9.2
E. Business Continuity und Disaster Recovery Pläne wurden erstellt und enthalten definierte Aufgaben für das zugeordnete Personal und die Wiederherstellungsteams. Die Pläne werden regelmäßig	8.6; 9.6; 10.3

	getestet (z. B. in einer „Tabletop-Übung“) und die Ergebnisse der Tests, einschließlich der Verbesserungsmöglichkeiten, werden Geschäftsleitung und Überwachungsorgan mitgeteilt.	
F.	Ein Prozess zur Änderung des Arbeitsumfelds bei Krisen, Disruptionen und Notfällen wurde eingeführt.	9.3
G.	Ein Prozess zum Continuous Monitoring und zur Meldung neu auftretender Bedrohungen und Schwachstellen, die die Resilienz der Organisation beeinträchtigen könnten, wurde eingeführt. Der Prozess dient der Identifizierung, Priorisierung und Umsetzung von Möglichkeiten zur Verbesserung der Resilienz der Organisation, einschließlich Whistleblowing-Systemen oder Systemen zur Sammlung von Risikoinformationen.	7.6
H.	Ein Prozess zur Ausbildung und Schulung des Personals in Bezug auf die Resilienz der Organisation wurde eingerichtet, um sicherzustellen, dass es die Richtlinien und Verfahren kennt, die zu befolgen sind, sowie die Maßnahmen, die zu ergreifen sind, wenn Krisen, Disruptionen und Notfälle auftreten. Der Prozess umfasst auch Übungen, in denen disruptive Szenarien simuliert werden.	10.2; 10.3
I.	Es wurde ein Prozess eingerichtet, der sicherstellt, dass die erforderlichen operativen, personellen, technologischen und finanziellen Ressourcen bei Krisen, Disruptionen und Notfällen eingeplant und verfügbar sind. Die zur Unterstützung der Resilienz der Organisation erforderlichen finanziellen Ressourcen werden regelmäßig analysiert und der Geschäftsleitung bzw. dem Überwachungsorgan mitgeteilt.	6.4; 7.6; 9.6
J.	Ein Prozess zur Überprüfung von Krisen, Disruptionen und Notfällen nach deren Eintreten und ein Lessons-Learned-Prozess zur Analyse der Überprüfungen nach einem Vorfall wurden eingerichtet, einschließlich der Integration der Erkenntnisse in die künftige Resilienzplanung der Organisation.	10.2, 10.3

Anhang D. Optionales Dokumentationstool

Von Internen Revisorinnen und Revisoren wird erwartet, dass sie die Anwendbarkeit der Anforderungen auf der Grundlage der Risikobeurteilung nach professioneller Beurteilung bestimmen und die Ausnahmen von bestimmten Anforderungen angemessen dokumentieren. Das Topical Requirement kann auf der Grundlage des professionellen Urteils der Prüferinnen oder Prüfer im Revisionsplan oder in den Arbeitspapieren dokumentiert werden. Die Anforderungen können in einem oder mehreren Revisionsaufträgen abgedeckt werden. Darüber hinaus sind möglicherweise nicht alle Anforderungen anwendbar. Dieses druckbare Formular bietet eine Möglichkeit, die Einhaltung des Topical Requirements „Resilienz von Organisationen" zu dokumentieren, seine Verwendung ist jedoch nicht verbindlich.

Resilienz von Organisationen – Governance

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
A. Eine formelle Strategie der Organisation, die sich mit der Resilienz befasst, wird von der Geschäftsleitung festgelegt und vom Überwachungsorgan angenommen und überwacht. Sie umfasst die operativen, technologischen und finanziellen Elemente, die zur Bewältigung von Veränderungen und zur Fortführung des Betriebs erforderlich sind. Die Resilienzziele stehen im Einklang mit dem Gesamtkonzept der Organisation für das Risikomanagement.		
B. Geschäftsleitung bzw. Überwachungsorgan werden regelmäßig über den Stand der Erreichung der Resilienzziele unterrichtet. Dadurch wird sichergestellt, dass die Resilienz in die strategische Beaufsichtigung, die langfristigen Planungsprozesse, die Nachfolgeplanung und die Organisationskultur eingebettet ist, einschließlich der Ressourcen- und Budgetüberlegungen, die zur Unterstützung kritischer Geschäftsaktivitäten erforderlich sind.		
C. Richtlinien und Verfahren für kritische operative, technologische und finanzielle Prozesse werden festgelegt und regelmäßig überprüft, getestet und bei Bedarf aktualisiert, um das Kontrollumfeld zu stärken.		

D.	Zur Überwachung und Unterstützung der Resilienzziele der Organisation wird eine Einsatzleitstruktur eingerichtet und genutzt. Dazu gehören Entscheidungshierarchien, Kommunikations- und Eskalationsprotokolle sowie Aufgaben und Verantwortlichkeiten in Führung und Betrieb.		
E.	Es wird ein Prozess eingerichtet, um die für den Erfolg der Resilienz erforderlichen Kompetenzen regelmäßig zu validieren und die Kompetenzen der Personen, die kritische Aufgaben in Resilienzprozessen einnehmen, neu zu beurteilen.		
F.	Es wird ein Prozess eingerichtet, der sicherstellt, dass alle relevanten internen und externen Stakeholder identifiziert, priorisiert und in die Einrichtung von Informations- und Berichtsstrukturen zur Erreichung der Resilienzziele der Organisation einbezogen werden. Zu den Stakeholdern gehören u. a. Geschäftsleitung, Betrieb, Risikomanagement, IT, Lieferkette/Beschaffung, Facility Management, Personalabteilung, Finanzabteilung, Rechtsabteilung, Assurance Provider (einschließlich Interne Revision), Compliance-Abteilung, Öffentlichkeitsarbeit, wichtige Lieferanten, Kunden und Aufsichtsbehörden.		

Resilienz von Organisationen – Risikomanagement

	Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
A.	Risiken im Zusammenhang mit der Resilienz der Organisation werden regelmäßig identifiziert, beurteilt und in der gesamten Organisation gesteuert. Die Resilienzrisiken werden den strategischen Zielen der Organisation zugeordnet. Der Prozess des Resilienz-Risikomanagements umfasst die Bewertung von Schlüsselprozessen.		
B.	Die Verantwortlichkeiten und Zuständigkeiten für das Resilienz-Risikomanagement der Organisation sind klar definiert. Eine benannte Person oder ein benanntes Team wird damit beauftragt, das Management der Resilienzrisiken der Organisation regelmäßig zu überwachen und darüber Bericht zu erstatten, einschließlich der für die Risikominderung erforderlichen Ressourcen und der Identifizierung neuer Bedrohungen für die Resilienz der Organisation.		

C.	Es wird ein Prozess eingerichtet, um das Ausmaß der (neu entstehenden oder bereits identifizierten) Resilienzrisiken der Organisation zu überwachen und solche Risiken schnell zu eskalieren, die ein Ausmaß erreichen, das gemäß den festgelegten Risikomanagementrichtlinien und der Risikotoleranz der Organisation oder den geltenden rechtlichen oder regulatorischen Anforderungen als inakzeptabel gilt. Die Auswirkungen des Resilienzrisikos der Organisation werden berücksichtigt.		
D.	Das Management hat einen Prozess eingerichtet und testet ihn regelmäßig, um auf Krisen, Disruptionen und Notfälle zu reagieren und sich davon zu erholen. Der Prozess der Reaktion auf Vorfälle und der Wiederherstellung umfasst die Erkennung, Priorisierung, Eindämmung, Wiederherstellung und Analyse nach dem Vorfall. Der Ansatz zur Reaktion auf Vorfälle umfasst Szenarioanalysen und regelmäßige Stresstests für eine Reihe von Störfällen.		

Resilienz von Organisationen – Kontrollen

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
A. Es wurde ein Prozess eingerichtet, um kritische Drittparteien (Lieferanten und Anbieter) zu identifizieren und die Mindestbestände zu bestimmen, die zur Aufrechterhaltung der wesentlichen Abläufe erforderlich sind. Dazu gehört auch das Führen einer aktuellen Liste alternativer Lieferanten.		
B. Für den Betrieb kritische Daten werden identifiziert und klassifiziert. Bei der Datenklassifizierung wird ermittelt, wo sich die Daten befinden, wer Zugang zu ihnen benötigt, wie auf sie zugegriffen wird und ob sie gesichert sind und im Notfall wiederhergestellt werden können.		
C. Kritische IT-Kontrollen und Continuous Monitoring wurden eingeführt, um die Risiken für die Informationssicherheit (einschließlich cyberbezogener Risiken) zu mindern und den Schutz sensibler Daten in Krisen, Disruptionen und Notfällen zu gewährleisten. Zu den Kontrollen und dem Continuous Monitoring gehören Echtzeit-Bedrohungsdaten und die Beschränkung des Zugangs auf autorisierte Benutzer.		

D.	Kritische IT-Assets sind inventarisiert. Zu diesen Assets gehören Hardware, Software und Dienstleistungen, die zur Unterstützung des Betriebs bei Krisen, Disruptionen und Notfällen erforderlich sind.		
E.	Business Continuity und Disaster Recovery Pläne wurden erstellt und enthalten definierte Aufgaben für das zugeordnete Personal und die Wiederherstellungsteams. Die Pläne werden regelmäßig getestet (z. B. in einer „Tabletop-Übung“) und die Ergebnisse der Tests, einschließlich der Verbesserungsmöglichkeiten, werden Geschäftsleitung und Überwachungsorgan mitgeteilt.		
F.	Ein Prozess zur Änderung des Arbeitsumfelds bei Krisen, Disruptionen und Notfällen wurde eingeführt.		
G.	Ein Prozess zum Continuous Monitoring und zur Meldung neu auftretender Bedrohungen und Schwachstellen, die die Resilienz der Organisation beeinträchtigen könnten, wurde eingeführt. Der Prozess dient der Identifizierung, Priorisierung und Umsetzung von Möglichkeiten zur Verbesserung der Resilienz der Organisation, einschließlich Whistleblowing-Systemen oder Systemen zur Sammlung von Risikoinformationen.		
H.	Ein Prozess zur Ausbildung und Schulung des Personals in Bezug auf die Resilienz der Organisation wurde eingerichtet, um sicherzustellen, dass es die Richtlinien und Verfahren kennt, die zu befolgen sind, sowie die Maßnahmen, die zu ergreifen sind, wenn Krisen, Disruptionen und Notfälle auftreten. Der Prozess umfasst auch Übungen, in denen disruptive Szenarien simuliert werden.		
I.	Es wurde ein Prozess eingerichtet, der sicherstellt, dass die erforderlichen operativen, personellen, technologischen und finanziellen Ressourcen bei Krisen, Disruptionen und Notfällen eingeplant und verfügbar sind. Die zur Unterstützung der Resilienz der Organisation erforderlichen finanziellen Ressourcen werden regelmäßig analysiert und der Geschäftsleitung bzw. dem Überwachungsorgan mitgeteilt.		
J.	Ein Prozess zur Überprüfung von Krisen, Disruptionen und Notfällen nach deren Eintreten und ein Lessons-Learned-Prozess zur Analyse der Überprüfungen nach einem Vorfall wurden eingerichtet, einschließlich der Integration der Erkenntnisse in die künftige Resilienzplanung der Organisation.		

Anhang E. Zusätzliche Referenz-Rahmenwerke

Bereich	ISO-Referenz	Geltungsbereich/Klauselüberschriften
Governance	ISO 22316:2017	Policy and strategy; leadership commitment; shared vision; culture; communication; continual improvement.
Risikomanagement	ISO 31000:2018	Scope/context/criteria; risk assessment; treatment; monitoring; communication.
Business Continuity/Disaster Recovery Grundlagen	ISO 22301: 2019; ISO/TS 22317:2021	BCMS context, leadership, planning, operation; BIA activities and outputs.
Resilienz in der Lieferkette	ISO/TS 22318:2021	Supplier dependency analysis; continuity strategies; alternates; assurance requirements.
Bereitschaft im Bereich der Informations- und Kommunikationstechnologie	ISO/IEC 27031	ICT continuity; recovery objectives; testing and improvement; BCMS alignment.

Über das Institute of Internal Auditors

Das IIA ist ein internationaler Berufsverband, der weltweit mehr als 265.000 Mitglieder betreut und mehr als 200.000 Zertifizierungen zum Certified Internal Auditor® (CIA®) vergeben hat. 1941 gegründet, ist The IIA weltweit für den Berufsstand als führend in Standards, Zertifizierungen, Ausbildung, Forschung und fachlichen Leitlinien anerkannt. Für weitere Informationen besuchen Sie bitte theiia.org.

Haftungsausschluss

Das IIA veröffentlicht dieses Dokument zu Informations- und Bildungszwecken. Dieses Material soll keine endgültigen Antworten auf spezifische individuelle Umstände geben und ist daher nur als Leitlinie gedacht. Das IIA empfiehlt, für jede spezifische Situation unabhängigen Expertenrat einzuholen. Das IIA übernimmt keine Verantwortung, falls sich jemand ausschließlich auf dieses Material verlässt.

Copyright

April 2026

The Institute of Internal Auditors

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