Resilienz von Organisationen

Topical Requirement

The Institute of Internal Auditors

Übersetzung durch

DIIR Deutsches Institut für Interne Revision e.V.

Resilienz von Organisationen
Topical Requirement

Das International Professional Practices Framework® des IIA umfasst die Global Internal Audit Standards™, die Topical Requirements und die Global Guidance. Die Topical Requirements sind verbindlich und in Verbindung mit den Standards zu verwenden, welche die maßgebliche Grundlage für die erforderlichen Praktiken darstellen.

Die Topical Requirements formulieren klare Erwartungen an die Internen Revisorinnen und Revisoren, indem sie einen Mindestrahmen für die Prüfung bestimmter Risikothemen vorgeben. Das Risikoprofil der Organisation kann es erforderlich machen, dass die Interne Revision zusätzliche Aspekte des Themas, einschließlich lokaler Vorschriften, berücksichtigt.

Die Einhaltung der Topical Requirements sorgt für konsistente Revisionsleistungen und verbessert die Qualität und Zuverlässigkeit der Revisionsleistungen und -ergebnisse. Letztlich werten die Topical Requirements den Berufsstand der Internen Revision auf.

Interne Revisorinnen und Revisoren müssen die Topical Requirements unter Einhaltung der Global Internal Audit Standards anwenden. Die Einhaltung der Topical Requirements ist für Prüfungsleistungen verbindlich. Für Beratungsleistungen wird sie empfohlen.

Das Topical Requirement ist anwendbar, wenn das Thema:

- Gegenstand eines Auftrags im Revisionsplan ist,
- während der Durchführung eines Auftrags identifiziert wurde oder
- Gegenstand eines Auftrags ist, der nicht im ursprünglichen Revisionsplan enthalten war.

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.

Weitere Informationen finden Sie im „Resilienz von Organisationen Topical Requirement User Guide“.

Resilienz von Organisationen

Resilienz von Organisationen wird von der International Organization for Standardization definiert als „die Fähigkeit einer Organisation, sich an ein sich veränderndes Umfeld anzupassen" (ISO 22316:2017). 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.

Resilienz von Organisationen ist ein Oberbegriff für Risiken, die die Fähigkeit einer Organisation, ihre Kernprodukte und -dienstleistungen zu liefern, das Vertrauen der Stakeholder aufrechtzuerhalten oder ihre strategischen Ziele zu erreichen, erheblich stören oder beeinträchtigen können. Diese Risiken können aus plötzlich auftretenden Ereignissen (wie Naturkatastrophen, Cyberangriffen oder einem geopolitischen Konflikt), anhaltenden Umweltbelastungen (wie Ressourcenknappheit oder Gesundheitskrisen) oder Veränderungen im externen Umfeld (wie technologische Disruptionen, regulatorischen Änderungen oder Reputationsverlust) resultieren.

Bei diesen Risiken kann es sich auch um allmähliche Veränderungen oder sich langsam aufbauenden Druck handeln, der mit der Zeit die Stabilität und Anpassungsfähigkeit einer Organisation beeinträchtigt. Inkrementelle Risiken wie diese können routinemäßig übersehen werden. Resiliente Organisationen antizipieren sowohl plötzliche als auch subtile Risiken und passen sich ihnen an, um erfolgreich zu sein.

Zu den inhärenten Risikofaktoren, die die Gefährdung der Resilienz erhöhen, gehören hochkomplexe Abläufe, globalisierte Lieferketten, zentralisierte Infrastrukturen oder Datensysteme, begrenzte Verfügbarkeit von Arbeitskräften, volatile Märkte und starke Abhängigkeit von kritischen Drittparteien oder geografischen Standorten. Organisationen in Sektoren mit hoher Anforderung an die Zuverlässigkeit oder solche, die unter intensiver behördlicher Beaufsichtigung stehen, können aufgrund der öffentlichen Wirkung und der Compliance-Verpflichtungen mit von Natur aus höheren Risiken konfrontiert sein.

Resilienz von Organisationen konzentriert sich auf die Bewältigung von Risiken vor, während und nach einer Disruption. Interne Revisorinnen und Revisoren beurteilen in der Regel IT-Prozesse und -Kontrollen im Zusammenhang mit Business Continuity und Disaster Recovery. Ein Business Continuity Plan beschreibt die Schritte, die eine Organisation unternimmt, um kritische Funktionen aufrechtzuerhalten und im Falle einer Katastrophe zu den normalen Betriebsabläufen zurückzukehren. Ein Disaster Recovery Plan beschreibt, wie Unternehmen ihre IT-Systeme, kritischen Daten und Abläufe nach einer Disruption wiederherstellen, um den normalen Geschäftsbetrieb wieder aufzunehmen.

Die Resilienz von Organisationen, die beide Pläne umfasst, erfordert strategische Planung, unternehmensweites Risikomanagement, wirksame Führung und Kultur sowie organisationsweite Kontrollprozesse. Starke Kontrollprozesse für die Resilienz von Organisationen ermöglichen es nicht nur, Veränderungen kontinuierlich zu antizipieren, sich darauf vorzubereiten, darauf zu reagieren und sich an sie anzupassen, sondern auch zu überleben und zu gedeihen.

Bewertung und Beurteilung von Governance, Risikomanagement und Kontrollprozessen bezüglich der Resilienz von Organisationen

Dieses Topical Requirement bietet einen konsistenten und umfassenden Ansatz für die Beurteilung der Konzeption und Implementierung von Governance, Risikomanagement und Kontrollprozessen bezüglich der Resilienz von Organisationen.

Governance

Anforderungen

Interne Revisorinnen und Revisoren müssen die folgenden Aspekte der Governance der Resilienz von Organisationen beurteilen:

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.

Risikomanagement

Anforderungen

Interne Revisorinnen und Revisoren müssen die folgenden Aspekte des Risikomanagements der Resilienz von Organisationen beurteilen:

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.

Kontrollprozesse

Anforderungen

Interne Revisorinnen und Revisoren müssen die folgenden Aspekte der Kontrollprozesse in Bezug auf die Resilienz von Organisationen beurteilen:

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.

Über das Institute of Internal Auditors

Das Institute of Internal Auditors (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.

Copyright

April 2026

The Institute of Internal Auditors

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