Entwurf für die öffentliche Konsultation Resilienz in 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, zusätzliche Aspekte des Themas zu berücksichtigen.

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 gemäß den Global Internal Audit Standards die Topical Requirements anwenden. Die Einhaltung der Topical Requirements ist für Prüfungsleistungen verbindlich. Für Beratungsleistungen wird sie empfohlen.

Das Topical Requirement ist anwendbar, wenn das Thema:

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

Nachweise dafür, dass die Anwendbarkeit jeder einzelnen Anforderung des Topical Requirement beurteilt wurde, sind zu dokumentieren und aufzubewahren. Nicht alle einzelnen Anforderungen sind bei jedem Auftrag anwendbar. Wenn Anforderungen ausgeschlossen werden, muss eine Begründung dokumentiert und aufbewahrt werden. Die Einhaltung des Topical Requirement ist verbindlich und wird im Rahmen der Qualitätsbeurteilung bewertet.

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

Resilienz in Organisationen

Resilienz in Organisationen wird in ISO 22316:2017, Security and resilience – Organizational resilience – Principles and attributes, herausgegeben von der International Organization for Standardization, definiert als die „Fähigkeit einer Organisation, ein sich veränderndes Umfeld zu absorbieren und sich anzupassen“. Die Resilienz

von Organisationen ist ein umfassendes Thema, das wichtige strategische, operative, technologische, menschliche, soziale und finanzielle Elemente umfasst. Resilienz in Organisationen befasst sich mit Risiken, die die Fähigkeit einer Organisation, ihre Kernprodukte und -dienstleistungen zu liefern, das Vertrauen der Stakeholder zu erhalten oder ihre strategischen Ziele zu erreichen, erheblich stören oder beeinträchtigen können. Diese Risiken können aus plötzlich auftretenden Ereignissen (wie Naturkatastrophen, Cyberangriffen und geopolitischen Konflikten), anhaltenden und kritischen Umweltbedingungen (wie Ressourcenknappheit oder Gesundheitskrisen) oder Veränderungen im externen Umfeld (wie technologische Disruptionen, regulatorische 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 gefährdet. 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 hohe betriebliche Komplexität, globalisierte Lieferketten, zentralisierte Infrastruktur oder Datensysteme, begrenzte Verfügbarkeit von Arbeitskräften, unbeständige Marktbedingungen und starke Abhängigkeit von kritischen Drittparteien oder geografischen Standorten. Organisationen in Sektoren mit hohen Zuverlässigkeitsanforderungen oder solche, die unter intensiver regulatorischer Beaufsichtigung stehen, können aufgrund der öffentlichen Wirkung und der Verpflichtungen zur Einhaltung von Vorschriften auch mit einem höheren Risiko konfrontiert sein.

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 nach einer Katastrophe zu den normalen Betriebsfunktionen zurückzukehren. Ein Disaster Recovery Plan beschreibt, wie Organisationen IT-Systeme und kritischen Daten während einer Unterbrechung schützen werden. Resilienz erfordert in Organisationen auch strategische Planung, unternehmensweites Risikomanagement, wirksame Führung und Kultur sowie organisationsweite Kontrollprozesse. Starke Kontrollprozesse für die Resilienz ermöglichen es Organisationen 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 für Resilienz in Organisationen

Dieses Topical Requirement liefert einen konsistenten, umfassenden Ansatz zur Beurteilung der Gestaltung und Implementierung von Governance, Risikomanagement und Kontrollprozessen für Resilienz in Organisationen. Die Anforderungen stellen einen Mindestrahmen für die Beurteilung der Resilienz in Organisationen dar.

Governance

Anforderungen:

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

A. Das Leitungs- und Überwachungsorgan hat eine formelle Strategie für die Resilienz der Organisation festgelegt und dokumentiert, die Ziele enthält, die mit dem Auftrag und der Vision der Organisation übereinstimmen und diese unterstützen. Die Strategie befasst sich mit den operativen, technologischen und finanziellen Elementen, die erforderlich sind, um Krisen, Disruptionen und Notfällen standzuhalten

und den Betrieb aufrechtzuerhalten, sowie mit der Frage, wie man sich anschließend erholt und anpasst. Die Strategie steht im Einklang mit dem Gesamtkonzept der Organisation für das Risikomanagement und wird regelmäßig überprüft und aktualisiert.

B. Das Leitungs- und Überwachungsorgan wird regelmäßig über den aktuellen Stand der Umsetzung der Strategie und der Ziele für Resilienz informiert. Dadurch wird sichergestellt, dass die Resilienz in die strategische Beaufsichtigung, die langfristigen Planungsprozesse und die Organisationskultur eingebettet ist, einschließlich der Ressourcen- und Budgetüberlegungen, die zur Unterstützung wichtiger Geschäftsaktivitäten erforderlich sind.

C. Kritische operative, technologische und finanzielle Prozesse im Zusammenhang mit der Resilienz der Organisation wurden ermittelt. Richtlinien und Verfahren für kritische Prozesse wurden eingeführt, die regelmäßig überprüft und bei Bedarf aktualisiert werden, um das Kontrollumfeld zu stärken.

D. Es wird eine Struktur für die Einsatzleitung eingerichtet, die Entscheidungshierarchien, Kommunikations- und Eskalationsverfahren sowie Führungs- und operative Aufgaben und Verantwortlichkeiten umfasst. Die Struktur dient der Überwachung und Unterstützung der Festlegung von Zielen der Resilienz in der Organisation.

E. Ein Prozess wurde eingerichtet, mithilfe dessen die Kompetenzen der Personen, die kritische Rollen in den Resilienzprozessen einnehmen, regelmäßig neu beurteilen werden. Es gibt einen Nachfolgeplan, in dem Schlüsselpositionen und potenzielle Kandidaten für die Nachfolge festgelegt sind.

F. Ein Prozess wurde eingerichtet, mithilfe dessen relevante interne und externe Stakeholder in die Identifizierung, Analyse und Reaktion auf bestehende Schwachstellen und neu auftretende Bedrohungen eingebunden werden, die das Erreichen der Resilienzziele der Organisation beeinträchtigen könnten. Zu den Stakeholdern gehören u. a. Geschäftsleitung, Betrieb, Risikomanagement, IT, die Lieferkette/Beschaffung, Immobilien, Personalabteilung, Finanzabteilung, Rechtsabteilung, Compliance-Abteilung, Öffentlichkeitsarbeit, kritische Lieferanten, Kunden und Aufsichtsbehörden.

RISIKOMANAGEMENT

Anforderungen:

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

A. Die Risikobeurteilungs- und Risikomanagementprozesse der Organisation umfassen die Identifizierung, Analyse, Minderung und Überwachung von Bedrohungen, die den Betrieb stören könnten. Die Risikomanagementstrategie für die Resilienz der Organisation wird in der gesamten Organisation bekannt gemacht und regelmäßig überprüft.

B. Die Risiken im Zusammenhang mit der Resilienz der Organisation werden regelmäßig beurteilt und in der gesamten Organisation gemanagt. Die Risikobeurteilung und das Risikomanagement können folgende Bereiche umfassen: Betrieb, unternehmensweites Risikomanagement, IT, Lieferkette/Beschaffung, Immobilien, Personal, Finanzen, Recht, Compliance, Öffentlichkeitsarbeit, kritische Lieferanten, Reputation, aufkommende Risiken und andere.

C. Rechenschaftspflicht und Verantwortung für das Risikomanagement der Resilienz in der Organisation sind festgelegt. Es wird eine Person oder ein Team bestimmt, die/das regelmäßig überwacht und berichtet, wie die Risiken der Resilienz der Organisation gehandhabt werden, einschließlich der Ressourcen, die zur Minderung der Risiken und zur Identifizierung neu aufkommender Bedrohungen der Resilienz der Organisation erforderlich sind.

D. Ein Prozess wurde eingerichtet, mithilfe dessen die (neu aufkommenden oder bereits identifizierten) Risiken für die Resilienz der Organisation überwacht werden und solche Risiken schnell eskaliert werden, die ein Niveau erreichen, das gemäß den festgelegten Risikomanagementrichtlinien und der Risikotoleranz der Organisation oder den geltenden rechtlichen oder regulatorischen Anforderungen als inakzeptabel gilt. Die finanziellen und nicht-finanziellen Auswirkungen des Risikos der Resilienz der Organisation werden berücksichtigt.

E. Das Management hat einen Prozess eingeführt und testet diesen regelmäßig, um auf Krisen, Disruptionen und Notfälle zu reagieren und sich davon zu erholen. Der Prozess der Reaktion auf einen Vorfall und der Wiederherstellung umfasst die Erkennung, die Eindämmung, die Wiederherstellung und die Analyse nach dem Vorfall. Der Ansatz zur Reaktion auf Vorfälle umfasst Szenarioanalysen und regelmäßige Stresstests für eine Reihe plausibler Störfälle. Die Ergebnisse dieser Übungen werden von der Geschäftsleitung bzw. dem Überwachungsorgan überprüft, wobei die Maßnahmen zur Verbesserung verfolgt und regelmäßig berichtet werden. Die Empfehlungen sind umsetzbar und enthalten klare Verantwortlichkeiten und Zeitvorgaben.

KONTROLLEN

Anforderungen:

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

A. Es wurde ein Prozess eingeführt, mithilfe dessen kritische Drittparteien (Lieferanten und Verkäufer) und Mindestlagerbestände ermittelt werden, die für die Aufrechterhaltung lebenswichtiger Vorgänge erforderlich sind. Dazu gehört auch das Führen einer 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 in einem Notfall wiederhergestellt werden können.

C. Es werden kritische IT-Kontrollen und eine kontinuierliche Überwachung 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 der kontinuierlichen Überwachung gehören Echtzeit-Bedrohungsdaten und die Beschränkung des Zugangs auf autorisierte Benutzer.

D. Kritische IT-Anlagen werden inventarisiert. Sie umfassen die 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. Die Pläne beinhalten definierte Aufgaben für das ihnen zugewiesene Personal und die Wiederherstellungsteams. Die Pläne werden in regelmäßigen Abständen getestet (z. B. in einer "Tabletop-Übung"), und die Ergebnisse der Tests,

einschließlich der Verbesserungsmöglichkeiten, werden der Geschäftsleitung und dem Überwachungsorgan mitgeteilt.

F. Ein Prozess zur Anpassung des Arbeitsumfelds bei Krisen, Disruptionen und Notfällen wurde 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.

G. Ein 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 der Organisation wurde eingeführt. Der Prozess kann Systeme für Meldungen durch Hinweisgeber oder die Sammlung von Risikoinformationen umfassen.

H. Es wurde ein Prozess eingerichtet, mithilfe dessen das Personal in Bezug auf die Resilienz der Organisation geschult und trainiert wird, um sicherzustellen, dass es die zu befolgenden Richtlinien und Verfahren sowie die zu ergreifenden Maßnahmen kennt, wenn Krisen, Disruptionen und Notfälle auftreten. Der Prozess umfasst Übungen, in denen Disruptionsszenarien simuliert werden.

I. Ein Prozess wurde eingeführt, mithilfe dessen sichergestellt wird, dass die erforderlichen personellen, technischen und finanziellen Ressourcen für Krisen, Disruptionen und Notfälle eingeplant und verfügbar sind. Der Prozess kann die Vorabgenehmigung der Finanzierung beinhalten.

J. Die zur Unterstützung der Resilienz der Organisation erforderlichen finanziellen Ressourcen werden regelmäßig analysiert und dem Leitungs- und Überwachungsorgan mitgeteilt. Die Analyse umfasst eine Beurteilung der Liquidität, des Versicherungsschutzes und der Finanzierungsvereinbarungen für unvorhergesehene Ereignisse.

K. Ein Prozess wurde eingeführt, mithilfe dessen Krisen, Disruptionen und Notfälle nach deren Eintreten und zur Analyse der Erkenntnisse nach dem Vorfall überprüft werden, einschließlich der Einbeziehung dieser Erkenntnisse in die künftige Planung der Resilienz der Organisation.

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. Das IIA wurde 1941 gegründet und ist weltweit als führend in den Bereichen Standards, Zertifizierungen, Bildung, Forschung und fachliche Leitlinien für den Berufsstand der Internen Revision anerkannt. Weitere Informationen finden Sie unter www.theiia.org.

Copyright

September 2025

