Cybersicherheit

Topical Requirement

The Institute of
Internal Auditors

Cybersicherheit Topical Requirement

Das International Professional Practices Framework® (Internationalen Grundlagen für die berufliche Praxis) umfasst die Global Internal Audit Standards™, die Topical Requirements und 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

A. Gegenstand eines Auftrags im Revisionsplan ist,
B. während der Durchführung eines Auftrags identifiziert wurde oder
C. 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 ausgeklammert 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 Cybersicherheit Topical Requirement User Guide.

Cybersicherheit

Das National Institute of Standards and Technology (NIST) definiert Cybersicherheit einfach als „die Fähigkeit, die Nutzung des Cyberraums vor Cyberangriffen zu schützen oder zu verteidigen". Cybersicherheit ist ein Teilbereich der übergreifenden Informationssicherheit, die das NIST wie folgt definiert: „Der Schutz von Informationen und Informationssystemen vor unbefugtem Zugriff, Verwendung, Offenlegung, Störung, Änderung oder Zerstörung, um Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten."

Cybersicherheit verringert das Risiko, indem sie das gesamte Kontrollumfeld stärkt und die Informationswerte einer Organisation vor unbefugtem Zugriff, Störung, Veränderung oder Zerstörung schützt. Cyberangriffe können zu direkten und indirekten Auswirkungen führen, die oft signifikant sind, da Computer, Netzwerke, Programme, Daten und sensible Informationen wichtige Bestandteile der meisten Organisationen sind.

Bewertung und Beurteilung von Governance, Risikomanagement und Kontrollprozessen der Cybersicherheit

Dieses Topical Requirement bietet einen konsistenten, umfassenden Ansatz für die Beurteilung der Gestaltung und Implementierung von Governance, Risikomanagement und Kontrollprozessen der Cybersicherheit. Die Anforderungen stellen einen Mindestrahmen für die Beurteilung der Cybersicherheit in einer Organisation dar.

GOVERNANCE: Bewertung und Beurteilung der Governance von Cybersicherheit

Anforderungen:

Interne Revisorinnen und Revisoren müssen in Bezug auf die Governance von Cybersicherheit der Organisation Folgendes beurteilen:

- **A.** Eine formale Strategie und Ziele für die Cybersicherheit werden festgelegt und regelmäßig aktualisiert. Aktualisierungen zur Erreichung der Cybersicherheitsziele werden regelmäßig kommuniziert und vom Leitungs- und Überwachungsorgan überprüft, einschließlich der Ressourcen und Budgetüberlegungen zur Unterstützung der Cybersicherheitsstrategie.
- **B.** Um das Kontrollumfeld zu stärken, wurden Richtlinien und Verfahren für die Cybersicherheit eingeführt und regelmäßig aktualisiert.
- **C.** Aufgaben und Verantwortlichkeiten, die die Ziele der Cybersicherheit unterstützen, sind festgelegt, und es gibt einen Prozess zur regelmäßigen Beurteilung der Kenntnisse, Fähigkeiten und Fertigkeiten der Personen, die diese Aufgaben übernehmen.
- **D.** Die relevanten Stakeholder werden einbezogen, um bestehende Schwachstellen und neu auftretende Bedrohungen im Bereich der Cybersicherheit zu diskutieren und darauf zu reagieren. Zu den Stakeholdern gehören die Geschäftsleitung, das operative Geschäft, das Risikomanagement, die Personalabteilung, die Rechtsabteilung, die Complianceabteilung, Lieferanten und andere.

RISIKOMANAGEMENT: Bewertung und Beurteilung des Risikomanagements der Cybersicherheit

Anforderungen:

Interne Revisorinnen und Revisoren müssen in Bezug auf das Risikomanagement der Cybersicherheit Folgendes beurteilen:

- **A.** Die Risikobeurteilungs- und Risikomanagementprozesse der Organisation umfassen die Identifizierung, Analyse, Minderung und Überwachung von Bedrohungen der Cybersicherheit und deren Auswirkungen auf die Erreichung strategischer Ziele.
- **B.** Das Risikomanagement der Cybersicherheit wird organisationsweit durchgeführt und kann folgende Bereiche umfassen: IT, organisationsweites Risikomanagement (ERM), Personalwesen, Recht, Compliance, operatives Geschäft, Lieferkette, Rechnungswesen, Finanzen und andere.
- **C.** Rechenschaftspflicht und Verantwortung für das Risikomanagement der Cybersicherheit sind festgelegt. Es wurde eine Person oder ein Team bestimmt, die/das regelmäßig überwacht und berichtet, wie Cybersicherheitsrisiken gemanagt werden, einschließlich

der Ressourcen, die zur Risikominderung und zur Identifizierung neuer Bedrohungen der Cybersicherheit erforderlich sind.

D. Es wurde ein Prozess eingerichtet, um jedes (neu auftretende oder bereits identifizierte) Cybersicherheitsrisiko, das ein inakzeptables Niveau erreicht, gemäß den festgelegten Risikomanagementrichtlinien der Organisation oder den geltenden rechtlichen und regulatorischen Anforderungen schnell zu eskalieren. Finanzielle und nichtfinanzielle Auswirkungen von Cybersicherheitsrisiken sollten berücksichtigt werden.

E. Es wurde ein Prozess eingerichtet, um das Bewusstsein für Cybersicherheitsrisiken an das Management und die Mitarbeiterinnen und Mitarbeiter zu kommunizieren und das Management zu veranlassen, Probleme, Lücken, Schwachstellen oder Versagen von Kontrollen regelmäßig zu überprüfen und zeitnah zu melden und zu beheben.

F. Die Organisation hat einen Prozess zur Reaktion auf Cybersicherheitsvorfälle und zur Wiederherstellung eingeführt, der die Erkennung, Eindämmung, Wiederherstellung und Analyse nach dem Vorfall umfasst. Der Prozess zur Reaktion auf Vorfälle und zur Wiederherstellung wird regelmäßig getestet.

KONTROLLEN: Bewertung und Beurteilung von Kontrollprozessen der Cybersicherheit

Anforderungen:

Interne Revisorinnen und Revisoren müssen in Bezug auf die Cybersicherheits-Kontrollprozesse Folgendes beurteilen:

A. Es wurde ein Prozess eingerichtet, der sicherstellt, dass sowohl interne Kontrollen als auch Kontrollen von Lieferanten vorhanden sind, um die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Daten der Organisation zu schützen. Es werden regelmäßig Bewertungen durchgeführt, um festzustellen, ob die Kontrollen so funktionieren, dass die Cybersicherheitsziele der Organisation erreicht und Probleme umgehend gelöst werden können.

B. Es wurde ein Talentmanagementprozess eingeführt, der Schulungen zur Entwicklung und Aufrechterhaltung technischer Kompetenzen im Zusammenhang mit Cybersicherheitsmaßnahmen umfasst. Dieser Prozess wird regelmäßig überprüft.

C. Es wurde ein Prozess zur kontinuierlichen Überwachung und Meldung neu auftretender Bedrohungen und Schwachstellen der Cybersicherheit sowie zur Identifizierung, Priorisierung und Implementierung von Möglichkeiten zur Verbesserung der Cybersicherheitsmaßnahmen eingeführt.

D. Die Cybersicherheit ist Teil des Lebenszyklusmanagements (Auswahl, Nutzung, Wartung und Stilllegung) aller IT-Ressourcen, einschließlich Hardware, Software und Dienste von Lieferanten.

E. Es wurden Prozesse zur Stärkung der Cybersicherheit eingerichtet, einschließlich Konfiguration, Verwaltung von Endbenutzergeräten, Verschlüsselung, Patches, Benutzerzugriffsverwaltung und Überwachung von Verfügbarkeit und Leistung. Cybersicherheitsaspekte werden in die Softwareentwicklung einbezogen (DevSecOps).

F. Es wurden netzwerkbezogene Kontrollen eingeführt, wie z. B. Netzwerkzugangskontrollen und -segmentierung, die Nutzung und Positionierung von Firewalls, limitierte Verbindungen von und zu externen Netzwerken, Virtual Private Networks (VPN)/Zero Trust Network Access (ZTNA), Netzwerkkontrollen für das Internet

der Dinge (IoT) und Systeme zur Erkennung und Verhinderung von Eindringlingen (IDS und IPS).

G. Sicherheitskontrollen für die Endpunktkommunikation wurden für Dienste wie E-Mail, Internetbrowser, Videokonferenzen, Messaging, soziale Medien, Cloud- und Datenaustauschprotokolle eingerichtet.

About The Institute of Internal Auditors

The Institute of Internal Auditors (The IIA) is an international professional association that serves more than 255,000 global members and has awarded more than 200,000 Certified Internal Auditor® (CIA®) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit www.theiia.org.

Copyright

Februar 2025

The Institute of Internal Auditors

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