Cybersicherheit

Topical Requirement

User Guide

The Institute of
Internal Auditors

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 Global Internal Audit 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. Sie 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 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.

Bei der Anwendung des Topical Requirement spielt die professionelle Beurteilung eine wichtige Rolle. Risikobeurteilungen sind die Grundlage für die Entscheidung der Revisionsleitung, welche Aufträge in den Revisionsplan aufgenommen werden (Standard 9.4 „Revisionsplan“). Darüber hinaus nutzen die Internen 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“). Anhang A „Praktische Anwendungsbeispiele" beschreibt, wie Interne Revisorinnen und Revisoren feststellen, ob ein Topical Requirement anzuwenden ist.

Es ist nachzuweisen, dass die Anwendbarkeit jeder Anforderung des Topical Requirement beurteilt wurde, einschließlich einer Begründung für den Ausschluss von Anforderungen. Die Einhaltung des Topical Requirement muss, wie in Standard 14.6 „Auftragsdokumentation“ beschrieben, gemäß der professionellen Beurteilung der Prüferinnen und Prüfer dokumentiert werden.

Das Topical Requirement Cybersicherheit nennt einen Grundstock an zu berücksichtigenden Kontrollprozessen, aber Organisationen, die das Cyberrisiko als sehr hoch einschätzen, müssen möglicherweise zusätzliche Aspekte beurteilen.

Stellt die Revisionsleitung fest, dass die Interne Revision nicht über die erforderlichen Kenntnisse für die Durchführung von Revisionsaufträgen zu einem Thema der Topical Requirements verfügt, kann der Auftrag outgesourct werden (Standard 3.1 „Kompetenz“, 7.2 „Qualifikation der Revisionsleitung“, 10.2 „Management personeller Ressourcen“). Aber selbst dann entbindet die Auslagerung die Interne Revision nicht von ihrer Verantwortung für die Einhaltung der Topical Requirements. 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“).

Leistung, 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“).

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 C kann als Referenz und zur Dokumentation der Tätigkeiten der Internen Revisorinnen und Revisoren verwendet werden.

Qualitätssicherung

Die Standards verlangen, dass die Revisionsleitung ein Programm zur Qualitätssicherung und Verbesserung entwickelt, umsetzt und aufrechterhält, das alle Aspekte der Internen Revision abdeckt (Standard 8.3 „Qualität“). 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 wird im Rahmen von Qualitätsbeurteilungen bewertet. Zur Vorbereitung auf eine Qualitätsüberprüfung können Interne Revisorinnen und Revisoren das Tool in Anhang C verwenden.

Cybersicherheit

Cybersicherheit ist ein umfassendes Thema, das die meisten technologischen Aspekte jeder Organisation betrifft. Neben der IT ist die Cybersicherheit in der Regel auch Teil der Geschäftsprozesse, sodass Interne Revisorinnen und Revisoren bei der Planung, der Festlegung des Umfangs und der Durchführung von Prüfungsaufträgen cyberbezogene Risiken beurteilen müssen.

Das National Institute of Standards and Technology (NIST), das zum US-Handelsministerium gehört, definiert Cybersicherheit einfach als „die Fähigkeit, die Nutzung des Cyberraums vor Cyberangriffen zu schützen oder zu verteidigen". Das Cybersicherheit Topical Requirement konzentriert sich auf die Außengrenzen, die Organisationen sichern, um Risiken durch unbefugte Benutzer und bösartige Cyberbedrohungen zu mindern. Cybersicherheit ist ein Teilbereich der übergreifenden Informationssicherheit, die das NIST definiert als „Schutz von Informationen und Informationssystemen vor unbefugtem Zugriff, Verwendung, Offenlegung, Störung, Änderung oder Zerstörung, um Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten".

Zu den Anforderungen des Cybersicherheit Topical Requirement gehören:

- Governance – klar definierte, grundlegende Cybersicherheitsziele und -strategien, die die Ziele, Richtlinien und Verfahren der Organisation unterstützen.
- Risikomanagement – Verfahren zur Identifizierung, Analyse, Steuerung und Überwachung von Cyberbedrohungen, einschließlich eines Verfahrens zur unverzüglichen Eskalation von Cyberrisiken.
- Kontrollen – vom Management eingerichtete und regelmäßig bewertete Kontrollprozesse zur Minderung von Cyberrisiken.

Überlegungen

Interne Revisorinnen und Revisoren können die folgenden Überlegungen bei der Beurteilung der Anforderungen im Cybersicherheit Topical Requirement zur Hilfe nehmen. Diese Überlegungen, die auf die Anforderungen verweisen, sind beispielhaft, aber nicht verbindlich. Interne Revisorinnen und Revisoren sollten sich auf ihr professionelles Urteil verlassen, wenn sie entscheiden, was sie in ihre Beurteilungen einbeziehen.

Überlegungen zur Governance

Um zu beurteilen, wie die Governance-Prozesse auf die Ziele der Cybersicherheit angewandt werden, können Interne Revisorinnen und Revisoren Folgendes überprüfen:

A. Formalisierter, dokumentierter Strategieplan und Ziele für die Cybersicherheit, einschließlich des Nachweises, dass das Leitungs- und Überwachungsorgan regelmäßig (in der Regel vierteljährlich) die von der Leitung der Informationssicherheitsfunktion, z. B. dem Chief Information Security Officer (CISO), vorgelegten Aktualisierungen zur Cybersicherheit überprüft. Der Nachweis kann die Berichterstattung über folgende Punkte umfassen:
   - Überwachung der Erreichung der strategischen Ziele.
   - Budgetbedarf zur Unterstützung der Cybersicherheitsziele.
   - Fokussierung auf Risiken und internen Kontrollen, einschließlich des Fortschritts bei der Behebung von Schwachstellen.
   - Leistungsindikatoren (KPIs) zur Erfolgsmessung.
   - Personelle Ressourcen, die für die Rekrutierung, Schulung und Entwicklung von Cybersicherheitspersonal benötigt werden.

B. Richtlinien, Verfahren und andere relevante Unterlagen, die zur Verwaltung von Cybersicherheitsprozessen verwendet werden, einschließlich:
   - Richtlinien, die mindestens jährlich überprüft und aktualisiert werden. Neu auftretende Cyberrisiken können eine häufigere Überprüfung und Aktualisierung erforderlich machen.
   - Ein Verfahren, mit dem festgestellt werden kann, ob die Richtlinien und Verfahren zur Unterstützung der Cybersicherheitsmaßnahmen ausreichen.
   - Anerkannte Rahmenwerke (NIST, COBIT und andere) zur Stärkung von Cybersicherheitsprozessen und internen Kontrollen.

C. Rollen und Verantwortlichkeiten, die das Erreichen von Cybersicherheitszielen unterstützen, einschließlich einer Struktur, die sicherstellt, dass die Cybersicherheitsfunktion einer Ebene in der Organisation unterstellt ist, die über eine ausreichende Sichtbarkeit verfügt, um organisatorische Unterstützung zu erhalten.
   - Ein Prozess zur regelmäßigen Beurteilung der Kenntnisse, Fähigkeiten und Fertigkeiten des Personals, das Aufgaben im Bereich der Cybersicherheit wahrnimmt.

D. Nachweis für die Zusammenarbeit mit relevanten Stakeholdern (z. B. Geschäftsleitung, operatives Geschäft, Risikomanagement, Personalabteilung, Rechtsabteilung, Compliance, strategische Lieferanten und andere), einschließlich der Kommunikation über bestehende und neu auftretende Cyberrisiken und bekannte potenzielle

Schwachstellen. Nachweise für die Kommunikation können Sitzungsprotokolle, Berichte oder E-Mails sein.

Überlegungen zum Risikomanagement

Um zu beurteilen, wie die Risikomanagementprozesse auf die Ziele der Cybersicherheit angewandt werden, können Interne Revisorinnen und Revisoren Folgendes überprüfen:

A. Wie die Organisation das Cybersicherheitsrisiko beurteilt und steuert, einschließlich der Art und Weise, wie Bedrohungen und Schwachstellen
   - ursprünglich identifiziert und gemeldet werden,
   - analysiert werden, um das Risiko für das Erreichen der Unternehmensziele 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.

B. Wie die Organisation regelmäßig Beiträge zum Cybersicherheitsrisikomanagement aus Funktionsbereichen wie IT, organisationsweites Risikomanagement (ERM), Personalwesen, Recht, Compliance, operatives Geschäft, Rechnungswesen und Finanzen einholt. Ein funktionsübergreifendes Cybersicherheitsteam oder ein IT-Lenkungsausschuss kann zur Informationsbeschaffung genutzt werden.

C. Die Art und Weise, wie die Organisation die Rechenschaftspflicht und Verantwortung für das Management von Cybersicherheitsrisiken einer Person oder einem Team zugewiesen hat.
   - Die verantwortliche(n) Person(en) sollte(n) in regelmäßigen Abständen (vierteljährlich, monatlich oder nach Bedarf) die laufenden Aktualisierungen der Cybersicherheitsrisiken in der gesamten Organisation bekanntgeben und gegebenenfalls auch den Ressourcenbedarf für Risikominderungsstrategien angeben.

D. Die Eskalationsprozesse für Cybersicherheitsrisiken, einschließlich der Art und Weise, wie der Grad der Bedrohung oder des Risikos bewertet, zugewiesen und priorisiert wird. Die Überprüfung kann auch Folgendes identifizieren:
   - Die von der Organisation definierten Risikostufen – z. B. hoch, mittel und niedrig – mit detaillierten Erläuterungen zu jeder Risikostufe und Eskalationsverfahren für jede Risikokategorie.
   - Liste der derzeit ermittelten Cybersicherheitsrisiken und der Status der Risikominderung für jedes einzelne Risikoereignis.
   - Anwendbare gesetzliche, regulatorische und Compliance-Anforderungen.
   - Sowohl finanzielle als auch nichtfinanzielle (z. B. Reputation) Risikoauswirkungen.

E. Den Prozess zur Kommunikation von Cybersicherheitsrisiken an das Management und die Mitarbeiterinnen und Mitarbeiter, der Folgendes umfasst:

- Regelmäßige (mindestens jährliche) Mitarbeiterschulungen zur Cybersicherheit, z. B. unangekündigte, simulierte Phishing-Kampagnen, um das Bewusstsein der Organisation zu testen und zu überprüfen.
- Aktuelle Informationen über die Behebung bestehender Cybersicherheitsprobleme mit voraussichtlichen Fertigstellungsterminen.
- Überwachung der Nichteinhaltung von Regelungen, einschließlich aktueller Informationen für Geschäftsleitung und Überwachungsorgan.
- Neubeurteilung von Bedrohungen, wenn sich Risikobereitschaft und Risikotoleranz der Organisation ändern.

F. Prozesse, die die Organisation in Bezug auf die Reaktion auf Vorfälle und die Wiederherstellung implementiert hat, einschließlich:

- Ein dokumentierter Plan, der überprüft und aktualisiert wird, wenn sich die Abläufe in der Organisation im Laufe der Zeit ändern. Der Plan sollte Folgendes enthalten:
  - Wie Vorfälle entdeckt und gemeldet werden.
  - Wie Vorfälle eingedämmt werden, um weiteren Schaden zu verhindern.
  - Wie die Organisation sich erholen und reagieren wird, um den Betrieb wieder aufzunehmen.
  - Wie der Vorfall analysiert wird, um Lehren daraus zu ziehen und ähnliche Vorfälle in Zukunft zu verhindern.
- Regelmäßige (mindestens jährliche) Tests (am Schreibtisch) und Berichterstattung der Ergebnisse an die Geschäftsleitung und relevante Stakeholder. Aus den Tests können sich Maßnahmenpläne ergeben.

Überlegungen zum Kontrollprozess

Um zu beurteilen, wie die Kontrollprozesse auf die Ziele der Cybersicherheit angewandt werden, können Interne Revisorinnen und Revisoren Folgendes überprüfen:

A. Den Ansatz des Managements für den Aufbau eines wirksamen internen Kontrollumfelds im Bereich der Cybersicherheit, einschließlich:

- Beurteilung und Umsetzung der internen Kontrollen auf der Grundlage des Prozesses zur Beurteilung der Unternehmensrisiken, die erforderlich sind, um erhöhte Risiken zu mindern und sensible, kritische, persönliche oder vertrauliche Daten zu schützen.
- Bestimmung des Ressourcenbedarfs für die Aufrechterhaltung wichtiger Cybersicherheitskontrollen.
- Berücksichtigung von Kontrollen bei den Lieferanten als Teil des Kontrollumfelds, einschließlich der Überprüfung von Berichten von Anbietern über die Kontrollen der Dienstleistungsorganisation (Service Organization Controls, SOC) vor Beginn der Geschäftsbeziehung und während der gesamten Dauer der Beziehung.
- Regelmäßige Tests, ob die Cybersicherheitskontrollen so funktionieren, dass die Risiken gemindert und die Cybersicherheitsziele erreicht werden.
- Verfahren zur Behebung von Mängeln bei den internen Kontrollen oder zur Behebung von Feststellungen, die sich aus der Beurteilung der Internen Revision oder anderer Assurance Provider ergeben (z. B. Penetrationstests).

B. Den Talentmanagementprozess der Organisation für die Rekrutierung und Schulung von Cybersicherheitsfachkräften, einschließlich der Art und Weise, wie die Organisation Möglichkeiten zur Steigerung der Fähigkeiten von Cybersicherheitsfachkräften identifiziert, um technisches Wissen zu unterstützen und das Bewusstsein der Organisation für neue Probleme zu verbessern.
   - Beispiele hierfür sind die Teilnahme an Schulungen, die Beteiligung an Gruppen zum Wissensaustausch und die laufende berufliche Weiterbildung, einschließlich der Erlangung cyberbezogenen Zertifizierungen.

C. Der kontinuierliche Prozess des Managements zur Identifizierung, Priorisierung, Überwachung und Berichterstattung neu auftretender Bedrohungen und Schwachstellen der Cybersicherheit, der sich auf den täglichen Betrieb konzentriert. Die Überprüfung kann auch beinhalten, dass Prozesse zur Beurteilung von Bedrohungen und Schwachstellen im Zusammenhang mit neuen oder aufkommenden Technologien, wie dem Einsatz künstlicher Intelligenz, eingerichtet werden.

D. Die Prozesse und Kontrollen des Managements zur Steuerung und zum Schutz von IT-Anlagen während des gesamten Lebenszyklus, einschließlich Auswahl, Nutzung, Wartung und Stilllegung von Hardware, Software und Anbieterdiensten. Zur Hardware gehören Server, Netzwerkgeräte (wie Router oder Firewalls), Desktops, Laptops, Handys, Tablets und Peripheriegeräte. Software umfasst Betriebssysteme (z. B. Windows), Enterprise Resource Planning (ERP) Software, Anwendungen, Antivirenprogramme und andere. Zu den Überlegungen zu Hardware und Software können gehören:
   - Einsatz von Verschlüsselung, Antivirensoftware, Verwaltung mobiler Geräte, komplexe Passwortanforderungen, Virtual Private Network (VPN)/Zero Trust Networking (ZTN) zur Authentifizierung und regelmäßige Aktualisierung der Firmware durch die Organisation.
   - Ein Bestandsverwaltungsprozess, der sicherstellt, dass die vom Unternehmen ausgegebene Hardware bei der Ausgabe eine angemessene Sicherheitskonfiguration aufweist und bei der Ausmusterung ordnungsgemäß entsorgt wird.
   - Datenbankbezogene Kontrollen, die die Beschränkung des Benutzer- und Administratorzugriffs, die Gewährleistung von Verschlüsselung, die Sicherung und das Testen von Datenbanken sowie das Vorhandensein starker Netzwerksicherheitskontrollen umfassen.
   - Wie Cybersicherheitsbedrohungen oder -Schwachstellen im Lebenszyklus der Systementwicklung (System Development Lifecycle, SDLC) berücksichtigt werden.
   - Der von Entwicklung, Sicherheit und Betrieb (DevSecOps) verwendete Ansatz, um sicherzustellen, dass der Softwareentwicklungsprozess Cybersicherheit beinhaltet, um Schwachstellen proaktiv zu identifizieren.

E. Prozesse zur Verbesserung der Cybersicherheit, einschließlich:
   - Konfiguration der Sicherheitseinstellungen zur Minimierung des Cybersicherheitsrisikos.
   - Die Verwaltung mobiler Geräte (einschließlich der Nutzung von E-Mail und Anwendungen) ist so konfiguriert, dass Cybersicherheitsrisiken gemindert werden und ein Fernzugriff möglich ist, falls das Gerät eines Benutzers kompromittiert ist.

- Die Verwendung von Verschlüsselung für Daten „im Ruhezustand“, wie z. B. auf einer Festplatte gespeicherte Informationen, oder für Daten „in Übertragung“, wie z. B. E-Mails.
- Patches für Server oder Software (z. B. Betriebssysteme) mit den neuesten Sicherheitsversionen.
- Management des Benutzerzugriffs, wie z. B. die Verwendung von Multifaktor-Authentifizierung (MFA) und eindeutige Benutzer-IDs mit komplexen Passwörtern, die in regelmäßigen Abständen ablaufen.
- Überwachung der eingerichteten Kontrollen, um festzustellen, ob die Verfügbarkeit und die Ressourcennutzung angemessen sind, was die Überprüfung und Analyse potenzieller Cybersicherheitsprobleme, die die Leistung gefährden, ermöglicht.
- Integration der Cybersicherheit in den SDLC, um Schwachstellen der Cybersicherheit zu erkennen und zu beheben, bevor die Software in Produktion geht.

F. Netzwerkbezogene Kontrollen, die die Außengrenzen der Organisation sichern, einschließlich der Art und Weise, wie die Organisation diese nutzt:
   - Netzwerksegmentierung.
   - Firewalls.
   - Kontrolle der Benutzerzugriffe.
   - Beschränkungen für externe und interne Verbindungen.
   - Kontrollen rund um das Internet der Dinge (IoT) für verbundene Netzwerke.
   - Systeme zur Erkennung und Verhinderung von Eindringlingen (Intrusion Detection/Prevention), um Angriffe auf die Cybersicherheit zu verhindern, zu erkennen und zu beheben.

G. Sicherheitskontrollen für die Endpunkt-Kommunikation, die für Dienste wie E-Mail, Internet-Browser, Videokonferenzen, Messaging (Zoom, MS Teams und andere), soziale Medien, Cloud und Datenaustauschprotokolle gelten. Zu den Kontrollen können die Beschränkung der Verwendung bestimmter Dateierweiterungen (z. B. .exe-Dateien) und die mehrstufige Authentifizierung für die gemeinsame Nutzung von Dateien gehören.

Anhang A. Praktische Anwendungsbeispiele

Die folgenden Beispiele beschreiben Szenarien, in denen das Cybersicherheit Topical Requirement anwendbar wäre.

Beispiel 1: Cybersicherheit ist ein im Revisionsplan enthaltener Revisionsauftrag.

Wenn die Interne Revision ihren risikoorientierten Planungsprozess abschließt und einen oder mehrere Aufträge zur Cybersicherheit in den Revisionsplan aufnimmt, ist das Topical Requirement für die Durchführung dieser Aufträge verbindlich. Die Einhaltung kann dadurch erreicht werden, dass die Anforderungen bei einem oder mehreren Aufträgen im Revisionsplan aufgenommen werden.

Das Thema Cybersicherheit ist breit gefächert und nicht jede Anforderung des Topical Requirement ist bei jedem Auftrag anwendbar. Wenn Interne Revisorinnen und Revisoren nach ihrer professionellen Beurteilung entscheiden, dass eine oder mehrere Anforderungen des Cybersicherheit Topical Requirement nicht anwendbar sind und daher von einem Auftrag ausgeschlossen werden sollen, müssen sie die Gründe für den Ausschluss dieser Anforderungen dokumentieren und aufbewahren. Die Begründung für den Ausschluss einiger Anforderungen könnte beispielsweise darin bestehen, dass die Interne Revision turnusmäßig verschiedene Cybersicherheitsaufträge durchführt oder festgestellt hat, dass die Bedeutung des Risikos für den Auftrag gering ist.

Beispiel 2: Cybersicherheitsrisiken werden während eines Revisionsauftrags identifiziert, der nicht auf Cybersicherheit ausgerichtet ist.

Interne Revisorinnen und Revisoren können Cybersicherheitsrisiken identifizieren, während sie einen Prozess beurteilen, der nicht direkt mit Cybersicherheit zu tun hat. So kann es beispielsweise vorkommen, dass Interne Revisorinnen und Revisoren den Prozess der Kreditorenbuchhaltung im Rahmen eines Auftrags beurteilen, der nicht auf Cybersicherheit ausgerichtet ist, und bei der Planung des Auftrags Cybersicherheitsrisiken nicht als Teil des Prüfungsumfangs identifizieren. Nach der ersten Durchsicht könnten sie jedoch feststellen, dass Cybersicherheitsrisiken Teil des Umfangs sein sollten. Sie identifizieren z. B. Cybersicherheitsrisiken im Zusammenhang mit der webbasierten Übermittlung einer ersten Bestellanforderung (Standard 13.2 „Risikobeurteilung zu einem Auftrag“).

Sobald die relevanten Risiken identifiziert sind, müssen Interne Revisorinnen und Revisoren das Cybersicherheit Topical Requirement überprüfen und bestimmen, welche Anforderungen anwendbar sind. In diesem Beispiel könnten sie den Prozess der Cybersicherheitsgovernance oder den Prozess des Cybersicherheitsrisikomanagements ausschließen. Sie müssen in den Arbeitspapieren die Gründe für den Ausschluss der anderen Anforderungen des Cybersicherheit Topical Requirement dokumentieren und die Dokumentation aufbewahren.

Beispiel 3: Es wird ein Cybersicherheitsauftrag angefordert, der ursprünglich nicht im Revisionsplan enthalten war.

Stakeholder wie das Leitungs- und Überwachungsorgan, das Management oder eine Aufsichtsbehörde könnten Interne Revisorinnen und Revisoren ersuchen, Beurteilungen der Cybersicherheit außerhalb des ursprünglichen Revisionsplans durchzuführen. Wenn Organisationen beispielsweise Ziel eines Cyberangriffs sind, kann das Leitungs- und Überwachungsorgan einen Revisionsauftrag zur Beurteilung der Cybersicherheitskontrollen anfordern. Das Topical Requirement ist anwendbar, die Anforderungen müssen beurteilt und etwaige Ausschlüsse müssen dokumentiert werden.

Anhang B. Zuordnung zu Rahmenwerken

Die Organisation hat möglicherweise ihre eigenen Cybersicherheitskonzepte und verwendet Risikomanagement- und Governance-Rahmenwerke wie COBIT oder NIST. Interne Revisorinnen und Revisoren haben möglicherweise bereits Arbeitsprogramme und Testverfahren auf der Grundlage dieser Rahmenwerke entwickelt. Sie sollten ihre beabsichtigten Kontrolltests zur Cybersicherheit mit dem Topical Requirement abgleichen, um eine adäquate Abdeckung zu gewährleisten. In der nachstehenden Tabelle wird das Cybersicherheit Topical Requirement zu drei häufig verwendeten Rahmenwerken zugeordnet: NIST Cybersecurity Framework 2.0, COBIT 2019 und NIST 800-53. Diese Rahmenwerke wurden ausgewählt, da sie ohne Weiteres und kostenlos verfügbar sind.

Anforderungen an die Governance	Rahmenwerk Referenzen		
	NIST CSF 2.0	NIST 800-53	COBIT 2019
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.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Um das Kontrollumfeld zu stärken, wurden Richtlinien und Verfahren für die Cybersicherheit eingeführt und regelmäßig aktualisiert.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
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.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Die relevanten Stakeholder werden einbezogen, um bestehende Schwachstellen und neu auftretende Bedrohungen im Bereich der Cybersicherheit zu erörtern und darauf zu reagieren. Zu den Stakeholdern gehören die Geschäftsleitung, das operative Geschäft, das Risikomanagement, die Personalabteilung, die Rechtsabteilung, die Complianceabteilung, Lieferanten und andere.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Anforderungen an das Risikomanagement	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
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.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
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.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
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.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

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.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
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.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
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.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07
Anforderungen an den Kontrollprozess	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**

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.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01
B. Es wurde ein Talentmanagementprozess eingeführt, der Schulungen zur Entwicklung und Aufrechterhaltung technischer Kompetenzen im Zusammenhang mit Cybersicherheitsmaßnahmen umfasst. Dieser Prozess wird regelmäßig überprüft.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Es wurde ein Prozess zur kontinuierlichen Überwachung und Meldung neu auftretender Bedrohungen und Schwachstellen der Cybersicherheit sowie zur Identifizierung, Priorisierung und Umsetzung von Möglichkeiten zur Verbesserung der Cybersicherheitsmaßnahmen eingeführt.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Die Cybersicherheit ist Teil des Lebenszyklusmanagements (Auswahl, Nutzung, Wartung und Stilllegung) aller IT-Ressourcen, einschließlich Hardware, Software und Dienste von Lieferanten.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06

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).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
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).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Sicherheitskontrollen für die Endpunktkommunikation wurden für Dienste wie E-Mail, Internetbrowser, Videokonferenzen, Messaging, soziale Medien, Cloud- und Datenaustauschprotokolle eingerichtet.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Anhang C. 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. Das nachstehende druckbare Formular bietet eine Möglichkeit, die Einhaltung des Cybersicherheit Topical Requirement zu dokumentieren, seine Nutzung ist jedoch nicht verbindlich.

Cybersicherheit – Governance

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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 erörtern und darauf zu reagieren. Zu den Stakeholdern gehören die Geschäftsleitung, das operative Geschäft, das Risikomanagement, die Personalabteilung, die Rechtsabteilung, die Complianceabteilung, Lieferanten und andere.		

Cybersicherheit – Risikomanagement

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.		

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.		

Cybersicherheit – Kontrollprozesse

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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.		

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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 Umsetzung 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).		

Anforderung	Abgedeckt oder Grund für Ausschluss	Referenz zur Dokumentation
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 www.theiia.org.

Disclaimer

Copyright

Februar 2025

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