Topical Requirement Cybersicherheit

Was sind Topical Requirements?

Die Topical Requirements sind ein wesentlicher Bestandteil des International Professional Practices Framework®, zu dem auch die Global Internal Audit Standards™ und Global Guidance gehören. Das Institute of Internal Auditors als Standardsetzer für den Berufsstand der Internen Revision versteht die verbindlichen Topical Requirements als Ergänzung zu den Global Internal Audit Standards, die als Grundlage für die in den Topical Requirements beschriebenen und mit Querverweisen versehenen verbindlichen Praktiken dienen.

Die Topical Requirements bieten eine Struktur für häufig geprüfte globale Themen, die typischerweise ein höheres Risiko darstellen und von Natur aus weit verbreitet sind. Während die Standards für alle Revisionsleistungen gelten, sind die Topical Requirements als zusätzliche verbindliche Anforderungen zu betrachten, die zu befolgen sind, wenn das Thema im Fokus eines Auftrags der Internen Revision steht.

Die Topical Requirements sind auf der Ebene der Einheit oder der Organisation auf Themen anzuwenden, die Auswirkungen auf die gesamte Organisation haben. Interne Revisorinnen und Revisoren müssen mit den Topical Requirements vertraut sein und bereit sein, sie anzuwenden, wenn das Thema in ihre jährlichen Revisionspläne aufgenommen wird, oder wenn dieses spezifische Thema im Fokus eines Auftrags der Internen Revision steht. Die Elemente der Topical Requirement müssen beim Scoping eines Auftrags beurteilt werden. Der Nachweis der Beurteilung und Behandlung des Themas ist zu dokumentieren und aufzubewahren. Bei Aufträgen, die irgendeinen Aspekt des Themas umfassen, müssen die für den Auftrag relevanten Anforderungen beurteilt werden, oder es muss dokumentiert werden, warum bestimmte Anforderungen nicht anwendbar sind. Anhang B enthält ein Tool, das Internen Revisorinnen und Revisoren dabei helfen soll, die Gründe für die Einbeziehung oder den Ausschluss von Anforderungen zu erläutern.

Warum sind die Topical Requirements notwendig?

Die Anwendung der Topical Requirements soll die kontinuierliche Relevanz der Internen Revision für die sich entwickelnde globale Risikolandschaft stärken und den Wert der Revisionsleistungen in allen Branchen und Sektoren erhöhen. Die Einhaltung der Topical Requirements hilft den Internen Revisorinnen und Revisoren, die Qualität und Konsistenz der Aufträge zu erhöhen.

Die Topical Requirements sind so strukturiert, dass sie Leitlinien für die Erbringung von Revisionsleistungen in drei Bereichen enthalten: Governance-, Risikomanagement- und Kontrollprozesse. Jeder Bereich umfasst:

- Anforderungen, die verbindlich sind und wesentliche organisatorische Ziele abdecken.
- Überlegungen, die nicht verbindlich sind, sondern als Best Practices für die Bewertung der Gestaltung und Umsetzung der organisatorischen Ziele dienen. Die in Anhang A aufgeführten Überlegungen sollen lediglich als Beispiele für die Validierung der Anforderungen verwendet werden.

Die Einhaltung der Topical Requirements wird bei Qualitätsbeurteilungen bewertet. Um die Einhaltung in Vorbereitung auf eine Qualitätsbeurteilung nachzuweisen, sollten Interne Revisorinnen und Revisoren das Tool in Anhang B

verwenden und die Einhaltung der einzelnen Anforderungen angeben oder erklären, warum die Einhaltung nicht erreicht wurde.

Topical Requirement Cybersicherheit

Bewertung und Beurteilung der Wirksamkeit von Governance-, Risikomanagement- und Kontrollprozessen der Cybersicherheit

Cybersicherheit schützt die Informationsressourcen einer Organisation vor unbefugten Nutzern, Störungen, Veränderungen oder Zerstörung und stärkt das gesamte Kontrollumfeld, um Risiken zu reduzieren. Cyberangriffe können zu direkten und indirekten Auswirkungen führen, die oft beträchtlich sind, da Computer, Netzwerke, Programme, Daten und sensible Informationen wichtige Bestandteile der meisten Organisationen sind. Da Organisationen in hohem Maße auf informationstechnische Ressourcen angewiesen sind, sollten klar definierte Cybersicherheitspläne, Ziele, inhärente Risiken und wirksame Kontrollen eine Priorität für das Management sein.

Dieses Topical Requirement bietet einen konsistenten und umfassenden Ansatz für die Beurteilung der Gestaltung und Umsetzung von Governance-, -Risikomanagement- und Kontrollprozessen der Cybersicherheit.

GOVERNANCE: Bewertung und Beurteilung der Governance von Cybersicherheit

Anforderungen:

Bei der Durchführung einer Prüfung der Internen Revision, die auch Ziele der Cybersicherheit umfasst, müssen die Internen Revisorinnen und Revisoren beurteilen, ob die Governance-Prozesse der Organisation Cybersicherheit angemessen berücksichtigen. Interne Revisorinnen und Revisoren müssen Folgendes beurteilen:

A. Es werden Richtlinien und Verfahren für das Management von Cybersicherheitsrisiken eingeführt und regelmäßig aktualisiert, einschließlich der Förderung von Praktiken zur Stärkung des Kontrollumfelds auf der Grundlage allgemein anerkannter Rahmenwerke (NIST, COBIT und andere).

B. Aufgaben und Zuständigkeiten, die die Ziele der Organisation im Bereich der Cybersicherheit unterstützen, sind klar festgelegt und diese Rollen sind mit Personen besetzt, die über die erforderlichen Kenntnisse, Fähigkeiten und Fertigkeiten verfügen.

C. Das Leitungs- und Überwachungsorgan wird regelmäßig über Aktualisierungen der Ziele, Strategien, Risiken und Kontrollmaßnahmen im Bereich der Cybersicherheit informiert.

D. Relevante Stakeholder (z. B. Führungskräfte, Operations, strategische Lieferanten und andere) werden einbezogen, um zu erörtern, wie die Prozesse des Cybersicherheits-Risikomanagements am besten etabliert und verbessert werden können.

E. Angemessene Ressourcen (wie z. B. Führungskräfte, Finanzierung, Talente, Hardware, Software und Schulung), die für die wirksame Durchführung von Verfahren zum Management von Cybersicherheitsrisiken erforderlich sind, werden dem Leitungs- und Überwachungsorgan mitgeteilt.

RISIKOMANAGEMENT: Bewertung und Beurteilung des Risikomanagements von Cybersicherheit

Anforderungen:

Bei der Durchführung einer Prüfung der Internen Revision, die auch Ziele der Cybersicherheit umfasst, müssen die Internen Revisorinnen und Revisoren beurteilen, ob die Risikomanagementprozesse der Organisation Cybersicherheit angemessen berücksichtigen. Interne Revisorinnen und Revisoren müssen Folgendes beurteilen:

A. Ein organisationsweiter Risikomanagementprozess ist eingerichtet, der die Identifizierung, Analyse und das Management von Risiken im Zusammenhang mit IT und Informationssicherheit umfasst, mit besonderem Augenmerk auf Cybersicherheitsrisiken und darauf, wie sich diese Risiken auf die Fähigkeit auswirken können, die Organisationsziele zu erreichen.

B. Die Prozesse des Cybersicherheits-Risikomanagements werden von einem funktionsübergreifenden Team durchgeführt, zu dem die Leitung der IT, das organisationsweite Risikomanagement, die Rechtsabteilung, die Compliance-Abteilung, das sonstige Management (Operations, Buchhaltung/Finanzen und andere) gehören, und beziehen gegebenenfalls auch externe Parteien (Anbieter, ausgelagerte Dienstleister, Lieferanten, Kunden und andere) mit ein.

C. Es wurden Richtlinien und Verfahren für das Cybersicherheits-Risikomanagement eingeführt, die regelmäßig aktualisiert werden, einschließlich der Förderung von Praktiken, die die Prozesse des Cybersicherheits-Risikomanagements auf der Grundlage weithin angenommener Risikomanagement-Rahmenwerke, maßgeblicher Leitlinien oder anderer Best Practices stärken.

D. Die Verantwortlichkeit und Zuständigkeit für das Management von Cybersicherheitsrisiken ist festgelegt und es wurde eine Person oder ein Team bestimmt, das regelmäßig überwacht und mitteilt, wie Cybersicherheitsrisiken gemanagt werden, einschließlich des Ressourcenbedarfs zur Risikominderung und der Identifizierung neuer Cybersicherheitsrisiken, die zuvor nicht erkannt wurden.

E. Es gibt ein Verfahren zur raschen Eskalation von (neu auftretenden oder bereits identifizierten) Cybersicherheitsrisiken, die auf der Grundlage der festgelegten Risikomanagement-Richtlinien der Organisation ein inakzeptables Niveau erreichen, oder zur Einhaltung geltender rechtlicher und/oder behördlicher Anforderungen.

F. Das Cybersicherheits-Risikomanagement umfasst die Koordination zwischen der Informationssicherheit, der Rechtsabteilung, der Compliance-Abteilung und anderer Managementbereiche, um alle rechtlichen und vertraglichen Verpflichtungen (wie z. B. Gesetze und Vorschriften) zu ermitteln und einzuhalten. Der Status der Einhaltung und Nichteinhaltung geltender Anforderungen wird in der Organisation regelmäßig kommuniziert.

G. Es gibt ein Verfahren zur Ermittlung und zum Management von Risiken im Zusammenhang mit der Cybersicherheit von Drittparteien. Anbieter, Lieferanten und andere Provider von ausgelagerten Prozessen und/oder Dienstleistungen sind vertraglich verpflichtet, wirksame Cybersicherheitskontrollen einzuführen, die die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme der Organisation und der Daten, auf die Drittparteien Zugriff haben, angemessen schützen.

H. Richtlinien und Prozesse in Bezug auf die Klassifizierung, Aufbewahrung, Vernichtung und Verschlüsselung von Daten sind angemessen konzipiert und werden wirksam eingesetzt. Dies bietet einen zielgerichteten Ansatz, der eine vollständige und genaue Aufzeichnung von Daten und die Vertraulichkeit und den Datenschutz sensibler Informationen gewährleistet.

I. Es gibt ein Verfahren für die Kommunikation von operationellen Risiken im Bereich der Cybersicherheit, um das Bewusstsein dafür bei Management und Mitarbeiterinnen und Mitarbeitern sicherzustellen. Alle Probleme, Lücken, Unzulänglichkeiten oder Kontrollmängel werden dem Leitungs- und Überwachungsorgan und dem Management mitgeteilt, und der Status der Abhilfemaßnahmen wird genau überwacht und gemeldet. Die Nichteinhaltung von Cybersicherheitsrichtlinien wird erkannt, untersucht, berichtet und zeitnah behoben.

KONTROLLEN: Bewertung und Beurteilung der Kontrollprozesse von Cybersicherheit

Anforderungen:

Bei der Durchführung einer Prüfung der Internen Revision, die auch Ziele der Cybersicherheit umfasst, müssen die Internen Revisorinnen und Revisoren beurteilen, ob die Kontrollprozesse der Organisation die Cybersicherheit angemessen berücksichtigen. Interne Revisorinnen und Revisoren müssen beurteilen, ob die Organisation:

A. Interne Kontrollen der Cybersicherheit priorisiert und sicherstellt, dass damit verbundene Budgets und Ressourcen (wie z. B. Personal, Software, Tools und andere) zugewiesen werden, um den erwarteten Nutzen zu maximieren.

B. Sicherstellt, dass die Kontrollen der Cybersicherheit so funktionieren, dass die Ziele der Organisation im Bereich der Cybersicherheit erreicht und Probleme rechtzeitig gelöst werden.

C. Ausreichende Schulungen des für Cybersicherheitsmaßnahmen zuständigen Personals anbietet.

D. Ausreichende Richtlinien und Verfahren entwickelt hat, um alle operativen Aspekte der Cybersicherheit und der damit verbundenen Kontrollen zu managen.

E. Sicherstellt, dass das Management über die notwendigen Ressourcen verfügt, um sich über aufkommende Cybersicherheitsprobleme durch neue Technologien auf dem Laufenden zu halten, Möglichkeiten zur Verbesserung der Abläufe zu erkennen und zu verstehen, wie Cybersicherheitsbemühungen am besten eingesetzt werden können, um die umfassenderen Organisationsziele zu beeinflussen.

F. Cybersicherheit angemessen in den Lebenszyklus der Systementwicklung für Geschäftsanwendungen, einschließlich Software und erworbener oder individuell entwickelter Anwendungen, integriert.

G. Cybersicherheit in das Management von Hardware (wie z. B. Laptops, Desktops, mobile Geräte) einbezogen hat.

H. Wirksame Kontrollen in Bezug auf die Unterstützung der Produktionshardware implementiert hat, wie z. B. Konfiguration, Patching, Unterstützung der Benutzerzugriffsverwaltung und Überwachung der Verfügbarkeit und Leistung. Die Organisation hat sowohl die Angemessenheit der Konzeption als auch die operative Wirksamkeit dieser Kontrollen bewertet.

I. Die netzbezogenen Kontrollen in Bezug auf die Netzsegmentierung, die Verwendung und Platzierung von Firewalls, begrenzte Verbindungen zu externen Netzen und/oder Systemen sowie den Einsatz von Präventiv- und Detektivtechnologien wie Systemen zur Erkennung und Verhinderung von Eindringlingen optimiert hat.

J. Wirksame Kontrollen für gängige Desktop-Kommunikationsdienste wie E-Mail, Internetbrowser, Videokonferenzen, Messaging und Protokolle zur gemeinsamen Dateinutzung eingeführt hat.

K. Geeignete Kontrollen für die Servicebereitstellung implementiert hat, um sicherzustellen, dass die folgenden Bereiche in die Überwachung der Cybersicherheit integriert sind: Change-Management, Service/Helpdesk und Verwaltung der Endbenutzergeräte.

L. Angemessene physische Sicherheitskontrollen implementiert hat, um Informationszentren mit hohem Risiko, wie z. B. Datenzentren, Netzwerkbetriebszentren und Sicherheitsbetriebszentren, vor Angriffen zu schützen.

M. Kontrollen für die Reaktion auf Vorfälle und die Wiederherstellung implementiert hat.

Zugehörige Standards:

3.1 Kompetenz
4.2 Berufliche Sorgfalt
9.1 Verstehen von Governance-, Risikomanagement- und Kontrollprozessen
9.4 Revisionsplan
12.3 Überwachung und Verbesserung der Leistung bei der Durchführung von Aufträgen
13.1 Auftragskommunikation
13.2 Risikobeurteilung zu einem Auftrag
13.3 Auftragsziele und Auftragsumfang
13.4 Bewertungskriterien
13.5 Auftragsressourcen
13.6 Arbeitsprogramm
14.1 Sammeln von Informationen für Analysen und Bewertungen
14.2 Analysen und potenzielle Feststellungen
14.3 Bewertung von Feststellungen
14.4 Empfehlungen und Maßnahmenpläne
14.5 Gesamturteil zu einem Auftrag
14.6 Auftragsdokumentation
15.1 Abschlusskommunikation
15.2 Bestätigung der Umsetzung von Empfehlungen oder Maßnahmenplänen

Zugehörige Global Technology Audit Guides (GTAGs):

Assessing Cybersecurity Risk: The Three Lines Model
Auditing Business Applications
Auditing Cyber Incident Response and Recovery
Auditing Cybersecurity Operations Prevention and Detection
Auditing Identity and Access Management
Auditing IT Governance
Auditing Mobile Computing
Auditing Network and Communications Management

Anhang A. Überlegungen

Überlegungen zu den einzelnen Anforderungen an die Governance:

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

A. Richtlinien, Verfahren und andere relevante Unterlagen, die von der Organisation für das Managen der täglichen Cybersicherheitsaufgaben verwendet werden, einschließlich:
   1. Eine klare, prägnante und konsistente Dokumentation, die regelmäßig aktualisiert wird, idealerweise wenn neue Cybersicherheitsrisiken erkannt werden und mindestens jährlich.
   2. Verfahren zur Identifizierung, Analyse, Behebung und Berichterstattung von Verstößen oder sonstigen Verlusten sensibler Daten.
   3. Dokumentation der Art und Weise, wie das Management sicherstellt, dass die Richtlinien und Verfahren zur Unterstützung der operativen Cybersicherheit ausreichend sind.

B. Aufgaben und Zuständigkeiten, die vom Leitungs- und Überwachungsorgan geschaffen wurden, um die Umsetzung der Cybersicherheitsstrategie zu unterstützen, einschließlich einer Berichtsstruktur, die sicherstellt, dass die Cybersicherheit auf einer Ebene innerhalb der Organisation berichtet wird, die eine ausreichende Sichtbarkeit hat, um die Unterstützung der Organisation zu erreichen.

C. Materialien zu Cybersicherheitsstrategie, -zielen, -risiken und -kontrollen, die dem Leitungs- und Überwachungsorgan vorgelegt werden, einschließlich folgender Analysen:
   1. Die Häufigkeit der Mitteilungen ist angemessen, erfolgt idealerweise vierteljährlich und wird von der Leitung der Informationssicherheitsfunktion, z. B. einem Chief Information Systems Officer (CISO), vorgelegt.
   2. Die dargestellten Informationen sind klar, prägnant und konsistent. Risiken und Kontrollen werden in einer Weise vermittelt, die für das Leitungs- und Überwachungsorgan leicht verständlich ist.
   3. Wichtige Key Performance Indicators oder andere wichtige Metriken/Statistiken zur Cybersicherheit sind enthalten.
   4. Gegebenenfalls werden die Anregungen des Leitungs- und Überwachungsorgans vom Management entgegengenommen und umgesetzt, wobei das Leitungs- und Überwachungsorgan über den aktuellen Stand der Änderungen informiert wird.

D. Belege für die Kommunikation des Managements mit den relevanten Stakeholdern (z. B. Führungskräfte, Operations, strategische Lieferanten und andere) über Cybersicherheit, einschließlich der Tatsache, dass die übermittelten Informationen klar, prägnant, konsistent und auf die Zielgruppe der Stakeholder zugeschnitten sind:
   1. Mitarbeiter.
   2. Anbieter/Lieferanten/ausgelagerte Dienstleister und Drittparteien.
   3. Kunden.
   4. Strategische Partner.

E. Analyse und Mitteilung des Ressourcenbedarfs durch das Management, einschließlich:
   1. Verstehen, wie Lücken identifiziert werden und welche wichtigen Metriken verwendet werden, um Änderungen der Anforderungen zu antizipieren.
   2. Wie das Management mit der Personalabteilung zusammenarbeitet, um den Bedarf an Talenten im Bereich Cybersicherheit zu analysieren.
   3. Wie das Management die aktuellen Hardware- und Softwarebestände analysiert und feststellt, ob zusätzliche Investitionen zur Unterstützung von Cybersicherheitsinitiativen erforderlich sind.

4. Ob die Internen Revisorinnen und Revisoren überprüfen, wie das Management Schulungsmaterialien zur Cybersicherheit erstellt und aktualisiert und Lücken identifiziert, einschließlich der Sicherstellung, dass Schulungen neue Ziele, Risiken und Kontrollen der Cybersicherheit abdecken.

Überlegungen zu den einzelnen Anforderungen an das Risikomanagement:

Um die erforderlichen Aspekte des Cybersicherheits-Risikomanagements zu beurteilen, können Interne Revisorinnen und Revisoren überprüfen:

A. Wie das Management anfänglich Cybersicherheitsrisiken identifiziert, einschließlich:
   1. Verstehen, welches Personal sowohl für die täglichen Bedrohungen, denen das Unternehmen ausgesetzt ist, als auch für neu auftretende Risiken in der Community der Informationssicherheit zuständig ist.
      a. Stellen Sie fest, ob diese Personen über die nötige Berufserfahrung und Ausbildung verfügen, um Bedrohungen wirksam zu erkennen und sie an das breiter aufgestellte Risikomanagement-Team zu eskalieren.
   2. Identifikation der Softwareanwendungen oder Anbieter, auf die sich das Management verlässt, um Cybersicherheitsrisiken zu erkennen.
   3. Dokumentation des Cybersicherheits-Risikomanagementprozesses, einschließlich:
      a. Sitzungsprotokolle.
      b. Maßnahmen.
      c. Listen der Teilnehmer oder Teammitglieder.
      d. Untersuchung nach einem Vorfall/Analyse der Grundursache.

B. Wie das Management die Mitglieder des Risikomanagementteams bestimmt oder ernennt und die damit verbundenen geschäftlichen Gründe oder Qualifikationen, die zur Beurteilung dessen herangezogen werden. Überprüfung der Nachweise für regelmäßiges Engagement in Diskussionen über Cybersicherheitsrisiken mit relevanten externen Parteien.

C. Der von der Organisation angewendete Prozess, um Richtlinien und Verfahren im Zusammenhang mit dem Management von Cybersicherheitsrisiken festzulegen und regelmäßig zu aktualisieren, was Folgendes beinhalten kann:
   1. Jährliche Überprüfung und Genehmigung von Richtlinien und Verfahren.
   2. Ein Verständnis dafür, wie die Organisation die Einhaltung ihrer Risikomanagementrichtlinien und -verfahren sicherstellt und wie das Personal in der Umsetzung der Richtlinien und Verfahren geschult wird.
      a. Ein Verständnis dafür, welche Rahmenwerke oder maßgeblichen Leitlinien das Management für die Behandlung von Cybersicherheitsrisiken nutzt (z. B. NIST, COBIT und andere) und wie die Organisation die Einhaltung der gewählten Rahmenwerke bestätigt.

D. Die Person(en), die für die Ausübung des Cybersicherheits-Risikomanagements verantwortlich ist/sind, einschließlich der Sicherstellung, dass ihr beruflicher Hintergrund, ihre Erfahrung, ihre Qualifikationen und ihre Befähigungsnachweise für das Management von Informationssicherheitsrisiken und -bedrohungen geeignet sind. Überprüfen Sie, ob die verantwortliche Person auf einer Ebene innerhalb der Organisation positioniert ist, die die Sichtbarkeit von Cybersicherheitsrisiken und die wirksame Kommunikation dieser Risiken ermöglicht.

E. Die Eskalationsprozesse, die die Organisation für die Kommunikation von Cybersicherheitsrisiken einsetzt, einschließlich der Art und Weise, wie die Bedrohungs- oder Risikostufe bewertet, zugewiesen und priorisiert wird. Überprüfen Sie, ob die Organisation Risikostufen definiert hat, z. B. hoch, moderat, niedrig, einschließlich einer detaillierten Erklärung für jede Risikostufe und der Eskalationsverfahren für jede Risikokategorie. Überprüfen Sie die Auflistung der aktuell identifizierten Cybersicherheitsrisiken und des Abhilfestatus der einzelnen Ereignisse.

F. Das Verfahren, das die Organisation einsetzt, um die Einhaltung aller geltenden Cybersicherheitsvorschriften zu gewährleisten, einschließlich:

1. Wie sich vorgeschlagene oder kürzlich verabschiedete Vorschriften auf die Organisation auswirken.
2. Das Vorhandensein einer Bestandsaufnahme der geltenden Vorschriften, die regelmäßig überwacht und aktualisiert und über die regelmäßig Bericht erstattet wird, um das Bewusstsein der Organisation dafür sicherzustellen.
    a. Überprüfen Sie bei allen Verstößen, ob sich das Management der damit verbundenen Risiken bewusst ist, einschließlich der regelmäßigen Berichterstattung.

G. Der Prozess der Organisation zur Durchführung des Cybersicherheits-Risikomanagements für Drittparteien. Stellen Sie sicher, dass die Cybersicherheitskontrollen von Anbietern vor Beginn einer Geschäftsbeziehung überprüft werden, und dass das Recht zur regelmäßigen Überprüfung während der Geschäftsbeziehung in die Verträge aufgenommen wird. Beziehen Sie die Anforderung und Analyse des SOC-Reports (Service Organization Controls) des Drittanbieters ein und verifizieren Sie, dass die Organisation ihre Überprüfung des SOC-Reports dokumentiert hat. Diese sollte beinhalten, dass Überlegungen zur Nutzerkontrolle umgesetzt wurden. Verschaffen Sie sich ein Verständnis vom Ansatz des Managements zur Feststellung, ob Drittparteien über ein angemessenes Kontrollumfeld verfügen, das den Kontrollen der Organisation entspricht.
    1. Wenn Schwachstellen in den Kontrollen von Drittanbietern gefunden werden, sollten Sie die Prozesse verstehen, die das Management anwendet, um sich zu vergewissern, dass die Schwachstellen die Cybersicherheit in Bezug auf Operations nicht gefährden, oder verstehen, wie das Unternehmen kommuniziert, dass Änderungen erforderlich sind, um die Beziehung zu dem betreffenden Anbieter aufrechtzuerhalten, oder dass möglicherweise ein Ersatzanbieter gefunden werden muss.

H. Die Richtlinien und Verfahren der Organisation in Bezug auf:
    1. Klassifizierung der Daten.
    2. Datenhaltung.
    3. Löschung von Daten.
    4. Verschlüsselung.
    5. Zugangs-/Identitätsmanagement.
    6. Wer die Dokumentation erstellt, überprüft und aktualisiert, wobei idealerweise Personal der Rechtsabteilung und der Compliance-Abteilung beteiligt sein sollte, um die Einhaltung der geltenden Vorschriften zu gewährleisten.
    7. Wie die Organisation die Datenklassifizierung durchführt, um sicherzustellen, dass vertrauliche und private Daten identifiziert und angemessen geschützt werden, z. B. durch die Beschränkung des Benutzerzugriffs.
    8. Wie die Organisation das Verfahren zur Klassifizierung von Daten regelmäßig überprüft, und ob der Prozess weiterhin die Ziele der Organisation in Bezug auf die Cybersicherheit unterstützt und mit den Unternehmensrichtlinien und den geltenden Vorschriften übereinstimmt.

I. Das Verfahren zur Kommunikation der operationellen Risiken der Cybersicherheit an das Management und an das Personal. Idealerweise sollte eine solche Kommunikation mit regelmäßigen Cybersicherheitsschulungen verbunden sein (mindestens jährlich). Verstehen Sie den Prozess des Managements zur Kommunikation von Aktualisierungen bestehender Abhilfemaßnahmen von Cybersicherheitsproblemen sowie die voraussichtlichen Fertigstellungstermine. Vergewissern Sie sich, dass die Nichteinhaltung von Vorschriften genau überwacht wird und der Geschäftsleitung und dem Überwachungsorgan aktuelle Informationen zur Verfügung gestellt werden.

Überlegungen zu den einzelnen Anforderungen an den Kontrollprozess:

Um die erforderlichen Aspekte der Kontrollen der Cybersicherheit zu beurteilen, können Interne Revisorinnen und Revisoren überprüfen:

A. Der Prozess des Managements zur Festlegung des Einsatzes budgetierter Ressourcen zur Unterstützung des Kontrollumfelds für die Cybersicherheit sollte eine jährliche strategische Planung beinhalten, um sicherzustellen, dass ein angemessenes Maß an organisatorischen Ressourcen zur Erfüllung der Cybersicherheitsziele verfügbar ist. Die formalen, dokumentierten Ergebnisse der jährlichen Planung und der regelmäßigen Überwachung des Ressourcenmanagements sollten überprüft werden.

B. Der Prozess des Managements zur regelmäßigen Bewertung, dass die Kontrollen der Cybersicherheit so funktionieren, dass die Ziele der Organisation für die Cybersicherheit erreicht werden. Überprüfen Sie, ob das Management die Wirksamkeit der Kontrollen überwacht und bewertet, ob die bestehenden Kontrollen angemessen gestaltet sind, oder ob neue Kontrollen erforderlich sind. In vielen Organisationen spielt die Interne Revision eine wichtige Rolle in diesem Prozess durch die Lieferung von Prüfungssicherheit mittels regelmäßiger (vierteljährlicher, jährlicher) Tests über die Konzeption und Wirksamkeit der Kontrollen. Überprüfen Sie die Prozesse des Managements zur Behebung von Kontrollschwächen oder der Handhabung von Feststellungen aus Beurteilungen der Internen Revision oder anderer Assurance Provider (z. B. Penetrationstests).

C. Der Prozess des Managements zur Bewertung von Schulungsbedarf für das Cybersicherheitspersonal innerhalb der Organisation und der Zuweisung von Ressourcen, um eine angemessene Schulung durchzuführen und sicherzustellen, dass aufkommende Cybersicherheitsbedrohungen verstanden und bewältigt werden. Verstehen Sie, wie das Management sicherstellt, dass das Personal in ausreichendem Maße an Cybersicherheitsschulungen teilnimmt, was Live-Schulungen, aufgezeichnete Schulungen oder den Abschluss von Schulungsmodulen umfassen kann.

D. Das Verfahren der Organisation zur Erstellung und Aktualisierung von Cybersicherheitsrichtlinien und -verfahren sowie die Art und Weise, wie das Management die Angemessenheit dieser Richtlinien und Verfahren bewertet. Verstehen Sie, wie das für Cybersicherheitsvorgänge und -kontrollen verantwortliche Personal für die Einhaltung der Richtlinien und Verfahren geschult und wie es im Hinblick auf die Einhaltung bewertet wird.

E. Das Verfahren der Organisation zur angemessenen Schulung des Managementteams, das für Cybersicherheits-Operations und Kontrollen verantwortlich ist, damit es aufkommende Trends erkennt und strategische Führung seiner Teams und der Organisation bietet. Verstehen Sie, wie die Organisation Möglichkeiten ermittelt, die Fähigkeiten des Managements zu verbessern, das Bewusstsein für neu auftretende Probleme zu fördern, z. B. durch Teilnahme an Schulungen und laufende berufliche Weiterbildung.

F. Wie die Organisation die Cybersicherheit innerhalb ihres Systementwicklungs-Lebenszyklus behandelt, einschließlich der folgenden Kontrollaspekte:
   1. Planung: Die Cybersicherheit wurde als Schlüsselkomponente bei der Bewertung von Risiken und der Analyse potenzieller Schwachstellen ermittelt. Der Umfang und die Ziele der Softwareimplementierung sollten bei der Bewertung der Cybersicherheitskontrollen in der Planungsphase berücksichtigt werden.
   2. Erfassen von Anforderungen: Die Anforderungen an die Cybersicherheit sind eine Komponente bei der Festlegung der funktionalen Anforderungen, die auch die Einhaltung aller geltenden gesetzlichen und regulatorischen Anforderungen umfassen sollten.
   3. Design: Überlegungen zur Cybersicherheit werden als integraler Bestandteil der detaillierten Verarbeitungsanforderungen einbezogen. Kontrollen sollten in allen Aspekten des Designs identifiziert werden, wenn die Organisation formell die Bedürfnisse der Konzeption der Systemarchitektur definiert (z. B. Plattformen, Benutzerschnittstellen, Datenbanken und andere).
   4. Entwicklung: Die Organisation hat eine sichere Umgebung eingerichtet und einen Entwicklungsprozess formell definiert, der Cyberschwachstellen minimiert (z. B. eingeschränkter Benutzerzugriff auf den Entwicklercode, angemessene Trennung von der Produktionsumgebung, Verwendung zugelassener Tools, Existenz von Audit Trails zur Nachverfolgung der Entwicklungsaktivitäten, spezifische Cybersicherheitsanforderungen für vom Anbieter entwickelte Software und andere).
   5. Testen: Die Organisation bezieht die Überprüfung und Beurteilung der Cybersicherheit in die Testphase ein (z. B. automatisierte Tests, Penetrationstests und Schwachstellenbeurteilung). Die Organisation sollte in der Lage sein, bei allen in den Tests festgestellten Cyberschwachstellen schnell alarmiert zu werden und diese zu beheben, einschließlich einer detaillierten Beschreibung der Schwachstelle und der als Reaktion darauf vorgenommenen Code-Änderungen oder mitigierenden Kontrollen.
   6. Bereitstellung: Wenn eine neue Software in Betrieb genommen wird, sollte die Organisation alle potenziellen Cybersicherheitsbedrohungen sorgfältig überwachen und sicherstellen, dass die Endbenutzer so geschult wurden, dass sie die Software auf eine Weise verwenden, die die Cybersicherheitsrisiken

minimiert. Die Organisation sollte sicherstellen, dass Ereignisse und Fehler protokolliert und in Bezug auf potenzielle Cybersicherheitsereignisse analysiert werden.

7. Wartung: Die Organisation sollte sicherstellen, dass alle sicherheitsrelevanten Softwareversionen rechtzeitig eingesetzt werden, und sollte eine offene Kommunikation mit Softwareanbietern betreiben, um sicherzustellen, dass neu auftretende Risiken und Bedrohungen angemessen kontrolliert und Endbenutzer über bekannte Schwachstellen informiert werden.

G. Kontrollen, die die Organisation eingerichtet hat, um Hardware (wie z. B. Desktops, Laptops, mobile Geräte und andere) vor Cybersicherheitsrisiken zu schützen. Dazu gehören die Verwendung von Verschlüsselung, Antivirensoftware, komplexe Passwortanforderungen, virtuelle private Netzwerke oder Zero-Trust-Networking für die Authentifizierung, regelmäßige Aktualisierung der Firmware und ein Asset-Management-Prozess, der sicherstellt, dass die vom Unternehmen ausgegebene Hardware eine angemessene Sicherheitskonfiguration aufweist und bei der Ausmusterung ordnungsgemäß entsorgt wird.

H. Kontrollen, die die Organisation eingerichtet hat, um sicherzustellen, dass die Produktionsunterstützung Schutz vor Cybersicherheitsrisiken bietet, wozu auch gehört, dass die Server rechtzeitig mit Sicherheitsversionen gepatcht werden, um aufkommende Risiken zu mindern. Überprüfen Sie die vorhandenen Überwachungskontrollen, um festzustellen, ob Verfügbarkeit und Ressourcennutzung angemessen sind und erlauben, potenzielle Cybersicherheitsprobleme, die die Leistung gefährden, zu überprüfen zu analysieren. Überprüfen Sie die datenbankbezogenen Kontrollen, die u. a. die Beschränkung des Benutzer- und Administratorzugriffs und die Gewährleistung der Verwendung von Verschlüsselung, von Backups und Tests der Datenbanken sowie das Vorhandensein starker Netzwerksicherheitskontrollen umfassen.

I. Netzwerkbezogene Kontrollen, die eine Segmentierung vorsehen, um Cybersicherheitsrisiken durch unbefugten Zugriff zu begrenzen. Überprüfen Sie, wie die Organisation Firewalls einsetzt, einschließlich der Standorte der Firewalls und des Verfahrens zur Überprüfung, Analyse und Einschränkung des Netzwerkzugriffs, um unbefugten Zugriff zu verhindern. Überprüfen Sie, wie die Organisation Systeme zur Erkennung und Verhinderung von Eindringlingen einsetzt, um Cybersicherheitsangriffe zu verhindern, zu erkennen und zu beheben.

J. Kontrollen, die die Organisation in Bezug auf gängige Desktop-Kommunikationsdienste eingerichtet hat, wie z. B. die Verwendung von E-Mail-Verschlüsselung, die Sicherstellung, dass Internet-Browser-Sicherheitsupdates rechtzeitig eingespielt werden, die Konfiguration von Sicherheitseinstellungen für Videokonferenzen/Messaging (z. B. MS Teams, Zoom und andere), die Einschränkung der Verwendung bestimmter Dateierweiterungen (wie z. B. .exe-Dateien) und die Verwendung einer Multi-Faktor-Authentifizierung für die gemeinsame Nutzung von Dateien.

K. Kontrollen, die die Organisation eingerichtet hat, um Cybersicherheitsrisiken im Zusammenhang mit der Erbringung von Dienstleistungen zu mindern, einschließlich:

1. Sicherstellung, dass der Change-Management-Prozess Cybersicherheitsrisiken berücksichtigt, wenn Änderungen bewertet und genehmigt werden, und eine rechtzeitige Reaktion auf cyberbezogene Vorfälle gewährleistet.
2. Der Benutzer-Helpdesk protokolliert alle von der Organisation gemeldeten Cybersicherheitsereignisse, sorgt für eine zeitnahe Lösung und eskaliert an das zuständige Mitglied des Managements.
3. Die Verwaltung mobiler Geräte (z. B. E-Mail, Apps an andere) ist so konfiguriert, dass Cybersicherheitsrisiken gemindert werden, und kann aus der Ferne verwaltet werden, wenn das Gerät eines Benutzers gefährdet ist.

L. Physische Sicherheitskontrollen zum Schutz von Informationen mit hohem Risiko, einschließlich des Schutzes vor Cybersicherheitsrisiken. Beispiele sind die Sicherstellung, dass der Zugriff durch Drittparteien/Lieferanten angemessen ist, und die Beschränkung des physischen Benutzerzugangs zu Rechenzentren, Netzwerkbetriebszentren und Sicherheitsbetriebszentren auf autorisiertes Personal.

M. Kontrollen, die die Organisation in Bezug auf die Reaktion auf einen Vorfall und die Wiederherstellung implementiert hat, die Folgendes umfassen sollten:

1. Ein dokumentierter Plan, der überprüft und aktualisiert wird, wenn sich die Abläufe in der Organisation im Laufe der Zeit ändern.
2. Regelmäßige Tests und Berichterstattung der Ergebnisse an das Management.
3. Feststellung, ob alle in den Tests identifizierten Probleme rechtzeitig behoben werden.

Anhang B. Tool zur Dokumentation der Einhaltung der Topical Requirements

Cybersicherheit – Governance

Anforderung	Einhaltung (Ja/Nein/Teilweise)	Erlangte Nachweise oder Gründe für den Ausschluss
A. Es werden Richtlinien und Verfahren für das Management von Cybersicherheits-Risiken eingeführt und regelmäßig aktualisiert, einschließlich der Förderung von Praktiken auf der Grundlage allgemein anerkannter Rahmenwerke (NIST, COBIT und andere), die das Kontrollumfeld stärken.		
B. Aufgaben und Zuständigkeiten, die die Ziele der Organisation im Bereich der Cybersicherheit unterstützen, sind klar festgelegt und diese Aufgaben sind angemessen besetzt.		
C. Das Leitungs- und Überwachungsorgan wird regelmäßig über Aktualisierungen der Ziele, Strategien, Risiken und Kontrollmaßnahmen im Bereich der Cybersicherheit informiert.		
D. Relevante Stakeholder werden einbezogen, um zu erörtern, wie die Prozesse des Cybersicherheits-Risikomanagements am besten etabliert und verbessert werden können.		
E. Angemessene Ressourcen (Führung, Finanzierung, Talente, Hardware, Software, Schulung und andere), die für die wirksame Durchführung von Verfahren zum Management von Cybersicherheitsrisiken erforderlich sind, werden dem Leitungs- und Überwachungsorgan mitgeteilt.		

Cybersicherheit – Risikomanagement

Anforderung	Einhaltung (Ja/Nein/Teilweise)	Erlangte Nachweise oder Gründe für den Ausschluss
A. Einführung eines organisationsweiten Risikomanagementprozesses, der die Identifizierung, Analyse und das Management von Risiken im		

Anforderung	Einhaltung (Ja/Nein/Teilweise)	Erlangte Nachweise oder Gründe für den Ausschluss
Zusammenhang mit IT und Informationssicherheit umfasst, mit besonderem Augenmerk auf Cybersicherheitsrisiken und darauf, wie sich diese Risiken auf die Fähigkeit der Organisation auswirken können, ihre Ziele zu erreichen.		
B. Die Prozesse des Cybersicherheits-Risikomanagements werden von einem funktionsübergreifenden Team durchgeführt, zu dem die Leitung der IT, das organisationsweite Risikomanagement, die Rechtsabteilung, die Compliance-Abteilung, das sonstige Management (z. B. Operations, Buchhaltung/Finanzen) und gegebenenfalls auch externe Parteien (Anbieter, Lieferanten, Kunden) gehören.		
C. Es wurden Richtlinien und Verfahren für das Cybersicherheits-Risikomanagement eingeführt, die regelmäßig aktualisiert werden, einschließlich der Förderung von Praktiken, die die Prozesse des Cybersicherheits-Risikomanagements auf der Grundlage weithin angenommener Risikomanagement-Rahmenwerke, maßgeblicher Leitlinien oder Best Practices stärken.		
D. Die Verantwortlichkeit und Zuständigkeit für das Management von Cybersicherheitsrisiken ist festgelegt, und es wurde eine Person oder ein Team bestimmt, das regelmäßig überwacht und mitteilt, wie die Cybersicherheitsrisiken gemanagt werden, einschließlich des Ressourcenbedarfs zur Risikominderung und der Identifizierung neuer Cybersicherheitsrisiken, die zuvor nicht erkannt wurden.		
E. Es gibt einen Prozess zur raschen Eskalation von (neu auftretenden oder bereits identifizierten) Cybersicherheitsrisiken, die auf der Grundlage der festgelegten Risikomanagement-Richtlinien der Organisation ein inakzeptables Niveau erreichen, oder zur Einhaltung geltender rechtlicher und/oder behördlicher Anforderungen.		

Anforderung	Einhaltung (Ja/Nein/Teilweise)	Erlangte Nachweise oder Gründe für den Ausschluss
F. Das Cybersicherheits-Risikomanagement umfasst die Koordination zwischen der Informationssicherheit, der Rechtsabteilung, der Compliance-Abteilung und anderer Managementbereiche, um alle rechtlichen und vertraglichen Verpflichtungen (Gesetze, Vorschriften) zu ermitteln und einzuhalten. Der Status der Einhaltung und Nichteinhaltung geltender Anforderungen wird der Organisation regelmäßig mitgeteilt.		
G. Es gibt einen Prozess zur Ermittlung und zum Management von Cybersicherheitsrisiken im Zusammenhang mit Drittparteien. Anbieter, Lieferanten und andere Provider von ausgelagerten Prozessen und/oder Dienstleistungen sind vertraglich verpflichtet, wirksame Cybersicherheitskontrollen einzuführen, die die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme der Organisation und der Daten, auf die sie Zugriff haben, angemessen schützen.		
H. Richtlinien und Prozesse in Bezug auf die Klassifizierung, Aufbewahrung, Vernichtung und Verschlüsselung von Daten sind angemessen konzipiert und werden wirksam eingesetzt. Dies bietet einen zielgerichteten Ansatz, der eine vollständige und genaue Aufzeichnung von Daten und die Vertraulichkeit und den Datenschutz sensibler Informationen gewährleistet.		
I. Es gibt ein Verfahren für die Kommunikation von operationelle Cybersicherheitsrisiken, um ein angemessenes Bewusstsein bei Management und Mitarbeiterinnen und Mitarbeitern sicherzustellen. Probleme, Lücken, Unzulänglichkeiten und Kontrollmängel werden dem Leitungs- und Überwachungsorgan und dem Management mitgeteilt, und der Status der Abhilfemaßnahmen wird eng überwacht und gemeldet. Die Nichteinhaltung von Cybersicherheitsrichtlinien wird erkannt, untersucht, berichtet und zeitnah behoben.		

Cybersecurity – Kontrollprozesse

Anforderung	Einhaltung (Ja/Nein/Teilweise)	Erlangte Nachweise oder Gründe für den Ausschluss
A. Priorisierung von Cybersicherheitskontrollen und Sicherstellung, dass damit verbundene Budgets und Ressourcen (z. B. Personal, Software, Tools) zugewiesen werden, um den erwarteten Nutzen zu maximieren.		
B. Sicherstellung, dass die Kontrollen der Cybersicherheit so funktionieren, dass die Ziele der Organisation im Bereich der Cybersicherheit erreicht werden und Probleme rechtzeitig gelöst werden.		
C. Anbieten ausreichender Schulungen des für Cybersicherheitsmaßnahmen zuständigen Personals.		
D. Entwicklung ausreichender Richtlinien und Verfahren, um alle operativen Aspekte der Cybersicherheit und der damit verbundenen Kontrollen zu managen.		
E. Sicherstellung, dass das Management über die notwendigen Ressourcen verfügt, um sich über aufkommende Cybersicherheitsprobleme durch neue Technologien auf dem Laufenden zu halten, Möglichkeiten zur Verbesserung der Abläufe zu erkennen, und zu verstehen, wie Cybersicherheitsbemühungen am besten eingesetzt werden können, um umfassendere Organisationsziele zu beeinflussen.		
F. Angemessene Integration von Cybersicherheit in den Lebenszyklus der Systementwicklung für Geschäftsanwendungen, einschließlich Software und erworbener oder individuell entwickelter Anwendungen.		
G. Einbeziehung von Cybersicherheit in das Management von Hardware (Laptops, Desktops, mobile Geräte).		
H. Implementierung wirksamer Kontrollen in Bezug auf die Unterstützung der Produktionshardware, wie z. B. Konfiguration, Patching, Unterstützung der Benutzerzugriffsverwaltung und Überwachung der Verfügbarkeit und Leistung. Die Organisation hat sowohl die		

Anforderung	Einhaltung (Ja/Nein/Teilweise)	Erlangte Nachweise oder Gründe für den Ausschluss
Angemessenheit der Konzeption als auch die operative Wirksamkeit dieser Kontrollen bewertet.		
I. Optimierung der netzbezogenen Kontrollen in Bezug auf die Netzsegmentierung, die Verwendung und Platzierung von Firewalls, begrenzte Verbindungen zu externen Netzen und/oder Systemen sowie den Einsatz von Präventiv- und Detektivtechnologien wie Systemen zur Erkennung und Verhinderung von Eindringlingen.		
J. Einführung wirksamer Kontrollen für gängige Desktop-Kommunikationsdienste wie E-Mail, Internetbrowser, Videokonferenzen, Messaging und Protokolle zur gemeinsamen Dateinutzung.		
K. Implementierung geeigneter Kontrollen für die Servicebereitstellung, um sicherzustellen, dass die folgenden Bereiche in die Überwachung der Cybersicherheit integriert sind: Change-Management, Service/Helpdesk und Verwaltung der Endbenutzergeräte.		
L. Implementierung angemessener physischer Sicherheitskontrollen, um Informationszentren mit hohem Risiko (wie z. B. Datenzentren, Netzwerkbetriebszentren und Sicherheitsbetriebszentren) vor Angriffen zu schützen.		
M. Implementierung von Kontrollen für die Reaktion auf Vorfälle und die Wiederherstellung.		

Über das The Institute of Internal Auditors

The Institute of Internal Auditors (IIA) ist ein Berufsverband, der weltweit mehr als 245.000 Mitglieder betreut und mehr als 195.000 Zertifizierungen zum Certified Internal Auditor (CIA) vergeben hat. The IIA wurde 1941 gegründet und ist für den Berufsstand der Internen Revision weltweit als führend in Standards, Zertifizierungen, Ausbildung, Forschung und fachlichen Leitlinien anerkannt. Weitere Informationen finden Sie unter www.theiia.org.

Haftungsausschluss

The IIA veröffentlicht dieses Dokument zu Informations- und Ausbildungszwecken. Dieses Material soll keine endgültigen Antworten auf spezifische individuelle Umstände geben und ist daher nur als Leitlinie gedacht. The IIA empfiehlt, in jeder spezifischen Situation unabhängigen Expertenrat einzuholen. The IIA übernimmt keine Verantwortung für jemanden, der sich ausschließlich auf dieses Material verlässt.

Urheberrecht

April 2024

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