Cybersecurity

Topical Requirement

The Institute of
Internal Auditors

Cybersecurity Topical Requirement[1]

Topical Requirements zijn een verplicht onderdeel van het International Professional Practices Framework®, samen met de Global Internal Audit Standards™ en de Global Guidance. De Topical Requirements moeten worden gebruikt in combinatie met de Global Internal Audit Standards, die de gezaghebbende basis vormen voor de beroepspraktijk.

Topical Requirements bieden duidelijke verwachtingen voor interne auditors door een minimum baseline vast te stellen voor het auditen van gespecificeerde risico onderwerpen. Het risicoprofiel van de organisatie kan vereisen dat interne auditors aanvullende aspecten van het onderwerp in overweging nemen.

Naleving van de Topical Requirements verhoogt de consistentie waarmee internal auditdiensten worden uitgevoerd en verbetert de kwaliteit en betrouwbaarheid van internal auditdiensten en -resultaten. Uiteindelijk zullen de Topical Requirements het beroep van internal auditor op een hoger plan brengen.

Interne auditors moeten de Topical Requirements toepassen in overeenstemming met de Global Internal Audit Standards. Conformiteit met de Topical Requirements is verplicht voor assurancediensten en wordt aanbevolen voor adviesdiensten.

De Topical Requirement is van toepassing als het onderwerp een van de volgende is:

A. Het onderwerp van een opdracht in het interne auditplan.
B. Geïdentificeerd tijdens het uitvoeren van een opdracht.
C. Het onderwerp van een opdrachtverzoek dat niet in het oorspronkelijke interne auditplan stond.

Bewijs dat elke vereiste in de Topical Requirement is beoordeeld op toepasbaarheid moet worden gedocumenteerd en bewaard. Het is mogelijk dat niet alle individuele vereisten in elke opdracht van toepassing zijn; als vereisten worden uitgesloten, moet een reden hiervoor worden gedocumenteerd en bewaard. Conformiteit met de Topical Requirement is verplicht en wordt geëvalueerd tijdens kwaliteitstoetsingen.

Raadpleeg voor meer informatie de Cybersecurity Topical Requirement Gebruikershandleiding .

[1] Deze vertaling is met de grootste zorgvuldigheid uitgevoerd, maar bij discussie over de vertaling en in het kader van het CIA-examen is de originele, Engelstalige tekst van toepassing. In deze vertaling zijn Engelse termen behouden voor woorden die in het spraakgebruik ingeburgerd zijn danwel tot mogelijke onduidelijkheid zouden leiden bij een vertaling. Voor deze vertalingen geldt het Auteursrecht.

Cybersecurity

Het National Institute of Standards and Technology (NIST) definieert cyberbsecurity eenvoudigweg als: "Het vermogen om het gebruik van cyberspace te beschermen of te verdedigen tegen cyberaanvallen". Cybersecurity is een subset van de overkoepelende informatiebeveiliging, die NIST definieert als: "De bescherming van informatie en informatiesystemen tegen ongeautoriseerde toegang, gebruik, openbaarmaking, verstoring, wijziging of vernietiging om vertrouwelijkheid, integriteit en beschikbaarheid te bieden".

Cybersecurity vermindert risico's door de algemene beheersmgeving te versterken en de informatiemiddelen van een organisatie te beschermen tegen ongeoorloofde toegang, verstoring, wijziging of vernietiging. Cyberaanvallen kunnen leiden tot directe en indirecte gevolgen die vaak aanzienlijk zijn, aangezien computers, netwerken, programma's, gegevens en gevoelige informatie cruciale onderdelen zijn van de meeste organisaties.

Evalueren en Beoordelen Cybersecurity governance, risicomanagement en beheersprocessen

Deze Topical Requirement biedt een consistente, allesomvattende aanpak voor het beoordelen van het ontwerp en de implementatie van processen voor cybersecurity governance, risicomanagement en beheersprocessen. De vereisten vormen een minimale basis voor het beoordelen van cybersecurity in een organisatie.

GOVERNANCE: Evalueren en Beoordelen Cybersecurity Governance

Vereisten:

Interne auditors moeten het volgende beoordelen in relatie tot de cybersecurity governancevan de organisatie:

- **A.** Een formele strategie en doelstellingen voor cybersecurity zijn vastgesteld en worden periodiek bijgewerkt. Updates over het bereiken van de cybersecurity-doelstellingen worden periodiek gecommuniceerd en beoordeeld door het bestuur, inclusief middelen en budgettaire overwegingen om de cybersecurity-strategie te ondersteunen.
- **B.** Beleid en procedures met betrekking tot cybersecurity zijn opgesteld en worden periodiek bijgewerkt om de beheersomgeving te versterken.
- **C.** Rollen en verantwoordelijkheden ie de cybersecurity-doelstellingen ondersteunen zijn vastgesteld d en er bestaat een proces om periodiek de kennis, vaardigheden en capaciteiten te beoordelen van de personen die de rollen vervullen.
- **D.** Relevante belanghebbenden worden ingeschakeld om bestaande kwetsbaarheden en opkomende bedreigingen in de cybersecurity-omgeving te bespreken en er actie op te ondernemen. Belanghebbenden zijn onder andere het senior management, operations, risicomanagement, human resources, juridische zaken, compliance en leveranciers.

RISICOMANAGEMENT: Evalueren en Beoordelen Cybersecurity Risicomanagement

Vereisten:

Interne auditors moeten het volgende beoordelen in relatie tot het risicomanagement van de organisatie op het gebied van cybersecurity:

A. De risicobeoordelings- en risicomanagementprocessen van de organisatie omvatten het identificeren, analyseren, beperken en monitoren van cybersecurity-bedreigingen en hun effect op het behalen van strategische doelstellingen.

B. Risicomanagement op het gebied van cybersecurity wordt in de hele organisatie uitgevoerd en kan de volgende gebieden omvatten: informatietechnologie, enterprise risk management, human resources, juridische zaken, compliance, operations, toeleveringsketen, boekhouding, financiën en andere.

C. Verantwoording en verantwoordelijkheid voor het management van cybersecurity-risico's zijn vastgesteld. Er is een persoon of team aangewezen dat periodiek controleert en rapporteert hoe de risico's op het gebied van cybersecurity worden gemanaged, inclusief de middelen die nodig zijn om risico's te beperken en nieuwe bedreigingen voor cybersecurity te identificeren.

D. Er is een proces vastgesteld om elk (nieuw of eerder geïdentificeerd) cybersecurity-risico dat een onaanvaardbaar niveau bereikt snel te escaleren volgens de vastgestelde richtlijnen voor risicomanagement van de organisatie of toepasselijke wet- en regelgeving. Er moet rekening worden gehouden met de financiële en niet-financiële gevolgen van cybersecurity-risico's.

E. Er is een proces ingesteld om het management en de werknemers bewust te maken van de risico's op het gebied van cybersecurity en om het management periodiek te laten kijken naar problemen, lacunes, tekortkomingen of falende controles, met tijdige rapportage en herstel.

F. De organisatie heeft een respons-- en herstelproces voor cybersecurity-incidenten geïmplementeerd dat detectie, indamming, herstel en analyse na het incident omvat. Het incidentrespons- en herstelproces wordt periodiek getest.

BEHEERSING: Evalueren en Beoordelen Cybersecurity Beheerprocessen

Vereisten:

Interne auditors moeten het volgende beoordelen met betrekking tot de beheersprocessen van de organisatie voor cybersecurity:

A. Er is een proces ingesteld om ervoor te zorgen dat zowel interne als door leveranciers uitgevoerde beheersmaatregelen aanwezig zijn om de vertrouwelijkheid, integriteit en beschikbaarheid van de systemen en gegevens van de organisatie te beschermen. Er worden periodiek evaluaties uitgevoerd om te bepalen of de beheersmaatregelen zodanig functioneren dat de doelstellingen van de organisatie op het gebied van cybersecurity worden behaald en problemen snel worden opgelost.

B. Er is een talentmanagementproces vastgesteld dat training omvat om technische competenties met betrekking tot cybersecurity-operaties te ontwikkelen en te onderhouden. Het proces wordt periodiek geëvalueeerd.

C. Er is een proces ingesteld om voortdurend nieuwe bedreigingen en kwetsbaarheden op het gebied van cybersecurity te bewaken en te rapporteren en om mogelijkheden voor verbetering van de cybersecurity-activiteiten te identificeren, prioriteren en implementeren.

D. Cybersecurity is opgenomen in het management van de levenscyclus (selectie, gebruik, onderhoud en buitengebruikstelling) van alle IT-middelen, inclusief hardware, software en leveranciersdiensten.

E. Er zijn processen vastgesteld om de cybersecurity te versterken, waaronder configuratie, beheer van eindgebruikersapparaten, encryptie, patching, beheer van gebruikerstoegang en monitoring van beschikbaarheid en prestaties. Cybersecurity-overwegingen worden meegenomen in softwareontwikkeling (DevSecOps).

F. Netwerkgerelateerde beheersmaatregelen zijn ingesteld, zoals beheersing van netwerktoegang en segmentatie; het gebruik en de plaatsing van firewalls; beperkte verbindingen van en naar externe netwerken; virtuele privénetwerken (VPN's)/zero trust network access (ZTNA); netwerkbeheersing voor Internet of Things (IoT); en inbraakdetectie/-preventiesystemen (IDS en IPS).

G. Beveiligingsmaatregelen voor endpoint-communicatie zijn ingesteld voor diensten zoals e-mail, internetbrowsers, videoconferenties, messaging, sociale media, cloud en protocollen voor het delen van bestanden.

Over het Instituut van Interne Auditors

Het Institute of Internal Auditors (IIA) is een internationale beroepsvereniging met wereldwijd meer dan 255.000 leden en wereldwijd meer dan 200.000 Certified Internal Auditor® (CIA®)-certificeringen. Het IIA is opgericht in 1941 en wordt over de hele wereld erkend als de leider van het internal auditberoep op het gebied van standaarden, certificeringen, onderwijs, onderzoek en technische begeleiding. Ga voor meer informatie naar www.theiia.org.

Copyright

Februari 2025

The Institute of Internal Auditors

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