Cybersecurity

Topical Requirement

Gebruikershandleiding

Inhoud[1]

[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.

Overzicht van Topical Requirements

Topical Requirements vormen een essentieel onderdeel van het International Professional Practices Framework®, samen met de Global Internal Audit Standards™ en de Global Guidance. Het Instituut van of Internal Auditors vereist dat de Topical Requirements worden gebruikt in combinatie met de Global Internal Audit Standards, die de gezaghebbende basis vormen voor de beroepspraktijk. Verwijzingen naar de Standaarden zijn in deze gebruikershandleiding opgenomen als bron van meer gedetailleerde informatie.

Topical Requirements formaliseren hoe internal auditors omgaan met veelvoorkomende risicogebieden om kwaliteit en consistentie binnen de beroepsgroep te bevorderen. Topical Requirements leggen een basis en bieden relevante criteria voor het uitvoeren van assurancediensten met betrekking tot het onderwerp van een Topical Requirement (Standaard 13.4 Evaluatiecriteria). Conformiteit met de Topical Requirements is verplicht voor assurancediensten en wordt aanbevolen voor evaluatie tijdens adviesdiensten. Het is niet de bedoeling dat Topical Requirements alle mogelijke aspecten omvatten waarmee rekening moet worden gehouden bij het uitvoeren van assurance-opdrachten; ze zijn eerder bedoeld om een minimale set vereisten te bieden om een consistente, betrouwbare beoordeling van het onderwerp mogelijk te maken.

De Topical Requirements sluiten duidelijk aan bij het Three Lines Model van het IIA en de Global Internal Audit Standards. Governance-, risicomanagement- en beheersprocessen zijn de belangrijkste onderdelen van de Topical Requirements ,die aansluiten bij Standaard 9.1 Inzicht in governance-, risicomanagement- en beheersprocessen. In verwijzing naar het Three Lines Model, is governance gekoppeld aan het bestuur/het bestuursorgaan, risicomanagement aan de tweede lijn en beheersing of beheersprocessen aan de eerste lijn. Terwijl het management vertegenwoordigd is in zowel de eerste als de tweede lijn, wordt de internal auditfunctie weergegeven in de derde lijn als een onafhankelijke en objectieve leverancier van zekerheid, die rapporteert aan het bestuur/het bestuursorgaan (Principe 8 Onder toezicht van het bestuur).

Toepasbaarheid, risico en professionele oordeelsvorming

Topical Requirements moeten worden nageleefd wanneer internal auditfuncties assurance-opdrachten uitvoeren met betrekking tot onderwerpen waarvoor een Topical Requirement bestaat of wanneer aspecten van de Topical Requirement worden geïdentificeerd binnen andere assurance-opdrachten.

Zoals beschreven in de Standaarden is het beoordelen van risico's een belangrijk onderdeel van de planning van het hoofd van de internal auditfunctie. Om te bepalen welke assurance-opdrachten in het internal auditplan moeten worden opgenomen, moeten de strategieën,

doelstellingen en risico's van de organisatie ten minste jaarlijks worden beoordeeld (Standaard 9.4 Internal Auditplan). Bij het plannen van individuele assurance-opdrachten moeten internal auditors de risico's beoordelen die relevant zijn voor de opdracht (Standaard 13.2 Risicobeoordeling in de opdracht).

Wanneer het onderwerp van een Topical Requirement wordt geïdentificeerd tijdens het risicogebaseerde planningsproces van de internal audit en wordt opgenomen in het auditplan, dan moeten de in de Topical Requirement beschreven vereisten worden gebruikt om het topic binnen de van toepassing zijnde opdrachten te beoordelen. Bovendien, wanneer internal auditors een opdracht uitvoeren (al dan niet opgenomen in het plan) en elementen van een Topical Requirement naar voren komen, moet de Topical Requirement worden beoordeeld op toepasbaarheid als onderdeel van de opdracht. Tot slot, als een opdracht wordt aangevraagd die oorspronkelijk niet in het plan was opgenomen en het onderwerp bevat, moet de Topical Requirement worden beoordeeld op toepasbaarheid.

Professionele oordeelsvorming speelt een belangrijke rol bij de toepassing van de Topical Requirement. Risicobeoordelingen vormen de basis voor beslissingen van hoofden van de internal auditfunctie over welke opdrachten in het internal auditplan moeten worden opgenomen (Standaard 9.4 Internal Auditplan). Daarnaast gebruiken internal auditors professionele oordeelsvorming om te bepalen welke aspecten binnen elke opdracht aan bod zullen komen (Standaard 13.3 Doelstellingen en scope van de opdracht, 13.4 Evaluatiecriteria en 13.6 Werkprogramma). In Bijlage A "Voorbeelden van praktische toepassingen" wordt beschreven hoe internal auditors bepalen of een Topical Requirement van toepassing is.

Er moet bewijs worden bewaard dat elke vereiste in de Topical Requirement is beoordeeld op toepasbaarheid, met inbegrip van een motivering voor de uitsluiting van eisen. Conformiteit met de Topical Requirement moet worden gedocumenteerd op basis van de professionele oordeelsvorming van de auditor zoals beschreven in Standaard 14.6 Documentatie van de opdracht.

Hoewel de Cybersecurity Topical Requirement een basislijn geeft van beheersprocessen om rekening mee te houden, moeten organisaties die het cyberrisico als zeer hoog inschatten mogelijk aanvullende aspecten beoordelen.

Als een hoofd van de internal auditfunctie vaststelt dat de internal auditfunctie niet over de vereiste kennis beschikt om controleopdrachten uit te voeren met betrekking tot een onderwerp uit de Topical Requirements, kunnen de werkzaamheden worden uitbesteed (Standaarden 3.1 Competentie, 7.2 Kwalificaties van hoofd van de internal auditfunctie, 10.2 Beheer van personele middelen). Zelfs in dat geval ontslaat uitbesteding de internal auditfunctie niet van haar verantwoordelijkheid om te voldoen aan de Topical Requirements. Het hoofd van de internal auditfunctie behoudt de eindverantwoordelijkheid voor het garanderen van conformiteit. Bovendien, als het hoofd van de internal auditfunctie vaststelt dat de internal audit middelen onvoldoende zijn, moet het hoofd van de internal auditfunctie het bestuur informeren over de impact van onvoldoende middelen en hoe eventuele tekorten aan middelen zullen worden aangepakt (Standaard 8.2 Middelen).

Prestaties, documentatie en rapportage

Bij het toepassen van Topical Requirements moeten internal auditors ook voldoen aan de Standaarden en hun werk uitvoeren in overeenstemming met Domein V: Uitvoeren van internal auditdiensten. De standaarden in domein V beschrijven het plannen van opdrachten (Principe 13 Plan Opdrachten Effectief), het uitvoeren van opdrachten (Principe 14 Voer opdrachtwerkzaamheden uit) en het communiceren van de resultaten van opdrachten (Principe 15 Communiceer opdrachtresultaten en monitor actieplannen).

De dekking van het Topical Requiremkan worden gedocumenteerd in het internal auditplan of in de werkdocumenten op basis van het professionele oordeel van de auditors. Een of meer internal auditopdrachten kunnen de vereisten afdekken. Daarnaast kan het zijn dat niet alle vereisten van toepassing zijn. Er moet bewijsmateriaal worden bewaard waaruit blijkt dat de onderhavige vereiste is beoordeeld op toepasbaarheid, met inbegrip van een motivering voor eventuele uitsluitingen.

Het optionele hulpmiddel in Bijlage C kan worden gebruikt als referentie en om het werk dat internal auditors uitvoeren te documenteren.

Kwaliteit

De Standaarden vereisen dat het hoofd van de internal auditfunctie een programma voor kwaliteitsborging en -verbetering ontwikkelt, implementeert en onderhoudt dat alle aspecten van de internal auditfunctie omvat (Standaard 8.3 Kwaliteit). De resultaten moeten worden gecommuniceerd naar het bestuur en het senior management. In de communicatie moet worden gerapporteerd over de conformiteit van de internal auditfunctie met de Standaarden en het behalen van de prestatiedoelstellingen.

Conformiteit met de Topical Requirements wordt geëvalueerd in kwaliteitsbeoordelingen. Om een kwaliteitsbeoordeling voor te bereiden, kunnen internal auditors gebruik maken van het hulpmiddel in Bijlage C.

Cybersecurity

Cyberbsecurity is een breed onderwerp dat betrekking heeft op de meeste technologische aspecten van elke organisatie. Naast informatietechnologie maakt cybersecurity vaak deel uit van bedrijfsprocessen, waardoor internal auditors cybergerelateerde risico's moeten beoordelen bij het plannen, afbakenen en uitvoeren van assurance-opdrachten.

Het National Institute of Standards and Technology (NIST), onderdeel van het Amerikaanse Ministerie van Handel, definieert cybersecurity eenvoudigweg als "Het vermogen om het gebruik van cyberspace te beschermen of te verdedigen tegen cyberaanvallen". De Cybersecurity Topical Requirement richt zich op de externe perimeter die organisaties beveiligen om risico's van onbevoegde gebruikers en kwaadaardige cyberbedreigingen te beperken. Cybersecurity is een onderdeel van de overkoepelende informatiebeveiliging, die NIST definieert als "De bescherming van informatie en informatiesystemen tegen onbevoegde toegang, onbevoegd gebruik, openbaarmaking, verstoring, wijziging of vernietiging om te zorgen voor vertrouwelijkheid, integriteit en beschikbaarheid".

Vereisten van de Cybersecurity Topical Requirement zijn onder andere:

- Governance - duidelijk gedefinieerde cybersecurity-doelen en -strategieën die de doelen, het beleid en de procedures van de organisatie ondersteunen.
- Risicomanagement - processen om cyberbedreigingen te identificeren, analyseren, beheren en bewaken, inclusief een proces om cyberrisico's snel te escaleren.
- Beheersing - door het management vastgestelde, periodiek geëvalueerde beheersprocessen om cyberrisico's te beperken.

Overwegingen

Internal auditors kunnen de volgende overwegingen gebruiken als hulpmiddel bij hun beoordeling van de vereisten in de Cybersecurity Topical Requirement. Deze overwegingen, die verwijzen naar de vereisten, zijn illustratief maar niet verplicht. Internal auditors moeten op hun professionele oordeel afgaan bij het bepalen wat ze in hun beoordelingen opnemen.

Governance overwegingen

Om te beoordelen hoe de governanceprocessen worden toegepast op cybersecurity-doelstellingen, kunnen internal auditors een review uitvoeren van:

A. Geformaliseerd, gedocumenteerd strategisch plan en doelstellingen voor cybersecurity, inclusief bewijs dat de raad van bestuur periodiek (over het algemeen elk kwartaal) de cybersecurity-updates beoordeelt die worden verstrekt door het hoofd van de informatiebeveiligingsfunctie, zoals de chief information security officer (CISO). Het bewijs kan bestaan uit rapportage over:
   - De monitoring van de realisatie van strategische doelstellingen.
   - Budgettaire behoeften om doelen en doelstellingen op het gebied van cybersecurity te ondersteunen.
   - Focus op risico's en interne beheersmaatregelen, inclusief de voortgang van herstelmaatregelen.
   - Key performance indicators (KPI's) om succes te meten.
   - Personele middelen die nodig zijn om cybersecurity-personeel aan te nemen, op te leiden en te ontwikkelen.

B. Beleid, procedures en andere relevante documentatie die wordt gebruikt om cybersecurity-processen te managen, waaronder:
   - Beleid dat ten minste jaarlijks wordt herzien en bijgewerkt. Opkomende cyberrisico's kunnen vereisen dat beoordelingen en updates vaker plaatsvinden.
   - Een proces om te bepalen of beleid en procedures voldoende zijn om cybersecurity-activiteiten te ondersteunen.
   - Wijdverbreide frameworks (NIST, COBIT en andere) om cybersecurity-processen en interne beheersing te versterken.

C. Rollen en verantwoordelijkheden die het bereiken van cybersecurity-doelstellingen ondersteunen, inclusief een structuur die ervoor zorgt dat de cybersecurity-functie rapporteert aan een niveau in de organisatie dat voldoende zichtbaarheid heeft om organisatorische steun te bereiken.
   - Een proces om periodiek de kennis, vaardigheden en capaciteiten te beoordelen van het personeel dat cybersecurity-functies vervult.

D. Bewijs van betrokkenheid bij relevante belanghebbenden (bijvoorbeeld senior management, operations, risicomanagement, human resources, juridische zaken, compliance, strategische leveranciers en anderen), inclusief communicatie over

bestaande en nieuwe cyberrisico's en bekende potentiële kwetsbaarheden. Bewijs van communicatie kan bestaan uit notulen van vergaderingen, rapporten of e-mails.

Overwegingen met betrekking tot risicomanagement

Om te beoordelen hoe risicomanagementprocessen worden toegepast op cybersecurity-doelstellingen, kunnen internal auditors een review uitvoeren van:

A. Hoe de organisatie cybersecurity-risico's beoordeelt en managet, inclusief hoe bedreigingen en kwetsbaarheden worden beoordeeld:
   - Allereerst geïdentificeerd en gerapporteerd.
   - Geanalyseerd om het risico voor het bereiken van de doelstellingen van de organisatie te evalueren.
   - Beperkt, inclusief actieplannen om het risico tot een aanvaardbaar niveau terug te brengen.
   - Bewaakt, inclusief een plan voor doorlopende rapportage totdat bedreigingen volledig zijn opgelost.

B. Hoe de organisatie periodiek input verkrijgt van functionele gebieden, zoals informatietechnologie, enterprise risk management, human resources, juridische zaken, compliance, operations, boekhouding en financiën. Een cross-functioneel cybersecurity-team of IT-stuurgroep kan worden gebruikt om informatie te verkrijgen.

C. Hoe de organisatie de verantwoordelijkheid en verantwoordelijkheid voor risicomanagement op het gebied van cybersecurity heeft toegewezen aan een individu of team.
   - De verantwoordelijke(n) moet(en) periodiek (driemaandelijks, maandelijks of indien nodig) de lopende updates van de risico's voor cybersecurity binnen de hele organisatie communiceren en kan (kunnen) ook de benodigde middelen voor risicobeperkende strategieën bevatten.

D. De escalatieprocessen voor cybersecurity-risico's, met inbegrip van de manier waarop het dreigings- of risiconiveau wordt geëvalueerd, toegewezen en geprioriteerd. De beoordeling kan het identificeren van de:
   - De gedefinieerde risiconiveaus van de organisatie - zoals hoog, gemiddeld en laag - met gedetailleerde uitleg over elk risiconiveau en escalatieprocedures voor elke risicocategorie.
   - Lijst van cybersecurity-risico's die momenteel zijn geïdentificeerd en de mitigatiestatus van elke risicogebeurtenis.
   - Toepasselijke wettelijke, regelgevende en nalevingsvereisten.
   - Zowel financiële als niet-financiële (bijvoorbeeld reputatie) risico's.

E. Het proces voor het communiceren van cybersecurity-risico's aan management en werknemers, waaronder:

- Periodieke (minstens jaarlijks) cybersecurity-training voor werknemers, zoals onaangekondigde, gesimuleerde phishing-campagnes om het bewustzijn van de organisatie te testen en bij te houden.
- Updates over het herstel van bestaande cybersecurity-problemen, met verwachte voltooiingsdata.
- Controle op niet-naleving, inclusief updates aan het bestuur en het senior management.
- Opnieuw beoordelen van bedreigingen wanneer de risicobereidheid en risicotolerantie van de organisatie verandert.

F. Processen die de organisatie heeft geïmplementeerd met betrekking tot respons op en herstel van incidenten, waaronder:

- Een gedocumenteerd plan dat wordt herzien en bijgewerkt als de activiteiten van de organisatie na verloop van tijd veranderen. Het plan moet het volgende omvatten
  - Hoe incidenten worden gedetecteerd en gerapporteerd.
  - Hoe incidenten onder controle worden gehouden om verdere schade te voorkomen.
  - Hoe de organisatie zal herstellen en reageren om de activiteiten te hervatten.
  - Hoe het incident zal worden geanalyseerd om lessen te trekken en hoe soortgelijke gebeurtenissen in de toekomst kunnen worden voorkomen.
- Periodiek (minstens jaarlijks) testen (tabletop exercise) en de resultaten rapporteren aan het senior management en relevante belanghebbenden. Uit de tests kunnen actieplannen voortvloeien.

Overwegingen voor beheersprocessen

Om te beoordelen beheersprocessen worden toegepast op cybersecurity-doelstellingen, kunnen internal auditors een review uitvoeren van:

A. De aanpak van het management voor het opbouwen van een effectieve interne beheersomgeving voor cybersecurity, inclusief:
- De interne beheersmaatregelen beoordelen en implementeren die nodig zijn om verhoogde risico's te beperken en gevoelige, kritieke, persoonlijke of vertrouwelijke gegevens te beschermen, op basis van het risicobeoordelingsproces van de organisatie.
- Bepalen welke middelen nodig zijn om de belangrijkste cybersecurity-beheersmaatregelen te onderhouden.
- Door leveranciers uitgevoerde controles beschouwen als onderdeel van de beheersomgeving, waaronder het beoordelen van service organisation controls

(SOC-rapporten) van leveranciers voor aanvang van de zakelijke relatie en gedurende de gehele relatie.

- Periodiek testen of cybersecurity-beheersmaatregelen werken op een manier die risico's beperkt en het behalen van cybersecurity-doelstellingen ondersteunt.
- Proces voor het verhelpen van tekortkomingen in de interne beheersing of het aanpakken van bevindingen uit beoordelingen die zijn uitgevoerd door de internal auditfunctie of andere assurance providers (bijvoorbeeld penetratietests).

B. Het talentmanagementproces van de organisatie voor het werven en trainen van cybersecurity-professionals, inclusief hoe de organisatie mogelijkheden identificeert om de capaciteiten van cybersecurity-professionals te vergroten om de technische kennis van de organisatie te ondersteunen en het bewustzijn van de organisatie van opkomende problemen te verbeteren.
   - Voorbeelden hiervan zijn deelname aan trainingen, betrokkenheid bij groepen die kennis delen en permanente professionele educatie, waaronder het behalen van cybergerelateerde certificeringen.

C. Het proces van het management voor het identificeren, prioriteren, monitoren en rapporteren van opkomende bedreigingen en kwetsbaarheden voor cybersecurityop een continue basis die gericht is op de dagelijkse activiteiten. De beoordeling kan inhouden dat er processen zijn vastgesteld om bedreigingen en kwetsbaarheden te beoordelen die verband houden met nieuwe of opkomende technologieën, zoals het gebruik van kunstmatige intelligentie.

D. De processen en beheersmaatregelen van het management die zijn ingesteld om IT-middelen gedurende de hele levenscyclus te beheren en te beschermen, waaronder de selectie, het gebruik, het onderhoud en de buitengebruikstelling van hardware, software en diensten van leveranciers. Hardware omvat servers, netwerkapparatuur (zoals routers of firewalls), desktops, laptops, mobiele telefoons, tablets en randapparatuur. Software omvat besturingssystemen (zoals Windows), software voor enterprise resource planning, applicaties, antivirusprogramma's en andere. Overwegingen met betrekking tot hardware en software kunnen zijn:
   - Het gebruik door de organisatie van encryptie, antivirussoftware, beheer van mobiele apparaten, complexe wachtwoordvereisten, virtual private network (VPN)/ zero trust networking (ZTN) voor verificatie en het periodiek bijwerken van firmware.
   - Een proces voor middelenbeheer dat ervoor zorgt dat de hardware die door het bedrijf wordt uitgegeven, bij uitgifte de juiste beveiligingsconfiguratie heeft en op de juiste manier wordt verwijderd wanneer de activa buiten gebruik worden gesteld.
   - Databasegerelateerde beheersmaatregelen, waaronder het beperken van de toegang van gebruikers en beheerders, het waarborgen van het gebruik van encryptie, het maken van back-ups en het testen van databases, en de aanwezigheid van sterke netwerkbeveiligingscontroles.

- Hoe cybersecurity-bedreigingen of kwetsbaarheden worden overwogen in de levenscyclus van de systeemontwikkeling (the system development life cycle, SDLC).
- De aanpak die wordt gebruikt door ontwikkeling, beveiliging en bedrijfsvoering (development, security, and operations, DevSecOps) om ervoor te zorgen dat het ontwikkelingsproces van software cybersecurity omvat om kwetsbaarheden proactief te identificeren.

E. Processen die worden gebruikt om de cybersecurity te versterken, waaronder:
   - Configuratie van beveiligingsinstellingen om het risico op cybersecurity te minimaliseren.
   - Het beheer van mobiele apparaten (inclusief het gebruik van e-mail en applicaties) is zodanig geconfigureerd dat cybersecurity-risico's worden beperkt en op afstand worden beheerd als het apparaat van een gebruiker is gecompromitteerd.
   - Het gebruik van versleuteling voor gegevens "in rust", zoals informatie opgeslagen op een harde schijf, of gegevens "in transit", zoals het versleutelen van e-mails.
   - Het patchen van servers of software (zoals een besturingssysteem) met de nieuwste beveiligingsreleases.
   - Toegangsbeheer voor gebruikers, zoals het gebruik van multifactorauthenticatie (MFA) en unieke gebruikers-ID's met complexe wachtwoorden die periodiek verlopen.
   - Monitoring om te bepalen of de beschikbaarheid en het gebruik van bronnen voldoende zijn, zodat mogelijke cybersecurity-problemen die de prestaties bedreigen, kunnen worden beoordeeld en geanalyseerd.
   - Integratie van cybersecurity in de SDLC om kwetsbaarheden op het gebied van cybersecurity te identificeren en aan te pakken voordat software in productie wordt genomen.

F. Netwerkgerelateerde controles die de perimeter van de organisatie beveiligen, inclusief hoe de organisatie deze gebruikt:
   - Netwerksegmentatie.
   - Firewalls.
   - Toegangscontroles voor gebruikers.
   - Beperkingen voor zowel externe als interne verbindingen.
   - Controles rond het Internet of Things (IoT) voor onderling verbonden netwerken.
   - Inbraakdetectie-/preventiesystemen om cybersecurity-aanvallen te voorkomen, op te sporen en te herstellen.

G. Beveiligingsmaatregelen voor endpoint-communicatie die van toepassing zijn op diensten zoals e-mail, internetbrowsers, videoconferenties, messaging (Zoom, MS

Teams en andere), sociale media, cloud en protocollen voor het delen van bestanden. Beheersmaatregelen kunnen bestaan uit het beperken van het gebruik van bepaalde bestandsextensies (zoals .exe-bestanden) en multifactorauthenticatie voor het delen van bestanden.

Bijlage A. Voorbeelden van praktische toepassingen

De volgende voorbeelden beschrijven scenario's waarin de Cybersecurity Topical Requirement van toepassing zou zijn:

Voorbeeld 1: Cybersecurity wordt geïdentificeerd voor een internal auditopdracht die is opgenomen in het internal auditplan.

Wanneer de internal auditfunctie haar risicogebaseerde planningsproces voltooit en één of meer opdrachten op het gebied van cybersecurity in het internal auditplan opneemt, is de Topical Requirement verplicht bij het uitvoeren van dergelijke opdrachten. Conformiteit kan worden bereikt door de vereisten op te nemen in één of meer opdrachten in het internal auditplan.

Cybersecurity is een breed onderwerp en niet elke vereiste in de Topical Requirement is mogelijk van toepassing op elke opdracht. Wanneer internal auditors op basis van hun professionele oordeelsvorming bepalen dat één of meer vereisten van de Cybersecurity Topical Requirement niet van toepassing zijn en daarom moeten worden uitgesloten van een opdracht, moeten internal auditors de reden voor het uitsluiten van deze vereisten documenteren en bewaren. De reden voor het uitsluiten van bepaalde vereisten kan bijvoorbeeld zijn dat de internal auditfunctie verschillende cybersecurity-opdrachten bij toerbeurt uitvoert of heeft vastgesteld dat het belang van het risico in de opdracht gering is.

Voorbeeld 2: Cybersecurity-risico's worden geïdentificeerd tijdens een auditopdracht die niet gericht is op cyberbeveiliging.

Internal auditors kunnen cybersecurity-risico's vaststellen terwijl ze een proces beoordelen dat niet direct verband houdt met cyberbeveiliging. Internal auditors kunnen bijvoorbeeld het crediteurenproces beoordelen in een opdracht die niet gericht is op cybersecurity en bij het plannen van de opdracht cybersecurity-risico's niet identificeren als behorend tot de scope. Echter, na het uitvoeren van de initiële walkthrough stellen internal auditors vast dat dergelijke risico's binnen de scope moeten vallen; ze stellen bijvoorbeeld cybersecurity-risico's vast met betrekking tot het webgebaseerd indienen van een initiële inkooporderaanvraag (Standaard 13.2 Risicobeoordeling in de opdracht).

Zodra de relevante risico's zijn geïdentificeerd, moeten internal auditors de Cybersecurity Topical Requirement bekijken en bepalen welke vereisten van toepassing zijn. In dit voorbeeld zouden ze het proces voor de governance of het risicomanagement van cybersecurity kunnen uitsluiten. Zij moeten in de werkdocumenten van de opdracht de reden

voor het uitsluiten van de andere vereisten van de Cybersecurity Topical Requirement documenteren en de documentatie bewaren.

Voorbeeld 3: Er wordt een opdracht voor cybersecurity aangevraagd die oorspronkelijk niet in het internal auditplan was opgenomen.

Belanghebbenden zoals het bestuur, het management of een toezichthouder kunnen internal auditors vragen om cybersecurity-beoordelingen uit te voeren buiten het oorspronkelijke auditplan. Bijvoorbeeld, wanneer organisaties het doelwit zijn van een cyberaanval, kan het bestuur vragen om een internal auditopdracht om de cybersecurity-beheersing te beoordelen. De Topical Requirement is van toepassing, de vereisten moeten worden beoordeeld en eventuele uitsluitingen moeten worden gedocumenteerd.

Bijlage B. Vergelijking met frameworks

De organisatie kan haar eigen inspanningen op het gebied van cybersecurity hebben, waarbij gebruik wordt gemaakt van raamwerken voor risicomanagement en governance, zoals COBIT of NIST. Internal auditors hebben mogelijk al auditprogramma's en testprocedures ontwikkeld op basis van deze raamwerken. Internal auditors moeten hun voorgenomen beoordelingen van de cybersecurity-maatregelen afstemmen op de Topical Requirement om ervoor te zorgen dat deze voldoende dekking bieden. In het onderstaande schema wordt de Cybersecurity Topical Requirement gerelateerd aan drie veelgebruikte raamwerken: NIST Cybersecurity Framework 2.0, COBIT 2019 en NIST 800-53. De relatie met deze raamwerken is in kaart gebracht omdat deze kosteloos beschikbaar zijn.

Vereisten voor Governance	Framework Referenties		
	NIST-CDF 2.0	NIST 800-53	COBIT 2019
A. Een formele cybersecurity-strategie en doelstellingen zijn vastgesteld en worden periodiek bijgewerkt. Updates over de verwezenlijking van de cybersecurity-doelstellingen worden periodiek meegedeeld en beoordeeld door de raad, met inbegrip van middelen en budgettaire overwegingen ter ondersteuning van de cybersecurity-strategie.	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. Beleid en procedures met betrekking tot cybersecurity zijn opgesteld en worden periodiek bijgewerkt om de beheersomgeving te versterken.	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. Rollen en verantwoordelijkheden die de cybersecurity-doelstellingen ondersteunen zijn vastgesteld en er bestaat een proces om periodiek de kennis, vaardigheden en capaciteiten te beoordelen van degenen die deze rollen vervullen.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

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 senior management, operations, risicomanagement, personeelszaken, juridische zaken, compliance en leveranciers.	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
Vereisten voor Risicomanagement	**NIST-CDF 2.0**	**NIST 800-53**	**COBIT 2019**
A. De risicobeoordelings- en risicomanagementprocessen van de organisatie omvatten de identificatie, analyse, beperking en bewaking van cybersecurity-bedreigingen en hun effect op het bereiken van strategische doelstellingen.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
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.	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. Verantwoording en verantwoordelijkheid voor het management van cybersecurity-risico's zijn vastgesteld en er is een persoon of team aangewezen dat periodiek controleert en rapporteert hoe cybersecurity-risico's worden gemanaged, inclusief de middelen die nodig zijn om risico's te beperken en nieuwe bedreigingen voor cybersecurity te identificeren.	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. 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.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. Er is een proces vastgesteld 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.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
G. 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.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

Vereisten voor Beheersprocessen	NIST-CDF 2.0	NIST 800-53	COBIT 2019
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.	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. 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 geëvalueerd.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. Er is een proces vastgesteld 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.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. Cybersecurity is opgenomen in het management van de levenscyclus (selectie, gebruik, onderhoud en buitengebruikstelling) van alle IT-middelen, inclusief hardware, software en leveranciersdiensten.	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. Er zijn processen vastgesteld om 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).	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. 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).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
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.	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

Bijlage C. Optioneel hulpmiddel voor documentatie

Van internal auditors wordt verwacht dat zij hun professionele oordeel gebruiken bij het bepalen van de toepasbaarheid van de vereisten op basis van de risicobeoordeling en dat zij de uitsluiting van bepaalde vereisten op passende wijze documenteren. De Topical Requirement kan worden gedocumenteerd in het internal auditplan of in de werkdocumenten van de betreffende opdracht, op basis van de professionele oordeelsvorming van de auditor. Eén of meer internal auditopdrachten kunnen de vereisten afdekken. Daarnaast kunnen niet alle vereisten van toepassing zijn. Het afdrukbare formulier hieronder biedt een optie voor het documenteren van conformiteit met de Cybersecurity Topical Requirement, maar het gebruik ervan is niet verplicht.

Cybersecurity - Governance

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
A. Een formele cybersecurity-strategie en doelstellingen zijn vastgesteld en worden periodiek bijgewerkt. Updates over de verwezenlijking van de cybersecurity-doelstellingen worden periodiek meegedeeld en beoordeeld door de raad, met inbegrip van middelen en budgettaire overwegingen ter ondersteuning van de cybersecurity-strategie.		
B. Beleid en procedures met betrekking tot cybersecurity zijn opgesteld en worden periodiek bijgewerkt om de beheersomgeving te versterken.		
C. Rollen en verantwoordelijkheden die de cybersecurity-doelstellingen ondersteunen zijn vastgesteld en er bestaat een proces om periodiek de kennis, vaardigheden en capaciteiten te beoordelen van degenen die deze rollen vervullen.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
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 senior management, operations, risicomanagement, personeelszaken, juridische zaken, compliance en leveranciers		

Cybersecurity - Risicomanagement

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
A. De risicobeoordelings- en risicomanagementprocessen van de organisatie omvatten de identificatie, analyse, beperking en bewaking van cybersecurity-bedreigingen en hun effect op het bereiken 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 en er is een persoon of team aangewezen dat periodiek controleert en rapporteert hoe cybersecurity-risico's worden gemanaged, inclusief de middelen die nodig zijn om risico's te beperken en nieuwe bedreigingen voor cybersecurity te identificeren		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
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 vastgesteld 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.		

Cybersecurity - Beheersprocessen

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
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 geëvalueerd.		
C. Er is een proces vastgesteld 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.		

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
E. Er zijn processen vastgesteld om 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.

Disclaimer

Het IIA publiceert dit document voor informatieve en educatieve doeleinden. Dit materiaal is niet bedoeld om definitieve antwoorden te geven op specifieke individuele omstandigheden en is als zodanig alleen bedoeld als leidraad. Het IIA raadt aan onafhankelijk deskundig advies in te winnen met betrekking tot een specifieke situatie. Het IIA aanvaardt geen verantwoordelijkheid voor personen die uitsluitend vertrouwen op dit materiaal.

Copyright

Februari 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