Organizational resilience

Topical Requirement

Gebruikershandleiding

The Institute of Internal Auditors

Vertaald door

Instituut van Internal Auditors Nederland

Inhoud

Overzicht van Topical Requirements[1]

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 Internal Auditors vereist dat de Topical Requirements worden gebruikt in combinatie met de Global Internal Audit Standards (Standaard 4.1 Conformiteit 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. Het mandaat van de internal auditfunctie definieert duidelijk de reikwijdte en de soorten diensten die door de internal auditfunctie worden uitgevoerd, waarbij ook rekening wordt houden met Topical Requirements (Standaard 6.1 Internal auditmandaat). 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.

Topical Requirements sluiten duidelijk aan op het Three Lines Model en de Standaarden van het IIA. 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).

---

[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.*

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. (Zie Standaard 9.4 met betrekking tot wijzigingen in het Internal auditplan).

Professionele oordeelsvorming speelt een belangrijke rol bij de toepassing van de Topical Requirement. Risicobeoordelingen vormen de basis voor beslissingen van hoofden internal audit 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) en om de middelen te identificeren die nodig zijn om de doelstellingen van de opdracht te bereiken (Standaard 13.5 Middelen voor de opdracht). In bijlage A, "Voorbeelden van praktische toepassingen", wordt beschreven hoe internal auditors de Topical Requirement van gebruiken.

Niet alle individuele vereisten zijn van toepassing op elke opdracht, en sommige kunnen via andere benaderingen worden ingevuld. Als een vereiste wordt uitgesloten of vervangen door andere wet- en regelgeving of contractuele vereisten, of wordt ingevuld door de implementatie van procedures in overeenstemming met de Standaarden, moet de onderbouwing daarvan worden gedocumenteerd en bewaard. Conformiteit wordt geëvalueerd tijdens kwaliteitstoetsingen.

Conformiteit met de Topical Requirement moet worden gedocumenteerd op basis van de professionele oordeelsvorming van auditors zoals beschreven in Standaard 14.6 Documentatie van de opdracht.

Hoewel de Topical Requirement Organizational resilience een basis biedt voor beheersprocessen waarmee rekening moet worden gehouden, kunnen organisaties die dit risicothema als zeer hoog inschatten, aanvullende aspecten moeten beoordelen.

Als een hoofd internal audit 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 aan een externe dienstverlener (Standaarden 3.1 Competentie, 7.2 Kwalificaties van het hoofd van de internal auditfunctie, 10.2 Beheer van personele middelen). Hoofden internal audit kunnen het Internal Auditing Competency Framework™ van het IIA als een nuttig hulpmiddel beschouwen. De Standaarden zijn van toepassing op elke persoon of functie die internal auditdiensten levert, ongeacht of een organisatie internal auditors rechtstreeks in dienst heeft, deze via een externe dienstverlener inhuurt, of beide. Het hoofd van de internal auditfunctie behoudt de eindverantwoordelijkheid voor het waarborgen 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 opdrachtresultaten (Principe 15 Communiceer opdrachtresultaten en monitor actieplannen).

Topical Requirements zijn bedoeld ter ondersteuning van consistente internal auditpraktijken van hoge kwaliteit. Ze moeten worden toegepast in combinatie met toepasselijke lokale wet- en regelgeving, verwachtingen van toezichthouders en andere professioneel erkende frameworks, die aanvullende of meer specifieke vereisten kunnen opleggen. Internal auditors hebben mogelijk al werkprogramma's en testprocedures ontwikkeld op basis van deze wet- en regelgeving en frameworks. Internal auditors dienen hun voorgenomen toetsing van beheersmaatregelen op het gebied van resillence evenals eventuele betrouwbare toetsing door andere interne en externe assurance providers (Standaard 9.5 Coördinatie en vertrouwen) af te stemmen op de Topical Requirement om een adequate dekking te waarborgen.

De dekking van de Topical Requirement kan worden gedocumenteerd in het internal auditplan of in het werkprogramma 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 Topical Requirement is beoordeeld op toepasbaarheid, met inbegrip van een motivering voor eventuele uitsluitingen.

Het optionele hulpmiddel in bijlage D 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, Standaard 8.4 Externe kwaliteitstoetsing, Standaard 12.1 Interne kwaliteitstoetsing). 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 moet worden genomen in toezichtactiviteiten op opdrachtniveau (Standaard 12.3 Toezicht op en verbeteren van prestaties in opdrachten) en zal worden beoordeeld bij kwaliteitstoetsingen. Om een kwaliteitstoetsing voor te bereiden, kunnen internal auditors gebruik maken van het hulpmiddel in bijlage D.

Organizational Resilience

Organizational Resilience verwijst naar het vermogen van een organisatie om veranderingen te weerstaan en zich eraan aan te passen, vooral in tijden van verstoring. Volgens het ISO 22316-framework van de International Organization for Standardization wordt het gedefinieerd als het "vermogen van een organisatie om veranderingen op te vangen en zich aan te passen in een veranderende omgeving". Hoewel deze definitie een duidelijk ambitie neerzet, lopen organisaties in de praktijk sterk uiteen in de manier waarop ze anticiperen op, reageren op, zich aanpassen aan en herstellen van verandering en verstoring. Omdat organizational resilience strategische, operationele, technologische, menselijke, sociale en financiële dimensies omvat, kunnen sommige organisaties veranderingen effectief opvangen, terwijl andere daar moeite mee hebben of in het licht van onzekerheid een andere aanpak kiezen.

Praktisch gezien zijn weerbare organisaties beter in staat om onverwachte uitdagingen te doorstaan en zich verder te ontwikkelen en succesvol te blijven functioneren wanneer ze daarmee worden geconfronteerd.

Talrijke verstoringen kunnen een organisatie verhinderen haar strategische doelen en doelstellingen te realiseren, waaronder, maar niet beperkt tot:

- Natuurrampen, zoals aardbevingen, branden, overstromingen, orkanen, tsunami's, tropische stormen en andere extreme weersomstandigheden.
- Cyberaanvallen, zoals ransomware, malware, denial of service, datalekken, insider threats en andere kwaadaardwillende acties die bedoeld zijn om een organisatie schade toe te brengen of haar te belemmeren bij de uitvoering van activiteiten.
- Geopolitieke conflicten, zoals economische sancties, handelsheffingen, terrorisme, oorlog en andere conflicten tussen landen.
- Omgevingsfactoren zoals schaarste aan grondstoffen, volksgezondheidcrises, duurzaamheidsfactoren of klimaatverandering.
- Verschuivende externe factoren, zoals technologische ontwikkelingen (waaronder artificial intelligence), veranderingen in compliance (wet- en regelgeving en financiële verslaglegging), ontwikkelingen op de arbeidsmarkt, consumentenvraag en reputatie.

- Financiële uitdagingen, zoals inflatie of deflatie, rentetarieven, wisselkoersen en heersende marktomstandigheden, zoals recessie of economische expansie.
- Operationele uitdagingen, zoals complexe processen, grote afhankelijkheid van third parties, geografische locatie, culturele uitdagingen, beperkte beschikbaarheid van personeel en ineffectief leiderschap of risicomanagement.
- Problemen in de supply chain, zoals het niet kunnen verkrijgen van grondstoffen, een gebrek aan diverse leveranciers en volatiele grondstofprijzen.
- Interne gebeurtenissen, zoals verloop van medewerkers in kritieke functies en operationele fouten.

Hoewel de aard van de verstorende gebeurtenis kan variëren, moet de organisatie beschikken over een goed gedefinieerde resilience-strategie en geformaliseerde processen om continu te anticiperen op, zich voor te bereiden op, te reageren op en zich aan te passen aan veranderingen. Organizational resilience is een overkoepelende term en de strategie kan verschillende onderdelen bevatten, afhankelijk van de organisatie, zoals business continuity, disaster recovery, matrices voor kritieke functies, opvolgingsplannen en recoverytests.

Vereisten van de Topical Requirement Organizational resilience omvatten:

- **Governance** - duidelijk gedefinieerde resilience-doelstellingen en strategieën die bijdragen aan het realiseren van de missie en visie van de organisatie.
- **Risicomanagement** - processen voor het identificeren, analyseren, beheersen en monitoren van resilience-dreigingen, inclusief een proces om incidenten die de organizational resilience raken tijdig te escaleren.
- **Beheersing** - door het management vastgestelde, periodiek geëvalueerde beheersprocessen om resilience risico's te adresseren.

Overwegingen

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

Beperkingen in internal auditopdrachten in de publieke sector als gevolg van wetgeving, overheidsstructuren of politieke omgevingen worden erkend als mogelijke belemmeringen voor het adresseren van bepaalde aspecten van deze werkzaamheden. Internal auditors in de publieke sector moeten dergelijke beperkingen in scope documenteren als onderdeel van hun risicobeoordelingsproces en professionele oordeelsvorming toepassen om de aangepaste scope van hun beoordeling duidelijk te definiëren en te communiceren.

Overwegingen voor governance

Om te beoordelen hoe de governanceprocessen worden toegepast op resilience-doelstellingen, kunnen internal auditors bewijs beoordelen van:

A. Een gedocumenteerde resilience-strategie die is opgesteld door het management, goedgekeurd door het bestuur en waarop door het bestuur toezicht wordt gehouden. Deze wordt formeel gecommuniceerd aan al het personeel en sluit nauw aan op en ondersteunt de missie, visie, cultuur en risicomanagementaanpak van de organisatie. De doelstellingen van het resilience strategisch plan zijn goedgekeurd door het bestuur, zijn afgestemd op de algehele aanpak van risicomanagement van de organisatie en worden periodiek getest en beoordeeld. Het plan kan operationele, technologische en financiële elementen bevatten, zoals:

   - Operationeel – resilience coördinatie binnen de gehele organisatie; resilience risicobeoordelingsprocessen; business continuity-planning inclusief periodieke toetsing en rapportage; crisismanagement; aanpassingsvermogen van het personeelsbestand (zoals capaciteit voor opschaling op afstand, minimale bezetting op locatie en cross-training voor kritieke functies); opvolgingsplanning voor cruciale posities; resilience van de supply chain; het vaststellen van key performance indicators (KPI's); en training voor bestuursleden om bewustwording te waarborgen.
   - Technologisch – vereisten voor de IT-infrastructuur; identificatie van kritieke gegevens (dataclassificatie); back-ups van gegevens; cybersecurity hardening en threat monitoring; onderhoud van kritieke technologische middelen (IT-assets); en

gedefinieerde recovery point objectives (RPO) en recovery times objectives (RTO) voor kritieke gegevens (gevalideerd door restore testing).

- Financieel – begrote middelen toegewezen aan resilience; kasreserves om de activiteiten tijdens een verstoring voort te zetten; financiële rapportageprocessen om transacties die verband houden met verstoringen nauwkeurig vast te leggen; verzekeringspolissen om risico's van verstoringsen te beperken; en beschikbaarheid van kredietfaciliteiten voor noodleningen.

B. Periodieke (bijvoorbeeld per maand of kwartaal) updates over resilience worden aan het bestuur verstrekt door de persoon of het team dat verantwoordelijk is voor organizational resilience. Deze updates kunnen gedefinieerde triggers voor risicotolerantie, KPI's of andere informatie bevatten om observaties of trends zichtbaar te maken. Updates geven inzicht in de status van de doelstellingen van de resilience-strategie , inclusief strategisch toezicht, monitoring en langetermijnplanning. De rapportage kan resultaten bevatten van monitoring over:

- Het bereiken van strategische resilience-doelstellingen en uitdagingen die het bereiken daarvan kunnen belemmeren.
- De budgettaire behoeften ter ondersteuning van de resilience-doelen en doelstellingen, zoals de behoefte aan technologische middelen.
- De status van resilience-risico's, inclusief significante veranderingen in de risico-omgeving die van invloed kunnen zijn op vastgestelde risicotolerantieniveaus.
- De effectiviteit van de interne beheersmaatregelen op het gebied van resilience, inclusief de voortgang van herstelmaatregelen.
- KPI's om het succes van resilience te meten.
- Personele middelen die nodig zijn om medewerkers met verantwoordelijkheden op het gebied van resilience aan te nemen, op te leiden en te ontwikkelen.

C. Beleid, procedures en andere relevante documentatie die worden gebruikt voor het beheren van operationele, technologische en financiële resilience processen, waaronder:

- Hoe kritieke resilience-processen worden geïdentificeerd en periodiek worden geanalyseerd om te bepalen of deze nog steeds een accuraat beeld geven van de meest vitale processen.
- Beleid wordt ten minste jaarlijks herzien en bijgewerkt (of vaker bij een hoger risiconiveau), en vaker indien nodig of op basis van opkomende resilience-risico's of lessen die zijn getrokken uit tests of daadwerkelijke verstorende gebeurtenissen.
- Een beoordelingsproces voor de toereikendheid van beleid en procedures ter ondersteuning van resilience-activiteiten.
- Of resilience-processen en interne beheersmaatregelen worden versterkt met behulp van breed toegepaste frameworks voor gerelateerde processen, zoals risicomanagement, informatietechnologie of governance. Voorbeelden die nuttig kunnen zijn om in overweging te nemen zijn frameworks van organisaties zoals NIST, COSO of ISO, in het bijzonder de ISO 22300-serie (22316 of 22336).

D. Een vastgestelde en gedocumenteerde incident command-structuur die leiderschapsrollen en verantwoordelijkheden beschrijft met betrekking tot het realiseren van de resilience-doelstellingen. Bewijs van vastgestelde besluitvormingsstructuren, zoals medewerkers die verantwoordelijk zijn voor resilience gerelateerde beslissingen tijdens verstoringen, en de goedkeuringen die vereist zijn voor operationele beslissingen, zoals het beschikbaar stellen van middelen of de mogelijkheid om rechtsgeldig contracten af te sluiten met een third party ter ondersteuning van de organisatie tijdens verstoringen. Andere overwegingen zijn gedocumenteerde escalatiepaden en tijdelijke beslissingsbevoegdheden tijdens verstoringen, waaronder financiële mandaten en drempelwaarden voor het contracteren van third parties.

E. Een vastgesteld proces om periodiek (bijvoorbeeld jaarlijks of halfjaarlijks) de kennis, vaardigheden en competenties te beoordelen van personen die verantwoordelijk zijn voor het uitvoeren en beheren van resilience-processen. Het proces kan onder meer het identificeren van trainingsprogramma's omvatten, zoals fysieke of virtuele trainingen, conferenties, on-demand cursussen of professionele certificeringen. Bewijs van opvolgingsplanning om kritieke rollen op het gebied van resilience te identificeren, inclusief het testen van scenario's om activiteiten te identificeren die slechts door één persoon of een beperkt aantal personen kunnen worden uitgevoerd. De vereiste kwalificaties voor vervangers zijn vastgelegd.

F. Een vastgesteld proces om relevante interne en externe stakeholders te identificeren en te betrekken bij het idenfiticeren van en reageren op bestaande kwetsbaarheden en opkomende dreigingen die van invloed kunnen zijn op het realiseren van de resilience-doelstellingen. Bewijs van deelname van stakeholders aan besprekingen over resilience kwetsbaarheden. Bewijs kan bestaan uit e-mails, notulen van vergaderingen of rapportages, inclusief aanwijzingen voor het gebruik van organisatiebrede metrics om de effectiviteit van resilience te meten en te monitoren.

Overwegingen voor risicomanagement

Om te beoordelen hoe risicomanagementprocessen worden toegepast op de resilience-doelstellingen, kunnen internal auditors bewijs beoordelen dat:

A. De risicobeoordelings- en risicomanagementprocessen van de organisatie het identificeren van resilience-risico's omvatten en continu worden uitgevoerd en gedocumenteerd, waarbij de resultaten binnen de organisatie worden gecommuniceerd. Het risicomanagementproces voor resilience omvat het evalueren van key processen, zoals operations, enterprise risk management, IT, supply chain/procurement, facilitair management, human resources, financiën, juridische zaken, compliance, wet- en regelgeving, public relations, kritieke leveranciers, reputatie en opkomende risico's. Naast het identificeren van resilience-risico's omvatten de processen ook het beoordelen van de wijze waarop dreigingen en kwetsbaarheden die de bedrijfsactiviteiten kunnen verstoren, worden:

- Initieel geïdentificeerd en gerapporteerd.
- Geanalyseerd om het risico van het realiseren van de organisatiedoelstellingen te evalueren.

- Gemitigeerd, inclusief actieplannen om het risico tot een aanvaardbaar niveau terug te brengen.
- Gemonitord, inclusief een plan voor doorlopende rapportage totdat dreigingen volledig zijn opgelost.

Aanvullend bewijs kan bestaan uit:

- Documentatie in de vorm van rapporten, e-mails of notulen van vergaderingen welke onderdelen van de organisatie deelnemen. Risicofactoren zoals impact, waarschijnlijkheid, snelheid waarmee risico's zich materialiseren en andere aspecten kunnen worden meegenomen.
- Sterk gecorreleerde of onderling afhankelijke risicofactoren worden geanalyseerd om de cumulatieve impact van verschillende risico's waaraan de organisatie is blootgesteld te beoordelen.
- De risicobeoordeling omvat de evaluatie van de beschermingslagen voor kritieke assets en voorzieningen om single points of failure te voorkomen.
- De risicobeoordeling wordt geactualiseerd door de lessen die zijn getrokken uit daadwerkelijke crises, verstoringen en de resultaten van testen en scenario's op te nemen.
- De organisatie prioriteert de gebieden die het hoogste risico vormen op basis van de potentiële impact en waarschijnlijkheid uit de business impact analysis.

B. De organisatie heeft accountability en responsibility voor het monitoren van en rapporteren over resilience-risico's toegewezen aan een individu of team en beoordeelt deze periodiek. Het individu of het team bestaat uit gekwalificeerde personen met ervaring in het managen van organizational resilience, idealiter binnen de sector van de organisatie (zoals de gezondheidszorg, financiële dienstverlening of de publieke sector). Het individu of het team neemt deel aan periodieke trainingen om op de hoogte te blijven van opkomende trends op het gebied van resilience-risico's.

C. De organisatie heeft een proces ingesteld om resilience-risico's (opkomende of eerder geïdentificeerde) te monitoren en risico's die een niveau bereiken dat als onaanvaardbaar wordt beschouwd snel te escaleren, zoals gedefinieerd door de richtlijnen voor risicomanagement en risicotolerantie van de organisatie of door toepasselijke wet- en regelgeving. Er wordt rekening gehouden met de impact van resilience-risico's, inclusief financiële en niet-financiële factoren. Voorbeelden van financiële maatstaven zijn omzet, kosten, winstgevendheid, kasstroom, schulden, aandelenkoers en totale ondernemingswaarde. Voorbeelden van niet-financiële maatstaven zijn merkreputatie, klanttevredenheid, milieu-impact en personeelsverloop. Het proces omvat:

- Initiële identificatie van risico's en tijdige escalatie.
- Analyse om het risico te evalueren en te beoordelen hoe dit het realiseren van de doelstellingen van de organisatie zou kunnen verhinderen.
- Voorgestelde en overeengekomen risicomitigerende actieplannen, inclusief hoe het risico tijdig tot een aanvaardbaar niveau kan worden teruggebracht. Actieplannen

zijn gebaseerd op de overkoepelende enterprise riskmanagement strategie. Het voorstel moet de benodigde risicomitigerende middelen bevatten, zoals financiële middelen, personeelsuren en aanvullende technologie en software die nodig zijn om de capaciteiten te versterken.

- Voortdurende risicomonitroing en rapportage over key risk indicators totdat dreigingen volledig zijn opgelost.

D. De organisatie heeft een proces geïmplementeerd om te reageren op en te herstellen van crises, verstoringen, noodsituaties of andere incidenten. Het proces wordt periodiek volledig getest, bijvoorbeeld per kwartaal of jaarlijks, en kan daarnaast vaker gedeeltelijk getest worden, bijvoorbeeld maandelijks. Kritieke diensten moeten mogelijk vaker worden getest. Het incident response en recovery proces kan bestaan uit:

- Detectie – voortdurende monitroing op cybergebeurtenissen. Dit kan het gebruik omvatten van een intrusion detection system, threat intelligence of security information en event management (SIEM). De SIEM kan artificial intelligence gebruiken om het proces te versterken. In het geval van natuurrampen of uitval van faciliteiten heeft de organisatie een communicatienetwerk ingericht (zoals waarschuwingsprotocollen of meldingen) om tijdig op de hoogte te zijn en informatie uitwisseling. Voor alle gebeurtenissen heeft de organisatie een proces gedefinieerd om toepassielijke hulpdiensten en bevoegde autoriteiten te informeren. Gebeurtenissen moeten worden geprioriteerd op basis van hun impact en urgentie.
- Response en Containment – de incident response-aanpak omvat scenario-analyses en periodieke stresstests voor een reeks verstorende gebeurtenissen. Om bijvoorbeeld verdere schade tijdens cybergebeurtenissen te voorkomen, heeft de organisatie een proces geïmplementeerd om gecompromitteerde assets te isoleren, zoals het omleiden van netwerkverkeer of het beperken van gebruikerstoegang tijdens een gebeurtenis. Voor fysieke gebeurtenissen heeft de organisatie een proces geïmplementeerd om ontwrichtende gebeurtenissen fysiek te isoleren om de impact te beperken, inclusief het verplaatsen van medewerkers naar een alternatieve locatie.
- Recovery – voor cyber- of IT-gerelateerde gebeurtenissen heeft de organisatie procedures opgesteld om prioriteit te geven aan het herstel van kritieke assets die nodig zijn om de activiteiten te hervatten (zoals het herstellen van gegevens uit back-ups of het weer online brengen van servers). Andere niet-IT middelen die nodig zijn om de activiteiten te hervatten moeten eveneens prioriteit krijgen bij herstel. Dit kan het plannen van een geleidelijke terugkeer van medewerkers in kritieke functies of kernfuncties omvatten.
- Post-incident analyse – de organisatie analyseert de gebeurtenissen om vast te stellen:
  - Root causes van verstorende gebeurtenissen.
  - Doeltreffendheid van ondernomen acties.
  - Verbeteringen die nodig zijn om resilience-processen te versterken, zoals het actualiseren van beleid, procedures, risico's of strategie.

Het testen van het response- en recoveryproces op degelijkheid en effectiviteit, door middel van desktop oefeningen, simulaties en drills met betrekking tot kritieke diensten/functies en hun afhankelijkheden, kan worden afgestemd op de risicotolerantieniveaus van de organisatie. Deze gebeurtenissen kunnen het gevolg zijn van interne of externe incidenten. De resultaten van deze oefeningen kunnen worden beoordeeld door het bestuur en het senior management, waarbij verbeteracties worden gevolgd en periodiek worden gerapporteerd. Aanbevelingen moeten uitvoerbaar zijn, met een duidelijke eigenaarschap en tijdslijnen.

Overwegingen voor beheersprocessen

Om te beoordelen hoe beheersprocessen worden toegepast op de doelstellingen voor organizational resilience, kunnen internal auditors bewijs beoordelen dat:

A. Er is een proces ingericht om kritieke third-party leveranciers (leveranciers en dienstverleners) en minimale voorraadniveaus die nodig zijn om vitale activiteiten voort te zetten te identificeren en te beoordelen. De beoordeling kan rekening houden met organizational resilience en business continuity van third parties en risico-scores voor elke leverancier bevatten. Naast het beoordelen van leveranciers voordat een formele overeenkomst wordt aangegaan, kan de organisatie leveranciers periodiek opnieuw beoordelen om risk ratings doorlopend te evalueren. De organisatie houdt een lijst bij van potentiële vervangende dienstverleners voor het geval dat een relatie wordt beëindigd.

B. Het management heeft een dataclassificatie uitgevoerd, waarbij met name kritieke gegevens zijn geïdentificeerd die nodig zijn om te herstellen van verstorende gebeurtenissen en activiteiten voort te zetten. De organisatie heeft effectieve interne beheersmaatregelen geïmplementeerd om kritieke gegevens te beschermen, waaronder het beperken van de toegang tot geautoriseerd personeel en het waarborgen dat kritieke gegevens worden geback-upt en tijdig kunnen worden hersteld.

C. Het management heeft kritieke IT-beheersmaatregelen en continuous monitoringprocessen ingesteld om informatiebeveiligingrisico's (inclusief cybergerelateerde risico's) te mitigeren en ervoor te zorgen dat gevoelige gegevens worden beschermd tijdens verstorende gebeurtenissen. Encryptie beschermt gevoelige gegevens. Continuous monitoring en real-time threat intelligince voorzien het management van waarschuwingen en problemen worden tijdig opgelost. Er kan gebruik worden gemaakt van algemeen aanvaarde frameworks van organisaties zoals NIST, COSO en ISO.

D. De organisatie heeft kritieke IT-assets geïnventariseerd, waaronder hardware, software en diensten die nodig zijn om activiteiten te ondersteunen tijdens crises, verstoringen en noodsituaties. IT-assets die moeilijker snel te verwerven zijn, worden geïdentificeerd als assets met hoge prioriteit.

E. Er zijn een business continuity plan en een disaster recovery plan opgesteld waarin personeel voor recoveryteams wordt geïdentificeerd op basis van de business impact analyse. De plannen worden periodiek getest, bijvoorbeeld elk kwartaal of elk jaar, door middel van desktop oefeningen of stresstests, waarbij verstoringen echte noodsituaties simuleren en communicatieprotocollen met zowel interne als externe belanghebbenden

worden getest. De resultaten van het testen, inclusief verbetermogelijkheden, worden gerapporteerd aan het bestuur en het senior management.

F. Er wordt een proces ingericht om de werkomgeving aan te passen tijdens verstorende gebeurtenissen. Aanpassingen kunnen bestaan uit het gebruik van alternatieve werklocaties, zoals thuiswerken of het tijdig en efficiënt opzetten van een tijdelijk kantoor. De organisatie kan gebruik maken van hybride of remote werkopties ter vervanging van werk op locatie. Andere aspecten kunnen protocollen omvatten voor het tijdig en efficiënt mobiliseren en heralloceren van middelen, waaronder IT en human resources.

G. Er is een proces ingericht om voortdurend opkomende dreigingen en kwetsbaarheden met betrekking tot organizational resilience te monitoren en hierover te rapporteren, en om mogelijkheden ter verbetering van processen voor organizational resilience te identificeren, te prioriteren en te implementeren. Monitoringactiviteiten kunnen bestaan uit key risk indicators (KRI's), risicodashboards en verkenningen van de risicohorizon. De organisatie kan updates geven aan alle medewerkers over opkomende dreigingen om het bewustwording te vergroten, inclusief risicomitigerende maatregelen of beheersmaatregelen. Alle klokkenluidersactiviteiten worden geregistreerd, geanalyseerd, tijdig afgehandeld en gecommuniceerd naar senior management. Voortdurende monitoring kan nodig zijn om problemen op te lossen, waarvoor aanvullende rapportage vereist kan zijn.

H. Er is een proces ingericht om personeel op te leiden en te trainen in beleid en de procedures voor organizational resilience die gevolgd moeten worden bij crises, verstoringen en noodsituaties. Het proces omvat trainingsoefeningen waarin ontwrichtende scenario's worden gesimuleerd. Trainingen worden periodiek gegeven, bijvoorbeeld per kwartaal of jaarlijks. Kritieke services moeten mogelijk vaker worden getest.

I. Er is een proces ingericht om ervoor te zorgen dat de benodige operationele, personele, technologische en financiële middelen worden gebudgetteerd en beschikbaar zijn tijdens crises, verstoringen en noodsituaties. Het management beoordeelt periodiek, bijvoorbeeld per kwartaal of jaarlijks, of de middelen toereikend zijn op basis van de waargenomen risiconiveaus en rapporteert behoeften aan het bestuur. Kritieke services moeten mogelijk vaker worden getest. De analyse omvat een beoordeling van de liquiditeit, verzekeringsdekking en arrangements voor noodfinanciering. De behoefte aan financiële middelen wordt bepaald op basis van factoren zoals de omvang, complexiteit, sector en het risicoprofiel van de organisatie. Het proces kan voorzien in voorafgaande goedkeuring van financiering.

J. Er is een proces ingericht voor het evalueren van crises, verstoringen en noodsituaties nadat deze hebben plaatsgevonden en voor het analyseren van post-incident reviews door middel van een lessons-learnedproces. De beoordelingen moeten worden gedocumenteerd in formele rapportages en de geleerde lessen moeten worden geïntegreerd in toekomstige resilience planning.

Bijlage A. Voorbeelden van praktische toepassingen

In de volgende scenario's wordt beschreven wanneer de Topical Requirement Organizational resilience van toepassing is. Daarnaast bevat het IIA "Topical Requirements Application Guidance" praktisch advies over het omgaan met verplichte vereisten, het aanpakken van beperkingen en het identificeren van kritieke risicodrempels.

Scenario 1: Organizational resilience is geïdentificeerd voor een internal auditopdracht die is opgenomen in het internal auditplan.

Wanneer de internal auditfunctie haar risicogebaseerde planningsproces voltooit en een of meer opdrachten met betrekking tot organizational resilience opneemt in haar internal auditplan, moet de Topical Requirement worden toegepast 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.

Organizational resilience is een breed onderwerp en niet elke vereiste in de Topical Requirements is van toepassing op elke opdracht. Wanneer internal auditors professionele oordeelsvorming toepassen en bepalen dat een of meer vereisten van de Topical Requirement Organizational resilience niet van toepassing zijn en daarom van een opdracht moeten worden uitgesloten, moeten internal auditors de onderbouwing voor het uitsluiten van deze vereisten documenteren en bewaren. De onderbouwing voor het uitsluiten van bepaalde vereisten kan bijvoorbeeld zijn dat de internal auditfunctie verschillende opdrachten op het gebied van organizational resilience roulerend uitvoert of heeft vastgesteld dat het belang van het risico binnen de opdracht gering is.

Scenario 2: Risico's voor organizational resilience worden geïdentificeerd tijdens een internal auditopdracht die niet is gericht op organizational resilience.

Internal auditors kunnen resilience-risico's identificeren tijdens het beoordelen van een proces dat niet direct verband houdt met resilience. Internal auditors kunnen bijvoorbeeld de HR-processen (zoals het aannemen en behouden van personeel) beoordelen in een opdracht die niet gericht is op de organizational resilience en bij de planning van de opdracht risico's voor resilience niet als onderdeel van de scope identificeren. Na het uitvoeren van de initiële walkthrough stellen internal auditors echter vast dat deze risico's binnen de scope vallen; ze identificeren bijvoorbeeld risico's met betrekking tot opvolgingsplanning die verband houden met de manier waarop de organisatie personeel in dienst houdt (Standaard 13.2 Risicobeoordeling in de opdracht).

Zodra de relevante risico's zijn geïdentificeerd, moeten internal auditors de Topical Requirement Organizational resilience beoordelen en bepalen welke eisen van toepassing zijn. In dit voorbeeld

richten ze zich misschien alleen op vereiste E binnen Governance en sluiten ze de andere vereisten met betrekking tot risicomanagement en beheersing uit. Zij moeten in de werkdocumenten van de opdracht de onderbouwing voor het uitsluiten van de overige vereisten van de Topical Requirement Organizational resilience documenteren en de documentatie bewaren.

Scenario 3: Er wordt gevraagd om een opdracht op het gebied van organizational resilience die oorspronkelijk niet in het internal auditplan was opgenomen.

Stakeholders zoals het bestuur, het management of een toezichthouder kunnen internal auditors verzoeken beoordelingen op het gebied van resilience uit te voeren buiten het oorspronkelijke auditplan. Wanneer organisaties bijvoorbeeld het doelwit zijn van een cyberaanval, kan het bestuur verzoeken een internal auditopdracht uit te voeren gericht op het beoordelen van beheersmaatregelen voor resilience, om te evalueren in hoeverre de organisatie is voorbereid op herstel na een cyberaanval. De Topical Requirement is van toepassing, de vereisten moeten worden beoordeeld en eventuele uitsluitingen moeten worden gedocumenteerd (Standaard 9.4 Internal auditplan).

Bijlage B. Voorbeelden van praktische toepassingen van auditopdrachten

Scenario 1: Het onderwerp is opgenomen als opdracht in het internal auditplan.

Publieke organisatie verantwoordelijk voor een centrale groothandelsmarkt

Tijdens het jaarlijkse risicogebaseerde planningsproces identificeert de internal auditfunctie de continuïteit van essentiële marktactiviteiten als een hoog risicogebied vanwege de blootstelling aan logistieke verstoringen, gebeurtenissen op het gebied van de volksgezondheid en afhankelijkheden van kritieke infrastructuur. Op basis van deze beoordeling stellen internal auditors vast dat de Topical Requirement Organizational resilience van toepassing is op de geplande opdracht.

Om de governance te evalueren, beoordelen internal auditors de notulen van het bestuur, strategische plannen en budgetdocumentatie om vast te stellen of resilience gerelateerde doelstellingen formeel zijn vastgelegd en of hierop toezicht wordt gehouden. Ze evalueren of het management periodiek rapporteert aan het bestuursorgaan over kritieke kwetsbaarheden, zoals afhankelijkheden in transport, infrastructuurbeperkingen en gezondheidsgerelateerde risico's. Wanneer er geen afzonderlijke resilience-strategiedocument bestaat, beoordelen internal auditors of elementen van resilience consistent zijn verankerd in de operationele en strategische documentatie.

Vanuit het perspectief van risicomanagement onderzoeken internal auditors het risicoregister van de organisatie en interviewen ze het operationele management om vast te stellen of risico's die de continuïteit van de levering kunnen beïnvloeden, zijn geïdentificeerd, beoordeeld en toegewezen aan eindverantwoordelijke functionarissen. Ze beoordelen of er tijdens eerdere gebeurtenissen escalatiemechanismen zijn geactiveerd, zoals tijdelijke sluitingen of toegangsbeperkingen, en stellen vast of de responsemaatregelen in lijn waren met de vastgestelde risicotolerantie-parameters.

De controleprocedures omvatten het beoordelen van regelingen voor operationele continuïteit, het inspecteren van bewijs van periodieke testen, oefeningen en het onderzoeken van documentatie over coördinatie met overheidsinstanties tijdens verstorende gebeurtenissen. Internal auditors beoordelen ook post-incident rapportages om vast te stellen of de geleerde lessen zijn verwerkt in geactualiseerde processen. Wanneer bepaalde vereisten van de Topical Requirement niet van toepassing zijn vanwege wettelijke of structurele beperkingen, documenteren internal auditors de onderbouwing voor uitsluiting in overeenstemming met de Standaarden.

Scenario 2: Het onderwerp wordt geïdentificeerd tijdens de uitvoering van een opdracht.

Wereldwijd opererend professioneel dienstverleningsbedrijf

Tijdens een opdracht gericht op governance en enterprise risk management identificeren internal auditors kwetsbaarheden met betrekking tot gedecentraliseerde besluitvorming, afhankelijkheid van key local leadership en blootstelling aan wet- en regelgeving in verschillende rechtsgebieden. Op basis van deze observaties stellen internal auditors vast dat bepaalde elementen van de Topical Requirement Organizational resilience van toepassing zijn op de opdracht.

Om de governance te beoordelen, beoordelen internal auditors het wereldwijde beleid, de rapportagematerialen voor het bestuur en de crisismanagementprotocollen om vast te stellen of de organisatie heeft gedefinieerd hoe activiteiten worden voortgezet bij wijzigingen in wet- en regelgeving, een groot verloop van personeel in kritieke functies of reputatie-incidenten in één rechtsgebied die een bredere impact kunnen hebben. Ze evalueren of het bestuursorgaan geconsolideerde rapportage ontvangt over kritieke risico's in verschillende rechtsgebieden en of de accountability voor toezicht op resilience duidelijk is belegd.

Vanuit het perspectief van risicomanagement onderzoeken internal auditors het enterprise risk management framework om vast te stellen of risico's met betrekking tot de afhankelijkheid van key personeel, grensoverschrijdende compliance met wet- en regelgeving en reputatierisico's zijn gekoppeld aan de strategische doelstellingen van de onderneming. Ze voeren steekproeven uit op geselecteerde incidenten om vast te stellen of lokale gebeurtenissen op passende wijze zijn geëscaleerd naar global leadership en of responsbeslissingen zijn genomen binnen de vastgestelde bevoegdheidsniveaus.

Controlegerelateerde procedures omvatten het beoordelen van business continuity-regelingen in verschillende rechtsgebieden, het onderzoeken of kritieke functies voldoende zijn afgedekt en of er reservepersoneel of adequaat ingerichte opvolgingsprocessen aanwezig zijn om continuïteitsrisico's het hoofd te bieden, en het beoordelen van de toereikendheid van de technologie-infrastructuur ter ondersteuning van gecoördineerde remote operations. Internal auditors beoordelen ook documentatie van post-event analyses om vast te stellen dat corrigerende maatregelen zijn geïmplementeerd. Wanneer alleen bepaalde vereisten van de Topical Requirement van toepassing zijn, documenteren internal auditors de onderbouwing voor de opname of uitsluiting.

Scenario 3: Het onderwerp vormt het onderwerp van een gevraagde opdracht.

Organisatie verantwoordelijk voor kritieke nationale infrastructuur

Een verwoestende orkaan in een naburig rechtsgebied leidt ertoe dat een bestuurslid de internal auditfunctie verzoekt een opdracht op het gebied van organizational resilience toe te voegen aan het auditplan om de blootstelling van de organisatie aan operationele verstoringen, afhankelijkheid van gespecialiseerde contractors, wettelijke verplichtingen en ernstige milieu-incidenten te beoordelen. In dit geval wordt de Topical Requirement Organizational resilience integraal toegepast.

Om de governance te beoordelen, beoordelen internal auditors het door het bestuur goedgekeurde strategische plan en de bijbehorende documentatie om vast te stellen dat de continuïteit van kritieke diensten formeel is verankerd in de langetermijnplanning. Ze

onderzoeken de rapportages aan het bestuur om vast te stellen of key indicators met betrekking tot operationele beschikbaarheid, onderhoud van kritieke assets en financiële contingency planning, waaronder verzekeringsdekking en financiële reserves, periodiek worden beoordeeld.

Vanuit risicomanagementperspectief evalueren internal auditors hoe risico's met betrekking tot verstoring van de infrastructuur, concentratie van aannemers, compliance met wet- en regelgeving en blootstelling aan milieurisico's worden geïdentificeerd, beoordeeld en gemonitord binnen het enterprise risk management-framework. Ze beoordelen of de verantwoordelijkheid voor het monitoren van deze risico's duidelijk is belegd en of escalatieprotocollen zijn gevolgd tijdens eerdere verstoringen van dienstverlening, inclusief coördinatie met toezichthouders en crisisbevoegde autoriteiten.

Testen van beheersmaatregelen omvatten het verifiëren van het bestaan van business continuity- en disaster recovery-plannen en het periodiek testen daarvan, het beoordelen van inventarissen van kritieke assets, het onderzoeken van contractuele afspraken met alternatieve leveranciers en het beoordelen van documentatie van post-incident analyses om vast te stellen of corrigerende maatregelen zijn gevolgd en geïmplementeerd. Wanneer bepaalde vereisten niet van toepassing zijn vanwege wettelijke of regelgevende bepalingen, documenteren internal auditors de onderbouwing in overeenstemming met de Standaarden.

Bijlage C. Vergelijking met Frameworks

De organisatie kan zelf al werkzaamheden hebben ingericht, waarbij gebruik wordt gemaakt van frameworks zoals die van ISO. Internal auditors hebben mogelijk al auditprogramma's en testprocedures ontwikkeld op basis van deze frameworks. Internal auditors moeten hun voorgenomen toetsing van beheersmaatregelen voor organizational resilience afstemmen op de Topical Requirement om een adequate dekking te waarborgen (Standaard 13.4 Evaluatiecriteria). De onderstaande tabel geeft een mapping weer van de Topical Requirement Organizational resilience naar het ISO 22336 Framework. Aanvullende verwijzingen naar frameworks zijn opgenomen bn Bijlage E.

Vereisten voor Governance	ISO 22336 Framework
A. Een formele organisatiestrategie die gericht is op resilience wordt vastgesteld door het management, waarbij het bestuur toezicht houdt, en omvat de operationele, technologische en financiële elementen die nodig zijn om veranderingen te beheren en de activiteiten voort te zetten. De resilience-doelstellingen sluiten aan bij de algehele benadering van risicomanagement van de organisatie.	4.1; 6.1; 6.2; 7.1; 8.4; 8.5; 9.1; 9.5
B. Updates over het behalen van de resilience-doelstellingen worden periodiek ter beoordeling aan het bestuur voorgelegd. Dit zorgt ervoor dat resilience is verankerd in strategisch toezicht, langetermijnplanningsprocessen, opvolgingsplanning en de cultuur van de organisatie, inclusief in de resource- en budgettaire overwegingen die nodig zijn ter ondersteuning van kritieke bedrijfsactiviteiten.	6.4; 8.6; 10.2
C. Beleid en procedures voor kritieke operationele, technologische en financiële processen worden opgesteld en periodiek beoordeeld, getest en waar nodig geactualiseerd om de beheersomgeving te versterken.	4.2; 6.3; 8.3; 8.4; 9.4
D. Er is een incident command-structuur ingericht en gebruikt om toezicht te houden op en ondersteuning te bieden aan de resilience-doelstellingen van de organisatie. Het omvat besluitvormingshiërarchieën, communicatie- en escalatieprotocollen en rollen en verantwoordelijkheden op het gebied van leiderschap en operations.	5.4
E. Er is een proces ingericht om periodiek de competenties te valideren die nodig zijn voor effectieve organisatorische resilience en om de competenties van de personen die kritieke rollen vervullen binnen het resilience-proces opnieuw te beoordelen.	9.6
F. Er wordt een proces opgezet om ervoor te zorgen dat alle relevante interne en externe stakeholders worden geïdentificeerd, geprioriteerd en betrokken bij het opzetten van informatie- en rapportagestructuren ter ondersteunen van het realiseren van resilience-doelstellingen van de organisatie. Stakeholders kunnen zijn: senior management, operations, risicomanagement, IT, supply chain/procurement, facilitair management, human resources, financiën, juridische zaken, assurance providers (inclusief internal audit), compliance, public relations, kritieke leveranciers, klanten, toezichthouders en anderen.	9.2; 9.5

Vereisten voor Risicomanagement	ISO 22336 Framework
A. Risico's met betrekking tot de organisatorische resilience van de organisatie worden periodiek geïdentificeerd, beoordeeld en beheerd binnen de gehele organisatie. Resilience-risico's zijn gekoppeld aan de strategische doelstellingen van de organisatie. Het risicomanagementproces voor resilience omvat het evalueren van key processen.	4.4; 5; 7.3; 7.4; 7.5, 7.6, 9.2, 9.3
B. Accountability en responsibility voor het risicomanagement van de organisatorische resilience zijn duidelijk belegd. Een aangewezen persoon of team is belast met het regelmatig monitoren van en rapporteren over het beheer van risico's met betrekking tot organisatorische resilience, inclusief de middelen die nodig zijn voor risicomitigatie en het identificeren van opkomende dreigingen voor organisatorische resilience.	4.3; 8.2; 9.6
C. Er is een proces ingericht om de niveaus van risico's met betrekking tot organisatorische resilience (opkomend of eerder geïdentificeerd) te monitoren en risico's die een als onaanvaardbaar beschouwd niveau bereiken snel te escaleren, zoals gedefinieerd in de vastgestelde richtlijnen voor risicomanagement en risicotolerantie van de organisatie of in toepasselijke wet- en regelgeving. Er wordt rekening gehouden met de impact van risico's met betrekking tot organisatorische resilience.	7.2; 7.6; 10.1
D. Het management heeft een proces geïmplementeerd en test dit periodiek om te reageren op en te herstellen van crises, verstoringen en noodsituaties. Het incident response- en recoveryproces omvat detectie, prioritering, containment, herstel en pst-incident analyse. De incident response-aanpak omvat scenarioanalyses en periodieke stresstests voor een reeks plausibele verstorende gebeurtenissen.	7.2; 7.6; 7.8

Vereisten voor Beheersprocessen	ISO 22336 Framwork
A. Er is een proces ingericht om kritieke third-party providers (leveranciers en dienstverleners) te identificeren en de minimale voorraadniveaus te bepalen die nodig zijn om essentiële activiteiten voort te zetten. Het proces omvat ook het bijhouden van een actuele lijst met alternatieve leveranciers.	7.7
B. Kritieke operationele data zijn geïdentificeerd en geclassificeerd. Dataclassificatie omvat het identificeren van waar de gegevens zich bevinden, wie er toegang toe heeft, hoe toegang wordt verkregen en of er een back-up van is gemaakt en de gegevens hersteld kunnen worden in een noodsituatie.	6.1
C. Kritieke IT-beheersmaatregelen en continuous monitoring zijn ingericht informatiebeveiligingrisico's (inclusief cybergerelateerde risico's) te mitigeren en ervoor te zorgen dat gevoelige gegevens worden beschermd tijdens crises, verstoringen en noodsituaties. De beheersing en continuous monitoring omvatten real-time threat intelligence en het beperken van toegang tot alleen geautoriseerde gebruikers.	7.5

D.	Kritieke IT-assets zijn geïnventariseerd. Assets omvatten hardware, software en diensten die nodig zijn om activiteiten te ondersteunen tijdens crises, verstoringen en noodsituaties.	9.2
E.	Business continuity- en disaster recovery-plannen zijn opgesteld en omvatten gedefinieerde rollen voor toegewezen personeel en recovery-teams. De plannen worden periodiek getest (bijvoorbeeld door middel van "desktop exercitie") en de resultaten van het testen, inclusief verbetermogelijkheden, worden gerapporteerd aan het bestuur en het senior management.	8.6; 9.6; 10.3
F.	Er is een proces ingericht om de werkomgeving aan te passen tijdens crises, verstoringen en noodsituaties.	9.3
G.	Er is een proces ingericht om voortdurend opkomende dreigingen en kwetsbaarheden die de organisatorische resilience kunnen beïnvloeden te monitoren en hierover te rapporteren. Het proces wordt gebruikt om mogelijkheden te identificeren, te prioriteren en te implementeren om de resilience van de organisatie en haar operations te verbeteren, waaronder systemen voor klokkenluiden of het verzamelen van risk intelligence.	7.6
H.	Er is een proces ingericht om personeel op te leiden en te trainen met betrekking tot organisatorische resilience, zodat ze bekend zijn met het beleid, de procedures en de te nemen acties bij crises, verstoringen en noodsituaties. Het proces omvat trainingsoefeningen waarin verstorende scenario's worden gesimuleerd.	10.2; 10.3
I.	Er is een proces ingericht om ervoor te zorgen dat de benodigde operationele, personele, technologische en financiële middelen worden gebudgetteerd en beschikbaar zijn tijdens crises, verstoringen en noodsituaties. Financiële middelen die nodig zijn ter ondersteuning van organisatorische resilience worden periodiek geanalyseerd en gerapporteerd aan het bestuur.	6.4; 7.6; 9.6
J.	Er is een proces ingericht voor het evalueren van crises, verstoringen en noodsituaties nadat ze zich hebben voorgedaan en voor het analyseren van post-incident reviews door middel van een lessons-learnedproces, inclusief het integreren van de getrokken lessen in toekomstige planning voor organisatorische resilience.	10.2, 10.3

Bijlage D. Optioneel hulpmiddel voor documentatie

Van internal auditors wordt verwacht dat zij professionele oordeelsvorming toepassen bij het bepalen van de Topical requirements op basis van de risicobeoordeling en dat zij uitsluitingen 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 kan het zijn dat niet alle vereisten van toepassing zijn. Dit afdrukbare formulier biedt een mogelijkheid voor het documenteren van conformiteit met de Topical Requirement Organizational resilience, maar het gebruik ervan is niet verplicht.

Organisatorische resilience - Governance

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
A. Een formele organisatiestrategie gericht op organisatorische resilience is vastgesteld door het management, waarbij het bestuur toezicht houdt, en omvat de operationele, technologische en financiële elementen die nodig zijn om veranderingen te beheersen en de activiteiten voort te zetten. De resilience-doelstellingen sluiten aan bij de algehele benadering van risicomanagement van de organisatie.		
B. Updates over het behalen van de resilience-doelstellingen worden periodiek ter beoordeling aan het bestuur voorgelegd. Dit zorgt ervoor dat reillence is ingebed in strategisch toezicht, langetermijnplanningsprocessen, opvolgingsplanning en in de cultuur van de organisatie, inclusief in de resource- en budgetoverwegingen die nodig zijn om kritieke bedrijfsactiviteiten te ondersteunen.		
C. Beleid en procedures voor kritieke operationele, technologische en		

	financiële processen zijn opgesteld en periodiek beoordeeld, getest en waar nodig geactualiseerd om de beheersomgeving te versterken.		
D.	Er is een incident command-structuur ingericht en gebruikt om toezicht te houden op en ondersteuning te bieden aan resilience doelstellingen van de organisatie. Het omvat besluitvormingshiërarchieën, communicatie- en escalatieprotocollen en verantwoordelijkheden op het gebied van leiderschap en operations.		
E.	Er is een proces ingericht om periodiek de competenties te valideren die nodig zijn voor een succesvol resilience proces en om de competenties van de personen die kritieke rollen vervullen binnen resilience-processen opnieuw te beoordelen.		
F.	Er is een proces ingericht om ervoor te zorgen dat alle relevante interne en externe stakeholders worden geïdentificeerd, geprioriteerd en betrokken bij het opzetten van informatie- en rapportagestructuren ter ondersteuning van het realiseren van organisatorische resilience-doelstellingen. Stakeholders kunnen zijn: senior management, operations, risicomanagement, IT, supply chain/procurement, facilitair management, human resources, financiën, juridische zaken, assurance providers (inclusief internal audit), compliance, public relations, kritieke leveranciers, klanten, toezichthouders en anderen.		

Organisatorische resilience - Risicomanagement

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
A. Risico's met betrekking tot resilience van de organisatie worden periodiek geïdentificeerd, beoordeeld en beheerd binnen de gehele organisatie. Risico's op het gebied van resilience zijn gekoppeld aan de strategische doelstellingen van de organisatie. Het risicomanagementproces voor resilience omvat het evalueren van key processen		

B.	Accountability en responsibility voor het risicomanagement van de organisatorische resilience zijn duidelijk belegd. Een aangewezen persoon of team is belast met het regelmatig monitoren van en rapporteren over het beheer van organisatorische resilience-risico's, inclusief de middelen die nodig zijn voor risicomitigatie en het identificeren van opkomende dreigingen voor de organisatorische resilience.		
C.	Er is een proces ingericht om de niveaus van risico's met betrekking tot organisatorische resilience (opkomende of eerder geïdentificeerde) te monitoren en die risico's die een als onaanvaardbaar beschouwd niveau bereiken snel te escaleren, zoals gedefinieerd in de richtlijnen voor risicomanagement en risicotolerantie van de organisatie of toepasselijke wet- en regelgeving. De impact van risico's met betrekking tot organisatorische resilience zijn beoordeeld		
D.	Het management heeft een proces geïmplementeerd en test dit periodiek om te reageren op en te herstellen van crises, verstoringen en noodsituaties. Het incident response- en recoveryproces omvat detectie, prioritering, containment, herstel en post-incident analyse. De incident response-aanpak omvat scenarioanalyses en periodieke stresstests gericht op een reeks verstorende gebeurtenissen.		

Organisatorische resilience - Beheersprocessen

Vereiste	Uitgevoerde dekking of reden voor uitsluiting	Documentatie referentie
A. Er is een proces om kritieke third-party leveranciers (leveranciers en dienstverleners) te identificeren en de minimale voorraadniveaus te bepalen die nodig zijn om essentiële activiteiten voort te zetten. Het proces omvat ook het bijhouden van een actuele lijst met alternatieve leveranciers.		
B. Kritieke operationele data zijn geïdentificeerd en geclassificeerd. Dataclassificatie omvat het identificeren waar gegevens zich		

	bevinden, wie toegang nodig heeft, hoe de toegang wordt verkregen, en of gegevens tijdens een noodsituatie zijn ge-back-upt en herstelbaar zijn.		
C.	Kritieke IT-beheersmaatregelen en continuous monitoring zijn ingericht om inform'tiebeveiligingrisico's (inclusief cybergerelateerde risico's) te mitigeren en ervoor te zorgen dat gevoelige gegevens worden beschermd tijdens crises, verstoringen en noodsituaties. De beheersmaatregelen en continuous monitoring omvatten realtime threat intelligence en het beperken van de toegang tot uitsluitend geautoriseerde gebruikers.		
D.	Kritieke IT-assets zijn geïnventariseerd. Assets omvatten de hardware, software en diensten die nodig zijn om activiteiten te ondersteunen tijdens crises, verstoringen en noodsituaties		
E.	Business continuity- en disaster recovery-plannen zijn opgesteld en omvatten gedefinieerde rollen voor toegewezen personeel en recovery-teams. De plannen worden periodiek getest (bijvoorbeeld door middel van een een "desktop exercitie") en de resultaten van het testen, inclusief verbetermogelijkheden, worden gerapporteerd aan het bestuur en het senior management.		
F.	Er is een proces ingericht om de werkomgeving aan te passen tijdens crises, verstoringen en noodsituaties.		
G.	Er is een proces ingericht om voortdurend opkomende dreigingen en kwetsbaarheden die de organisatorische resilience kunnen beïnvloeden te monitoren en hierover te rapporteren. Het proces wordt gebruikt om mogelijkheden te identificeren, te prioriteren en te implementeren of ter verbetering van organisatorische resilience, waaronder systemen voor klokkenluiden en het verzamelen van risk intelligence.		
H.	Er is een proces ingericht om personeel op te leiden en te trainen met betrekking tot organisatorische resilience, zodat ze bekend zijn met het beleid, de procedures die gevolgd moeten worden en de acties die ondernomen moeten worden wanneer crises, verstoringen en noodsituaties zich voordoen. Het proces omvat trainingsoefeningen waarin verstorende scenario's worden gesimuleerd.		

I.	Er is een proces ingericht om ervoor te zorgen dat de benodigde operationele, personele, technologische en financiële middelen worden gebudgetteerd en beschikbaar zijn tijdens crises, verstoringen en noodsituaties. De financiële middelen die nodig zijn ter ondersteuning van organisatorische resilience, worden periodiek geanalyseerd en gerapporteerd aan het bestuur.		
J.	Er is een proces ingericht voor het evalueren van crises, verstoringen en noodsituaties nadat deze zich hebben voorgedaan en voor het analyseren van post-incident reviews door middel van een lessons-learnedproces, inclusief het integreren van de geleerde lessen in toekomstige planning voor organisatorische resilience.		

Bijlage E. Aanvullende framework referenties

Gebied	ISO referentie	Toepassingsgebied/claausules
Governance	ISO 22316:2017	Beleid en strategie; commitment van leiderschap; gedeelde visie; cultuur; communicatie; voortdurende verbetering.
Risicomanagement	ISO 31000:2018	Scope/context/criteria; risicobeoordeling; risicobehandeling; monitoring; communicatie.
Fundamenten voor business continuity en disaster recovery	ISO 22301: 2019; ISO/TS 22317:2021	BCMS-context, leiderschap, planning, operations; BIA-activiteiten en -uitkomsten.
Resilience van de supply chain	ISO/TS 22318:2021	Analyse van leveranciersafhankelijkheden; continuïteitsstrategieën; alternatieve leveranciers; assurancevereisten.
Readiness van informatie- en communicatietechnologie	ISO/IEC 27031	ICT-continuïteit; hersteldoelstellingen; testen en verbeteren; afstemming met het BCMS.

Over het Instituut van Internal Auditors

Het IIA is een internationale beroepsvereniging met wereldwijd meer dan 265.000 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 theiia.org.

Disclaimer

Copyright

April 2026

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