Organizational Resilience

Topical Requirement

The Institute of Internal Auditors

Vertaald door

Instituut van Internal Auditors Nederland

Organizational Resilience Topical Requirement[1]

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

Topical Requirements bieden duidelijke verwachtingen voor internal auditors door een minimum baseline vast te stellen voor het auditen van specifieke risicogebieden. Het risicoprofiel van de organisatie kan vereisen dat internal auditors aanvullende aspecten van het onderwerp in overweging nemen, waaronder lokale regelgeving.

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

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

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

- Het onderwerp van een opdracht in het internal auditplan.
- Geïdentificeerd tijdens het uitvoeren van een opdracht.
- Het onderwerp van een opdrachtverzoek dat niet in het oorspronkelijke internal auditplan stond.

Het is mogelijk dat niet alle individuele vereisten in elke opdracht van toepassing zijn, en aan sommige kan worden voldaan via andere benaderingen. 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 Global Internal Audit Standards,

[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.*

moet de reden hiervoor worden gedocumenteerd en bewaard. Conformiteit wordt geëvalueerd tijdens kwaliteitstoetsingen.

Raadpleeg voor meer informatie de Gebruikershandleiding voor de Topical Requirement Organizational resilience.

Organizational resilience

Organizational resilience wordt door de International Organization for Standardization gedefinieerd als het "vermogen van een organisatie om schokken op te vangen en zich aan te passen in een veranderende omgeving" (ISO 22316:2017). Hoewel deze definitie een duidelijk doel stelt, 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, zijn sommige organisaties beter in staat om veranderingen op te vangen, terwijl andere daar moeite mee hebben of in situaties van onzekerheid andere keuzes maken.

Organizational resilience is een overkoepelende term voor risico's die het vermogen van een organisatie om haar kernactiviteiten en dienstverlening te leveren, het vertrouwen van belanghebbenden te behouden of haar strategische doelstellingen te realiseren, aanzienlijk kunnen verstoren of aantasten. Deze risico's kunnen voortkomen uit plotselinge gebeurtenissen (zoals natuurrampen, cyberaanvallen en geopolitieke conflicten), aanhoudende maatschappelijke, economische of ecologische druk (zoals schaarste aan grondstoffen en crises op het gebied van de volksgezondheid) of veranderingen in de externe context (zoals technologische ontwrichting, wijzigingen in wet- en regelgeving en aantasting van de reputatie).

Deze risico's kunnen ook bestaan uit geleidelijke veranderingen of uit druk die zich geleidelijk opbouwt en na verloop van tijd de stabiliteit en het aanpassingsvermogen van een organisatie ondermijnen. Toenememde risico's zoals deze kunnen gemakkelijk over het hoofd worden gezien. Weerbare organisaties anticiperen op zowel plotselinge als minder zichtbare risico’s en passen zich hieraan om succesvol te zijn.

Inherente risicofactoren die de weerbaarheid van een organisatie onder druk kunnen zetten, zijn onder andere zeer complexe bedrijfsactiviteiten, mondiale toeleveringsketens, gecentraliseerde infrastructuur of datasystemen, beperkte beschikbaarheid van personeel, volatiele marktomstandigheden en sterke afhankelijkheid van kritieke third-parties of geografische locaties. Organisaties in sectoren waar betrouwbaarheid cruciaal is of organisaties die onder intensief toezicht staan, kunnen ook te maken krijgen met inherent hogere risico’s vanwege hun maatschappelijke impact en verplichting uit wet- en regelgeving.

Organizational resilience richt zich op het beheersen van risico's vóór, tijdens en na een verstoring. Internal auditors beoordelen vaak IT-processen en -beheersmaatregelen rond bedrijfscontinuïteit en disaster recovery. Een bedrijfscontinuïteitsplan beschrijft de stappen die een organisatie neemt om kritieke functies in stand te houden en de normale bedrijfsvoering te hervatten wanneer zich een calamiteit voordoet. Een disaster recovery plan beschrijft hoe organisaties hun IT-systemen, kritieke gegevens en bedrijfsactiviteiten herstellen na een verstoring om de normale bedrijfsvoering te hervatten.

Organizational resilience, waarvan beide plannen onderdeel zijn, vereist strategische planning, enterprise risicomanagement, effectief leiderschap en cultuur en organisatiebrede beheersprocessen. Sterke beheersingsrocessen voor organizational resilience stellen organisaties niet alleen in staat om voortdurend te anticiperen op veranderingen, zich daarop voor te bereiden, erop te reageren en zich eraan aan te passen, maar stelt ook om te overleven en succesvol te blijven.

Evalueren en beoordelen van organizational resilience governance, risicobeheer en beheersprocessen

Deze Topical Requirement biedt een consistente en integrale aanpak voor het beoordelen van het ontwerp en de implementatie van governance, risicomanagement en beheersprocessen voor organizational resilience. De vereisten vormen de minimale basis voor het beoordelen van organizational resilience.

Governance

Vereisten:

Internal auditors moeten de volgende aspecten van de governance van organizational resilience beoordelen:

A. Een formele organisatiestrategie gericht op resilience wordt vastgesteld door het management, goedgekeurd en onder toezicht van het bestuur uitgevoerd, en omvat de operationele, technologische en financiële elementen die nodig zijn om veranderingen te beheersen en de bedrijfsvoering voort te zetten. De resilience-doelstellingen sluiten aan bij de overkoepelende benadering van risicomanagement binnen de organisatie.

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 sturing, langetermijnplanningsprocessen, succession planning en de cultuur van de organisatie, inclusief de resource- en budgettaire overwegingen die nodig zijn om kritieke bedrijfsactiviteiten te ondersteunen.

C. Beleid en procedures voor kritieke operationele, technologische en financiële processen worden opgesteld en periodiek beoordeeld, getest en waar nodig bijgewerkt om de beheersomgeving te versterken.

D. Er wordt 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 besluitvormingsstructuren, communicatie- en escalatieprotocollen en rollen en verantwoordelijkheden op bestuurlijk en operationeel niveau.

E. Er is een proces ingericht om periodiek te toetsen welke competenties nodig zijn om resilience effectief te ondersteunen en om de competenties van personen die kritieke resilience-rollen vervullen 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 inrichten van informatie- en rapportagestructuren die bijdragen aan het realiseren van de resilience-doelstellingen van de organisatie. Stakeholders kunnen onder meer zijn: senior management, operations, risicomanagement, IT, supply chain/inkoop, facilitair management, human resources, financiën, juridische zaken, assurance providers

(waaronder internal audit), compliance, public relations, kritieke leveranciers en dienstverleners, klanten, toezichthouders en andere relevante partijen.

Risicomanagement

Vereisten:

Internal auditors moeten de volgende aspecten van risicomanagement rondom organizational resilience beoordelen:

A. Risico's met betrekking tot organizational resilience worden periodiek organisatiebreed geïdentificeerd, beoordeeld en beheerd. Resilience-risico's worden 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 organizational resilience zijn duidelijk gedefinieerd. Een aangewezen persoon of team wordt belast met het regelmatig monitoren van en rapporteren over het beheer van resilience-risico's, inclusief de middelen die nodig zijn voor risicomitigatie en de identificatie van opkomende dreigingen voor de organizational resilience.

C. Er is een proces ingericht om de niveaus van risico's met betrekking tot organizational resilience (opkomend of eerder geïdentificeerde) te monitoren en risico's die een door de organisatie als onaanvaardbaar niveau bereiken snel te escaleren. Daarbij wordt uitgegaan van de vastgestelde richtlijnen voor risicomanagement, risicotolerantie en toepasselijke wet- en regelgeving . De impact van risico's met betrekking tot organizational resilience wordt 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 incidentresponse- en herstelproces omvat detectie, prioritering, containment, herstel en post-incidentanalyse. De incident response-aanpak omvat scenario-analyses en periodieke stresstests voor uiteenlopende verstorende gebeurtenissen.

Beheersing

Vereisten:

Internal auditors moeten de volgende aspecten van de beheersprocessen met betrekking tot de organizational resilience beoordelen:

A. Er is een proces om kritieke third-party providers (leveranciers en dienstverleners) te identificeren en de minimale voorraadniveaus te bepalen die nodig zijn om essentiële bedrijfsactiviteiten voort te zetten. Het proces omvat ook het actueel bijhouden van een lijst met alternatieve leveranciers.

B. Bedrijfskritieke gegevens zijn geïdentificeerd en geclassificeerd. De gegevensclassificatie omvat het vaststellen waar de gegevens zich bevinden, wie toegang nodig heeft, hoe toegang wordt verkregen en of zij in noodsituaties zijn geback-upt en herstelbaar zijn.

C. Kritieke IT-beheersmaatregelen en continuous monitoring zijn ingericht om informatiebeveiligingrisico's (inclusief cybergerelateerde risico's) te mitigeren en ervoor te zorgen dat gevoelige gegevens tijdens crises, verstoringen en noodsituaties worden

beschermd. De beheersing en continuous monitoring omvatten real-time threat intelligence en het beperken van toegang tot uitsluitend geautoriseerde gebruikers.

D. Kritieke IT-assets zijn geïnventariseerd. IT-assets omvatten de hardware, software en diensten die nodig zijn om de bedrijfsvoering tijdens crises, verstoringen en noodsituaties te ondersteunen.

E. Business continuity and disaster recoveryplannen zijn opgesteld en omvatten gedefinieerde rollen voor aangewezen medewerkers en recoveryteams. De plannen worden periodiek getest (bijvoorbeeld een "desktop exercitie") en de testresultaten, inclusief verbetermogelijkheden, worden gerapporteerd aan het bestuur en senior management.

F. Er is een proces ingericht om de werkomgeving tijdens crises, verstoringen en noodsituaties aan te passen.

G. Er is een proces ingericht om opkomende dreigingen en kwetsbaarheden die de organizational resilience kunnen beïnvloeden continu te monitoren en hierover te rapporteren. Het proces wordt gebruikt om mogelijkheden ter verbetering van de organizational resilience te identificeren, te prioriteren en te implementeren, waaronder systemen voor whistleblowing of het verzamelen van risk intelligence.

H. Er is een proces ingericht om personeel op te leiden en te trainen met betrekking tot organizational resilience, zodat ze op de hoogte zijn van het beleid en de procedures die gevolgd moeten worden en de acties die ondernomen moeten worden wanneer crises, verstoringen en noodsituaties zich voordoen. Het proces omvat trainingsoefeningen waarbij scenario's met verstoringen worden gesimuleerd.

I. Er is een proces ingericht om ervoor te zorgen dat de benodigde operationele, personele, technologische en financiële middelen zijn gebudgetteerd en beschikbaar zijn tijdens crises, verstoringen en noodsituaties. De financiële middelen die nodig zijn ter ondersteuning van organizational resilience worden periodiek geanalyseerd en aan het bestuur gerapporteerd.

J. Er is een proces ingericht voor het evalueren van crises, verstoringen en noodsituaties nadat ze zich hebben voorgedaan en het analyseren van post-incident reviews via een lessons-learned proces, inclusief het verwerken van de geleerde lessen in toekomstige plannen voor organizational resilience.

Over het Instituut van Internal Auditors

Het IIA is een internationale beroepsvereniging met wereldwijd meer dan 265.000 leden en wereldwijd meer dan 200.000 Certified Internal Auditor® (CIA®)-certificeringen heeft uitgereikt. 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.

Copyright

April 2026

The Institute of Internal Auditors

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