Handleiding voor internal audit

Toetsen en adviseren over **Business Continuity Management** en **Crisismanagement**

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

AON
Empower Results®

COT | Instituut voor Veiligheids- en Crisismanagement
an Aon company

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

INHOUD

Uitgave
September 2019

Auteurs
De handleiding is opgesteld in opdracht van de ledengroep Intern en Overheidsaccountants (LIO) van de Koninklijke Nederlandse Beroepsorganisatie van Accountants. Deze handleiding is uitgewerkt door Aon/COT, te weten Abderrahman Kaouass (Aon/COT, Instituut voor Veiligheids- en Crisismanagement) en Iwan Drost (Aon Global Risk Consulting)

Begeleiding door werkgroep
Aon/COT is bij de uitwerking van deze handleiding begeleid door een werkgroep.
De werkgroep bestond uit de volgende leden:
- de heer Ali Ahrouch, Hoofd Audit en Risk Royal FloraHolland, bestuurslid LIO
- de heer Johan Scheffe, Afdeling Beroep & Maatschappij bij Koninklijke Nederlandse Beroepsorganisatie van Accountants
- de heer René Zendijk, Hoofd Internal Audit bij Scildon
- de heer Raymond Wondergem, Auditor bij Woonbron
- de heer Gerard Boerma, Senior Internal Auditor bij Royal FloraHolland

INLEIDING

In een dynamische wereld worden risico's voor bedrijven en instellingen complexer en nemen onzekerheden toe. Geen enkele organisatie is incidentvrij. Er kan altijd iets misgaan. Soms met verstrekkende gevolgen voor personen, het voortbestaan van de organisatie, de financiële situatie of de benodigde capaciteit. De oorzaken kunnen variëren van cyberaanvallen, sociale onrust, verstoring van de bedrijfsvoering, claims tot en met kwetsbaarheden in de supply chain. Inzicht in risico's is cruciaal om incidenten te voorkomen en om de negatieve impact te beperken als het incident zich toch voordoet. Dit lukt door veerkracht te tonen en weerbaar te zijn.

De laatste jaren groeit de rol van internal auditors. Zij toetsen niet alleen of hun organisatie voldoet aan vastgestelde kwaliteitsnormen, maar worden steeds actiever betrokken bij het beheersen van organisatiebrede risico's. De internal auditfunctie kan een belangrijke rol spelen in het toetsen van veerkracht en weerbaarheid. Daarnaast kan deze toets leiden tot belangrijke adviezen, waardoor de internal auditfunctie ook een belangrijke adviesrol heeft.

Deze handleiding gaat over de toegevoegde waarde van de internal auditors voor de veerkracht en weerbaarheid van hun organisaties. Daarnaast zoomt het in op de normen voor veerkracht en weerbaarheid. In deze handleiding focussen wij op twee benaderingen die bedrijven en instellingen in staat stellen om de negatieve impact te beperken als het voorkomen niet lukt, te weten:

- Er is sprake van verstoring van de continuïteit van de bedrijfsvoering > Business Continuity Management (hierna: BCM)
- Er is sprake van een grote crisis met een bedreiging van de license to operate en de bedrijfsreputatie > Crisismanagement.

De uitdaging van bedrijven en instellingen is om bij daadwerkelijk continuïteitsverlies en/of een crisis adequaat te reageren, de schade te beperken en een snel herstel te bevorderen. Juist dan kunnen bedrijven en instellingen laten zien wat zij waard zijn en het vertrouwen van hun klanten en andere stakeholders behouden.

Opzet van deze handleiding

Deze handleiding is bedoeld als praktische gids en hulpmiddel voor internal auditors om hen in staat te stellen hun organisaties te toetsen op BCM en Crisismanagement. We reiken internal auditors ook de benodigde bouwstenen aan voor hun adviesfunctie bij het verbeteren van BCM en Crisismanagement. Deze handleiding is dan ook een hulpmiddel en komt niet in de plaats van de huidige normen voor BCM en Crisismanagement.

LEESWIJZER

Deze handleiding bestaat uit de volgende onderdelen:

1. De beschrijving en definiëring van BCM en Crisismanagement en hoe dit zich verhoudt tot risicomanagement. Dit is uitgewerkt in hoofdstuk 1.
2. In hoofdstuk 2 is een stappenplan uitgewerkt om de organisatie te toetsen op BCM en Crisismanagement. Het stappenplan in deze handleiding is als volgt:

STAP 1: Bepaal de relevantie van BCM en Crisismanagement voor de organisatie

- Aan de hand van kenmerken voor BCM en Crisismanagement, kunt u de relevantie bepalen voor de eigen organisatie.
- Indien de kenmerken voor BCM en Crisismanagement van toepassing zijn op de organisatie, kunt u de huidige status van BCM en crisismanagement bepalen in stap 2.

STAP 2: Bepaal de status van BCM en Crisismanagement binnen de organisatie

- Aan de hand van een toetsingkader voor BCM en Crisismanagement wordt u gevraagd om een uitspraak te doen over de huidige status van BCM en Crisismanagement.
- De status wordt bepaald aan de hand van een drietal classificaties, te weten 'onderhouden', 'enige aandacht nodig' en 'veel aandacht nodig'. De 3 classificaties zijn nader omschreven in een kader.

STAP 3: Stel vast wat de kwetsbaarheid is van de organisatie

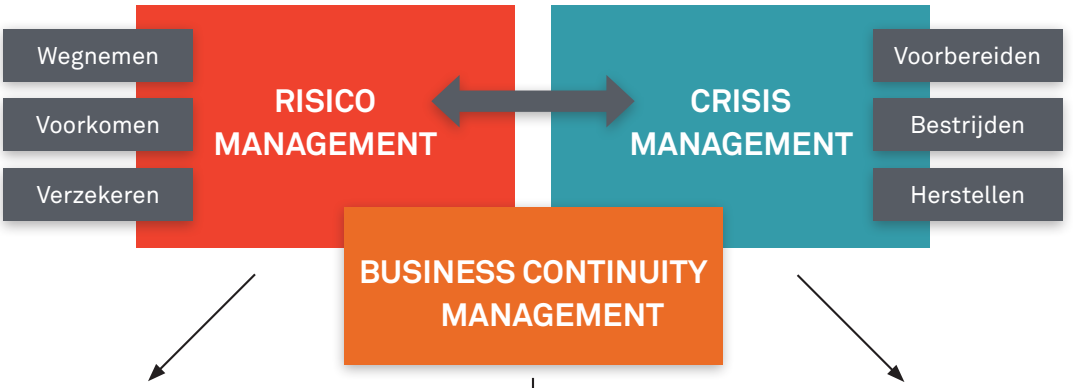
- Op basis van de resultaten van de toetsing van BCM en Crisismanagement uit stap 2, wordt u gevraagd om een overall status te geven voor beide disciplines.
- De kwetsbaarheid van uw organisatie is afhankelijk van de vastgestelde status. Des te meer aandacht voor beide disciplines is benodigd, des te kwetsbaarder de organisatie is.

3. Nadat de internal auditor de huidige status heeft bepaald, kan worden vastgesteld wat er nodig is om BCM en Crisismanagement door te ontwikkelen. Hiertoe hebben we in hoofdstuk 3 een selectie opgenomen van 10 inhoudelijke en procesmatige (draagvlak en borging) tips voor het ontwikkelen en het verstevigen van de adviesrol van internal audit bij BCM en Crisismanagement.

HOOFDSTUK 1

WAT ZIJN BCM EN CRISISMANAGEMENT EN WAT IS DE RELATIE MET RISICOMANAGEMENT?

Risicomanagement, BCM en Crisismanagement tezamen vormen het kwaliteitssysteem voor veerkracht en weerbaarheid.



De capaciteit die de organisatie heeft om bedreigingen voor de doelstellingen te voorkomen.

(naar: ISO 3100:2009)

De capaciteit die een organisatie heeft om na (of anticiperend op) een verstoring de continuiteit op een vooraf vastgesteld niveau te houden.

(naar: BS ISO 22300:2012)

De capaciteit die een organisatie heeft om strategische doelen, reputatie en voortbestaan onder afwijkende, abnormale en complexe omstandigheden te waarborgen.

(naar: BS PAS 200:2011 en CEN/TS 17091)

Hieronder geven we een verdere toelichting op BCM en Crisismanagement.

Business Continuity Management

Wat houdt het in?	BCM richt zich op het vermogen van de organisatie om na een bedrijfsverstorend incident producten of diensten te kunnen blijven leveren, binnen van tevoren gedefinieerde en geaccepteerde serviceniveaus. BCM identificeert potentiële bedreigingen en de impact die deze bedreigingen hebben op de continuïteit van de bedrijfsvoering. Daarnaast voorziet het in een raamwerk voor het opbouwen van organisatorische weerbaarheid en veerkracht, door te investeren in het vermogen om een effectieve respons te realiseren en zodoende de belangen van stakeholders, de reputatie, merk en waarde creërende activiteiten te beschermen.
Welke normen zijn er?	De belangrijkste norm voor BCM betreft de certificeerbare norm NEN ISO 22301:2012, waarin de vereisten van een Business Continuity Management Systeem zijn vastgelegd. Deze norm is eind 2012 gepubliceerd en wordt vergezeld door een 'guidance' norm, de NEN ISO 22313:2013. Deze norm is een richtlijn en geeft duiding aan hoe de verschillende eisen van de ISO 22301 moeten worden geïnterpreteerd en toegepast. Daarnaast heeft het British Continuity Institute (BCI) een syllabus gepubliceerd, de zogenaamde Good Practice Guidelines 2018. De syllabus geeft aan de hand van best practises duidelijke handvatten over BCM zelf, alsook hoe de verschillende onderdelen van BCM dienen te worden opgezet en geïmplementeerd. IIA heeft ook een guideline ontwikkeld, namelijk *Practice Guide business continuity management*.
Hoe verhouden deze zich tot elkaar?	Een continuïteitsprobleem kan uitgroeien tot een crisis, maar dat hoeft niet. Dit is afhankelijk van de impact en mede van de vraag hoe beheersbaar het continuïteitsprobleem is. Continuïteitsmanagement is dan ook niet hetzelfde als Crisismanagement, maar is hier mogelijk wel een onderdeel van. Daarnaast zijn er incidenten en crises die geen continuïteitsproblemen tot gevolg hebben en toch negatieve impact hebben

Crisismanagement

Een crisis is een ernstigste uitdaging of incident waarvoor een organisatie zich gesteld kan zien. Een crisis is een buitengewone verstoring, onstabiele en/of een impactvolle en complexe situatie die een mogelijke bedreiging vormt voor de strategische doelstellingen, veiligheid van medewerkers of omgeving, reputatie en, uiteindelijk, de continuïteit en het bestaan van een organisatie.

Momenteel zijn er twee normen voor Crisismanagement. De British Standard 11200:2014 en de Europese norm CEN/TS 17091 'Crisis management – Guidance for developing a strategic capability'.

Beide normen beogen organisaties handvatten te bieden hun bekwaamheid om met crisissituaties om te gaan te ontwikkelen en verbeteren.

op de organisatie. Vaak ligt het vergrootglas op de organisatie waardoor zelfs dagelijkse werkzaamheden niet volgens hun normale routine kunnen worden uitgevoerd. De ruimte die een organisatie krijgt - de 'license to operate' - neemt snel af. Onzekerheid, tijdgebrek en de noodzaak tot het nemen van fundamentele beslissingen kenmerken de situatie. In deze situaties moet er vaak worden samengewerkt met veel (en nieuwe) partijen. Bijvoorbeeld een integriteitsschandaal, slachtoffers medewerkers/bezoekers bij een ongeval, reputatieschade als gevolg van klokkenluiders.

Gijzeling tijdens NOS Acht uur Journaal

Rond 20.00 uur op donderdag 17 augustus 2017 wordt een beveiliger van de NPO bedreigd door een man met een (achteraf nep gebleken) pistool, waarna hij de beveiliger dwingt om hem binnen te laten in het pand. De persoon bedreigt medewerkers van NOS en eiste zendtijd op het Acht uur Journaal. De man beweert onderdeel uit te maken van een hackerscollectief en wilde wereldzaken bespreken op live televisie. Na contact tussen de gijzelnemer en een onderhandelaar, slaagt een arrestatieteam van de politie er in om de situatie te beeindigen en de gijzelnemer aan te houden. De dreiging noodzaakte een acute reactie van verschillende actoren zoals beveilighing, BHV, NPO functionarissen, NOS en politie. De gijzelnemer zorgde voor angst, onrust en onzekerheid bij de omroep. De impact van de gebeurtenis is groot, met de gijzeling bij de NOS van 2015 en de gebeurtenissen in Parijs omtrent Charlie Hebdo nog vers in het geheugen.

Grootschalige evacuatie van patiënten VUmc

Op 8 september 2015 breekt een waterleiding nabij het VUmc. Grote hoeveelheden water stroomden het gebouw van VUmc binnen en de kracht van dit water veroorzaakte forse schade aan (kritische) installaties. Toen deze situatie zich voltrok waren er 339 patiënten in het pand. Het ziekenhuis besloot, dat onder deze omstandigheden, er niet langer verantwoorde zorg kon worden geboden en dat patiënten elders moesten worden ondergebracht. Vervolgens is een grootschalige operatie op gang gebracht om dit mogelijk te maken, met de hulp van vele partijen zoals hulpdiensten en defensie. Ook was er intensieve media-aandacht en een forse informatie-opgave richting patiënten en hun familie. Het VUmc was onder deze omstandigheden genoodzaakt om onder grote tijdsdruk en te midden van onzekerheid een passende reactie te organiseren op deze dynamische, complexe en veelal emotionele situatie.

HOOFDSTUK 2

HET TOETSEN VAN DE ORGANISATIE OP BCM EN CRISISMANAGEMENT

In deze handleiding bieden we handvatten voor het toetsen van en adviseren over BCM en Crisismanagement. Dit deel van de handleiding gaat over het toetsen van BCM en Crisismanagement.

STAP 1: Bepaal de relevantie van BCM en Crisismanagement voor de organisatie

Waarom zou de organisatie aandacht moeten hebben voor continuïteit, incidenten en crises? Om deze vraag te beantwoorden is het van belang de relevantie van BCM en Crisismanagement aan de hand van specifieke kenmerken van de organisatie te onderzoeken. Met andere woorden: wanneer is BCM en Crisismanagement handig en wanneer is het noodzakelijk?

Hieronder is een tabel opgenomen met daarin relevante vragen vanuit BCM en Crisismanagement. Kort gezegd komt het erop neer dat bij positieve antwoorden op de vragen, de organisatie kwetsbaar wordt voor discontinuïteit en/of er sprake kan zijn van een brede impact die een risico in het ergste geval kan hebben.

Kenmerken voor relevantie van BCM voor de organisatie	**Kenmerken van relevantie van Crisismanagement voor de organisatie**
Type organisatie In welke mate is de organisatie afhankelijk van middelen? Denk hierbij aan de afhankelijkheid van productiemiddelen (gebouwen, installaties, machines, ICT, mensen, utiliteiten, etc.) en toeleveranciers.	**Merk/branche** Heeft de organisatie/de branche politieke aandacht? Zijn er actuele gevoelige dossiers? Heeft de organisatie eerder te maken gehad met incidenten met grote en brede impact? Wat is de reputatie? Wat is de perceptie van stakeholders over het bedrijf/instelling?
Grootte en complexiteit van de organisatie Heeft u voldoende inzicht in de grootte en complexiteit van de organisatie en de impact die een mogelijk verstoring heeft?	**Kernactiviteiten** Kunnen de producten of diensten voor grote materiële schade zorgen? Of voor gezondheidsschade? Gaat het om klanten die

Hoewel organisaties van alle groottes kwetsbaar zijn, zal een bedrijfsonderbreking bij grotere organisaties vaak een grotere financiële impact hebben. Naast grootte is complexiteit ook een kenmerk. Dit kan betrekking hebben op het primaire productieproces en de afhankelijkheid van toeleveranciers. Dit kan resulteren in langere hersteltijden door uitval van complexe productiemiddelen en/of unieke leveranciers.

Mate waarin de organisatie zich continuïteitsverlies kan permitteren

In hoeverre kan de organisatie zich een eventueel continuïteitsverlies permitteren? Factoren die hierbij een belangrijke rol spelen betreffen:

- De concurrentiepositie van de organisatie en de bereidheid en het gemak waarmee de klanten kunnen overstappen naar een concurrent.
- De maatschappelijke functie van de organisatie (denk aan energiebedrijven, telecom, drinkwatervoorzieningen, gezondheidszorg, etc.).
- De risicobereidheid van de organisatie. Binnen de risicobereidheid wordt bepaald in hoeverre de impact op bijvoorbeeld de continuïteit van de operatie, financiën, reputatie, wet- en regelgeving en veiligheid acceptabel is of niet.

Eisen die vanuit de omgeving van de organisatie worden gesteld aan continuïteitsmanagement

Zijn er specifieke eisen die vanuit wet- en regelgevende instanties of andere stakeholders worden gesteld aan continuïteitsmanagement voor de organisatie?
Er kunnen continuïteitseisen vanuit wet- en kwetsbaar zijn (ouderen, kinderen)? Bent u direct verantwoordelijk voor de veiligheid van personen? Kan het de persoonlijke levenssfeer van klanten en medewerkers raken? Hebben de activiteiten van de organisatie maatschappelijke impact? Is er een merkbare, grote impact als die activiteiten verstoord worden?

Veiligheidscultuur

Zijn de medewerkers zich bewust van de risico's van hun werkomgeving? Is er een cultuur waar er aandacht is voor risico's?

Structuur van de organisatie

Onderneemt u kernactiviteiten en/of heeft u productielocaties in meerdere landen? Is bekend hoe incidenten/calamiteiten/crises bij een toeleverancier impact kunnen hebben op het bedrijf? Is er een opeenhoping van verschillende kwetsbare functietaken bij één of beperkt aantal personen, zoals

regelgeving worden gesteld (Agentschap Telecom, DNB, EU, etc.) of vanuit andere belanghebbenden zoals klanten, verzekeraars en banken.

Ervaring uit het verleden met bedrijfsverstorende incidenten en de mate waarin deze hebben geleid tot onacceptabele impact

Hebben er in het verleden incidenten plaatsgevonden die hebben geleid tot onacceptabele impact?

Overwegend geldt voor organisaties die een bedrijfsverstorend incident hebben ervaren of bij hun collega's, dat zij het nut en de noodzaak van BCM inzien, zeker in het geval van onacceptabele impact. Daarnaast zijn deze organisaties geneigd om, mede op aandringen van stakeholders, interne eisen te stellen ten aanzien van BCM.

vertrouwelijke informatie, aanbestedingen en inkoop, toezichthoudende taken? Raken de activiteiten aan geopolitieke ontwikkelingen of belangen? Acteert u in onveilige gebieden? Werkt u/levert u aan landen met een streng juridisch klimaat?

Cyber

Heeft de organisatie een businessmodel dat voor een belangrijk deel volledig gestoeld is op de continue werking en beschikbaarheid van ICT, bijv. substantiële loss of business als internet uitvalt? Is het mogelijk dat door technische storingen en/of bewuste pogingen daartoe privacygevoelige gegevens op straat komen te liggen van werknemers, klanten, zakenrelaties, overheden? Bezit de organisatie vertrouwelijke informatie die bij bekendmaking ervan grote schade kan toebrengen aan het bedrijf, de sector en/of samenleving?

Stakeholders

Is de organisatie op de hoogte van het risicoprofiel van de zakenrelaties? Heeft u adequate beheersmaatregelen genomen voor het risicoprofiel van de zakenrelaties? Weegt u het risicoprofiel mee in besluiten om zaken te doen met potentiële zakenrelaties? Hoe is de houding van toezichthouders t.o.v. de organisatie/sector? Zijn er toezichthouders die vergaand in kunnen grijpen? Hoe zichtbaar is ingrijpen door de toezichthouder?

Cyberaanval op APM Terminals in Rotterdamse haven

Op 27 juni 2017 worden de APM terminals getroffen door een cyberaanval in de vorm van ransomware. De cyberaanval blijkt niet direct gericht te zijn aan de APM terminals, maar aan het moederbedrijf MAERSK waarvan de software wordt gebruikt. Ondanks dat het geen gerichte aanval was op APM terminals, heeft de aanval grote impact gehad. Door de digitale kaping lag het werk op de Maasvlakte stil. Ook in de media was er volop aandacht voor de cyberaanval. Doordat de getroffen terminal vanwege het uitvallen van telefonie en de interne crisis slecht bereikbaar was, werd er onterecht in de media gespeculeerd dat de hele Rotterdamse haven was geraakt door de randsomeware. De cybercrisis betekende een onzekere situatie voor APM waar met name de continuïteit van de bedrijfsvoering, de veiligheid van medewerkers en de impact op de directe omgeving in het geding waren.

Hoe bepaalt u de status van BCM en Crisismanagement? Hieronder treft u een tabel aan met daarin 3 classificaties (onderhouden, enige aandacht nodig, veel aandacht nodig) voor de huidige status van BCM en Crisismanagement voor uw organisatie.

Toetsingskader - huidige status	Omschrijving
Onderhouden	Van de componenten (zie stap 2) is het merendeel in de basis aanwezig. De opzet en het bestaan van alle elementen voldoen aan de daaraan gestelde normen en er is sprake van een adequate werking. *Dit komt bijvoorbeeld tot uiting doordat:* • *Er sprake is van een systematisch geborgd proces, dat onderdeel uitmaakt van de dagelijkse bedrijfsvoering en besluitvorming.* • *BCM en CM zijn belegd op alle managementniveaus binnen de organisatie, met een duidelijk mandaat en specifiek budget.* • *De organisatie kent haar kwetsbaarheden en beheerst deze stelselmatig door het implementeren van maatregelen en het meten van en sturen op prestaties.* • *Er wordt voortdurend geïnvesteerd in de competenties van betrokken medewerkers door training, simulatieoefeningen, evaluatie en inhuur van kennis, zodat de organisatie erop kan vertrouwen dat BCM en CM ook zullen werken in de praktijk.* • *(Bijna)incidenten worden stelselmatig geregistreerd en geëvalueerd. De zogenaamde "lessons learned" worden gerapporteerd en breed gedeeld binnen de organisatie.*
Enige aandacht nodig	Van de betreffende component zijn slechts bepaalde elementen aanwezig, en derhalve gefragmenteerd. Van opzet, bestaan en werking is slechts gedeeltelijk sprake. *Dit komt bijvoorbeeld tot uiting doordat:* • *Slechts voor specifieke onderdelen van de organisatie of voor specifieke risico's formele processen zijn geïmplementeerd en geborgd.* • *De aandacht voor BCM en CM slechts op bepaalde niveaus (operationeel, tactisch, strategisch) binnen de organisatie is belegd.*

	• *Het implementeren van maatregelen ter bevordering van BCM en CM in de meeste gevallen incident gedreven plaatsvindt.* • *In geval van een continuïteitsbedreigende calamiteit of een crisis het de vraag is of de organisatie kan vertrouwen op een adequate respons.*
Veel aandacht nodig	Van de betreffende component ontbreekt iedere formele status en zijn hooguit bepaalde elementen informeel aanwezig. Van opzet, bestaan en werking is geen sprake. *Dit komt bijvoorbeeld tot uiting doordat:* • *De betreffende component, of elementen daarvan, vooralsnog niet relevant wordt gevonden of nog informeel is geregeld.* • *De organisatie niet kan vertrouwen op een adequate respons indien zich een continuïteitsbedreigende calamiteit of een crisis voordoet. Hierdoor kan de impact onacceptabel groot zijn en het voortbestaan direct in gevaar komen.*

STAP 2: Bepaal de status van BCM en Crisismanagement voor de organisatie

Met onderstaande componenten kunnen internal auditors per onderdeel een inschatting maken van de status van BCM en Crisismanagement.

	Onderdelen Business Continuity Management
Organisatorische context *In hoeverre is BCM in lijn met de context waarin de organisatie opereert, wordt rekening gehouden met de (wettelijke) eisen en verwachtingen die door stakeholders worden gesteld aan de organisatie?*	De organisatie beschikt over een actueel en kloppend overzicht van de meest essentiële bedrijfsactiviteiten ('bedrijfskritische processen').
	De organisatie beschikt over een actueel en kloppend overzicht van de belangrijkste ('kritieke') afhankelijkheden binnen én buiten de organisatie.
	De organisatie beschikt over een actueel en gedocumenteerd inzicht in de bedrijfsimpact ('effecten') bij uitval van essentiële bedrijfsactiviteiten en/of het wegvallen van kritieke afhankelijkheden.
	Het risico- en continuïteitsmanagement van de organisatie krijgt integraal vorm.
	De einddoelen voor BCM van de organisatie zijn geformuleerd en gedocumenteerd.
	De grenzen (reikwijdte) van BCM zijn vastgesteld en gedocumenteerd.

	Voorbeelden waaruit dit blijkt	Status
	• Dit overzicht is mede het resultaat van de Business Impact Analyse (BIA) die periodiek wordt uitgevoerd. • De bedrijfskritische processen staan centraal in het Business Continuity Plan (BCP).	
	• Er is gedocumenteerd welke onderlinge afhankelijkheden er intern bestaan, bijvoorbeeld tussen ICT en uitvoerende delen van de organisatie, maar ook tussen uitvoerende delen onderling. • Er is gedocumenteerd welke cruciale afhankelijkheden er met welke leveranciers bestaan en voor welke producten de aanvoer kwetsbaar is.	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig
	Dit is het resultaat van de Business Impact Analyse (BIA) die periodiek wordt uitgevoerd.	
	• De belangrijkste risico's voor de continuïteit zijn in beeld gebracht en vormen onderdeel van het algemene risicoprofiel. • BCM sluit naadloos aan op het risicoprofiel: de belangrijkste continuïteitsrisico's worden middels BCM geadresseerd. • Daarnaast levert de organisatie aantoonbaar inspanningen om de belangrijkste continuïteitsrisico's te reduceren.	
	De einddoelen staan vermeld in het BCM-beleid van de organisatie. De doelen hebben betrekking op wat de organisatie wil bereiken, wat ze wil beschermen en welke maximale uitval tijden voor kritische activiteiten gelden.	
	De scope staat eveneens vermeld in het BCM-beleid van de organisatie.	

	Onderdelen Business Continuity Management
	BCM houdt rekening met alle van toepassing zijnde (formele) externe eisen en verwachtingen.
Leiderschap *In hoeverre tonen alle relevante managementlagen binnen de organisatie de benodigde commitment en leiderschap voor BCM en de doelen die hiermee worden nagestreefd?*	Het management van de organisatie vindt BCM aantoonbaar belangrijk en draagt het belang actief uit.
	Het management van de organisatie ziet er actief op toe dat de (herstel)doelen van BCM worden behaald.
	Het management van de organisatie vult de randvoorwaarden voor het BCM van de organisatie in, en stelt de benodigde (hulp) middelen beschikbaar.
	Het management van de organisatie beschouwt BCM als onderdeel van het (integraal) kwaliteitsmanagement.
	De benodigde verantwoordelijkheden en mandaten voor BCM zijn door het management van de organisatie toegewezen.
Planning *In hoeverre wordt BCM planmatig, taak- en actiegericht geïmplementeerd en onderhouden, zodat de gestelde beleidsdoelen binnen het programma worden gehaald?*	BCM functioneert optimaal. BCM wordt aantoonbaar geëvalueerd en steeds verder verbeterd.

	Voorbeelden waaruit dit blijkt	Status
	• De organisatie beschikt over een overzicht van relevante (formele) eisen en verwachtingen. • BCM houdt rekening met wettelijke/contractuele verplichtingen met afnemers.	
	• Het management communiceert regelmatig over het belang van BCM. • BCM staat regelmatig op de agenda bij het management overleg binnen alle lagen van de organisatie.	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig
	• De (herstel)doelen zijn vastgelegd en de eigenaren leggen periodiek verantwoording af tijdens de management review (rapportages en bila's). • Er vindt actieve sturing plaats op het behalen van de doelen.	
	• Voldoen aan de ISO 22301 door certificering wordt gebruikt als randvoorwaarde. • Middelen die beschikbaar zijn gesteld voor het vervullen van de taken die voortvloeien uit het opzetten, implementeren en onderhouden van BCM (tijd), het documenteren (tooling), het investeren in competenties door (externe) trainingen, lidmaatschap van kennisinstituten, communicatiemiddelen, investeren in bewustwordingscampagnes, etc.	
	BCM is aantoonbaar een onderdeel van het kwaliteitsmanagement systeem.	
	Betrokkenen weten wat er van hen wordt verwacht c.q. waarvoor zij verantwoordelijk zijn.	
	De risico's voor het functioneren van het managementsysteem zijn in beeld en worden actief beheerst dan wel weggenomen. • Er is een actieplan voor het programma waarbij periodiek alle relevante componenten (Business Impact Analyse, risicoanalyse, beheersmaatregelen, planvorming, training, testen en onderhoud) worden geëvalueerd door actiehouders op voortgang, afwijking, bijsturing en verbetering. • Het programma wordt voortdurend geactualiseerd op basis van management review, auditresultaten, substantiële	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig

Stroomstoring Schiphol

Een defect in een verdeelstation op 29 april 2017 in Amsterdam Zuidoost, veroorzaakte een stroomstoring en daarmee de uitval van incheck- en bagagesystemen op Schiphol. De uitval van de systemen heeft geleid tot verstoring van de primaire luchthavenprocessen, wat uiteindelijk leidde tot effecten op de openbare orde en veiligheid en de verkeersmobiliteit op de luchthaven en de omgeving. De regionale crisisorganisatie is hierbij opgeschaald naar GRIP 2. De luchthaven en crisispartners werden geconfronteerd met de consequenties van de stroomstoring op het primaire luchthavenproces en de (mogelijke) effecten op de openbare orde en veiligheid en de mobiliteit op en rond de luchthaven.

Uitval alarmnummer 112

Op maandag 24 juni 2019 was gedurende bijna 4 uur het alarmnummer 112 niet bereikbaar vanwege een storing bij KPN. Naast 112 was ook politienummer 0900-8844 niet bereikbaar. De urenlange telefoniestoring was veroorzaakt door een softwarefout. KPN gebruikt vier routeringssystemen en volgens het telecombedrijf traden er gelijktijdig fouten op in al deze systemen. Vervolgens zouden de monitoringssystemen „onvoldoende adequaat gereageerd" hebben. Lange tijd was er geen alternatief noodnummer. Pas rond 18.15 uur verspreidde de politie via berichtensysteem NL-Alert een landelijk alternatief nummer, samen met een nummer voor WhatsApp. Een uur later moest de politie dat tweede nummer corrigeren, want de politie had per abuis de tiplijn van De Telegraaf verspreid. Deze uitval is niet de eerste uitval van het alarmnummer 112. Op 21 juni 2012 was er ook al een grote storing, die uiteindelijk 6 uur heeft geduurd. Naar aanleiding van de storing in 2012 zijn diverse maatregelen getroffen ter voorkoming van uitval, met name in de back-up en redundantie van systemen. De politie achtte het door de getroffen maatregelen zeer onwaarschijnlijk dat 112 nogmaals zou uitvallen, hetgeen toch is gebeurd. Er is niet geoefend met het scenario van complete uitval van 112.

	Onderdelen Business Continuity Management
	BCM is volledig gedocumenteerd.
	BCM voldoet aan de normen voor documentmanagement.
Support *In hoeverre investeert de organisatie in de benodigde capaciteit voor het succesvol implementeren, onderhouden en verbeteren van BCM?*	Alle collega's die betrokken zijn bij BCM zijn zich bewust van het belang van BCM en weten wat er van hen wordt verwacht.
	De organisatie beschikt over een toereikende procedure voor communicatie met alle betrokkenen binnen en buiten de organisatie.
Werking *In hoeverre heeft de organisatie een werkend en periodiek BCM-proces ingericht?*	Impact Analyses en risicoanalyses worden periodiek uitgevoerd conform de eisen uit ISO 22301.
	De organisatie beschikt over continuïteitsstrategieën om de kritieke activiteiten te waarborgen.

	Voorbeelden waaruit dit blijkt	Status
	wijzigingen in de organisatie en de keten van afhankelijkheden (leveranciers), (bijna) incidenten, etc.	
	Er is een documentenregister, met unieke documenten- en versienummers, data, wijzingenregisters, etc.	
	Denk hierbij aan eisen ten aanzien van documentinformatie als toegankelijkheid, volledigheid en juistheid.	
	• Alle betrokkenen zijn actief bewust gemaakt van het belang van BCM en weten wat er van hen wordt verwacht. Denk hierbij aan het delen van relevante informatie (schriftelijk), het organiseren van bewustwordingsbijeenkomsten. • Collega's die bij het BCM zijn betrokken beschikken over de benodigde kennis, competenties en ervaring. Denk bijvoorbeeld aan het bieden van relevante opleidings-, trainings- en oefenmogelijkheden.	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig
	• Alle stakeholders binnen en buiten de organisatie zijn in beeld gebracht; hun contactinformatie is actueel en volledig. • Er is rekening gehouden met bereikbaarheid – ook buiten kantooruren. • De organisatie beschikt over communicatiemiddelen die bereikbaarheid garanderen én waarvan de werking periodiek wordt getoetst.	
	• Wanneer is de laatste risicoanalyse uitgevoerd? • Wat omvat deze risicoanalyse? Zo dient de impact analyse per kritische activiteit een overzicht te bevatten van benodigde middelen en afhankelijkheden, en geeft de analyse een duidelijke prioritering van de activiteit ten aanzien van het herstel in de tijd. De risicoanalyse geeft duidelijk aan wat de kans van optreden en de impact bij uitval is en in hoeverre de organisatie kwetsbaar is.	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig
	• De strategie omvat voor de kritieke activiteiten duidelijke maatregelen om discontinuïteit te voorkomen en maatregelen om de impact te beperken (alternatieven voor fall-back, uitwijk, herstel).	

	Onderdelen Business Continuity Management
	De organisatie beschikt over continuïteitsstrategieën ter beheersing van continuïteitsverstoringen, inclusief een structuur voor incident response, continuïteitsplannen en herstel.
	Procedures worden beoefend en betrokkenen worden getest.
Meten en verbeteren *Zijn de prestaties voor BCM duidelijk gedefinieerd? Hoe worden de prestaties gemeten? Hoe vindt voortdurende bijsturing en verbetering plaats?*	De prestaties van BCM worden planmatig geëvalueerd, zowel in het licht van de doelstellingen als de ISO-standaard.
	De resultaten van de planmatige evaluaties zijn goed gedocumenteerd.
	Er wordt periodiek intern ge-audit op de doelmatigheid, inbedding en effectiviteit van BCM; resultaten worden gedeeld met het management.
	Het management evalueert BCM periodiek en stuurt zo aan op doorontwikkeling en verbetering.

	Voorbeelden waaruit dit blijkt	Status
	• De procedures dienen heldere escalatie-, notificatie en activatieprocedures te bevatten, een governance structuur voor incident response, uitgewerkte actieplannen voor scenario's te bevatten die het herstel tot een acceptabel niveau terugbrengen binnen een van tevoren gedefinieerde tijdsinterval.	
	• Er is een programma opgesteld waarbij betrokkenen op reguliere basis worden beoefend en getest op bereikbaarheid, besluitvorming, het herstel zelf, etc. • Betrokkenen tekenen voor deelname aan het programma en weten wat van ze verwacht wordt tijdens een incident dat leidt tot discontinuïteit.	
	• Er zijn KPI's voor BCM vastgesteld (hoe vaak dient de BIA te worden uitgevoerd/geactualiseerd, hoe vaak wordt geoefend). • Worden verbetermaatregelen geïmplementeerd en leidt dit tot reductie van het risico (zowel aan de oorzaak als de gevolgkant)? • Hoe vaak wordt er geëvalueerd en zijn er duidelijke momenten voor evaluatie vastgesteld (bijvoorbeeld bij veranderingen)? Van wanneer dateert de laatste evaluatie?	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig
	• Hoe worden de resultaten vastgelegd (binnen welk systeem), hoe worden ze gedeeld, wie heeft toegang, maken ze onderdeel van het document management systeem, etc.?	
	• BCM is onderdeel van het jaarlijkse auditplan. • Er vindt periodiek een onafhankelijke audit plaats. • De input voor het auditplan is gebaseerd op een risico-beoordeling. • De auditresultaten worden gerapporteerd aan het bestuur en/of auditcommittee.	
	• Minimaal 1 keer per jaar worden alle resultaten van voortgangsrapportages, management reviews en audits besproken door het management. • Ongewenste afwijkingen worden gesignaleerd, onderzocht, systematisch aangepakt en verholpen.	

Onderdelen Crisismanagement	
Anticiperen *Hoe identificeert de organisatie crises, wat is haar crisisprofiel en wat is haar visie en ambitie?*	De organisatie heeft inzicht in de belangrijkste risico's die uit kunnen groeien tot een potentiële crisis (risicoprofiel).
	De organisatie heeft haar top risico's benoemd en heeft zicht op de meest kwetsbare processen en activiteiten die van vitaal belang zijn.
	De organisatie beseft dat crises kunnen plaatsvinden, ongeacht de effectiviteit van bestaande risicomaatregelen, en realiseert zich dat zij daarom voldoende voorbereid moet zijn om deze crises doeltreffend te managen. De organisatie heeft dit verwoord in een visie en ambitie (wat wil ze kunnen) ten aanzien van crises en crisismanagement.
Preparatie *Heeft de organisatie zich voorbereid om specifieke risico's het hoofd te bieden en om te gaan met crises die niet te voorzien zijn?*	De organisatie beschikt over een integraal crisismanagementplan met daarin de uitwerking van het onderdeel 'Respons'.
	De organisatie beschikt over specifieke voorbereiding op haar top-3/top-5 risico's d.m.v. van deelplannen, draaiboeken, scenariokaarten, etc.
	De organisatie heeft veerkracht ingebouwd voor de crisisteams door zowel een basissamenstelling in te richten als vervangers aan te wijzen.
	De organisatie beschikt over een OTO-plan (opleidingsprogramma, oefenprogramma, onderhoud van kennis en vaardigheden).
	De organisatie heeft risico- en crisiscommunicatie opgenomen in de bestaande communicatieplannen.
	De organisatie heeft zicht op wie betrokken zijn en/of impact ondervinden van een crisis bij de organisatie. Er is zicht op kritieke stakeholders (intern, extern, supply chain) en de bijzonderheden die voor hen gelden: wat is de impact voor de stakeholder, welke reactie vergt dit van de organisatie, wat heeft de organisatie hiervoor geregeld en wie zijn hier binnen de organisatie verantwoordelijk voor?

	Status
	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig
	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig

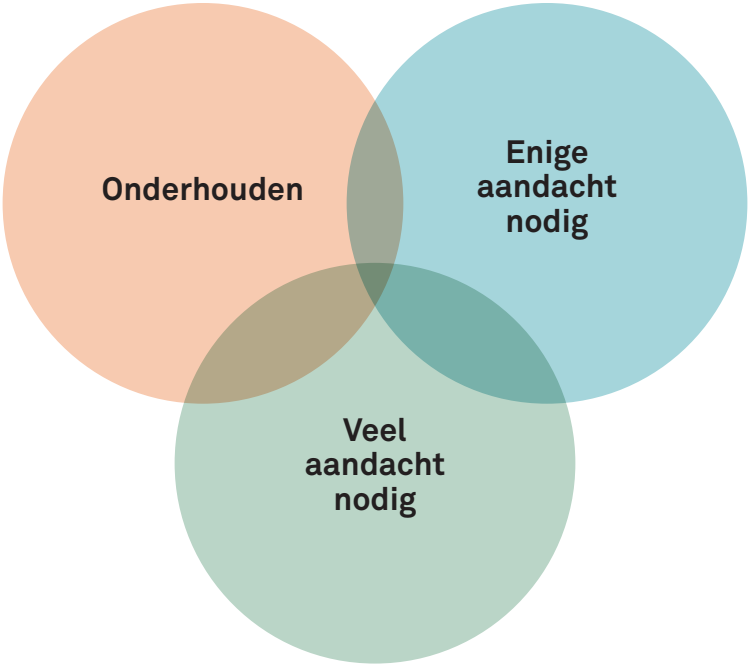
Onderdelen Crisismanagement	
	De relatie tussen Business Continuity Management, ICT-respons en andere calamiteitenplannen is opgenomen in het crisismanagementplan.
Respons *Heeft de organisatie genoeg in huis voor de crisisorganisatie om snel en op een geïnformeerde manier te handelen in tijden van crisis?*	De organisatie heeft beschreven wanneer er wordt opgeschaald en hoe de opschaling in zijn werk gaat. De volgende onderdelen zijn uitgewerkt: signalering, melding, opschaling, activering crisisteams (operationeel, tactisch en/of strategisch), coördinatie en afstemming tussen crisisteams, afschaling en start nafase.
	De rollen, taken en bevoegdheden van (indien aanwezig) operationele, tactische en strategische crisisteams zijn beschreven. De organisatie beschikt over gedocumenteerde informatie per crisistype (scenariokaarten, doelen en uitgangspunten etc.), die gebruikt kan worden tijdens de crisis.
	De organisatie beschikt over een 'crisisruimte' en weet naar welke ruimten zij kan uitwijken mocht de crisisruimte niet beschikbaar zijn.
	Een crisisvergaderagenda en vergaderstructuur (beeldvorming, oordeelsvorming en besluitvorming) zijn beschikbaar voor het team.
	Het team heeft nagedacht over een manier van informatiemanagement tijdens crises, en beschikt over de benodigde middelen om dit goed uit te voeren.
Herstel *Heeft de organisatie de crisisrespons in de nafase vastgelegd?*	De organisatie beschikt over plannen en protocollen die een goede overgang naar de nafase organiseren: relevante nafase thema's worden benoemd, interne en externe stakeholders voor de nafase thema's worden benoemd en reguliere functionarissen die een rol hebben in de nafase worden vastgesteld.
Evalueren en borgen *Kan de organisatie op de eigen ervaringen reflecteren?*	De organisatie heeft een kwaliteitscheck ingebouwd in de crisismanagementorganisatie: lessen worden geleerd van zowel crisismanagementvoorbereidingen als de respons na een crisis, en plannen worden wanneer nodig aangepast.

	Status
	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig
	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig
	• Onderhouden • Enige aandacht nodig • Veel aandacht nodig

STAP 3: Stel vast wat de kwetsbaarheid is van de organisatie

Als internal auditor heeft u bij stap 2 de status van BCM en CM bepaald. De volgende stap is om aan de hand van de optelsom van de classificaties (onderhouden, enige aandacht nodig, veel aandacht nodig) zelf te bepalen wat voor type kwetsbare organisatie u bent.

We willen u als internal auditor helpen door een selectie te maken van 1 van de volgende drie statussen. De optelsom van de antwoorden in stap 2 (en dat vraagt om een expert judgement van de internal auditor zelf) geeft een logische uitkomst. Waar staat u als organisatie?



Nu u als internal auditor de huidige status heeft bepaald, kunt u kijken wat er nodig is om BCM en Crisismanagement door te ontwikkelen. In het volgende hoofdstuk hebben we een selectie opgenomen van zowel inhoudelijke tips als tips voor draagvlak en borging.

HOOFDSTUK 3

10 TIPS EN HANDVATTEN VOOR ONTWIKKELING VAN BCM EN CRISISMANAGEMENT VANUIT INTERNAL AUDIT

1. **Ontwikkel als internal auditor kennis van BCM en Crisismanagement.** De in hoofdstuk 1 genoemde normen en Good Practice Guidelines vormen een goed startpunt. Investeer in relevante opleidingen die op BCM en Crisismanagement worden gegeven.

2. **Bespreek binnen het auditteam het belang van BCM en Crisismanagement en neem voor de jaarplanning nadrukkelijk BCM en Crisismanagement mee.** Baseer de aanpak en te auditen BCM-onderwerpen op de geïdentificeerde continuïteitsrisico's of (bijna) incidenten die hebben plaatsgevonden. Betrek daarbij eventueel de kennis en ervaring van de risk manager en/of stel kritische vragen over het eventueel ontbreken van continuïteits- en crisis risico's in het aanwezige risicoregister.

3. **Leg de relevante normen voor BCM en Crisismanagement vast als toetsingskader voor de audits.** Gebruik daarbij het in deze handleiding gehanteerde toetsingskader voor BCM en Crisismanagement.

4. **Toets in welke mate de organisatie richtlijnen heeft voor de governance voor BCM en Crisismanagement.** Dit gaat om het vastleggen van rollen, taken en verantwoordelijkheden voor het strategische, tactische en operationele niveau.

5. **Toets in welke mate de organisatie een functieprofiel heeft voor de BCM- en/of Crisismanager.** Dit gaat over coördineren, initiëren, agenderen en faciliteren van BCM en/of Crisismanagement.

6. **Breng het control framework op één lijn met het brede risicoprofiel.** In de huidige basis voor het beoordelen van de risico's en maatregelen dienen ook continuïteits- en crisisrisico's opgenomen te worden. Op deze manier worden in het control framework zowel onderwerpen meegenomen die over preventie als over herstel/repressie gaan.

7. **Agendeer BCM en Crisismanagement bij de riskmanager, directie/bestuur en RvC/RvT.** Neem als internal audit het initiatief om het control framework te verbreden naar BCM en Crisismanagement. Ga in gesprek met de riskmanager én RvC/RvT om het belang te benadrukken van deze verbreding in het licht van alle noodzakelijke maatregelen om risico's te voorkomen én tijdig en adequaat te beheersen en te herstellen. Is de auditagenda vol? Maak dan gebruik van een externe partij.

8. **Neem bij BCM- en Crisisoefeningen deel als observator en zorg ervoor dat internal audit geïnformeerd wordt over de evaluaties van BCM-incidenten en crises.** Betrek bij de oefeningen ook eventuele kritische partners of leveranciers.

9. **Vervul als internal audit de verbinding** tussen de verschillende risicodisciplines binnen de organisatie. Doe dit door vanuit het auditen van processen de samenhang tussen risicomanagement, BCM en Crisismanagement te bewaken en hiermee de veerkracht en weerbaarheid van de organisatie te vergroten.

10. **Breid de reikwijdte van het auditplan uit naar kritieke leveranciers.** Audit daarbij op de beheersing op het risico van uitval of misstanden, zoals op het gebied van arbeid, milieu en duurzaamheid.

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

NBA

Antonio Vivaldistraat 2
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
E nba@nba.nl
I www.nba.nl