

ARTIKELN | 1 JULI 2019

WAAROM BCM EN CRISISMANAGEMENT BELANGRIJK IS

Auteur: Drs. Abderrahman Kaouass - Drs. Iwan Drost - Mr. Saida Nhass CIPP/E

Beeld: Adobe Stock - Sammie Chaffin - Andrea Piacquadio

Leestijd: 8 min



Het is van belang dat internal audit de eigen organisatie actief toetst op business continuity management (BCM) én crisismanagement. De third line of defense kan hiermee een belangrijke en actieve bijdrage leveren aan het verminderen van kwetsbaarheden bij een incident of crisis en aan het vergroten van de veerkracht van de organisatie.

Het voorkomen van risico's staat bij de meeste organisaties hoog op de agenda. De aandacht hiervoor komt voort uit de dynamiek en complexiteit waarin organisaties opereren én uit een toename van eisen vanuit de omgeving. Bijvoorbeeld de steeds complexer wordende toeleveranciersketen door globalisering, een toename van eisen op het gebied van wet- en regelgeving (zoals de privacywetgeving) of een toename aan eisen die door klanten worden gesteld (duurzaamheids-, leverbetrouwbaarheids- en kwaliteitseisen). Organisaties proberen het hoofd te bieden aan deze ontwikkelingen door in control te zijn en te blijven.

In control

AUDIT

MAGAZINE

Voor veel organisaties wordt het in control zijn voornamelijk toegespitst op het inrichten van een adequate governancestructuur, een planning & controlcyclus en de implementatie van het three-lines-of-defense model. Hierbij wordt een focus aangebracht op het mogelijk voorkomen van risico's. Met andere woorden, het voorkomen van onvoorziene gebeurtenissen die kunnen leiden tot onaangename verrassingen of, erger nog, die het voortbestaan van de organisatie bedreigen.



Echter, de praktijk wijst uit dat niet alle risico's kunnen worden voorkomen. Geen enkele organisatie is incidentvrij. Er kan namelijk altijd iets misgaan. Soms met verstrekende gevolgen voor individuen, de financiële situatie of zelfs het voortbestaan van de organisatie. In iedere organisatie vinden nu eenmaal incidenten plaats waarop niet vooraf is en kan worden geanticipeerd. Dit kan leiden tot een verstoring van de bedrijfscontinuïteit en in sommige gevallen zelfs tot een crisis.

Binnen het risicomanagement zien wij (beroepsmatig) dan ook een ontwikkeling naar een meer integrale toepassing van

risicomanagement, te weten de 'resiliencegedachte'. Vanuit deze resiliencegedachte wordt structureel gewerkt aan het verminderen van kwetsbaarheden én het vergroten van de veerkracht van organisaties indien risico's zich toch voordoen (de wat-als vraag). De twee disciplines die zich daar voornamelijk op richten zijn BCM en crisismanagement. Om deze twee disciplines op een juiste wijze in te zetten en te borgen, gaan we in op de belangrijke rol die de auditpraktijk hierbij, in onze optie, kan en hoort te spelen.

In de kern bestaan er twee disciplines voor veerkracht: BCM in een situatie waarbij de bedrijfscontinuïteit bedreigd kan worden en crisismanagement bij een grote crisis waarin het bestaansrecht van de organisatie afneemt

Wat is BCM én crisismanagement?

Organisaties werken dagelijks aan hun weerbaarheid. Dit doen ze deels door te voorkomen dat risico's ontstaan. Werken aan weerbaarheid vraagt ook om goed en tijdig te reageren op risico's die toch ontstaan. Dit noemen we 'veerkracht en weerbaarheid'. Maar hoe organiseer je nu veerkracht en weerbaarheid? In de kern bestaan er twee disciplines voor veerkracht: BCM in een situatie waarbij de bedrijfscontinuïteit bedreigd kan worden en crisismanagement bij een grote crisis waarin het bestaansrecht van de organisatie afneemt. We lichten beide disciplines kort toe.

BCM

Bedrijfscontinuïteit is het vermogen van de organisatie om na een bedrijfsverstoring incident producten of diensten te kunnen blijven leveren, binnen van tevoren gedefinieerde en geaccepteerde serviceniveaus. Om dit te kunnen bereiken richt een organisatie BCM in. BCM identificeert potentiële bedreigingen en de impact die deze bedreigingen hebben op de continuïteit van de bedrijfsvoering. Deze discipline voorziet in een structuur voor het realiseren van organisatorische weerbaarheid en veerkracht. Dit door vooral gericht te investeren in de bekwaamheid van de organisatie om een tijdig en voldoende herstel te realiseren. Herstel door de juiste prioritering, snelheid en capaciteit, zodat de belangen van stakeholders, de reputatie, het merk en waardecreërende activiteiten optimaal worden beschermd. De belangrijkste norm voor BCM is de certificeerbare norm NEN ISO 22301:2012. Deze norm is een richtlijn en geeft duiding aan hoe de verschillende eisen van BCM moeten worden geïnterpreteerd en toegepast.

Crisismanagement

Een crisis is een van de ernstigste uitdagingen waarvoor een organisatie zich gesteld kan zien. Een crisis is een abnormale en buitengewone verstoring, impactvol, en gekenmerkt door een onstabiele en complexe situatie die een mogelijke bedreiging vormt voor de strategische doelstellingen, veiligheid van medewerkers of omgeving, reputatie en, uiteindelijk, de continuïteit en het voortbestaan van een organisatie. Crisismanagement richt zich op de brede impact die een groot scala aan ernstige gebeurtenissen (denk aan fraude, datalekken, brand, ernstige ongevallen, et cetera) kan hebben op de reputatie en het voortbestaan van de 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 voor crisismanagement bieden organisaties handvatten voor het ontwikkelen van hun bekwaamheden om met crisissituaties om te gaan en deze te verbeteren. Niet elke uitdaging op het gebied van bedrijfscontinuïteit is een crisis en niet elke crisis gaat alleen over het herstellen van producten en/of diensten. De impact bij een crisis is dan breder dan alleen bedrijfscontinuïteit. Wanneer bijvoorbeeld een gebouw uitbrandt vindt uitwijk van de productie plaats, er kunnen slachtoffers zijn die tevens veel media-aandacht genereren en er is zorg voor familieleden en collega's.



Waarom noodzakelijke verbreding van risicomanagement?

Een studie uitgevoerd onder meer dan vierhonderd business executives toont aan dat organisaties steeds meer het belang inzien van het verbreden van risicomanagement naar het reeds genoemde resilienceconcept, waarbij risicomanagement, BCM en crisismanagement met elkaar verbonden worden.¹ Het overgrote deel van de business executives (80%) is ervan overtuigd dat resilience zelfs een absolute prioriteit is om op langere termijn te overleven.

Het door Aon uitgevoerde onderzoek, genaamd 'Global Risk Management Survey 2019', laat zien dat bedrijven minder goed voorbereid zijn op risico's. Reputatieschade wordt genoemd als de op een na grootste zorg. Opvallend is dat de risicomanagers melden dat zij nog nooit zo weinig voorbereid zijn op risico's, omdat veel van de toprisico's, zoals economische teruggang en toenemende concurrentie, onverzekerbaar zijn.² Naar onze mening komen bij een juiste focus op de onverzekerbare risico's de onderwerpen discontinuïteit en crises meer tot hun recht.

Sinds 2015 wordt door COT, Instituut voor Veiligheids- en Crisismanagement (onderdeel van Aon) onderzoek verricht, waaruit blijkt dat de kwetsbaarheid voor crises toeneemt. Ook is gebleken dat bedrijven/organisaties steeds vaker en eerder een daadwerkelijke crisis ervaren. De voorbereidingen op crises zijn vaker een eigen keuze en tegelijkertijd is ook compliance steeds vaker een reden om te investeren in de voorbereiding op crises.³

Regeldruk leidt tot meer verplichte audits, waardoor er minder ruimte is voor audits naar complexe onderwerpen als BCM en crisismanagement

Is de internal auditpraktijk voldoende voorbereid?

Deze belangrijke verbreding van risicomanagement naar BCM en crisismanagement heeft consequenties voor de reikwijdte van de auditpraktijk. Internal audit vervult immers een essentiële rol om een onafhankelijk en objectief oordeel te vellen over het in control zijn van de organisatie. Hierbij is het verminderen van kwetsbaarheden binnen de organisatie en het vergroten van de veerkracht van organisaties een belangrijk onderdeel. Wij zien in onze adviespraktijk dat deze veranderende rol voor internal audit een uitdaging kan vormen. Dit komt door de volgende factoren:

1. In de meeste control frameworks ontbreken duidelijke normen voor BCM

AUDIT

MAGAZINE

en crisismanagement – Het uitvoeren van audits kent een zekere cyclus, te weten de audit en de opvolgaudit. De thema's zijn in eerste instantie meer gericht op compliance en het meer klassieke risicomanagement. De bredere kijk op resilience – waar BCM en crisismanagement onderdelen van zijn – wordt daarom nog niet altijd toegepast. Daarnaast wordt om de auditagenda vast te stellen veel gebruikgemaakt van richtlijnen en informatie zoals door (internationale) auditororganisaties worden gepubliceerd. In deze richtlijnen wordt niet of nauwelijks gewezen op het belang van een BCM- en crisismanagementaudit. Wij zien dat er meer aandacht is voor gerelateerde onderwerpen zoals cybersecurity en dataprotectie die door het IIA als hot topic worden beschreven. Tot slot ligt er nog een uitdaging om BCM en crisismanagement binnen het opleidingscurriculum van internal auditors te plaatsen, zodat auditors zelf over voldoende kennis en vaardigheden beschikken om onafhankelijk en adequaat te kunnen toetsen en het topmanagement van de juiste adviezen te kunnen voorzien.

2. De toename van wet- en regelgeving zorgt voor regeldruk – De toename van wet- en regelgeving vanuit de EU zorgt ook voor regeldruk bij internal audit. Vanuit de EU wordt steeds vaker opgelegd dat periodieke audits verplicht zijn, wat leidt tot een toename van wettelijk verplichte audits. In onze adviespraktijk zien we dat regeldruk leidt tot meer verplichte audits, waardoor er minder ruimte is voor audits naar complexe onderwerpen als BCM en crisismanagement. In de meeste gevallen worden eerst de wettelijk verplichte audits op de agenda geplaatst, pas daarna komen eventuele andere onderwerpen in beeld.
3. De rol van de diverse stakeholders bij de auditplanning – Welke rol de directie c.q. het bestuur speelt bij de bepaling van de auditagenda verschilt per organisatie. In ieder geval levert de internal auditor een aanzet hiertoe en houdt hij hierbij rekening met eventuele specifieke opdrachten. De internal auditor is zich niet altijd bewust van het belang om BCM en crisismanagement als onderwerp op de agenda te plaatsen. Dit wordt ook nog eens gevoed door het strategische niveau dat zich ook niet altijd bewust is van de noodzaak om BCM en crisismanagement te laten toetsen.

In veel gevallen vertrouwt het strategische niveau te veel op het operationele vermogen van organisaties om met ernstige calamiteiten om te gaan en zijn ze zich onvoldoende bewust van hun eigen rol en verantwoordelijkheid. Immers, het wel of niet overleven van een ernstige crisis is in een grote mate afhankelijk van het op dat moment getoonde leiderschap. In veel gevallen komen BCM en crisismanagement pas op de agenda nadat de betreffende organisatie een ernstig(e) incident/crisis heeft meegemaakt, of omdat er een directe eis ligt uit hoofde van compliance. Hier ligt dus een mooie uitdaging voor de risicomanager in samenwerking met internal audit.



Beoordelen en adviseren

Uit het hiervoor genoemde blijkt dat de internal auditfunctie een belangrijke rol kan en – in onze optiek – behoort te spelen in het beoordelen van veerkracht en weerbaarheid en het adviseren hierover. Om deze redenen stelt de NBA-LIO in samenwerking met Aon/COT in 2019 een handleiding op die bedoeld is als praktische gids en hulpmiddel voor internal auditors om hun organisaties te toetsen op BCM en crisismanagement.⁴

Op basis van de constatering hiervoor komen wij tot de volgende aanbevelingen die ertoe bij kunnen dragen dat BCM en crisismanagement veel meer in beeld komen bij internal audit:

1. *Ontwikkel als internal auditor kennis van BCM en crisismanagement en hanteer de relevante normen als toetsingskader voor de audits* – Beide onderwerpen hebben normen die door internal auditors gebruikt kunnen worden om de eigen organisatie te toetsen. IIA heeft bijvoorbeeld de Practice Guide business continuity management ontwikkeld. In 2018 is een Europese norm gepubliceerd die richtlijnen bevat voor crisismanagement, de CEN/TS 17091 'Crisis management – Guidance for developing a strategic capability'. Deze norm beoogt organisaties handvatten te bieden om hun bekwaamheid om met crisissituaties om te gaan, te ontwikkelen en te verbeteren.
2. *Breng het control framework op een lijn met het brede risicoprofiel* – In de huidige basis voor het beoordelen van de risico's en maatregelen dienen ook continuïteits- en crisissrisico's opgenomen te worden. Op deze manier worden in het control framework zowel onderwerpen meegenomen die over preventie als over herstel/repressie gaan.
3. *Agendeer BCM en crisismanagement bij de riskmanager en RvC/RvT* – Neem als internal audit het initiatief om het control framework te verbreden naar BCM en de crisismanagement. Ga in gesprek met de riskmanager en de RvC/RvT om het belang te benadrukken van deze verbreding in het licht van alle noodzakelijke maatregelen om risico's te voorkomen én deze risico's tijdig en adequaat te beheersen en te herstellen. Is de auditagenda vol? Maak dan gebruik van een externe partij.

Noten

1. 'Organisational Resilience: Building an enduring enterprise', *The Economist Intelligence Unit*, 2015.
2. Aon voert de '[Global Risk Management Survey](#)' sinds 2007 elke twee jaar uit. In het laatste kwartaal van 2018 ondervroeg Aon 2672 risicomangers, CRO's, CFO's en andere verantwoordelijken in 60 landen en 33 bedrijfstakken.
3. COT voert sinds 2015 periodiek een onderzoek uit naar [crisismanagement in het bedrijfsleven](#).
4. Deze richtlijn is toepasbaar binnen elke organisatie en zal in het najaar van 2019 beschikbaar zijn voor internal auditors. Zodra de handleiding is afgerond, wordt dit bekendgemaakt op onder andere de website van NBA, Aon en COT.

AUDIT

MAGAZINE

Over

Abderrahman Kaouass is managing consultant bij COT (onderdeel van Aon) en gespecialiseerd in strategische organisatievraagstukken rond crisismanagement. Hij adviseert organisaties bij de professionalisering van het crisisvermogen.

Iwan Drost is managing consultant bij Aon Global Risk Consulting en adviseert organisaties bij de implementatie van risicomanagement en in het bijzonder BCM. Hij is lid van de NEN BCM-commissie.

Saida Nhass is managing consultant bij Aon Global Risk Consulting en is in haar hoedanigheid van practice lead compliance consulting verantwoordelijk voor de advisering van organisaties op het gebied van compliance.

Tags: crisismanagement

Bron url: <https://auditmagazine.nl/artikelen/waarom-bcm-en-crisismanagement-belangrijk-is/>