AUDIT
MAGAZINE

ARTIKELEN | 3 FEBRUARI 2021

NIET VERRAST WORDEN DOOR HET (ON)VERWACHTE

Auteur: G. Kogenhop (Hon.) MBCI
Beeld: Markus Winkler - Adobe Stock
Leestijd: 9 min



Business continuity management (BCM) gaat over het beschermen van uw organisatie tegen de gevolgen van omvangrijke verstoringen en (on)bekende risico's. Anno 2021 geen overbodige luxe. Helaas denken velen nog steeds onvoldoende na over hoe een calamiteit gestructureerd aan te pakken en te overleven, terwijl de risico's zich voor menige sector ontwikkelen in een ongunstige richting.

Gebeurtenissen als de brexit en de coronacrisis zijn actueel, maar er volgt helaas meer. Wat, wanneer en hoe blijft ongewis, maar dat u zich zo optimaal mogelijk dient voor te bereiden, lijkt duidelijk. En als er al continuïteitsplannen zijn binnen een organisatie en er aldus inspanningen worden verricht in dit kader, dienen organisaties wel zorg te dragen voor een effectief plan B wanneer dit nodig is, als het er echt op aankomt. Geen papieren tijgers dus, bijvoorbeeld ter 'geruststelling' van de buitenwacht. Hier spelen naast oefenen en testen, onderhouden en verbeteren, ook interne audits een belangrijke rol. ISO 9001 (kwaliteit), ISO 14001 (milieuzorg) en bijvoorbeeld ISO 27001 (informatiebeveiliging) zijn inmiddels bekende normen binnen organisaties. Deze zijn, met in het vizier het 'risk based thinking'-thema van de kwaliteitsnorm, te verrijken door direct aan het bestaande managementsysteem business continuity management toe te voegen, al dan niet gecertificeerd conform ISO 22301.

AUDIT
MAGAZINE

Halsstarrig de andere kant op blijven kijken, de kop in het zand steken of denken: dat overkomt mij niet, is geen verstandige strategie

Vooruitkijken

Verkoop, productie, logistiek, eigenlijk alle functies binnen de onderneming zijn voornamelijk bezig met de dagelijkse uitvoering van activiteiten, de plannen opgesteld door het management en de huidige en wellicht toekomstige orders. Terwijl de aandacht minder is gericht op bekende en onbekende risico's die het mogelijke voortbestaan van de onderneming ernstig kunnen bedreigen. Het halen van de (financiële) doelstellingen staat bovenaan elke agenda en dat is volledig begrijpelijk. Business continuity, oftewel – in goed Nederlands – bedrijfscontinuïteit (BC), en dan natuurlijk iets specifieker het managen hiervan, verdient zeker een meer prominente plek op diezelfde agenda. De pandemie heeft dit wel duidelijk gemaakt. Indien de continuïteit van de onderneming in gevaar komt als direct gevolg van een ernstig incident, komen clichés als: 'Hadden we maar …' naar voren. Helaas dan wel vaak té laat.

Aanvaardbare tijdskaders

Bedrijfscontinuïteit kan worden omschreven als het vermogen van een organisatie om tijdens een verstoring producten en diensten met een vooraf vastgestelde capaciteit binnen aanvaardbare tijdskaders te blijven leveren (ISO 22301:2019). Het belangrijkste deel uit deze definitie is 'een vooraf vastgestelde capaciteit binnen aanvaardbare tijdskaders', daar dit betekent dat u dient te weten wat die capaciteit is en wat deze aanvaardbare tijdskaders zijn. 'Voorbereiding is 90% van het resultaat', zouden we op een BCM-tegeltje kunnen zetten, dat is wel waar het over gaat. Zo optimaal mogelijk voorbereid zijn. BCM dientengevolge is het complete managementproces dat mogelijke gevaren met betrekking tot de continuïteit van de bedrijfsvoering vaststelt en een kader schept voor het opbouwen van weerstandsvermogen en veerkracht ('resilience'). Door effectief reageren worden de organisatiebelangen, de reputatie alsmede het merk, bewaakt. Tevens wordt de uitvoering van de waardecreërende activiteiten gewaarborgd.

Engeland loopt voorop

In de ICT is het managen van continuïteit dé nummer 1-prioriteit. Sterker nog, wij eisen van de ICT-functie binnen onze organisatie minimaal 99,99% betrouwbaarheid en uptime. Zeker wanneer deze is uitbesteed aan een derde partij, wat steeds vaker het geval is. De bekende cloud, oftewel de opslagruimte van iemand anders. Er mag niets gebeuren en als er iets gebeurt, moeten we zo snel mogelijk verder kunnen zonder al te veel vertraging en dataverlies. De afgelopen jaren is men zich gaan realiseren dat dit eigenlijk zou moeten gelden voor álle belangrijke functies binnen de organisatie. Engeland loopt daarin duidelijk voorop. Het land heeft rond de eeuwwisseling in korte tijd een groot aantal rampen en bijna-rampen te verwerken gekregen. Denk hierbij bijvoorbeeld aan de grootste naoorlogse brand bij Hemel Hempstead in december 2005 (Hertfordshire Oil Storage Terminal), diverse grote overstromingen, terroristische aanslagen en gevallen van gekkekoeienziekte, vogelgriep en mond- en klauwzeer. In het geval van de enorme brand in Hemel Hempstead is uiteindelijk driekwart van de bedrijven op het aangrenzende bedrijventerrein failliet gegaan als direct aanwijsbaar gevolg hiervan. Ook vliegveld Heathrow ondervond direct nadelige gevolgen van deze brand, aangezien een zeer groot deel van de benodigde kerosine door deze Oil Storage Terminal werd geleverd.

© AuditMagazine.nl



Nadelige gevolgen

Wat we hiervan kunnen leren is dat niet alleen het bedrijf zelf de nadelige gevolgen van een incident ondervindt, maar ook buren, klanten en wellicht zelfs leveranciers, die (voorlopig) een afnemer kwijt zijn. Dichter bij huis zijn daar ook voorbeelden genoeg van. De continue cyberdreiging (MAERSK en de Universiteit van Maastricht); het voor langere tijd uitvallen van mobiel telefoonverkeer, 112, PIN, elektriciteit en internet (waar we eigenlijk niet meer zonder kunnen). Denk echter ook aan de mogelijke gevolgen van een staking, de beschikbaarheid van belangrijke grondstoffen of verpakkingsmaterialen die u nodig hebt. Of die grote, trouwe klant die niet meer voor u kiest.

Langdurige aanslag

En dan momenteel de coronacrisis. Een verstoring van hoe wij werken die al bijna een jaar voortduurt. Een langdurige aanslag op de continuïteit van veel organisaties. Ondanks dat van de goed voorbereide organisaties mét een continuïteitsplan een deel geen specifiek scenario had voor een pandemie, konden deze organisaties tóch adequaat reageren. Dit heeft te maken met de inrichting van het business continuity management system (BCMS). Ook al is er geen specifiek plan en denkt u heel even: dit had ik niet verwacht!, het feit dat de organisatie voorbereid is op onverwachte (en verwachte) gebeurtenissen leidt tot de mogelijkheid snel de controle terug te pakken door onderdelen uit verschillende wel aanwezige scenario's samen te voegen en te zoeken naar de optimale mix. Zo ook in dit geval. De klassieke, standaard reactie op een pandemie is: 'We hebben onvoldoende mensen om onze (kritische) activiteiten uit te voeren'. Dit bleek maar in enkele situaties het geval. Buiten het van overheidswege sluiten en verbieden van activiteiten zoals bijvoorbeeld in de horeca, reisbranche, entertainment en sportscholen, waren bezettingsproblemen bij bedrijven die wel door konden draaien, niet echt een showstopper. Waar thuiswerken mogelijk was, kon men dit vrij snel op een redelijke wijze organiseren, gebruikmakend van de vaak niet-optimale oplossingen als Zoom, Microsoft Teams, BlueJeans, GoToMeeting en andere vergader/meeting-apps. Maar toch, het leidde tot werkbare situaties. Soms vanaf de zolder of aan de keukentafel, met kinderen op de voor- of achtergrond. We konden door.

Optimale voorbereiding

Veel groter waren de problemen met toeleveranciers (grondstoffen, producten en diensten) die niet konden leveren door quarantainemaatregelen of simpelweg omdat er geen transport mogelijk was. Men werkte in die gevallen met alternatieve leveranciers of bronnen conform de hiervoor genoemde scenario's. Dit gold ook voor klanten die niet bereikt konden worden (door de lucht of over de weg naar het buitenland) of die (verplicht) gesloten waren. In enkele gevallen was er de mogelijkheid over te schakelen naar alternatieve afzetgebieden of klantgroepen. De optimale voorbereiding op een ernstige verstoring of crisis is dan ook scenariogedreven, rekening houdend met de aanwezige (on)mogelijkheden. En door in dit geval de combinatie van 'geplande en geoefende' acties te initiëren, werd de schade

beperkt. De scenario's waar voornamelijk uit geput kon worden, waren gerelateerd aan risico's leidend tot:

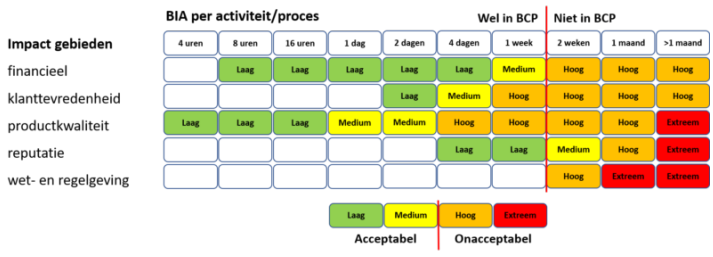
- onvoldoende personeel;
- de werklocatie is niet beschikbaar/toegankelijk/bruikbaar;
- een belangrijke leverancier levert niet;
- transport/vervoer is niet mogelijk;
- klanten kunnen de levering niet ontvangen.

Onder de huidige economische omstandigheden zijn vele bedreigingen actueler dan ooit. Wanneer u dit zo leest, slaat de angst u wellicht om het hart. Dat is misschien wel goed, zeker wanneer u niet goed voorbereid bent. Halsstarrig de andere kant op blijven kijken, de kop in het zand steken of denken: dat overkomt mij niet, is in ieder geval geen verstandige strategie.

'Voorbereiding is 90% van het resultaat', kunnen we zo op een BCM-tegeltje zetten. Dat is namelijk wel waar het over gaat. Zo optimaal mogelijk voorbereid zijn

Bepaal de scope

In twee stappen analyseren we de organisatie. Uitgaande van een organisatie, bepaalt u allereerst de belangrijkste producten en/of diensten (of alles vanzelfsprekend). Nadat deze zijn vastgesteld worden alle activiteiten tegen het licht gehouden en die activiteiten geselecteerd, die een directe bijdrage leveren aan het tot stand komen van deze producten en/of diensten (of alles vanzelfsprekend), de scope. Deze binnen de scope vallende activiteiten worden geanalyseerd door middel van de bedrijfsimpactanalyse (BIA) en beoordeeld, in geval van stilstand, op gevoeligheid voor een aantal van tevoren vastgestelde impactgebieden (zie *figuur 1*). Dit kan zijn: financiële impact, wat dit betekent voor onze klanttevredenheid, productkwaliteit, reputatie en of het wel of niet voldoen aan wet- en regelgeving. We bepalen een impactschaal, bijvoorbeeld laag, medium, hoog, extreem, en definiëren voor elk een waarde. Impact hoog financieel kan dan zijn: schade als gevolg van margeverlies of extra kosten tussen de € 200.000 en € 500.000. Impact extreem op het gebied van reputatie kan zijn: negatieve landelijke media-aandacht en trending topic social-mediaberichten. Vervolgens bepalen we wat wij niet meer acceptabel vinden. Stel, in alle impactgebieden willen we nooit op het niveau hoog komen. Om te voorkomen dat dit ooit wordt bereikt willen we een plan B hebben (business continuity plan). Na deze vaststelling bepalen we tevens dat wanneer dit niveau hoog wordt bereikt ná één week, we geen plan nodig hebben. Dat geeft ons voldoende tijd om zonder plan adequaat te reageren. Maar wanneer binnen een week dit niveau wordt bereikt, willen we zo optimaal mogelijk voorbereid zijn om niet verrast te worden en mogelijk de controle te verliezen.



Figuur 1. Voorbeeld BIA per activiteit/proces

Grenswaarden

Deze drempelwaarde van één week, zoals hierboven aangegeven, kan overigens ook vier dagen of twee weken zijn. Dit bepaalt u zelf als organisatie. Deze twee drempels, hoog en één week, zijn de grenswaarden als het gaat om

acceptabele impact. De allesbepalende factoren binnen de BIA. We gaan alle activiteiten beoordelen en die activiteiten waarvan we bepalen dat de impact hoog is binnen één week, waarbij het niet uitmaakt op welk impactgebied, markeren we vervolgens als kritisch. De risicobeoordeling (RB) geeft inzicht in welke risico's voor de onderneming reëel zijn, algemene risico's, risico's behorend bij de aard van de activiteiten (advocatenkantoor of chemieconcern) en de vestigingsplaats (nabij water, spoor, tankstation aan de overkant, wie zijn de buren?). Het gaat hier om de kans en de mogelijke impact van het feit dat een bedreiging een ernstige verstoring veroorzaakt. Niet alle risico's kunnen vanzelfsprekend worden uitgesloten en er zal altijd een restrisico overblijven.

Wat gaan we doen?

Na bepaling van de gevaarlijke combinatie van reële risico's en de eerder vastgestelde kritische activiteiten die onze belangrijke producten en/of diensten ondersteunen, dienen de volgende mogelijkheden te worden overwogen:

1. Gaan we dit behandelen/afdekken in continuïteitsplannen (treat)?
2. Accepteren we dit risico (tolerate)?
3. Dragen we dit risico over aan derden door middel van uitbesteding of een vorm van verzekering (transfer)?
4. Beëindigen of veranderen we deze activiteit of schorten we deze op (terminate)?

Vervolgens wordt besloten 'wat vervolgens te doen'. En, nog belangrijker en uitermate krachtig: 'hoe kunnen we het weerstandsvermogen en de veerkracht (resilience) van de organisatie vergroten?' Hoe kunnen we de kritische activiteiten minder kritisch maken en hoe kunnen we de kans of de impact van een bedreiging verlagen? Het vinden van soms eenvoudige mogelijkheden gedurende en na de implementatie van BCM in de onderneming, levert een enorme toegevoegde waarde op. Het tot de conclusie komen dat er enkele uitermate belangrijke medewerkers rondlopen die specifieke kennis en vaardigheden bezitten ('single point of knowledge'), kan leiden tot de beslissing om de vastlegging van procedures en werkvoorschriften nóg strakker te organiseren en tevens de implementatie van plannen met betrekking tot opvolging, kennisdeling en het rouleren van medewerkers tot gevolg hebben.

De invulling

De invulling met betrekking tot 'wat vervolgens te doen' wordt in een belangrijke mate bepaald door een aantal factoren. Ten eerste: welke activiteiten (met de juiste prioriteit) betreft het?, en vervolgens: welke (en hoeveel) mensen en middelen? Denk hierbij aan welke machines, gereedschappen, IT-applicaties, formulieren, leveranciers, nodig zijn om deze uit te kunnen voeren. U hoeft niet altijd direct 100% te functioneren, maar welk percentage dan wel, met welke machines en bezetting, welke producten of diensten voor welke klanten? Gaan bepaalde klanten voor, wilt u uw productportfolio in een bepaalde volgorde opstarten en leveren, of wilt u eerst dat bepaalde processen met voorrang gaan draaien?

Niet alleen het bedrijf zelf ondervindt de nadelige gevolgen van een incident, maar ook buren, klanten en wellicht zelfs leveranciers, die (voorlopig) een afnemer kwijt zijn

Uitwerken scenario's

Er worden diverse scenario's uitgewerkt. Simpelweg gesteld zijn dit scenario's met als uitgangspunt: hoe leveren wij zo snel mogelijk aan onze klanten in de volgende situaties?:

- uitval van ICT (internet, techniek, hack, ransomware);
- onvoldoende mensen (pandemie, staking openbaar vervoer, geen personeelsaanbod);
- uitval van nutsvoorzieningen (elektra/water/gas);
- ontoegankelijke locatie (wegafsluiting, afgebrand, explosiegevaar bij de buren, coronamaatregelen);

- specifieke scenario's voor uw organisatie (chemie, financiële sector, voedselindustrie, transport & logistiek).

Uiteindelijk bent u dan zo optimaal mogelijk voorbereid op een ernstige verstoring, ook al gebeurt er iets waar u nu nét níet een scenario voor hebt ingericht. De denk- en werkwijze zit nu in uw genen, dus u zult even verrast zijn, maar niet de controle verliezen.

Logisch controlepunt

Een managementsysteem, en dus ook BCMS, volgt in principe de Deming Cycle: plan-do-check-act, dus alle elementen komen voorbij. Als interne auditor liggen er vele elementen als een soort 'logisch controlepunt' vast. De focus zal echter moeten komen te liggen op de 'do-fase', de feitelijke kern van het BCMS (conform ISO 22301):

- het gebruik van de juiste tijdlijn in de BIA, impactgroepen, maatstaven, drempelwaarden en bijbehorende definities;
- de juistheid van de scenariovaststelling op basis van de risicobeoordeling;
- de juiste detailniveaus van de (deel)plannen – worden de hersteldoelstellingen gehaald;
- de optimale samenwerking van het crisis managementteam en het business continuity managementteam – werkt dit op het 'moment suprême'?;
- borging en continu verbeteren;
- check- en act-fasen – controls van de 'deliverables';
- functies, rollen en verantwoordelijkheden (governance);
- budgettaire ruimte voor verbeteringen;
- topmanagement commitment, involvement en engagement.

Het doel moet u te allen tijde voor ogen blijven staan. Dit is namelijk het garanderen van bedrijfscontinuïteit, het vermogen van een organisatie om tijdens een verstoring producten en diensten met een vooraf vastgestelde capaciteit binnen aanvaardbare tijdskaders te blijven leveren. De invulling van het managementsysteem is de wijze waarop we dit doen en de interne auditfunctie levert een belangrijke bijdrage aan de optimale inrichting en uitvoering hiervan.

Over
Gert Kogenhop is directeur van bcm^{+}. Hij is voorzitter van de BCM- en crisismanagement-normcommissie bij NEN. gk@bcmplus.nl

Tags: Business continuity management, crisismanagement

Bron url: https://auditmagazine.nl/artikelen/niet-verrast-worden-door-het-onverwachte/