

PLATFORM VOOR MVO EN KWALITEITSMANAGEMENT

# KWALITEIT IN BEDRIJF

# 5

JULI 2017



**ARBO**  
DE ARBOWET WIJZIGT:  
HOE GAAT U VOLDOEN?

**ACCOLADE**  
VERANDEREN VAN  
ONDEROP

**ISO 20400**  
HOE GAAN WE  
DUURZAMER INKOPEN?

# HOE VOORBEREID BENT Ú OP HET ONVERWACHTE?

**MEDICATIEVEILIGHEID**  
MEDEYE BRENGT FOUTLOZE  
TOEDIENING BINNEN BEREIK

Business Continuity Management

# HOE VOORBEREID BENT Ú OP HET ONVERWACHTE?

Business Continuity Management (BCM) gaat over het beschermen van uw organisatie tegen de gevolgen van omvangrijke verstoringen en (on)bekende risico's. Dit is anno 2017 geen overbodige luxe. Elke organisatie heeft wel een crisisplan, -team en -organisatie, maar helaas denken nog velen onvoldoende na over hoe ze een calamiteit gestructureerd operationeel dienen aan te pakken. Is er een goed beeld van de huidige bedreigingen en mogelijke risico's? Denk hierbij bijvoorbeeld aan de stroomstoring in januari in de regio Amsterdam en de ransomware-aanvallen van kortgeleden. Voor beiden geldt, dat was niet de eerste keer en zeker ook niet de laatste. Er verandert in de ICT-wereld heel veel en gezien de alleen maar toenemende afhankelijkheid hiervan moet dit wel tot bedenkelijk fronsen en voor sommigen zelfs slapeloze nachten leiden. Leidt de strakke Supply Chain met uitdagende levertijden (Just In Time), planningen en beperkte flexibiliteit soms niet tot onverantwoorde situaties? Extra aandacht voor dit onderwerp op de directieagenda lijkt logisch, tóch? Hoe staat het er bij u voor? Hoe kunt u beoordelen wat de status is als het gaat om bedrijfscontinuïteit, uw BCM-Readiness zogezegd?

Door Gert Kogehop, bcm+

Verkoop, productie, logistiek; eigenlijk alle functies binnen de organisatie zijn voornamelijk bezig met de dagelijkse uitvoering van activiteiten, de plannen opgesteld door het management, de huidige en wellicht toekomstige orders... Terwijl de aandacht minder is gericht op bekende en onbekende risico's die het voortbestaan van de organisatie ernstig kunnen bedreigen. Het halen van de (financiële) doelstellingen staat bovenaan elke agenda en dat is niet meer dan logisch. Business Continuity oftewel in goed Nederlands bedrijfscontinuïteit — en dan natuurlijk iets specifieker het managen hiervan — verdient zeker een meer prominente plek op diezelfde agenda dan momenteel het geval is. Indien de continuïteit van de organisatie in gevaar komt als direct gevolg van een ernstig incident, komen clichés als: 'Hadden we maar ...' naar voren, helaas dan té laat. Hadden is wanneer hebben is geweest!

Bedrijfscontinuïteit kan worden omschreven als het vermogen van een organisatie om te plannen voor en te reageren op incidenten met als direct gevolg een ernstige

verstoring van de organisatie, om zodoende te waarborgen dat men operationeel op minimaal een van tevoren vastgelegd niveau kan functioneren. 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. Door effectief reageren worden de organisatiebelangen, de reputatie alsmede het merk bewaakt. Tevens wordt de uitvoering van de waardecreërende activiteiten gewaarborgd.

In de ICT is het managen van continuïteit dé nummer één prioriteit. Sterker nog, wij eisen van de ICT-functie binnen onze organisatie minimaal 99,9% betrouwbaarheid en 'uptime' en zeker ook wanneer deze functie is uitbesteed aan een derde partij, wat steeds vaker het geval is. Heeft u zich ooit gerealiseerd dat een geaccepteerde downtime van 0,1% toch nog bijna negen uren per jaar zijn? En wat is die garantie waard? Dat zal maar net bijvoorbeeld op de drukste dag zijn, of drie keer drie uren tijdens piektijden of vlak voor een deadline. Een recent

voorbeeld: Cloud provider Amazon Web Services (AWS) kreeg in februari van dit jaar te maken met een uitval van liefst vijf uren. Dit leidde tot een enorme impact voor onder andere populaire online diensten als Netflix, Tinder en Airbnb en zij 'garanderen' een beschikbaarheid van 99,9999% ... voor wat het waard is.

Wilt u daar niet op voorbereid zijn of bent u van mening dat dit soort incidenten altijd bij anderen gebeuren en niet in uw organisatie, omdat u het uitstekend voor elkaar heeft? Er mag niets gebeuren en als er iets gebeurt, moeten we zo snel mogelijk verder kunnen zonder al te veel vertraging en dataverlies. Het antwoord van de ICT-functie op deze (terechte) eisen is dat er onder andere back-upprocedures zijn ontwikkeld en dezelfde 'realtime data' op verschillende plaatsen (in de wereld) beschikbaar is gemaakt. De hersteltijden van applicaties en apparatuur plus mogelijk dataverlies door uitval is speerpunt nummer één. Redundancy is momenteel het magische woord in dit kader. 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. Klanten, in welke vorm dan ook, zullen het in ieder geval zeker op prijs stellen wanneer u zich voorbereidt op het onverwachte.

#### **HOE STAAT U ERVOOR?**

Beoordeel eens de huidige situatie binnen uw organisatie door een aantal vragen te stellen en met het managementteam te discussiëren over nut en noodzaak van het implementeren van een Business Continuity Management System (BCMS). Een kleine moeite met wellicht een verrassende uitkomst. Indien u het inderdaad uitstekend geregeld heeft, kunt u gerust gaan slapen: 'Keep Calm, Carry On and Sleep Well'. Echter: Awareness is het begin van Preparedness.

#### **DE BCM-READINESS ANALYSE**

In eerste instantie gaat het om een fundamentele discussie binnen het managementteam, namelijk: 'Weten we wat er minimaal nodig is in de organisatie om de gestelde doelstellingen te halen en zo niet:

'Hoe bepalen we dit?'. Dit moet absoluut niet aangevlogen worden vanuit een soort bangmakerij of 'vermeende' risico's. Het gaat over de bepaling van die producten, diensten en in het verlengde daarvan activiteiten, die essentieel zijn voor de organisatie om de doelstellingen te halen. Vanuit een analyse van alle activiteiten blijkt uiteindelijk wat de voor de organisatie meest kritische activiteiten zijn en dus welke de basis vormen voor de herstelstrategie. Wat moet er in welke volgorde gebeuren om in geval van een calamiteit of crisis de juiste keuzes te maken conform onze strategie?

Daarna volgt de bepaling van de omzet die we minimaal nodig hebben, hoeveel klanten, hoeveel en welke mensen en middelen, de ICT-behoefte (systemen en applicaties), welke leveranciers hebben we minimaal nodig, enzovoort. Dit geldt voor zowel de normale bedrijfsvoering, als ook voor wat nodig is om te overleven na een ernstig incident, bijvoorbeeld op een andere locatie. Nadat vastgesteld is wat deze niveaus zijn, ligt de doelstelling op tafel, namelijk: 'Vanuit een continuïteitsperspectief mogen we hier

nooit onder komen, dus hoe gaan we dit voorkomen en wat gaan we aldus doen?'. Dit is een exercitie die niet tijdrovend is, maar die wel uitermate belangrijk is om een beeld te kunnen vormen van de situatie.

U bent zojuist tot de wellicht reeds lang bekende, maar misschien weggeschoven conclusie gekomen dat u van vele zaken, deels buiten uw macht, afhankelijk bent. Dit is dan direct ook de volgende fase van de analyse.

afhankelijkheid is 'Die ene leverancier waarvoor geen alternatief voorhanden is' (Single Sourcing). Heeft u de afhankelijkheid van uw belangrijkste leveranciers wel eens geanalyseerd? Regelmatig wordt die afhankelijkheid zelfs (on)bewust gecreëerd door de doelstellingen van de afdeling inkoop. De beste prijs bij een leverancier wordt immers vaak verkregen door deze alles te laten leveren, door exclusiviteit te verlenen. Goeie deal, maar de bijwerking is het creëren van een onge-

stroomuitval, extreem winterweer of een griep epidemie bijvoorbeeld, door wat we doen (een bank kent andere bedreigingen dan een staalconstructiebedrijf of een bakkerij) en waar we gevestigd zijn (naast water, een vliegveld, een chemiebedrijf of een spoorlijn).

Na bepaling van de 'gevaarlijke' combinatie van bedreigingen, risico's en de eerder vastgestelde activiteiten die onze belang-

## 'HET GAAT OM HET BALANCEREN TUSSEN RISICO'S EN MOGELIJKHEDEN'

Deze afhankelijkheid speelt een cruciale rol in dit geheel. Het beperken van de gevonden afhankelijkheden is de eerste verbetering die u kunt 'scoren'. Indien u goed in beeld heeft hoe afhankelijk u bent van mensen — of soms zelfs van één specifiek persoon in de organisatie (Single Point of Knowledge) — des te beter u hierop kunt reageren en anticiperen door bijvoorbeeld optimalisatie van de vastlegging van werkinstructies, kennisdeling, job rotation of succession planning. Hetzelfde geldt voor de afhankelijkheid van ICT, een specifieke machine of een specifiek proces (Single Point of Failure). Een ander bekend fenomeen in het kader van

wenste afhankelijkheid. Ga op zoek naar de afhankelijkheden in uw organisatie en laat u niet verrassen door deze vaak te verhelpen bedreigingen. 'Voorbereiding is 90% van het resultaat' is een oude en misschien wel afgezaagde tegeltjeswijsheid, maar in dit geval een goed advies.

Voorts dient men zich de vraag te stellen: 'Weten wij wat de bedreigingen en risico's zijn die kunnen leiden tot een situatie waarin we onder (één van) de vastgestelde minimumniveaus komen?'. Denk hierbij aan de bedreigingen die voor iedereen gelden, zoals brand, ICT-storing,

rijke 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 middels uitbesteding of een vorm van verzekering (Transfer)?
4. Beëindigen/opschorten/veranderen van deze activiteit (Terminate)?

Wanneer u uw risico's en uw eigen organisatie kent, dan hoeft u niet te vrezen voor een ernstig incident. Indien u uw eigen organisatie en uw prioriteiten goed kent, maar niet weet welke risico's u mogelijk loopt, dan wordt de kans op een acceptabele uitkomst in geval van een ernstig incident tot de helft gereduceerd. Wanneer u geen enkel inzicht heeft zal het resultaat waarschijnlijk onbevredigend of zelfs desastreus zijn.

Onderzoek vervolgens wat er al is op alle hiervoor genoemde gebieden binnen de organisatie. Zijn er bijvoorbeeld al eerder bedrijfsimpactanalyses gemaakt? Is er al eens een risicoanalyse gemaakt vanuit een continuïteitsperspectief? Hebben we alternatieve werkwijzen en wellicht (productie)locaties, hebben we meerdere leveranciers voor onze belangrijkste behoeften, is er een flexibele 'pool' van mensen die het werk kunnen uitvoeren, zijn er ICT-continuïteitsplannen? Wellicht



Bedreigingen kunnen ook ontstaan vanuit de omgeving waar we gevestigd zijn.

is er meer dan we denken, maar hebben we die nooit gezien als onderdeel van bedrijfscontinuïteitsbeheer.

### WAT LEVERT U DIT OP?

Een BCM-Readiness Analyse op deze wijze uitgevoerd geeft antwoord op de volgende vragen:

- Wat zijn onze belangrijkste producten en diensten?
- Wat zijn de kritische activiteiten die deze mogelijk maken en ondersteunen?
- Wat is het minimale niveau dat we nodig hebben om onze doelstellingen te halen?
- Waar zijn we afhankelijk van?
- Wat zijn onze risico's vanuit een continuïteitsperspectief?



Vervolgens:

- Wat is de status van onze inspanningen om de continuïteit van leveren onder alle omstandigheden en te allen tijde te kunnen garanderen?

En ten slotte:

- Kunnen we het ons veroorloven om niets te doen aan bedrijfscontinuïteitsbeheer, aan Business Continuity Management?

Indien het laatste antwoord 'Nee' luidt, is de implementatie van een Business Continuity Management System een logische vervolgstap of zult u toch zeker de belangrijkste onderdelen een invulling moeten geven.

Het gaat dan om: 'Wat te doen om er voor te zorgen dat we nooit onder de minimaal benodigde niveaus komen die cruciaal zijn voor het succes van onze inspanningen' en nog belangrijker en uitermate krachtig: 'Hoe kunnen we het weerstandsvermogen en de veerkracht van de organisatie verhogen?'. Hoe kunt u de kritische activiteiten minder kritisch maken en hoe kunt u kans op of de impact van een bedreiging verlagen? Het vinden van soms eenvoudige mogelijkheden gedurende en na de implementatie van BCM in de organisatie levert een enorme toegevoegde waarde op. Denk alleen al eens aan de focus op alle mogelijke afhankelijkheden en wat het effect is van het, zo veel mogelijk, verlagen van die

Heeft u de afhankelijkheid van uw belangrijkste leveranciers wel eens geanalyseerd?

afhankelijkheden: of het nu om mensen, leveranciers, ICT of een productielocatie gaat.

Als laatste en zeker niet het minst belangrijke moet erop gewezen worden dat in geval van ernstige bedrijfsschade of erger (faillissement of bedrijfsbeëindiging) de aandeelhouders en andere betrokkenen met een belang, mogelijk de correctheid van de handelswijze van bestuurders tijdens de calamiteit in twijfel kunnen trekken. 'Kennelijk onbehoorlijk bestuur' kan leiden tot individuele aansprakelijkheid van bestuurders op grond van bestuurdersaansprakelijkheid of zelfs onrechtmatige daad. Het mag duidelijk zijn dat wanneer de bestuurder kan aantonen dat een BCMS is geïmplementeerd en er een correcte en zorgvuldige uitvoering van de geproduceerde plannen heeft plaatsgevonden, dit de kans (en impact) hierop uitsluitend positief beïnvloedt.

### DE LINK MET KWALITEITS-MANAGEMENT

Er wordt behoorlijk veel geschreven en gesproken over wat Risk-based thinking binnen kwaliteitsmanagement inhoudt. De hoofdlijnen zijn volgens de ingewijden: 'Zorgen dat bij alles wat u doet, van het begin tot het eind, u rekening houdt met de risico's daarvan' en 'Preventie onderdeel maken van de strategie en de plannen'. Het gaat om het balanceren tussen risico's en

mogelijkheden (Risks and Opportunities): wat is acceptabel en wat niet? Het uitvoeren van een risicoanalyse is echter geen verplicht onderdeel van de standaard. Volgens Charles Corrie, Committee Secretary van ISO 9001, heeft het risicodenken altijd al in de kwaliteitsnorm gezeten, maar is het nooit expliciet benoemd. Hij geeft aan dat het moet worden gezocht op drie gebieden: het niet voldoen van de producten en diensten aan de vereiste specificaties, het niet bereik van de gewenste klanttevredenheid en het niet effectief zijn van het kwaliteitsmanagementsysteem. De relatie tussen BCM en kwaliteit is in dit kader aldus vastgesteld: het niet (kunnen) leveren leidt tot het niet voldoen aan de afspraken (specificaties) en vervolgens tot klantontevredenheid. Kwaliteit en continuïteit gaan hand in hand, Business Continuity Management regelen is kwaliteit leveren én tevens verantwoord ondernemen.

Door het versterken van het weerstandsvermogen en de veerkracht van de organisatie via een geïmplementeerd Business Continuity Management System (BCMS) wordt het overduidelijk dat de kosten van deze inspanning moeten worden gezien als 'cost of doing business'. Oftewel: onderdeel uitmaken van de dagelijkse gang van zaken, hoe wij hier werken en niet iets erbij of er bovenop ('Wat kost dat en wat levert het op?'). Welke organisatie kan het zich veroorloven dit onderwerp niet op de agenda te zetten? **Q**