4.2.2 Eisen uit wet- en regelgeving

Alle managementsystemen behoren uitgevoerd te worden binnen het kader van wet- en regelgeving waarin de organisatie actief is. De organisatie behoort daarom in haar BCMS alle relevante en toepasselijke eisen betreffende wet- en regelgeving die zij onderschrijft en behoeften van belanghebbenden te identificeren en zich hieraan aan te passen.

De informatie betreffende deze eisen behoort te worden gedocumenteerd en actueel te worden gehouden. Nieuwe of aangepaste eisen uit wet- en regelgeving en andere eisen behoren kenbaar te worden gemaakt aan werknemers en andere belanghebbenden waarop de eisen betrekking hebben.

Bij het inrichten, implementeren en onderhouden van het BCMS behoort de organisatie rekening te houden met toepasselijke wettelijke eisen, overige eisen die zij onderschrijft en behoeften van belanghebbenden.

De organisatie behoort te garanderen dat haar BCMS werkt binnen en ter ondersteuning van haar wettelijke verplichtingen en relevante eisen van belanghebbenden.

De organisatie behoort huidige en hangende eisen betreffende wet- en regelgeving op hun locaties te beoordelen. Hiertoe kunnen behoren:

a) reactie op incidenten: met inbegrip van management van noodsituaties, en wetgeving op het gebied van gezondheid, veiligheid en welzijn;

b) continuïteit: dit kan het toepassingsgebied van het programma aangeven of de omvang of de snelheid van de reactie;

c) risico: eisen die het toepassingsgebied of de methoden van een risicomanagementprogramma definiëren; en

d) gevaren: uitvoeringseisen in verband met gevaarlijke materialen die op de locatie zijn opgeslagen.

OPMERKING Organisaties die op meerdere locaties actief zijn moeten vaak voldoen aan de eisen van verschillende rechtsgebieden.

4.3 Het toepassingsgebied van het BCMS vaststellen

4.3.1 Algemeen

De organisatie behoort het toepassingsgebied van het BCMS vast te stellen en te bewerkstelligen dat het op de juiste manier wordt gecommuniceerd aan belanghebbenden. Het is belangrijk dat de grenzen en toepasselijkheid van het BCMS duidelijk zijn en dat voor het toepassingsgebied rekening wordt gehouden met de onderwerpen die in 4.1 en 4.2 worden behandeld.

Het toepassingsgebied stelt vast voor welke producten en diensten, locaties, functies, processen en activiteiten het BCMS geldt. Daaruit volgt dat alle afhankelijkheden tot het toepassingsgebied behoren, zelfs als ze niet expliciet in de verwoording van het toepassingsgebied zijn geïdentificeerd. Als bijvoorbeeld 'beloning werknemer' in het toepassingsgebied is vermeld, dan behoren, zonder tegenindicatie, de beschikbaarheid van middelen, toestemming van het management en instructies aan de financiële instelling om de betaling uit te voeren, ook tot het toepassingsgebied.

De organisatie behoort het toepassingsgebied en de context van het BCMS duidelijk te documenteren.

4.3.2 Toepassingsgebied van het BCMS

De organisatie behoort het toepassingsgebied van het BCMS te definiëren en te documenteren op een manier die passend is voor de omvang, aard en complexiteit van de organisatie.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

In het toepassingsgebied behoren:

a) die delen van de organisatie die in het BCMS zijn geïdentificeerd, te worden opgenomen;

b) de eisen van het BCMS van de organisatie te worden vastgesteld, rekening houdend met de missie, doelen, wettelijke verantwoordelijkheden en interne en externe verplichtingen;

c) de producten en diensten van de organisatie te worden geïdentificeerd op een manier waardoor alle gerelateerde activiteiten, middelen en toeleveringsketens kunnen worden geïdentificeerd; en

d) de behoeften en belangen van belanghebbenden in aanmerking te worden genomen.

In het toepassingsgebied kan ook:

— een aanwijzing worden opgenomen over de omvang van incidenten waar het BCMS betrekking op heeft en de risicobereidheid van de organisatie; en

— worden geïdentificeerd hoe het BCMS past in de totale risicomanagementstrategie (indien aanwezig).

Als een deel van een organisatie is uitgesloten van het toepassingsgebied van het BCMS van de organisatie, behoort de organisatie de uitsluiting te documenteren en te verklaren.

Het doel van het definiëren van het toepassingsgebied is dat aan alle relevante activiteiten, locaties en leveranciers aandacht wordt besteed (8.2.1, figuur 6).

4.4 Managementsysteem voor bedrijfscontinuïteit

Dit is een normatieve verwijzing naar ISO 22301:2012 die de eisen voor een BCMS beschrijft. Er worden geen richtlijnen gegeven.

5 Leiderschap

5.1 Leiderschap en betrokkenheid

Alle niveaus van relevant management in de hele organisatie behoren betrokkenheid en leiderschap te tonen met betrekking tot het implementeren van beleid en doelstellingen voor bedrijfscontinuïteit. Dit kan worden getoond door gebruik te maken van motivatie, betrokkenheid en empowerment.

5.2 Betrokkenheid van de directie

De directie behoort haar betrokkenheid bij het BCMS te tonen.

De directie behoort het bewijs te tonen van haar betrokkenheid bij de ontwikkeling en implementatie van het BCMS en van haar continue inzet om de doeltreffendheid ervan te verbeteren, door:

a) te voldoen aan toepasselijke wettelijke eisen en aan andere eisen die de organisatie onderschrijft (4.2.2);

b) BCMS-processen te integreren in de onderhouds- en beoordelingsprocedures die in de organisatie zijn vastgesteld;

c) beleid en doelstellingen voor bedrijfscontinuïteit vast te stellen in overeenstemming met de doelstellingen, verplichtingen en strategische richting van de organisatie (5.3);

d) een of meer personen met passende bevoegdheid en competentie te benoemen die verantwoordelijk zijn voor het BCMS en aansprakelijk voor de doeltreffende uitvoering ervan (5.4);

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

e) te bewerkstelligen dat rollen, verantwoordelijkheden en competenties met betrekking tot het BCMS worden vastgesteld (5.4);

f) te bewerkstelligen dat voldoende middelen beschikbaar zijn, met inbegrip van een passend niveau van financiering (7.1);

g) het belang van het uitvoeren van het bedrijfscontinuïteitsbeleid en haar doelstellingen te communiceren met de organisatie (7.4);

h) actief deel te nemen aan oefeningen en tests (8.5);

i) te bewerkstelligen dat interne BCMS-audits worden uitgevoerd (9.2);

j) doeltreffende directiebeoordelingen van het BCMS uit te voeren (9.3); en

k) verbetering van het BCMS aan te sturen en te ondersteunen (hoofdstuk 10).

Betrokkenheid van de directie kan ook worden aangetoond door:

— betrokkenheid bij de uitvoering via stuurgroepen;

— het opnemen van bedrijfscontinuïteit als vast agendapunt van directievergaderingen.

5.3 Beleid

De directie behoort het bedrijfscontinuïteitsbeleid te definiëren in termen van de doelstellingen van de organisatie en haar verplichtingen, en ervoor te zorgen dat het:

— passend is voor het doel van de organisatie (in het licht van haar omvang, aard en complexiteit en om haar cultuur, afhankelijkheden en werkveld weer te geven);

— een kader biedt om doelstellingen vast te stellen;

— duidelijke verplichtingen bevat in relatie met toepasselijke eisen, met inbegrip van verplichtingen betreffende wet- en regelgeving en continue verbetering van het BCMS;

— binnen de organisatie wordt gecommuniceerd en begrepen;

— complementair is aan ander relevant beleid; en

— beschikbaar wordt gesteld aan belanghebbenden die door het management zijn goedgekeurd.

Er behoren passende voorzieningen te worden getroffen om het beleid goed te keuren, om er gedocumenteerde informatie over te bewaren en om het periodiek te beoordelen (bijv. jaarlijks), en als zich significante wijzigingen voordoen bij interne of externe factoren (bijv. een wijziging in de directie of invoering van nieuwe wetgeving). De geschiktheid van dergelijke voorzieningen hangt af van de omvang, complexiteit, aard en omvang van de organisatie.

Het beleid behoort ook:

— sturing te bieden voor het toepassingsgebied en de grenzen van de bedrijfscontinuïteit van de organisatie met inbegrip van beperkingen en uitsluitingen;

— vereiste bevoegdheden en machtigingen te identificeren, met inbegrip van de persoon of personen die verantwoordelijk is/zijn voor het BCMS van de organisatie;

— de criteria vast te stellen voor soort en schaal van incidenten die worden aangepakt; en

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

— verwijzingen naar normen, richtlijnen, voorschriften of beleid te bevatten waar het BCMS rekening mee moet houden of waar het aan moet voldoen.

Het bedrijfscontinuïteitsbeleid kan het volgende bevatten:

— belangrijke termen;

— financieringsverplichtingen;

— verwijzingen naar ander gerelateerd beleid;

— een eis om bedrijfscontinuïteit te implementeren;

— betrokkenheid om bedrijfscontinuïteit te oefenen en te onderhouden.

5.4 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie

De directie behoort toekenning en communicatie van verantwoordelijkheden en bevoegdheden binnen het BCMS te waarborgen.

Een lid van de directie behoort algeheel verantwoordelijk en aansprakelijk voor het BCMS te zijn.

De directie van de organisatie behoort een of meer specifieke managementvertegenwoordigers te benoemen die, ongeacht andere verantwoordelijkheden, gedefinieerde rollen, verantwoordelijkheden en bevoegdheid behoren te hebben om:

— te bewerkstelligen dat BCM wordt vastgesteld, geïmplementeerd en onderhouden in overeenstemming met het bedrijfscontinuïteitsbeleid;

— aan de directie te rapporteren over de prestatie van het BCM, ter beoordeling en als basis voor verbetering;

— in de hele organisatie bewustzijn van bedrijfscontinuïteit te promoten; en

— de doeltreffendheid te bewerkstelligen van procedures die zijn ontwikkeld voor reactie op incidenten, maar niet noodzakelijk ten aanzien van de implementatie tijdens een incident.

De managementvertegenwoordiger kan:

— als functiebenaming 'bedrijfscontinuïteitsmanager' hebben;

— andere verantwoordelijkheden binnen de organisatie dragen; en

— zich in veel delen van een organisatie bevinden, afhankelijk van de omvang, schaal en complexiteit van de organisatie.

Vanuit elke functie of locatie van de organisatie mogen vertegenwoordigers worden geïdentificeerd om te helpen het BCMS te implementeren. Hun rollen, aansprakelijkheden, verantwoordelijkheden en bevoegdheden behoren te worden opgenomen in functiebeschrijvingen die bekrachtigd kunnen worden door ze op te nemen in het beleid van de organisatie inzake beoordeling, beloning en waardering.

De directie kan andere organen, bijv. een stuurgroep, benoemen om toezicht te houden op de implementatie en voortdurende monitoring van het BCM.

Alle rollen, verantwoordelijkheden en bevoegdheden voor het BCM behoren te worden gedefinieerd en gedocumenteerd en te worden onderworpen aan audits.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

6 Planning

6.1 Acties om risico's en kansen op te pakken

De organisatie behoort vast te stellen hoe de in hoofdstuk 4.1 geïdentificeerde onderwerpen en de eisen in hoofdstuk 4.2 worden behandeld.

Dit impliceert dat geëvalueerd behoort te worden of er behoefte bestaat aan een actieplan om:

— onbedoelde resultaten te voorkomen;

— te profiteren van kansen om het BCMS te verbeteren.

Indien nodig zou ook in het actieplan moeten worden opgenomen:

— integreren en implementeren van deze acties in het BCMS-proces (8.1); en

— ervoor zorgen dat gedocumenteerde informatie beschikbaar is om te evalueren of de handelingen doeltreffend zijn geweest (zie 7.5).

6.2 Doelstellingen voor bedrijfscontinuïteit en de planning om ze te bereiken

Voor het inrichten en beheren van BCM (zoals beschreven in hoofdstuk 8) behoort een plan te worden opgesteld waarin verantwoordelijkheden en het stellen van passende en realistische taakstellingen voor het uitvoeren van taken zijn opgenomen. Het plan behoort gebaseerd te zijn op de continuïteitsdoelstellingen die zijn vastgesteld voor en gecommuniceerd naar relevante functies en niveaus binnen de organisatie. Vooruitgang in het plan behoort te worden gemonitord en gedocumenteerd.

Dit plan behoort te worden beoordeeld en mogelijk regelmatig te worden geactualiseerd in overeenstemming met de ontwikkelingen in het BCMS.

Hierna volgen voorbeelden van bedrijfscontinuïteitsdoelstellingen die mogelijk, in bepaalde omstandigheden, voldoen aan de eisen die zijn beschreven in ISO 22301:

— 'een BCMS inrichten dat consistent is met ISO 22313 per *datum*';

— 'certificatie behalen tegen ISO 22301:2012 per *datum*';

— 'per *datum* is bedrijfscontinuïteit van kracht die in overeenstemming is met onze verplichtingen tegenover belangrijke klanten'; en

— 'beschikken over BCM dat belangrijke producten en diensten per *datum* beschermt'.

7 Ondersteuning

7.1 Middelen

7.1.1 Algemeen

De organisatie behoort de middelen vast te stellen en te leveren die nodig zijn voor het BCMS die:

a) haar bedrijfscontinuïteitsbeleid en -doelstellingen halen;

b) voldoen aan de veranderende eisen van de organisatie;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

c) doeltreffende communicatie over aangelegenheden betreffende BCMS, intern en extern, mogelijk maken; en

d) voorzien in de voortdurende uitvoering en continue verbetering van het BCMS.

Deze behoren tijdig en doelmatig te worden verschaft.

7.1.2 Middelen voor het BCMS

Bij het vaststellen van de middelen die voor het BCMS nodig zijn, behoort de organisatie voldoende te voorzien in:

a) personen en persoonsgerelateerde middelen, met inbegrip van:

   1) de tijd die nodig is om rollen en verantwoordelijkheden van het BCMS te vervullen;

   2) training, opleiding, bewustzijn en oefening;

   3) aansturing van BCMS-personeel;

b) faciliteiten, met inbegrip van geschikte werkplekken en infrastructuur;

c) informatie- en communicatietechnologie (ICT), met inbegrip van toepassingen die doeltreffend en doelmatig programmamanagement ondersteunen;

d) beheren en beheersen van alle vormen van gedocumenteerde informatie;

e) communicatie met belanghebbenden (zie figuur 4); en

f) financiën en financiering.

Middelen en de toekenning ervan behoren periodiek te worden beoordeeld om te beoordelen of deze nog toereikend zijn. Het kan passend zijn om de directie bij deze beoordeling te betrekken.

7.1.3 Personeel dat op incidenten reageert

De organisatie behoort personeel te benoemen dat op incidenten reageert en dat beschikt over de nodige verantwoordelijkheid, bevoegdheid en competentie om een incident te beheren.

Personeel dat op incidenten reageert behoort een groep te vormen die verantwoordelijk is voor het beheren van verstorende incidenten met significante of potentieel significante gevolgen voor de organisatie.

Personeel kan worden benoemd in teams op basis van hun getoonde competentie om met verschillende aspecten van reactie op incidenten om te kunnen gaan, bijvoorbeeld:

— incidentmanagement/strategisch management (8.4.4.3.1);

— communicatie (8.4.4.3.2);

— veiligheid en welzijn (8.4.4.3.3);

— berging en veiligheid (8.4.4.3.4);

— activiteiten hervatten (8.4.4.3.5);

— herstel van ICT (8.4.4.3.6).

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

Al het personeel dat deel uitmaakt van deze groepen behoort duidelijk gedefinieerde verantwoordelijkheden en bevoegdheden te hebben die gelden vóór, tijdens en na een incident.

7.2 Competentie

De organisatie behoort een passend en doeltreffend systeem vast te stellen voor het beheren van de competentie van personen die onder haar gezag werkzaamheden uitvoeren die onder het BCMS vallen.

Het management behoort de vereiste competenties vast te stellen voor alle rollen en verantwoordelijkheden die onder het BCMS vallen, en voor bewustzijn, kennis, inzicht, vaardigheden en ervaring die nodig is om ze te vervullen. Alle personen aan wie binnen de organisatie taken zijn toegekend behoren blijk te geven van de nodige competenties, en behoren training, opleiding, ontwikkeling en andere ondersteuning te krijgen die hiervoor nodig is. Dit kan aangeduid worden als een competentieontwikkelingsprogramma, dat kan omvatten:

— beoordeling van competenties voor uit te voeren rollen;

— het creëren van een persoonlijk ontwikkelingsprogramma dat training, opleiding, ontwikkeling en andere ondersteuning identificeert die nodig zijn om competenties te verwerven;

— het voorzien in training en begeleiding, met inbegrip van selectie van passende methoden en materialen;

— het delen van kennis;

— deeltijdarbeid;

— het inhuren of contracteren van competente personen;

— het trainen van doelgroepen;

— het documenteren en monitoren van gevolgde training;

— evaluatie van gevolgde training tegenover gedefinieerde trainingsbehoeften en -eisen om conformiteit te verifiëren met de trainingseisen krachtens het BCMS; en

— indien nodig verbetering van het ontwikkelingsprogramma.

De organisatie behoort te beschikken over een proces voor het identificeren en presenteren van de trainingseisen voor alle deelnemers voor bedrijfscontinuïteit en voor het evalueren van de doeltreffendheid waarmee dit heeft plaatsgevonden.

De volgende soorten training kunnen voor bepaalde rollen passend zijn:

a) het BCMS inrichten en beheren:

   1) BCM inrichten en beheren;

   2) een bedrijfsimpactanalyse uitvoeren;

   3) risicobeoordeling;

   4) communicatievaardigheden;

   5) bedrijfscontinuïteitsdocumentatie ontwikkelen en implementeren; en

   6) een oefenprogramma in werking stellen.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

b) reactie op incidenten en bedrijfsactiviteiten herstellen:

1) incidenten beoordelen;

2) evacuatie en schuilgelegenheid aanwezig, beheer met inbegrip van controleprocessen ten behoeve van werknemers;

3) voorzieningen op alternatieve werklocaties; en

4) vragen van media behandelen.

Voor werknemers van de hele organisatie behoren vaardigheden en competentie met betrekking tot reactie op incidenten te worden ontwikkeld door praktische training, met inbegrip van actieve deelname aan oefeningen.

Reactie- en herstelteams behoren opleiding en training voor hun verantwoordelijkheden en taken te krijgen, met inbegrip van interactie met eerste hulpverleners en overige belanghebbenden. Teams behoren met regelmatige tussenpozen te worden getraind (ten minste jaarlijks), en nieuwe leden behoren te worden getraind als ze deel gaan uitmaken van de reactiestructuur. Deze teams behoren ook training te ontvangen over het voorkómen van incidenten die tot crises kunnen escaleren.

Veranderingen in de bedrijfsomgeving en de uitvoering zijn van invloed op de benadering en de manier waarop activiteiten met betrekking tot bedrijfscontinuïteit worden gepland, ontworpen en geïmplementeerd. De organisatie kan blijk geven van bewustzijn van trends in BCM door bijvoorbeeld actief te participeren in branchespecifieke BCM-activiteiten, waartoe kunnen behoren:

— lidmaatschap van een branchespecifieke belangengroepering;

— lidmaatschap van een comité dat een conferentie organiseert;

— presentaties geven tijdens conferenties en seminars; en

— lokale of mondiale BCM-conferenties bijwonen.

Blijk geven van actief participeren kan op een of meer van de volgende manieren:

— lidmaatschap van comité dat conferenties en seminars organiseert; en

— een lezing houden tijdens conferenties en seminars.

Competentie kan door de volgende activiteiten worden versterkt:

— integratie van resultaten van BCMS in de procedure van de organisatie voor beloning en waardering;

— integratie van resultaten van BCMS in de procedure van de organisatie voor prestatie en beoordeling;

— integratie van rollen, aansprakelijkheden, verantwoordelijkheden en bevoegdheden die samenhangen met het BCMS in de functieomschrijvingen en vaardigheden die door de organisatie worden gehanteerd; en

— actieve participatie door gebruikers en directie in het repeteren, oefenen en testen.

De organisatie behoort trainings- en bewustzijnsprogramma's vast te stellen voor alle actuele werknemers die getroffen kunnen worden door een verstorend incident en te eisen van contractanten die namens haar werkzaamheden verrichten, aan te tonen dat personen die onder haar gezag werkzaamheden uitvoeren, beschikken over de vereiste competentie voor het BCMS en voor de reactierollen die zij zullen uitvoeren.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

7.3 Bewustzijn

Personen die onder het gezag van de organisatie werken, behoren een passend bewustzijn van het BCMS te hebben.

Tot dergelijke personen kunnen personeel, contractanten en leveranciers behoren. Zij behoren zich bewust te zijn van het bedrijfscontinuïteitsbeleid en:

— hun rol en verantwoordelijkheid met betrekking tot voorkoming, opsporing, beperking, zelfbescherming, evacuatie, reactie, continuïteit en herstel van/tijdens/op/na incidenten;

— het belang van conformiteit aan bedrijfscontinuïteitsbeleid en -procedures;

— de implicaties van veranderingen in de bedrijfsuitvoering van de organisatie;

— hun bijdrage aan de doeltreffendheid van het BCMS, met inbegrip van de voordelen van verbeterde BCMS-prestaties; en

— hun rol en verantwoordelijkheid in het bereiken van conformiteit aan de eisen.

De organisatie behoort een cultuur binnen de organisatie te bouwen, promoten en in te bedden die:

— deel gaat uitmaken van de kernwaarden en management van de organisatie; en

— belanghebbenden bewust maakt van het bedrijfscontinuïteitsbeleid en hun rol in procedures die ermee samenhangen.

Organisaties met een positieve bedrijfscontinuïteitscultuur:

— ontwikkelen bedrijfscontinuïteit doeltreffender;

— boezemen vertrouwen in bij hun belanghebbenden (vooral personeel en klanten) in hun vermogen om verstorende incidenten te behandelen;

— verhogen hun veerkracht in de loop der tijd door te waarborgen dat implicaties van bedrijfscontinuïteit bij beslissingen op alle niveaus in aanmerking worden genomen; en

— verkleinen de waarschijnlijkheid en de gevolgen van verstoringen.

Het ontwikkelen van een bedrijfscontinuïteitscultuur wordt ondersteund door:

— inschakelen van al het personeel in de organisatie;

— leiderschap dat gespreid is over de organisatie;

— toekenning van verantwoordelijkheden;

— meting gebaseerd op prestatie-indicatoren;

— integreren van bedrijfscontinuïteit in de normale managementpraktijken;

— kweken van bewustzijn;

— vaardigheidstraining; en

— oefenen van bedrijfscontinuïteitsplannen.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

Een bewustzijnsprogramma kan omvatten:

— een raadplegingsproces met personeel in de hele organisatie betreffende inrichten en beheren van BCM;

— bespreken van bedrijfscontinuïteit in nieuwsbrieven, instructies, introductieprogramma of kranten van de organisatie (met inbegrip van oriëntatie van nieuwe werknemers);

— opnemen van bedrijfscontinuïteit op relevante internetpagina's;

— opnemen van BCM als agendapunt voor vergaderingen van staf en managementteam;

— selectieve publicatie van post-incidentrapporten;

— instructies voor de directie;

— bezoeken aan aangewezen alternatieve locatie (bijv. een uitwijklocatie); en

— instructie van belangrijke leveranciers en distributeurs over de voorzieningen van de organisatie betreffende bedrijfscontinuïteit.

7.4 Communicatie

Bij het inrichten en beheren van het BCMS behoort de organisatie te beschikken over doeltreffende communicatie- en raadplegingsprocedures voor het uitwisselen van informatie met belanghebbenden.

Deze procedures behoren alle volgende aspecten te omvatten:

a) interne communicatie tussen belanghebbenden, met inbegrip van personeel binnen de organisatie;

b) externe communicatie met klanten, leveranciers, de plaatselijke gemeenschap en andere belanghebbenden, waaronder de media;

c) het ontvangen, documenteren en reageren op communicatie van alle belanghebbenden;

d) aanpassing aan en integratie van nationale of regionale adviessystemen voor bedreigingen of vergelijkbare systemen in planning en operationeel gebruik, voor zover en indien van toepassing;

e) het waarborgen van de beschikbaarheid van communicatiemiddelen tijdens een verstorend incident;

f) het waarborgen van het vermogen van de organisatie om te kunnen communiceren met externe autoriteiten en, indien van toepassing, het waarborgen dat andere organisaties en personeel onderling kunnen communiceren; en

g) het uitvoeren en testen van communicatievoorzieningen die bedoeld zijn voor gebruik tijdens verstoring van normale communicatievoorzieningen.

De organisatie kan externe instanties die betrokken kunnen zijn bij reactie op incidenten – zoals de brandweer, politie, volksgezondheid en derde aanbieders – uitnodigen om met het management relevante delen van haar bedrijfscontinuïteitsprocedures te beoordelen.

De organisatie kan in nieuwsbrieven en instructies voor leveranciers en klanten verwijzingen naar haar BCMS en haar bedrijfscontinuïteitsvoorzieningen opnemen.

De organisatie behoort te voorzien in doeltreffende externe communicatie als onderdeel van haar bewustzijnsprogramma (7.3) en na een incident (8.4).

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

7.5 Gedocumenteerde informatie

7.5.1 Algemeen

Gedocumenteerde informatie levert bewijs van conformiteit aan eisen en doeltreffende uitvoering van het managementsysteem.

De term 'procedure' betekent een gespecificeerde wijze van uitvoeren van een activiteit of een proces. Een 'gedocumenteerde procedure' betekent dat de procedure op een medium behoort te zijn ingericht en onderhouden.

De eisen voor een of meer gedocumenteerde procedures kunnen in een enkel document zijn beschreven, en een eis voor een gedocumenteerde procedure kan meer dan een document beslaan.

De gedocumenteerde informatie die deze internationale norm vereist omvat:

— de context van de organisatie (4.1);

— wettelijke, regelgevende en andere eisen en bewijs van nakoming (4.2.2);

— het toepassingsgebied van het BCMS en eventuele uitsluitingen (4.3.2);

— het bedrijfscontinuïteitsbeleid (5.3);

— de bedrijfscontinuïteitsdoelstellingen (6.2);

— competentie (7.2);

— de bedrijfsimpactanalyse en de risicobeoordelingsprocedure (8.2);

— de bedrijfscontinuïteitsstrategie (8.3), met inbegrip van de opties die voor de strategie in overweging zijn genomen;

— procedures voor continuïteit, incidentmanagement en herstel (8.4);

— rapporten volgend op de oefeningen (8.5);

— BCMS-monitoring (9.1);

— interne audits (9.2);

— directiebeoordelingen (9.3);

— afwijkingen en corrigerende maatregelen (10.1).

Bovendien kan gedocumenteerde informatie over de volgende onderwerpen vereist zijn om de doeltreffendheid van het BCMS te waarborgen:

— klantencontracten en serviceniveaus;

— resultaten van bedrijfsimpactanalyses;

— resultaten van risicobeoordelingen;

— vaststelling en selectie van bedrijfscontinuïteitsstrategieën;

— overzicht van reactie op incidenten;

— bewustzijnsprogramma;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

— communicatie over het BCMS en incidenten met personeel en belanghebbenden – zoals nieuwsbrieven, aantekeningen van vergaderingen en waarschuwingen;

— trainingsprogramma's voor de organisatie en voor personen;

— oefenschema;

— contracten en dienstverleningsovereenkomsten met leveranciers;

— mededelingen aan en reactieprocedures voor contractanten en leveranciers;

— bewijs van inspectie, onderhoud en kalibratie;

— post-incidentrapporten en rapporten over bijna-ongelukken;

— notulen van de vergadering over de BCMS-beoordeling.

7.5.2 Creëren en actualiseren

Om te voldoen aan de eisen voor het creëren en actualiseren van gedocumenteerde informatie:

— behoort alle gedocumenteerde informatie de identificatie en omschrijving te bevatten (bijv. titel, naam, datum, auteur, nummer revisieverwijzing enz.);

— behoren voor het vastleggen en de presentatie van gedocumenteerde informatie acceptabele formats te worden vermeld (bijv. taal, softwareversie, afbeeldingen) en media (bijv. papier, elektronisch);

— behoort alle gedocumenteerde informatie op toereikendheid te worden beoordeeld en goedgekeurd.

Bij het vastleggen en presenteren van gedocumenteerde informatie behoort het te gebruiken format te worden vermeld (bijv. taal, softwareversie, afbeeldingen) en het te gebruiken medium (bijv. papieren of elektronisch document).

De omvang van gedocumenteerde informatie voor het BCMS kan tussen organisaties verschillen in verband met de volgende factoren:

— de omvang van de organisatie, haar producten en diensten en het soort activiteiten dat zij uitvoert;

— de complexiteit van de activiteiten en hun interacties; en

— de competentie van de personen.

7.5.3 Beheersing van gedocumenteerde informatie

Alle vereiste gedocumenteerde informatie behoort te worden beheerst.

Het doel van beheersen van documentatie is om te waarborgen dat organisaties documenten creëren, onderhouden en beschermen op een manier die passend en voldoende is om het BCMS te implementeren en uit te voeren. De primaire focus behoort op dit doel te zijn gericht in plaats van op het vaststellen van een complex beheersingssysteem.

Voorbeelden van beschermen zijn voorkomen dat documenten worden gecompromitteerd, gewijzigd zonder passende bevoegdheid en onbedoeld verwijderd.

Er kunnen verschillende toegangsniveaus en combinaties worden toegekend, bijvoorbeeld alleen raadplegen, raadplegen en wijzigen en beperkt raadplegen.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

Er behoort een gedocumenteerde procedure te worden vastgesteld om de beheersmaatregelen te definiëren die nodig zijn om:

a) gedocumenteerde informatie te distribueren;

b) er toegang toe te verlenen (toegang omvat bijvoorbeeld de toestemming en bevoegdheid om gedocumenteerde informatie te raadplegen of te wijzigen);

c) documenten goed te keuren op geschiktheid voordat ze worden uitgegeven;

d) documenten te beoordelen en indien nodig te actualiseren en opnieuw goed te keuren;

e) te bewerkstelligen dat veranderingen en de actuele revisiestatus van de documenten zijn geïdentificeerd;

f) te bewerkstelligen dat relevante versies van documenten die van toepassing zijn op werkplekken beschikbaar zijn;

g) te bewerkstelligen dat documenten leesbaar en gemakkelijk te identificeren blijven;

h) te waarborgen dat documenten van externe herkomst die volgens besluit van de organisatie nodig zijn voor de planning en uitvoering van het BCMS zijn geïdentificeerd en de distributie ervan wordt beheerst;

i) onbedoeld gebruik van vervallen documenten te voorkomen, en om passende identificatie toe te passen als ze om welke reden dan ook worden bewaard;

j) parameters voor het bewaren en archiveren van documenten vast te stellen; en

k) te waarborgen dat vertrouwelijke informatie wordt beschermd en niet openbaar wordt gemaakt.

Organisaties behoren de integriteit van gedocumenteerde informatie te waarborgen door te bewerkstelligen dat de informatie niet gecompromitteerd kan worden, er veilig een back-up van is gemaakt, alleen toegankelijk is voor bevoegd personeel en is beschermd tegen beschadiging, achteruitgang en verlies.

De organisatie behoort volledig te voldoen aan alle relevante wet- en regelgeving betreffende het bewaren van gedocumenteerde informatie, en de processen die nodig zijn om naleving te bereiken vast te stellen, te implementeren en te onderhouden.

8 Uitvoering

8.1 Operationele planning en beheersing

De organisatie behoort de activiteiten die nodig zijn om te voldoen aan haar bedrijfscontinuïteitsbeleid en -doelstellingen vast te stellen, te plannen, te implementeren en te beheersen en te voldoen aan de van toepassing zijnde behoeften en eisen.

Deze acties kunnen worden gecombineerd om een programma te ontwikkelen om te waarborgen dat de bedrijfscontinuïteit van de organisatie passend wordt beheerd en de doeltreffendheid ervan wordt gehandhaafd.

De organisatie behoort binnen het programma controlemechanismen vast te stellen, waartoe behoren:

a) besluiten hoe deze activiteiten behoren te worden vastgesteld, gepland, geïmplementeerd en beheerst, bijvoorbeeld door een implementatieplan vast te stellen en een passende methodologie om BCM te implementeren;

b) waarborgen dat over deze activiteiten beheersmaatregelen zijn geïmplementeerd die in overeenstemming zijn met de genomen besluiten, bijvoorbeeld door mijlpalen voor het project te bepalen en de vereiste leveringen te omschrijven; en

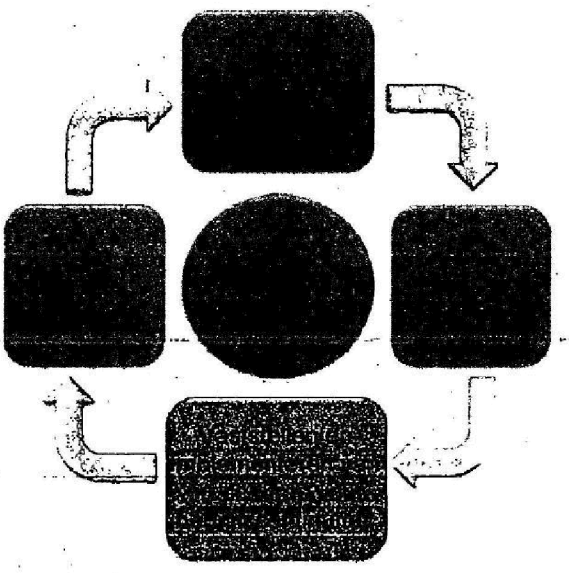
Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

c) gedocumenteerde informatie bijhouden om aan te tonen dat de processen zijn uitgevoerd zoals gepland.

De organisatie behoort te waarborgen dat geplande veranderingen worden beheerst, onbedoelde veranderingen worden beoordeeld en dat passende maatregelen worden genomen.

8.1.1 Elementen van BCM

BCM omvat de volgende elementen, zoals geïllustreerd in figuur 5:



Figuur 5 — Elementen van bedrijfscontinuïteitsmanagement (BCM)

Onderstaand wordt aangegeven om welke elementen het gaat en waar zij in deze internationale norm worden behandeld:

a) **Operationele planning en beheersing** (8.1)

Doeltreffende operationele planning en beheersing is de kern van bedrijfscontinuïteitsmanagement. Het behoort te worden geleid door een verantwoordelijke persoon die is benoemd door de directie.

b) **Bedrijfsimpactanalyse en risicobeoordeling** (8.2)

Verkrijgen van overeenstemming en inzicht in prioriteiten en eisen voor bedrijfscontinuïteit wordt bereikt door middel van bedrijfsimpactanalyse (BIA) en risicobeoordeling. De BIA stelt de organisatie in staat om activiteiten die haar producten en diensten ondersteunen voor hervatting te prioriteren. Risicobeoordeling bevordert inzicht in de risico's voor geprioriteerde activiteiten en hun afhankelijkheden, en de potentiële gevolgen van een verstorend incident. Dit inzicht stelt de organisatie in staat om passende bedrijfscontinuïteitsstrategieën te kiezen.

c) **Strategie voor bedrijfscontinuïteit** (8.3)

Door een reeks opties voor de strategie voor bedrijfscontinuïteit te identificeren en evalueren is de organisatie in staat om passende manieren te kiezen om te voorkomen dat haar geprioriteerde activiteiten worden verstoord en om verstoringen die plaatsvinden aan te pakken. Gekozen strategieën voor bedrijfscontinuïteit zorgen voor hervatting van activiteiten tot een aanvaardbaar niveau van bedrijfsvoering en binnen overeengekomen tijdsbestekken.

OPMERKING De gekozen strategie behoort rekening te houden met vormen van risicobehandeling die al binnen de organisatie van kracht zijn (8.3.3).

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

d) **Vaststellen en implementeren van procedures voor bedrijfscontinuïteit** (8.4)

Het implementeren van bedrijfscontinuïteitsvoorzieningen resulteert in het creëren van een structuur voor reactie op incidenten (8.4.2), de middelen om een incident op te sporen en erop te reageren (8.4.3), bedrijfscontinuïteitsplannen (8.4.4) en procedures om terug te keren naar 'business as usual' (8.4.5).

e) **Oefenen en testen** (8.5)

Oefenen en testen geeft de organisatie de gelegenheid om:

— bewustzijn bij personeel en competentieontwikkeling te stimuleren;

— te waarborgen dat bedrijfscontinuïteit en bedrijfscontinuïteitsprocedures volledig, actueel en passend zijn; en

— kansen te identificeren om haar bedrijfscontinuïteit te verbeteren.

8.1.2 De BCM-omgeving beheren

Doeltreffend beheer van de BCM-omgeving omvat:

a) het waarborgen van de continue relevantie van het toepassingsgebied, de rollen en verantwoordelijkheden voor bedrijfscontinuïteit;

b) het bevorderen en inbedden van continuïteit in de hele organisatie en, indien van toepassing, andere belanghebbenden;

c) het beheren van kosten die samenhangen met bedrijfscontinuïteit;

d) het vaststellen en monitoren van regimes voor verandermanagement en opvolgingsmanagement binnen het BCMS;

e) het regelen van of voorzien in passende training en bewustzijn van personeel; en

f) het bijhouden van de programmadocumentatie passend bij de omvang en complexiteit van de organisatie.

Elk onderdeel van de BCM-voorzieningen van een organisatie, met inbegrip van documentatie, behoort regelmatig te worden beoordeeld, geoefend en geactualiseerd. Deze voorzieningen behoren ook te worden beoordeeld en geactualiseerd als zich een significante verandering voordoet in uitvoeringskader, structuur, locaties, personeel, processen of technologie, of als een oefening of een incident tekortkomingen aangeeft.

De organisatie kan gebruikmaken van een erkende projectmanagementmethode om te waarborgen dat het BCM-programma doeltreffend wordt beheerd.

8.1.3 Bedrijfscontinuïteit in stand houden

Doeltreffende bedrijfscontinuïteit in stand houden omvat:

a) BCM actueel houden door middel van goede werkwijzen;

b) het oefenprogramma administreren;

c) het coördineren van de regelmatige beoordeling en update van bedrijfscontinuïteit, met inbegrip van het beoordelen of bijwerken van bedrijfsimpactanalyses (BIA's) en risicobeoordelingen; en

d) waarborgen dat bedrijfscontinuïteitsprocedures in stand worden gehouden zoals passend is voor de behoeften van reactieteams.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

8.1.4 Doeltreffendheid meten

Het meten van de doeltreffendheid behoort betrekking te hebben op zowel:

a) het monitoren van de prestatie van bedrijfscontinuïteit; als

b) het monitoren en beoordelen van de bedrijfscontinuïteitsvoorzieningen voor uitbestede activiteiten en de BCM-capaciteiten van leveranciers.

Voorbeelden van meeteenheden die gebruikt kunnen worden om de doeltreffendheid te meten zijn:

— activiteiten en middelen zijn herstelbaar binnen de gegeven hersteltijddoelstelling en de informatie is van de vereiste gangbaarheid (beoogd herstelpunt);

— de vereiste accommodatie en uitrusting zijn beschikbaar op (een) alternatieve locatie(s) om herstel en hervatting van activiteiten mogelijk te maken;

— de vereiste competenties om de geprioriteerde activiteiten binnen de gegeven hersteltijddoelstelling te hervatten zijn aangetoond; en

— de vereiste competenties voor reactie op incidenten en om incidenten te beheren zijn aangetoond.

8.1.5 Resultaten

Resultaten die een aanwijzing vormen voor doeltreffend BCM kunnen het volgende omvatten:

a) een capaciteit om incidenten te beheren is mogelijk gemaakt en biedt een doeltreffende reactie;

b) het inzicht dat de organisatie van zichzelf en de relaties met andere organisaties, relevante regelgevende instanties of overheidsinstellingen, lokale autoriteiten en de hulpverleningsdiensten heeft, is juist ontwikkeld, gedocumenteerd en begrepen;

c) regelmatige oefening waarborgt dat personeel is getraind om doeltreffend op een incident of verstoring te reageren;

d) eisen van belanghebbenden zijn begrepen en kunnen worden nagekomen;

e) personeel ontvangt toereikende ondersteuning en berichtgeving in geval van een verstoring;

f) de reputatie van de organisatie is beschermd;

g) de organisatie blijft haar verplichtingen betreffende wet- en regelgeving naleven; en

h) gedurende een incident worden financiële beheersmaatregelen gehandhaafd.

8.2 Bedrijfsimpactanalyse en risicobeoordeling

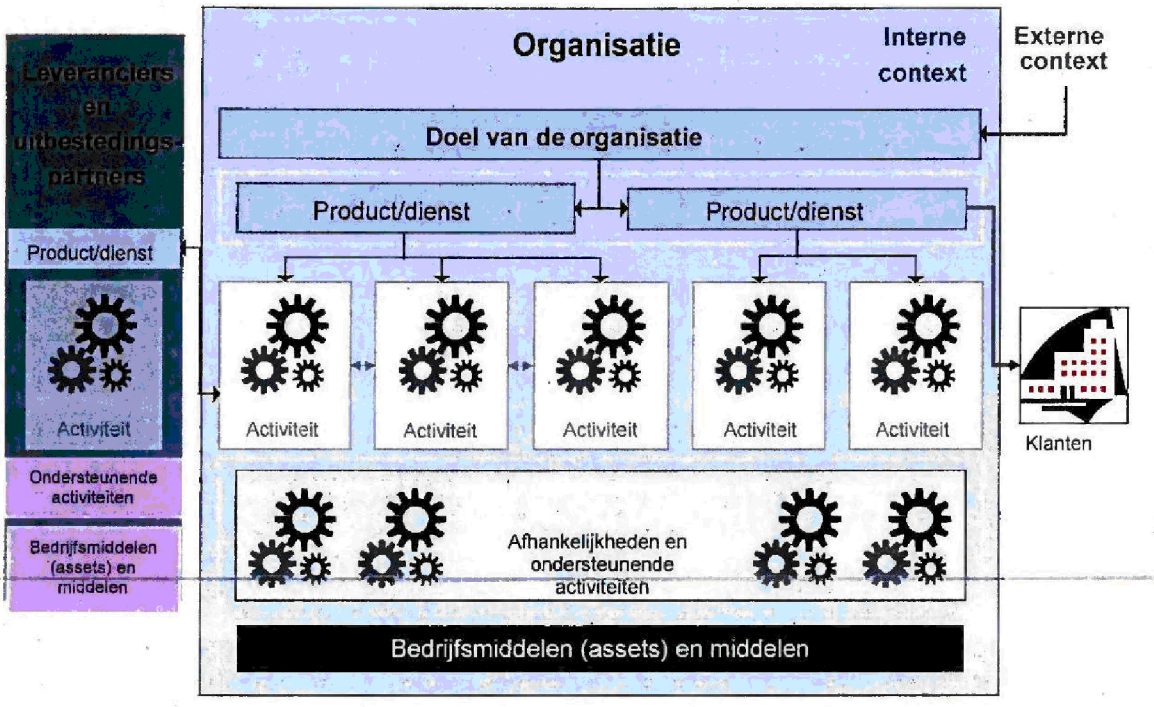
8.2.1 Algemeen

De organisatie behoort een formeel en gedocumenteerd proces voor bedrijfsimpactanalyse en risicobeoordeling vast te stellen, te implementeren en te onderhouden. Het inzicht dat in de hele organisatie uit de BIA en de risicobeoordeling is verkregen biedt de basis voor doeltreffende bedrijfscontinuïteit.

Een organisatie bereikt haar doel door haar producten en diensten aan klanten te leveren. Het is daarom belangrijk inzicht te creëren in de nadelige gevolgen die verstoring van deze producten en diensten in de loop der tijd hebben op de doelstellingen en bedrijfsuitvoering van de organisatie. Het is ook belangrijk om inzicht te hebben in de onderlinge relaties en de eisen voor de middelen van de activiteiten die producten en diensten ondersteunen en in de bedreigingen waar zij onderhevig aan zijn.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014



Figuur 6 — Inzicht in de organisatie

Op basis van inzicht is de organisatie in staat om te bewerkstelligen dat haar bedrijfscontinuïteit in overeenstemming is met haar doel, wettelijke plichten en verplichtingen tegenover haar belanghebbenden. Inzicht wordt bereikt door middel van het proces van bedrijfsimpactanalyse en risicobeoordeling. Deze processen leveren de informatie die de organisatie nodig heeft om bedrijfscontinuïteitsstrategieën vast te stellen en te kiezen (8.3.1).

De BIA en de risicobeoordeling behoren de organisatie in staat te stellen om maatregelen te identificeren die:

a) de gevolgen van een verstoring op de organisatie beperken;

b) de duur van de verstoring verkorten; en

c) de waarschijnlijkheid van verstoring verminderen.

De context, evaluatiecriteria en het format van het resultaat van de BIA en de risicobeoordeling behoren vooraf te worden gedefinieerd en overeengekomen. Verzamelde informatie behoort regelmatig te worden beoordeeld, in het bijzonder tijdens perioden van verandering.

8.2.2 Bedrijfsimpactanalyse

De organisatie behoort een formeel en gedocumenteerd evaluatieproces vast te stellen om prioriteiten, doelstellingen en taakstellingen voor continuïteit en herstel te bepalen.

Het doel van de BIA is om:

— inzicht te verkrijgen in de belangrijke producten en diensten van de organisatie en de activiteiten waar zij uit voortkomen;

— prioriteiten en tijdsbestekken voor herstel van activiteiten bepalen;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

— de belangrijkste middelen te identificeren die waarschijnlijk vereist zijn voor continuïteit en herstel; en

— afhankelijkheden te identificeren (zowel intern als extern).

De bedrijfsimpactanalyse behoort te omvatten:

a) identificatie van activiteiten die de levering van de belangrijkste producten en diensten van de organisatie ondersteunen – 'belangrijkste producten' betekent de producten die zijn opgenomen in het toepassingsgebied van het BCMS;

b) het beoordelen van de potentiële gevolgen van verstoringen in de loop der tijd die het resultaat zijn van niet-beheerste, niet-specifieke gebeurtenissen met betrekking tot deze activiteiten. Bij het beoordelen van de gevolgen behoort de organisatie zich te richten op de gevolgen die verband houden met haar bedrijfsdoelen, bedrijfsdoelstellingen en haar belanghebbenden. Hiertoe kunnen behoren:

   1) nadelige effecten op personeel of maatschappelijk welzijn;

   2) consequenties van wettelijke plichten of van eisen van regelgeving;

   3) schade aan reputatie;

   4) verminderde financiële draagkracht;

   5) verslechtering van kwaliteit van producten of diensten; en

   6) schade aan het milieu.

OPMERKING 1 Verstoring van activiteiten kan de levering van producten en diensten indirect verstoren. Als de organisatie bijvoorbeeld niet in staat is leveranciers te betalen kan haar reputatie worden geschaad. Het gevolg hiervan kan zijn dat leveranciers weigeren de organisatie goederen te leveren waardoor producten niet kunnen worden gefabriceerd of diensten niet kunnen worden geleverd.

OPMERKING 2 Activiteiten kennen in het algemeen dagelijkse variaties en kunnen cyclisch van aard zijn. Er zijn vaak seizoensgebonden variaties en hogere niveaus van activiteit die samenhangen met wekelijkse, maandelijkse of jaarlijkse deadlines of met leveringsdatums van projecten. Simuleren dat de verstoring plaatsvindt op het ongunstigste tijdstip tijdens deze cycli waarborgt dat de grootst mogelijke gevolgen worden beoordeeld.

c) het taxeren van hoe lang het zou duren voordat de gevolgen die samenhangen met de verstoring van de activiteiten van de organisatie onacceptabel worden;

OPMERKING 3 De tijdsduur die aangeeft wanneer gevolgen onaanvaardbaar worden kan variëren tussen seconden en een paar maanden, afhankelijk van de aard van de activiteit. Activiteiten die tijdgevoelig zijn moeten mogelijk met een hoge nauwkeurigheid worden genoteerd, bijv. per minuut of uur. Lagere nauwkeurigheid is aanvaardbaar voor activiteiten die minder tijdgevoelig zijn.

OPMERKING 4 De tijd die verstrijkt tot het punt waarop gevolgen onaanvaardbaar worden, kan worden aangeduid als 'maximaal aanvaardbare duur van verstoring', 'maximaal aanvaardbare duur' of 'maximaal aanvaardbare storingstijd'. Het minimumniveau van een product of dienst dat aanvaardbaar is voor de organisatie kan worden verwoord als de minimumdoelstelling voor bedrijfscontinuïteit.

d) het vaststellen van geprioriteerde tijdsbestekken voor hervatting van deze activiteiten op een aangegeven minimaal aanvaardbaar niveau, gebaseerd op de beoordeling van potentiële gevolgen en rekening houdend met andere relevante factoren.

e) het identificeren van afhankelijkheden tussen activiteiten; en

f) het identificeren van de afhankelijkheid van elke activiteit van de ondersteunende middelen, met inbegrip van leveranciers en andere relevante belanghebbenden.

Het geprioriteerde tijdsbestek voor hervatting van een activiteit kan worden aangeduid als hersteltijddoelstelling. De hersteltijddoelstelling kan rekening houden met afhankelijkheden van onderling

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

samenhangende activiteiten en met de tijd waarbinnen de gevolgen van het niet hervatten van de activiteit onaanvaardbaar worden (zie punt c) hiervoor].

OPMERKING 5 Vanaf dit punt wordt in deze internationale norm de term 'hersteltijddoelstelling' of de afkorting 'RTO' gebruikt in plaats van 'geprioriteerd tijdsbestek'.

Het resultaat van de bedrijfsimpactanalyse behoort te worden gedocumenteerd en identificatie te bevatten van:

— producten, diensten en activiteiten;

— prioriteiten voor herstel;

— significante afhankelijkheden en ondersteunende middelen.

Informatie voor de bedrijfsimpactanalyse kan afkomstig zijn uit:

— vraaggesprekken;

— vragenlijsten;

— workshops; en

— overige interne en externe bronnen.

8.2.3 Risicobeoordeling

De organisatie behoort een formele risicobeoordelingsprocedure vast te stellen die systematisch het risico van verstoring van de geprioriteerde activiteiten en de processen, systemen, informatie, personen, bedrijfsmiddelen (assets), leveranciers en andere bronnen die hen ondersteunen, identificeert, analyseert en evalueert.

Risicobeoordeling levert een gestructureerd proces om risico´s te analyseren in termen van gevolgen en waarschijnlijkheid alvorens te beslissen over verdere behandeling die nodig kan zijn. Dit gestructureerde proces probeert een aantal fundamentele vragen te beantwoorden:

a) Wat kan gebeuren en waarom (risico-identificatie)?

b) Wat kunnen de consequenties zijn?

c) Hoe waarschijnlijk is het dat deze zich voordoen? en

d) Is er iets dat de consequenties kan beperken of de waarschijnlijkheid kan verkleinen?

Bij het proces behoren financiële, overheids- en maatschappelijke verplichtingen in aanmerking te worden genomen.

De organisatie behoort zich bewust te zijn van de bedreigingen voor en de kwetsbaarheden van de middelen die nodig zijn voor de activiteiten van de organisatie, en in het bijzonder van de middelen:

— die nodig zijn voor een activiteit met een hoge prioriteit; of

— met een significante vervangingstijd.

De organisatie behoort een passende methode te kiezen voor het identificeren, analyseren en evalueren van risico's die kunnen resulteren in verstoringen. ISO 31000 beschrijft de principes van risicomanagement en gerelateerde richtlijnen. Typische elementen die in de context van deze internationale norm behoren te worden opgenomen zijn:

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

— **het identificeren van risico's:** Risico's voor verstoring van de geprioriteerde activiteiten van de organisatie identificeren evenals de processen, systemen, informatie, mensen, bedrijfsmiddelen (assets), leveranciers en andere middelen die deze activiteiten ondersteunen. Deze kunnen afkomstig zijn van:

  — specifieke bedreigingen die omschreven kunnen worden als gebeurtenissen of acties die op een bepaald moment activiteiten en middelen kunnen verstoren (bijv. bedreigingen zoals brand, overstroming, stroomuitval, verlies van personeel, personeelsverzuim, computervirussen en hardwarestoringen; en

  — verstorende incidenten die kunnen voortkomen uit zwakke punten in middelen (bijv. op zich staande storingen, gebreken in brandbeveiliging, te krappe stroomvoorziening, ontoereikende personeelsniveaus en slechte beveiliging en herstelvermogen van de IT);

— **het evalueren van risico's:** Evalueren welke risico's die verband houden met verstoring behandeling vereisen. Dit behoort gericht te zijn op de middelen die nodig zijn voor activiteiten met een hoge prioriteit of op middelen met een significante vervangingstijd; en

— **het identificeren van maatregelen:** Het identificeren van maatregelen die de doelstellingen voor bedrijfscontinuïteit kunnen realiseren en in overeenstemming zijn met de risicobereidheid van de organisatie (4.1).

OPMERKING Als een andere risicoanalyse door de organisatie of door externe organen is uitgevoerd, kan deze nuttige informatie leveren die relevant is voor de risicobeoordeling.

Maatschappelijke behoeften of regulatorische verplichtingen kunnen eisen dat de organisatie sommige resultaten van de risicobeoordeling met sommige belanghebbenden deelt.

8.3 Strategie voor bedrijfscontinuïteit

8.3.1 Bepaling en selectie

8.3.1.1 Algemeen

Bepalen van bedrijfscontinuïteitsstrategie gaat over het identificeren van de actie die nodig is om de bevindingen van de BIA en risicobeoordelingen aan te pakken op een manier die voldoet aan de doelstellingen van bedrijfscontinuïteit van de organisatie. Een dergelijke actie is waarschijnlijk nodig voor, tijdens en na een verstorend incident, en kan bijvoorbeeld inhouden:

— een productielijn over twee locaties splitsen;

— een stroomgenerator installeren; of

— het algehele gevolg van een verstorend incident verminderen door middel van voorzieningen voor bedrijfscontinuïteit die de duur van de verstoring verkorten en de intensiteit verlagen tot aanvaardbare niveaus.

De bepaling en selectie van een bedrijfscontinuïteitsstrategie behoort gebaseerd te zijn op de output van de bedrijfsimpactanalyse en de risicobeoordeling (8.2).

De organisatie behoort passende strategieopties te bepalen om:

— de geprioriteerde activiteiten te beschermen;

— geprioriteerde activiteiten te stabiliseren, te vervolgen, te hervatten en te herstellen;

— om gevolgen te beperken, erop te reageren en deze te beheren.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

De organisatie behoort te beschikken over een mechanisme voor het beoordelen en goedkeuren van aanbevolen oplossingen.

8.3.1.2 Geprioriteerde activiteiten beschermen

Het beschermen van geprioriteerde activiteiten kan erop gericht zijn om:

— het risico voor de activiteit te verkleinen;

— de activiteit aan een derde over te dragen (hoewel de verantwoordelijkheid bij de organisatie blijft); en

— de activiteit te stoppen of te veranderen als uitvoerbare alternatieven beschikbaar zijn.

Opties voor het beschermen van geprioriteerde activiteiten behoren te worden gekozen overeenkomstig:

— de waargenomen kwetsbare punten van de activiteit;

— de kosten van de maatregelen in vergelijking met de getaxeerde voordelen;

— (optioneel) de urgentie van de activiteit – omdat er minder tijd beschikbaar is om de kwestie op te lossen; en

— de totale haalbaarheid en geschiktheid van de optie.

Als de organisatie inschat dat een dreiging 'uiterst onwaarschijnlijk' is, of de kosten van het beschermen van een geprioriteerde activiteit excessief hoog zijn, kan zij ervoor kiezen het risico te accepteren en het te herevalueren als onderdeel van haar voortdurende prestatie-evaluatie in het kader van het BCMS (hoofdstuk 10).

8.3.1.3 Geprioriteerde activiteiten stabiliseren, voortzetten, hervatten en herstellen

Het stabiliseren, voortzetten, hervatten en herstellen van geprioriteerde activiteiten behoort ook betrekking te hebben op hun afhankelijkheden en ondersteunende middelen;

Opties voor bedrijfscontinuïteitsstrategieën kunnen o.a. zijn:

a) **Verplaatsing van activiteiten:** Het overbrengen van een aantal of alle activiteiten hetzij intern naar een ander deel van de organisatie, of extern naar een derde, hetzij onafhankelijk of via een wederzijdse overeenkomst of een overeenkomst voor wederzijdse hulpverlening.

b) **Verplaatsing of verschuiving van middelen:** Middelen, met inbegrip van personeel worden overgebracht naar een andere locatie of activiteit binnen de organisatie of extern naar een derde.

c) **Alternatieve processen en reservecapaciteit:** Alternatieve processen vaststellen of reservecapaciteit creëren in processen en/of inventaris.

d) **Vervanging van middelen en vaardigheden:** Versterken van capaciteiten van personen, met inbegrip van 'multi-skilling' van kernmedewerkers of creëren van toegang tot extra capaciteit via uitbesteding. Vervangende middelen worden geleverd door een derde of uit voorraad die elders door de organisatie wordt gehouden of door overeenkomsten voor wederzijdse hulpverlening met externe organisaties en belangrijke belanghebbenden te sluiten om tijdelijk extra capaciteit beschikbaar te stellen; en

e) **Tijdelijk alternatief:** Voor sommige activiteiten kan een andere werkwijze worden gehanteerd die voor een beperkte tijd aanvaardbare resultaten levert. Het is waarschijnlijk dat het alternatief meer tijd kost en/of arbeidsintensiever is (bijv. handmatige uitvoering tegenover een geautomatiseerd systeem). Om deze redenen zijn alternatieven in het algemeen alleen geschikt voor korte tijdsduur of om terugkeer naar de normale bedrijfsvoering uit te stellen.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

f) Bij het overwegen van locaties om een activiteit te hervatten, behoren de beschadigde/getroffen locaties en onbeschadigde alternatieve locaties in de opties voor bedrijfscontinuïteit te worden opgenomen.

Om te bewerkstelligen dat activiteiten binnen de hersteltijddoelstellingen kunnen worden hervat, kunnen ook voor hun afhankelijkheden en ondersteunende middelen hersteltijddoelstellingen worden bepaald. Bij het bepalen van deze hersteltijddoelstellingen moet mogelijk rekening worden gehouden met:

— de mogelijkheid van een minimumdienstverlening voor tijdelijke duur tot het moment waarop volledige hervatting vereist is;

— alternatieven (zoals handmatige processen) die de behoefte aan hervatting van de afhankelijkheid van ondersteunende middelen uitstellen;

— achterstanden en tijd die nodig is om verloren gegevens te herstellen; en

— de complexiteit en de omvang van eisen voor herstel of de behoefte aan specialistische uitrusting met een lange leveringstijd.

De organisatie behoort alle opties voor strategie te evalueren om vast te stellen of deze maatregelen zelf nieuwe risico's hebben geïntroduceerd.

Opties voor bedrijfscontinuïteitsstrategieën om een geprioriteerde activiteit te stabiliseren, vervolgen, hervatten of herstellen kunnen vaak excessief duur zijn. Als de organisatie meent dat dit het geval is, behoort zij hetzij alternatieve strategieën te kiezen die aanvaardbaar zijn en voldoen aan haar doelstellingen voor bedrijfscontinuïteit of betrokken producten en diensten te behandelen als uitsluitingen van het toepassingsgebied van het BCMS in overeenstemming met 4.3.2.

8.3.1.4. Gevolgen beperken, erop reageren en beheren

Opties om de gevolgen en duur van een incident te beperken kunnen o.a. zijn:

a) **Verzekering:** Het afsluiten van verzekeringen kan een zekere financiële compensatie voor bepaalde verliezen bieden, maar zal niet alle kosten dekken (bijv. waarde van onverzekerde gebeurtenissen, schade aan merken, reputatie, waarde van belanghebbenden, marktaandeel en persoonlijke gevolgen). Eén financiële regeling alleen biedt de organisatie geen afdoende bescherming en voldoet niet aan de verwachtingen van belanghebbenden. Verzekeringsdekking wordt waarschijnlijk meer gebruikt tezamen met een of meer andere strategieën.

b) **Bedrijfsmiddelen (assets) herstellen:** Stand-by-diensten contracteren van ondernemingen die zich specialiseren in het reinigen of repareren van beschadigde bedrijfsmiddelen (assets); en

c) **Reputatie beheren:** Een doeltreffend waarschuwings- en communicatiesysteem ontwikkelen (8.4.3) en doeltreffende communicatieprocedures vaststellen (8.4.4.3.2).

8.3.1.5 Bedrijfscontinuïteit van leveranciers

De organisatie behoort te bewerkstelligen dat de bedrijfscontinuïteit van leveranciers wordt geëvalueerd. De organisatie kan ervoor kiezen zich hierbij te concentreren op leveranciers die in geval van gebrekkige levering heel snel geprioriteerde activiteiten zouden verstoren. Hierbij kunnen de volgende technieken worden toegepast:

— opnemen van eisen in aanbestedingen en contracten;

— periodieke audits van de plannen van leveranciers;

— gezamenlijke oefeningen voor bedrijfscontinuïteit.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

8.3.2 Vaststelling van eisen voor middelen

8.3.2.1 Algemeen

De organisatie behoort de eisen voor de middelen te bepalen om de geselecteerde strategieën te implementeren.

De organisatie hoort te zorgen voor:

a) passende teams of, voor kleine organisaties, personen met passende autoriteit om toezicht te houden op het voorbereid zijn op incidenten en het reactie- en herstelvermogen van de organisatie;

b) logistieke capaciteiten en procedures om diensten, personeel, middelen, materialen en geproduceerde of gedoneerde faciliteiten ter ondersteuning van het BCMS te lokaliseren, verwerven, op te slaan, te testen, en er rekenschap van te geven.

c) financiële, logistieke en administratieve procedures om de voorzieningen voor bedrijfscontinuïteit voor, tijdens en na een incident te ondersteunen. Procedures behoren:

   1) te waarborgen dat fiscale besluiten versneld kunnen worden afgehandeld; en

   2) in overeenstemming te zijn met vastgestelde bevoegdheidsniveaus, met bestuur en met boekhoudingsprincipes;

d) doelstellingen voor middelenbeheer met betrekking tot reactietijden, personeel, uitrusting, training, faciliteiten, financiering, verzekering, beheersing van aansprakelijkheid, expertkennis, materialen en de tijdsbestekken waarbinnen elk hiervan nodig is uit de middelen van de organisatie en van leveranciers; en

e) procedures voor hulp van belanghebbenden, communicatie, strategische overeenkomsten en wederzijdse hulp.

8.3.2.2 Mensen

De organisatie behoort passende maatregelen te identificeren om de beschikbaarheid van kernvaardigheden en kennis bij te houden en te verbreden voor het geval dat het incident resulteert in vermindering van beschikbaar personeel. Deze maatregelen behoren betrekking te hebben op werknemers, contractanten en andere belanghebbenden die uitgebreide specialistische vaardigheden en kennis bezitten. Technieken om deze vaardigheden te beschermen of te vergroten kunnen o.a. zijn:

— back-uplijst van geschoolde specialisten en oproepplan;

— multi-skilltraining van personeel en contractanten;

— scheiding van kernvaardigheden om de gevolgen van een incident te verkleinen, met inbegrip van fysieke scheiding van personeel met kernvaardigheden op meer dan een locatie;

— gebruikmaken van derden;

— opvolgingsplanning; en

— documenteren van processen en andere vormen van kennisbehoud en beheer.

Procedures die verband houden met de verplaatsing van personeel na een incident moeten mogelijk rekening houden met:

— transport van personeel naar een andere locatie;

— behoeften van personeel op de uitwijklocatie zoals:

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

— accommodatie;

— cateringfaciliteiten;

— persoonlijke en gezinsverplichtingen; en

— training op verschillende uitrusting;

— kwesties die verband houden met thuiswerken.

Specialistische rollen kunnen zijn:

— beveiliging;

— logistiek van transport; en

— welzijn en noodsituaties.

8.3.2.3 Gegevens en informatie

Informatie die essentieel is voor de bedrijfsuitvoering van de organisatie behoort te worden beschermd en herstelbaar te zijn in overeenstemming met de tijdsbestekken die binnen het BIA zijn geïdentificeerd. Opslaan en herstel van gegevens behoort in overeenstemming te zijn met relevante wetgeving.

OPMERKING 1 Nadere richtlijnen over het waarborgen van de actualiteit van elektronische gegevens zijn opgenomen in ISO/IEC 27031. ISO/IEC 27002 biedt richtlijnen voor het waarborgen van de voortdurende vertrouwelijkheid, integriteit en beschikbaarheid van gegevens.

Informatie die nodig is om reactie en herstel door de organisatie mogelijk te maken behoort te beschikken over een passende mate van:

— **vertrouwelijkheid:** bijvoorbeeld als de activiteit naar een andere locatie is verplaatst;

— **integriteit:** dat de informatie betrouwbaar is en vertrouwd kan worden;

— **beschikbaarheid:** dat de informatie beschikbaar is zodra de activiteit dit vereist. Informatie die nodig is tijdens de reactie kan onmiddellijk nodig zijn, terwijl andere gegevens pas enige tijd na het incident nodig zijn; en

— **actualiteit:** zo actueel als vereist om uitvoering van de activiteit mogelijk te maken – hoewel gegevens die in verband met het incident verloren zijn gegaan mogelijk opnieuw gecreëerd moeten worden.

In alle gevallen behoort informatie die nodig is voor een activiteit voldoende actueel te zijn. Deze actualiteit kan worden aangeduid als herstelpuntdoelstelling. Als gegevens worden gekopieerd kunnen verschillende methoden worden gebruikt, met inbegrip van elektronische back-ups of back-ups op band, microfiche, fotokopieën en het creëren van dubbele kopieën.

Voor het herstel van informatie die nog niet is gekopieerd of waarvan een back-up is gemaakt naar een veilige locatie behoren informatiestrategieën te worden gedocumenteerd.

Informatiestrategieën behoren te worden uitgebreid tot:

— fysieke (hardcopy)formats; en

— virtuele (elektronische) formats, enz.

OPMERKING 2 Als gekopieerde informatie te dicht bij het origineel wordt bewaard, kan het verstorende incident de integriteit ervan compromitteren of toegang onmogelijk maken. Een grote afstand kan echter maken dat de informatie niet beschikbaar is als deze nodig is. Het zou passend zijn om te beschikken over schriftelijk bewijs van hoe deze conflicterende belangen zijn opgelost.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

De in deze paragraaf opgenomen informatie kan o.a. bevatten:

— contactinformatie;

— gegevens betreffende leveranciers en belanghebbenden;

— juridische documenten (bijv. contracten, verzekeringspolissen, eigendomsakten); en

— andere servicedocumenten (bijv. contracten en dienstverleningsovereenkomsten).

8.3.2.4 Gebouwen, werkomgeving en bijbehorende voorzieningen

Strategieën voor werklocaties kunnen significant variëren en er kan een reeks opties beschikbaar zijn. In verband met verschillende soorten incidenten of bedreigingen kan het nodig zijn verschillende of meerdere opties voor werklocaties te implementeren. De passende tactiek zal ten dele worden bepaald door de omvang, sector en spreiding van activiteiten, door belanghebbenden en door de geografische basis. Openbare autoriteiten zullen bijvoorbeeld een frontlijndienstverlening in hun gemeenten moeten onderhouden, terwijl sommige organisaties kunnen opereren vanuit een ander land of werelddeel.

De organisatie behoort een strategie te bedenken om de gevolgen van het niet beschikbaar zijn van haar normale werklocatie(s) te verkleinen. Dit kan een of meer van de volgende opties omvatten:

a) alternatieve gebouwen (locaties) binnen de organisatie, met inbegrip van verplaatsing van andere activiteiten;

b) alternatieve gebouwen beschikbaar gesteld door andere organisaties (al dan niet zijnde een wederzijdse overeenkomst);

c) controlecentra voor noodsituaties;

d) alternatieve gebouwen die beschikbaar zijn gesteld door hierin gespecialiseerde derden;

e) vanuit huis of op afstand werken;

f) andere overeengekomen passende gebouwen; en

g) het benutten van alternatieve arbeidskrachten op een vastgestelde locatie.

Alternatieve gebouwen behoren zorgvuldig te worden gekozen door rekening te houden met een geografisch gebied dat kan worden getroffen door hetzelfde incident. Een incident zoals een natuurramp kan schade in uitgestrekte gebieden veroorzaken en essentiële diensten treffen zoals elektriciteit, gas, water en communicatie. Als een dergelijk risico wordt verwacht behoren alternatieve gebouwen ver verwijderd te zijn van een dergelijke mogelijk getroffen zone.

Als personeel verplaatst moet worden naar alternatieve gebouwen, behoort de afstand tot deze gebouwen zodanig te zijn dat het personeel bereid en in staat is ernaartoe te reizen, rekening houdend met mogelijke problemen die door het incident zijn veroorzaakt. Maar de alternatieve gebouwen behoren zich niet op een dermate korte afstand te bevinden dat het waarschijnlijk is dat ze door hetzelfde incident worden getroffen.

Gebruikmaken van alternatieve gebouwen voor continuïteitsdoelen behoort te worden ondersteund door een duidelijke mededeling of de vereiste middelen in de alternatieve gebouwen exclusief door de organisatie gebruikt kunnen worden. Als de alternatieve gebouwen met andere organisaties worden gedeeld, behoort een plan te worden ontwikkeld en gedocumenteerd om de kans te beperken dat deze gebouwen niet beschikbaar zijn.

In bepaalde situaties (bijv. een productielijn of een callcenter) kan het een passende oplossing zijn om in plaats van het personeel het werk te verplaatsen. Hierdoor kan op de alternatieve locatie behoefte zijn aan extra capaciteit of extra personeel (hetzij via overwerk of via werving) en kan het nodig zijn andere middelen beschikbaar te maken.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

8.3.2.5 Faciliteiten, uitrusting en verbruiksmaterialen

De organisatie behoort een inventaris te identificeren en te onderhouden van essentiële voorraden die haar geprioriteerde activiteiten ondersteunen.

Bepaalde voorzieningen en machines zijn mogelijk moeilijk te verwerven, zeer kostbaar (waardoor goedkeuring veel tijd kost) of hebben mogelijk een lange leveringstijd. Bij oplossingen om zulke middelen beschikbaar te maken moet mogelijk met dergelijke omstandigheden rekening worden gehouden. Het veranderen van de bedrijfspraktijken zoals voorraadbeheersing of gebouwbeheer, kunnen oplossingen bieden.

De aanpak hiervoor kan o.a. zijn:

— opslaan van extra goederen op een andere locatie;

— regelingen met derden betreffende levering van voorraad op korte termijn;

— verlegging van just-in-timeleveringen naar andere locaties;

— materialen opslaan in magazijnen of op verzendlocaties;

— subeenheden van de bedrijfsuitvoering overbrengen naar een alternatieve locatie waar voorraden aanwezig zijn;

— alternatieve/vervangende goederen identificeren; en

— gefaseerde identificatie van faciliteiten, uitrusting en multi-optieplanning.

Als activiteiten afhankelijk zijn van goederen van specialisten, behoort de organisatie de belangrijkste leveranciers en enkele leveringsbronnen te identificeren. Om de continuïteit van leveringen te beheren kunnen de volgende strategieën worden toegepast:

— het aantal leveranciers verhogen;

— leveranciers aanmoedigen, of van hen eisen dat zij bedrijfscontinuïteit hebben;

— contractuele en/of dienstverleningsovereenkomsten met de belangrijkste leveranciers; en

— alternatieve, capabele leveranciers identificeren.

Als activiteiten worden verplaatst behoort te worden geverifieerd dat leveranciers in staat zijn hun producten of diensten daadwerkelijk op de alternatieve locatie te leveren.

8.3.2.6 Systemen voor informatie en communicatietechnologie (ICT)

In veel organisaties kunnen activiteiten niet worden verricht zonder ICT-systemen en deze moeten worden hersteld voordat activiteiten kunnen worden hervat. Waar mogelijk en praktisch kan de organisatie handmatige bedrijfsactiviteiten implementeren terwijl haar ICT-diensten worden hersteld.

Technologie-opties zijn afhankelijk van de aard van de toegepaste technologie en de relatie met activiteiten, maar zijn typisch een combinatie van de volgende:

— binnen de organisatie getroffen voorziening;

— diensten die door een derde aan de organisatie worden verleend; en

— externe diensten waarop de organisatie zich abonneert.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

Om ICT-systemen te verschaffen die nodig zijn voor geprioriteerde activiteiten kunnen de volgende technieken worden toegepast:

— geografische spreiding, bijvoorbeeld dezelfde technologie toepassen op verschillende locaties die niet door hetzelfde verstorende incident worden getroffen;

— oudere uitrusting bewaren als noodvervanging of reserve; en

— gecontracteerde levering van uitrusting of herstelservice.

Vanwege de complexiteit van de ondersteunende technologieën zijn voor ICT-systemen vaak complexe voorzieningen nodig om te bewerkstelligen dat ze tijdig kunnen worden hersteld. Daarom behoort aandacht te worden geschonken aan:

— het bepalen van hersteltijddoelstellingen voor ICT-systemen, waardoor geprioriteerde activiteiten binnen hun hersteltijddoelstellingen kunnen worden hervat;

— speciale aandacht schenken aan de ligging van technologielocaties en de afstand ertussen;

— technologie distribueren over een aantal afzonderlijke locaties;

— toereikende faciliteiten verschaffen voor grotere aantallen gebruikers met toegang op afstand;

— het inrichten van zowel onbemande locaties ('dark sites') als bemande locaties;

— het verbeteren van telecommunicatieaansluitingen en toenemende niveaus van redundante routering;

— het voorzien in automatische 'failover' in plaats van handmatige interventie om de ICT-voorziening om te leiden;

— rekening houden met veroudering van ICT; en

— voorzien in extra aansluitingen en externe links.

Als een techniek van 'failover' van de ene locatie naar een andere is ingericht, kan het nodig zijn aandacht te schenken aan de afstand van het netwerkpad tussen de twee locaties. Als er een zeer grote afstand tussen de locaties bestaat, kan dit de reactie van het systeem vertragen en de ICT-systemen minder doeltreffend maken.

Als een organisatie haar ICT-systemen op meer dan één locatie host, kan er een mogelijkheid bestaan om een 'wederzijdse ICT-strategie' te implementeren waardoor de omvang van elke locatie wordt aangepast aan de gecombineerde ICT-capaciteit van meer dan één locatie.

Als een organisatie gebruikmaakt van gespecialiseerde technologieën of technologie op maat met een lange leveringstijd, kan het nodig zijn om te overwegen de bescherming van haar ICT te vergroten door speciale voorzieningen voor vervanging of herstel te treffen.

OPMERKING Verdere richtlijnen over ICT-continuïteit zijn opgenomen in ISO/IEC 27031, ISO/IEC 27002 en ISO/IEC 20000 (beide delen).

8.3.2.7 Transport

Mogelijk moet na een incident in vervoer worden voorzien voor:

— personeel dat naar huis is gestuurd als hun normale vervoermiddel niet beschikbaar is;

— personeel dat is overgeplaatst naar een alternatieve werklocatie; en

— middelen die op een andere locatie nodig zijn.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

De organisatie behoort vooraf opties te bepalen voor alternatieve vervoermiddelen die mogelijk nodig zijn na een verstorend incident. Hiertoe kunnen behoren:

— mogelijke scenario's identificeren van logistieke verstoringen die direct door een incident en ongebruikelijke situaties kunnen zijn veroorzaakt; en

— zorgen voor alternatieve logistieke middelen en routes door rekening te houden met verkeersomstandigheden, vervoermiddelen en andere logistieke netwerken;

— overeenkomsten met aanbieders van transport.

8.3.2.8 Financiën

De organisatie behoort opties vast te stellen om te waarborgen dat de nodige financiën beschikbaar zijn tijdens en na een verstorend incident. Dit kan inhouden:

— zorgen voor financiering van aankopen voor noodgevallen zoals voedsel, accommodatie, faciliteiten, verbruiksmaterialen en transport;

— vergoeden van onkosten van personeel;

— grote uitgaven voor, bijvoorbeeld, huren of kopen van gebouwen en uitrusting.

Om bescherming te bieden tegen misbruik of om verzekeringsclaims te faciliteren kan het nodig zijn om doeltreffende financiële beheersmaatregelen aan te tonen, door bijvoorbeeld te voorzien in formele registratie van kosten tijdens en na een verstorend incident.

8.3.2.9 Partners en leveranciers

Als een product, dienst of activiteit is uitbesteed, blijft de verantwoordelijkheid en aansprakelijkheid voor dat product, die dienst of activiteit bij de organisatie. Daarom behoort een organisatie zich ervan te vergewissen dat haar belangrijkste leveranciers over doeltreffende continuïteitsvoorzieningen beschikken. Een methode om dit te doen is om bewijs te verkrijgen van de uitvoerbaarheid van de continuïteitsplannen van de belangrijkste leveranciers en hun oefen- en onderhoudsprogramma's. Zie 8.3.1.5.

8.3.3 Bescherming en beperking

Voor geïdentificeerde risico's die behandeling nodig hebben en in overeenstemming met haar totale houding ten opzichte van risico, behoort de organisatie manieren te overwegen om de waarschijnlijkheid van een verstoring te verkleinen, de duur ervan te verkorten en de gevolgen ervan te beperken.

8.4 Vaststellen en implementeren van procedures voor bedrijfscontinuïteit

8.4.1 Algemeen

De organisatie behoort procedures in te stellen en te documenteren die voorzien in totale beheersing van de reactie op een verstorend incident en de activiteiten binnen de hersteltijddoelstellingen hervatten. De procedures voor bedrijfscontinuïteit behoren het passende interne en externe communicatieprotocol vast te stellen en behoren:

a) specifiek te zijn – met betrekking tot de stappen die bij een verstoring onmiddellijk genomen behoren te worden;

b) flexibel te zijn – zodat ze gebruikt kunnen worden om te reageren op bedreigingsscenario's waar niet op geanticipeerd is en op veranderende interne en externe omstandigheden;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

c) gericht te zijn – ze behoren duidelijk verband te houden met de gevolgen van gebeurtenissen die de bedrijfsactiviteiten mogelijk kunnen verstoren en te worden ontwikkeld op basis van vastgestelde veronderstellingen en een analyse van onderlinge verbanden; en

d) doeltreffend te zijn – in het minimaliseren van gevolgen, door implementatie van geschikte strategieën voor mitigatie.

8.4.2 Structuur voor reactie op incidenten

De organisatie behoort procedures en een managementstructuur in te stellen die haar in staat stellen zich voor te bereiden op verstorende incidenten, deze te beperken en er doeltreffend op te reageren.

Via de reactiestructuur behoort te worden bewerkstelligd dat:

— drempelwaarden voor gevolgen worden geïdentificeerd die het initiëren van een formele reactie rechtvaardigen;

— de aard en omvang van een verstorend incident en de mogelijke gevolgen ervan worden beoordeeld;

— maatregelen worden getroffen om te zorgen voor het welzijn van getroffenen;

— een passende reactie wordt geïnitieerd op een verstorend incident;

— er processen en procedures zijn voor het activeren, uitvoeren, coördineren en communiceren van de reactie;

— er middelen beschikbaar zijn om de processen en procedures voor het beheer van een verstorend incident te ondersteunen, teneinde de gevolgen ervan te minimaliseren, en

— communicatie met belanghebbenden plaatsvindt, met inbegrip van in het bijzonder, autoriteiten en de media.

De reactiestructuur behoort eenvoudig te zijn en snel gevormd te kunnen worden. Bij het vaststellen van de structuur behoort erop te worden gelet dat:

— een of meer competente personen beschikbaar zijn om de consequenties van het incident vast te stellen en om de gevolgen of potentiële gevolgen van het incident en de tijdschaal te evalueren;

— het mogelijk is om teams te mobiliseren die de leiding in handen nemen, het incident te beheersen en de passende reactie initiëren; en

— passende middelen worden gekozen, zoals personeel, contractanten, uitrusting en financiële middelen.

Grote of complexe organisaties kunnen gebruikmaken van een gelaagde aanpak om op incidenten te reageren en kunnen verschillende teams vormen die zich richten op reactie op incidenten, beheren van incidenten, communicatie, welzijn en hervatting van werkzaamheden. In kleine organisaties kunnen alle aspecten van reactie op incidenten door één team worden behandeld, maar deze behoren nooit de verantwoordelijkheid van een enkele persoon te zijn.

Elk team behoort procedures te hebben om de activiteiten te besturen en behoort te beschikken over personeel met de nodige verantwoordelijkheid, bevoegdheid en competentie. De competentie van personen en van het team kunnen worden aangetoond door training en oefening.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

8.4.3 Waarschuwingen en communicatie

8.4.3.1 Algemeen

De organisatie behoort waarschuwings- en communicatieprocedures vast te stellen, te implementeren en bij te houden. Via deze procedures behoort/behoren:

a) een incident te worden gedetecteerd en reactiepersoneel te worden gewaarschuwd;

b) een incident voortdurend te worden gemonitord;

c) interne communicatie plaats te vinden tussen de verschillende niveaus en functies binnen de organisatie;

d) externe communicatie plaats te vinden met belanghebbenden;

e) communicatie van belanghebbenden te worden ontvangen, gedocumenteerd en beantwoord;

f) communicatie van nationale of regionale adviesorganen voor risico's te worden ontvangen, gedocumenteerd en te worden beantwoord;

g) belanghebbenden te worden gewaarschuwd die mogelijk gevolgen ondervinden van een feitelijk of dreigend verstorend incident;

h) de beschikbaarheid van communicatiemiddelen tijdens een verstorend incident te worden bewerkstelligd;

i) gestructureerde communicatie met hulpdiensten te worden gefaciliteerd;

j) te worden bewerkstelligd dat meerdere organisaties en personeel die reageren samen kunnen werken;

k) essentiële informatie over het incident, genomen maatregelen en besluiten te worden vastgelegd; en

l) een communicatiefaciliteit te functioneren.

Een organisatie moet mogelijk een besluit nemen over al dan niet en in welke fase communiceren met externe belanghebbenden met betrekking tot haar waarschuwings- en communicatieprocedures. Veiligheid van mensen behoort de eerste overweging in deze besluitvorming te zijn. Het besluit en de beweegredenen behoren te worden gedocumenteerd.

Een organisatie die bijvoorbeeld gevaarlijke activiteiten uitvoert die de veiligheid van omwonenden kunnen bedreigen moet mogelijk bewerkstelligen dat omwonenden op de hoogte worden gesteld van mogelijk gevaar. Dit kan betekenen dat ze moeten weten hoe alarm wordt gegeven en hoe te reageren.

De organisatie behoort te beschikken over doeltreffende procedures en faciliteiten om waarschuwingen, alarm en externe communicatie snel te kunnen geven/doen plaatsvinden. Voor belanghebbenden met specifieke behoeften kunnen speciale voorzieningen vereist zijn, bijvoorbeeld voor ouderen en gehandicapten. Het waarschuwings- en communicatiesysteem behoort regelmatig te worden geoefend. Zie 8.5 voor richtlijnen voor oefenen.

8.4.3.2 Communicatieprocedures voor incidenten

Er behoren procedures te worden vastgesteld waardoor het, voorafgaand aan een potentieel incident, mogelijk is om:

— communicatie van nationale of regionale adviesorganen voor risico's te ontvangen, te documenteren en daarop te reageren; deze communicatie kan betrekking hebben op bedreigingen die op deze locatie kunnen voorkomen – zoals waarschuwingen voor een tsunami, aardbeving of een orkaan; en

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

— belanghebbenden die mogelijk worden getroffen door een feitelijk of dreigend verstorend incident te waarschuwen – als de organisatie een wettelijke of morele verantwoordelijkheid heeft om te waarschuwen.

Als een incident plaatsvindt, behoort de organisatie procedures te ontwikkelen die bewerkstelligen dat:

— het incident voortdurend wordt gemonitord, via lokale observatie of monitoring op afstand, en ontwikkelingen aan de juiste personen worden gecommuniceerd;

— gestructureerde communicatie met reactieteams plaatsvindt;

— meerdere organisaties en medewerkers die reageren onderling samenwerken in zoverre dit de verantwoordelijkheid is van de organisatie;

— er communicatie plaatsvindt tussen de verschillende hulpteams en de organisatie;

— er regelmatige communicatie plaatsvindt met personeel en anderen voor wie een zorgplicht bestaat, zoals bezoekers en contractanten – dit moet mogelijk in eerste instantie plaatsvinden op evacuatiepunten, op de thuislocatie of op alternatieve locaties; en

— essentiële informatie over het incident, genomen maatregelen en besluiten worden vastgelegd – door de personen die deze hebben genomen of door een persoon die voor elk team is benoemd voor de verslaglegging.

Er zijn ook procedures nodig om doeltreffende communicatie tussen belanghebbenden zoals klanten en de media te faciliteren.

De organisatie behoort de communicatie met deze partijen te onderhouden tot aan de terugkeer naar de normale bedrijfsactiviteiten waarbij het passend kan zijn een bericht uit te doen gaan dat het einde van het incident aangeeft.

8.4.3.3 Communicatiefaciliteiten voor incidenten

Deze procedures kunnen worden gefaciliteerd door gebruikmaking van een aangewezen of een ad-hoc-communicatiefaciliteit. Deze behoort op voldoende afstand van de getroffen locatie te zijn gesitueerd zodat de uitvoering niet wordt belemmerd door het incident en mag zich op dezelfde locatie bevinden als andere hulpverleningsfaciliteiten.

Bij de communicatie-uitrusting behoort er rekening mee gehouden te worden dat het incident mogelijk de werking van de normale communicatiemiddelen heeft aangetast, zodat een verscheidenheid aan alternatieven beschikbaar behoort te zijn, zoals:

— megafoons of geluidssystemen;

— reserve mobiele telefoons; en

— radio's met zend- en ontvangstinstallatie.

8.4.4 Bedrijfscontinuïteitsplannen

8.4.4.1 Algemeen

De organisatie behoort gedocumenteerde procedures vast te stellen waardoor de organisatie op een incident kan reageren, en hervatting en herstel van haar activiteiten op een passende manier kan afhandelen.

Deze procedures behoren betrekking te hebben op alle aspecten die te maken hebben met reactie op incidenten, met speciale aandacht voor het beveiligen van mensenlevens, en behoren aandacht te schenken

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

aan de eisen van de personen die de procedures gebruiken. Om de eisen vast te stellen kan het nuttig zijn om:

— degenen die de procedures gaan gebruiken te betrekken bij het ontwikkelen ervan;

— feedback van oefenen en lessen die zijn geleerd van verstorende incidenten te gebruiken.

Tijdschalen en prestatieniveaus behoren te zijn gebaseerd op de informatie die is verzameld gedurende de bedrijfsimpactanalyse (8.2.2) en de gekozen strategie voor bedrijfscontinuïteit (8.3.1).

De volgende aspecten behoren binnen elk plan duidelijk identificeerbaar te zijn:

— doel en toepassingsgebied;

— doelstellingen en criteria voor succes in termen van geprioriteerde activiteiten;

— criteria en procedures voor activering;

— procedures voor implementatie;

— rollen, verantwoordelijkheden en bevoegdheden;

— eisen en procedures voor communicatie;

— interne en externe onderlinge afhankelijkheden en interacties;

— vereiste middelen; en

— informatiestromen en documentatieprocessen.

Bij het afhandelen van een verstorend incident is er een aantal maatregelen dat mogelijk moet worden overwogen. Deze behoren te worden opgenomen in gedocumenteerde procedures (8.4.4.2 en 8.4.4.3) en omvatten:

a) reageren op het incident en het incident beoordelen:

   1) Wat gebeurde er en wat was de toedracht?

   2) Welke delen van de organisatie en welke belanghebbenden zijn of zouden kunnen zijn getroffen?

   3) Wat is de geanticipeerde duur van het incident en de gevolgen ervan? en

   4) Kan het incident worden beheerd door routinevoorzieningen?

b) de beoordeling van het incident evalueren tegen de activatiecriteria voor elk van de procedures;

c) een incident uitroepen en de procedures activeren als activatiecriteria zijn gesteld;

d) stabilisatie-, continuïteits-, hervattings- en herstelactiviteiten;

e) de locatie voor het beheren van het incident vaststellen en in werking stellen;

f) kwesties en activiteiten prioriteren die aan de orde zijn in het kader van het beheren van het incident en de gevolgen ervan;

g) alle geactiveerde procedures beheersen en coördineren;

h) vervangende locaties activeren of vaststellen voor het herstellen van de IT of van andere infrastructuur en voor de tijdelijke uitvoering van de activiteiten van de organisatie;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

i) het incident tijdens de duur monitoren;

j) plannen als reactie op veranderende omstandigheden beoordelen en aanpassen;

k) neerschalen van plannen en terugkeren naar routinebeheer als betrouwbare capaciteit is bereikt;

l) een nabespreking houden en leermogelijkheden identificeren; en

m) goed bestuur bewerkstelligen en ordening en veiligstelling van documentatie die is verzameld tijdens het beheer en herstel na het incident.

Om te bereiken dat de organisatie tijdig de levering van producten en diensten hervat, behoren de gedocumenteerde procedures voor het hervatten van elke activiteit:

— te voldoen aan de hersteltijddoelstelling van de activiteit die dat product of die dienst ondersteunt; en

— voldoende betrouwbaar te zijn.

Dit kan worden bereikt door:

— eigendom of beheersing van de methoden en middelen om de procedure te bepalen; en

— contracten, overeenkomsten of dienstverleningsovereenkomsten met derden.

Om te bewerkstelligen dat de uitvoering van de procedures niet wordt getroffen door dezelfde verstoring, kan de organisatie voorzorgsmaatregelen nemen, bijvoorbeeld personeel en IT over meerdere locaties verdelen. Een totale scheiding voor alle schalen en soorten incidenten is echter niet mogelijk, en deze beperking behoort te worden geïdentificeerd en goedgekeurd door de directie. Deze beperking kan worden uitgedrukt in termen van afstand, minimum aan personeel of ernst en kan worden vastgesteld door de reactie van burgerlijke autoriteiten op een ernstig en/of wijdverspreid incident.

8.4.4.2 Inhoud van plannen voor bedrijfscontinuïteit

Een plan voor bedrijfscontinuïteit kan bestaan uit een enkele gedocumenteerde procedure of meerdere procedures die alle eisen en het toepassingsgebied omvatten van het BCMS.

Het doel, het toepassingsgebied en doelstellingen van elke gedocumenteerde procedure behoren te zijn gedefinieerd en begrijpelijk te zijn voor de personen die deze in werking stellen. Relaties met andere vereiste en relevante gedocumenteerde procedures of documenten behoren duidelijk te worden vermeld en de methode om ze te verkrijgen en te bereiken behoren te worden omschreven.

Binnen de plannen voor bedrijfscontinuïteit behoren de volgende aspecten duidelijk identificeerbaar te zijn (zie ook 8.4.4.3):

a) rollen en verantwoordelijkheden:

   1) gedefinieerde rollen, verantwoordelijkheden en bevoegdheden voor personen en teams die het bedrijfscontinuïteitsplan gebruiken. Als het bedrijfscontinuïteitsplan meer dan een gedocumenteerde procedure bevat, behoren de rollen, verantwoordelijkheden en bevoegdheden voor elke procedure te worden gedefinieerd; en

   2) richtlijnen en criteria met betrekking tot wie bevoegd is om de procedures in werking te stellen en onder welke omstandigheden dit plaatsvindt volgens gedefinieerde escalatiestadia.

b) activeren en deactiveren:

   1) een proces om de reactie van de organisatie op een verstorend incident te activeren en binnen elke gedocumenteerde procedure, de activatiecriteria en -procedures daarvan. Het kan relevant zijn om te overwegen of dit binnen of buiten normale werkuren plaatsvindt;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

2) een proces voor deactiveren van teams als het incident voorbij is; en

3) primaire en alternatieve plaatsen voor bijeenkomsten.

c) beheer van incidenten:

1) beheren van de directe gevolgen van een verstorend incident met gepaste aandacht voor het welzijn van getroffen personen (met inbegrip van teamleden), opties om te reageren op de verstoring (deze kunnen worden omschreven als strategisch, tactisch en operationeel) en voorkoming of verder verlies of niet beschikbaar zijn van geprioriteerde activiteiten;

2) elke gedocumenteerde procedure behoort te beschikken over:

i. implementatieprocedures die maatregelen en taken identificeren die uitgevoerd moeten worden, in het bijzonder in verband met hoe de organisatie haar geprioriteerde activiteiten binnen de vastgestelde tijdsbestekken vervolgt of herstelt;

ii. eisen voor middelen (8.3.2) die relevant zijn voor de gedocumenteerde procedure; en

iii. de middelen om belangrijke informatie over het incident, genomen maatregelen en besluiten vast te leggen.

d) contactinformatie binnen elke gedocumenteerde procedure:

1) contactgegevens voor teamleden en anderen met rollen en verantwoordelijkheden – als lokale wetgeving voor gegevensbescherming geldt, behoren contactgegevens hiermee in overeenstemming te worden bewaard; en

2) contact- en mobilisatiegegevens voor relevante instanties, organisaties en middelen die mogelijk nodig zijn.

e) communicatie (8.4.3):

1) gegevens over de manier waarop en de omstandigheden waaronder de organisatie communiceert met werknemers en hun familieleden, belanghebbenden en contactpersonen voor noodsituaties; en

2) gegevens van de mediareactie van de organisatie na een incident, met inbegrip van haar communicatiestrategie, voorkeursinterface met de media, richtlijnen of sjablonen voor het opstellen van mediaberichten en identificatie van geschikte woordvoerders.

8.4.4.3 Specifieke soorten procedures

8.4.4.3.1 Procedures voor incidentmanagement/strategisch management

Het doel van incidentmanagement is om te bewerkstelligen dat de reactie van de organisatie op een verstorend incident op strategisch niveau doeltreffend is.

De procedures behoren de basis te omvatten voor het beheren van alle mogelijke aangelegenheden waar een organisatie tijdens een incident mee te maken heeft, met inbegrip van zaken met betrekking tot belanghebbenden.

De organisatie behoort een locatie, vertrek of ruimte vast te stellen vanwaaruit een incident wordt beheerd. Als dat heeft plaatsgevonden behoort deze locatie het centrale punt voor de reactie van de organisatie te zijn. Ook behoort een alternatief ontmoetingspunt te worden aangewezen voor het geval dat de primaire locatie niet toegankelijk is. Elke locatie behoort toegang te hebben tot geschikte middelen waardoor het team dat het incident beheert onmiddellijk doeltreffende beheeractiviteiten kan initiëren.

De locatie kan zo eenvoudig zijn als een hotelkamer of de woning van een medewerker. De locatie mag zo complex zijn als een specifiek 'commandocentrum' met pc's, videoconferentie en meerdere telefoons. In eerste instantie kan het nodig zijn een virtuele bijeenkomst of een vergadering elders te houden, bijv.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

telefonisch, via tele- of videoconferentie, zodat belangrijke beslissingen onmiddellijk genomen kunnen worden.

De gekozen locatie behoort voor het doel geschikt te zijn en kan omvatten:

— ruimte voor het vereiste aantal personen;

— doeltreffende primaire en secundaire communicatiemiddelen; en

— faciliteiten voor toegang tot en delen van informatie, met inbegrip van het monitoren van de nieuwsmedia.

Andere reactieteams hebben mogelijk gelijksoortige faciliteiten nodig.

8.4.4.3.2 Communicatieprocedures

Communicatieprocedures kunnen worden opgenomen in reactieprocedures voor incidentbeheer of kunnen gescheiden worden gehouden om indien van toepassing door een ander team te worden gebruikt.

Er is behoefte aan het actief beheren en coördineren van de vele berichten die tijdens het incident worden afgegeven en ontvangen. Deze procedure behoort te bevatten:

a) gegevens over de manier waarop en de omstandigheden waaronder de organisatie communiceert met werknemers en hun familieleden, contactpersonen voor noodsituaties en andere belanghebbenden;

b) gegevens over de communicatie van de organisatie met de media na een incident; dit omvat:

   1) de communicatiestrategie betreffende het incident;

   2) bij voorkeur te gebruiken interface met de media;

   3) richtlijn of model om een verklaring aan de media op te stellen; en

   4) passende aantallen getrainde, competente woordvoerders die bevoegd zijn om informatie aan de media te verstrekken.

Voorbereide informatie kan vooral nuttig zijn in de vroege stadia van een incident. Het stelt een organisatie in staat gegevens te verstrekken over de organisatie en haar bedrijfsactiviteiten terwijl informatie over het incident nog wordt vastgesteld.

Het kan passend zijn om:

— een geschikte ontmoetingsplaats vast te stellen om het onderhoud met de media of andere groepen belanghebbenden te ondersteunen;

— een passend aantal competente, getrainde mensen aan te stellen om telefonische vragen om informatie van de pers te beantwoorden;

— alle voor de organisatie beschikbare communicatiekanalen te gebruiken, met inbegrip van sociale media; en

— achtergrondinformatie over de organisatie en haar bedrijfsactiviteiten voor te bereiden (deze informatie behoort voor openbaarmaking te zijn goedgekeurd).

Met belangen- of actiegroepen die collectief macht of invloed op de organisatie hebben moet mogelijk ook rekening worden gehouden.

Er behoort een proces te zijn om communicatie met andere belangrijke belanghebbenden te identificeren en te prioriteren. Het kan nodig zijn om een afzonderlijke procedure te ontwikkelen om belanghebbenden te

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

beheren, om criteria te bieden om prioriteiten te stellen en om personen toe te wijzen aan een stakeholder of groep stakeholders.

8.4.4.3.3 Procedures voor veiligheid en welzijn

Organisatie hebben een directe verantwoordelijkheid om het welzijn van medewerkers, contractanten, bezoekers en klanten te beschermen als een incident een direct risico vormt voor leven, levensonderhoud en welzijn. Er behoort speciale aandacht te worden gegeven aan groepen met beperkingen of met andere specifieke behoeften (bijv. zwangerschap, tijdelijke handicap i.v.m. verwonding). Vooruit plannen om aan deze eisen te voldoen kan risico's verkleinen en betrokkenen geruststellen. De langetermijngevolgen van incidenten mogen niet worden onderschat. Passende strategieën ontwikkelen ter ondersteuning van menselijk welzijn kan direct het fysieke en mentale herstel binnen de organisatie bevorderen. Hierbij behoort rekening gehouden te worden met relevante maatschappelijke en culturele overwegingen.

Bij hulpverlening behoort met de volgende elementen rekening te worden gehouden:

— evacuatie van de locatie (met inbegrip van interne schuilplaats) en verzamelpunten;

— het mobiliseren van veiligheids-, eerste hulp- of evacuatieteams; en

— het lokaliseren van en zorg dragen voor personen die ter plaatste of in de directe omgeving waren.

Voor de volgende aspecten kunnen ook voorzieningen worden getroffen:

— vertaaldiensten;

— hulp bij vervoer inclusief instructies, indien nodig;

— benoemde contactpersonen en contactinformatie voor hulpverleningsdiensten, de aangewezen instanties en EHBO'ers;

— personeel of contractanten lokaliseren;

— telefonische hulpverlening beheren; en

— rehabilitatie en counseling (fysiek en mentaal).

De organisatie kan middelen inschakelen om diensten te bieden om getroffen personeel na een incident te horen, raad en langetermijnhulp te geven. Deze dienstverlening kan extern worden ingehuurd of kan worden verleend als aanvulling op bestaande bedrijfsgezondheids- en ondersteuningsprogramma's voor personeel.

De organisatie behoort personeel in dienst te hebben met passende bevoegdheidsniveaus om waar van toepassing contacten te onderhouden met hulpverleningsdiensten. Hulpverleningsdiensten spelen een primaire rol bij het beschermen van levens en het verlichten van lijden tijdens noodsituaties. Daarom kunnen vroegtijdige contacten, planning en real-time coördinatie van incidenten tussen de organisatie en de eerstehulpverleners en hulpverleningsdiensten de doelmatigheid van hulp na een incident verbeteren.

Alle middelen behoren specifiek te worden geïdentificeerd. Een hulpmiddel behoort tijdig beschikbaar te zijn en het vermogen te hebben om de beoogde functie te verrichten. Er behoort rekening gehouden te worden met de beperkingen die voor het gebruik van het hulpmiddel gelden, en het toepassen ervan behoort niet meer aansprakelijkheden met zich mee te brengen dan het niet-gebruiken. De kosten van het hulpmiddel behoren niet zwaarder te wegen dan de voordelen.

Tot middelen die nodig kunnen zijn voor reacties met betrekking tot welzijn behoren, maar zijn niet beperkt tot de volgende:

— de locaties, hoeveelheden, toegankelijkheid, uitvoerbaarheid en onderhoud van uitrusting (bijv. voor zwaar gebruik, bescherming, vervoer, monitoren, ontsmetting, reactie, persoonlijke bescherming);

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

— benodigdheden (bijv. medische artikelen, artikelen voor persoonlijke hygiëne, verbruiksgoederen, administratieve benodigdheden, ijs);

— energiebronnen (bijv. elektrische, brandstof);

— noodstroomvoorziening (generatoren);

— communicatiesystemen;

— voedsel en water;

— technische informatie;

— kleding en onderdak;

— gespecialiseerd personeel (bijv. medisch, religieus, vrijwilligersorganisaties, managementpersoneel van rampenbestrijdings-/hulpverleningsdiensten, generiek inzetbare nutsvoorzieningen, begrafenisondernemers en particuliere aannemers);

— gespecialiseerde vrijwilligersgroeperingen (bijv. op het gebied van amateur radio, religieuze hulporganisaties, liefdadigheidsorganisaties);

— vrijwillige, gemeentelijke en noodhulpondersteuning; en

— externe internationale, nationale, provinciale, van stammen, territoriale en lokale instanties.

8.4.4.3.4 Procedures voor berging en veiligheid

De organisatie kan gedocumenteerde procedures voorbereiden die betrekking hebben op berging en veiligheid. Deze kunnen richtlijnen bevatten betreffende:

— bergingsprioriteiten voor faciliteiten, uitrusting en gedocumenteerde informatie; en

— veiligheid van de locatie nadat deze is overgedragen door de hulpverleningsdiensten.

— de organisatie kan voorafgaand aan het incident gespecialiseerde bergingsdiensten aanstellen. Doeltreffende berging van faciliteiten, uitrusting en gedocumenteerde informatie kan de gevolgen beperken en een snellere terugkeer naar een normale werksituatie mogelijk maken.

8.4.4.3.5 Procedures voor hervatting van activiteiten

Elke procedure behoort te specificeren wat de:

— geprioriteerde activiteiten zijn die hervat moeten worden;

— tijdsbestekken zijn waarbinnen ze hervat moeten worden;

— herstelniveaus zijn die voor elke geprioriteerde activiteit nodig zijn; en

— situaties zijn waarin de procedure kan worden toegepast.

Elke procedure behoort indien van toepassing gedetailleerd te vermelden welke middelen op verschillende tijdstippen nodig zijn om de doelstellingen te halen. Deze vermelding kan omvatten:

— aantallen middelen;

— vaardigheden en kwalificaties;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

— technische uitrusting;

— telecomfaciliteiten; en

— beschikbaarheid van gecontracteerde middelen, middelen op basis van wederzijdse hulp of middelen die waarschijnlijk beschikbaar zijn.

Ingeval het ontbreken van een dienst of hulpmiddel een bedreiging vormt voor het hervatten van activiteiten, behoren escalatiemaatregelen te worden gedefinieerd. Deze maatregelen kunnen omvatten:

— mobilisatie van externe middelen en middelen van derden;

— communicatie van herstelmaatregelen; en

— procedures voor het implementeren van handmatige alternatieven, systeemherstel, alternatieve processen enz.

Aan middelen gestelde eisen behoren te worden gedocumenteerd en kunnen omvatten:

— essentiële registraties (hardcopy en elektronisch);

— operationele en procedurele handleidingen;

— technische herstelplannen en procedures betreffende IT;

— locatie van externe opslagfaciliteiten die door de organisatie worden gebruikt;

— alternatieve locaties;

— bevoegdheden/machtigingen voor het betalen van nooduitgaven.

— een lijst van personeel met expertise die de uitvoerende afdelingen nodig heeft;

— documentatie van IT-infrastructuur en toepassingen;

— leverancier van ondersteuning voor telecommunicatie;

— leverancier van kantoor- en gespecialiseerde uitrusting; en

— contactinformatie nutsvoorzieningen (water, elektriciteit enz.).

8.4.4.3.6 Herstel van systemen voor informatie- en communicatietechnologie (ICT)

De procedures voor hervatting van activiteiten behoren de ICT-systemen te vermelden waar de hervatting afhankelijk van is en alle bestaande ICT-continuïteitsprocedures.

Eventuele ICT-continuïteitsprocedures behoren minimaal betrekking te hebben op:

— inwerkingstelling van de vereiste ICT-reactie en herstel en inzetten van ICT-personeel;

toegang tot back-upgegevens en verkrijging van alternatieve dienstverlening; en

— herstel van gegevens, informatiediensten en communicatie en ondersteuning;

— het tijdschema van beschikbaarheid en capaciteitseisen die vermeld zijn in de procedures voor bedrijfscontinuïteit waardoor activiteiten hun hersteltijddoelstellingen kunnen halen.

OPMERKING Verdere richtlijnen zijn te vinden in ISO 27031.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

8.4.5 Herstel

De organisatie behoort te beschikken over gedocumenteerde procedures om bedrijfsuitvoering te herstellen en hervatten na de tijdelijke maatregelen die werden getroffen ter ondersteuning van de eisen voor normale bedrijfsvoering na een incident. Deze behoren invulling te geven aan relevante eisen betreffende audit en het besturen van de onderneming.

Het doel van herstel is om bedrijfsactiviteiten ter herstellen ter ondersteuning van de normale bedrijfseisen na een verstorend incident. Terugkeren naar een normale situatie kan worden bereikt door:

— herstel van de schade die door het incident is veroorzaakt;

— de bedrijfsuitvoering van de tijdelijke locatie terugbrengen naar de herstelde oorspronkelijke bedrijfslocatie; of

— verhuizing naar een nieuwe locatie.

Een beslissing over de beste manier om 'terug te keren naar normaal' behoort te worden genomen op basis van de ernst van de schade die door het incident is veroorzaakt en schattingen betreffende de tijd die ermee gemoeid is om de nodige faciliteiten in te richten.

De gedocumenteerde procedures behoren te voorzien in een gedetailleerde beoordeling van de situatie en de gevolgen ervan en de vaststelling van taken en stappen die nodig zijn voor herstel. Gedurende het herstel kan voor de organisatie de noodzaak bestaan om:

a) middelen en infrastructuur voor herstel vast te stellen;

b) de bedrijfsactiviteiten te verrichten in een herstelfaciliteit;

c) beschadigde faciliteiten te herstellen;

d) te zorgen voor noodinkopen en -financiering;

e) uitrusting in beschadigde faciliteiten te bergen;

f) claims in te dienen tegen bestaande verzekeringspolissen;

g) extra menskracht te verkrijgen ter ondersteuning van het herstel;

h) opties te kiezen voor herstel en terugkeer naar normaal;

i) de bedrijfsuitvoering over te brengen naar herstelfaciliteiten;

j) verloren gedocumenteerde informatie herstellen;

k) met relevante belanghebbenden te communiceren met de juiste frequentie;

l) de bedrijfsuitvoering te normaliseren op de herstelde faciliteiten;

m) een beoordeling na herstel uit te voeren; en

n) gepaste zorgvuldigheid te betrachten bij de eisen betreffende audit en het besturen van de onderneming.

De gedocumenteerde procedures voor herstel behoren te voorzien in hervatting van alle activiteiten en niet alleen van activiteiten die zijn geïdentificeerd als geprioriteerde activiteiten. Hiermee wordt onderkend dat activiteiten met een lagere prioriteit op een bepaald tijdstip moeten worden hervat en eisen voor middelen inhouden (8.3.2).

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

8.5 Oefening en testen

8.5.1 Algemeen

De procedures en voorzieningen voor de bedrijfscontinuïteit van een organisatie kunnen niet betrouwbaar worden geacht totdat ze geoefend zijn en tenzij ze actueel zijn gehouden. Oefening is essentieel om te waarborgen dat de strategieën, het beleid, de plannen en procedures die zijn ingericht toereikend zijn, en voldoen aan de doelstellingen voor bedrijfscontinuïteit. Oefening ontwikkelt samenwerking, competentie, vertrouwen en kennis, en behoort de personen erbij te betrekken die de procedures mogelijk moeten uitvoeren.

8.5.2 Oefenprogramma

Hoe goed ontworpen en uitgedacht een procedure ook lijkt te zijn, een reeks robuuste en realistische oefeningen zal aspecten voor verbetering identificeren.

Een oefenprogramma behoort consistent te zijn met het toepassingsgebied van de procedures voor bedrijfscontinuïteit, en gepaste aandacht te hebben voor relevante wet- en regelgeving.

Er behoort een oefenprogramma te worden ontworpen dat gedurende een bepaalde tijd objectieve zekerheid toont dat de procedures en voorzieningen voor bedrijfscontinuïteit zoals geanticipeerd werken indien ze nodig zijn. Het programma behoort:

a) de technische, logistieke, administratieve, procedurele en andere uitvoerende systemen van de procedures te oefenen;

b) alle personen met verantwoordelijkheden binnen die procedures te oefenen;

c) de voorzieningen en infrastructuur voor bedrijfscontinuïteit te oefenen (met inbegrip van bijvoorbeeld incidentmanagementlocaties en werkgebieden); en

d) het herstel van de technologie en telecommunicatie te valideren, met inbegrip van de beschikbaarheid en verplaatsing van personeel.

De mate en complexiteit van de oefeningen behoort in overeenstemming te zijn met de doelstellingen voor de bedrijfscontinuïteit van de organisatie.

Er behoort een gepland schema van oefeningen te bestaan. De frequentie van de oefeningen behoort af te hangen van de behoeften van de organisatie, de omgeving waarin zij actief is en de eisen van belanghebbenden. Het oefenprogramma behoort echter ook flexibel te zijn en rekening te houden met veranderingen binnen de organisatie en de uitkomst van voorgaande oefeningen. Een significante verandering in de organisatie kan aanleiding geven om een oefening op te nemen die de gewijzigde voorzieningen onderzoekt.

Het oefenprogramma behoort de rollen van alle partijen in aanmerking te nemen, met inbegrip van belangrijke derde aanbieders, leveranciers en anderen die naar verwachting deelnemen aan herstelactiviteiten. Een organisatie kan dergelijke partijen in haar oefeningen opnemen en kan deelnemen aan oefeningen die zij organiseren.

Het toepassingsgebied en de mate van detail van de oefeningen behoren zich gedurende het programma te ontwikkelen gebaseerd op de ervaring, middelen en capaciteiten van de organisatie. In vroege stadia van ontwikkeling kan oefenen en testen worden beperkt tot het gebruik van controlelijsten, gebruikelijke procedures en bewustzijnsoefeningen. Als het programma volwassener wordt, kan het worden uitgebreid met table-topoefeningen en simulaties van werkelijke situaties.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

8.5.3 Bedrijfscontinuïteitsplannen oefenen

Oefeningen zijn activiteiten die zijn ontworpen om te onderzoeken in hoeverre de organisatie, nadat zij is geconfronteerd met specifieke verstorende scenario's, in staat is te reageren, te herstellen en de vastgelegde bedrijfsfuncties doeltreffend te blijven uitvoeren. De organisatie behoort gebruik te maken van oefeningen en van de gedocumenteerde resultaten van oefeningen om de doeltreffendheid en gereedheid van haar bedrijfscontinuïteitsplannen te bewerkstelligen.

Elke oefening en test behoort duidelijk gedefinieerde doelen en doelstellingen te hebben en gebaseerd te zijn op een scenario dat passend is om deze te halen.

Oefeningen kunnen:

— anticiperen op een vooraf vastgestelde uitkomst, bijvoorbeeld op basis van een vooraf opgesteld(e) planning en toepassingsgebied; en

— de organisatie in staat stellen innovatieve oplossingen te ontwikkelen.

Oefeningen behoren realistisch, zorgvuldig gepland en overeengekomen te zijn met relevante partijen, zodat het risico minimaal is dat bedrijfsprocessen worden verstoord en dat zich een incident voordoet als direct gevolg van de oefening. Dit kan worden bereikt door de oefening uit te voeren binnen een beheerste en geïsoleerde omgeving, mits hierdoor niet de integriteit van de geteste doelstellingen wordt geschaad.

De organisatie behoort oefenscenario's te ontwerpen waarin wordt voldaan aan de doelstellingen van de oefening en kan hierin bedreigingen uit de risicobeoordeling of andere passende gebeurtenissen verwerken.

De doeltreffendheid van sommige aspecten van bedrijfscontinuïteit vereist dat bepaalde personen of personen die specifieke posities bekleden over specifieke kennis, vaardigheden en inzichten beschikken. Deze situatie behoort voorafgaand aan de oefening te bestaan zodat de deelnemers deze specifieke kennis, vaardigheden en inzichten in relevante scenario's en simulaties kunnen toepassen.

Oefeningen behoren zo te worden ontworpen en uitgevoerd dat hierdoor een of meer van de volgende aspecten worden bewerkstelligd:

a) verificatie dat hersteltijddoelstellingen haalbaar zijn (8.3.1);

b) vertrouwen dat informatie vereist door activiteiten voldoende courant is (8.3.2.3);

c) verbeterd inzicht in afhankelijkheden van de bedrijfscontinuïteit van leveranciers en van andere belanghebbenden;

d) verbeterd bewustzijn van de context en prioriteiten van de organisatie;

e) verbeterd inzicht in de inhoud en het gebruik van procedures voor bedrijfscontinuïteit;

f) verbeterd vertrouwen in reactie op incident;

g) een kans om bekwaamheden te verbeteren;

h) een beoordeling van het nut en de toepasselijkheid van bedrijfscontinuïteitsstrategieën;

i) een evaluatie van de geschiktheid van ontworpen capaciteiten en toewijzing van middelen;

j) een identificatie van voorheen niet-gedocumenteerde eisen en werkwijzen die bij het beheren van een incident of verstoring zijn toegepast;

k) een kans om andere onvolkomenheden in de vastgelegde procedures voor bedrijfscontinuïteit en de implementatie ervan te identificeren;

l) de verzekering dat procedures voor bedrijfscontinuïteit indien vereist geïmplementeerd kunnen worden;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

m) toegenomen vertrouwen van belanghebbenden betreffende het voorbereid zijn van de organisatie; en

n) een middel om te voldoen aan wettelijke en contractuele eisen, of aan eisen die gelden voor het besturen van de organisatie.

Oefeningen kunnen diverse verschillende formats hebben. Het besluit of een bepaald soort oefening geschikt is behoort genomen te worden op basis van de context voor BCM, de doelstellingen voor de oefening, budget, beschikbaarheid van deelnemers en de tolerantie van de organisatie ten opzichte van verstoring van de uitvoering die door de oefening wordt veroorzaakt.

De belangrijkste soorten oefeningen zijn omschreven in ISO 22398 (*Societal security – Guidelines for exercises and testing*).

Als onderdeel van de oefening behoort een beoordeling ingepland te worden om met alle deelnemers belangrijke punten en geleerde lessen te bespreken. Deze informatie behoort te worden gedocumenteerd, en voor zover van toepassing behoren de procedures te worden geactualiseerd.

De organisatie behoort na de oefening een nabespreking te houden en te analyseren in welke mate de doelen en doelstellingen van de oefening zijn gehaald. Na de oefening behoort een rapport te worden opgesteld dat aanbevelingen bevat en een tijdschema voor de implementatie ervan.

Lessen uit oefeningen en echte incidenten behoren tijdens toekomstige oefeningen opnieuw te worden doorgenomen. Oefeningen die ernstige gebreken of onnauwkeurigheden in de procedures laten zien behoren opnieuw te worden uitgevoerd nadat corrigerende maatregelen zijn genomen.

Oefeningen en testen kunnen de volgende voordelen opleveren:

— validatie van gepland toepassingsgebied, aannamen en strategieën;

— zekerheid over het correct functioneren van technische faciliteiten en middelen;

— zekerheid over de capaciteit van de alternatieve faciliteiten;

— toegenomen doelmatigheid en reducties in de tijd die nodig is om processen uit te voeren (bijv. gebruikmaken van herhalingsoefeningen om reactietijden te verkorten);

— toegenomen bewustzijn van belanghebbenden; en

— ontwikkeling van competentie en bewustzijn bij deelnemers.

9 Evaluatie van de prestaties

9.1 Monitoren, meten, analyseren en evalueren

9.1.1 Algemeen

In de procedures voor de prestaties en de doeltreffendheid van het BCMS behoren prestatiemeeteenheden te worden vastgesteld, beoordeling van het beschermen van geprioriteerde activiteiten, bevestiging van het voldoen aan eisen, onderzoek van historisch bewijs en het gebruiken van gedocumenteerde informatie om vervolgens corrigerende maatregelen te faciliteren. In de procedures behoren ook beleid en doelstellingen voor bedrijfscontinuïteit te worden opgenomen.

De procedures voor het monitoren van prestaties behoren de volgende aspecten te omvatten:

a) prestatiemeeteenheden vaststellen met inbegrip van kwalitatieve en kwantitatieve metingen die passen bij de behoeften van de organisatie;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

b) monitoren in welke mate beleid en doelstellingen voor bedrijfscontinuïteit van de organisatie worden gehaald;

c) identificeren wanneer monitoren en meten plaats behoren te vinden;

d) beoordelen van de prestatie van processen, procedures en functies die de geprioriteerde activiteiten beschermen;

e) proactieve metingen van de prestatie die de naleving van het BCMS monitoren tegen van toepassing zijnde wetgeving en statutaire en regelgevingseisen.

f) reactieve prestatiemetingen om fouten, incidenten, afwijkingen (met inbegrip van bijna-fouten en vals alarm) te monitoren en ander historisch bewijs van gebrekkige prestatie van het BCMS; en

g) gegevens en resultaten van monitoring en meting voldoende registreren om analyse van corrigerende maatregelen mogelijk te maken.

De procedures behoren te voorzien in regelmatige systematische meting, monitoring en evaluatie van de bedrijfscontinuïteit van de organisatie. Om zowel het managementsysteem als de uitkomsten te meten behoort een reeks prestatie-indicatoren te worden ontwikkeld. Metingen kunnen zowel kwantitatief als kwalitatief zijn. Prestatie-indicatoren kunnen management-, uitvoerende of economische indicatoren zijn. Indicatoren behoren nuttige informatie te leveren om zowel successen als gebieden die gecorrigeerd of verbeterd moeten worden te identificeren.

Het BCMS behoort op basis van monitoren en meten gegevens te leveren waardoor patronen kunnen worden geïdentificeerd en informatie over de prestatie wordt verkregen. Deze gegevens behoren te worden gebruikt om te bewerkstelligen dat het beleid en de doelstellingen van de organisatie worden gehaald, alsmede om corrigerende maatregelen en gebieden voor verbetering te identificeren.

De organisatie behoort in staat te zijn om aan te tonen dat zij wettelijke en andere eisen die zij onderschrijft heeft geïdentificeerd, geëvalueerd en deze is nagekomen.

Van alle periodieke evaluaties en de resultaten daarvan behoren registraties te worden bijgehouden.

De organisatie behoort de uitkomsten van monitoren en meten te analyseren en met geplande tussenpozen te evalueren.

9.1.2 Evaluatie van procedures voor bedrijfscontinuïteit

De organisatie behoort haar procedures voor bedrijfscontinuïteit te evalueren, om de continue geschiktheid, toereikendheid en doeltreffendheid ervan te bewerkstelligen.

De evaluaties behoren betrekking te hebben op de mogelijke behoefte aan veranderingen met betrekking tot beleid, doelstellingen, strategieën en andere elementen van het BCMS in het licht van aspecten als oefenresultaten, post-incidentbeoordelingen, veranderende omstandigheden en verplichtingen inzake continue verbetering.

Evaluaties kunnen de vorm hebben van interne of externe audits of zelfbeoordelingen. De frequentie en timing van beoordelingen kunnen worden beïnvloed door wet- en regelgeving, afhankelijk van de afmeting, aard en juridische status van de organisatie. Ze kunnen ook worden beïnvloed door de eisen van belanghebbenden.

Een evaluatie van de procedures voor de bedrijfscontinuïteit van de organisatie behoort te verifiëren dat:

a) alle belangrijke producten en diensten en hun ondersteunende activiteiten en middelen zijn geïdentificeerd en opgenomen in de bedrijfscontinuïteitsstrategie van de organisatie;

b) het beleid, de strategieën, het kader en procedures betreffende bedrijfscontinuïteit nauwkeurig haar prioriteiten en eisen (de doelstellingen van de organisatie) weerspiegelen;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

c) de competentie van personen en de bedrijfscontinuïteit van de organisatie doeltreffend en geschikt zijn en management, controle, beheersing en coördinatie mogelijk maken van de reactie van de organisatie op een verstorend incident.

d) de oplossingen van de organisatie voor bedrijfscontinuïteit doeltreffend, actueel en geschikt zijn, en passen bij het risiconiveau dat voor de organisatie geldt;

e) de programma's van de organisatie voor onderhoud en oefening van bedrijfscontinuïteit doeltreffend zijn geïmplementeerd;

f) de strategieën en procedures voor bedrijfscontinuïteit de verbeteringen inhouden die tijdens incidenten, oefening en in het onderhoudsprogramma zijn geïdentificeerd;

g) de organisatie een continuprogramma voor training en bewustzijn van bedrijfscontinuïteit heeft;

h) procedures voor bedrijfscontinuïteit doeltreffend zijn gecommuniceerd aan relevant personeel, en dat dit personeel zijn rollen en verantwoordelijkheden begrijpt; en

i) processen om verandering te beheersen aanwezig zijn en doeltreffend functioneren.

Er behoort een duidelijk gedefinieerd en gedocumenteerd onderhoudsprogramma vastgesteld te worden. Dit programma behoort:

— te bewerkstelligen dat veranderingen (intern of extern) die gevolgen hebben voor de organisatie, worden beoordeeld in relatie tot BCM;

— nieuwe producten en diensten en hun afhankelijke activiteiten die in het BCMS moeten worden opgenomen te identificeren;

— te bewerkstelligen dat de bedrijfscontinuïteit van de organisatie doeltreffend, geschikt en actueel blijft; en

— het mogelijk te maken dat bestaande oefenschema's worden gewijzigd als zich een significante verandering heeft voorgedaan in een bedrijfscontinuïteitsstrategie of in gerelateerde bedrijfsprocessen.

OPMERKING De organisatie kan de gevolgen van grote bedrijfsveranderingen doeltreffend beoordelen door de bedrijfsimpactanalyse (8.2.2) in een zo vroeg mogelijk stadium te beoordelen, en gebaseerd op de uitkomst veranderingen in andere elementen van BCM aan te brengen.

De uitkomsten van het onderhoudsproces behoren te bevatten:

— gedocumenteerd bewijs van het proactieve beheer en bestuur van het BCM van de organisatie;

— verificatie dat belangrijke personen die de strategie en procedures voor bedrijfscontinuïteit moeten implementeren, getraind en competent zijn;

— verificatie van de uitvoerende planning en beheersing van het BCM;

— bewijs dat de organisatie de naleving van haar procedures voor bedrijfscontinuïteit heeft geëvalueerd; en

— bewijs dat significante veranderingen in de structuur, producten, diensten en activiteiten van de organisatie tijdig worden weerspiegeld in de procedures voor bedrijfscontinuïteit.

In geval van een incident dat de geprioriteerde activiteiten van de organisatie verstoort of een reactie vereist, behoort een post-incidentbeoordeling te worden uitgevoerd. Deze beoordeling kan omvatten:

— het identificeren van de aard en oorzaak van het incident;

— het beoordelen van de toereikendheid van de reactie van het management;

— het beoordelen van de doeltreffendheid waarmee de organisatie haar hersteltijddoelstellingen haalt;

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 · 16-11-2016 11:19:17

— het beoordelen van de toereikendheid van de bedrijfscontinuïteitsvoorzieningen om medewerkers op het incident voor te bereiden;

— het identificeren van verbeteringen die aangebracht moeten worden in de bedrijfscontinuïteitsvoorzieningen;

— het vergelijken van de werkelijke gevolgen met de gevolgen waarop de bedrijfsimpactanalyse is gebaseerd (8.2.2); en

— het verkrijgen van feedback van belanghebbenden en van personen die aan de reactie hebben deelgenomen.

In de context van continue verbetering kan de organisatie kennis over nieuwe BCM-technologie en -werkwijzen verwerven, met inbegrip van nieuwe instrumenten en technieken. Deze behoren te worden geëvalueerd om hun potentiële voordelen voor de organisatie vast te stellen.

Als bewijs van de evaluaties behoort gedocumenteerde informatie van alle periodieke evaluaties en de resultaten te worden bewaard.

9.2 Interne audit

De organisatie behoort met geplande tussenpozen interne audits uit te voeren zodat zij kan bewerkstelligen dat het BCMS in overeenstemming is met de eigen eisen en de eisen van deze internationale norm.

Het is essentieel om interne audits op het BCMS uit te voeren om te bewerkstelligen dat het BCMS zijn doelstellingen haalt, in overeenstemming is met zijn eigen geplande voorzieningen en op de juiste manier is geïmplementeerd en wordt onderhouden, en om verbeterkansen te identificeren. Interne audits van het BCMS behoren met geplande tussenpozen te worden uitgevoerd om informatie over de geschiktheid en doeltreffendheid van het BCMS vast te stellen en aan de directie te leveren, alsmede om een basis te creëren om doelstellingen voor continue verbetering van de BCMS-prestatie vast te stellen.

De organisatie behoort een auditprogramma vast te stellen (zie ISO 19011) om het plannen en uitvoeren van audits te leiden, en om de audits te identificeren die nodig zijn om te voldoen aan de doelstellingen van het programma. Het programma behoort te zijn gebaseerd op de aard van de activiteiten van de organisatie in termen van risicobeoordeling en analyse van de gevolgen, de resultaten van voorgaande audits en andere relevante factoren.

Een intern auditprogramma behoort te zijn gebaseerd op het volledige toepassingsgebied van het BCMS, maar elke audit behoeft niet meteen betrekking te hebben op het hele systeem. Audits kunnen worden verdeeld in kleinere delen als het auditprogramma maar waarborgt dat alle delen, functies, activiteiten en systeemelementen en het volledige toepassingsgebied van het BCMS een audit ondergaan in het kader van het auditprogramma, binnen de tijdsperiode die door de organisatie is gesteld.

Het resultaat van een interne BCMS-audit kan worden geleverd in de vorm van een rapport en worden gebruikt om specifieke afwijkingen te corrigeren of te voorkomen en input te geven aan het uitvoeren van de managementbeoordeling.

Interne audits van het BCMS kunnen worden uitgevoerd door medewerkers van de eigen organisatie, of door externe personen die door de organisatie zijn geselecteerd en in opdracht van haar werken. In beide gevallen behoren de personen die de audit verrichten, competent te zijn en in een positie te verkeren om dat onpartijdig en objectief te doen. In kleine organisaties kan de onafhankelijkheid van de auditor worden aangetoond door een auditor te kiezen die geen verantwoordelijkheid draagt voor de activiteit waarop de audit wordt uitgevoerd.

9.3 Directiebeoordeling

De directie behoort met geplande tussenpozen het BCMS van de organisatie te beoordelen, om de continue geschiktheid, toereikendheid en doeltreffendheid, met inbegrip van de doeltreffende uitvoering van de continuïteitsprocedures en -capaciteiten te bewerkstelligen.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

De directiebeoordeling behoort een beoordeling te bevatten betreffende:

— de status van acties die voortgekomen zijn uit voorgaande beoordelingen;

— de prestatie van het managementsysteem met inbegrip van trends die blijken uit afwijkingen en corrigerende maatregelen, de resultaten van monitoren en meten, en bevindingen van audits;

— veranderingen in de organisatie en haar context (4.1) die mogelijk gevolgen hebben voor het managementsysteem; en

— kansen voor continue verbetering.

Een directiebeoordeling biedt de directie de kans om de voortdurende geschiktheid, toereikendheid en doeltreffendheid van het managementsysteem te evalueren. De directiebeoordeling behoort het toepassingsgebied van het BCMS te dekken, hoewel niet alle elementen meteen behoeven te worden beoordeeld en het beoordelingsproces over een langere periode mag plaatsvinden.

Beoordeling door de directie van de implementatie en de uitkomsten van het BCMS behoort regelmatig te worden ingepland en te worden geëvalueerd. Hoewel voortdurende beoordeling van het systeem raadzaam is, behoort formele beoordeling te worden gestructureerd, passend te worden gedocumenteerd en op basis van een geschikt schema te worden ingepland. Personen die betrokken zijn bij het implementeren van het BCMS en de middelen toewijzen, behoren bij de directiebeoordeling te worden betrokken.

Naast de regelmatig geplande directiebeoordeling kunnen de volgende factoren aanleiding geven tot een beoordeling en bovendien behoren ze te worden onderzocht wanneer een beoordeling is gepland:

a) **Sector-/branchetrends:** Bij grote sector-/branche-initiatieven behoort een BCMS-beoordeling te worden geïnitieerd. Algemene trends en best practices in de sector/branche en in bedrijfs-/uitvoerende technieken voor continuïteitsplanning kunnen worden gebruikt voor benchmarkdoeleinden;

b) **Eisen vanuit regelgeving:** In geval van nieuwe regelgevingseisen kan een beoordeling van het BCMS nodig zijn; en

c) **Ervaring na een incident:** Na een verstorend incident behoort een beoordeling te worden uitgevoerd, ongeacht of de reactieprocedure was geactiveerd. Als de reactieprocedure was geactiveerd behoort de beoordeling de geschiedenis van de reactieprocedure in aanmerking te nemen, hoe deze werkte, waarom hij is geactiveerd enz. Als de reactieprocedure niet is geactiveerd behoort de beoordeling te onderzoeken waarom dit niet is gebeurd en of dit al dan niet een juiste beslissing was.

Een directiebeoordeling behoort te resulteren in verbetering van de doelmatigheid en de prestatie van het BCMS, en kan de volgende veranderingen als gevolg hebben:

— variaties in het toepassingsgebied;

— verbeteringen in de doelmatigheid;

— updates voor de procedures voor bedrijfscontinuïteit; en

— veranderingen in beheersmaatregelen en in het meten van de doeltreffendheid ervan.

De organisatie behoort gedocumenteerde informatie te bewaren als bewijsmateriaal van de resultaten van de directiebeoordeling, en behoort:

— de resultaten van de directiebeoordeling kenbaar te maken aan relevante belanghebbenden; en

— geschikte maatregelen te nemen die betrekking hebben op die resultaten.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

10 Verbetering

10.1 Afwijkingen en corrigerende maatregelen

De organisatie behoort afwijkingen te identificeren, maatregelen te nemen om ze onder controle te krijgen, te beheersen, en te corrigeren, de gevolgen ervan aan te pakken en te evalueren of de noodzaak bestaat om maatregelen te nemen om de oorzaken ervan weg te nemen.

De organisatie behoort doeltreffende procedures vast te stellen om te bewerkstelligen dat niet-voldoen aan een eis, de aanpak van de planning en zwakke punten in samenhang met het BCMS tijdig worden geïdentificeerd en gecommuniceerd om te voorkomen dat deze situatie zich nog eens voordoet, en om de hoofdoorzaken te identificeren en aan te pakken. De procedures behoren voortdurende opsporing, analyse en verwijdering van daadwerkelijke en potentiële oorzaken van afwijkingen mogelijk te maken.

Afwijkingen behoren tijdig te worden geïdentificeerd en aangepakt, en bijbehorende corrigerende maatregelen behoren tijdig te worden geïdentificeerd en uitgevoerd. De corrigerende maatregel kan voortkomen uit een goed gedefinieerde afwijkingsverklaring die duidelijk het probleem aangeeft en die wordt begrepen.

Als een afwijking is geïdentificeerd behoort een onderzoek naar de hoofdoorzaak te worden uitgevoerd, en een corrigerend-actieplan behoort te worden ontwikkeld om het probleem onmiddellijk aan te pakken. Het actieplan behoort te worden ontworpen om consequenties te beperken en om de veranderingen te identificeren die aangebracht moeten worden om de situatie te corrigeren, om de normale bedrijfsvoering te herstellen en om de oorzaak/oorzaken weg te nemen om te voorkomen dat het probleem zich nog eens voordoet. De aard en timing van maatregelen behoren in overeenstemming te zijn met de mate en aard van de afwijking en de potentiële consequenties.

Er kan een potentieel probleem worden geïdentificeerd terwijl geen daadwerkelijke afwijking bestaat. Potentiële problemen kunnen worden geëxtrapoleerd uit corrigerende maatregelen voor daadwerkelijke afwijkingen die zijn geïdentificeerd tijdens het interne BCMS-auditproces of de analyse van branchetrends en -gebeurtenissen. Identificatie van potentiële afwijkingen kan ook tot deel worden gemaakt van routineverantwoordelijkheden van personen die zich bewust zijn van het belang om potentiële of daadwerkelijke problemen op te merken en te communiceren.

Procedures vaststellen om daadwerkelijke en potentiële afwijkingen aan te pakken en om steeds corrigerende maatregelen te nemen, levert een bijdrage om de betrouwbaarheid en doeltreffendheid van het BCMS te waarborgen. De procedures behoren verantwoordelijkheden en bevoegdheden te definiëren, evenals stappen die gezet moeten worden om corrigerende maatregelen te plannen en uit te voeren. De directie behoort te bewerkstelligen dat corrigerende maatregelen worden geïmplementeerd en dat er een systematische opvolging is om de doeltreffendheid ervan te evalueren.

10.2 Continue verbetering

De organisatie behoort continu de doeltreffendheid van het BCMS te verbeteren.

Continue verbetering vindt plaats op alle niveaus binnen de PDCA-cyclus en behoort te worden aangedreven door beleid en doelstellingen van bedrijfscontinuïteit, auditresultaten, analyses van gemonitorde gebeurtenissen, corrigerende maatregelen en directiebeoordeling.

Veranderingen die voortkomen uit corrigerende maatregelen behoren te worden weergegeven in de BCMS-documentatie.

Continue verbetering vereist een proces dat problemen en afwijkingen op de juiste manier identificeert en ze vervolgens oplost. Dit proces behoort de aard van het probleem en de omgeving waarbinnen het probleem bestaat aan te pakken en daarbij tevens veranderingen aan te brengen in de omgeving om te bewerkstelligen dat het probleem zich niet herhaalt. Elke stap behoort voort te bouwen en een verbetering te vormen op de voorgaande stap zodat de verbetering meer aspecten dekt dan alleen het originele geïdentificeerde probleem en een breder, veelzeggender effect heeft op de organisatie.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

De implementatie van corrigerende maatregelen behoort als doeltreffend te worden gevalideerd. Elke actie behoort een geschatte voltooiingsdatum te hebben. Na die datum behoort de organisatie te bewerkstelligen dat de voorgeschreven maatregel uitgevoerd en doeltreffend is. Als de beoordeling aantoont dat de maatregel niet volgens planning gehaald is, behoort een nieuwe datum te worden bepaald.

Het continue verbeterproces behoort hetzelfde basisproces te volgen als gebruikt voor corrigerende maatregelen en behoort het volgende in te houden:

— identificeren wat moet worden aangepakt en de huidige conditie (afwijking);

— het huidige proces en beheersmaatregelen (hoofdoorzaak) identificeren; en

— vaststellen welke veranderingen geïmplementeerd moeten worden (corrigerende maatregel).

Corrigerende maatregelen pakken tekortkomingen in het BCMS aan en bewerkstelligen dat het functioneert zoals het bedoeld is, terwijl continue verbetering het BCMS naar een hoger niveau van doelmatigheid en doeltreffendheid brengt.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

Bibliografie

ISO 19011:2011, *Guidelines for auditing management systems*

ISO 20000 (all parts), *Information technology – Service management*

ISO 22398 [1)], *Societal security – Guidelines for exercises*

ISO/PAS 22399:2007, *Societal security – Guideline for incident preparedness and operational continuity management*

ISO 27002:2005, *Information technology – Security techniques – Code of practice for information security management*

ISO 27031:2011, *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*

ISO 31000:2009, *Risk management – Principles and guidelines*

BSI 25999-1:2006, *Business continuity management – Code of practice*

BSI 25999-2:2007, *Business continuity management – Specification*

HB 221:2004, *Business continuity management, Standards Australia/Standards New Zealand, ISBN 0-7337-6250-6*

SI 24001:2007, *Security and continuity management systems – Requirements and guidance for use, Standards Institution of Israel*

NFPA. 1600:2007, *Standard on disaster/emergency management and business continuity programs, National Fire Protection Association (USA)*

Business Continuity Plan Drafting Guideline. Ministry of Economy, Trade and Industry, Japan, 2005

Business Continuity Guideline, Central Disaster Management Council, Cabinet Office, Government of Japan, 2005

NASI/ASIS SPC.1:2009, *Organizational Resilience: Security, Preparedness, and Continuity Managements Systems – Requirements with Guidance for Use*

ANSI/ASIS/BSI BCM.01:2010, *Business Continuity Management Systems: Requirements with Guidance for Use*

SS 540:2008, *Singapore Standard for Business Continuity Management*

1) Nog te verschijnen.

Dit document is door NEN onder licentie verstrekt aan: / This document has been supplied under license by NEN to:
Rijksoverheid NEN Connect 2016-2020 16-11-2016 11:19:17

1100056 00014

bylage 34

Item 29:
In onderstaande mailwisseling, ontvangen door Persoonsgegevens op 28-05-2018, wordt door DF&A een verwijzing gedaan naar de statistische relevantie (gele arcering door Persoonsgegevens aangebracht). Dit is later in de PIA sessie ook bevestigd en in het GEB-document opgenomen. Ik beschik niet over 'Statistische onderbouwede ervaringgegevens van DF&A' zoals in het Excel-document Overzicht AP vragen staat beschreven.

----- Doorgestuurd door Persoonsgegevens op 28-05-2018 15:10 -----
Van Persoonsgegevens
Aan: Persoonsgegevens @Belastingdienst
Datum: 28-05-2018 13:44
Onderwerp: Fw: Aanvraag FSV-data
ter info
Met vriendelijke groet, Persoonsgegevens ..... Belastingen Gravinnen van Nassauboulevard 75 - 4811 BN BREDA ..... Persoonsgegevens
Persoonsgegevens @belastingdienst.nl
----- Doorgestuurd door Persoonsgegevens op 28-05-2018 13:43 -----

Van: Persoonsgegevens
Aan: Persoonsgegevens @BELASTINGDIENST
Cc: Persoonsgegevens @Belastingdienst, Persoonsgegevens @Belastingdienst, Persoonsgegevens Persoonsgegevens @Belastingdienst, Persoonsgegevens @Belastingdienst
Datum: 25-05-2018 12:16
Onderwerp: Aanvraag FSV-data

Beste collega's,

Bij deze vraag ik namens DF&A, Handhaving BTW-fraudebestrijding en Toezicht toegang tot de data uit Dagboek FSV.

Algemeen

De applicatie Dagboek FSV (Fraude Signalering Voorziening) is bestemd voor de registratie van fraudesignalen die voorheen in dagboek PIT werden geregistreerd.
Primair is deze applicatie ontwikkeld voor de registratie van alle soorten signalen van "systeemfraude". Hiermee wordt hoofdzakelijk bedoeld het min of meer opzettelijke misbruiken van fiscale regelingen. Dit kan gelden voor inkomstenbelasting, loonbelasting, omzetbelasting, maar ook voor de verschillende Toeslagen (huur, zorg, kinderopvang enzovoort). De applicatie kan ook gebruikt worden voor de registratie van tips/kliks/signalen, projecten (per segment, regionaal, plaatselijk) in het Subject Gerichte Toezicht (S.G.T.) en voor de registratie van bijzondere verzoeken om informatie, bijvoorbeeld verzoeken in het kader van strafrechtelijke onderzoeken (bijv. zogenaamde art. 126nd verzoeken), misbruik van bijstandsuitkeringen, RIEC verzoeken, enzovoort.)
Indien een belastingplichtig is gesignaleerd in FSV, is dat een attentiesignaal voor de risicomodellen Omzetbelasting. Het is immers dat de (mogelijke) fraudeur niet gericht is op een bepaald middel (IH, toeslagen, etc), maar op de mogelijkheden om onrechtmatig geld tot zich te nemen. En verdienen derhalve ook extra aandacht in de risicomodellen Omzetbelasting.

(Beoogd) gebruik data

In het verleden heeft DF&A een proeflevering gekregen met gegevens uit het jaar 2015. Deze gegevens heeft DF&A alleen gebruikt voor verkenningen van fraude-analyses en projecten. Ook in de toekomst zou deze data alleen voor fraudeverkenningen gebruikt worden. Alle gevoelige data, waaronder fraudesignalen, worden apart behandeld binnen DF&A. Hiervoor is een apart, afgeschermd datafundament en datagebied ingericht. Alleen medewerkers met een speciale autorisatierol kunnen hierbij en het gebruik van data door interne projecten wordt vooraf beoordeeld met een WMK-toets. Voor ieder DF&A-project wordt een PIA uitgevoerd.

Nut voor de business

Uit de verkenningen met de proeflevering van FSV zijn twee producten ontwikkeld: een applicatie waarmee btw-carrouselfraude gedetecteerd wordt en een applicatie die risico's detecteert voorafgaand aan afgifte btw-nummers. Deze producten zijn in productie.
- De btw-carrouselfraudetool is gebouwd in samenwerking met de FIOD. De tool levert risico-inschattingen plus onderbouwing aan 15 landelijke analisten die vervolgens de signalen nader opwerken en vervolgens uitzetten naar de relevante kantoren. Deze tool zorgt kort gezegd voor de systematische aanpak van btw-carrouselfraude in Nederland.
- De applicatie voor afgifte btw-nummers probeert het risico in te schatten dat de aanvrager (carrousel-)fraude pleegt. Op deze manier wil de Belastingdienst fraude voorkomen door bekende risico-personen extra in de gaten te houden of het btw-nummer te weigeren. Dit is ook een landelijke actie.
Het product is nu bijna een jaar in productie en de resultaten zijn positief.
De gegevens uit FSV blijken statistisch relevant voor deze producten. Met name bij de aanvraag van een btw-nummer blijkt het voorkomen van een persoon op de fraudelijst een goede risico-indicatie. Zonder deze gegevens zal de hit-rate van beide producten verminderen, dit effect is het sterkst voor de applicatie Afgifte btw-nummer.

Conclusie verzoek

De proeflevering is heel nuttig gebleken, maar de gegevens zijn verouderd. DF&A kan niet met verouderde gegevens (blijven) werken. Graag zouden we met het oog op de kwaliteit van onze producten een reguliere ontsluiting van de (relevante) data uit FSV opzetten. Wij willen graag in gesprek over onder andere de voorwaarden voor de ontsluiting, beveiliging en data-minimalisatie.

Wij begrijpen dat een WMK-toets noodzakelijk is en willen daarvoor graag een afspraak maken, waarbij zowel DF&A als de business vertegenwoordigd zullen zijn.
Mocht u nog vragen hebben, dan verzoek ik u contact met mij op te nemen.
Met vriendelijke groet,

Persoonsgegevens

Belastingdienst
Data & Analytics
Team Data
Croeselaan 14 | 3521 BJ | Utrecht

Persoonsgegevens

www.belastingdienst.nl
Woensdag niet aanwezig.

bylage 35

tabblad "rollen met FSV"

Bedrijfsrolnaam	Omschrijving_bedrijfsrol	Aantal medewerkers	Permissie_omschrijving in de bedrijfsrol
B_GO-32	B_GO_FSV-Raadpleger	6	FSV - Raadpleger
B_GO-33	B_GO_FSV-Raadpleger Aangifte Fraude	8	FSV - Raadpleger Aangifte Fraude
B_GO-34	B_GO_FSV-Raadpleger Aangifte Fraude met BI	2	FSV - Raadpleger Aangifte Fraude Met BI
B_GO-35	B_GO_FSV-Behandelaar	3	FSV - Behandelaar
B_GO-36	B_GO_FSV-Behandelaar Aangifte Fraude	5	FSV - Behandelaar Aangifte Fraude
B_GO-37	B_GO_FSV-Senior Behandelaar	1	FSV - Senior Behandelaar
B_GO-38	B_GO_FSV-Beheerder	1	FSV - Beheerder
B_GO-IH-03	B_GO-Specialist IH	866	FSV - Raadpleger
B_LKB-BV-EHI-04	B_LKB_BV_Expertisecentrum Handhaving en Intelligence Raadplegen	10	FSV - Raadpleger Aangifte Fraude
B_LKB-DA-03	B_LKB-DataAnalytics-Raadplegen	74	FSV - Raadpleger
B_MKB-50	B_MKB_FSV-Raadpleger	372	FSV - Raadpleger
B_MKB-51	B_MKB_FSV-Raadpleger Aangifte Fraude	114	FSV - Raadpleger Aangifte Fraude
B_MKB-52	B_MKB_FSV-Raadpleger Aangifte Fraude met BI	44	FSV - Raadpleger Aangifte Fraude Met BI
B_MKB-53	B_MKB_FSV-Behandelaar	142	FSV - Behandelaar
B_MKB-54	B_MKB_FSV-Behandelaar Aangifte Fraude	103	FSV - Behandelaar Aangifte Fraude
B_MKB-55	B_MKB_FSV-Senior Behandelaar	77	FSV - Senior Behandelaar
B_MKB-56	B_MKB_FSV-Beheerder	10	FSV - Beheerder
B_MKB-BBK-IH-03	B_MKB-BBK-IH-03 Bezwaar Beroep en Klachtenafhandeling	0	FSV - Raadpleger
B_MKB-FR-02	B_MKB_Fraudeteam Basis	401	FSV - Behandelaar
B_MKB-FR-02	B_MKB_Fraudeteam Basis	401	FSV - Raadpleger
B_MKB-IH-03	B_MKB-IH_Vaststelling-aanslag	3039	FSV - Raadpleger
B_MKB-IH-04	B_MKB-IH_ABS en OKA muteren	1501	FSV - Raadpleger
B_MKB-INV-CP-01	B_MKB-Invordering-Medewerker Centraal Punt	21	FSV - Raadpleger
B_PDB-32	B_PDB_FSV-Raadpleger	25	FSV - Raadpleger
B_PDB-33	B_PDB_FSV-Raadpleger Aangifte Fraude	66	FSV - Raadpleger Aangifte Fraude
B_PDB-34	B_PDB_FSV-Raadpleger Aangifte Fraude met BI	2	FSV - Raadpleger Aangifte Fraude Met BI
B_PDB-35	B_PDB_FSV-Behandelaar	60	FSV - Behandelaar
B_PDB-37	B_PDB_FSV-Senior Behandelaar	25	FSV - Senior Behandelaar
B_PDB-BBK-IH-03	B_PDB-BBK-IH-03 Bezwaar Beroep en Klachtenafhandeling	701	FSV - Raadpleger
B_PDB-BTL-11	B_PDB-BTL-FSV-Behandelaar	2	FSV - Behandelaar
B_PDB-BTL-12	B_PDB-BTL-FSV-Behandelaar Aangifte Fraude	8	FSV - Behandelaar
B_PDB-BTL-ALG-03	B_PDB-BTL-FSV Raadpleger Aangifte Fraude	11	FSV - Raadpleger Aangifte Fraude
B_PDB-BTL-IH-03	B_PDB-BTL-IH Vaststelling Aanslag	143	FSV - Raadpleger
B_PDB-BTL-INV-CP-01	B_PDB-BTL-Invordering-Medewerker Centraal Punt	2	FSV - Raadpleger
B_PDB-DV-02	B_PDB-Dienstverlening_Medewerker	235	FSV - Baliemedewerker
B_PDB-IH-03	B_PDB-IH_Vaststelling-aanslag	1769	FSV - Raadpleger
B_PDB-IH-FR-01	B_PDB-IH-Fraudemedewerker	119	FSV - Behandelaar Aangifte Fraude
B_PDB-KBB-02	B_PDB-Klachtbehandeling_Klachtbehandelaar en Administratief Medewerker	93	FSV - Baliemedewerker
C_4-1	UPL-Herstel-TOR	5	FSV - Raadpleger Aangifte Fraude
C_Taak_1640	FSV - Beh Aang Fraude	3	FSV - Behandelaar Aangifte Fraude
C_Taak_1644	FSV - Beheerder	2	FSV - Beheerder
C_Taak_1646	FSV - Raadpleger Aangifte Fraude	2	FSV - Raadpleger Aangifte Fraude
C_Taak_1650	FSV - Raadpleger	2	FSV - Raadpleger
C_Taak_1652	FSV - Senior Beh	0	FSV - Senior Behandelaar
CAP_FunctioneelBeheer_02	CAP_Functioneel Beheer - Toezicht	10	FSV - Beheerder
CAP_LIC_02	CAP_LIC_Medewerker	815	FSV - Raadpleger
CAP_LIC_CP_01	CAP_LIC_Medewerker Serviceteams Centraal Punt	8	FSV - Raadpleger
CAP_LIC_ETM_01	CAP_LIC_Medewerker ETM Behandelaar	19	FSV - Raadpleger
CAP_LIC_ETM_02	CAP_LIC_Medewerker ETM Accordant	1	FSV - Raadpleger
CAP_LIC_TL_ETM_00	CAP_LIC_Teamleider ETM	1	FSV - Raadpleger
CD-DFenA_Fraude_Analist_01	CD-DFenA_Fraude Analist	2	FSV - Raadpleger
F_012	FIOD Account-OT	155	FSV - Raadpleger
F_016	FIOD Infodesk Centraal	25	FSV - Raadpleger
F_026	FIOD AMLC	19	FSV - Raadpleger
F_362	FSV - Raadpleger	4	FSV - Raadpleger
GO_Administratie_Milieubelastingen_01	GO_Administratie Milieubelastingen	3	FSV - Raadpleger
GO_Assistent_Klantcoordinator_01	GO_Assistent_Klantcoordinator	3	FSV - Raadpleger
GO_Heffer_IH_01	GO_Heffer Inkomensheffing	7	FSV - Raadpleger
GO_Heffer_LH_01	GO_Heffer Loonheffing	1	FSV - Raadpleger
GO_Heffer_Milieubelastingen_01	GO_Heffer Milieubelastingen	21	FSV - Raadpleger
GO_Heffer_OB_01	GO_Heffer Omzetbelasting	2	FSV - Raadpleger
GO_Heffer_OVB_01	GO_Heffer Overdrachtsbelasting	61	FSV - Raadpleger
GO_Heffer_VpB_01	GO_Heffer Vennootschapsbelasting	10	FSV - Raadpleger
GO_Heffer_ZVP_01	GO_Heffer Zeer Vermogende Personen	19	FSV - Raadpleger
GO_Invorderaar_01	GO_Invorderaar	0	FSV - Raadpleger
GO_Invorderaar_administratie_01	GO_Invorderaar administratief medewerker	0	FSV - Raadpleger
GO_Klantcoordinator_01	GO_Klantcoordinator	7	FSV - Raadpleger
Toeslagen_0003	Management M2 Plusprofiel Fraude	2	FSV - Raadpleger
Toeslagen_0112	Bedrijfsvoering Plusprofiel FSV Fraude BI	7	FSV - Raadpleger Aangifte Fraude Met BI
Toeslagen_1000	Fraude Basis profiel	51	FSV - Behandelaar
Toeslagen_1005	Fraude Plusprofiel FSV Senior Behandelaar	3	FSV - Senior Behandelaar
Toeslagen_1101	Handhavingsregie Analist	22	FSV - Raadpleger
Toeslagen_1308	Klacht Expert FSV	10	FSV - Raadpleger
Toeslagen_1401	Productieregie Kwaliteitsregie	13	FSV - Raadpleger
Toeslagen_1403	Productieregie QL	6	FSV - Raadpleger Aangifte Fraude Met BI
Toeslagen_1408	Productieregie Ketenregie	8	FSV - Raadpleger
Toeslagen_1450	IST Basis profiel	73	FSV - Raadpleger
Toeslagen_1452	IST CAV Profiel	37	FSV - Behandelaar
VR_CD-DFenA_Analist_Fraude	CD-DFenA_Analist Fraude	0	FSV - Raadpleger

tabblad "aug groepen"

AUTORISATIES FSV

aug-groep	aantal
aug_FSV_BalieMedewerker	297
aug_FSV_Behandelaar	691
aug_FSV_BehandelaarAangiftefraude	227
aug_FSV_Beheerder	22
aug_FSV_Raadpleger	8891
aug_FSV_RaadplegerAangiftefraude	216
aug_FSV_RaadplegerAangiftefraudeMetBI	66
aug_FSV_SeniorBehandelaar	105
aug_FSV_Special	

tabblad "rollen acceptatieomgeving"

B_ALG-FSV-ACC-01	B_ALG-FSV Acceptatie en Testomgeving	8	FSV - Ballemedewerker Acc
			FSV - Behandelaar Aangifte Fraude Acc
			FSV - Behandelaar Acc
			FSV - Beheerder Acc
			FSV - Raadpleger Aangifte Fraude Acc
			FSV - Raadpleger Aangifte Fraude Met BI Acc
			FSV - Raadpleger Acc
			FSV - Senior Behandelaar Acc
B_DB-ACC-FSV-03	B_DB-Test-omgeving_FSV-BehandelaarAangiftefraude	3	FSV - Behandelaar Aanglfte Fraude Acc
B_DB-ACC-FSV-04	B_DB-Test-omgeving_FSV-Beheerder	1	FSV - Beheerder Acc
B_DB-ACC-FSV-05	B_DB-Test-omgeving_FSV-RaadplegerAangiftefraude	6	FSV - Raadpleger Aangifte Fraude Acc
B_DB-ACC-FSV-06	B_DB-Test-omgeving_FSV-RaadplegerAangiftefraude Met BI	3	FSV - Raadpleger Aangifte Fraude Met BI Acc
B_DB-ACC-FSV-07	B_DB-Test-omgeving_FSV-SeniorBehandelaar	33	FSV - Senior Behandelaar Acc
C_Taak_1653	FSV - Senior Beh Acc	0	FSV - Senior Behandelaar Acc