Checklist bedrijfscontinuïteit

Dit moet je opnemen in jullie bedrijfscontinuïteitsplan. Met een goed bedrijfscontinuïteitsplan ben je beter voorbereid op crisissituaties. Het doel van bedrijfscontinuïteit is het voorkomen of beperken van onderbrekingen van bedrijfsactiviteiten door de uitval van bepaalde schakels. Met andere woorden: slim ingerichte bedrijfscontinuïteit beschermt kritische processen tegen een mogelijke crisis of verstoring.
Hoewel een verstoring van kritische processen veelal onverwacht komt, is het wel degelijk mogelijk om jullie organisatie erop voor te bereiden. Dit doet jullie organisatie door middel van een bedrijfscontinuïteitsplan (bcp).

Deze checklist bevat de elementen die je moet opnemen in een bcp, zodat je niets over het hoofd ziet. Het doel van een bedrijfscontinuïteitsplan (bcp) is het minimaliseren van de impact van een crisis op de continuïteit van de kernprocessen van jullie organisatie. In een bcp leg je vast welke zaken, mensen en diensten jullie organisatie definiëren en wat de aanpak is op het moment dat deze elementen in hun bestaan worden bedreigd. Op deze manier ligt vast welke stappen jullie organisatie wil en moet zetten als een crisis zich voordoet.

Kritische processen

In een bcp identificeer je eerst de kritische processen en analyseer je wat de gevolgen van de crisis of verstoring zijn. Een eerste stap bij het in kaart brengen hiervan is het uitvoeren van een Business Impact Analyse (BIA). In een BIA beoordeel je de gevolgen van gebeurtenissen zoals rampen, incidenten en het uitvallen van diensten. Hiermee geeft een BIA inzicht in de belangrijkste elementen waar jullie organisatie zich op moet focussen.

De eerste stap in de uitvoering van een BIA is het identificeren en definiëren van kritieke processen. Een proces kan als kritiek gezien worden als een onderbreking van de continuïteit van dit proces een onacceptabele impact op jullie organisatie heeft. Bekijk de primaire processen vóór de ondersteunende processen.
Een volgende stap is het identificeren en uitwerken van de afhankelijkheden die bestaan binnen de kritische processen van jullie organisatie. Vervolgens kijk je naar de waarschijnlijke impact van het uitvallen van een proces en de mogelijke gevolgschade hiervan.

Een primair proces kan bijvoorbeeld inkoop van programma, productie en verkoop van tickets zijn. De impact van het uitvallen van een primair proces is niet moeilijk in te schatten, omdat het primaire proces directe toegevoegde waarde levert aan de hoofdactiviteit die jullie organisatie uitvoert. Secundaire processen zijn processen die de primaire processen ondersteunen. Secundaire processen zijn bijvoorbeeld human resources, ICT en financiële administratie. Ook deze processen

kunnen als kritisch proces worden geïdentificeerd, als er geen alternatief voorhanden is en het wegvallen betekent dat de primaire processen ook direct stoppen.

Kritische middelen

De kritische middelen zijn alle middelen die noodzakelijk zijn om de continuïteit van jullie kernprocessen te garanderen. Analyseer welke benodigdheden essentieel zijn in de uitvoering van het proces.
Aan de hand van de informatie die je verkrijgt uit jullie analyse van kritische middelen, moet er voor elk middel in jullie organisatie een tijdsdoel voor het herstel vastgesteld worden. Daarnaast moet je bepalen hoeveel informatie er verloren mag gaan. Dit wordt uitgedrukt in de tijd uit waarin jullie organisatie minimaal de gegevenssystemen met informatie moet kunnen herstellen.

Voorbeeld. Stel dat er brand is in een podiumzaal of festivaltent. Een onderneming in de dienstverlenende sector kan zich sneller herstellen van een brand omdat deze hoofdzakelijk werkt (of kan werken) met laptops en dit ook vanuit andere locaties kan, als er een goedwerkende internetverbinding aanwezig is. Dit geldt niet voor een VNPF-lid . Bij een brand moet er naar alternatieve locaties gekeken worden om publiek te kunnen blijven ontvangen.

Kritische data

Of je nu veel of weinig informatie hebt voor elke organisatie geldt dat het belangrijk is om te weten welke data van bedrijfskritische waarde zijn.
Hiervoor is het verstandig om eerst op basis van de inventarisatie van de kritische processen te bepalen welke gegevens noodzakelijk zijn als gewenste input en output, wie hier verantwoordelijk voor is en welke gegevens tussen afdelingen maar ook tussen klanten (bezoekers) en leveranciers worden uitgewisseld. Vergeet hierbij ook niet om te kijken naar de metadata, zoals het format en de gegevensdrager.

Is duidelijk welke data relevant zijn voor de kritische bedrijfsprocessen van jullie organisatie, dan is het tijd voor een inventarisatie van deze kritische data. Denk hierbij zowel aan gestructureerde data (in databases en systemen), als aan ongestructureerde data (dossiers, documenten, foto's, e-mail, video's en archieven die zich op verschillende informatiedragers bevinden).
Ruim bij de inventarisatie van data ook apart tijd in voor data met persoonsgegevens, omdat hier aanvullende eisen voor gelden op basis van de Algemene Verordening Gegevensbescherming (AVG).

Kritische personen

Naast processen, middelen en data zijn ook mensen van essentieel belang voor jullie organisatie. Vanuit jullie kritische processen kan je de vertaalslag maken naar kritische functies. De werkzaamheden die binnen deze functie vallen mogen dus niet worden onderbroken, of moeten binnen een bepaalde tijd kunnen worden hervat. Denk na over wat de gepaste samenstelling is van de kritische functies. Die samenstelling moet het hele proces omvatten dat nodig is om een dienst te leveren.
Nadat de kritische functies geïdentificeerd zijn, ga je verder met het identificeren van kritische

werknemers die toegewezen zijn aan de functies. Breng vervolgens in kaart of de kennis en expertise van deze werknemers ook elders binnen jullie organisatie aanwezig zijn, of hoe deze kennisdeling gerealiseerd kan worden.

Kritische relaties en leveranciers

Niet alleen kan er bij jullie eigen organisatie een crisis voorkomen, dit kan ook gebeuren bij een van jullie relaties of leveranciers. Als er een crisis is bij een externe partij waar jullie organisatie afhankelijk van is, kan dit een crisis veroorzaken voor jullie eigen activiteiten en de continuïteit van jullie kritische processen in gevaar brengen. Je moet met jullie kritische externe relaties en leveranciers afspraken maken in een overeenkomst over onder andere de hersteltijd en de juridische aansprakelijkheid. Dit soort afspraken worden gemaakt in een *service level agreement*. Denk ook na over eventuele uitwijkmogelijkheden of alternatieve leveranciers, voor het geval dat je problemen heeft met jullie eigen middelen of één van jullie kritische leveranciers een crisis heeft.

Analyse risico's en dreigingen

Als je jullie kritische processen, middelen, data, personen en relaties in kaart hebt gebracht, kan je analyseren in hoeverre deze elementen in het geding komen bij een crisis. Hierbij maak je onderscheid tussen risico en dreiging.

Risico's

Een risico is de kans dat een dreiging invloed heeft op een kwetsbare schakel in jullie organisatie, en de bijbehorende impact daarvan. Een risico bepaalt uiteindelijk de impact voor jullie organisatie, en betekent dat het 'voorstelbaar' is dat er iets kan gebeuren.

Voorbeelden van risico's voor jullie organisatie
Bij een risico is er geen specifieke informatie bekend dat er iets staat te gebeuren. De kans is alleen niet helemaal uitgesloten. Voorbeelden van risico's zijn:

- Geen beschikbaarheid van gebouw/infrastructuur. Voorbeeld: risico van brand of overstroming die de faciliteiten van jullie organisatie treft en dus ook de continuïteit van de activiteiten.
- Geen beschikbaarheid van werknemers/expertise. Voorbeeld: risico op pandemie, stakingen die de continuïteit treffen van de werkzaamheden.
- Geen beschikbaarheid van ICT of communicatiemethode. Voorbeeld: risico van stroomoverbelasting, *hacks*, of storing bij de telefoonprovider die de continuïteit treft van de werkzaamheden.

Dreigingen

Een dreiging gaat een stap verder dan een risico. Bij een dreiging is namelijk specifieke informatie bekend dat er iets staat te gebeuren. Een dreiging komt voort uit een niet-gewenst incident en kan als gevolg daarvan schade toebrengen aan uw onderneming. Er zijn verschillende dreigingen per land, per sector en dus ook per onderneming. Hoe specifieker

de dreiging met bijvoorbeeld locatie, tijdstip of middelen, hoe gerichter u maatregelen kunt treffen om de dreiging weg te nemen of de gevolgen ervan te beperken.

Beheersmaatregelen

Als je de kritische processen, middelen, data, mensen en relaties en leveranciers hebt geïdentificeerd, moet je beheersmaatregelen implementeren om bescherming te bieden tegen een potentieel risico. De beheersmaatregelen moeten:

- de waarschijnlijkheid van een onderbreking verminderen;
- de periode van de onderbreking verkorten;
- de impact van een onderbreking van de kritische processen beperken.

Scenario's en draaiboeken

Een bcp kan instructies bevatten voor één of meerdere scenario's. Welke scenario's jullie organisatie wel of niet uitwerkt, hangt onder andere af van de uitkomsten van de risicoanalyse. Naast scenario's moet jullie organisatie ook een draaiboek hebben om in het geval van een crisis te weten welke stappen jullie moeten ondernemen. Het bcp bevat op basis van risico's en prioriteiten een draaiboek met daarin opgenomen de stappen en communicatielijnen om jullie organisatie weer continuïteit te bieden.
Het calamiteitendraaiboek is een dynamisch document, het moet altijd up-to-date zijn, zodat je over de laatste informatie beschikt. Om ervoor te zorgen dat het up-to-date houden van het calamiteitendraaiboek geen lastige en tijdrovende klus is, moet jullie organisatie ervoor waken dat het geen lijvig, onleesbaar of onbruikbaar document wordt.

Communicatie en training

Jullie organisatie moet de opgestelde plannen, scenario's en draaiboeken formaliseren en communiceren naar de werknemers. Zorg er daarnaast voor dat jullie organisatie regelmatig trainingen geeft en verschillende scenario's belicht. Maak trainingen interactief, zodat werknemers meemaken en wennen aan wat er tijdens een crisis kan gebeuren.
Het is daarnaast van belang om tijdens de crisis, verschillende kanalen tot je beschikking te hebben voor communicatie. Daarnaast moet er beschreven zijn op welke manieren jullie organisatie zowel intern naar werknemers, als ook extern naar leveranciers, partners en media kan communiceren. Met een communicatieplan wordt inzichtelijk wat jullie organisatie wil bereiken op het gebied van communicatie ten tijde van een crisis. Het beschrijft jullie communicatiestrategie waarin je bepaalt wie jullie doelgroep is, welke boodschapje wilt overbrengen en met welke middelen.

Onderhoud

Nadat je de kritische processen, middelen, werknemers en relaties en leveranciers hebt geïdentificeerd, de risico's en dreigingen heeft geanalyseerd en de maatregelen geïmplementeerd, rest de vraag, of dit alles natuurlijk ook echt werkt als er een crisis is?
Daarom zal je als onderneming verschillende testscenario's op moeten stellen om het crisisplan regelmatig te testen en te evalueren. Zorg voor een volledige evaluatie van het testen van het crisisplan, zodat het crisisplan up-to-date is en bruikbaar blijft.