Handreiking Informatie-beveiligingsbeleid BIO

Plan van Aanpak Bedrijfscontinuïteits-beheer (BCM)

Handreiking Bedrijfscontinuïteits-beheer (BCM)

Model Continuïteits-strategie BIO (BCM)

PvA 10: Er worden minimaal jaarlijks oefeningen of testen uitgevoerd om de bedrijfscontinuïteitsplannen te toetsen (opzet, bestaan en werking), om te waarborgen dat ze actueel en doeltreffend blijven. Aan de hand van de resultaten worden de bedrijfscontinuïteitsplannen bijgesteld en wordt de gemeente bijgeschoold. Het oefenen dient te worden geborgd middels een programma.

PvA 11: De gemeente dient een beheerd proces voor bedrijfscontinuïteit te ontwikkelen en bij te houden, zodat de naleving van eisen voor informatiebeveiliging wordt geborgd die nodig zijn voor de continuïteit van de bedrijfsvoering. Speciale aandacht dient uit te gaan naar veranderingen die invloed hebben op het bedrijfsproces of de systemen. Vanuit hetzelfde oogpunt is het van belang dat al bij het inkoopproces oog is voor keuzes die van invloed kunnen zijn op de bedrijfscontinuïteit. Denk b.v. aan redundantie van systemen, cloudoplossingen, etc.

PvA 12: Het bedrijfscontinuïteitsplan dient periodiek te worden geactualiseerd: veranderingen gaan snel en ook bedreigingen en daarmee risico's veranderen in de tijd. Deze hebben hiermee mogelijk effect op de (mitigerende) maatregelen die moeten worden genomen om ervoor te zorgen dat de bedrijfscontinuïteit op het gewenste niveau blijft. Het verdient de aanbeveling om deze actualisatie mee te laten lopen in de planning voor de actualisatie van het informatiebeveiligingsbeleid en het informatiebeveiligingsplan, omdat hiervoor naar dezelfde risico's wordt gekeken.

PvA 1.1: Het is effectiever om eerst generieke maatregelen te nemen voordat er naar de bedrijfsprocessen wordt gekeken.

Generieke maatregelen o.a. tegen brand en blikschade, stroomuitval, overstromingen, verlies van communicatiemiddelen, fysieke toegang tot kritische ruimten en om medewerkers te beschermen.
Vaak is er al een overzicht van alle bedrijfsprocessen voorhanden vanuit een DSP of vanuit het verwerkingsregister. Als er nog geen overzicht is dan kunnen een aantal behulpzame vragen uit het Plan van Aanpak gebruikt worden.
Hierbij dient ook aandacht te zijn voor de afhankelijkheid van ketenpartners en leveranciers. Inventariseer die bestaande maatregelen en toets op afhankelijkheden.

PvA 2.1: Zeker als net wordt begonnen met bedrijfscontinuïteit, dient de focus vooral te liggen op kritische bedrijfsprocessen. Kritische bedrijfsprocessen mogen niet uitvallen. Bij de uitvoering van deze kritische processen zijn middelen nodig (ICT, elektriciteit, huisvesting, medewerkers). En deze middelen kunnen geraakt worden doordat de dreiging van uitval werkelijkheid is geworden. Een kritisch bedrijfsproces valt nooit rechtstreeks uit door een dreiging. Het zijn immers de middelen die kwetsbaar zijn. En de kritische bedrijfsprocessen zijn afhankelijk van deze middelen. Veel van deze middelen vallen onder de bij 3.1 getroffen generieke maatregelen.

De bedrijfsprocessen worden vervolgens geclassificeerd naar impact op de organisatie bij uitval. Nadruk ligt op de beschikbaarheid van het proces dan wel de beschikbaarheid van de informatie. Hier ligt een relatie met het BBN (Basis Beveiligingsniveau) van de BIO en de dataclassificatie. Als uitkomst van deze classificatie komt een overzicht van de kritische bedrijfsprocessen. Pak het praktisch aan door bijv. vergelijkbare bedrijfsprocessen samen te voegen om in één keer de noodzakelijke maatregelen te bepalen.

PvA 3: Van de kritische bedrijfsprocessen worden de risico's in kaart gebracht; de kans op het optreden van een bepaald risico en de impact hiervan op de gemeente als geheel. Denk hierbij aan brand, bliksem. overstromingen, internetstoring, stroomstoring, pandemie. Gebeurtenissen die tot onderbreking / discontinuïteit van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd door het uitvoeren van een Bedrijfs Impact Analyse. (zie PvA 2.2) Aan de hand van een (uitgebreide) risicoanalyse dienen de waarschijnlijkheid en de gevolgen van de onderbreking/discontinuïteit in kaart gebracht te worden in termen van tijd, schade en herstelperiode. Gebruik eventueel, om niks te vergeten de MAPGOOD aanpak uit de diepgaande risicoanalyse. Ook de afhandeling van incidenten levert hiervoor bruikbare informatie.

PvA 4: Het kan zijn dat de verantwoordelijke proceseigenaren (bij een beperkte impact) dan wel de directie en het college wenst om bepaalde risico's te accepteren. Middels het besluitvormingsproces zal dit helder moeten worden. Voor geaccepteerde risico's hoeft geen calamiteitenscenario te worden gemaakt, het is niet zinvol om mitigerende maatregelen te treffen en kosten te maken voor bedrijfsprocessen waarvan uitval wordt geaccepteerd. Het is van belang om deze stap middels formele besluitvorming te doorlopen, zodat verderop in het bedrijfsproces ook voor directie en college helder is dat onder andere benodigde budgetten (zie ook PvA 8.1) een direct voortvloeisel zijn uit deze besluitvorming en is vastgelegd welke risico's worden geaccepteerd.

PvA 5: Nadat de kritische bedrijfsprocessen zijn benoemd en het verantwoordelijk management en het college hebben besloten dat de bedrijfsprocessen dienen te worden beheerd op het gebied van bedrijfscontinuïteit, dienen maatregelen hiertoe te worden genomen. Een aantal maatregelen is generiek en soms zelfs wettelijk verplicht (zie ook PvA 3.1). Naast generieke maatregelen dient er ook aandacht te zijn voor onderdelen van de gemeente die essentieel zijn voor de dienstverlening aan de inwoners, zoals de website (digitale producten) en de publieksbalie. Daarnaast zijn er meer proces-specifieke maatregelen noodzakelijk. Om te bepalen welke maatregelen dit zijn worden vijf stappen doorlopen (7.1 t/m 7.5).

5.1: Hoewel bij bedrijfscontinuïteit in eerste instantie gedacht dient te worden aan het 'beschikbaarheidsaspect' van informatiebeveiliging, dienen de overige twee aspecten (integriteit en vertrouwelijkheid) niet vergeten te worden.

5.2: Tijdens een calamiteit kunnen niet alle bedrijfsprocessen doorgaan: daarvoor zijn over het algemeen te weinig middelen en medewerkers beschikbaar. Er dienen dus keuzes te worden gemaakt. Op basis van de classificatie en de impact van de uitval van bepaalde systemen en bedrijfsprocessen dient een prioritering te worden aangebracht: welke kritische bedrijfsprocessen en systemen moeten als eerste worden hersteld alvorens andere (kritische) bedrijfsprocessen weer worden opgestart.

5.3: Het is mogelijk dat de risico's bij uitval zo groot zijn, of herstel zoveel tijd in beslag neemt, dat er redundante maatregelen moeten worden getroffen om bij voorbeeld noodzakelijke informatie op kortere termijn beschikbaar te hebben. Te denken valt aan het bewaren of beschikbaar houden van essentiële informatie op papier, reserve capaciteit van ICT-systemen, inhuur van mensen, etc.

5.4: Documentatie die noodzakelijk is om bedrijfsprocessen en systemen weer op te starten dient onder alle omstandigheden beschikbaar en raadpleegbaar te zijn, mogelijk ook niet digitaal.

5.5: Medewerkers dienen de kennis en deskundigheid in huis te hebben om bedrijfsprocessen en systemen weer op te starten.

PvA 7: De uitvoering van de te nemen noodzakelijke maatregelen dient te worden geborgd zodat de maatregelen ook daadwerkelijk worden uitgevoerd. Zorg dat de maatregelen planmatig worden uitgevoerd. Generieke maatregelen met een positieve impact op meerdere dan wel alle bedrijfsprocessen zullen meestal voorrang krijgen boven proces specifieke maatregelen.

PvA 8: Uiteindelijk worden er een bedrijfscontinuïteitsplan en een communicatieplan opgesteld.
8.1: Bedrijfscontinuïteitsplan: De gemeente dient een enkelvoudig kader voor bedrijfscontinuïteitsplannen te ontwikkelen/adopteren. Dit om te waarborgen dat alle plannen consistent zijn, om informatiebeveiligingseisen op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud. Hiertoe heeft de IBD een format ontwikkeld: zie het PvA. Hierin wordt onder meer vastgelegd wie het bedrijfscontinuïteitsplan mag activeren en wanneer, en wanneer gecontroleerd mag worden teruggegaan.
8.2: Communicatieplan: uitgewerkt dient te worden – gelet op de mogelijke uitval van specifieke communicatiemiddelen- welke middelen de gemeente in voorkomend geval nog ter beschikking staan om te communiceren met een doelgroep of stakeholders. Op welke wijze wordt met medewerkers gecommuniceerd die een rol hebben in het crisisbeheer? Daarna volgt nog een uitwerking per bedrijfsproces: welke doelgroepen en welke boodschappen?

PvA 9: Opzetten crisisbeheersorganisatie
9.1 Crisisbeheer
Bij een calamiteit neemt het crisisbeheerteam tijdelijk de verantwoordelijkheid van de normale managementstructuur over. Op hoofdlijnen moet worden bepaald hoe het crisisbeheer ingericht wordt waaronder: wie besluit om het crisisbeheerteam te activeren? en wie neemt deel in het crisisbeheerteam? (zie PvA). Dit zal in het bedrijfscontinuïteitsplan (10.1) worden.
9.2: Relatie leggen met rampen- / calamiteitenorganisatie gemeente
Iedere gemeente heeft een (interne) rampen-/calamiteitenorganisatie. Het is aan te bevelen om, indien mogelijk, gebruik te maken van deze bestaande structuren voor wat betreft het crisisbeheerteam en naar behoefte mensen toe te voegen aan het team.
9.3: Emergency response checklist geeft een praktische checklist van zaken waaraan gedacht moet worden als er daadwerkelijk een calamiteit optreedt (zie PvA). Stel eventueel het bedrijfscontinuïteitsplan bij en neem eventueel aanvullende preventieve maatregelen.

PvA 6.1: Redundantie maatregelen en voorbereidingen voor de bedrijfscontinuïteit kosten geld. En geld is altijd schaars: gemeenten moeten keuzes maken voor welke doelen deze schaarse middelen worden ingezet. De keuze voor noodzakelijke maatregelen t.b.v. de bedrijfscontinuïteit is niet het eerste aandachtspunt van een gemeente. Daarom is het ook van belang dat in stap 6 (risicoacceptatie) formele besluitvorming onderdeel is van het bedrijfsproces zodat op voorhand al bekend is dat budget nodig is om de risico's tot een acceptabel niveau terug te brengen. Waarbij de relatie met de instandhouding van bedrijfsprocessen t.b.v. de dienstverlening aan de inwoners ook bij bestuur en management helder is. Op basis van de uitwerking van de noodzakelijke te nemen maatregelen en voorbereidingen kunnen de hiervoor noodzakelijke budgetten worden toegevoegd. De benodigde middelen zullen, wanneer niet al voorhanden of te dekken uit al bestaande budgetten, middels het formele besluitvormingsproces door de raad ter beschikking dienen te worden gesteld.

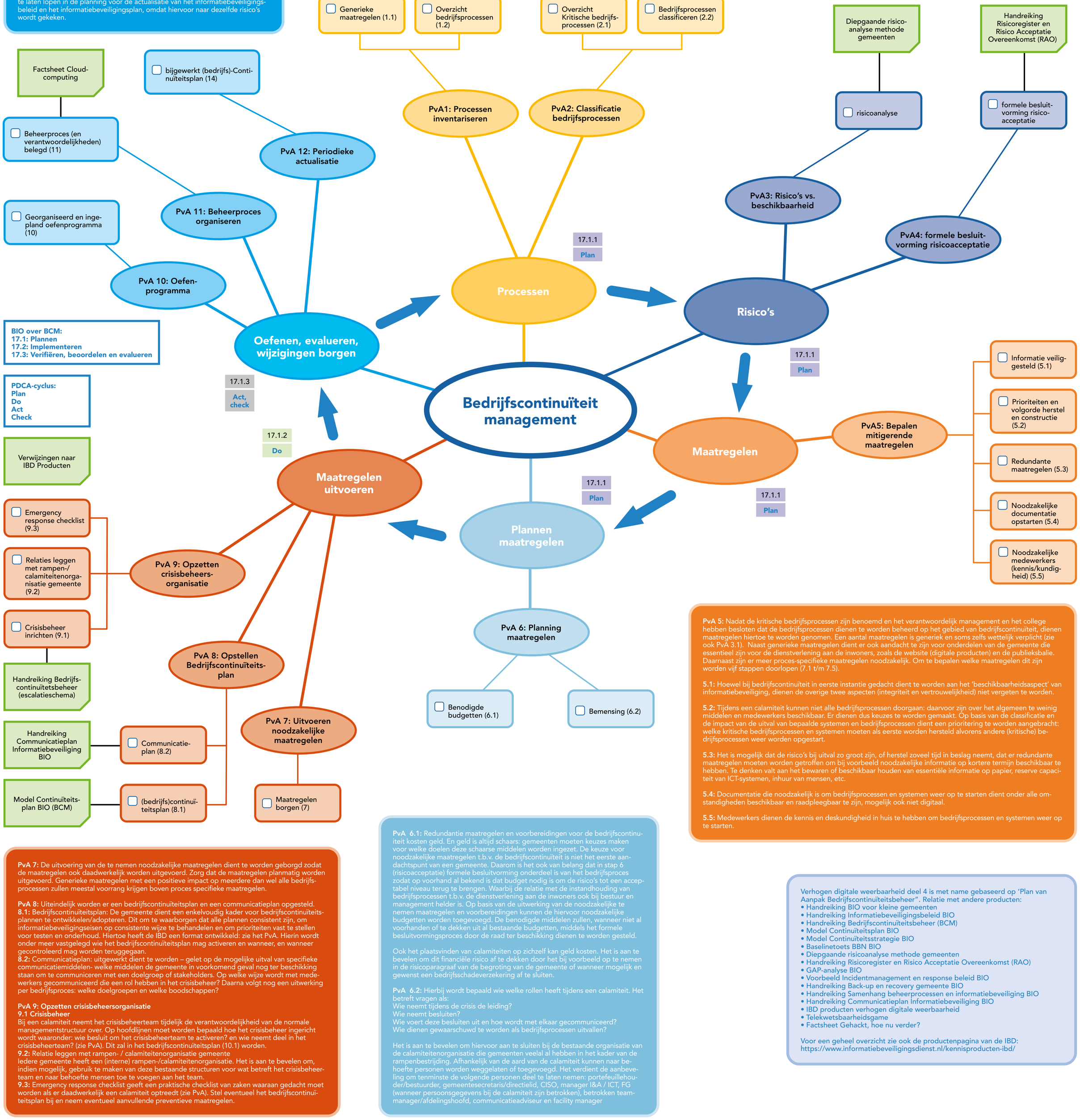
Ook het plaatsvinden van calamiteiten op zichzelf kan geld kosten. Het is aan te bevelen om dit financiële risico af te dekken door het bij voorbeeld op te nemen in de risicoparagraaf van de begroting van de gemeente of wanneer mogelijk en gewenst een bedrijfsschadeverzekering af te sluiten.

PvA 6.2: Hierbij wordt bepaald wie welke rollen heeft tijdens een calamiteit. Het betreft vragen als:
Wie neemt tijdens de crisis de leiding?
Wie neemt besluiten?
Wie voert deze besluiten uit en hoe wordt met elkaar gecommuniceerd?
Wie dienen gewaarschuwd te worden als bedrijfsprocessen uitvallen?

Het is aan te bevelen om hiervoor aan te sluiten bij de bestaande organisatie van de calamiteitenorganisatie die gemeenten veelal al hebben in het kader van de rampenbestrijding. Afhankelijk van de aard van de calamiteit kunnen naar behoefte personen worden weggelaten of toegevoegd. Het verdient de aanbeveling om tenminste de volgende personen deel te laten nemen: portefeuillehouder/bestuurder, gemeentesecretaris/directielid, CISO, manager I&A / ICT, FG (wanneer persoonsgegevens bij de calamiteit zijn betrokken), betrokken teammanager/afdelingshoofd, communicatieadviseur en facility manager

Verhogen digitale weerbaarheid deel 4 is met name gebaseerd op 'Plan van Aanpak Bedrijfscontinuïteitsbeheer". Relatie met andere producten:
- Handreiking BIO voor kleine gemeenten
- Handreiking Informatiebeveiligingsbeleid BIO
- Handreiking Bedrijfscontinuïteitsbeheer (BCM)
- Model Continuïteitsplan BIO
- Model Continuïteitsstrategie BIO
- Baselinetoets BBN BIO
- Diepgaande risicoanalyse methode gemeenten
- Handreiking Risicoregister en Risico Acceptatie Overeenkomst (RAO)
- GAP-analyse BIO
- Voorbeeld Incidentmanagement en response beleid BIO
- Handreiking Back-up en recovery gemeente BIO
- Handreiking Samenhang beheerprocessen en informatiebeveiliging BIO
- Handreiking Communicatieplan Informatiebeveiliging BIO
- IBD producten verhogen digitale weerbaarheid
- Telekwetsbaarheidsgame
- Factsheet Gehackt, hoe nu verder?

Voor een geheel overzicht zie ook de productenpagina van de IBD:
https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/



VNG Realisatie

INFORMATIE BEVEILIGINGS DIENST