Alarm fase	Kenmerk	Impact	Opschaling	Bijzonderheden
		effectbestrijding.		is optioneel.
3	Concernbreed ICT-incident (en mogelijk andere gemeenten)	Impact op de GBT dienstverlening wordt echt ervaren.	Kernteam komt bij elkaar. Afhankelijk van het incident (impact) treedt de GRIP structuur in werking. Bestuur, CIO en directies worden geïnformeerd.	Melding aan CISO. Melding bij IBD (indien nodig). GBT afdeling communicatie is vereist.
4	ICT-Incident is concern overstijgend (landelijk)	Impact op de GBT dienstverlening is manifest.	Mogelijk treedt de GRIP structuur in werking. Het kernteam is dan in beginsel adviserend en voert desgewenst coördinatie (binnen het ICT domein).	Er is sprake van landelijke opschaling via de technische lijn (IBD→ NCSC) of via de maatschappelijke lijn (NCC).

9 Bedrijfscontinuïteit

Risico's

- Wanneer er niet of nauwelijks invulling gegeven wordt aan de continuïteitsplanning is er naast een vals gevoel van veiligheid, ook grote kans op ad hoc maatregelen als een calamiteit zich voordoet.
- Het uitvallen van medewerkers (ziekte, sterven, ontslag) kan een reële bedreiging zijn.

Doelstelling

Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

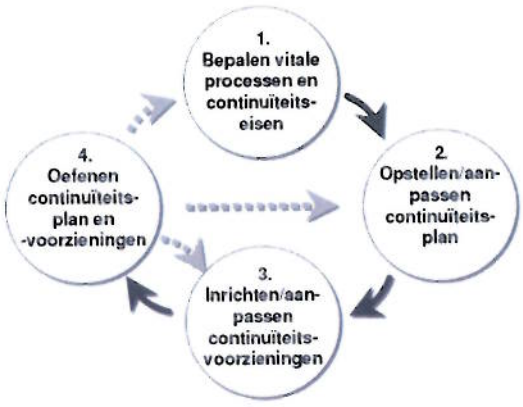
Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.

Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de organisatie.

- Elke GBT afdeling voert een business impactanalyse uit. Afhankelijk van de bevindingen worden per afdeling vervolgacties gepland.
- Elke afdeling heeft een eigen plan voor Business Continuity Management (BCM) (bedrijfscontinuïteitsbeheer). In de continuïteitsplannen wordt minimaal aandacht besteed aan:
  - risico's;
  - identificatie van essentiële procedures voor bedrijfscontinuïteit;
  - wie het plan mag activeren en wanneer, maar ook wanneer er weer gecontroleerd wordt teruggegaan;
  - veilig te stellen informatie (aanvaardbaarheid van verlies van informatie);
  - prioriteiten en volgorde van herstel en reconstructie;
  - documentatie van systemen en processen;
  - kennis en kundigheid van personeel om de processen weer op te starten.
- Er worden minimaal jaarlijks oefeningen of testen gehouden om de BCM plannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

Beleidsuitgangspunt

Er zijn voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen.
Continuïteitsplannen moeten regelmatig worden getest en actueel worden gehouden.



Figuur 4:• BCM Cyclus

10 Naleving

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen.

10.1 Organisatorische aspecten

- Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle GBT processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. De kwaliteit wordt gemeten aan:
  - de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
  - efficiency en effectiviteit van de geïmplementeerde maatregelen;
  - de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.
- De CISO zorgt namens de directeur van het GBT voor het toezicht op de uitvoering van het IB-beleid.
- ICT en externe hosting providers leggen verantwoording af aan hun opdrachtgevers over de naleving van het IB-beleid. Bij uitbestede (beheer)processen kan een verklaring bij leveranciers worden opgevraagd (TPM of ISAE3402-verklaring).
- Naleving van regels vergt in toenemende mate ook externe verantwoording, bijvoorbeeld voor het gebruik van DigiD, SUWI en GBA. Aanvullend op dit concern IB-beleid kunnen daarom specifieke normen gelden voor clusters.[30]
- Periodiek wordt de kwaliteit van informatieveiligheid in opdracht van de CIO onderzocht door GBT auditors en door onafhankelijke externen (bijvoorbeeld door middel van 'penetratietesten'). Jaarlijks worden ca. 3 audits/onderzoeken gepland. De bevindingen worden gebruikt voor de verdere verbetering van de informatieveiligheid.
- In de P&C cyclus wordt gerapporteerd over informatieveiligheid aan de hand van het 'in control' statement.
- Er wordt een beveiligingsdocumentatiedossier aangelegd en onderhouden. Dit dossier bevat alle relevante verplichte en niet verplichte documenten waaruit blijkt of kan worden aangetoond dat aan de specifieke beveiligingseisen is voldaan.

10.2 (Wettelijke) kaders

- Een overzicht van relevante wet en regelgeving is te vinden bij KING.[31] Zo is het gebruik van persoonsgegevens geregeld in de Wet Bescherming Persoonsgegevens.[32]
- Voor elk type registratie wordt de bewaartermijn, het opslagmedium en eventuele vernietiging bepaald in overeenstemming met wet, regelgeving, contractuele verplichtingen en bedrijfsmatige eisen. Bij de keuze van het opslagmedium wordt rekening gehouden met de bewaartermijn, de achteruitgang van de kwaliteit van het medium in de loop van de tijd en de

[30] Binnen de sector gemeenten wordt gestreefd naar een uniform audit-kader om de verantwoordingslast zo veel mogelijk te beperken.
[31] Een concept overzicht van wetten, regelingen en andere kaders is beschikbaar op de website van KING.
[32] Zie ook: CBP richtsnoeren

voortdurende beschikbaarheid van hulpmiddelen (zoals hard- en software) om de gegevens te raadplegen en te bewerken.

- Bij het (laten) vervaardigen en installeren van programmatuur, wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar op rusten niet worden geschonden.

11 Bijlage: Relevante documenten en bronnen

11.1 Intern

- Het GBT kan hier zelf verwijzen naar eigen standaarden en procedures. Vanuit VNG/KING worden in 2013 nog meerdere producten geleverd die hier benoemd kunnen worden.
- Algemene Inkoop Voorwaarden, Gemeentelijk Belastingkantoor Twente.

11.2 Extern

- NEN/ISO 27001 (2005) en 27002 (Code voor Informatiebeveiliging)(2007)
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), KING, 2013
  - strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- CBP richtsnoeren 'beveiliging van persoonsgegevens', 2013: http://www.cbpweb.nl/Pages/pb_20130219_richtsnoeren-beveiliging-persoonsgegevens.aspx
- GEMMA: http://www.kinggemeenten.nl/king-kwaliteitsinstituut-nederlandse-gemeenten/e-dienstverlening-verbeteren/gemma

Aldus vastgesteld door het algemeen bestuur van de gemeenschappelijke regeling Gemeentelijk Belastingkantoor Twente.

Hengelo, 15 april 2015

De secretaris,

.....

dr. R. Toet

de voorzitter,

.....

mr. drs. R.G. Welten

INFORMATIE BEVEILIGINGS DIENST

INFORMATIEBEVEILIGINGSDIENST
V00R GEMEENTEN (IBD)

NASSAULAAN 12
2514 JS DEN HAAG

POSTBUS 30435
2500 GK DEN HAAG

HELPDESK 070 373 80 11
ALGEMEEN 070 373 80 08
FAX 070 363 56 82

IBD@KINGGEMEENTEN.NL
WWW.KINGGEMEENTEN.NL

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN