



Bedrijfscontinuïteitsmanagement

hoe kunnen we daarin samenwerken

MBO Digitaal Conferentie 8 maart 2023

Workshop 4.4

Charlie van Genugten, Rob Gerritsen, Henk Links

Programma

1. (N)OZON
2. Bedrijfscontinuïteitsmanagement
3. Hoe pak je dat aan?





SURF

Hoe zijn we hier beland?

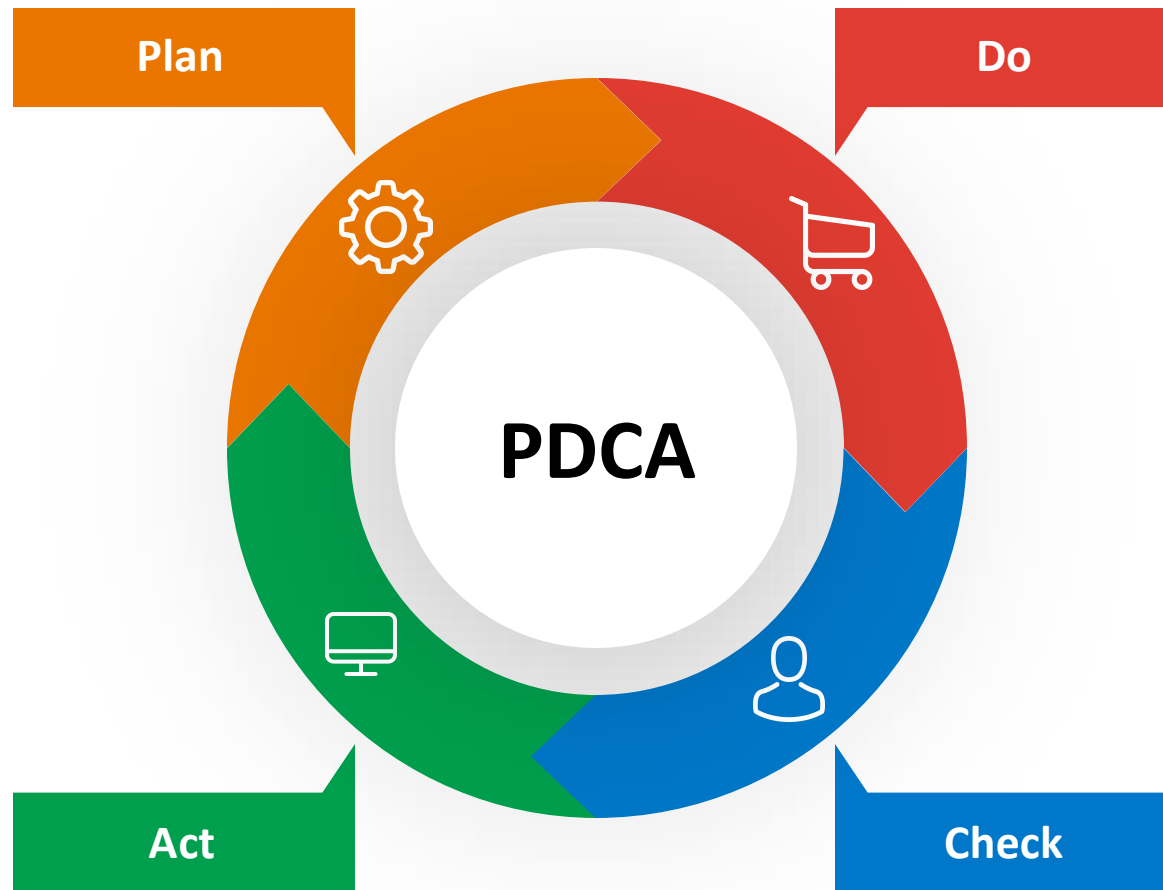
Charlie van Genuchten, SURF

11 March, 2024

| OZON, NOZON en andere crises



SURF



Bedrijfscontinuïteitsmanagement



Bedrijfscontinuïteitsmanagement (BCM) is het vermogen van een organisatie zo snel mogelijk weer aan de slag te kunnen na een tegenslag.

Door te werken aan plannen, rolverdelingen en terugvalopties kunnen de belangrijkste bedrijfsprocessen op een acceptabel niveau doorgaan.

Daarbij spelen altijd afwegingen: wat zijn de belangrijkste bedrijfsprocessen, en wat is een acceptabel niveau?

Bij deze afwegingen baseer je je op de bedrijfsdoelen van de organisatie, en hoeveel **risico** ze bereid is te dragen.

14 Bedrijfscontinuïteitsmanagement

- **14.1 Bedrijfscontinuïteitsplan(ning)**

Het **Bedrijfscontinuïteitsplan** is gericht op het identificeren van potentiële bedreigingen en de impact die deze bedreigingen hebben op de continuïteit van de bedrijfsvoering.

- **14.2 Testen van de Disaster recovery**

- 14.3 Offsite backupopslag
- 14.4 Gegevensreplicatie

- **14.5 Crisismanagement**

Het **Crisisplan** is gericht op het beheersen van de situatie en het minimaliseren van schade.

Kernmerken Crisis

Een (cyber)crisis is een abnormale en instabiele situatie waarin strategische doelen, reputatie en betrouwbaarheid (opzettelijk of onopzettelijk) worden bedreigd door een verstoring in de kern van de organisatie.

- Substantiële dreiging voor de organisatie
- Verrassingselement
- Korte beslistijden
- Urgentie en snelle ontwikkelingen
- Hoge mate van onzekerheid
- Beperkte (soms onjuiste) informatie
- Media aandacht (waaronder social media)

14.1 (BC.01) Bedrijfscontinuïteitsplanning

- Bedrijfs- en it-continuïteitsplannen zijn gedefinieerd, geïntegreerd en goedgekeurd door het senior management.
- De organisatie heeft een **bedrijfsimpactanalyse** uitgevoerd, op basis waarvan recoverytime- doelen zijn bepaald en volledig gedocumenteerde it-herstelplannen en bedrijfs- continuïteitsplannen zijn opgesteld om deze doelen te bereiken.
- De plannen betreffen gebruikershandleidingen, rollen, verantwoordelijkheden, crisismanagement, communicatieprocessen en de testmethode.

Dankzij deze plannen kan de organisatie waarschijnlijk belangrijke operationele processen voortzetten in het geval van een grote onderbreking.

14.2 (BC.02) Testen van Disaster recovery

- Bedrijfs- en it-continuïteitsplannen worden getest via goedgekeurde, geïntegreerde **test-/ herstelscenario's**.
- Bedrijfs- en it-continuïteitsplannen worden op regelmatige basis getest (ten minste eenmaal per jaar) om ervoor te zorgen dat essentiële systemen effectief kunnen worden hersteld, dat tekortkomingen worden aangepakt en dat het plan up-to-date blijft.
- Er is voorzien in een gedegen voorbereiding, documentatie, rapportage van de testresultaten en, afhankelijk van de resultaten, uitvoering van een actieplan.

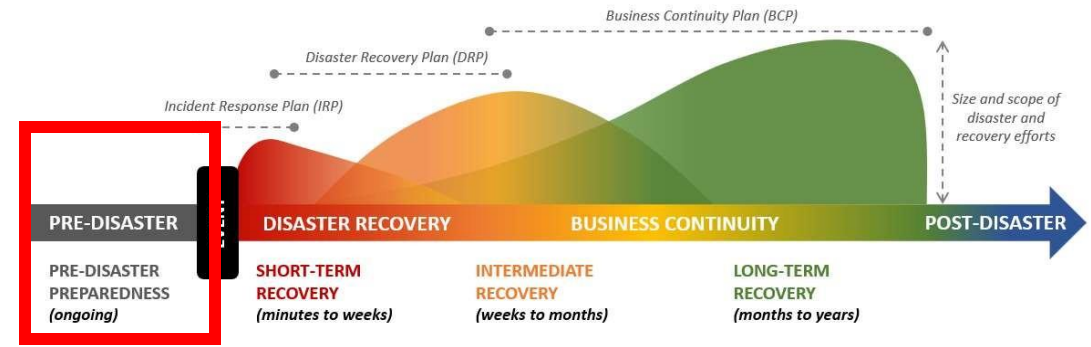
14.5 (BC.05) Crisismanagement

- Er is een crisismanagementplan dat **onderdeel is van het bedrijfscontinuïteitsplan (BCP)**, waardoor de organisatie de essentiële bedrijfsvoering weer kan oppakken, terwijl het crisismanagementteam zich op de crisis richt.
- Alle betrokkenen zijn op de hoogte van de verantwoordelijkheden tijdens een crisis.
- Er zijn periodiek crisisoefeningen voor crisismanagementteams.

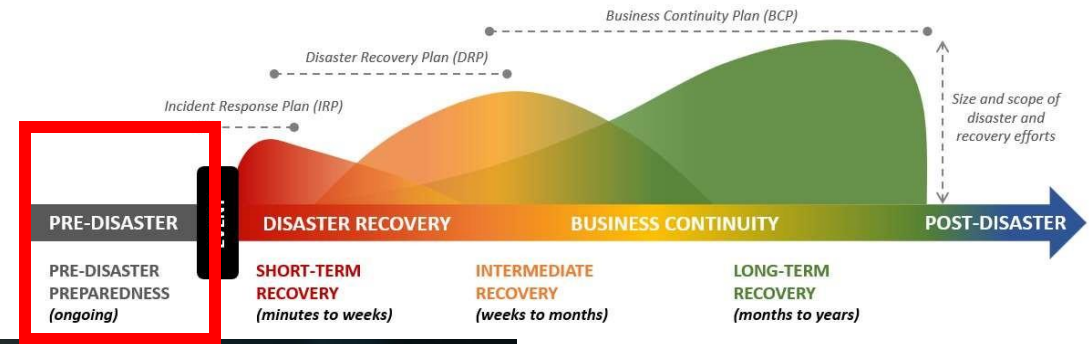
Aan de slag

- **Stap 1 | Stel kritische bedrijfsprocessen, systemen en leveranciers vast**
 - **Stap 2 | Bespreek wat je zou doen bij uitval van kritische systemen**
 - **Stap 3 | Leg terugvalopties en andere werkwijzen vast in een bedrijfscontinuïteitsplan**
- *Stap 4 | Oefen met het bedrijfscontinuïteitsplan en evalueer*
 - *Stap 5 | Neem besluiten over aanvullende maatregelen en afspraken*
 - *Stap 6 | Voer aanvullende maatregelen en afspraken in*
 - **Stap 7 | Oefen jaarlijks en verbeter het bedrijfscontinuïteitsplan**

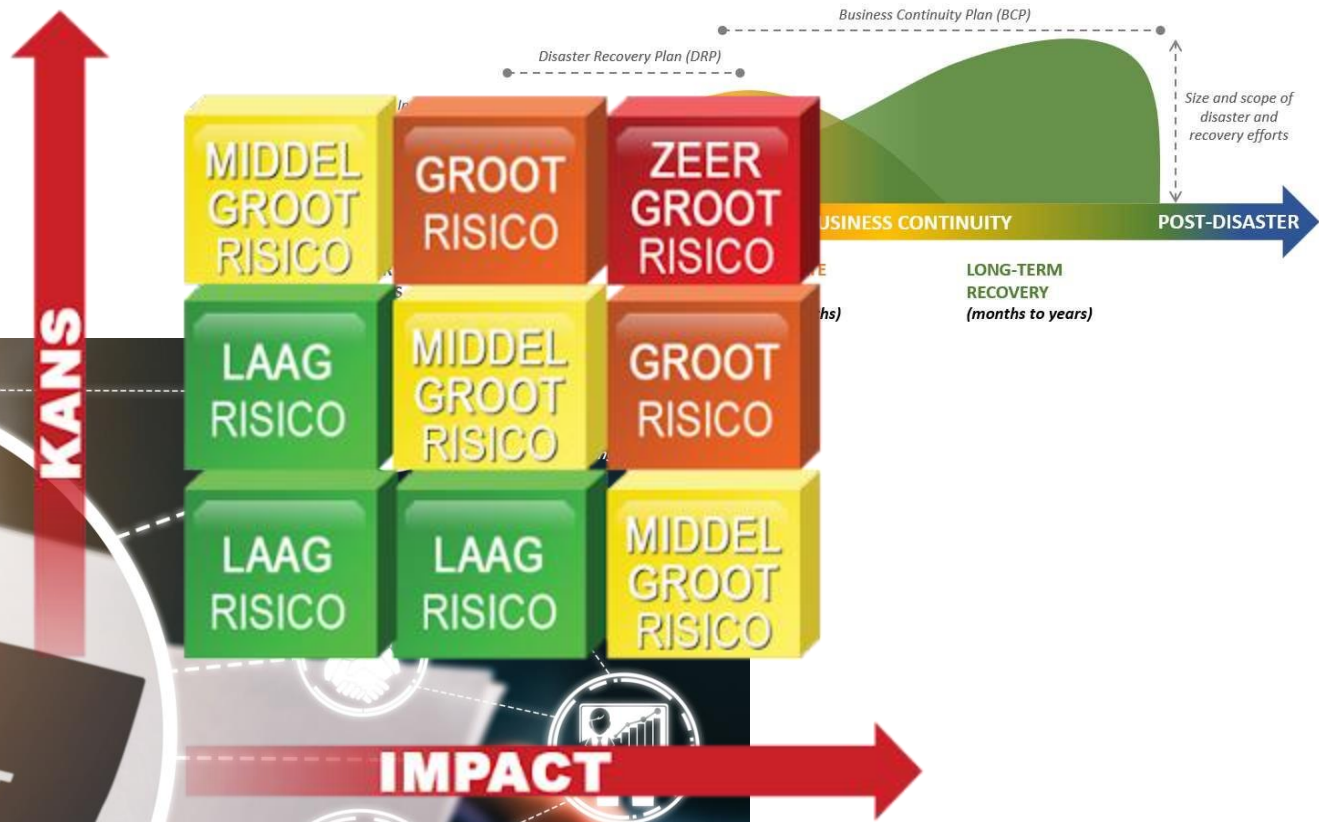
En hoe pak je dat aan?

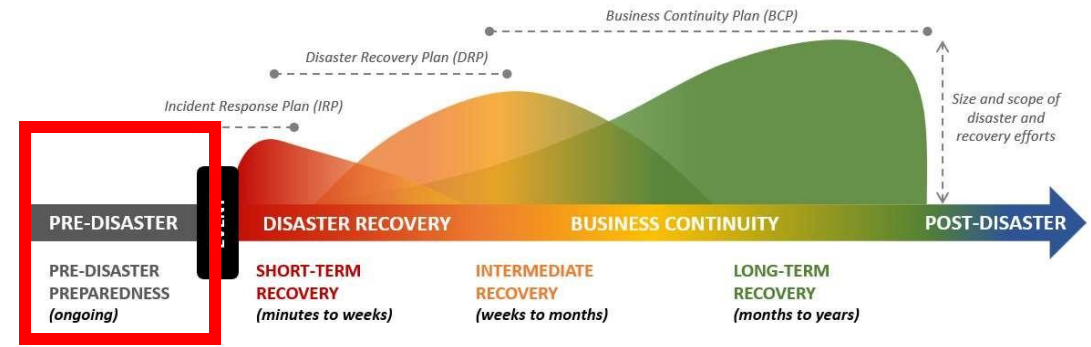


En hoe pak je dat aan?



En hoe pak je dat aan?



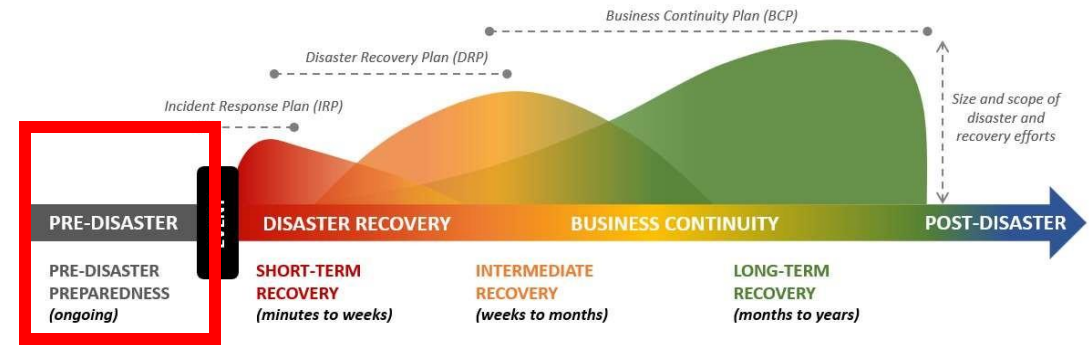


2. BIV-Classificatie

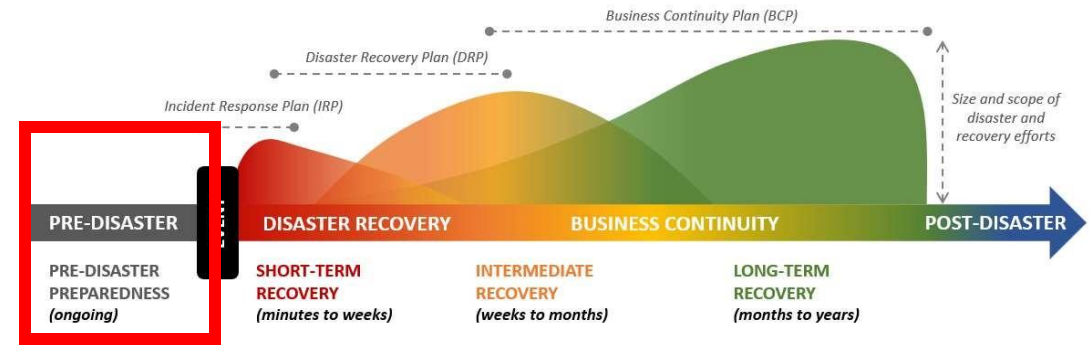
	RISICO WAARDEN			
	1	2	3	4
BESCHIKBAARHEID				
Niet nodig	X			
Benodigd		X		
Noodzakelijk			X	
Essentieel				X
INTEGRITEIT				
Niet noodzakelijk	X			
Noodzakelijk		X		
Weselst			X	
Absoluut				X
VERTROUWELIJKHEID				
Openbaar	X			
Intern		X		
Vertrouwelijk			X	
Geheim				X
RISICO				



... En dan?



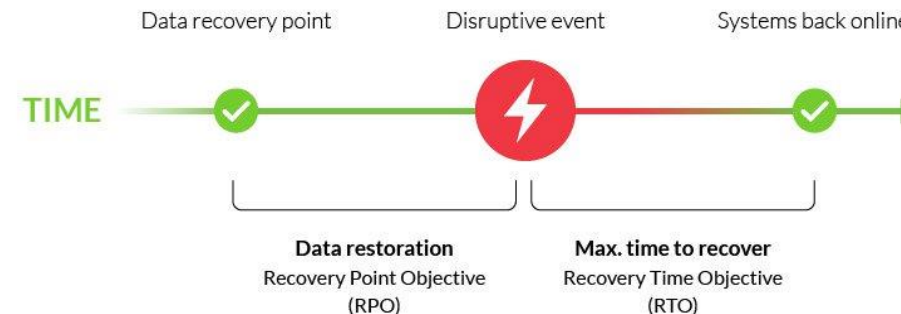
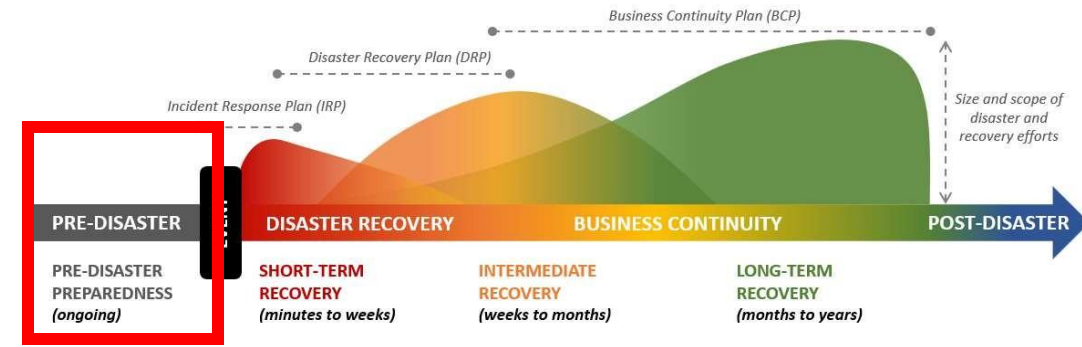
... En dan?



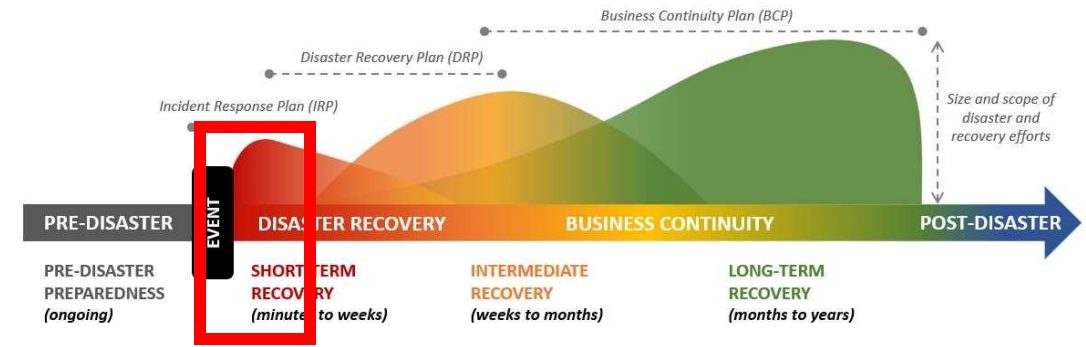
(CYBER) BUSINESS IMPACT ANALYSE

1. Identificeren van business processen en eigenaren
2. Kwantificeren van business waarde en mogelijk verlies
3. Definiëren van acceptable disruptie op de business
4. Identificeren van key IT services
5. Identificeren van key IT systemen

BUSINESS CONSULTANCY EN STRATEGIE



Incident response plan



Incident response plan

Preparation

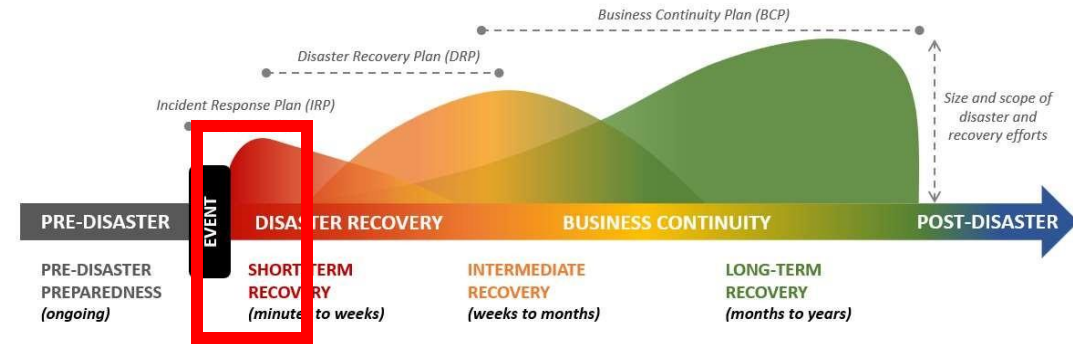
Identification

Containment

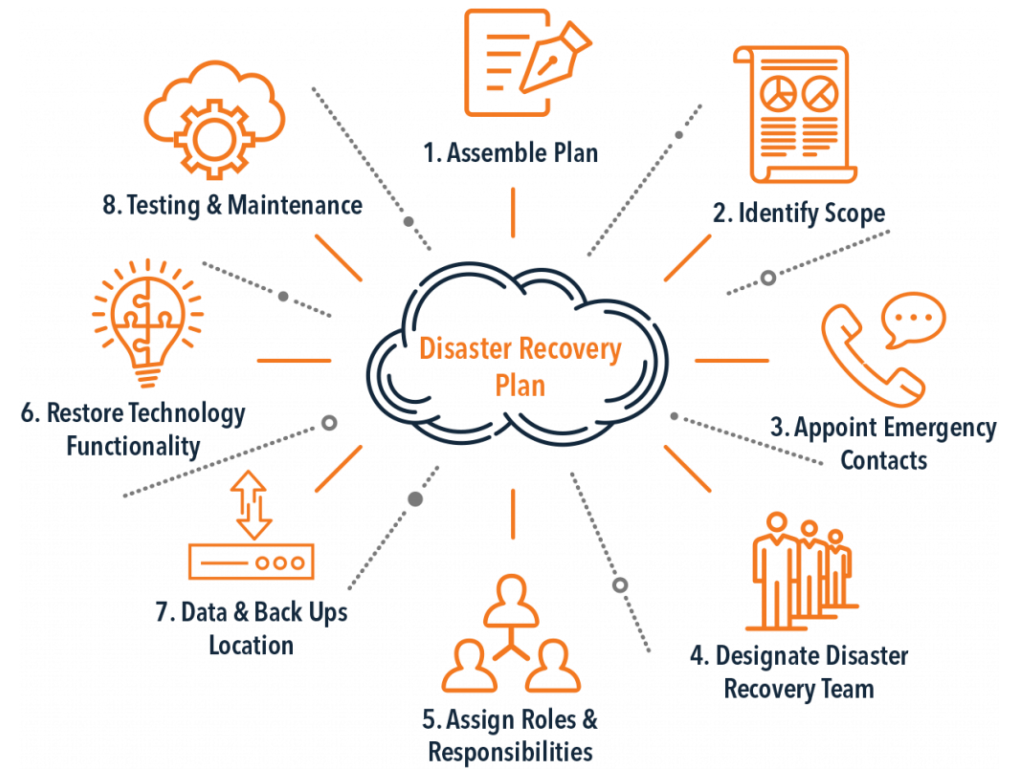
Eradication

Recovery

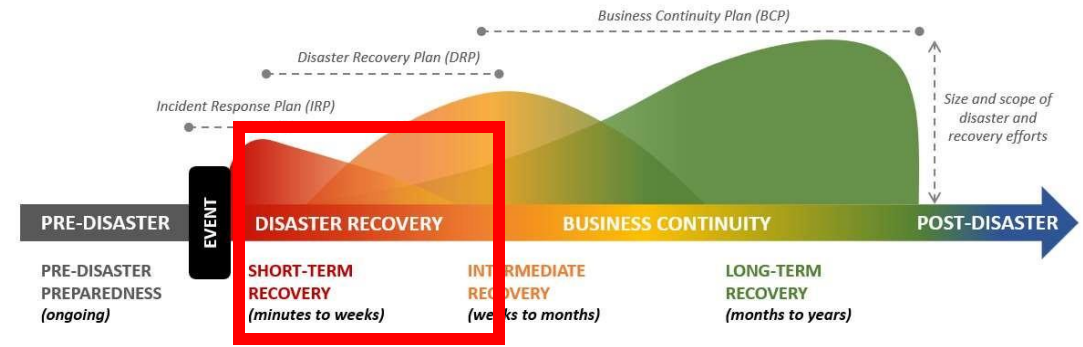
Lessons Learned



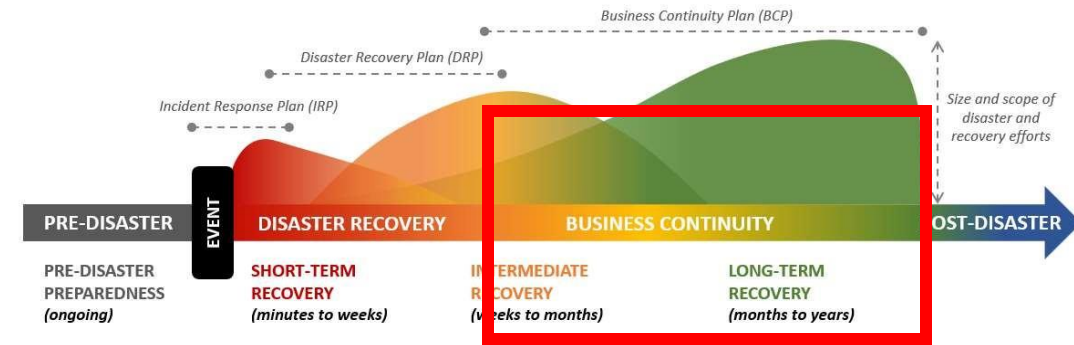




En dan... Draaiboeken?



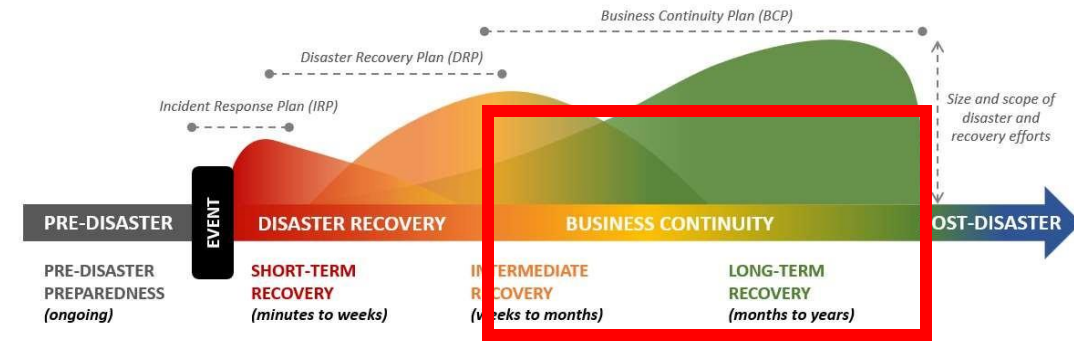
En dan... Draaiboeken?



- Dataclassificatie op orde
- Risicomanagement ingebed (niet alleen digitaal domein)
- Eigenaarschap belegd (voor proces en data)
- Crisisorganisatie op orde (en trainen/oefenen)
- Disaster recovery plan (in PDCA)

En dan... Draaiboeken?

- Dataclassificatie op orde
- Risicomanagement ingebed (niet alleen digitaal domein)
- Eigenaarschap belegd (voor proces en data)
- Business Impact Analyse uitgevoerd
- Crisisorganisatie op orde (en trainen/oefenen)
- Disaster recovery plan (in PDCA)



En dan... Draaiboeken!

