[logo organisatie]

[naam organisatie]

METHODOLOGIE VOOR BUSINESS IMPACT ANALYSE

Code:	
Versie:	
Versiedatum	
Gemaakt door:	
Goedgekeurd door:	
Classificatie:	

Comment [DK1]: Om meer te weten over de business impact analyse, lees dit artikel: How to implement business impact analysis (BIA) according to ISO 22301 http://www.iso27001standard.com/blog/2013/12/03/how-to-implement-business-impact-analysis-bia-according-to-iso-22301/

Comment [DK2]: Om te leren hoe dit document in te vullen, zie deze videohandleiding "How to Write the Business Impact Analysis Methodology According to ISO 22301":
- Indien u de toolkit hebt gekocht, dan vindt u het op het ISO 27001 & ISO 22301 Klantenportaal: https://epps.customerhub.net/
- Indien u de toolkit niet heeft gekocht, dan vindt u de preview van de handleiding hier: http://www.iso27001standard.com/tutorial/video-tutorial-how-to-write-the-business-impact-analysis-methodology-according-to-iso-22301/

Comment [DK3]: Alle velden in dit document gemarkeerd met spekhaken [ ] moeten worden ingevuld.

Comment [DK4]: De documentcodering moet in overeenstemming zijn met het bestaande organisatiecoderingssysteem; indien een dergelijk systeem niet is geïmplementeerd, dan kan deze regel worden verwijderd.

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
DD/MM/JJJJ	0.1	Dejan Kosutic	Concept Basisdocument

Inhoudsopgave

1. Doel, toepassingsgebied en gebruikers

Het doel van dit document is het definiëren van de methodologie en het proces voor het beoordelen van de verstorende gevolgen voor de activiteiten van [naam organisatie], en voor het bepalen van continuïteits- en herstelprioriteiten, doelstellingen en doelen.

Business impact analyse is van toepassing op het hele toepassingsgebied van het Managementsysteem voor Informatiebeveiliging (ISMS), d.w.z. voor alle activiteiten die de producten en diensten van [naam organisatie] ondersteunen.

Gebruikers van dit document zijn alle werknemers van [naam organisatie] die deelnemen aan het vaststellen en implementeren van het ISMS.

Comment [DK5]: Indien allen bedrijfscontinuïteit is geïmplementeerd (niet de informatiebeveiliging) dan schrijf deze tekst daarvoor in de plaats: 'Managementsysteem voor Bedrijfscontinuïteit (BCMS)'.

Comment [DK6]: Of 'BCMS'

2. Gerefereerde documenten

- ISO 22301 norm clausules 8.2.1 en 8.2.2
- BS 25999-2 clausule 4.1.1
- Bedrijfscontinuïteitsbeleid
- Bedrijfscontinuïteit Strategie
- Lijst van Wetgevende, Regelgevende, Contractuele en Andere Verplichtingen

3. Business impact analyse methodologie

Comment [DK7]: Deze Methodologie dient te worden aangepast indien vereist is door wetgevende en regelgevende eisen of contractuele verplichtingen.

3.1. Organisatie

Business impact analyse wordt geïmplementeerd door middel van Business Impact Analyse vragenlijsten. Het proces wordt gecoördineerd door [Functie], en de analyse van individuele activiteiten wordt uitgevoerd door de verantwoordelijk in elke activiteit.

Business impact analyse wordt uitgevoerd nadat de risicobeoordeling is afgerond, zodat de informatie over de benodigde middelen kan worden verzameld gedurende risicobeoordeling.

Behandeling van vertrouwelijke documenten gemaakt volgens deze Methodologie dient volgens [naam document] te worden gedaan.

Comment [DK8]: Bijv. Beleid voor de behandeling en beschikbaarheid informatie

3.2. Identificatie van activiteiten

[Functie] is verantwoordelijk voor de identificatie van alle activiteiten die de levering van producten en diensten ondersteunen, en voor het definiëren van de verantwoordelijke voor elke activiteit.

3.3. Gevolgen van een verstorend incident

De gevolgen (impact) van een verstorend incident op een activiteit worden beoordeeld door middel van (1) algemene gevolgen (kwalitatieve beoordeling), en (2) financiële gevolgen (kwantitatieve beoordeling). Beide van deze gevolgen worden beoordeeld voor de volgende tijdvakken:

- 2 uur
- 4 uur

- 24 uur
- 48 uur
- 1 week

Indien een activiteit minder tijdsgevoelig is, dan kunnen de tijdvakken voor die specifieke activiteit worden uitgerekt, bijv. Van 4 uur naar 2 weken of vergelijkbaar.

Voor een algemene beoordeling (1) worden de gevolgen (impact) als volgt geclassificeerd:

Marginale impact	1	Duur van het verstorende incident veroorzaakt verwaarloosbare schade aan de cashflow, wettelijke of contractuele verplichtingen van de organisatie of haar reputatie.
Acceptabele impact	2	Duur van het verstorende incident veroorzaakt schade aan de cashflow, wettelijke of contractuele verplichtingen van de organisatie of haar reputatie. Echter dergelijke schade is nog steeds acceptabel gezien de grootte ervan en de specifieke omstandigheden.
Hoge impact	3	Duur van het verstorende incident veroorzaakt schade aan de cashflow, wettelijke of contractuele verplichtingen van de organisatie of haar reputatie. Dergelijke schade is onacceptabel gezien de grootte ervan en de specifieke omstandigheden.
Catastrofale impact	4	Duur van het verstorende incident veroorzaakt schade aan de cashflow, wettelijke of contractuele verplichtingen van de organisatie of haar reputatie. Zodanig dat ze het meeste van haar kapitaal zal verliezen en/of haar bedrijfsvoering blijvend zal moeten staken.

Voor een financiële beoordeling (2) worden de gevolgen in de locale munteenheid uitgedrukt.

3.4. Bepalen Maximale Toelaatbare Uitvalsduur (MUD)

Maximaal toelaatbare uitvalsduur / Maximaal Toelaatbare periode van verstoring wordt bepaald in uren of dagen, als volgt:

- De kortste tijd waarin de algemene impact van niveau 3 is (of niveau 4 indien niveau 3 niet wordt genoemd), of
- De kortste tijd waarin de financiële gevolgen onacceptabel zijn vergeleken met eigen vermogen/winst/budget/inkomsten.

3.5. Hoeveelheid werk

In dit gedeelte van de analyse worden de perioden met de pieken met de hoogste werklast geïdentificeerd en minimale bedrijfscontinuïteitsdoelstelling bepaald.

3.6. Middelen nodig voor herstel

De volgende soorten middelen dienen te worden geïdentificeerd:

- Mensen
- Applicaties / databases

- Gegevens opgeslagen in elektronische vorm (niet opgenomen in applicaties en databases)
- Gegevens opgeslagen op papieren media
- IT en communicatie apparatuur
- Communicatiekanalen
- Andere apparatuur
- Faciliteiten en infrastructuur
- Werkkapitaal
- Externe diensten

Voor elk middel dient het volgende te worden bepaald:

- Hoeveelheid middelen die nodig zijn voor het herstel van een activiteit
- Of het middel in kwestie het Single Point of Failure is
- Na hoeveel tijd de resource vereist is (de tijd na de hervatting van de activiteit)

3.7. Afhankelijkheid van anderen

In dit deel van de analyse dienen de afhankelijkheden van (1) andere activiteiten, (2) uitbestedingspartners en (3) leveranciers te worden geïdentificeerd.

Voor elke uitbestedingspartner en leverancier dient het volgende te worden geanalyseerd:

- Welk document definieert de vereisten in geval van een verstorend incident
- Het bestaande niveau van vermogen tot handelen met betrekking tot bedrijfscontinuïteit

3.8. Maximaal gegevensverlies

Voor elke database, applicatie of informatie geïdentificeerd in de analyse, dient het maximum aan gegevens dat verloren kan gaan te worden beoordeeld. Het gegevensverlies wordt beoordeeld voor de hoeveelheid gegevens dat is gecreëerd in de laatste:

- 1 uur
- 4 uur
- 24 uur
- 48 uur
- 1 week

Indien nodig kunnen de tijdvakken in afzonderlijke activiteiten kunnen worden ingekort/verlengd teneinde het type gegevens in die activiteit te passen.

Het gevolg (impact) van verlies daarvan wordt als volgt geclassificeerd:

Marginale impact	1	Hoeveelheid verloren gegevens veroorzaakt verwaarloosbare schade aan de cashflow, wettelijke of contractuele verplichtingen van de organisatie of haar reputatie.
Acceptabele impact	2	Hoeveelheid verloren gegevens veroorzaakt schade aan de cashflow, wettelijke of contractuele verplichtingen van de organisatie of haar reputatie. Echter dergelijke schade is acceptabel gezien de grootte ervan en de specifieke omstandigheden.

Hoge impact	3	Hoeveelheid verloren gegevens veroorzaakt schade aan de cashflow, wettelijke of contractuele verplichtingen van de organisatie of haar reputatie. Dergelijke schade is onacceptabel gezien de grootte ervan en de specifieke omstandigheden.
Catastrofale impact	4	Hoeveelheid verloren gegevens veroorzaakt zeer grote schade van de cashflow, wettelijke of contractuele verplichtingen aan de organisatie of haar reputatie. Zodanig dat ze het meeste van haar kapitaal zal verliezen en/of haar bedrijfsvoering blijvend zal moeten staken.

3.9. De resultaten rapporteren

De informatie verzameld door middel van de Business Impact Analyse Vragenlijsten wordt verstuurd naar [functie], wiens verantwoordelijkheid het is om het samen te voegen en de gegevens te documenteren via de Bedrijfscontinuïteit Strategie.

3.10. Reguliere herbeoordeling van de business impact analyse

[Functie] dient een herbeoordeling uit te voeren van de Business Impact Analyse Vragenlijsten en de Bedrijfscontinuïteit Strategie dienovereenkomstig bij te werken. De herbeoordeling wordt minstens één keer per jaar uitgevoerd, of vaker bij significante organisatieveranderingen, significante technologische verandering, verandering van bedrijfsdoelstellingen, veranderingen in de bedrijfsomgeving, enz.

4. Registratiebeheer op basis van dit document

Naam registratie	Opslaglocatie	Persoon verantwoordelijk voor opslag	Beveiligingsmaatregelen voor registraties	Bewaartermijn
Business Impact Analyse Vragenlijsten (elektronische vorm - Excel document)	Computer van [functie]	[functie]	Vragenlijsten dienen te worden opgeslagen in alleen-lezen formaat.	Gegevens worden opgeslagen voor 5 jaar.

Alleen [functie] kan andere werknemers toegang verlenen tot een van de bovengenoemde documenten.

5. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

De eigenaar van dit document is [functie]. Hij/zij dient het document te controleren en indien nodig het minstens eens per jaar bij te werken, voor de reguliere herbeoordeling van de Business Impact Analyse Vragenlijsten.

Comment [DK9]: Dit is slechts een aanbeveling, pas de frequentie zo nodig aan.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de volgende criteria in ogenschouw te worden genomen:

- het aantal middelen niet opgenomen in de Business Impact Analyse Vragenlijsten
- het niet erin slagen om activiteiten te herstellen als gevolg van fouten in het business analyse proces
- het aantal fouten in het business impact analyse proces als gevolg van onduidelijke definitie van rollen en verantwoordelijkheden

6. Bijlage

- Business Impact Analyse Vragenlijst

[functie]
[naam]

_____
[handtekening]

Comment [DK10]: Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.