Beleidslijn informatieveiligheid en privacy

Risico-beoordeling

(BLD RISK)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

Het begrip “risico” kan op verschillende wijzen worden geïnterpreteerd. In deze beleidslijnen wordt het begrip "risico" omschreven als de **kans** (“waarschijnlijkheid”) dat een bepaalde bedreiging zich voordoet met een welbepaalde **impact** (“ernst”) tot gevolg.

Het begrip “risico-beoordeling” verwijst naar het geheel van procedures dat er toe strekt om risico’s te identificeren, analyseren en beoordelen.

- **Identificatie** van risico’s verwijst naar het proces dat ertoe strekt om risico’s te onderzoeken, erkennen en beschrijven.
- De **analyse** van het risico verwijst naar het proces dat er toe strekt om de aard van een risico na te gaan en om het risiconiveau te bepalen.
- De **evaluatie** van het risico bestaat in een vergelijking van het resultaat van de risico analyse met vooraf bepaalde risico-criteria om te bepalen of het risico (en/of de grootte daarvan) al dan niet aanvaardbaar of draaglijk is.

Bij risicobeheer wordt een onderscheid gemaakt tussen het “inherente” risico en het “residuele” risico.

- Het “**inherente**” risico verwijst naar de waarschijnlijkheid dat een negatieve impact zich zal voordoen wanneer er geen beschermingsmaatregelen genomen worden.
- Het “**residuele**” risico verwijst daarentegen naar de waarschijnlijkheid dat een negatieve impact zich zal voordoen, ondanks de maatregelen die genomen worden om het (inherent) risico te beïnvloeden (beperken)

Dit document beschrijft de beleidslijnen rond de risico-beoordeling van informatieveiligheid en privacy.

2. Risico-beoordeling van informatieveiligheid en privacy

De organisatie onderschrijft de volgende beleidslijnen van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

1. De organisatie moet bij elk proces en bij elk project een risico-beoordeling rond informatieveiligheid en privacy uitvoeren, valideren, communiceren en onderhouden
2. De organisatie moet alle risico-beoordelingen met een hoog residueel risico communiceren naar de directie voor bespreking en beslissing : behandelen of aanvaarden.
3. De organisatie moet de richtlijn rond risico-beoordeling toepassen zoals vermeld in bijlage C van de beleidslijn ‘Risico-beoordeling’.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2017		V2017	Integratie EU GDPR	07/03/2017	07/03/2017

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen de contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:

- VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 April 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)
- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- ISACA, “COBIT 5 for Risk”, june 2013, 218 blz.
- ISACA, “Risk IT practitioner guide”, November 2009, 137 blz.

Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:

- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32016R0679&qid=1488526812774&from=en
- https://www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-0
- https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
- https://www.enisa.europa.eu/topics/data-protection
- https://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia
- https://www.enisa.europa.eu/publications/tsp2-risk
- https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment
- http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf
- http://www.ccb.belgium.be/nl/documents
- https://www.ksz-bcss.fgov.be/nl

Bijlage C: Richtlijnen rond risico-beoordeling

Een risicobeoordeling steeds dient plaats te vinden in functie van het geheel van bijzondere omstandigheden van elke verwerking (of groep van vergelijkbare verwerkingen)

De waarschijnlijkheid en de ernst van het risico voor de rechten en vrijheden van de betrokkene moeten worden bepaald onder verwijzing naar de aard, het toepassingsgebied, de context en de doeleinden van de verwerking. Het is dus in functie van het geheel van bijzondere omstandigheden van elke verwerking dat de verwerkingsverantwoordelijke de risico's voor het privéleven en voor de rechten en vrijheden van personen moet inschatten en de passende maatregelen moet nemen om de toepassing van de bepalingen van de verordening te waarborgen.

Minimale kenmerken van een behoorlijk risicobeheer

In de regel beslist de verwerkingsverantwoordelijke vrij over de procedure en methodologie die hij wenst te hanteren bij het inschatten en beheren van risico's, op voorwaarde dat deze beantwoordt aan een aantal minimumkenmerken van betrouwbaarheid en objectiviteit. Het gaat hier om minimale kenmerken, die op zich geen garantie inhouden dat de beoogde verwerking(en) zal (zullen) plaatsvinden.

1. Methodologisch onderbouwd : Risicobeheer en risicobeoordeling dienen methodologisch onderbouwd te zijn, bij voorkeur aan de hand van reeds bestaande methodologieën inzake risicobeheer. Internationale standaarden, zoals deze ontwikkeld door ISO, alsook gedragscodes ontwikkeld of erkend op Europees niveau, zijn hierbij van bijzonder belang. De verwerkingsverantwoordelijke dient uitdrukkelijk aan te geven welke methodologie gekozen werd en dient erover te waken dat deze op een consistente wijze wordt toegepast doorheen het risicobeoordelingsproces.
2. Gestructureerd: Een behoorlijk risicobeheer verloopt op een gestructureerde wijze, waarbij men doorgaans de volgende stappen kan onderscheiden:
   - definitie van de relevante context (bestaande uit de externe en interne parameters die in rekening gebracht dienen te worden bij de beheersing van risico's);
   - definitie van maatstaven om de risico's voor de rechten en vrijheden van natuurlijke personen in te schatten;
   - identificatie en analyse van risico's (inclusief de identificatie van kwetsbaarheden, bedreigingen, en de toekenning van een risicowaarde);
   - definitie van aanvaardbare risicowaarden (inclusief een bepaling van welke risicowaarden onaanvaardbaar zijn); en
   - identificatie van passende risico-beperkende maatregelen (i.e. de technische en organisatorische maatregelen die noodzakelijk zijn om het risico tot een aanvaardbaar niveau te herleiden).
3. Op maat: Een risicobeoordeling is steeds maatwerk. Een behoorlijke risicobeoordeling bestaat niet uit een eenvoudig kopiëren van eerder gevoerde analyses maar vergt een concrete inschatting op basis van de specifieke context (i.e. onder verwijzing naar de aard, het toepassingsgebied, de context en de doeleinden van de verwerking). Niets belet daarentegen dat een verwerkingsverantwoordelijke gebruik maakt van procedures of modellen die door (of te samen met) andere entiteiten werden ontwikkeld (bijv. op niveau van een bepaalde sector of bedrijfstak) bij het uitvoeren van risicobeoordeling.
4. Begrijpelijk: De uitkomst van een risicobeoordeling dient leesbaar en toegankelijk zijn voor een zo breed mogelijk publiek. De uitkomst mag niet enkel leesbaar is voor (risico)experten, technici of gespecialiseerd personeel. Beknopte samenvattingen en visuele weergaves (zoals kleurgrafiek, tabel met cijfers) kunnen de toegankelijkheid van de risicobeoordeling (zowel het proces als de schriftelijke weergave daarvan) bevorderen.
5. Voldoende genuanceerd: Een risicobeoordeling dient voldoende schalen te bevatten teneinde een genuanceerde evaluatie van geïdentificeerde risico mogelijk te maken. Het voorzien van slechts drie schalen (laag, medium en hoog) om risico's te beoordelen is onvoldoende om tot een correcte appreciatie te leiden.
6. Communicatie en consultatie: Een behoorlijk systeem van risicobeheersing betrekt diegenen die best geplaatst zijn om bij te dragen aan het proces van identificatie, analyse, evaluatie en beheersing van risico's. Tot deze groep behoort niet enkel aan de functionaris voor de gegevensbescherming en/of

veiligheidsconsulent, maar ook de ontwikkelaars van nieuwe toepassingen, zij die strategische beslissingen inzake projectontwikkeling nemen en de personeelsleden (of hun vertegenwoordigers) die gebruik zullen maken van de persoonsgegevens in kwestie bij de uitoefening van hun taken.

7. Beheer en nazicht: Er dient een gedateerde en schriftelijke rapportering van de uitgevoerde risicobeoordelingen te bestaan. Een intern gemandateerd orgaan dat beslissingen neemt (zaols directiecomité, strategisch comité of veiligheidscomité met een mandaat van de raad van bestuur) dient periodiek op de hoogte te worden gebracht van de uitkomst (of status) van het risicobeoordelingsproces. Dit gemandateerd orgaan dient de inschatting van de risico's alsook de maatregelen ter beperking van de risico's formeel goed te keuren. Het proces van risicobeoordeling mag evenwel niet herleid worden tot een louter bureaucratisch proces. De verwerkingsverantwoordelijke dient passende maatregelen te nemen om ervoor te zorgen dat het behoorlijk beheer van risico's onderdeel wordt van de "bedrijfscultuur" van de verwerkingsverantwoordelijke. Een uitgevoerde risicobeoordeling dient periodiek nagezien te worden en minstens in het geval van wijzigende omstandigheden die een wezenlijke invloed kunnen uitoefenen op een beoordeling die in het verleden werd uitgevoerd. In het kader van een goed risicobeheer wordt verwacht dat de verwerkingsverantwoordelijke minstens om de 2 jaar een nazicht inbouwt. Bovendien wordt aangeraden dat de uitkomst van het nazicht formeel ter goedkeuring van het hoogste orgaan in de organisatie van de verwerkingsverantwoordelijke wordt voorgelegd.

De methodologie voor het inschatten en beheer van risico's

Het is aan de verwerkingsverantwoordelijke om een methodologie te hanteren die hem in staat stelt om de vereisten na te leven.
Iedere verwerkingsverantwoordelijke die een risico-beoordeling onderneemt zal een methodologie hanteren die aangepast is aan de noden en context van de organisatie.

Een organisatie krijgt begrip van huidige situatie door:

- Het identificeren van de (strategische en operationele) doelstellingen, verplichtingen ten aanzien van de belanghebbenden, statutaire verplichtingen en de omgeving waarin de organisatie opereert;
- Identificeren van activiteiten, goederen en middelen, inclusief deze buiten de organisatie, die ondersteuning bieden voor leveren van deze producten en diensten.
- Identificeren en evalueren van de zichtbare bedreigingen die onderbreking kunnen veroorzaken van de processen en de kritische activiteiten, goederen en middelen die deze ondersteunen.
- Evalueren van de frequentie, de impact en bestaande controlemaatregelen.

Het is belangrijk dat de organisatie de afhankelijkheden tussen de activiteiten begrijpt, evenals elke externe afhankelijkheden, die zelfs gedeeld kan zijn met derden.

In het algemeen bestaat een goed risicobeheer uit volgende stappen:

1. Inschatten van het risico naar frequentie, impact en bestaande controlemaatregelen
2. Analyseren van het verschil tussen de huidige controlemaatregelen voor dit risico en de te bereiken controlemaatregelen voor dit risico
3. Aanvaarden van het residuele risico of het vermijden, transfereren of verminderen van het risico tot een aanvaardbaar niveau
4. Continue risico opvolging en monitoring

Waarom risico analyse?

Informatieveiligheid en privacy zullen zeer zwaar beïnvloed worden door risicobeheer, niet door kansen op bepaalde gebeurtenissen, maar door essentiële risico's die zich realiseren op basis van onverwachte gebeurtenissen. Vanuit het referentiekader rond risicobeheer, dient de strategie rond informatieveiligheid en privacy bepaald te worden aan de hand van een analyse van de belangrijke processen, informatiestromen, en vereiste infrastructuurelementen en -middelen.

Het is belangrijk dat de organisatie zich niet enkel beschermt tegen specifieke gebeurtenissen – want de organisatie kan ze onmogelijk allemaal voorzien - maar ook dat de nodige maatregelen worden geïmplementeerd om de gevolgen op de belangrijke activiteiten op te vangen ongeacht de oorzaak en de gevolgen.

Een risico analyse wordt gebruikt om kritische processen te identificeren die moeten hersteld worden na een ernstig incident of ramp. De doelstellingen van deze analyse zijn om de specifieke risico's te analyseren ten opzichte van de bestaande controlemaatregelen ontworpen om de kans van voorkomen te verminderen en de gevolgen ervan te beperken.

Risico's zijn kwetsbaarheden voor bedreigingen. Een bedreiging is een ongewenste gebeurtenis die geen waarschuwing geeft en de mogelijkheid heeft tot het veroorzaken van een schade voor de organisatie. De meeste bedreigingen reden op tijdens momenten wanneer de meeste mensen niet in de buurt zijn om te beseffen dat iets fouts zich heeft voorgedaan. De variabele voor bedreiging is de waarschijnlijkheid dat de bedreiging effectief optreedt. De variabele voor risico is de mate van kwetsbaarheid, of hoe goed controlemaatregelen de impact zal verkleinen van de bedreiging als die effectief optreedt. De variabele voor proces is de waarde van elk proces dat bedreigd wordt. Deze waarde kan objectief en meetbaar zijn, zoals de exacte vervangwaarde van een materiaal, of kan subjectief zijn, zoals de goodwill.
Een risico is het directe resultaat van een bedreiging die optreedt. Enkele voorbeelden van risico's zijn onder stroomuitval veroorzaakt door een overstroming of onderspanning, ongeautoriseerde toegang tot het centrum als gevolg van een inbraak, of verlies van gegevens als gevolg van onvoldoende back-up procedures.

Risico-analyse is een manier om systematisch de mogelijke risico's van verschillende zware incidenten of rampen te beoordelen. Gewoonlijk worden de risico's van andere type incidenten (zoals schending van de vertrouwelijkheid of integriteit van gegevens) gelijktijdig onderzocht, maar dit hoeft niet het geval zijn.
De risico-analyse is bedoeld om de mate van het potentiële verlies (en andere ongewenste effecten), die zouden kunnen optreden te helpen begrijpen. Het gaat daarbij niet alleen om directe financiële schade, maar veel andere kwesties, zoals het verlies van vertrouwen van de eindgebruiker, reputatieschade, regulerende effecten, enz.

Zouden volgende gebeurtenissen voor de organisatie als een ernstig incident of ramp bestempeld worden:

- Continue systeem onderbrekingen
- Mislukte upgrades van computers, systemen of software
- Desastreuze programmatiefouten
- Verlies van een productievestiging, van een kantoor of ander lokale vestiging
- Mislukte opstart van een nieuwe dienstverlening aan eindgebruikers omdat deze niet blijkt te werken of er onvoldoende capaciteit is om te voldoen aan de vraag
- Een hoofdleveranciers wordt getroffen door een ernstig incident of ramp
- Eén van de essentiële werknemers komt om in een verkeersongeval

In sommige gevallen kan de organisatie besluiten om enkel plannen te maken voor grootschalige, niet-specifieke incidenten of rampen: in dat geval is het raadzaam om niet te veel tijd besteden aan het analyseren van wat deze niet-specifieke gebeurtenissen kunnen zijn. Tegelijkertijd kan het begrijpen en het vermijden van kleinere risico's van onschatbare waarde zijn om te voorkomen dat kleinere gebeurtenissen zoals een stroomuitval plots een veel grotere impact hebben dan voorzien, bijvoorbeeld door het gebruik van noodgeneratoren.

Bepalen van relevante risico scenario's

Identificeer de specifieke risico's die te maken hebben met (on)beschikbaarheid van processen van de organisatie. Mogelijke risicofenomenen moeten gecategoriseerd worden, zoals bijvoorbeeld:

- Natuurgerelateerd - zoals overstroming, bliksem, windhoos;
- Organisatiegerelateerd – zoals brand, afval, evacuatie, blokkade;
- Geopolitiek gerelateerd - zoals spionage, oorlog, terrorisme, machtsvacuüm;
- Werknemersgerelateerd – zoals staking, vervoersproblemen, fraude, sabotage, fouten;
- Technologie gerelateerd - zoals hacking, virussen, softwarefout of IT panne;
- Leverancier gerelateerd - zoals faillissement, panne, sabotage of vijandige overname;
- Gezondheid gerelateerd - zoals een griep epidemie, kanker;

- Productie gerelateerd – zoals materiaalpanne, voorraadtekort, kwaliteitsprobleem, certificatieprobleem.

Om te vermijden dat de organisatie enkel symptomen analyseert, oppervlakkig te werk gaat, of enkel het evidente bekijkt, is een eenvoudig maar volledig referentiekader onontbeerlijk. Het meest gebruikte risicomodel omvat drie belangrijke risico domeinen:

- Omgevingsrisico (ook wel externe risico's genoemd), dat inhoudt dat bedreigingen in de industrieomgeving of het politieke, financiële of economische klimaat, ofwel de organisatie buiten werking stellen ofwel de grondbeginselen van het bestaan van de organisatie met haar objectieven en strategieën significant veranderen ;
- Procesrisico (ook wel interne risico's genoemd), wat inhoudt dat de processen niet duidelijk gedefinieerd zijn of niet optimaal afgestemd zijn op de strategie. Of zijn ze niet doeltreffend noch efficiënt in het voldoen aan behoeften van eindgebruikers, creëren ze geen waarde of stellen ze de financiële, fysieke en intellectuele activa bloot aan onaanvaardbare verliezen, verduistering of wangebruik ;
- Risico bij informatie voor beslissingsneming (ook wel directie risico's genoemd), wat inhoudt dat informatie die gebruikt wordt om strategische, operationele en financiële beslissingen te ondersteunen, niet relevant of betrouwbaar is. Veel beslissingen worden genomen op basis van indicatoren van performantie of resultaten van industriële of financiële analyses. Als maatregelen niet afgestemd zijn op de strategie of niet realistisch, verstaanbaar en opvolgbaar blijken, concentreert de organisatie zich niet op de juiste problemen en voorziet het systeem stimuli voor beslissingen die inconsistent zijn met de strategie. Indien de informatie gebruikt voor beslissingsname niet betrouwbaar of relevant is, dan zal ze ofwel genegeerd worden ofwel leiden tot ongewenste maatregelen of gedrag.

Elk van deze drie gebieden is eng verbonden met elkaar waardoor ze de basis vormen voor classificatie en voorstelling van de aanwezige risico's binnen de markt en de organisatie. Dit model laat organisaties toe om een breed gamma aan risico's die in hun gebeuren aanwezig zijn te beschouwen en te analyseren.
De risico analyse voor alle locaties moet zich altijd primair richten op de gezondheid en de veiligheid van de werknemers, de veiligheid en mogelijke gevolgen voor het milieu om ervoor te zorgen dat de functies de middelen hebben die ze nodig hebben om succesvol te zijn.

De vijf meest weerkerende zware incident/ramp scenario's zijn:

- Onbeschikbaarheid van belangrijk gebouw / fysieke infrastructuur
- Onbeschikbaarheid van belangrijke werknemers
- Onbeschikbaarheid van belangrijke ICT infrastructuur
- Onbeschikbaarheid van belangrijke externe leverancier
- Onbeschikbaarheid of uitlekken van belangrijke informatie

Bepalen van inherente risico

Naast elk risicogebeurtenis, moet de waarschijnlijkheid en mogelijke frequentie van haar optreden beoordeeld worden. Onverwachte gebeurtenissen komen in alle "soorten en gewichten". Zelfs kleine, schijnbare onschuldige incidenten kunnen een zeer zware impact hebben. Of zeer spectaculaire rampen kunnen een zeer beperkte impact hebben. Voor sommige situaties (zoals overstromingen of burgerlijke onrust), kan informatie over de frequentie en waarschijnlijkheid worden gevonden door contact op te nemen met de overheid of de politie. Het is altijd beter te starten met een afhankelijkheids- en kwetsbaarheidsanalyse vanuit de kritische processen.

1. Waarschijnlijkheidsanalyse
In deze fase wordt de waarschijnlijkheid, kans of frequentie van een ernstig incident of ramp geïdentificeerd en dit op een kwantitatieve manier. Het gaat hier over een tijdsdimensie waarbij een antwoord wordt gegeven op de vraag : "hoeveel keer komt dergelijk ernstig incident of ramp voor bij een dergelijk scenario?"
De waarschijnlijkheid waarmee een ernstig incident of ramp kan gebeuren is af te leiden uit diverse bronnen.
De waarschijnlijkheid dient te worden gemeten in de tijd. Hoeveel minuten/uren/dagen/weken/maanden na een ernstig incident of ramp zullen de gevolgen zichtbaar worden? Hoeveel dagen heeft men nodig voordat de werking van de organisatie terugkeert naar 75 % functionaliteit, wat betekent dat 75 % van de mensen, middelen en processen terug werken. Hoeveel dagen duurt het voordat de organisatie de verloren middelen kan vervangen, zoals het huren van een nieuw gebouw of het gebouw functioneel maken na een brand. Men moet beslissen over een redelijke

maximale tijd van uitval die men wenst te meten, en vervolgens de impact per interval beoordelen vanaf het punt van impact tot de maximale impact. Bijvoorbeeld, na 10 minuten, 1 uur, 4 uur, 12 uur, 1 dag, 1 week, 1 maand, 3 maanden.

2. Impact analyse

In deze fase wordt de gevolgen na een ernstig incident of ramp geïdentificeerd en dit op een kwantitatieve en kwalitatieve manier. Op basis van deze stap worden dan de meest relevante functies met hun herstel prioriteiten en onderlinge afhankelijkheden uitgewerkt zodat de gestelde hersteldoelstellingen kunnen gehaald worden.
De analyse van de impact is de belangrijkste stap. Het houdt de beoordeling van de impact van een bepaald scenario op een activiteit (in de tijd). Het scenario kan specifiek zijn, zoals het optreden van inherente risico's (risico's zonder controlemaatregelen) of generiek, zoals verlies van toegang tot een locatie. De impact analyse moet worden uitgevoerd op basis van de risico-analyse die de meest relevante risico's heeft geïdentificeerd die de organisatie ernstig zou kunnen verstoren. Kortom, een impact analyse is een gestructureerd proces waarbij deorganisatie de impact gaat bepalen en documenteren van een onderbreking van proces ondersteunende activiteiten. Een impact analyse zal de organisatie de volgende resultaten moeten bieden:

- het identificeren van tijdgevoelige kritische processen
- het analyseren van de financiële en operationele gevolgen voor de organisatie
- het inschatten van de termijnen waarin de tijdgevoelige operaties, processen en functies hervat moeten worden
- het inschatting van middelen nodig voor een succesvolle hervatting en herstel.

De bedoeling is na te gaan hoe groot de gevolgen zouden zijn van een ernstig incident of ramp op de organisatie. Dit laat de organisatie toe om prioriteiten toe te kennen aan investeringen om de paraatheid / beschikbaarheid te verbeteren of te verzekeren, maatregelen te coördineren en plannen te implementeren voor als het fout gaat bij kritische systemen en de organisatie de impact van een ernstig incident of ramp wil beperken.
Aan de ene kant gaat de organisatie daarbij kijken naar kwantificeerbare factoren zoals inkomensverlies, boetes, interestverlies enz. Aan de andere kant gaat de organisatie ook kijken naar meer indirecte domeinen van impact, zoals eindgebruikersverlies, imagoverlies, verlies van vertrouwen en zo meer. Typisch gaat de organisatie daarbij na wat de gevolgen zijn op de activiteiten van een onbeschikbaarheid met verschillende tijdsduren, zoals een halve dag, een dag, een week of een maand. Daaruit leidt de organisatie dan de maximale duur van onbeschikbaarheid af ("maximum downtime") van de kritische toepassingen en IT waarop ze draaien. Aan de hand daarvan gaat de organisatie dan bepalen welke alternatieve oplossingen de meest aangewezen zijn.
De aanpak houdt in dat men eerst elk departement moet opdelen in functionele processen en in kritieke activiteiten. Als deze taak op zich ingewikkeld is, dan kan jet de moeite waard zijn om een Business Process Analyse uit te voeren vooraleer met deze fase te starten. Voor elk functioneel proces zal de persoon aangeduid door het centrale programma-team de nodige achtergrondinformatie over hun omgeving moeten aanleveren, zoals het procesbeschrijvingen en de verantwoordelijke directeur.
Processen mogen apart worden behandeld indien ze verschillende werknemers (bijvoorbeeld rollen), dienstverleners (bijvoorbeeld outsourcing) of middelen (bijvoorbeeld IT-systemen) hebben.
Vervolgens moet de impact van een incident op elk proces worden gemeten. Een andere analyse kan worden uitgevoerd om de impact van elke potentiële bedreiging voor de organisatie te beoordelen, maar het kan net zo inzichtelijk (en veel minder tijdrovend) zijn om een "worst case scenario" van totaal verlies van toegang tot faciliteiten, technologie en mensen te beoordelen.
Bij het evalueren van de impact moet men de effecten die er zijn op het behalen van de doelstellingen of de effecten voor de belanghebbenden mee in rekening brengen. De mogelijke gevolgen (secundaire impact) zijn:

Externe omgeving

- niet of niet tijdig behalen van de doelstellingen
- schade aan relaties
- verzwakte beslissingen/uitvoering
- schade aan het milieu
- schade aan reputatie/imago

Planning, processen en systemen

- schade aan, of verlies van, middelen, faciliteiten, technologie of informatie
- schade aan financiële levensvatbaarheid, onvoorziene kosten, boetes, budget overschrijdingen
- fraude of onregelmatigheden

- achteruitgang van de kwaliteit van producten of diensten

Mensen

- gezondheid en veiligheid – impact op werknemers en algemeen welzijn
- verlies van moraal/productiviteit van werknemers

Wettelijke aspecten en regelgeving

- impact van schendingen van wettelijke plichten en of regelgevingen
- schadeclaims, boetes en wettelijke aansprakelijkheid

Hieronder volgen voorbeelden van technologie geïnspireerde risicothema's met hun potentiële impact:

Risico thema	Impact	Overweging voor de directie
Mobile toestellen	• Meer mobiele toestellen op de werkvloer • Grotere afhankelijkheid van technologie om productief te blijven • Meer toegang aan processen en werkstromen van buiten de organisatie • Directere snellere rapportering van gebeurtenissen • Meer mobiele toestellen die niet zijn goedgekeurd door de organisatie (Bring Your Own Device of BYOD) meegebracht door werknemers of leveranciers met toegang tot informatie.	• Mobiele toestellen moeten opgenomen worden in de plan voor ondersteuning aan belangrijke functies binnen de organisatie • Mobiele toestellen die gebruikt worden moeten regelmatig onderhouden en verbeterd worden • In de opleiding moet ook de rol van mobiele toestellen besproken worden • In de plannen moet men de aanwezigheid van mobiele toestellen voor communicatie toelichten zoals sms, sociale netwerken, berichten, enzovoort • In de contracten met de telecommunicatie leveranciers moeten ook de vereisten zitten in verband met verlies, diefstal of vernietiging van mobiele toestellen en hoe (snel) deze vervangen worden
Sociale netwerken	• Zeer snelle publicatie en verspreiding van gebeurtenissen via sociale netwerken • Goedkoop medium om berichten te verspreiden	• De aanpak moet een specifiek beleid en richtlijnen omvatten rond het gebruik van sociale media tijdens crisis situaties, met inbegrip van de lijst van erkende woordvoerders voor de organisatie • Enkel specifiek aangeduide personen mogen berichten of status doorgeven op sociale media voor de organisatie • Tijdens de opleiding en oefeningen worden ook simulaties gedaan van gebruik van sociale media
Server virtualisatie	• Lagere afhankelijkheid van fysieke systemen om de IT infrastructuur te ondersteunen • Minder personen nodig voor het ondersteunen van virtuele omgevingen • Meer gecentraliseerd serverbeheer • Minder impact bij onderhoudsactiviteiten	• Strikt bijhouden van de virtuele omgevingen in de organisatie om deze te kunnen opsommen voor plannen • Virtuele omgevingen moeten geoefend worden naar zwakheden. • Virtuele omgevingen meenemen tijdens oefeningen • Nadenken over virtuele herstel omgevingen die permanent actief staan
Desktop virtualisatie	• Uitbreiden van werklocatie naar locaties buiten de organisatie • Sneller uitrollen van nieuwe desktop omgeving • Gecentraliseerd desktopbeheer • Afhankelijk van internet en telecommunicatie	• Virtuele desktop kan gebruikt worden voor de tijdelijke omgeving bij activatie van de plan • Relevante oplossing voor de belangrijke functies in de organisatie • Beveiliging van de virtuele desktop moet regelmatig gecontroleerd en verbeterd worden
Cloud computing	• Grotere afhankelijkheid van externe dienstenleveranciers (en hun herstel plannen) • Minder directe controle over eigen IT processen en infrastructuur • Betere flexibiliteit en snellere manier om toepassingen en informatie te verschuiven tussen verschillende infrastructuren	• Risico analyse nodig vooraleer u naar cloud oplossingen migreert • Vereisten in contracten duidelijk vastleggen en oefenen • Regelmatig oefeningen uitvoeren met de hulp van de cloud service provider • Data recuperatie oefeningen vanuit de cloud

Risico thema	Impact	Overweging voor de directie
	• Betere capaciteitsplanning mogelijkheden dankzij grotere flexibiliteit • Enkel betalen voor wat u gebruikt	service provider (snelheid en volledigheid) • Zorgen voor eigen data backup ongeacht de data backup oplossing van de cloud service provider • Regelmatig de status van de cloud service provider nagaan (financieel, reputatie, evoluties, nieuwe diensten, enz.) • Eigen data beveiliging inbouwen in de cloud oplossing zowel in productie als backup omgeving (encryptie) • Cloud overwegen voor simuleren van grote IT infrastructuur problemen en voor grote herstel oefeningen.

Niveau van impact inschatten. Bij het meten van financiële gevolgen, moet de omvang van de mogelijke schade zo goed mogelijk worden gekwantificeerd. Aangezien dit een hypothetische oefening is, kan het moeilijk zijn om uit te voeren, maar het is een basis voor een solide business case. Reputatieschade kan worden gekwantificeerd indien er voorbeelden uit het verleden of van andere eindgebruikers bestaan. In geval van niet-kwantificeerbare impact kan een schaal van, bijvoorbeeld, 1 tot 5, worden opgesteld en vastgelegd voor de deelnemers om de impact in te schatten, waarbij 5 staat voor een hoge impact en 1 voor een verwaarloosbare impact. (Een andere schaal kan hier worden gebruikt, afhankelijk van het niveau van vereiste granulariteit.) Kwantitatieve impact analyse gaat over het toewijzen van waarschijnlijkheden en een monetaire waarde aan potentiële verliezen. Kwalitatieve impact analyse kan meer effectief zijn om de gevolgen van de risico's en potentiële kwetsbaarheden te beschrijven. De impact van het realiseren van een risico moet dan worden vastgesteld om te begrijpen wat de mate van verstoring is die het zou kunnen veroorzaken en dus de urgentie waarmee het moet worden vermeden of ingepland. In dit stadium moet teveel detail vermeden worden en moeten de impact en de waarschijnlijkheid eenvoudig beoordeeld worden op een schaal van 1 tot 5 bijvoorbeeld, waarbij een overstroming score 5 heeft voor impact maar score 1 heeft voor waarschijnlijkheid, waardoor de totale risicoscore 6 is (indien men beide scores zou optellen). Op eenzelfde manier kan een grote netwerkpanne score 4 krijgen voor impact en score 3 krijgen voor de waarschijnlijkheid, waardoor een totale score van 7 wordt bekomen. Men kan bijvoorbeeld beslissen om alleen te werken aan de risico's die hoger dan 5 scoren. Voor zover middelen belangrijk of zelfs essentieel zijn voor de organisatie, heeft dit dus gevolgen voor de kritische processen en creëert een ernstig incident of ramp een significante impact.
Indicatoren van belangrijkheid zijn:

- Het proces ondersteunt het leven of van mensen de gezondheid en veiligheid.
- Het proces is nodig omwille van wettelijke of statutaire vereisten.
- Verstoring van het proces beïnvloedt direct en duidelijk de resultaten van de organisatie.
- Er is een heel duidelijke impact op reputatie en imago.

De methode voor het meten van de impact moet duidelijk worden uitgelegd en de antwoorden moeten worden uitgedaagd om consistente, accurate en grondige antwoorden te garanderen. De potentiële impact kan geklasseerd worden: bijvoorbeeld als “Kritiek, Hoog, Gemiddeld, Laag, Zeer Laag”. Er zijn meerdere criteria mogelijk om impact te bepalen. Het is dus niet zo dat er enkel sprake kan zijn van een financiële impact. Er zijn ook gevolgen op menselijk vlak, veiligheidsvlak, kwaliteitsvlak en management vlak. Het belangrijkste is dat dergelijk schema overal gelijk is in de organisatie op een gegeven moment. Op basis van praktijk ervaring kan dergelijk schema verfijnd en aangepast worden, mits het overal hetzelfde is in de organisatie.
Het is inderdaad belangrijk om relevante gebeurtenissen zowel intern als extern te duiden die een potentieel negatieve impact kunnen hebben op de organisatie en op de dienstverlening naar de eindgebruikers van de organisatie. Het is inderdaad belangrijk om keuzes te kunnen maken en prioriteiten te zetten en dit op een zo objectieve manier als mogelijk. Het is ook van belang dat hierbij de medewerking wordt gevraagd en verkregen van de relevante betrokken partijen.
De resultaten van deze oefening zal toelaten om de domeinen voor herstel te prioriteren, afhankelijk van de tijd waarin zij zouden moeten worden hersteld en het potentiële verlies voor de organisatie als dit niet lukt. Er zijn een aantal manieren om informatie te verzamelen en de business impact analyse uit te voeren: geautomatiseerde tool, e-mail vragenlijst, papieren enquête, face-to-face interview, workshops, enz. Men kan gebruik maken van interviews en vooraf opgemaakte vragenlijsten om de sleutelpersonen en belanghebbenden te bevragen. Sommige mensen hebben

de neiging om het belang van hun eigen afdeling voor de organisatie als geheel te overschatten, terwijl anderen hun waarde volledig onderschatten en bijna als verwaarloosbaar voorstellen.
Het is belangrijk dat individuen die bijdragen aan de impact analyse beschikken over nauwkeurige en realistische gegevens, omdat de gegevens uit deze fase in alle volgende fases van het programma zullen gebruikt worden om beslissingen te nemen en de planning te verfijnen.
Tenslotte nog opmerken dat degene die de informatie over de gevolgen van ernstige incidenten of rampen verzamelt cruciaal is voor het identificeren van de resultaten en de beslissingen van de directie.

Bepalen van het residuele risico

Analyseer de kwetsbaarheden door te kijken naar de reeds aanwezige controlemaatregelen om de geïdentificeerde risicofenomenen tegen te gaan. Risico-beperkende controlemaatregelen omvatten beveiliging en omgevingscontroles, de veiligheid en noodprocedures, data back-up en recovery procedures en personeelspraktijken. Als er geen controlemaatregelen bestaan om de waarschijnlijkheid of impact van een bepaald risico te verminderen, dan zullen deze moeten ontwikkeld en geïmplementeerd worden. Uiteindelijk zullen er een aantal risico's overblijven die niet voorkomen kunnen worden (zoals terreur aanslagen en natuurrampen). Deze kunnen alleen beperkt worden door de ontwikkeling van specifieke regelingen.
Controlemaatregelen kunnen de kans van bedreigingen verminderen, zoals het verwijderen van brandbare producten; of kunnen de gevolgen verminderen, zoals brandalarm en sprinklers de schade van een brand kunnen verminderen.

Het elimineren of verminderen van de gevolgen van mogelijke bedreigingen gebeuren door het nemen van de juiste controlemaatregelen, procedures en praktijken vooraleer de zware incidenten of rampen plaatsvinden. De risico beoordeling richt zich op het identificeren van potentiële bedreigingen en bestaande controlemaatregelen en kan leiden tot aanbevelingen voor verbetering. Het doel van deze activiteit is om ofwel de kans te verminderen op een potentiële bedreiging of de impact ervan te verkleinen indien een ernstig incident of ramp zich zou voordoen.
Typisch gaat de organisatie controlemaatregelen voorzien voor de meest essentiële infrastructuurelementen, met als gedachte dat hiermee het belangrijkste er dan toch al is en dat voor de rest er wel een oplossing zal komen. Hierbij dient de organisatie zich de vraag te stellen of het met deze oplossing de kritische informatiestromen kan hernemen.
Daarenboven zijn deze infrastructuurgerichte oplossingen relatief duur, aangezien ze niets "opleveren" zolang er geen ernstig incident of ramp is. Het blijkt doorgaans moeilijk te zijn om de kost ervan te justifiëren, wat een reden te meer geeft om zich te beperken tot de echt essentiële elementen. Tevens kan de organisatie zich de vraag stellen of met deze controlemaatregelen de doelstellingen verwezenlijkt worden. In de realiteit merken we zelfs dat doelstellingen niet eenduidig vooropgezet worden. Als het objectief is de IT toepassingen te kunnen herstarten, dan wordt dit (hopelijk) wel gehaald. Als het objectief is de continuïteit in dienstverlening te verzekeren, dan is het minder duidelijk of deze doelstelling wel gehaald zal worden wanneer de organisatie zich concentreert op de infrastructuurelementen.

Risico-matrix

Op basis van de drie vorige activiteiten moet men in staat zijn om een (residuele) risico matrix te maken die de risico's identificeert, tesamen met hun waarschijnlijkheid en impact, de bestaande controlemaatregelen.
Het waarschijnlijkheid, de impact en de controlemaatregelen voor risico's die kunnen leiden tot zware incidenten of rampen moeten geëvalueerd worden op basis van de huidige stand van zaken.
Deze analyse wordt gebruikt op dezelfde manier om de directie te informeren over welke processen of diensten het eerst of op het laatst kunnen worden gestopt wanneer de activiteit overbelast geraakt of herstelt van een ernstig incident of ramp.
De risico analyse geeft aan de directie de broodnodige informatie die hen helpt om het belang van de voorgestelde alternatieve aanpak te evalueren. Het uitvoeren van de analyse tijdens simulatie oefeningen (ter voorbereiding van incidenten of rampen) helpt om de mogelijke impact correcter te identificeren en zorgt voor de nodige goedkeuring voor de algemene resultaten en beperkende controlemaatregelen.
Er zijn duidelijke verbanden tussen risico-analyse en evaluatie, evenals risicobeheer binnen de organisatie. Een juiste analyse van de business impact kan managers helpen om weloverwogen keuzes te maken en de impact te verminderen van een scala van problemen, van kleine evenementen tot grote rampen. Het is pas op het moment dat de risico matrix gemaakt is, dat de stuurgroep 1 van de 4 beslissingsopties kan/moet maken per risico.

- Beslissingsoptie 1 : Delen van het risico

  Het risico wordt deels overgedragen aan (getransfereerd naar)een derde partij. Dit kan gebeuren door de gewone verzekering of door contractuele afspraken met een gespecialiseerde leverancier, of het kan

gebeuren door een derde partij te betalen om het risico op te nemen op een andere manier. Alhoewel een juiste verzekering de financiële impact van een ernstig incident of ramp heel wat kan verzachten, kan een verzekering er nooit voor zorgen dat de processen van de organisatie snel hernomen worden.

- Beslissingsoptie 2: Vermijden van het risico

  In sommige omstandigheden is het aan te raden om de dienst, product, activiteit, functie of proces aan te passen, uit te stellen of af te sluiten. Deze optie kan worden overwogen wanneer er geen conflicten zijn met de doelstellingen, (statutaire) verplichtingen en verwachtingen van de belanghebbenden. Deze optie zal waarschijnlijk worden overwogen wanneer een dienst, product, activiteit, functie of proces een beperkte levensverwachting heeft.

- Beslissingsoptie 3: Beperken van het risico

  Deze optie wordt gebruikt voor het beperken van financiële risico's of risico's bij goederen. Het risico wordt overgedragen om de risicoblootstelling van de organisatie te verminderen of omdat een andere organisatie meer bekwaam is in het effectief beheren van het risico.

- Beslissingsoptie 4: Aanvaarden van het risico

  Het risico wordt aanvaard zonder dat er verdere actie wordt ondernomen. Indien de organisatie kiest een risico te aanvaarden, dient de organisatie te weten dat daarmee ook de mogelijke gevolgen van voorkomen op zich neemt. Een organisatie zal, voor die risico's van een ernstig incident of ramp die een kritisch risico zouden realiseren, zelden beslissen het risico zomaar te aanvaarden. Zelfs als deze niet aanvaardbaar is, kan het vermogen om iets te doen aan het risico beperkt zijn of kan de kost voor het ondernemen van acties onevenredig zijn met de potentiële voordelen (kosten-batenafweging). In deze gevallen kan het huidige risico niveau volstaan binnen de risico comfortzone (aanvaardbaar residueel risico rekening houdend met de risico appetijt) van de organisatie. Deze optie kan aangevuld worden met een plan om de impact op te vangen als het risico zich effectief realiseert. Welke strategie de beste is om het risico op te vangen, is het onderwerp van de verdere analyse.

Finale tips rond risicobeheer

- Zorg voor zichtbare steun van de directie: zonder hen lukt het nooit
- Zorg dat de directie en de risicocoördinator zeer goed met elkaar samenwerken: gemeenschappelijke schalen en evaluatiecriteria zorgen voor een betere en snellere assimilatie in de organisatie
- Kijk niet enkel naar de financiële schade/gevolgen, maar ook naar de reputatieschade en hoeveel middelen het zal vergen om die schade op te lossen
- Kijk niet enkel naar de eigen organisatie, maar ook naar de besluiten rond risicobeoordeling van collega's, leveranciers, partners, enz.: deel kennis op een wederzijdse manier
- Besef dat de directie bepaalde risico's zal aanvaarden: dat is nu eenmaal hun privilege en mandaat: beslissen om alles (voorlopig) te laten zoals het is.
- Gebruik slechts 3 vragen om te peilen naar het verschillende risico's : kans, impact en huidige controle status.
- Gebruik altijd een duidelijke tijdslimiet voor de risico analyse fase: anders blijft men bezig
- Zorg voor een duidelijke definitie van "slechtste scenario" ("worst case scenario") zodat iedereen hetzelfde begrijpt.
- Besteed enkel die zaken uit aan externe partners die men begrijpt en waarbij men kennis heeft van het plan van de gekozen externe partners.

Bijlage D: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

ISO-norm 27002:2013	
Veiligheidsbeleid	**Ja**
Organisatie van de informatieveiligheid.	
Veilig personeel	
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	
Fysieke beveiliging en beveiliging van de omgeving	
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	**Ja**

***** EINDE VAN DIT DOCUMENT *****