****

**${DOCUMENT}**

**${COMPANY}**

**Informatiebeveiliging -**

**MONARC**

**Algemene informatie**

Versie: ${VERSION}

Staat document: ${STATE}

Classificatie: ${CLASSIFICATION}

Vennootschap: ${COMPANY}

Documentnaam: ${DOCUMENT}

Datum: ${DATE}

Veiligheidsconsulent(en): ${SMILE}

Vertegenwoordiger(s) klant: ${CLIENT}

**Samenvatting**

${SUMMARY\_EVAL\_RISK}

**Kaart van de actuele risico's**

${CURRENT\_RISK\_MAP}

**Kaart van de restrisico's**

${TARGET\_RISK\_MAP}

Inhoudsopgave

[1 Inleiding 4](#_Toc102395738)

[1.1 Context van de risicoanalyse 4](#_Toc102395739)

[1.2 Doelstellingen van het document 4](#_Toc102395740)

[1.3 Referenties 4](#_Toc102395741)

[1.4 Afkortingen/glossarium 4](#_Toc102395742)

[1.5 Beschrijving van de "Geoptimaliseerde methode voor risicoanalyse CASES" (MONARC) 5](#_Toc102395743)

[2 Bepaling van de context 7](#_Toc102395744)

[2.1 Omschrijving van de context 7](#_Toc102395745)

[2.2 Definitie van de risicobeoordelingscriteria 7](#_Toc102395746)

[2.2.1 Informatierisico's 7](#_Toc102395747)

[2.2.1.1 Impactschaal 7](#_Toc102395748)

[2.2.1.2 Dreigingsschalen 7](#_Toc102395749)

[2.2.1.3 Kwetsbaarheidsschalen 7](#_Toc102395750)

[2.2.1.4 Acceptatiedrempels voor de risico's 8](#_Toc102395751)

[2.2.2 Operationele risico’s 8](#_Toc102395752)

[2.2.2.1 Impactschaal 8](#_Toc102395753)

[2.2.2.2 Waarschijnlijkheidsschaal 8](#_Toc102395754)

[2.2.2.3 Acceptatiedrempels voor de risico's 8](#_Toc102395755)

[2.3 Evaluatie van de trends en de dreigingen 9](#_Toc102395756)

[3 Modellering van de context 10](#_Toc102395757)

[3.1 Identificatie van de activa 10](#_Toc102395758)

[3.2 Identificatie van de kwetsbaarheden 10](#_Toc102395759)

[3.3 Beoordeling van de gevolgen 10](#_Toc102395760)

[4 Evaluatie en behandeling van de risico's 11](#_Toc102395761)

[4.1 Samenvatting van de risicobeoordeling 11](#_Toc102395762)

[4.1.1 Information risks 11](#_Toc102395763)

[4.1.2 Operational risks 11](#_Toc102395764)

[4.2 Behandeling van de risico's 12](#_Toc102395765)

[4.2.1 Soort behandeling 12](#_Toc102395766)

[4.2.2 Risicobehandelingsplan 12](#_Toc102395767)

[Bijlage A: Interview en informatieverzameling 13](#_Toc102395768)

[Bijlage B: Evaluatie van de trends 14](#_Toc102395769)

[Bijlage C: Evaluatie van de dreigingen 15](#_Toc102395770)

[Bijlage D: Activa context 16](#_Toc102395771)

[Bijlage E: Risico-eigenaars 17](#_Toc102395772)

[Bijlage F: Aantekeningen en opmerkingen van de consultant 18](#_Toc102395773)

[Informatierisico's 18](#_Toc102395774)

[Operationele risico's 19](#_Toc102395775)

# Inleiding

## Context van de risicoanalyse

${CONTEXT\_ANA\_RISK}

## Doelstellingen van het document

Dit document bevat een samenvatting van de methodologie en de resultaten van de risicoanalyse uitgevoerd met MONARC in de omgeving van de klant. MONARC valt onder de internationale ISO-27005:2011-norm.

De aldus verkregen resultaten hebben tot doel de belangrijkste risico's te identificeren, het bestaande beveiligingsniveau in acht te nemen en aanbevelingen te doen voor het invoeren van veiligheidsmaatregelen. De partijen begrijpen dat deze aanbevelingen noch exclusief, noch exhaustief zijn.

De lijst van gedetecteerde risico's is gebaseerd op informatie die door de klant en/of zijn vertegenwoordigers is verstrekt zonder dat naar bewijzen is gezocht. De analyse die het resultaat is van deze beoordeling mag Luxembourg House of Cybersecurity niet binden voor omissies of fouten die aan een betrokken persoon of derden te wijten zijn.

## Referenties

1. ISO/IEC 27005 (2011), beheer van risico's in verband met de informatieveiligheid.
2. <https://www.iso.org/standard/56742.html>. De ISO-27005-norm legt in detail uit hoe risico's moeten worden beoordeeld en behandeld in het kader van de informatieveiligheid.

## Afkortingen/glossarium

**Activa:** Elk element dat waarde heeft voor de onderneming.

**Vertrouwelijkheid**: Informatie die niet beschikbaar is voor of verspreid mag worden onder niet-gemachtigde individuen, entiteiten of processen.

**Beschikbaarheid**: Toegankelijk en bruikbaar zijn op verzoek van een gemachtigde entiteit.

**Integriteit:** Behouden van de juistheid en volledigheid van een goed.

**MONARC**: Geoptimaliseerde methode voor risicoanalyse CASES.

## Beschrijving van de "Geoptimaliseerde methode voor risicoanalyse CASES" (MONARC)

De risicoanalysemethode MONARC bestaat uit vier fasen:



Meer bepaald:



MONARC vereenvoudigt het risicobeheer door een oplossing voor te stellen voor risicobeheer, en zelfs informatiebeveiligingsgovernance, gebaseerd op de state of the art in het domein. Het maakt het mogelijk om in korte tijd een analyse uit te voeren vanuit bestaande en personaliseerbare modellen, en tegelijk te voldoen aan de internationale ISO/IEC-27005:2011-norm.

MONARC is gebaseerd op een bibliotheek van risicomodellen die objecten voorstellen die bestaan uit risicoscenario's per activa of groepen activa. Deze aanpak vereenvoudigt het beheer van de meest voorkomende risico's en verhoogt de objectiviteit en efficiëntie. Aangezien MONARC volledig iteratief is, kunnen deze resultaten worden uitgediept en aangepast aan de maturiteit van elke organisatie door de granulariteit van de risicoscenario's te verhogen.

**Bepaling van de context**

Deze eerste stap is bedoeld om de context, het belang en de prioriteiten in kaart te brengen die eigen zijn aan de onderneming of organisatie die haar risico's wil analyseren.

Het doel is om onder meer de kernactiviteiten en de kritieke processen van de onderneming te identificeren om de risicoanalyse te richten op de belangrijkste elementen. Hiervoor wordt een kick-offmeeting georganiseerd met de leden van het management en de sleutelpersonen. Het doel is om te weten wat de onderneming ten goede komt en wat ze zou kunnen schaden, alsook om de sleutelprocessen, de interne en externe dreigingen en de organisatorische, technische en menselijke kwetsbaarheden te identificeren.

**Modellering van de context**

Deze fase omvat de modellering van de boomstructuur. De activa werden in de vorige fase gedefinieerd. Ze moeten nu gedetailleerd en geformaliseerd worden in een schema dat de onderlinge afhankelijkheid weergeeft.

De impact wordt gedefinieerd op het niveau van de primaire activa (diensten of informatie). De secundaire activa erven de impact van het primaire actief waaraan ze zijn verbonden (boomstructuur).

De effecten op het niveau van de secundaire activa kunnen handmatig worden gewijzigd.

**Evaluatie en behandeling van de risico's**

De evaluatie bestaat uit het kwantificeren van de dreigingen, de kwetsbaarheden en de effecten om de risico's te berekenen.

Daartoe is het noodzakelijk te beschikken over kwaliteitsvolle informatie over de exacte waarschijnlijkheid van dreigingen, het gemak waarmee kwetsbaarheden kunnen worden uitgebuit en potentiële effecten... Vandaar het belang om te vertrouwen op meeteenheden die door deskundigen zijn gevalideerd.

Wanneer uit de risicobeoordeling blijkt dat het risico groter is dan het aanvaardbare niveau (risicoaanvaardingsschema), moeten risicomanagementmaatregelen worden genomen om het risico tot een aanvaardbaar niveau te reduceren.

**Implementering en toezicht**

Zodra de eerste behandeling van de risico's is uitgevoerd, is het noodzakelijk om een fase van continu beveiligingsbeheer in te gaan, met terugkerend toezicht en controle van de beveiligingsmaatregelen, om deze duurzaam te kunnen verbeteren.

Deze vierde fase maakt het ook mogelijk om de veiligheid continu te optimaliseren door de granulariteit van de gebruikte objecten te verhogen door de reikwijdte van de risicoanalyse uit te breiden.

# Bepaling van de context

## Omschrijving van de context

${CONTEXT\_GEST\_RISK}

## Definitie van de risicobeoordelingscriteria

### Informatierisico's

### Impactschaal

De onderstaande tabel geeft de omvang van de impact en de gevolgen weer die een risico voor de onderneming kan hebben. 0 betekent geen impact, dus geen risico.

${SCALE\_IMPACT}

### Dreigingsschalen

De onderstaande tabel geeft de waarschijnlijkheidsschaal voor het optreden van een dreiging weer.

${SCALE\_THREAT}

### Kwetsbaarheidsschalen

De onderstaande tabel geeft de kwetsbaarheidsschaal van het actief weer. Bij het kwalificeren van de kwetsbaarheid wordt rekening gehouden met de geldende veiligheidsmaatregelen.

${SCALE\_VULN}

### Acceptatiedrempels voor de risico's

De onderstaande tabel geeft de berekening van de risico's weer. De kleuren dienen uitsluitend ter indicatie en moeten worden aanvaard en/of gewijzigd door de Raad van Bestuur / het Directiecomité.

Rood: Onaanvaardbaar risico dat moet worden behandeld.

Oranje: Gemiddeld risico dat al dan niet moet worden behandeld, naargelang het geval.

Groen: Klein risico waarvoor geen actie is vereist.

${TABLE\_RISKS}

### Operationele risico’s

### Impactschaal

${OP\_RISKS\_SCALE\_IMPACT}

### Waarschijnlijkheidsschaal

${OP\_RISKS\_SCALE\_LIKELIHOOD}

### Acceptatiedrempels voor de risico's

${TABLE\_OP\_RISKS}

## Evaluatie van de trends en de dreigingen

${SYNTH\_EVAL\_THREAT}

De onderstaande tabel geeft de dreigingen weer waar bijzondere aandacht aan werd besteed.

${TABLE\_THREATS}

# Modellering van de context

## Identificatie van de activa

${SYNTH\_ACTIF}

## Identificatie van de kwetsbaarheden

Met behulp van de modellering van MONARC en zijn objecten kunnen kwetsbaarheden worden geïdentificeerd met voldoende granulariteit voor deze herhaling van de risicoanalyse.

Het blijft echter aan de consultants om nieuwe contextuele risico's te creëren die ze mogelijk tijdens de opdracht ontdekken.

## Beoordeling van de gevolgen

De onderstaande tabel geeft de impact weer voor de essentiële activa van ${COMPANY}. Om tijd te besparen zullen alle secundaire activa die in de modellering van de essentiële activa zullen worden opgenomen deze effecten standaard erven, maar ze zullen handmatig kunnen worden verfijnd.

${IMPACTS\_APPRECIATION}

# Evaluatie en behandeling van de risico's

Het resultaat van het verzamelen van informatie, de invoer en de verschillende evaluaties wordt verwerkt in de MONARC-tool en staat ter beschikking van de klant. Een deel van deze informatie is ook terug te vinden in de bijlage bij dit document.

Verder in dit hoofdstuk worden de resultaten en aanbevelingen voorgesteld die deze risicoanalyse afronden.

## Samenvatting van de risicobeoordeling

${SUMMARY\_EVAL\_RISK}

### Information risks

${DISTRIB\_EVAL\_RISK}

${GRAPH\_EVAL\_RISK}

### Operational risks

${DISTRIB\_EVAL\_OP\_RISK}

${GRAPH\_EVAL\_OP\_RISK}

## 

## Behandeling van de risico's

### Soort behandeling

${RISKS\_KIND\_OF\_TREATMENT}

### Risicobehandelingsplan

De volgende tabel bevat de belangrijkste aanbevelingen uit de risicoanalyse en het risicobeheerplan. De evaluatie en de formulering van de aanbevelingen verlopen volgende deze schaal:

●●● : Prioritaire aanbeveling.

●● : Aanbeveling die een specifieke actie vereist om een kwetsbaarheid of een goede praktijk die tekortschiet te verhelpen.

● : Nuttige aanwijzing voor de veiligheid, advies.

Informatierisico's

${RISKS\_RECO\_FULL}

Operationele risico's

${OPRISKS\_RECO\_FULL}

# Bijlage A: Interview en informatieverzameling

De informatie die het mogelijk maakte de analyse uit te voeren, werd verzameld door middel van interviews met sleutelfiguren in het vakgebied en technische verantwoordelijken.

We danken de volgende personen voor hun actieve bijdrage tijdens de interviews en bezoeken in het kader van onze opdracht:

${TABLE\_INTERVIEW}

# Bijlage B: Evaluatie van de trends

${TABLE\_EVAL\_TEND}

# Bijlage C: Evaluatie van de dreigingen

${TABLE\_THREATS\_FULL}

# Bijlage D: Activa context

${TABLE\_ASSET\_CONTEXT}

# Bijlage E: Risico-eigenaars

${TABLE\_RISK\_OWNERS}

# Bijlage F: Aantekeningen en opmerkingen van de consultant

## Informatierisico's

${TABLE\_AUDIT\_INSTANCES}

## Operationele risico's

${TABLE\_AUDIT\_RISKS\_OP}