



cases.lu
Secure. Innovate. Lead.

WORKSHOP MONARC **(GEOPTIMALISEERDE** **RISICOANALYSEMETHODE CASES)**

OPLEIDING MONARC V2.0

19 SEPTEMBER 2018

VERTALING EN UPDATE UITGEVOERD DOOR PETER GEELEN @ CCB

**SECURITY
MADEIN.LU**





cases.lu
Secure. Innovate. Lead.

SECURITYMADEIN.LU



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



Juridische vorm: E.S.V. (Economisch Samenwerkingsverband)



circl

*Computer Incident
Response Center
Luxembourg*



cases

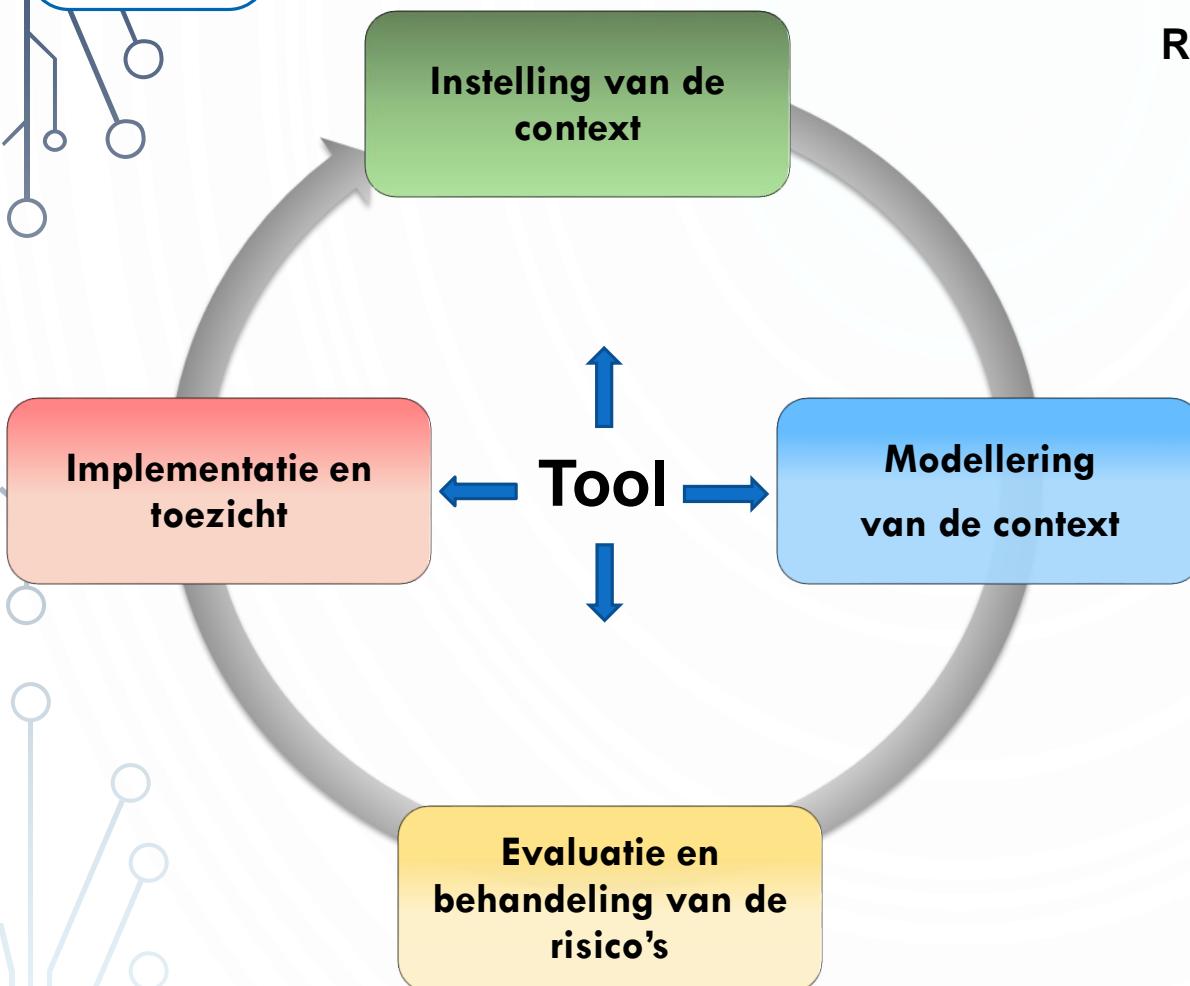
*Cyberworld Awareness
and Security Enhancement
Services*

www.securitymadein.lu
www.cases.lu

AGENDA

- ▶ **Wat is MONARC?**
- ▶ Ontdekking en gebruik van de tool
- ▶ Gebruik van de methode
- ▶ Nieuwe functies
- ▶ Tips & Tricks
- ▶ Diensten

MONARC : GEOPTIMALISEERDE ANALYSEMETHODE VAN RISICO CASES



Risico-analysemethode

- **Gestructureerd**
 - 1. ...
 - 2. ...
 - n. ...
- **Iteratief**
 - Plan
 - Do
 - Check
 - Act
- **Kwalitatief : Impact / gevolgen**
 - Reputatie,
 - Beheer,
 - Legaal,
 - Financieel
 - Personen,
 - ...



cases.lu
Secure. Innovate. Lead.

MONARC: DE METHODE





cases.lu
Secure. Innovate. Lead.

MONARC: VERGELIJKING ISO27005

MONARC

Instelling van de context

Deliverable: Validatie Context

Modellering van de context

Deliverable: Model Valideatie

Evaluatie en Behandeling van de risico's

Deliverable: Finaal Rapport

Implementatie en toezicht

ISO/IEC 27005

Instelling van de context

Waardering risico's

Risico identificatie

Risico analyse

Risico evaluatie

Risicobehandeling

Beslissingspunt 1

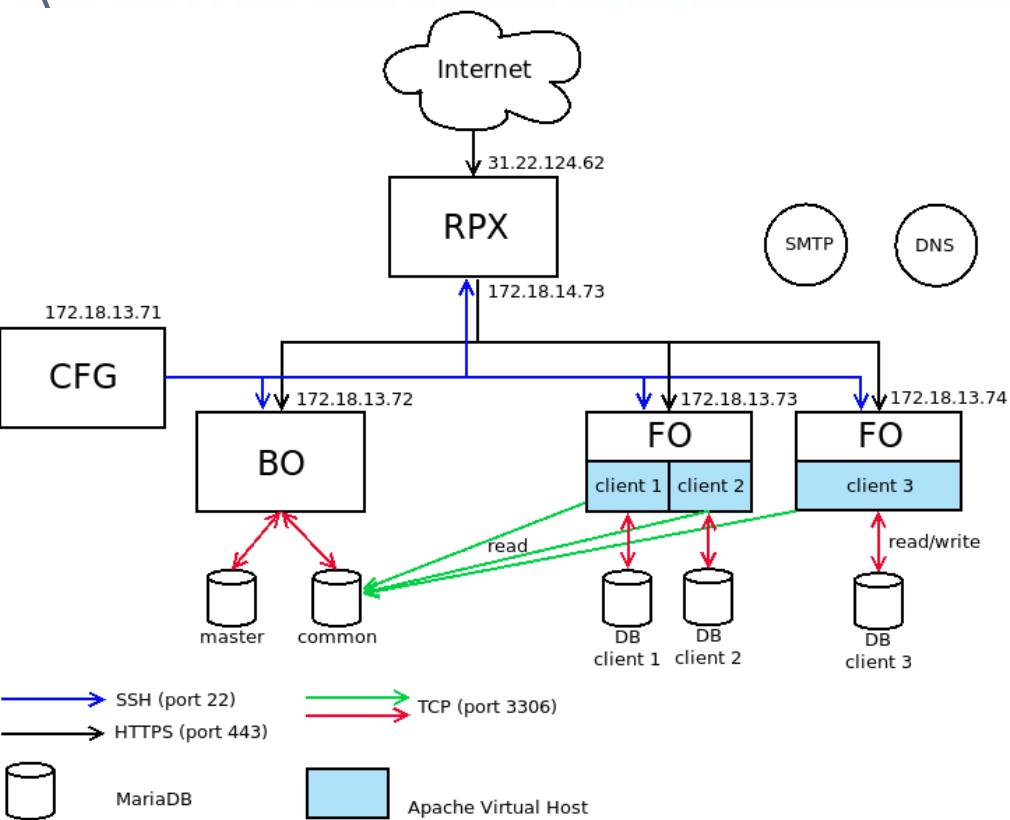
Beslissingspunt 2

Opvolging en herevaluatie van de risico's



cases.lu
Secure. Innovate. Lead.

ARCHITECTUUR



Back-Office [BO]

Administratie

gemeenschappelijke DB,
FO-servers, modellen en
gebruikers

Front-Office [FO]

Interface klanten

Administratie common
DB

klant en gebruikers

MONARC: TE ONTHOUDEN

Open source

www.github.com/monarc-project

AGPL v3.0 (GNU Affero General Public License version 3)

Risicobeheer (ISO/IEC 27005)

Informatierisico's ($R = I \times M \times V$)

Impact op de VIB (Vertrouwelijkheid, Integriteit, beschikbaarheid)

Secundaire assets

Operationele risico's ($R = I \times P$)

Impact op de ROLFP (Reputatie, Operationeel, Legaal, Financieel, Personeel)

Bruto /Netto

Primaire assets



cases.lu
Secure. Innovate. Lead.

MONARC: TE ONTHOUDEN

- ▶ **Delen van risicoanalyses**
- ▶ **Geoptimaliseerd (modellen, deliverables, erfenis, globalisering)**
- ▶ **Meertalig (EN, FR, DE, NL)**

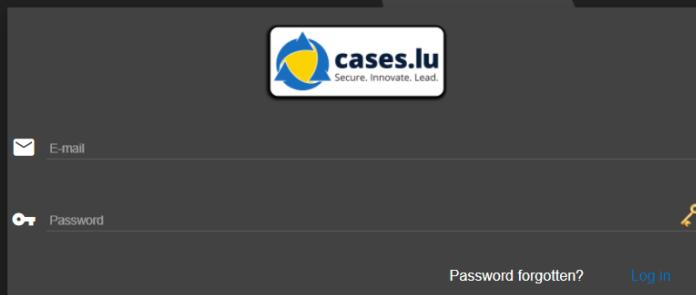
AGENDA

- ▶ Wat is MONARC?
- ▶ **Ontdekking en gebruik van de tool**
- ▶ Gebruik van de methode
- ▶ Nieuwe functies
- ▶ Tips & Tricks
- ▶ Diensten



cases.lu
Secure. Innovate. Lead.

ONTDEKKING EN GEBRUIK VAN DE TOOL





cases.lu
Secure. Innovate. Lead.

BASIS NAVIGATIE

The screenshot shows the 'Demo Analysis NL CASES' application. The top navigation bar has several items: 'Startpagina' (highlighted with red number 3), 'Demo Analysis NL CASES' (highlighted with red number 3), 'Risicoanalyse' (highlighted with red number 3), 'Informatierisico's (highlighted with red number 2), 'Operationele risico's (highlighted with red number 3), and a system menu with icons for settings, user, and others (highlighted with red number 5). Below the navigation bar, there are two tabs: 'Informatierisico's' (selected) and 'Operationele risico's'. A sidebar on the left contains sections for 'Risicoanalyse' (with a search bar and 'Alles uitvoeren/Alles opvouwen' button), 'Activbibliotheek' (with a search bar and buttons for '+ Basisbeginselen' and '+ EBIOS'), and a button '+ Een risicoanalyse creëren'. The main content area displays a message: 'Er zijn geen risico's voor dit actief, of uw filters hebben geen resultaat opgeleverd'. At the bottom right of the content area, there are buttons for 'Sorteren' (MAX risico, Dalend), 'Soort behandeling' (dropdown), and search/filter options. The footer of the application window includes 'Copyright 2012-2018 CASES' and 'MONARC v. 2.7.1'.

1. Overzicht Risico analyses
2. Details & beheer risico analyse
3. Stappenplan/methode
4. Detail configuratie
5. Systeem menu (Administratie, gebruiker, taal)

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

BASIS NAVIGATIE: RISICO ANALYSE

The screenshot shows a navigation bar at the top with two tabs: '1 Risicoanalyse' (highlighted in yellow) and '2'. Below the navigation bar is a sidebar with sections: 'Risicoanalyse' (with 'Alles uitvouwen/Alles opvouwen' and a search bar), 'Mijn Analyse' (with '+ Wettelijke verplichtingen AVG'), and 'Activabibliotheek'. The main content area is titled 'Mijn Analyse' and displays '0 risico's van de'. A context menu is open on the right side, listing: 'De risicoanalyse wijzigen', 'Een risicoanalyse importeren', 'De volledige risicoanalyse exporteren' (highlighted in grey), and 'De analyse verwijderen'.

1. Overzicht Risico analyses
2. **Details & beheer risico analyse**
3. Stappenplan/methode
4. Detail configuratie
5. Systeem menu (Administratie, gebruiker, taal)

DEMONSTRATIE



Secure. Innovate. Lead.

BASIS NAVIGATIE: METHODE

The screenshot shows a web-based application for risk analysis. At the top, there's a blue header bar with the text "Startpagina > Mijn Analyse". Below the header, a horizontal navigation bar is divided into four segments, each with a yellow circle containing a number (1, 2, 3, 4) and a corresponding color bar above it:

- Segment 1 (Yellow):** "Instelling van de context" (Context setting). It includes a list of tasks:
 - Context van de risicoanalyse
 - Evaluatie van de tendensen, van de bedreigingen en synthese
 - Organisatie van het risicobeheer
 - Definitie van de risico-evaluatiecriteria
 - deliverable Validering van de context**
- Segment 2 (Green):** "Mijn Analyse" (My Analysis) and "Operatiele risico's" (Operational risks). It shows "0 risico's" and has a "Modellering van de context" (Modeling of the context) button.
- Segment 3 (Blue):** "Evaluatie en behandeling van de risico's" (Evaluation and treatment of risks). It includes:
 - Raming, evaluatie en behandeling van de risico's
 - Beheer van het risicobehandelingsplan
- Segment 4 (Red):** "Implementatie en toezicht" (Implementation and supervision). It includes:
 - Beheer van de implementatie van het risicobehandelingsplan
 - deliverable Implementatieplan**

Below the segments, there's a search bar with placeholder text "Een actie zoeken..." and a sidebar with links to "BSG - Baseline Security Guidelines", "Basisbeginselen", and "EBIOS". On the right side of the interface, there are sorting and filtering options like "Sorteren MAX risico", "Sorteer richting Dalend", and a download button.

1. Overzicht Risico analyses
2. Details & beheer risico analyse
3. **Stappenplan/methode**
4. Detail configuratie
5. Systeem menu (Administratie, gebruiker, taal)

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

BASIS NAVIGATIE: CONFIGURATIE

Risicoanalyse

boordtabel

Evaluatieschalen

Knowledge base

Tabel van de interviews

Verklaring van toepasselijkheid

Snapshots

1. Overzicht Risico analyses
2. Details & beheer risico analyse
3. Stappenplan/methode
- 4. Detail configuratie**
5. Systeem menu (Administratie, gebruiker, taal)

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

BASIS NAVIGATIE: SYSTEEM MENU

The screenshot displays a system menu interface. On the left, there's a navigation bar with a user icon and a '4' notification. A dropdown menu is open, showing options: 'De gebruikers beheren' (Manage users), 'Organisatie' (Organization), and 'Leverbare sjablonen' (Available templates). To the right of this is a language selection dropdown with flags for French, English, German, and Dutch, with 'Dutch' currently selected. Below these are search and filter tools, including 'Soort behandeling' (Treatment type), a search icon, a refresh icon, and download icons. The main content area shows a table with columns for 'Sorteren' (Sort by) and 'Sorteer richting' (Sort direction). At the bottom, there are pagination controls ('Regels per pagina: 20') and navigation arrows. A modal window titled 'Gevarenzone' (Danger zone) is open, containing a red button labeled 'Verwijder je account' (Delete your account).

1. Overzicht Risico analyses
2. Details & beheer risico analyse
3. Stappenplan/methode
4. Detail configuratie
5. Systeem menu (Administratie, gebruiker, taal)

DEMONSTRATIE

AGENDA

- ▶ Wat is MONARC?
- ▶ Ontdekking en gebruik van de tool
- ▶ **Gebruik van de methode**
- ▶ Nieuwe functies
- ▶ Tips & Tricks
- ▶ Diensten



cases.lu
Secure. Innovate. Lead.

MONARC: DE METHODE





Secure. Innovate. Lead.

BASIS NAVIGATIE: METHODE

The screenshot shows the software interface for 'Mijn Analyse'. The top navigation bar has four items: 1. Instelling van de context, 2. Mijn Analyse, 3. Evaluatie en behandeling van de risico's, and 4. Implementatie en toezicht. A red arrow points to the fourth item. The interface is divided into four main sections: 'Instelling van de context' (left), 'Mijn Analyse' (center-left), 'Evaluatie en behandeling van de risico's' (center-right), and 'Implementatie en toezicht' (right). Each section contains a list of tasks or deliverables. The 'Mijn Analyse' section shows 0 risks.

1. Overzicht Risico analyses
2. Details & beheer risico analyse
3. **Stappenplan/methode**
4. Detail configuratie
5. Systeem menu (Administratie, gebruiker, taal)

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

1.1 CONTEXT VAN DE RISICO ANALYSE

The screenshot shows a software application window titled 'Context van de risicoanalyse'. On the left, there is a navigation sidebar with a tree view of organizational units like 'Back Office', 'Gebouw', 'Informatica', etc., and sections for 'Activbibliotheek' and 'Basisbeginselen'. The main content area contains several text boxes and a 'Actions' section at the bottom right. The text boxes include:

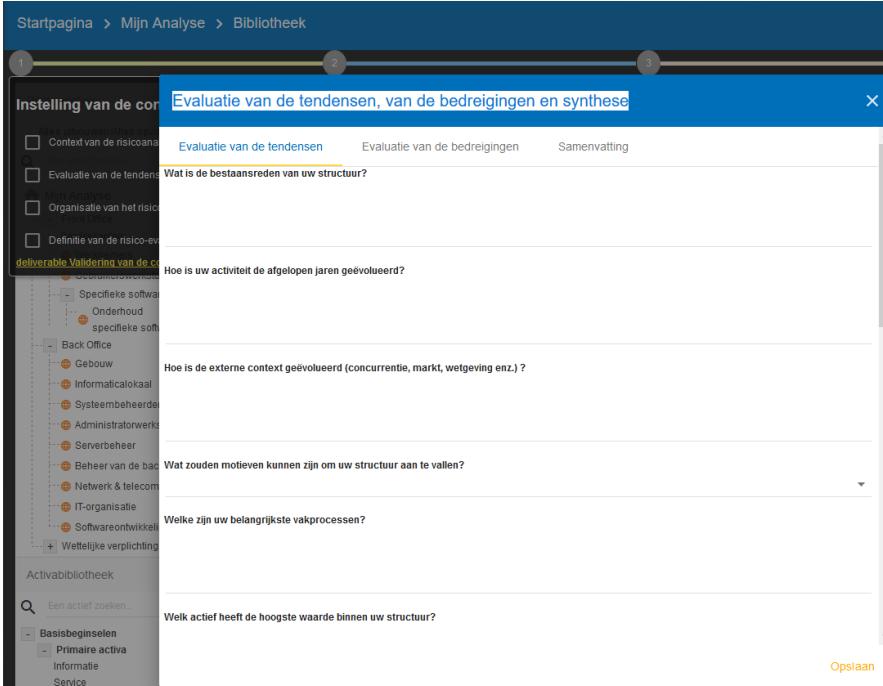
- Algemene overwegingen: Reden(en) waarvoor de analyse wordt gemaakt? Beheer van ISMS, opmaak continuiteitsplan, beheer van de incidenten, juridische aspecten
- Aanpak van het risicobeheer: herhalingen bezig, keuze van de middelen
- Basiscriteria:
 - risico-evaluatiecriteria: strategische informatie- of proceswaarden, wettelijke, reglementaire of contractuele verplichtingen
 - effectriteria: gevolgen voor de business, het imago, de klanten, ...
 - Risicoaanslageringscriteria: ROSI (Return On Secure Investment), wettelijke en reglementen, toekomstige aanpak van het risico, strategie van de firma
- Doelen en grenzen: afdelen te delken proces, doelstellingen van de organisatie, begrenzingen en uitsluiting van de analyse (geografisch, logistisch...), wettelijke verplichtingen, socioculturele omgeving, andere verplichtingen...

At the bottom right of the main content area, there is a red 'X' icon in a box labeled 'Acties'.

- ▶ Ontdekkingsfase van de doelorganisatie
- ▶ Loopt parallel met ISO27005
 - ▶ Algemene overwegingen: Hoofdstuk 7.1
 - ▶ Aanpak risicobeheer: hoofdstuk 7.2.1
 - ▶ Basis criteria: hoofdstukken 7.2.2, 7.2.3, 7.2.4
 - ▶ Doelen en grenzen: hoofdstuk 7.3

DEMONSTRATIE

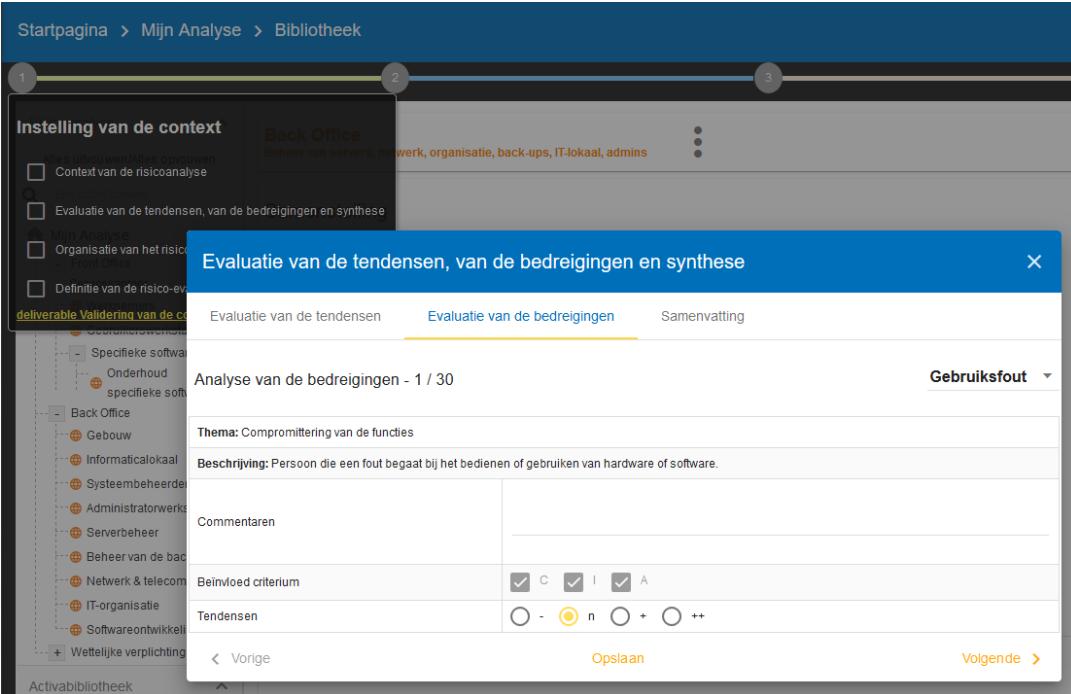
1.2. EVALUATIE VAN DE TENDENSEN, VAN DE BEDREIGINGEN EN SYNTHESE



- ▶ Kick-off meeting: Kernpersonen (management, diensthoofden, IT, Quality, ...)
- ▶ Algemene vragen om context te ontdekken
- ▶ Preciseert de scope en de focus van de analyse
- ▶ Verzamelen van info

DEMONSTRATIE

1.2. EVALUATIE VAN DE TENDENSEN, VAN DE BEDREIGINGEN EN SYNTHESE



- ▶ Doorlopen van meerderheid bedreigingen, discussie aanwakkeren, context ontdekken
- ▶ Informatie verzamelen voor de face-2-face interviews

DEMONSTRATIE

1.2 SAMENVATTING

Evaluatie van de tendensen, van de bedreigingen en synthese X

Evaluatie van de tendensen Evaluatie van de bedreigingen Samenvatting (selected)

B I S P T " <> --- --- --- --- R L i

Opslaan

- ▶ Samenvatting van relevante informatie, verzameld gedurende de evaluatie van trends en bedreigingen
- ▶ Deze tekst laat toe om de deliverable op te vullen

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

1.3 ORGANISATIE VAN RISICOBEHEER

The screenshot shows a software application window titled 'Organisatie van het risicobeheer'. The window has a blue header bar with the title and a white content area. On the left, there is a sidebar with a tree-like navigation structure under 'Instelling van de context'. The main content area contains a large empty text editor with a toolbar above it. At the bottom right of the window are 'Annuleren' and 'Opslaan' buttons. The status bar at the bottom of the window shows '0 operationele risico's'.

- ▶ Aanvullende informatie voor het risicobeheer van de organisatie
- ▶ Parallel aan de ISO27005
 - ▶ Organisatie van risicobeheer: Hoofstuk 7.4

DEMONSTRATIE

1.4 DEFINITIE VAN EVALUATIE CRITERIA, ACCEPTATIE EN IMPACT

Effectenschaal: [0 - 4]

 De verborgen effecten weergeven

Schaal van de kwetsbaarheden: [0 - 5]

- 0. Geen kwetsbaarheid
- 1. Zeer geringe kwetsbaarheid: er werden doeltreffende maatregelen genomen. De goede praktijken werden geïmplementeerd.
- 2. Geringe kwetsbaarheid: er werden doeltreffende maatregelen genomen. De goede praktijken werden geïmplementeerd.
- 3. Normale kwetsbaarheid: er zijn maatregelen getroffen, en die werken zonder dat er naar verbetering wordt gestreefd.
- 4. Hoge kwetsbaarheid: er zijn maatregelen getroffen, maar die zijn niet bijzonder efficiënt of onaangepast.
- 5. Zeer hoge kwetsbaarheid: geen maatregelen getroffen.

		Aanvaardingsdempels voor informatierisico's														
		0	1	2	3	4	5	6	8	9	10	12	15	16	20	
Effect	MxV	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
		1	0	1	2	3	4	5	6	8	9	10	12	15	16	20
2	0	2	4	6	8	10	12	16	18	20	24	30	32	40		
3	0	3	6	9	12	15	18	24	27	30	36	45	48	60		
4	0	4	8	12	16	20	24	32	36	40	48	60	64	80		

► Parallel met ISO27005

► Organisatie van risicobeheer: hoofdstuk 7.2.2, 7.2.3, 7.2.4

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

1.5. DELIVERABLE: CONTEXT VALIDATIE

Startpagina > Mijn Analyse

1 2 3 4

deliverable

x

Status
Klad
Sjabloon *
Validation de contexte

Versie

Classificatie

Naam van het document

Klantverantwoordelijke(n)

Veiligheidsconsultant(s)

Anuleren Opslaan

Huidig risico

Soort behandeling	Datum	Behandeld door	Huidig risico
Soort behandeling	Datum	Behandeld door	C I A
Niet beha	-	-	-
Niet beha	-	-	-
Niet beha	-	-	-

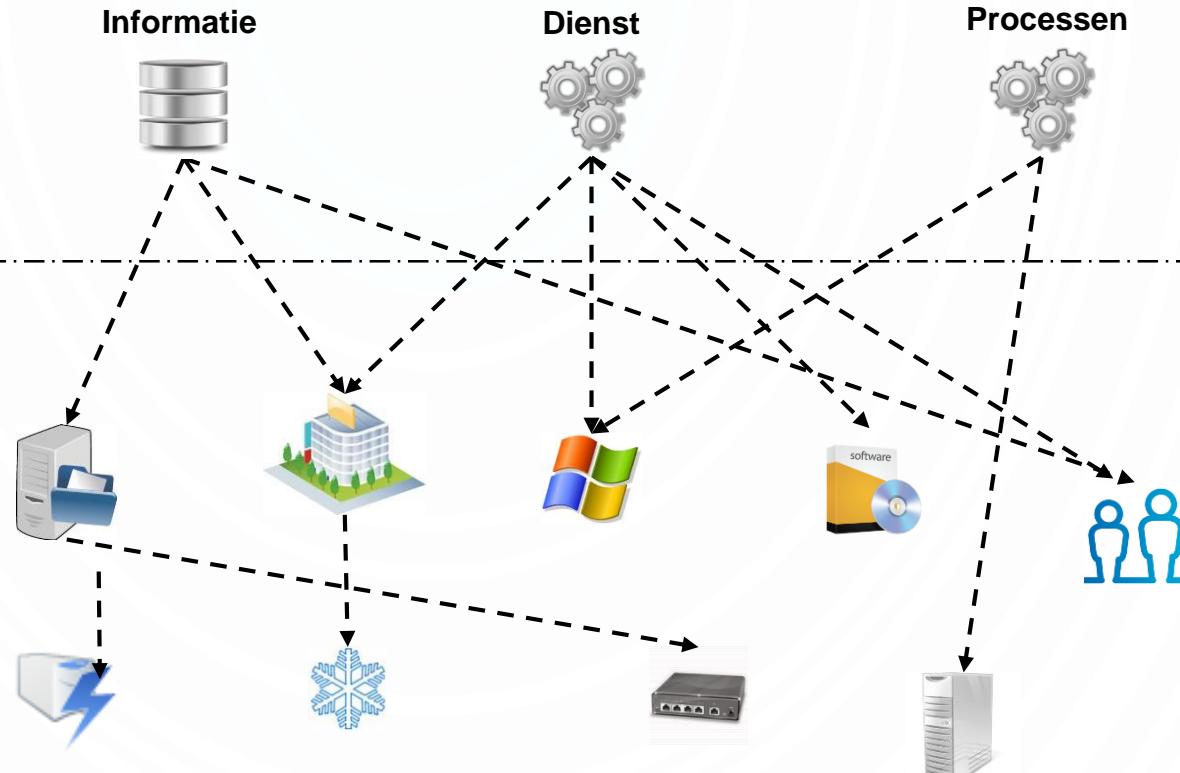
- ▶ Opsomming van alle verzamelde informatie, opgenomen in de fase van de context definitie
- ▶ Wordt gebruikt om de informatie te valideren voor de identificatie van risico's
- ▶ Document formaat = MS Word

DEMONSTRATIE

2.1 – IDENTIFICATIE VAN DE ASSETS, DE KWETSBAARHEDEN EN EVALUATIE VAN DE IMPACT

Primaire assets
(business)

Secundaire assets
(ondersteunend)



De gecumuleerde risico's van de ondersteunende assets gaan terug naar de businessassets via overerving van de VIB-criteria

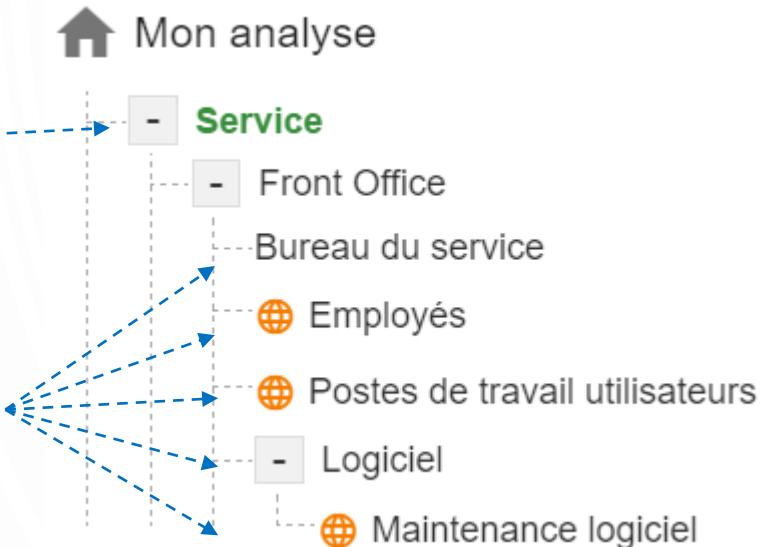


cases.lu
Secure. Innovate. Lead.

FORMALISATIE VAN DE MODELLERING

Hiërarchie van de assets

Primaire assets



Secundaire assets

Type asset

- [SERV]
- [CONT]
- [OV_BATI]
- [OV_UTIL]
- [OV_POSTE_FIXE]
- [OV_LOGICIEL]
- [OV_MAINTENANCE]

OV_BATI

Menace	Vulnérabilité
Vol ou destruction de supports, de documents ou de matériel	Failles dans les périmètres d'accès physiques
Vol ou destruction de supports, de documents ou de matériel	Le principe du moindre privilège n'est pas appliqué
Vol ou destruction de supports, de documents ou de matériel	La gestion des autorisations comporte des failles
Abus de droits	Absence de vigilance lors d'une intervention d'un tiers (fournisseur, femme de ménage, etc.)
Sinistre environnemental (Incendie, eau, poussière, saleté, etc.)	Les locaux ne sont pas sécurisés ou peuvent être compromis par des éléments externes



cases.lu
Secure. Innovate. Lead.

GLOBAAL OF LOKAAL ASSET

Lokaal

Mon analyse

- Base de données N°1
 - Logiciel
 - Backup NAS
 - Salle informatique.
- Base de données N°2
 - Logiciel
 - Backup NAS
 - Salle informatique.

30 risico's

Base de données N°1



Base de données N°2



Globaal

Mon analyse

- Base de données N°1
 - Logiciel
 - Backup NAS
 - Salle informatique
- Base de données N°2
 - Logiciel
 - Backup NAS
 - Salle informatique

21 risico's

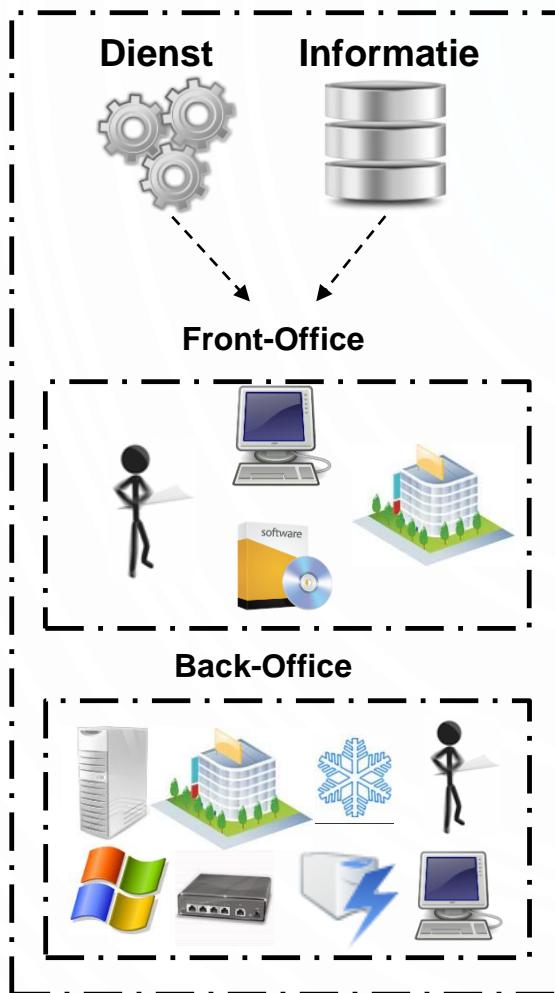
Base de données N°1 Base de données N°2





cases.lu
Secure. Innovate. Lead.

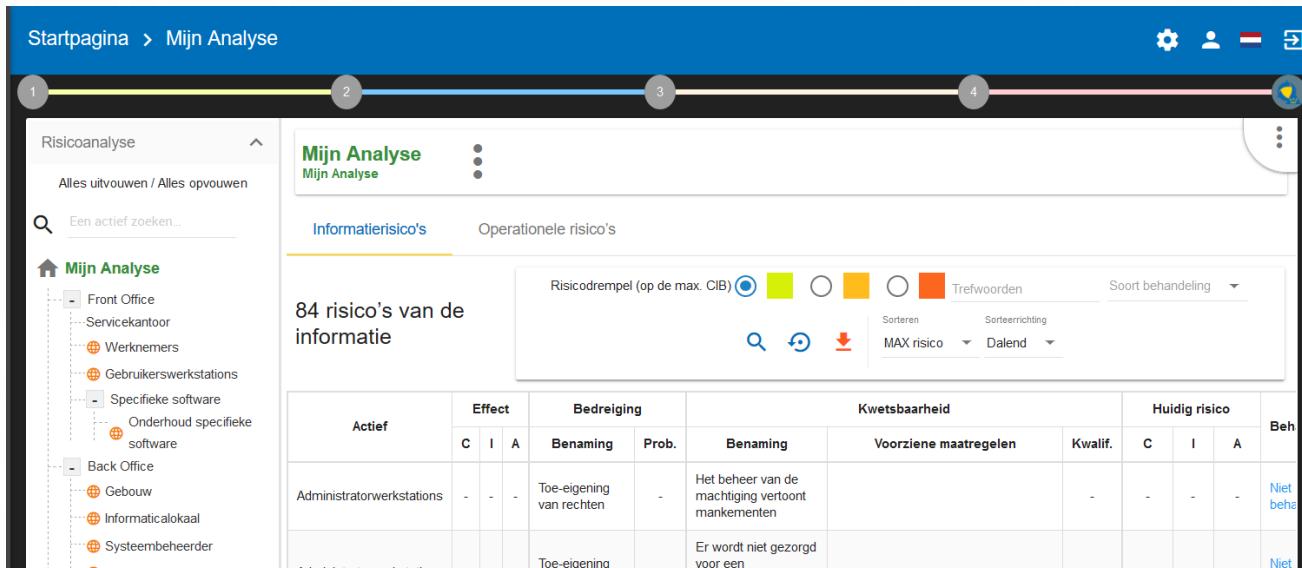
MODELLERING CASES



Mijn Analyse

- Front Office
 - Servicekantoor
 - Werknemers
 - Gebruikerswerkstations
 - Specifieke software
 - Onderhoud
 - specifieke software
- Back Office
 - Gebouw
 - Informaticalokaal
 - Systeembeheerder
 - Administratorwerkstations
 - Serverbeheer
 - Beheer van de back-ups
 - Netwerk & telecom
 - IT-organisatie
 - Softwareontwikkelingen

2.1 IDENTIFICATIE ACTIVA, KWETSBAARHEDEN, EN INSCHATTING IMPACT

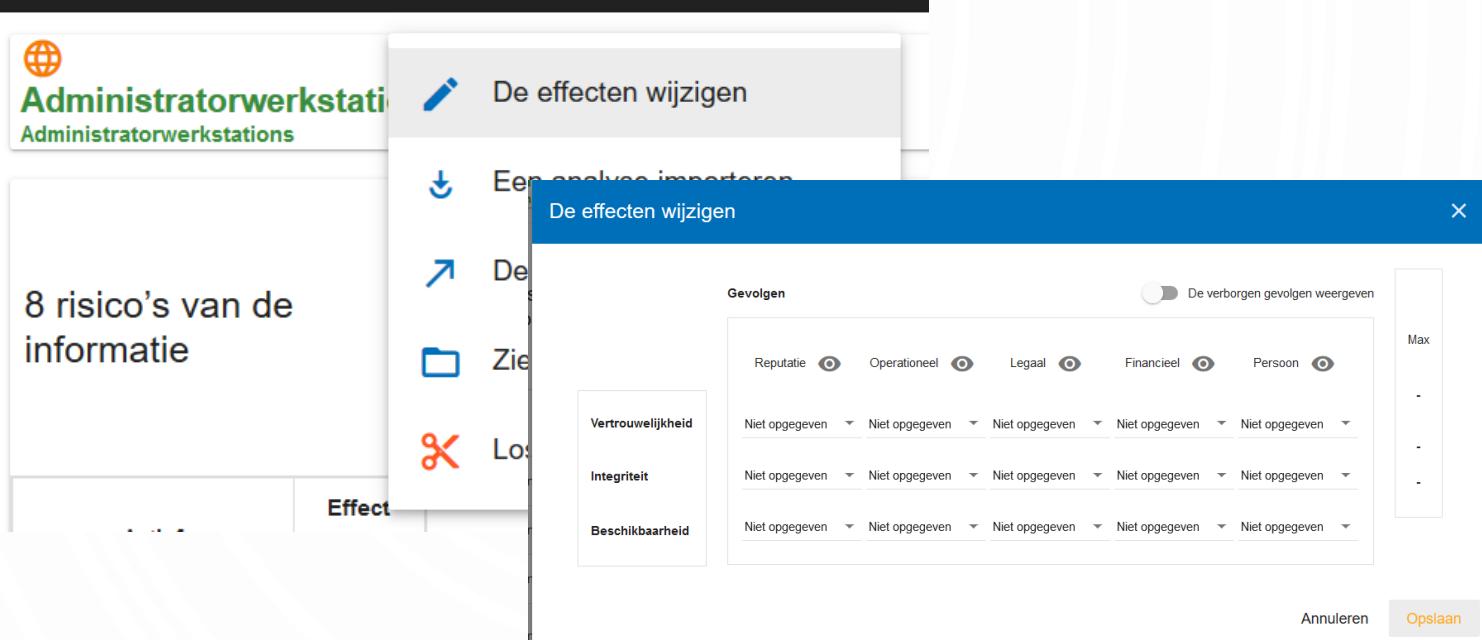


The screenshot shows the 'Startpagina > Mijn Analyse' page. On the left, there's a navigation tree under 'Risicoanalyse' for 'Alles uitvouwen / Alles opvouwen'. The tree includes categories like Front Office, Servicekantoor, Werknemers, Gebruikerswerkstations, Specifiche software, Back Office, Gebouw, Informaticalokaal, and Systeembeheerder. The main area displays '84 risico's van de informatie' with a table. The table has columns for Actief, Effect (C, I, A), Bedreiging, Benaming, Prob., Kwetsbaarheid, Voorziene maatregelen, Kwalif., Huidig risico (C, I, A), and Beh. Two rows are visible: one for 'Administratorwerkstations' and another for 'Toe-eigening'. The 'Administratorwerkstations' row shows 'Het beheer van de machtiging vertoont mankementen' as a threat, while the 'Toe-eigening' row shows 'Er wordt niet gezorgd voor een'.

- ▶ Belangrijkste overzicht van MONARC
 - ▶ Creatie van riskmodellen
- ▶ Parallel met ISO27005
 - ▶ Identificatie activa: hoofdstuk 8.2.2.
 - ▶ Identificatie van kwetsbaarheden: hoofdstuk 8.2.5.

DEMONSTRATIE

2.1 IDENTIFICATIE ACTIVA, KWETSBAARHEDEN, EN INSCHATTING IMPACT

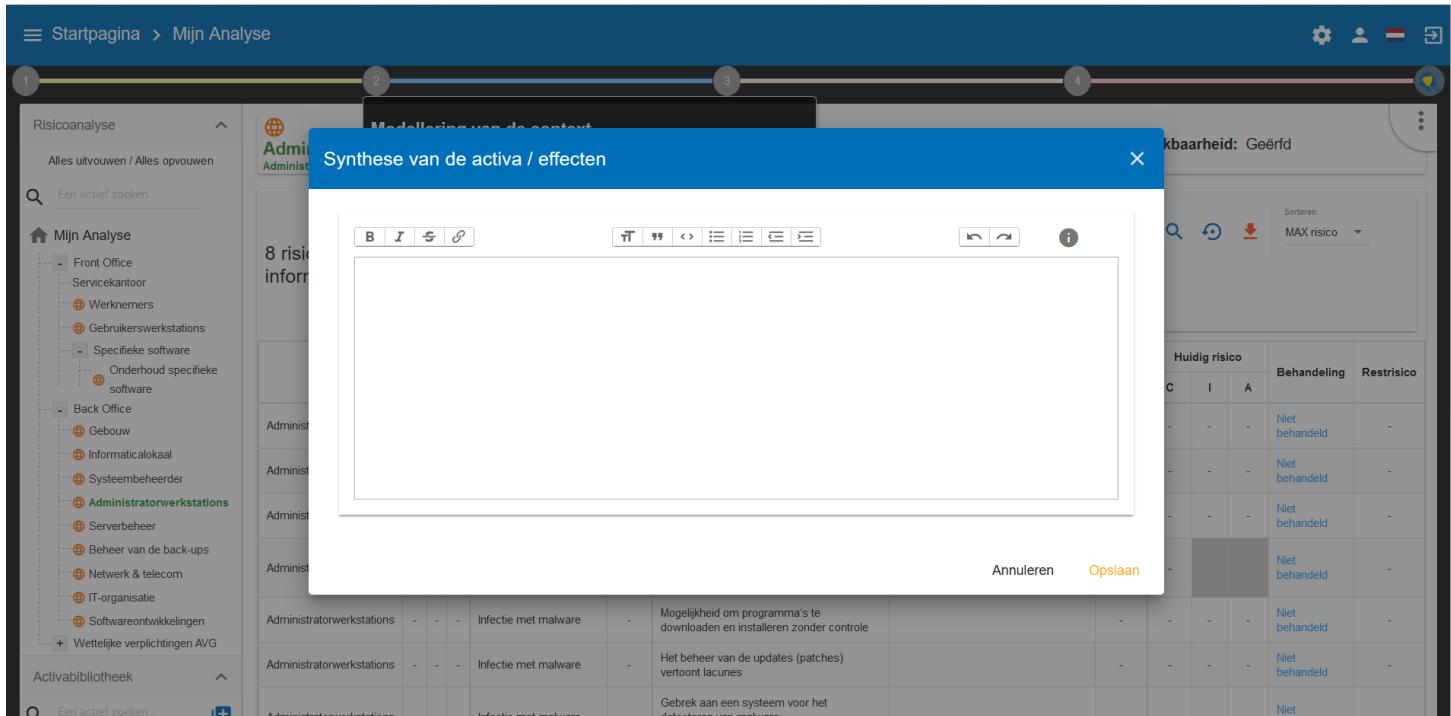


The screenshot shows a software interface titled "Administratorwerkstation" with a sub-section "Administratorwerkstations". On the left, there's a sidebar with the text "8 risico's van de informatie" and a section labeled "Effect" with icons for "Ziekenhuis" and "Los". A modal window titled "De effecten wijzigen" is open, showing a grid for estimating consequences across five categories: Reputatie, Operationeel, Legaal, Financieel, and Persoon. The grid has five rows for each category, with dropdown menus for "Niet opgegeven" (Not specified). There are also sections for "Vertrouwelijkheid" (Confidentiality), "Integriteit" (Integrity), and "Beschikbaarheid" (Availability). Buttons for "Annuleren" (Cancel) and "Opslaan" (Save) are at the bottom right of the modal.

- ▶ Belangrijkste overzicht van MONARC
 - ▶ Inschatting impact en consequenties
- ▶ Parallel met ISO27005
 - ▶ Identificatie consequenties: hoofdstuk 8.3.2.

DEMONSTRATIE

2.2 SYNTHESE VAN ACTIVA/IMPACT



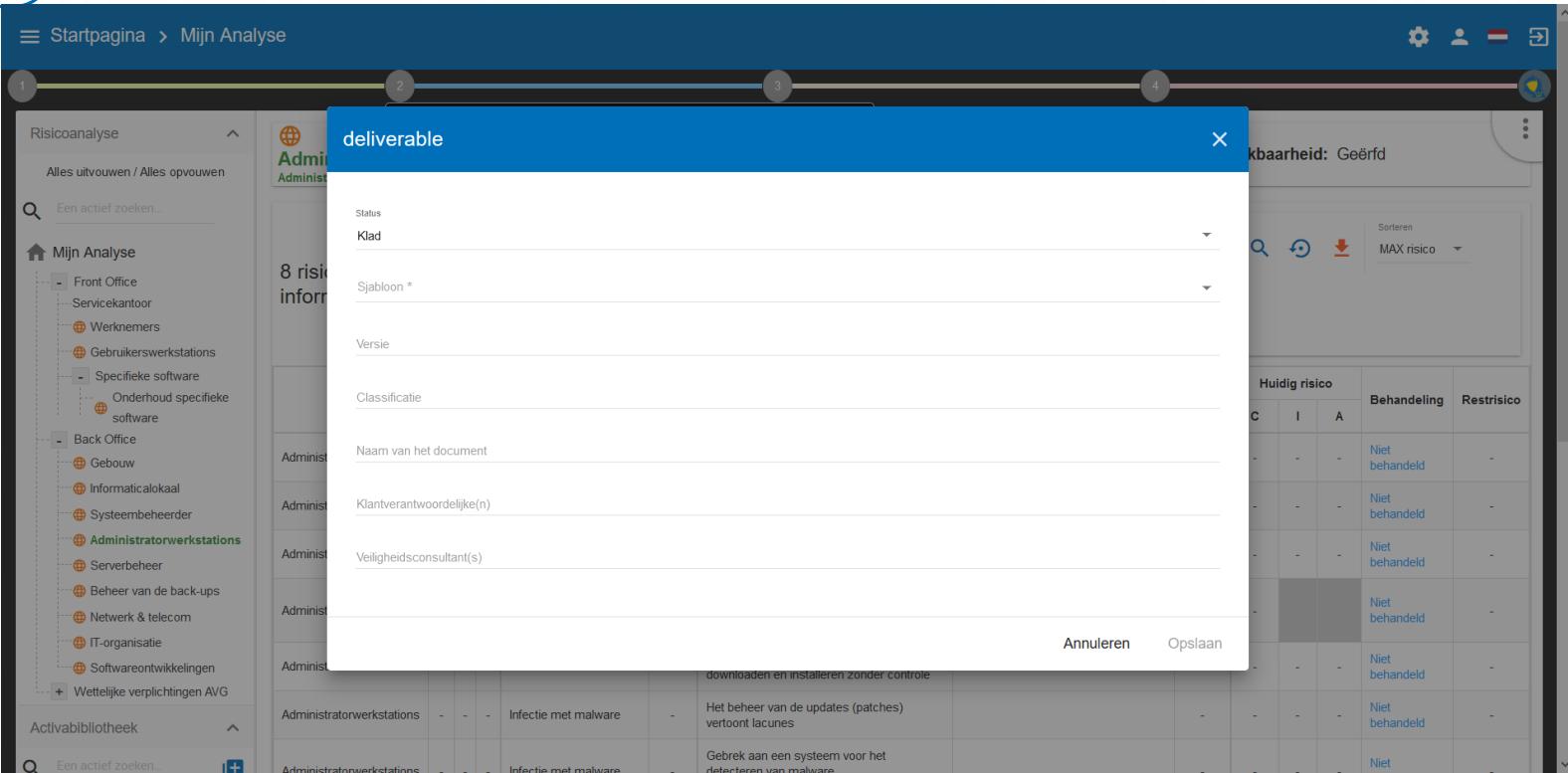
The screenshot shows the software's main interface with a sidebar for 'Risicoanalyse' and a central workspace for 'Mijn Analyse'. A modal window titled 'Synthese van de activa / effecten' is open, containing a text editor and a table. The table details various risks across different categories (C, I, A) and includes columns for treatment and residual risk.

C	I	A	Behandeling	Restrisico
-	-	-	Niet behandeld	-
-	-	-	Niet behandeld	-
-	-	-	Niet behandeld	-
-	-	-	Niet behandeld	-
-	-	-	Niet behandeld	-
-	-	-	Niet behandeld	-
-	-	-	Niet behandeld	-
-	-	-	Niet behandeld	-

- ▶ Tekst die de keuze van activa en impact justifieert
- ▶ Bedoeld om de deliverable me op te vullen

DEMONSTRATIE

2.3 DELIVERABLE: VALIDATIE VAN MODEL



The screenshot shows a software application for risk analysis. On the left, there's a sidebar with categories like 'Front Office', 'Back Office', and 'Administratorwerkstations'. The main area has a blue header bar with four circular icons. A modal window titled 'deliverable' is open, containing fields for 'Status' (set to 'Klad'), 'Sjabloon *', 'Versie', 'Classificatie', 'Naam van het document', 'Klantverantwoordelijke(n)', and 'Veiligheidsconsultant(s)'. At the bottom of the modal are 'Annuleren' and 'Opslaan' buttons. In the background, there's a grid titled 'Risicoanalyse' with columns for 'Huidig risico' (C, I, A), 'Behandeling', and 'Restrisico'. The grid rows show various risk items like 'Administratorwerkstations' with 'Infectie met malware'.

- ▶ Herhaling van de belangrijke primaire activa uit het model
(vastgelegde impact criteria)
- ▶ Herhaling van het overzicht van activa
- ▶ Export formaat = MS Word

DEMONSTRATIE

3.1 RAMING, EVALUATIE EN BEHANDELING VAN DE RISICO'S

Demo Analysis FR CASES
Demo Analysis FR CASES

Informatierisico's Operationele risico's

Evaluatie en behandeling van de risico's

Raming, evaluatie en behandeling van de risico's

Beheer van het risicobehandelingsplan

deliverable eindrapport

Risicodempel (op de max. CIB)  Trefwoorden

Soort behandeling   

Sorteren MAX risico

137 risico's van de informatie

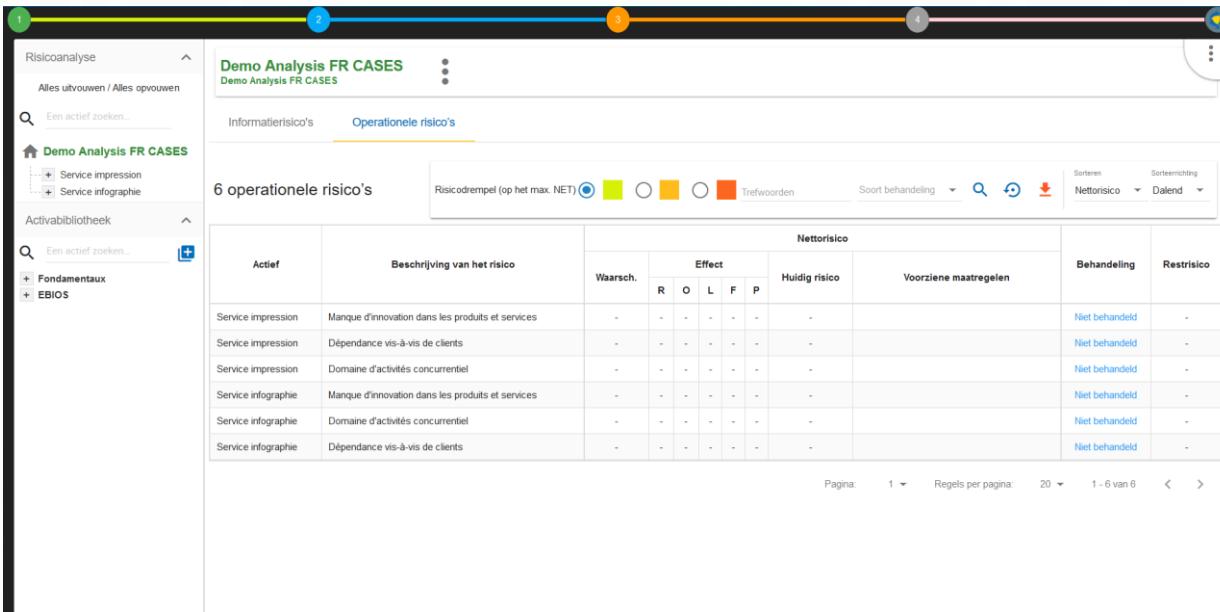
Sorteerrichting Dalend

Actief	Effect			Bedreiging		Kwetsbaarheid				Huidig risico			Behandeling	Restrisko
	C	I	A	Benaming	Prob.	Benaming	Voorzien maatregelen	Kwalif.	C	I	A			
Opérateurs rotative	3	3	4	Atteinte à la disponibilité du personnel	3	Non-redondance du personnel stratégique	L'opérateur rotative à des compétences uniques.	5			60	Reductie	12	
Opérateurs rotative	3	3	4	Erreur d'utilisation	3	Les utilisateurs ne sont pas sensibilisés à la sécurité de l'information	La personne en place ne veut pas de formation. Il part en retraite en 2016.	4	36	36	48	Anvaard	48	
Postes de travail utilisateur	2	2	3	Usurpation de droits	3	La gestion des autorisations comporte des failles	Contrôle d'accès inexistant	5	30	30	45	Niet behandeld	45	
Organisation informatique	2	2	3	Usurpation de droits	3	Absence de contrôle périodique des autorisations d'accès logique	La revue de droit sur l'Active Directory est faite, mais n'est pas optimale.	4	24	24	36	Reductie	27	
Rotatives	3	3	4	Erreur d'utilisation	3	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes...)	L'atelier de production. est bruyant	3	27	27	36	Niet behandeld	36	

- ▶ Belangrijkste overzicht van MONARC
- ▶ Evaluatie van enkele informatie risico's

DEMONSTRATIE

3.1 RAMING, EVALUATIE EN BEHANDELING VAN DE RISICO'S

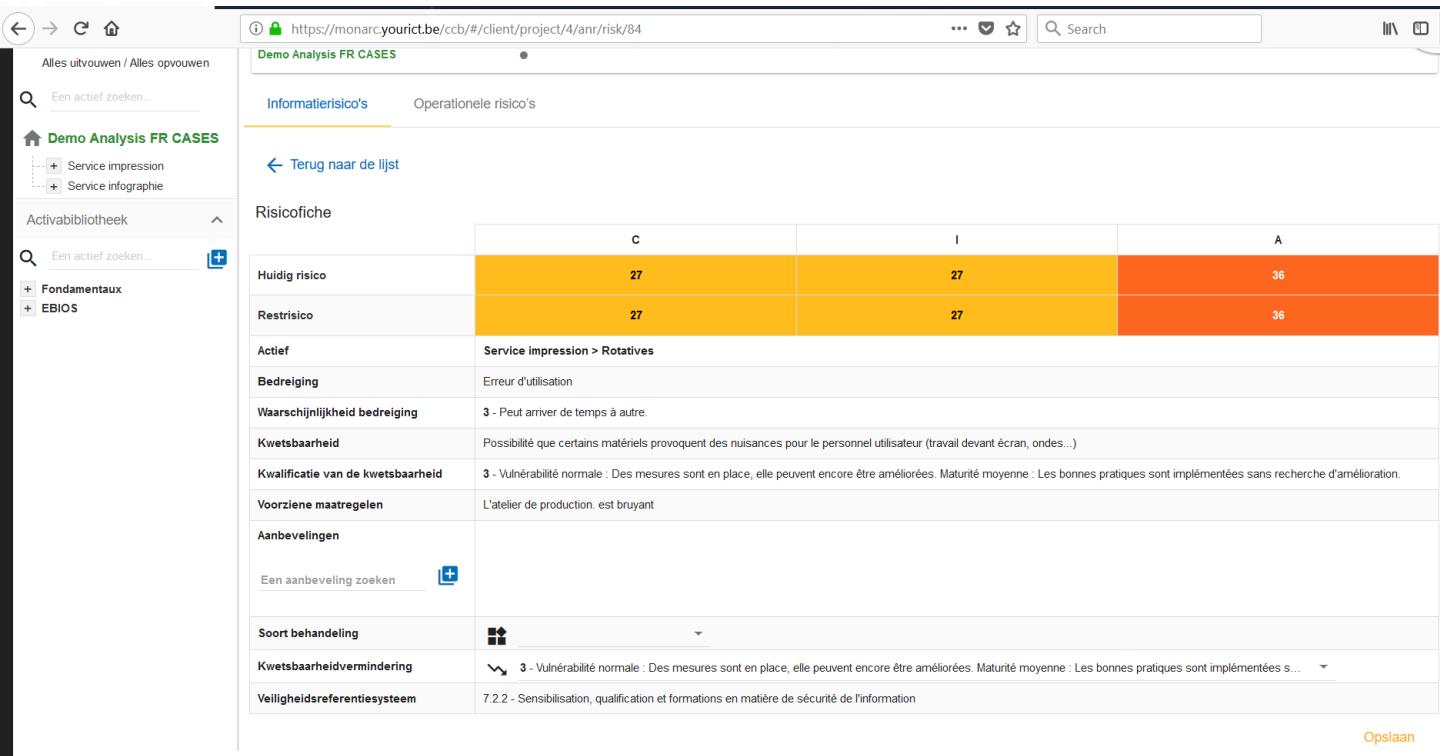


The screenshot shows the cases.lu software interface for risk analysis. The top navigation bar includes tabs for 'Risicoanalyse' (Risk Analysis), 'Informatierisico's (Information Risk), and 'Operatiele risico's (Operational Risk). The current view is on 'Operatiele risico's'. A search bar at the top right allows filtering by 'Riscodrempel (op het max. NET)' (Risk Threshold) and 'Trefwoorden' (Keywords). The main area displays a table titled '6 operationele risico's' (6 operational risks) with columns for 'Actief' (Active), 'Beschrijving van het risico' (Description of the risk), 'Waarsch.' (Warning), 'Effect' (Impact), 'Huidig risico' (Current risk), 'Voorzien maatregelen' (Measures taken), 'Behandeling' (Treatment), and 'Restrisico' (Residual risk). The 'Effect' column uses a color-coded scale from green (Low) to red (High). The 'Huidig risico' column contains mostly green circles, indicating low current risk. The 'Behandeling' column shows 'Niet behandeld' (Not treated) for all listed items. The table footer includes pagination controls (Pagina: 1, Regels per pagina: 20, 1 - 6 van 6).

- ▶ Belangrijkste overzicht van MONARC
- ▶ Evaluatie van enkele operationele risico's

DEMONSTRATIE

3.1 RAMING, EVALUATIE EN BEHANDELING VAN DE RISICO'S



The screenshot shows a web-based application for risk analysis. The URL is https://monarc.yourict.be/ccb/#/client/project/4/anr/risk/84. The page title is "Demo Analysis FR CASES". On the left, there's a sidebar with navigation links like "Alles uitvouwen / Alles opvouwen", "Een actief zoeken...", "Demo Analysis FR CASES" (selected), "Activabibliotheek", and "Fondamentaux" (selected). The main content area has tabs for "Informatierisico's" (selected) and "Operationele risico's". Below that is a link "Terug naar de lijst". The central part is titled "Risicofiche" and contains a table with columns C, I, and A. The table rows include:

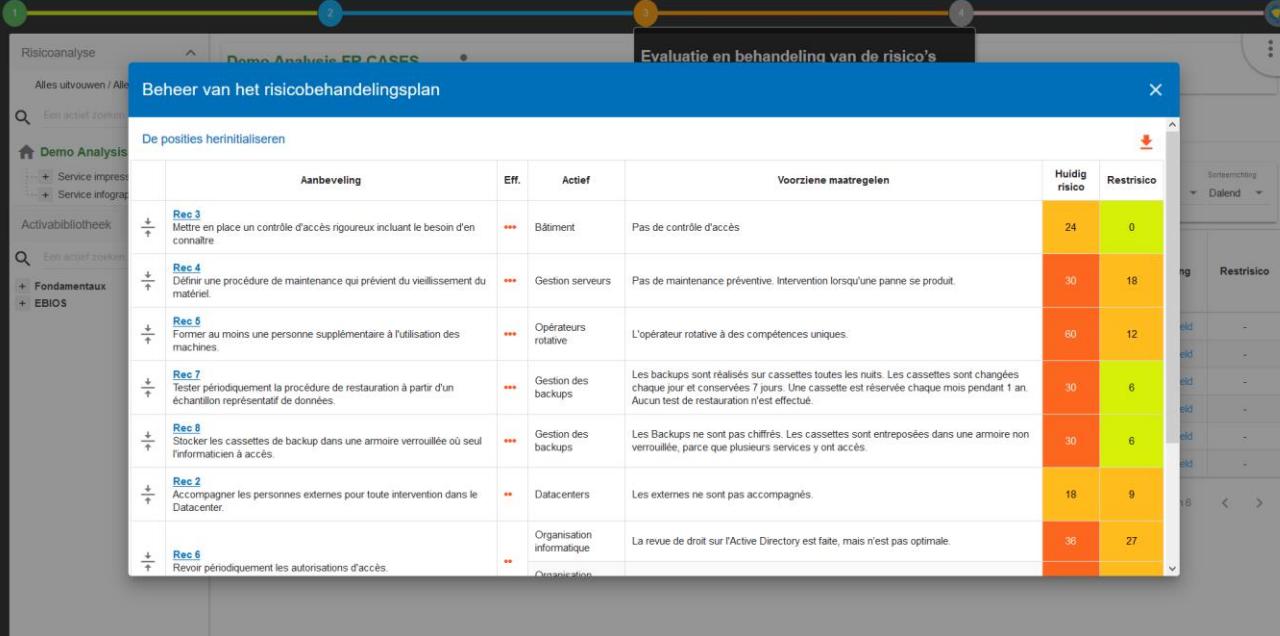
	C	I	A
Huidig risico	27	27	36
Restrisico	27	27	36
Actief	Service impression > Rotatives		
Bedreiging	Erreur d'utilisation		
Waarschijnlijkheid bedreiging	3 - Peut arriver de temps à autre.		
Kwetsbaarheid	Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes...)		
Kwalificatie van de kwetsbaarheid	3 - Vulnérabilité normale : Des mesures sont en place, elle peuvent encore être améliorées. Maturité moyenne : Les bonnes pratiques sont implémentées sans recherche d'amélioration.		
Voorziene maatregelen	L'atelier de production. est bruyant		
Aanbevelingen			
Een aanbeveling zoeken	<input type="button" value="L"/>		
Soort behandeling	<input checked="" type="checkbox"/>		
Kwetsbaarheidvermindering	3 - Vulnérabilité normale : Des mesures sont en place, elle peuvent encore être améliorées. Maturité moyenne : Les bonnes pratiques sont implémentées s... <input type="button" value="▼"/>		
Veiligheidsreferentiesysteem	7.2.2 - Sensibilisation, qualification et formations en matière de sécurité de l'information		

At the bottom right of the form is an "Opslaan" button.

- ▶ Risicofiche van asset
- ▶ Creeren van raadgevingen

DEMONSTRATIE

3.2 BEHEER PLAN VOOR RISICOBEHANDELING



	Aanbeveling	Eff.	Actief	Voorzien maatregelen	Huidig risico	Restrisico
Rec 3	Mettre en place un contrôle d'accès rigoureux incluant le besoin d'en connaître	***	Bâtiment	Pas de contrôle d'accès	24	0
Rec 4	Définir une procédure de maintenance qui prévient du vieillissement du matériel.	***	Gestion serveurs	Pas de maintenance préventive: Intervention lorsqu'une panne se produit.	30	18
Rec 5	Former au moins une personne supplémentaire à l'utilisation des machines.	***	Opérateurs rotative	L'opérateur rotative à des compétences uniques.	60	12
Rec 7	Tester périodiquement la procédure de restauration à partir d'un échantillon représentatif de données.	***	Gestion des backups	Les backups sont réalisés sur cassettes toutes les nuits. Les cassettes sont changées chaque jour et conservées 7 jours. Une cassette est réservée chaque mois pendant 1 an. Aucun test de restauration n'est effectué.	30	6
Rec 8	Stocker les cassettes de backup dans une armoire verrouillée où seul l'information accès.	***	Gestion des backups	Les Backups ne sont pas chiffrés. Les cassettes sont entreposées dans une armoire non verrouillée, parce que plusieurs services y ont accès.	30	6
Rec 2	Accompagner les personnes externes pour toute intervention dans le Datacenter.	**	Datacenters	Les externes ne sont pas accompagnés.	18	9
Rec 6	Revoir périodiquement les autorisations d'accès.	**	Organisation informatique	La revue de droit sur l'Active Directory est faite, mais n'est pas optimale.	36	27
			Organisation			

- ▶ Overzicht van alle risico's die deel uitmaken van een advies
- ▶ Informatie risico's en operationele risico's

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

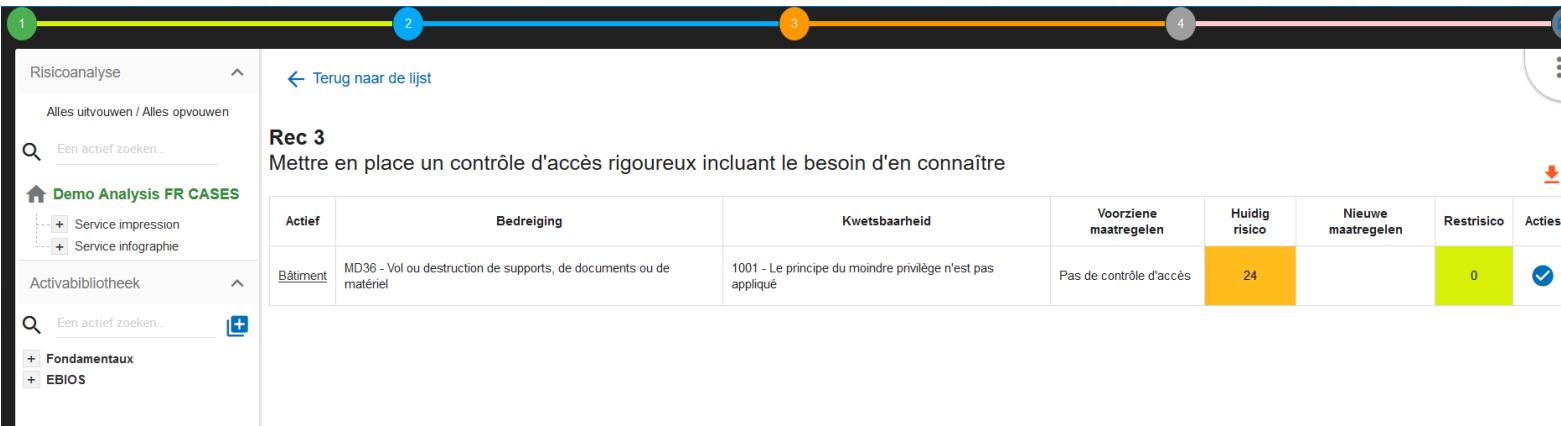
3.3 EINDRAPPORT

Risico	Behandeling	Restrisko
1	Niet behandeld	-
2	Niet behandeld	-
3	Niet behandeld	-
4	Niet behandeld	-
5	Niet behandeld	-
6	Niet behandeld	-

- ▶ Uitgebreid overzicht van alle informatie die verzameld en opgenomen is
- ▶ Mogelijkheid om een analyse overzicht te krijgen
- ▶ Export formaat: MS Word

DEMONSTRATIE

4.1 BEHEER VAN DE IMPLEMENTATIE VAN HET RISICOBEHANDELINGSPLAN



Risicoanalyse

Alles uitvoeren / Alles opvouwen

Een actief zoeken...

Demo Analysis FR CASES

- + Service impressie
- + Service infographie

Activabibliotheek

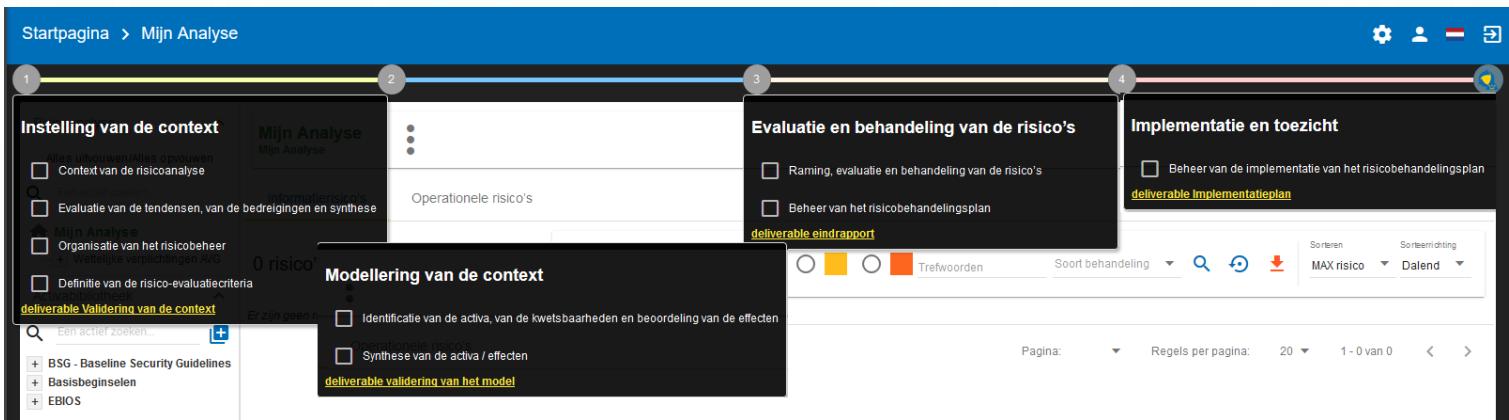
Een actief zoeken...

Actief	Bedreiging	Kwetsbaarheid	Voorziene maatregelen	Huidig risico	Nieuwe maatregelen	Restrisico	Acties
Bâtiment	MD36 - Vol ou destruction de supports, de documents ou de matériel	1001 - Le principe du moindre privilège n'est pas appliqué	Pas de contrôle d'accès	24		0	<input checked="" type="checkbox"/>

- ▶ Validatie van de status wijziging van ieder risico
- ▶ Wijziging van risicowaarde: risico wordt huidige risico

DEMONSTRATIE

4.1 BEHEER VAN IMPLEMENTATIE RAADGEVINGEN



The screenshot shows a software interface for risk analysis, specifically the 'Mijn Analyse' module. The process is divided into four main phases:

- Instelling van de context**: Includes tasks like 'Context van de risicoanalyse' and 'Evaluatie van de tendensen, van de bedreigingen en synthese'. A yellow box highlights the deliverable 'Validering van de context'.
- Mijn Analyse Mijn Analyse**: Shows '0 risico's'.
- Evaluatie en behandeling van de risico's**: Includes tasks like 'Raming, evaluatie en behandeling van de risico's' and 'Beheer van het risicobehandelingsplan'. A yellow box highlights the deliverable 'eindrapport'.
- Implementatie en toezicht**: Includes the task 'Beheer van de implementatie van het risicobehandelingsplan'. A yellow box highlights the deliverable 'implementatieplan'.

The central area is labeled 'Modellering van de context' and includes tasks like 'Identificatie van de activa, van de kwetsbaarheden en beoordeling van de effecten' and 'Synthese van de activa / effecten'. A yellow box highlights the deliverable 'validering van het model'.

At the bottom, there are search and filter options, and navigation links for 'BSG - Baseline Security Guidelines', 'Basisbeginselen', and 'EBIOS'.

1. Overzicht Risico analyses
2. Details & beheer risico analyse
3. Stappenplan/methode
4. Detail configuratie
5. Systeem menu (Administratie, gebruiker, taal)

DEMONSTRATIE

AGENDA

- ▶ Wat is MONARC?
- ▶ Ontdekking en gebruik van de tool
- ▶ Gebruik van de methode
- ▶ **Nieuwe functies**
- ▶ Tips & Tricks
- ▶ Diensten

TOEKOMSTIGE FUNCTIONALITEITEN

- ▶ Dashboard
- ▶ SOA-beheer en gap analysis
- ▶ Repository voor modellen
- ▶ Register GDPR-behandelingen
- ▶ Roadmap: <https://github.com/monarc-project/MonarcAppFO/wiki/Roadmap>

AGENDA

- ▶ Wat is MONARC?
- ▶ Ontdekking en gebruik van de tool
- ▶ Gebruik van de methode
- ▶ Nieuwe functies
- ▶ **Tips & Tricks**
- ▶ Diensten



cases.lu
Secure. Innovate. Lead.

CREATIE VAN EEN NIEUW RISICO

Startpagina > Mijn Analyse > Knowledge base

1 2 3 4

Activatype	Bedreigingen	Kwetsbaarheden	Maatregelen 27002	Categorieën	Informatierisico's	Tags	Operationele risico's
Activatype	+ Zoeken...						
<input type="checkbox"/> Status	Benaming		Code	Type	Beschrijving		
<input checked="" type="checkbox"/>	Bedrijvengids	SYS_ANU	Secundair	Bedrijvengids			
<input checked="" type="checkbox"/>	Vaktoepassing	LOG_APP	Secundair	Maat- of standaardvaktoepassing			
<input checked="" type="checkbox"/>	Andere dragers	MAT_NELE	Secundair	Documenten, fax, brief, bestelbon, informatie op papier enz.			
<input checked="" type="checkbox"/>	Back-up	OV_BACKUP	Secundair	Kwalificatie van de back-ups			
<input checked="" type="checkbox"/>	Gebouw, kantoor of lokaal	OV_BATI	Secundair	Gebouw, kantoor of lokaal			
<input checked="" type="checkbox"/>	Container	CONT	Primair	Activacontainer			
<input checked="" type="checkbox"/>	Besluitvormer	PER_DEC	Secundair	Besluitvormer			
<input checked="" type="checkbox"/>	Toepassingsontwikkelingen	OV_DEVELOPPEMENT	Secundair	Toepassingsontwikkelingen			
<input checked="" type="checkbox"/>		

Risicoanalyse
boordtafel
Evaluatieschalen
Knowledge base
Tabel van de interviews
Verklaring van toepasselijkheid
Snapshots

1. Creatie van een nieuwe asset (activa)
2. Creatie van een bedreiging
3. Creatie van een kwetsbaarheid
4. Koppeling activa/bedreiging/kwetsbaarheid
5. Creatie van activa in de bibliotheek
6. Gebruik van de activa in de analyse

DEMONSTRATIE



Secure. Innovate. Lead.

IMPORTEREN VAN ACTIVA

The screenshot shows the 'Mijn Analyse' dashboard. On the left, there's a sidebar with a search bar ('Een actief zoeken...'), a 'Activabibliotheek' section containing 'BSG - Baseline Security Guidelines', 'Basisbeginselen', and 'EBIOS', and a 'Wettelijke verplichtingen AVG' section. The main area displays a message: '0 risico's van de' followed by 'Er zijn geen risico's voor dit' and a button labeled 'Een actief toevoegen'. A yellow box highlights this button. In the foreground, a modal window titled 'Een actief toevoegen' is open, featuring a search bar ('Een actief zoeken...'), a sidebar with the same navigation as the dashboard, and a central area with a file upload input ('Een actief importeren') and a 'Benamingen en beschrijvingen' section.

- Mogelijkheid om activa te importeren of te creëren

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

EXPORTEREN VAN ACTIVA

Startpagina > Mijn Analyse > Bibliotheek

1 2 3

Risicoanalyse

Alles uitvouwen/Alles opvouwen

Een actief zoeken...

Mijn Analyse

+ Wettelijke verplichtingen AVG

Activabibliotheek

Een actief zoeken...

+ BSG - Baseline Security Guidelines

- Basisbeginselen

- Primaire activa

Informatie

Service

Vakdatabase

+ Modelstructuur

Informatie
Te beveiligen informatie in elektronische vorm

Samenstelling

Informatie

0 operationele risico's

Er zijn geen operationele risico's voor dit actief.

Het actief wijzigen

Het actief kopiëren

Het actief exporteren

Het actief verwijderen

- Mogelijkheid om activa te exporteren

DEMONSTRATIE



cases.lu
Secure. Innovate. Lead.

IMPORTEREN/EXPORTEREN VAN ANALYSE

Startpagina > Mijn Analyse > Bibliotheek

1 Risicoanalyse
Alles uitvouwen/Alles opvouwen

Een actief zoeken...

2 Informatie
Te beveiligen informatie in elektronische vorm

3 Samenstelling

Informatie [+] 0 operationele risico's

Er zijn geen operationele risico's voor dit actief.

Het actief wijzigen
Het actief kopiëren
Het actief exporteren
Het actief verwijderen

- Mogelijkheid om analyse te importeren/exporteren van
 - Bibliotheek
 - Met of zonder evaluatie

DEMONSTRATIE

AGENDA

- ▶ Wat is MONARC?
- ▶ Ontdekking en gebruik van de tool
- ▶ Gebruik van de methode
- ▶ Nieuwe functies
- ▶ Tips & Tricks
- ▶ Diensten



cases.lu
Secure. Innovate. Lead.

DIENSTEN

- ▶ Gepersonaliseerde installatie
- ▶ Opleidingen op aanvraag
- ▶ Hulp bij gebruik van Monarc
- ▶ Ontwikkeling op maat



cases.lu
Secure. Innovate. Lead.

CONTACTEER ONS



info@cases.lu



monarc.lu



[monarc-project](https://github.com/monarc-project)