



cases.lu
Secure. Innovate. Lead.

WORKSHOP MONARC **(OPTIMISED RISK ANALYSIS METHOD)**

MONARC V2.0 TRAINING

INFO@CASES.LU

**SECURITY
MADEIN.LU**





cases.lu
Secure. Innovate. Lead.

SECURITYMADEIN.LU



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG



Legal Form: G.I.E (Groupement d'Intérêt Economique)



circl

*Computer Incident
Response Center
Luxembourg*



cases

*Cyberworld Awareness
and Security Enhancement
Services*

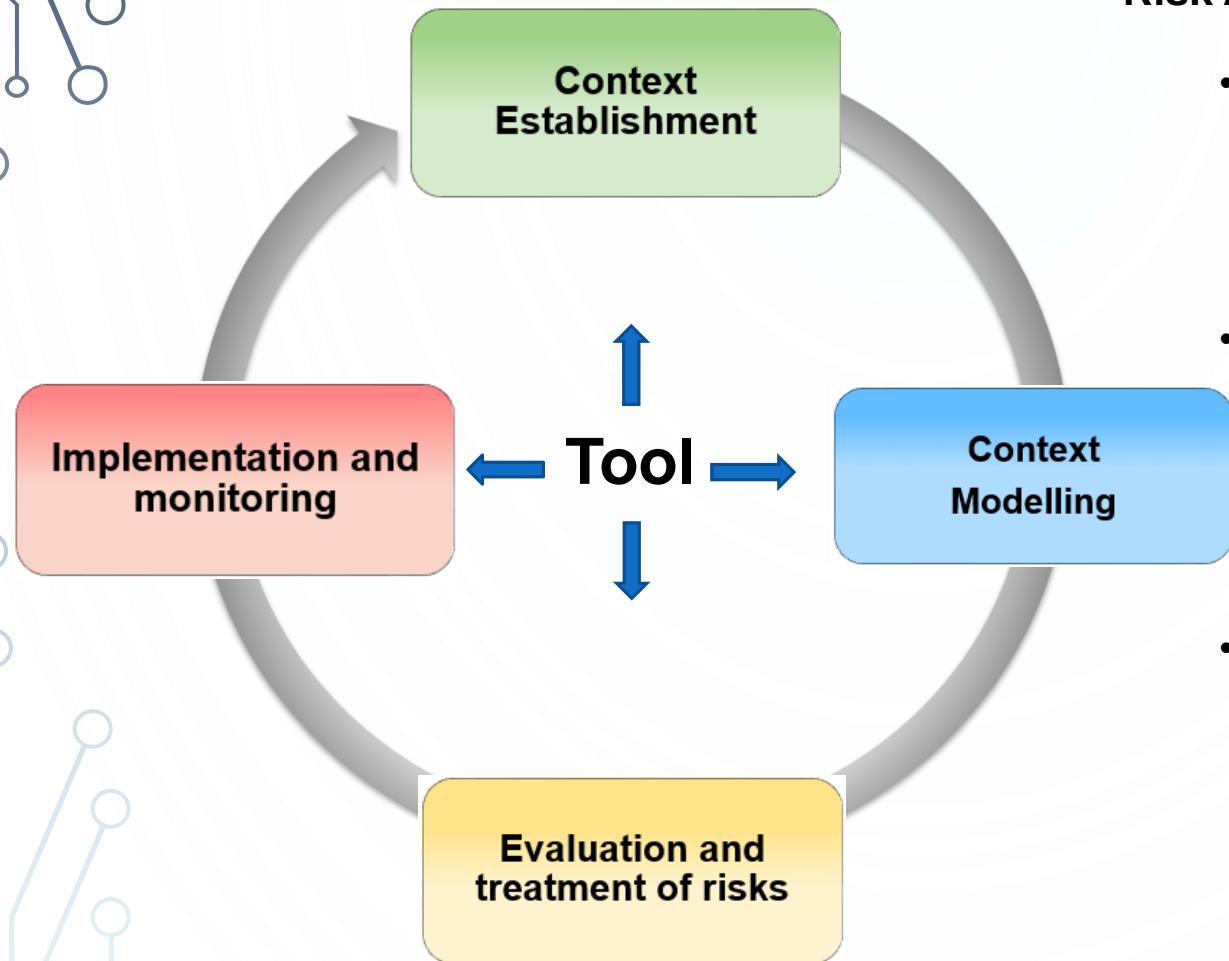
www.securitymadein.lu
www.cases.lu



AGENDA

- ▶ What is MONARC ?
- ▶ Discovery and usage of the tool
- ▶ Run-through of the method
- ▶ Tips & Tricks

MONARC: OPTIMISED RISK ANALYSIS METHOD



Risk Analysis Method

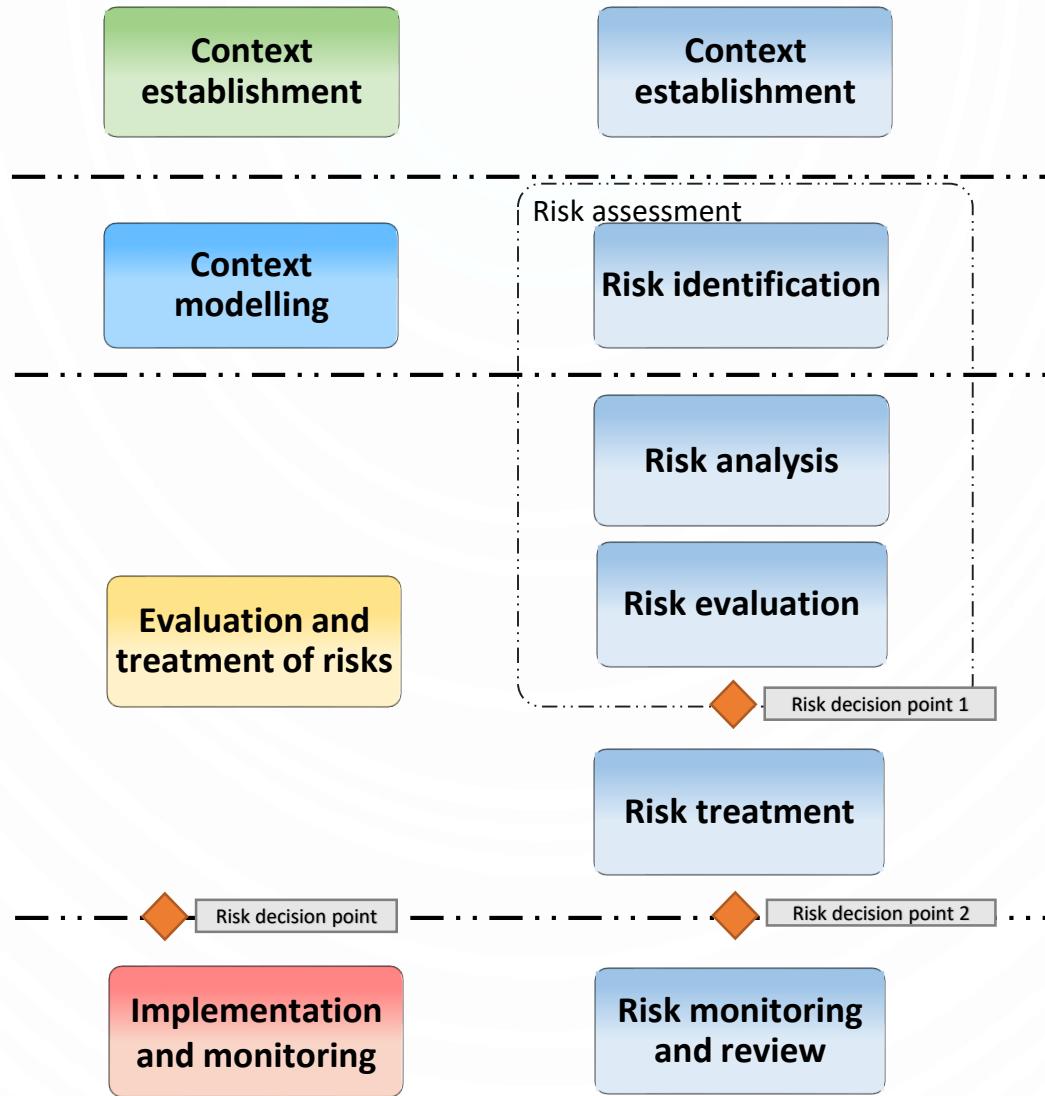
- **Structured**
 - 1. ...
 - 2. ...
 - n. ...
- **Iterative**
 - Plan
 - Do
 - Check
 - Act
- **Qualitative : Values / consequences**
 - Reputation, Image
 - Operation
 - Legal
 - Financial
 - Person (to the)
 - ...



cases.lu
Secure. Innovate. Lead.

MONARC : THE METHOD

MONARC



MONARC : À RETENIR

Open source

www.github.com/CASES-LU/MonarcAppFO

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

Risk Management

Information Risks ($R = I \times M \times V$)

Impact on the CIA

Secondary Assets

Operational Risks ($R = I \times P$)

Impact on the ROLFP

Gross/Net

Primary Assets

Sharing of Risk Models

Optimised (models, deliverables, inheritance, globalisation)

AGENDA



- ▶ What is MONARC ?
- ▶ **Discovery and usage of the tool**
- ▶ Run-through of the method
- ▶ Tips & Tricks



cases.lu
Secure. Innovate. Lead.

MAIN FEATURES/FUNCTIONALITIES

The screenshot shows the cases.lu software interface for 'DemoCompany'. The left sidebar includes links for 'DPIA v0.7', 'DemoCompany', 'Mon analyse', 'MyCompany', 'MyPrint', and 'xxxx', along with a '+ Create a risk analysis' button. The main area displays a risk analysis report for 'DemoCompany' with 84 information risks. The report includes sections for 'Information risks' and 'Operational risks'. A table provides detailed information about each risk, including Asset, Impact (C, I, A), Threat (Label, Prob.), Vulnerability (Label, Existing controls, Qualif.), Current risk (C, I, A), Processing status, and Target risk. The processing status for most risks is 'Not processed'.

Asset	Impact			Threat		Vulnerability			Current risk			Processing	Target risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	-	-	-	Forging of rights	-	Authorisation management is flawed			-	-	-	Not processed	-
Administrator workstations	-	-	-	Forging of rights	-	User authentication is not ensured			-	-	-	Not processed	-
Administrator workstations	-	-	-	Forging of rights	-	The user workstation is not monitored			-	-	-	Not processed	-
Administrator workstations	-	-	-	Retrieval of recycled or discarded media	-	Presence of residual data unknown to the user of reallocated or discarded equipment			-	-	-	Not processed	-
Administrator workstations	-	-	-	Malware infection	-	Programs can be downloaded and installed without monitoring			-	-	-	Not processed	-
Administrator workstations	-	-	-	Malware infection	-	Update management (patches) is flawed			-	-	-	Not processed	-
Administrator workstations	-	-	-	Malware infection	-	No detection system of malicious programs			-	-	-	Not processed	-
Administrator workstations	-	-	-	Abuse of rights	-	No procedures for system install and configuration			-	-	-	Not processed	-
Backup management	-	-	-	Equipment malfunction or failure	-	Backups are not carried out in accordance with the state of the art			-	-	-	Not processed	-
Backup management	-	-	-	Theft or destruction of media, documents or equipment	-	Backup media are not stored in a suitable place			-	-	-	Not processed	-
Building	-	-	-	Theft or destruction of media, documents or equipment	-	The principle of least privilege is not applied			-	-	-	Not processed	-



cases.lu
Secure. Innovate. Lead.

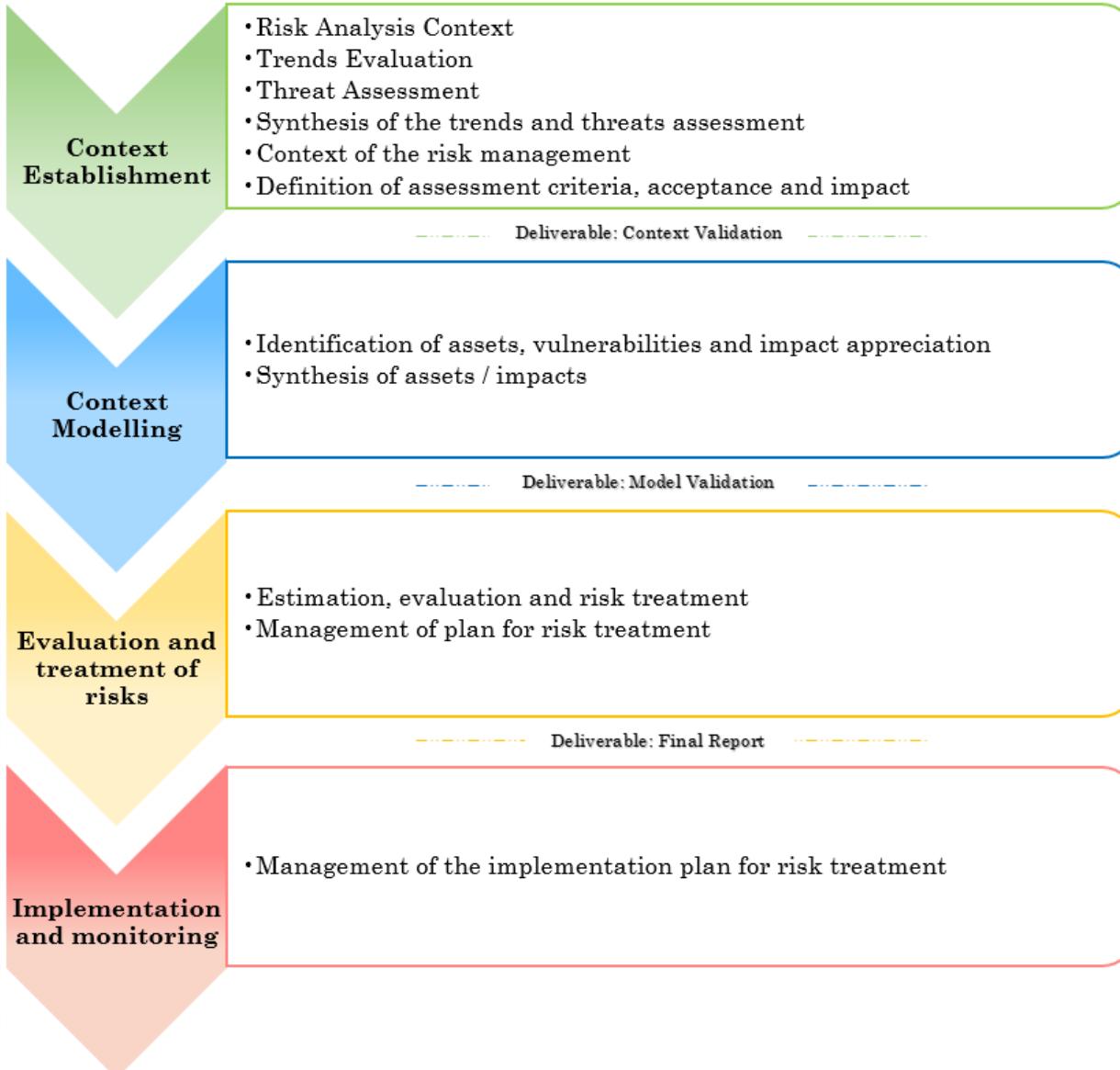
AGENDA

- ▶ What is MONARC ?
- ▶ Discovery and usage of the tool
- ▶ **Run-through of the method**
- ▶ Tips & Tricks



cases.lu
Secure. Innovate. Lead.

MONARC : LA MÉTHODE EN DÉTAILS





cases.lu
Secure. Innovate. Lead.

1.1 – CONTEXT OF THE RISK ANALYSIS

The screenshot shows a software application for risk management. At the top, there's a navigation bar with 'Home > DemoCompany' and a gear icon. The main area has a dark header with the title 'Risks analysis context'. Below the header is a toolbar with icons for bold, italic, and other text styles, along with a search bar and a help icon.

The central content area is titled 'Additional information'. It contains several sections with descriptive text:

- General considerations:** What is the purpose of the information security risk management? ISMS Management, preparation of a business continuity plan or incident response plan, legal compliance.
- Risk management approach:** ongoing iteration, provision of resources.
- Basic Criteria:**
 - Risk evaluation criteria: The process strategic value or importance, legal obligations, regulatory requirements or contractuals
 - Impact criteria: Consequences on business, image, legal, ...
 - Risk acceptance criteria: ROSI (Return On Security Investment), legal and regulatory aspects, future security risk management, company strategy
- Scope and boundaries:** Activity, business processes, organization's objectives, limits and exclusion of the analysis (geographical, logical...), legal requirements, socio-cultural environment, other requirements.
- General Considerations**
- Risk management approach**
- Basic criteria**
- Scope and boundaries**

At the bottom right of the dialog box are 'Cancel' and 'Save' buttons. The background shows a sidebar for 'Context Establishment' and a main panel with a tree view of assets like 'Administrator workstations' and 'Backup management' under 'Fundamentals'.

- Discovering the target organisation
 - Links with ISO 27005:2011
 - General considerations
 - Risk Management Approach
 - Basic Criteria
 - Targets and Limits

- : Chapter 7.1
- : Chapter 7.2.1
- : Chapters 7.2.2, 7.2.3, 7.2.4
- : Chapter 7.3



cases.lu
Secure. Innovate. Lead.

1.2 – EVALUATION OF TRENDS

The screenshot shows the software interface for 'Evaluation of Trends and Threat, and synthesis'. The top navigation bar includes 'Home', 'DemoCompany', a gear icon, a user icon, and a search bar. A progress bar at the top indicates steps 1 through 4. The main area contains several questions:

- What is the purpose of your organization?
- What is the progression of your business in recent years?
- What is the evolution of the external environment (competition, market evolution, laws, etc.)?
- What might be the attack reasons on your structure?
- What are your most important business processes?
- What is the most valuable asset in your organization?

Below the questions is a table with columns for 'Existing controls', 'Qualif.', 'C', 'I', 'A', 'Processing', and 'Target risk'. The table contains numerous rows, each with a status of 'Not processed' in the 'Processing' column. At the bottom right of the main area is a 'Save' button.

- Kick-off meeting : Key people (management, team coordinators, IT, Quality, ...)
- Broad/general questions to identify the context
- Define the scope and focus of the analysis
- Information collection

DEMO



cases.lu
Secure. Innovate. Lead.

1.2 – EVALUATION OF THREATS

The screenshot shows the software interface for threat evaluation. At the top, there's a navigation bar with 'Home > DemoCompany' and various icons. Below it is a sidebar titled 'Context Establishment' with sections like 'Risks analysis context' (checked), 'Evaluation of Trends and Threat, and synthesis' (unchecked), and 'Definition of the risk evaluation criteria' (unchecked). A 'Deliverable: Context validation' section contains a search bar and buttons for 'Fundamentals' and 'EBIOS'. The main area has tabs for 'Trends assessment' (disabled) and 'Threats assessment' (selected). The 'Threats assessment' tab shows a table for 'Administrator workstations' with columns for Asset, Impact (C, I, A), and various threat details like 'Theme: Compromise of functions' and 'Description: A person commits an operating error, input error or utilisation error on hardware or software.' There's also a 'Comments' field and a 'Probability' dropdown. To the right, a large table lists threats across different asset types like 'Building' and 'Employees', with columns for 'Qualif.', 'Current risk' (C, I, A), 'Processing', and 'Target risk'. A legend indicates 'Error in use' with a red circle. At the bottom, there are 'Previous' and 'Next' buttons, and a 'Save' button.

- Go through some Threats, involve the group, define the context
- Collect information before individual interviews

DEMO



cases.lu
Secure. Innovate. Lead.

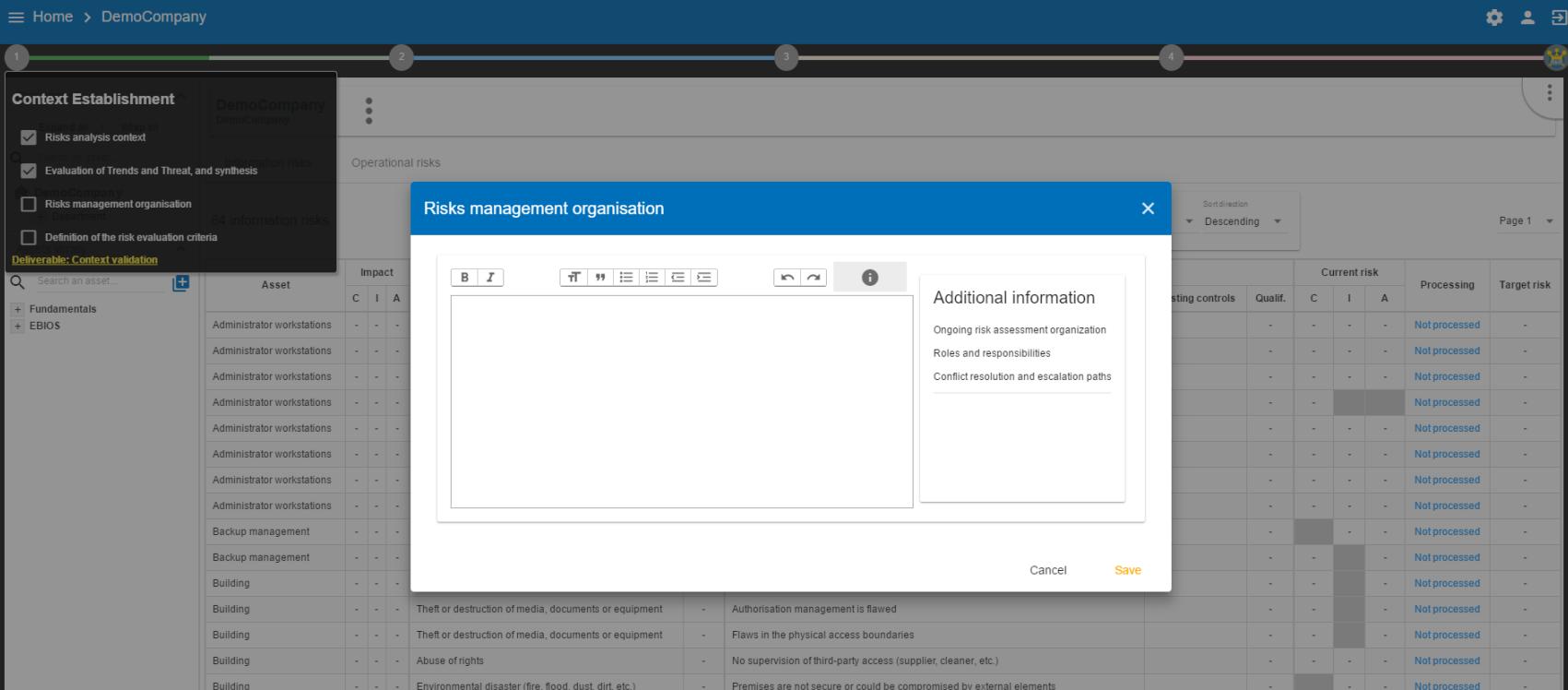
1.2 – SUMMARY

The screenshot shows the software interface for 'DemoCompany'. A navigation bar at the top includes 'Home', 'DemoCompany', and icons for settings, user profile, and export. Below the navigation is a progress bar with four steps: 1. Context Establishment (green), 2. Evaluation of Trends and Threat, and synthesis (blue), 3. Risks management organisation (grey), and 4. Definition of the risk evaluation criteria (pink). The main area displays the 'Evaluation of Trends and Threat, and synthesis' module. It has tabs for 'Trends assessment', 'Threats assessment', and 'Summary'. The 'Summary' tab is active, showing a table with columns for Asset, Impact (C, I, A), Existing controls, Qualif., Current risk (C, I, A), Processing, and Target risk. The table lists various assets like 'Administrator workstations' and 'Building', along with their respective risks and status. A modal window titled 'Evaluation of Trends and Threat, and synthesis' is open, containing sections for 'Trends assessment' and 'Threats assessment', with a 'Save' button at the bottom right.

- Summarise the important information collected during the evaluation of trends and threats.
- This information will complete the first deliverable

DEMO

1.3 – ORGANISATION OF THE RISK MANAGEMENT



The screenshot shows a software application for risk management. On the left, there's a sidebar with 'Context Establishment' settings, including 'Risks analysis context' (checked) and 'Evaluation of Trends and Threat, and synthesis' (checked). Below this is a table of assets with columns for Impact (C, I, A) and various rows like 'Administrator workstations' and 'Backup management'. In the center, a modal window titled 'Risks management organisation' is open, containing a large text area and a 'Save' button at the bottom right. To the right of the modal is a grid table with columns for 'Current risk' (Qualif., C, I, A), 'Processing' (Status: Not processed), and 'Target risk' (Status: -). The table lists multiple rows of risk items.

	Qualif.	C	I	A	Processing	Target risk
Theft or destruction of media, documents or equipment	-	-	-	-	Not processed	-
Theft or destruction of media, documents or equipment	-	-	-	-	Not processed	-
Abuse of rights	-	-	-	-	Not processed	-
Environmental disaster (fire, flood, dust, dirt, etc.)	-	-	-	-	Not processed	-
Theft or destruction of media, documents or equipment	-	-	-	-	Not processed	-
Flaws in the physical access boundaries	-	-	-	-	Not processed	-
No supervision of third-party access (supplier, cleaner, etc.)	-	-	-	-	Not processed	-
Premises are not secure or could be compromised by external elements	-	-	-	-	Not processed	-

- Additional information on risk management within the organisation
- Links with ISO 27005:2011
 - Organisation of risk management: Chapter 7.4



cases.lu
Secure. Innovate. Lead.

1.4 – DEFINITION OF EVALUATION, ACCEPTANCE AND IMPACT CRITERIA

Acceptance thresholds of information risks



Acceptance thresholds of operational risks



TxV

	0	1	2	3	4	5	6	8	9	10	12	15	16	20
0	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

$$R = I \times (T \times V)$$

R: Risk, I: Impact, T: Threat, V: Vulnerability

Impacts scale: [0 - 4]

Show hidden impacts

	Confidentiality	Integrity
0	Nonexistent impact. The confidentiality criterion is not important.	Nonexistent impact The integrity criteric important.
1	Weak impact, insignificant. Information leaks are negative to the organization's interests. Examples: - Internal information leaks which shouldn't be outside the company. - Memorandum - Internal phone directory	Weak impact, insigr Corruption easy to i consequences. Example: - Internal mail or let
2	Average impact, acceptable. Information leaks harm organization's interests. Examples: - Moderately sensitive information leaks which are only for a group of people.	Average impact, ac Corruption which bi inconvenience to th Recovery is easy. Example:

Probability

$$R = I \times P$$

R: Risk, I: Impact, P: Probability

Threats scale: [0 - 4]

- 0. Impossible
- 1. Very unlikely: never happened, requires a high level of expert knowledge, or it is very expensive to execute.
- 2. Unlikely: might have happened, rare phenomenon which requires a good level of expert knowledge, or it is expensive to execute.
- 3. Could happen occasionally
- 4. Very likely: easy to execute, no mentionable investment or knowledge necessary

Vulnerabilities scale: [0 - 5]

- 0. No vulnerabilities.
- 1. Very weak vulnerability: Some efficient measures have been already taken, and their effectiveness is controlled.
Very high maturity: Good practices are implemented and frequently verified.
- 2. Weak vulnerability: Some efficient measures have been already taken.
High maturity: Good practices are implemented.
- 3. Average vulnerability: Some measures have been already taken, even though they could be better.
Average maturity: Good practices are implemented without searching a better way.
- 4. Strong vulnerability: Some measures have been already taken, even though they are ineffective or unadapted.
Low maturity: Good practices aren't implemented, but there are some positive reactions without any thoughts.
- 5. Very strong vulnerability: No measures have been implemented.
Very low maturity or no maturity at all.

- Link with ISO 27005:2011
 - Organisation of risk management: Chapter 7.2.2, 7.2.3, 7.2.4

DEMO



cases.lu
Secure. Innovate. Lead.

1.5 – DELIVERABLE: CONTEXT VALIDATION

The screenshot shows the cases.lu software interface. On the left, there's a sidebar titled 'Context Establishment' with several checked items: 'Risks analysis context', 'Evaluation of Trends and Threats, and synthesis', 'Risks management organisation', and 'Definition of the risk evaluation criteria'. Below this is a section for 'Deliverable: Context validation' with a search bar and two categories: 'Fundamentals' and 'EBIOS'. The main area is titled 'Operational risks' and contains a table with columns 'Asset', 'Impact' (C, I, A), and several rows of data. A modal window titled 'Deliverable' is open in the center, containing fields for 'Status' (set to 'Final'), 'Version' (1.0), 'Classification' (Confidential), 'Document name' (Context Establishment Report), 'Client manager(s)' (M. Tee, M. Bond), and 'Security consultant(s)' (M. Meel). At the bottom of the modal are 'Cancel' and 'Save' buttons. In the background, there's a large table with columns 'Existing controls', 'Qualif.', 'Current risk' (C, I, A), 'Processing', and 'Target risk'.

- Compile all the information collected during the context establishment
- Report is used to validate the collected information before the identification of risks starts.
- Export format: Microsoft Word

DEMO

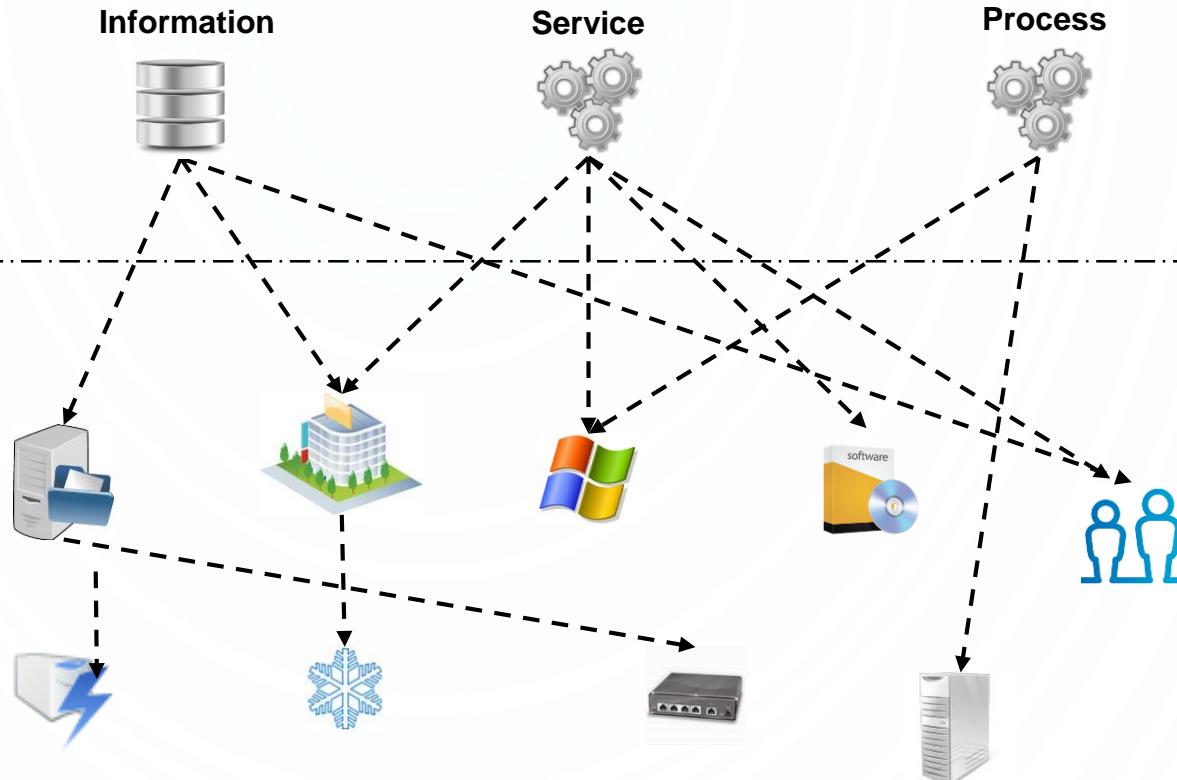


cases.lu
Secure. Innovate. Lead.

2.1 – IDENTIFICATION OF ASSETS, VULNERABILITIES AND EVALUATION OF IMPACTS

**Primary Assets
(Business)**

**Secondary Assets
(Supporting)**



The combination of risks of an supporting asset is transmitted to the business asset through inheritance of the CIA evaluation



cases.lu
Secure. Innovate. Lead.

FORMALISATION OF THE MODELLING

Hierarchy of Assets

Primary Assets

Mon analyse

- Service

- Front Office

Bureau du service

Employés

Postes de travail utilisateurs

- Logiciel

Maintenance logiciel

Secondary Assets

Type of Assets

[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.

« GLOBAL » OR « LOCAL » ASSET

“Local”

Mon analyse

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

30 risks

Base de données N°1



Base de données N°2



“Global”

Mon analyse

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

21 risks

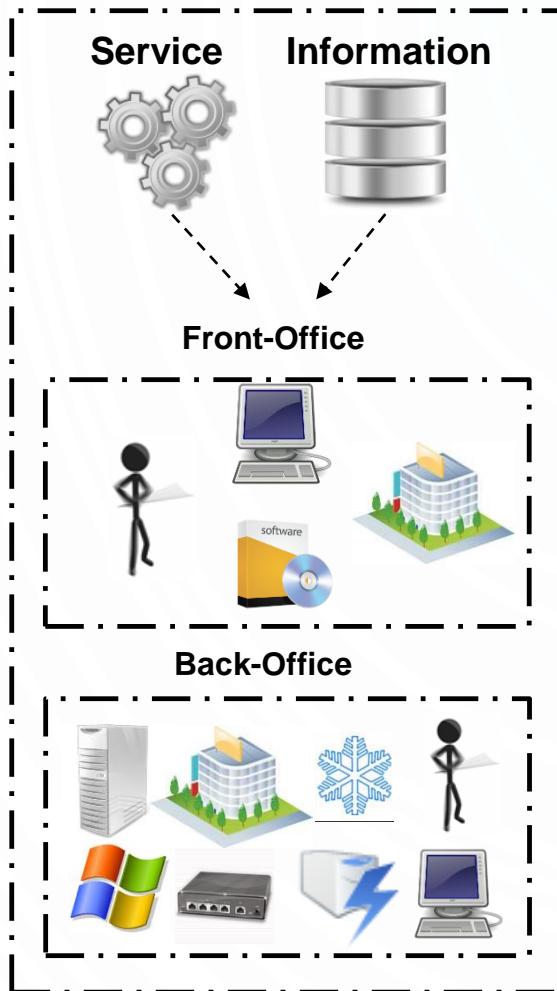
Base de données N°1 Base de données N°2





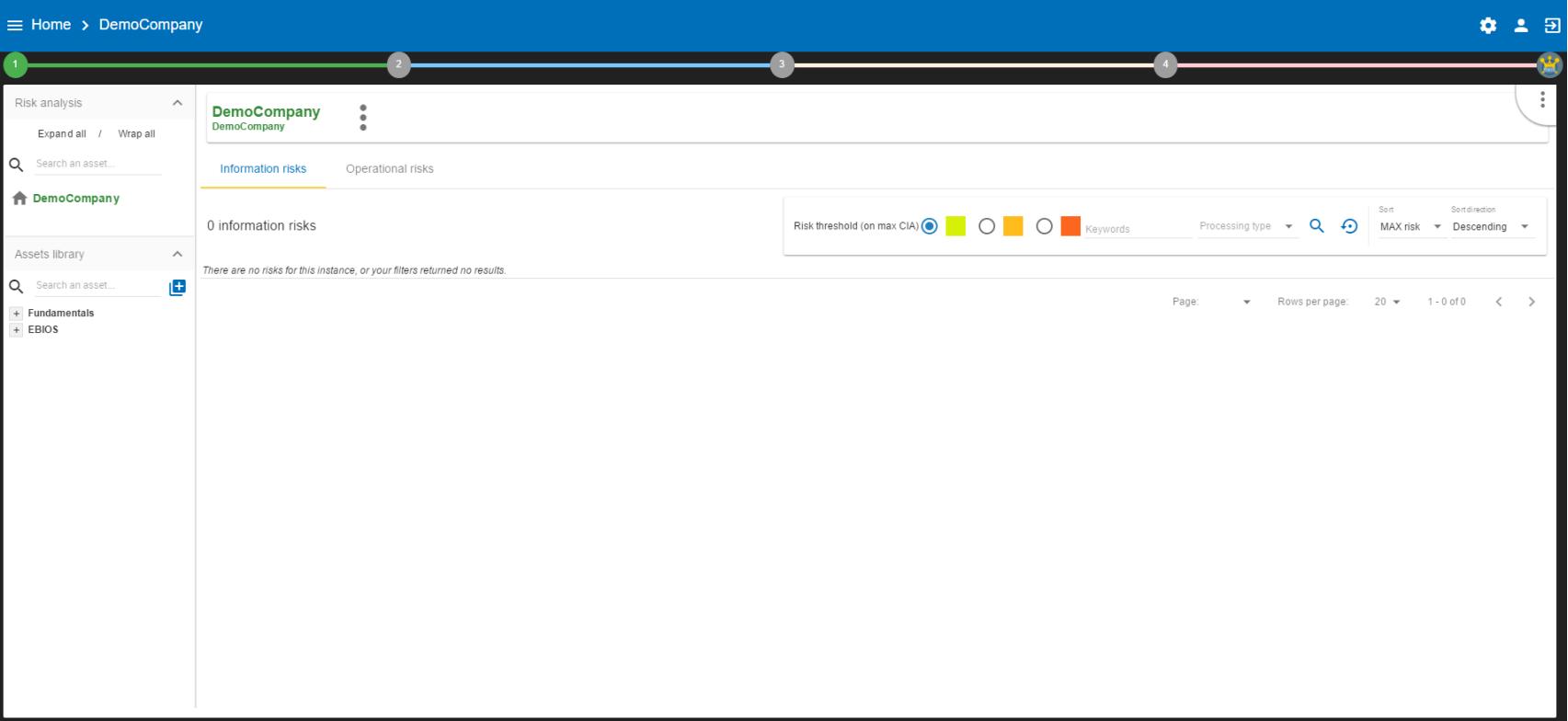
cases.lu
Secure. Innovate. Lead.

CASES MODELLING



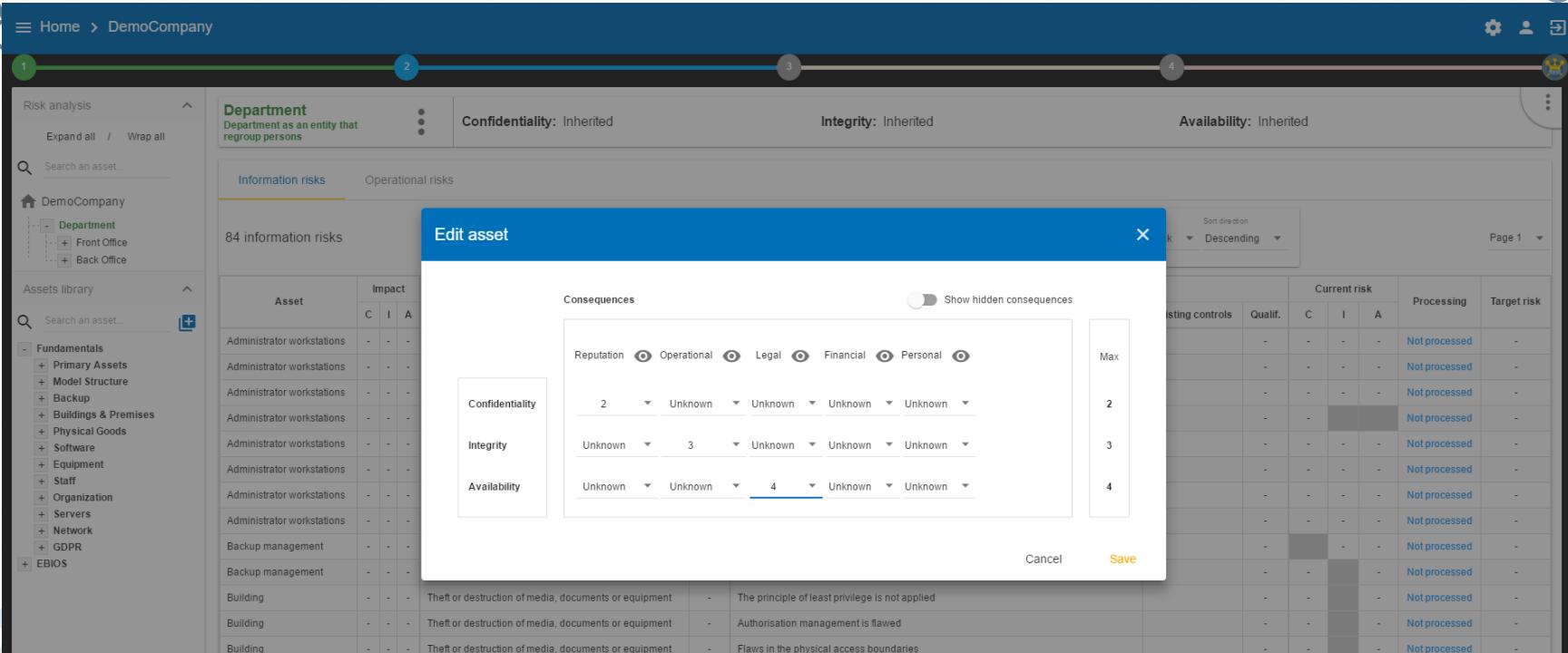
- **Service**
 - Front Office
 - Bureau du service
 - Employés
 - Postes de travail utilisateurs
 - Logiciel spécifique
 - Maintenance logiciel spécifique
- **Back Office**
 - Bâtiment
 - Salle informatique
 - Administrateur système
 - Postes de travail admin
 - Gestion serveurs
 - Gestion des backups
 - Réseau & télécom
 - Organisation informatique
 - Développements logiciels

2.1 – IDENTIFICATION OF ASSETS, VULNERABILITIES AND IMPACTS



- Main view of MONARC
 - Creation of a risk model
- Link with ISO 27005:2011
 - Identification of assets: Chapitre 8.2.2
 - Identification of vulnerabilities: Chapitre 8.2.5

2.1 – IDENTIFICATION OF ASSETS, VULNERABILITIES AND IMPACTS



The screenshot displays the MONARC software interface. At the top, there's a navigation bar with 'Home > DemoCompany'. Below it is a search bar and a sidebar for 'Risk analysis' and 'Assets library'. The main area shows a table of 'Information risks' for 'DemoCompany'. One row is selected, opening a modal dialog titled 'Edit asset' for 'Administrator workstations'. The dialog contains sections for 'Consequences' (with tabs for Confidentiality, Integrity, and Availability) and a note about least privilege principle. The background table lists various assets like 'Administrator workstations', 'Backup management', and 'Building' with their respective risk levels and descriptions.

- Main view of MONARC
 - Identification of impacts and consequences
- Link with ISO 27005:2011
 - Identification of Impacts: Chapter 8.3.2



cases.lu
Secure. Innovate. Lead.

2.2 – SYNTHESIS OF ASSETS / IMPACTS

The screenshot shows the cases.lu software interface for risk analysis. A context modeling dialog is open, with the 'Identification of assets, vulnerabilities and impacts appreciation' checkbox selected. Below it, a 'Synthesis of assets / impacts' dialog is open, titled 'Synthesis of assets / impacts'. This dialog contains a table with columns for Asset, Impact (C, I, A), and a large text area for notes. The notes section contains three entries:

Asset	Impact	Notes
Administrator workstations	C - -	Theft or destruction of media, documents or equipment
Administrator workstations	I - -	Authorisation management is flawed
Administrator workstations	A - -	Flaws in the physical access boundaries
Administrator workstations	C - -	Abuse of rights
Administrator workstations	I - -	No supervision of third-party access (supplier, cleaner, etc.)

At the bottom right of the dialog are 'Cancel' and 'Save' buttons. In the background, there's a main dashboard with sections for Risk analysis, DemoCompany (84 information risks), and an Assets library (Fundamentals, Physical Goods, etc.). A navigation bar at the top shows steps 1 through 4.

- Content justifying the choice of assets and impacts
- Designed to complete the deliverable

DEMO



cases.lu
Secure. Innovate. Lead.

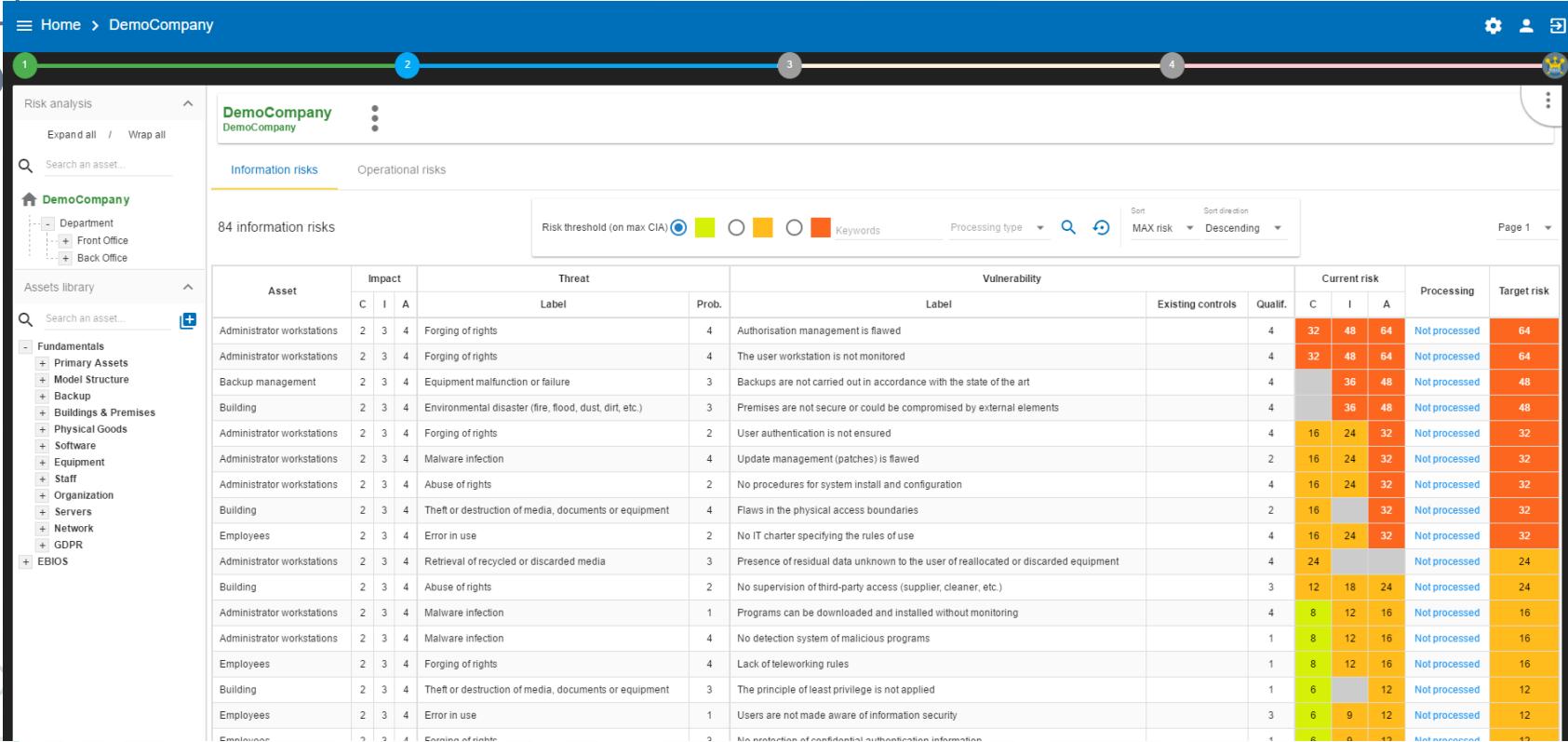
2.3 – DELIVERABLE: MODEL VALIDATION

The screenshot shows the cases.lu software interface. At the top, there's a navigation bar with 'Home > DemoCompany'. Below it is a sidebar with sections like 'Risk analysis' and 'Assets library'. The main area has a 'Context modeling' panel open, which includes a checklist for 'Identification of assets, vulnerabilities and impacts appreciation' and 'Synthesis of assets / impacts'. A 'Deliverable' dialog box is overlaid on the screen, containing fields for 'Status' (set to 'Final'), 'Version' (1.0), 'Classification' (Confidential), 'Document name' (Context Modelling Report), 'Client manager(s)' (M. Tee, M. Bond), and 'Security consultant(s)' (M. Mee). At the bottom of the dialog are 'Cancel' and 'Save' buttons. In the background, there's a table titled 'Sort direction' with columns for 'Existing controls', 'Qualif.', 'Current risk' (with sub-columns C, I, A), 'Processing', and 'Target risk'. The table rows show various status entries like 'Not processed'.

- Contains the important, primary assets of the model (impact criteria defined)
- Contains the synthesis of assets and impacts
- Export format: Microsoft Word

DEMO

3.1 – ESTIMATION, EVALUATION AND RISK TREATMENT



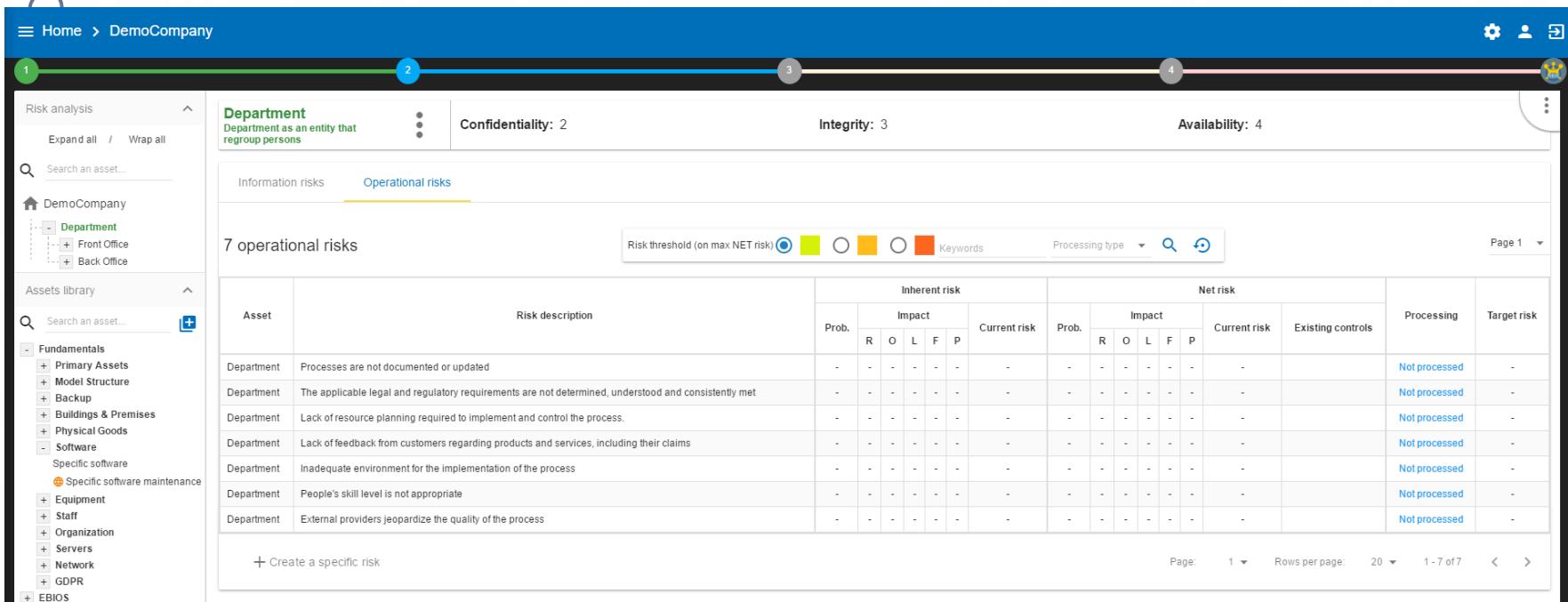
The screenshot shows the MONARC software interface for 'DemoCompany'. The left sidebar contains navigation links for 'Risk analysis' (with 'Expand all' and 'Wrap all' options), a search bar ('Search an asset...'), and an 'Assets library' section listing categories like 'Fundamentals', 'Physical Goods', 'Software', etc. The main content area displays '84 information risks' under the 'Information risks' tab. It includes filters for 'Risk threshold (on max CIA)' (using colored circles for Confidentiality, Integrity, and Availability) and 'Keywords'. A table lists risks categorized by Asset (e.g., Administrator workstations, Backup management, Building, Employees), Threat (e.g., Forging of rights, Malware infection, Abuse of rights), and Vulnerability (e.g., Authorisation management is flawed, Backups are not carried out in accordance with the state of the art). The table also shows Current risk scores (C, I, A) and processing status (e.g., Not processed, 64). A legend at the bottom right indicates that green, yellow, and orange colors correspond to different risk levels or categories.

Asset	Impact			Threat		Vulnerability			Current risk			Processing	Target risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	2	3	4	Forging of rights	4	Authorisation management is flawed			32	48	64	Not processed	64
Administrator workstations	2	3	4	Forging of rights	4	The user workstation is not monitored			32	48	64	Not processed	64
Backup management	2	3	4	Equipment malfunction or failure	3	Backups are not carried out in accordance with the state of the art			36	48		Not processed	48
Building	2	3	4	Environmental disaster (fire, flood, dust, dirt, etc.)	3	Premises are not secure or could be compromised by external elements			36	48		Not processed	48
Administrator workstations	2	3	4	Forging of rights	2	User authentication is not ensured			16	24	32	Not processed	32
Administrator workstations	2	3	4	Malware infection	4	Update management (patches) is flawed			16	24	32	Not processed	32
Administrator workstations	2	3	4	Abuse of rights	2	No procedures for system install and configuration			16	24	32	Not processed	32
Building	2	3	4	Theft or destruction of media, documents or equipment	4	Flaws in the physical access boundaries			16	24	32	Not processed	32
Employees	2	3	4	Error in use	2	No IT charter specifying the rules of use			16	24	32	Not processed	32
Administrator workstations	2	3	4	Retrieval of recycled or discarded media	3	Presence of residual data unknown to the user of reallocated or discarded equipment			24			Not processed	24
Building	2	3	4	Abuse of rights	2	No supervision of third-party access (supplier, cleaner, etc.)			12	18	24	Not processed	24
Administrator workstations	2	3	4	Malware infection	1	Programs can be downloaded and installed without monitoring			8	12	16	Not processed	16
Administrator workstations	2	3	4	Malware infection	4	No detection system of malicious programs			8	12	16	Not processed	16
Employees	2	3	4	Forging of rights	4	Lack of teleworking rules			8	12	16	Not processed	16
Building	2	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied			6		12	Not processed	12
Employees	2	3	4	Error in use	1	Users are not made aware of information security			6	9	12	Not processed	12
Employee	2	3	4	Forging of rights	2	No protection of confidential authentication information			6	9	12	Not processed	12

- Main View of MONARC
 - Evaluation of some information risks.

DEMO

3.1 – ESTIMATION, EVALUATION AND RISK TRAITEMENT

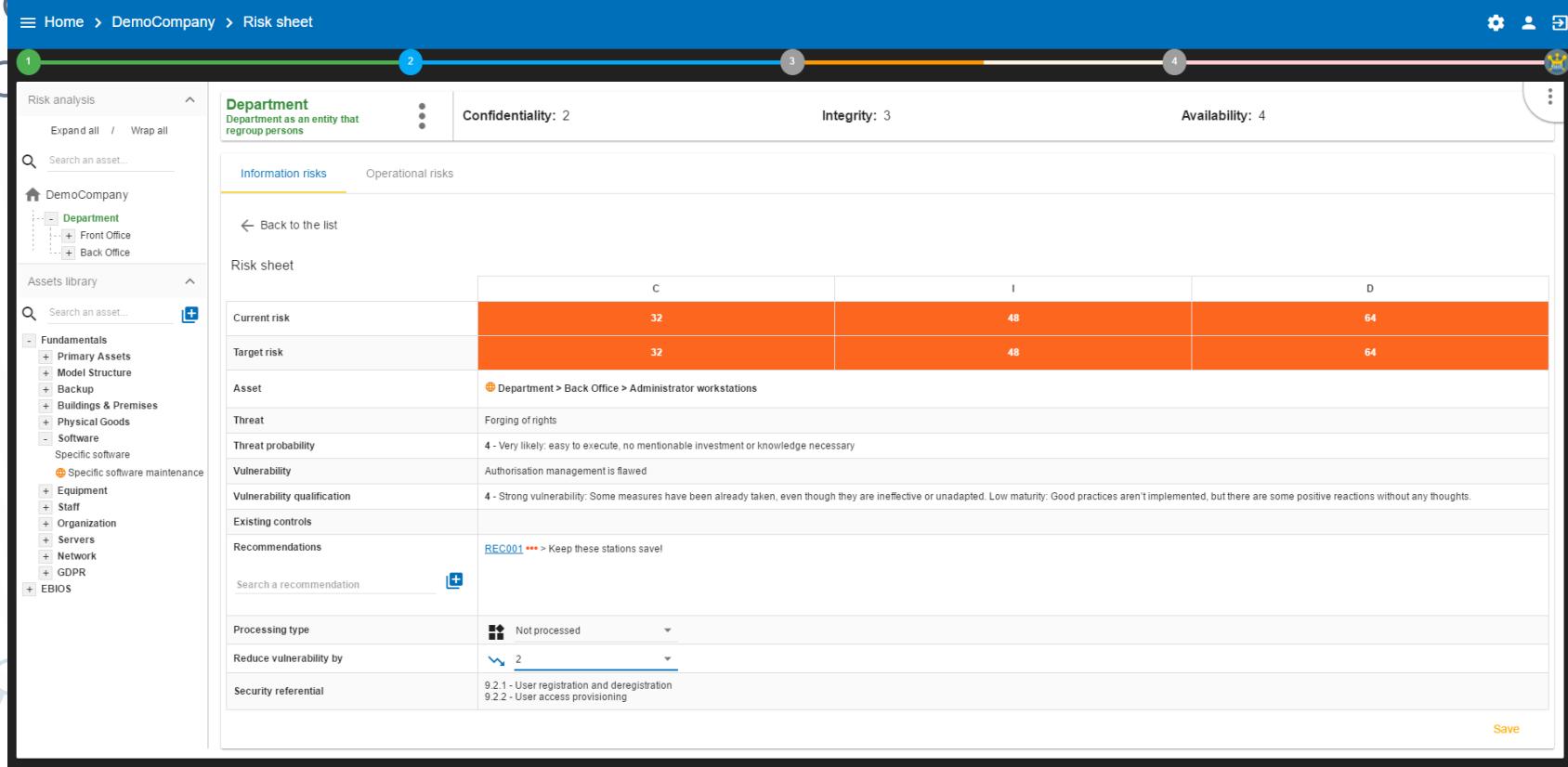


The screenshot shows the main view of the MONARC risk management system. The top navigation bar includes 'Home' and 'DemoCompany'. The left sidebar has sections for 'Risk analysis' (with 'Expand all' and 'Wrap all' buttons), a search bar ('Search an asset...'), and an 'Assets library' with categories like 'Fundamentals' (Primary Assets, Model Structure, Backup, Buildings & Premises, Physical Goods, Software, Specific software, Specific software maintenance), 'Equipment', 'Staff', 'Organization', 'Servers', 'Network', 'GDPR', and 'EBIOS'. The main content area displays '7 operational risks' for the 'Department' asset. The 'Operational risks' tab is selected. The table has columns for Asset (Department), Risk description, Inherent risk (Prob., Impact R, O, L, F, P, Current risk), Net risk (Prob., Impact R, O, L, F, P, Current risk, Existing controls), Processing, and Target risk. Each row lists a specific risk: 'Processes are not documented or updated', 'The applicable legal and regulatory requirements are not determined, understood and consistently met', 'Lack of resource planning required to implement and control the process.', 'Lack of feedback from customers regarding products and services, including their claims', 'Inadequate environment for the implementation of the process', 'People's skill level is not appropriate', and 'External providers jeopardize the quality of the process'. A 'Create a specific risk' button is at the bottom left, and page navigation controls are at the bottom right.

- Main View of MONARC
 - Evaluation of some operational risks

DEMO

3.1 – ESTIMATION, EVALUATION AND RISK TREATMENT



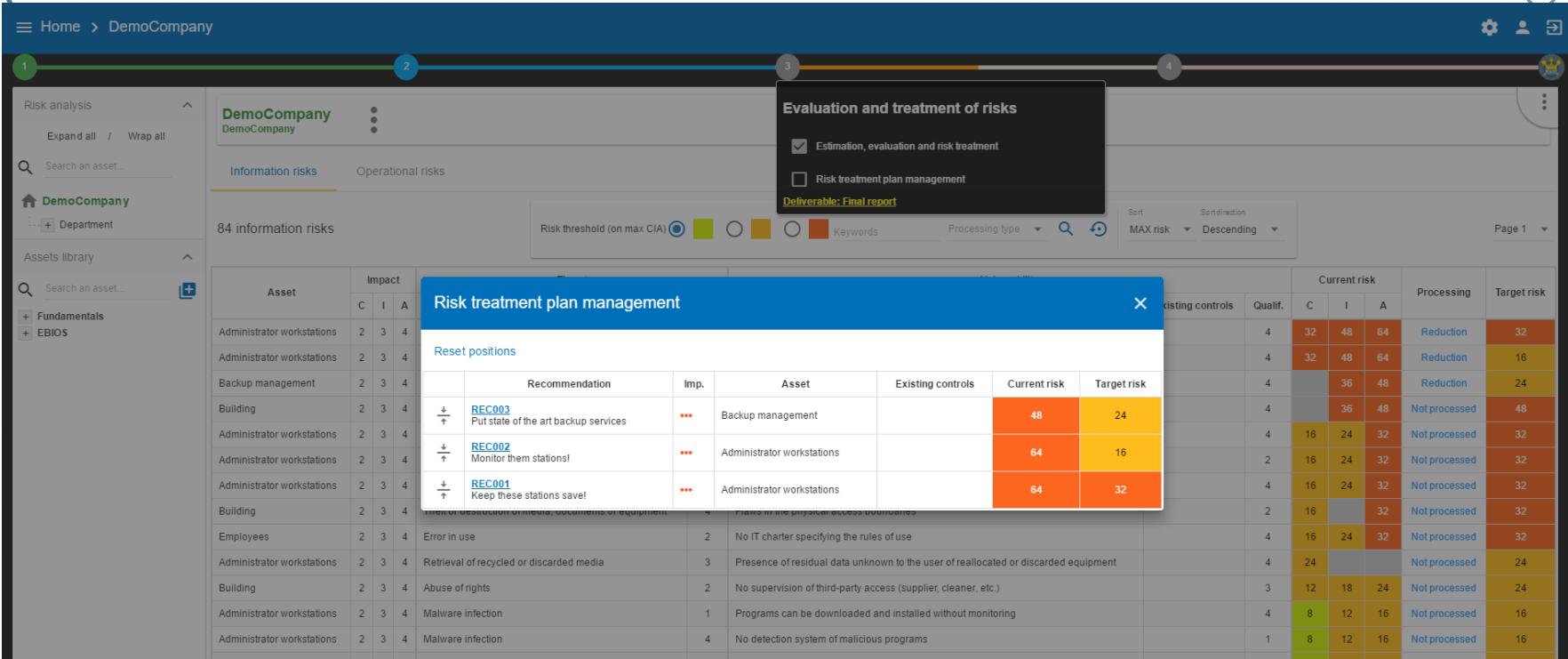
The screenshot shows the Risk sheet for the 'Department' entity. The navigation bar indicates the path: Home > DemoCompany > Risk sheet. The main area displays the following information:

- Department:** Department as an entity that regroup persons. Confidence level: 2.
- Integrity:** 3.
- Availability:** 4.
- Risk sheet:**

	C	I	D
Current risk	32	48	64
Target risk	32	48	64
- Asset:** Department > Back Office > Administrator workstations.
- Threat:** Forging of rights.
- Threat probability:** 4 - Very likely: easy to execute, no mentionable investment or knowledge necessary.
- Vulnerability:** Authorisation management is flawed.
- Vulnerability qualification:** 4 - Strong vulnerability: Some measures have been already taken, even though they are ineffective or unadapted. Low maturity: Good practices aren't implemented, but there are some positive reactions without any thoughts.
- Existing controls:** None listed.
- Recommendations:** RECO001 *** > Keep these stations save!
- Processing type:** Not processed.
- Reduce vulnerability by:** 2.
- Security referential:** 9.2.1 - User registration and deregistration
9.2.2 - User access provisioning.

- List of risks
- Creation of recommendations

3.2 –MANAGEMENT OF PLAN FOR RISK TREATMENT



The screenshot shows the cases.lu software interface for risk management. A modal window titled "Risk treatment plan management" is open, displaying a table of recommendations:

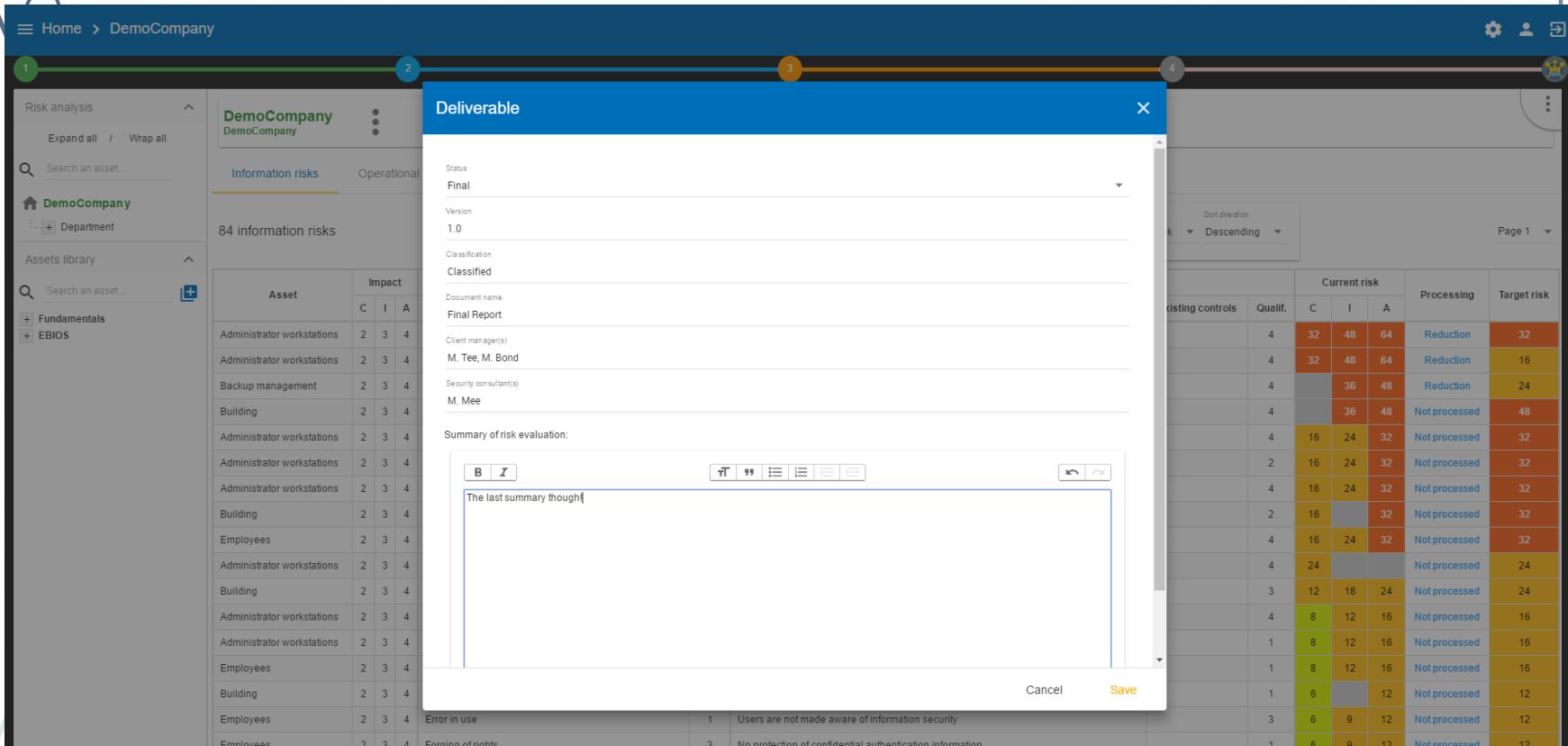
	Recommendation	Imp.	Asset	Existing controls	Current risk	Target risk
REC003	Put state of the art backup services	***	Backup management		48	24
REC002	Monitor them stations!	***	Administrator workstations		64	16
REC001	Keep these stations save!	***	Administrator workstations		64	32

The main interface shows a navigation bar with "Home > DemoCompany". The left sidebar includes sections for "Risk analysis", "Information risks" (selected), "Operational risks", "Assets library", and "EBIOS". The central area displays "84 information risks" and a "Risk treatment plan management" section with checkboxes for "Estimation, evaluation and risk treatment" and "Risk treatment plan management".

- List of all the risks that have a recommendation
- Both: information risks and operational risks

DEMO

3.3 – DELIVERABLE: FINAL REPORT



The screenshot shows the cases.lu software interface. A modal window titled "Deliverable" is open in the center. The modal contains fields for Status (Final), Version (1.0), Classification (Classified), Document name (Final Report), Client manager(s) (M. Tee, M. Bond), and Security consultant(s) (M. Mee). Below these fields is a "Summary of risk evaluation:" section with a rich text editor containing the text "The last summary though!". At the bottom of the modal are "Cancel" and "Save" buttons. The background shows a navigation bar with "Home > DemoCompany" and a sidebar with sections like "Risk analysis", "Information risks", "Operational", "Assets library", and a table of 84 information risks. To the right of the modal, there is a large table titled "Existing controls" with columns for Qualif., Current risk (C, I, A), Processing, and Target risk. The table lists various risk items with their respective values.

Existing controls	Qualif.	Current risk			Processing	Target risk
		C	I	A		
	4	32	48	64	Reduction	32
	4	32	48	64	Reduction	16
	4	36	48	64	Reduction	24
	4	36	48	64	Not processed	48
	4	16	24	32	Not processed	32
	2	16	24	32	Not processed	32
	4	16	24	32	Not processed	32
	2	16	24	32	Not processed	32
	4	16	24	32	Not processed	32
	4	24	32	48	Not processed	24
	3	12	18	24	Not processed	24
	4	8	12	16	Not processed	16
	1	8	12	16	Not processed	16
	1	6	12	16	Not processed	12
	3	6	9	12	Not processed	12
	1	6	9	12	Not processed	12

- Complete list of all the collected information
- Possibility to add a summary for the analysis.
- Export format: Microsoft Word

DEMO

4.1 – MANAGEMENT OF THE IMPLEMENTATION PLAN FOR RISK TREATMENT

Home > DemoCompany > Implementation of the risk treatment plan

1 Risk analysis 2 Implementation of the risk treatment plan 3 Open the implementation history 4 Status

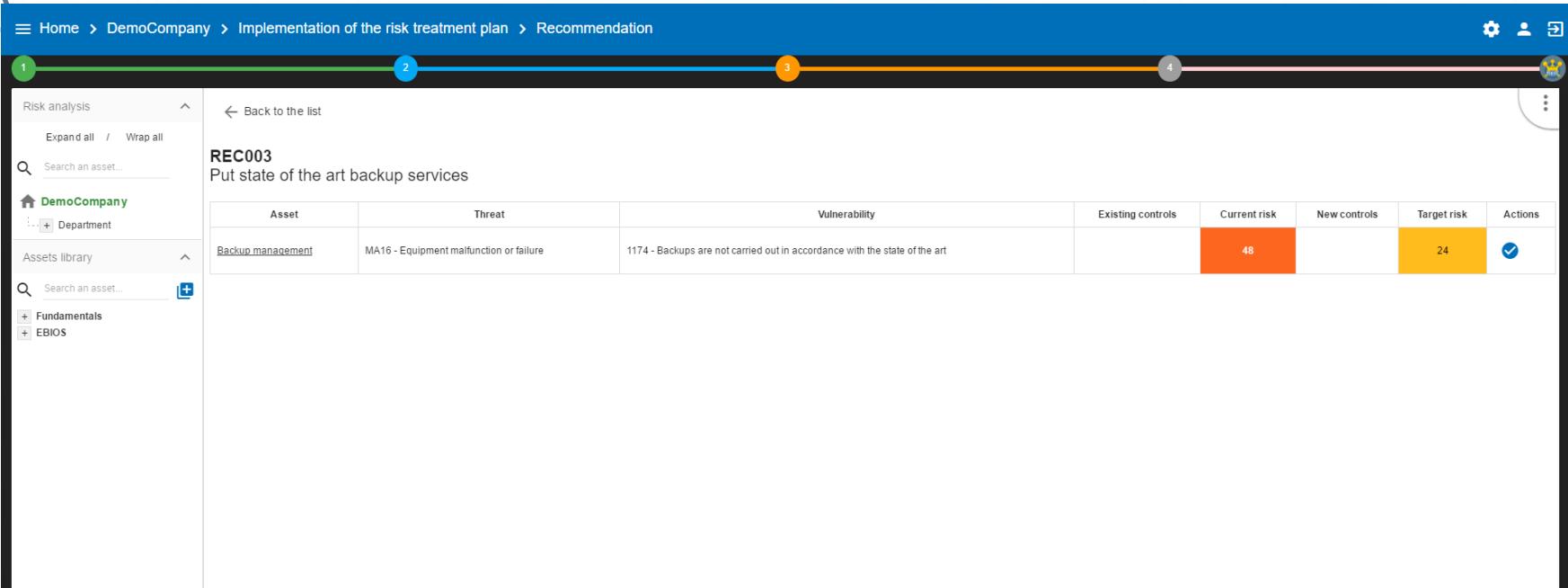
Implementation of the risk treatment plan

Open the implementation history

⌚	Recommendation	Imp.	Comment	Manager	Deadline	Status	Actions
⌚	REC003 Put state of the art backup services	...			jj-mm-yyyy	Coming	<input type="button" value=""/>
⌚	REC002 Monitor them stations!	...			jj-mm-yyyy	Coming	<input type="button" value=""/>
⌚	REC001 Keep these stations save!	...			jj-mm-yyyy	Coming	<input type="button" value=""/>

- Delegate a person in charge and fix deadlines for the implementation of each recommendation
- Validation risk by risk of their state change
- Change the value of the risk: the target risk becomes the actual risk

4.1 – MANAGEMENT OF THE IMPLEMENTATION PLAN FOR RISK TREATMENT



The screenshot shows a software interface for managing risk treatment plans. The top navigation bar includes 'Home', 'DemoCompany', 'Implementation of the risk treatment plan', and 'Recommendation'. On the left, there's a sidebar with 'Risk analysis' (expand all / wrap all), a search bar ('Search an asset...'), and sections for 'DemoCompany' (Department), 'Assets library' (Fundamentals, EBIOS), and another search bar ('Search an asset...'). The main content area displays a recommendation titled 'REC003 Put state of the art backup services'. It includes a table with columns: Asset, Threat, Vulnerability, Existing controls, Current risk, New controls, Target risk, and Actions. One row is shown: Backup management, MA16 - Equipment malfunction or failure, 1174 - Backups are not carried out in accordance with the state of the art, 48, 24, and a checked checkbox in the Actions column.

- Delegate a person in charge and fix deadlines for the implementation of each recommendation
- Validation risk by risk of their state change
- Change the value of the risk: the target risk becomes the actual risk



AGENDA

- ▶ What is MONARC ?
- ▶ Discovery and usage of the tool
- ▶ Run-through of the method
- ▶ **Tips & Tricks**



cases.lu
Secure. Innovate. Lead.

T&T: CREATION OF A RISK

The screenshot shows the cases.lu software interface. At the top, there is a navigation bar with links for Home, DemoCompany, Knowledge base, and other settings. Below the navigation is a horizontal bar with numbered circles (1, 2, 3, 4) corresponding to steps in the process. The main area is titled "Asset types" and contains a table of asset types. The table has columns for Status, Label, Code, Type, Description, and Actions (edit and delete icons). The data in the table includes:

Status	Label	Code	Type	Description	Actions
<input type="checkbox"/>	Company directory	SYS_ANU	Secondary	Company directory	
<input type="checkbox"/>	Business application	LOG_APP	Secondary	Custom business application or standard	
<input type="checkbox"/>	Other media	MAT_NELE	Secondary	Paper, slide, transparency, documentation, fax.	
<input type="checkbox"/>	Backup	OV_BACKUP	Secondary	Backup	
<input type="checkbox"/>	Building, office or premises	OV_BATI	Secondary	Building, office or premises	
<input type="checkbox"/>	Container	CONT	Primary	Asset container	
<input type="checkbox"/>	Decision maker	PER_DEC	Secondary	Decision maker	
<input type="checkbox"/>	Software development	OV_DEVELOPPEMENT	Secondary	Software development	
<input type="checkbox"/>	Developer	PER_DEV	Secondary	Developer	
<input type="checkbox"/>	Internet access device	SYS_INT	Secondary	Internet access device	
<input type="checkbox"/>	Paper document	OV_INFOPHY	Secondary	Information in physical form	
<input type="checkbox"/>	Operator / Maintenance	PER_EXP	Secondary	Operator / Maintenance	
<input type="checkbox"/>	Structure of the organisation	ORG_GFN	Secondary	Structure of the organisation	

1. Creation of an asset type
2. Creation of a threat
3. Creation of a vulnerability
4. Link assets, threats and vulnerability
5. Creation of an asset in the library
6. Use of an asset in the analysis

DEMO



cases.lu
Secure. Innovate. Lead.

T&T: IMPORT / EXPORT ASSETS

Home > DemoCompany



1 2 3 4

Risk analysis													
Expand all / Wrap all													
Search an asset...													
DemoCompany													
Department													
Assets library													
Search an asset...													
+ Fundamentals													
+ EBIOS													
84 information risks													
Asset		Impact		Threat		Vulnerability		Current risk					
C	I	A		Label	Prob.	Label	Existing controls	Qualif.	C	I	A	Processing	Target risk
Administrator workstations	2	3	4	Forging of rights	4	Authorisation management is flawed		4	32	48	64	Reduction	32
Administrator workstations	2	3	4	Forging of rights	4	The user workstation is not monitored		4	32	48	64	Reduction	16
Backup management	2	3	4	Equipment malfunction or failure	3	Backups are not carried out in accordance with the state of the art		4	36	48	64	Reduction	24
Building	2	3	4	Environmental disaster (fire, flood, dust, dirt, etc.)	3	Premises are not secure or could be compromised by external elements		4	36	48	Not processed	48	
Administrator workstations	2	3	4	Forging of rights	2	User authentication is not ensured		4	16	24	32	Not processed	32
Administrator workstations	2	3	4	Malware infection	4	Update management (patches) is flawed		2	16	24	32	Not processed	32
Administrator workstations	2	3	4	Abuse of rights	2	No procedures for system install and configuration		4	16	24	32	Not processed	32
Building	2	3	4	Theft or destruction of media, documents or equipment	4	Flaws in the physical access boundaries		2	16	24	32	Not processed	32
Employees	2	3	4	Error in use	2	No IT charter specifying the rules of use		4	16	24	32	Not processed	32
Administrator workstations	2	3	4	Retrieval of recycled or discarded media	3	Presence of residual data unknown to the user of reallocated or discarded equipment		4	24			Not processed	24
Building	2	3	4	Abuse of rights	2	No supervision of third-party access (supplier, cleaner, etc.)		3	12	18	24	Not processed	24
Administrator workstations	2	3	4	Malware infection	1	Programs can be downloaded and installed without monitoring		4	8	12	16	Not processed	16
Administrator workstations	2	3	4	Malware infection	4	No detection system of malicious programs		1	8	12	16	Not processed	16
Employees	2	3	4	Forging of rights	4	Lack of teleworking rules		1	8	12	16	Not processed	16

- Possibility to import and export assets:
 - From/into the library
 - From/into the analysis – with or without the evaluation.

DEMO