cases.lu
Secure. Innovate. Lead.

WORKSHOP MONARC
(OPTIMISED RISK ANALYSIS METHOD)

MONARC V2.0 TRAINING

INFO@CASES.LU

SECURITY MADEIN.LU

cases MONARC

SECURITYMADEIN.LU

cases.lu
Secure. Innovate. Lead.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

bigi
Syndicat Intercommunal de Gestion Informatique

SYVICOL

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

circl
Computer Incident Response Center Luxembourg

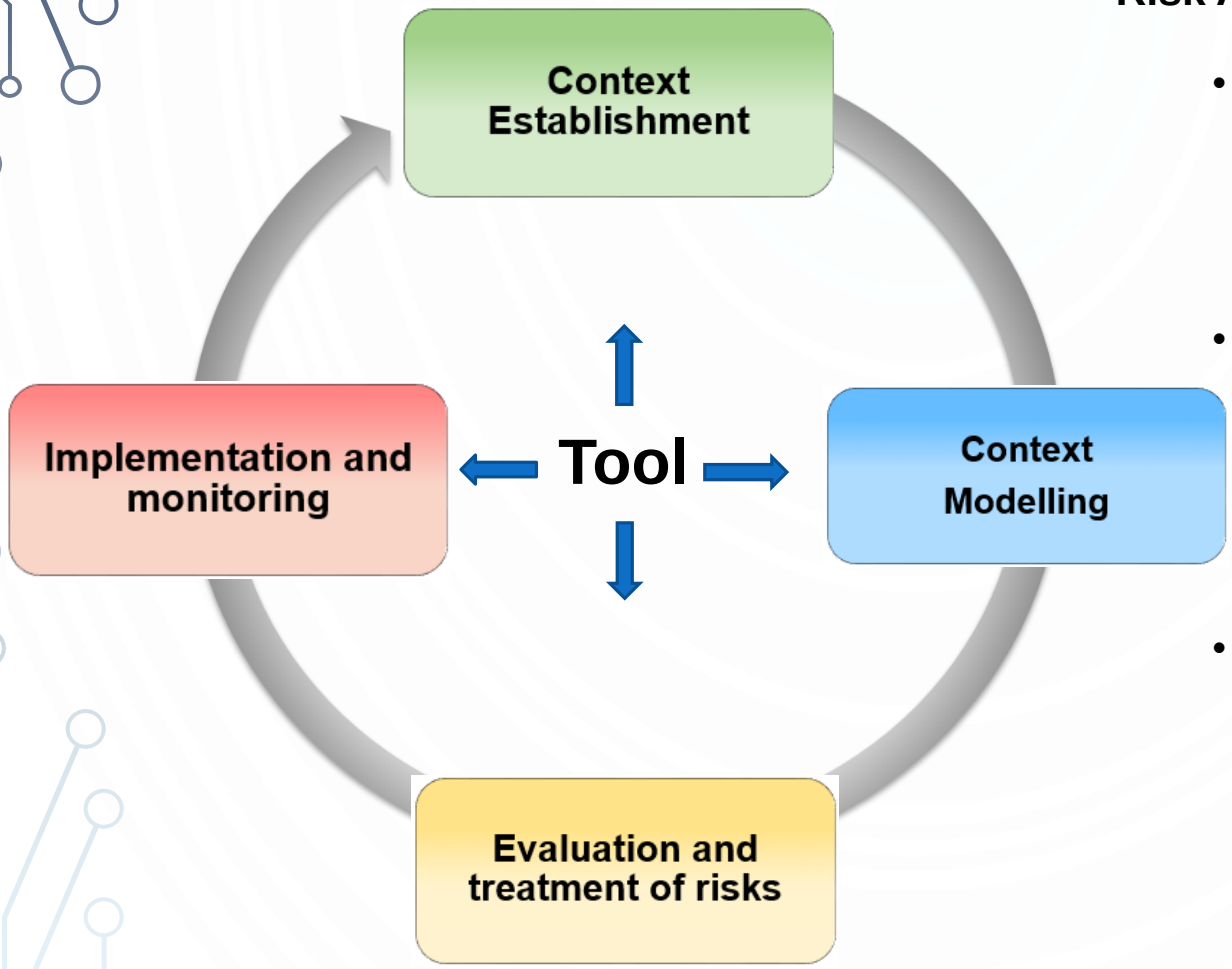
cases
Cyberworld Awareness and Security Enhancement Services

www.securitymadein.lu
www.cases.lu

AGENDA

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

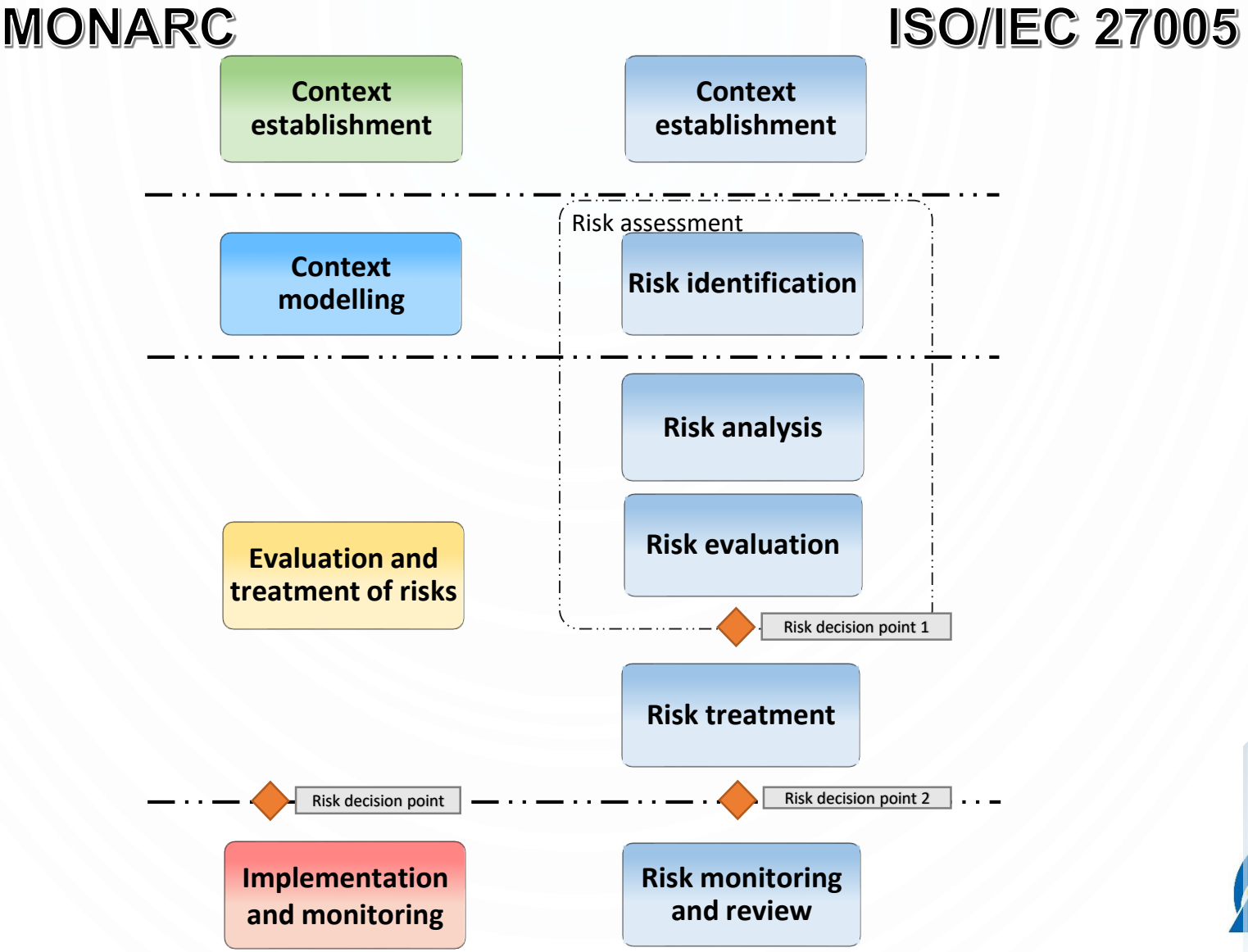
MONARC:
OPTIMISED RISK ANALYSIS METHOD



Risk Analysis Method

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

MONARC : THE METHOD



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 x M x V)

- Impact on the CIA
- Secondary Assets

Operational Risks (R = I x P)

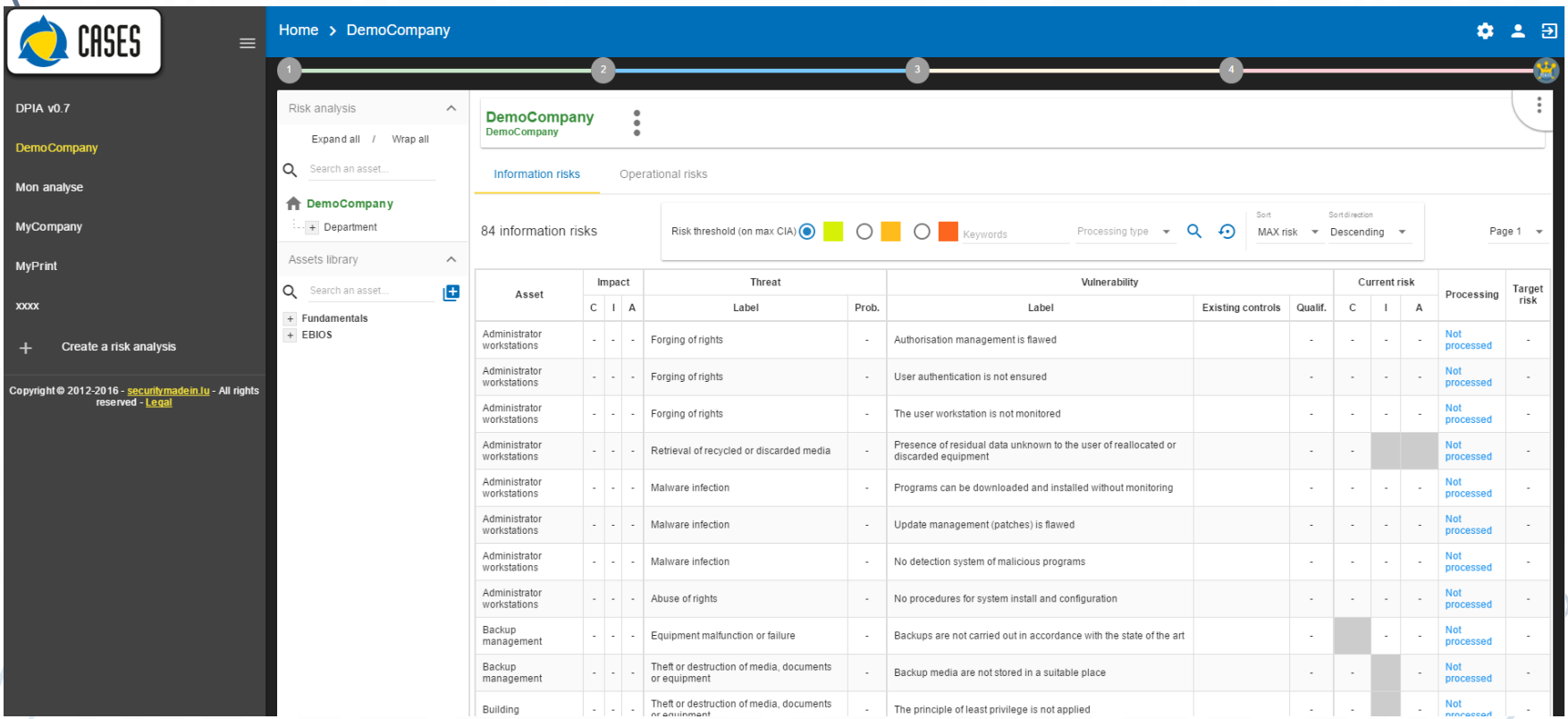
- Impact on the ROLFP
- Gross/Net
- Primary Assets

- **Sharing of Risk Models**
- **Optimised (models, delivrables, inheritance, globalisation)**

AGENDA

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

MAIN FEATURES/FUNCTIONALITIES



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	-

Démonstration

AGENDA

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

MONARC : LA MÉTHODE EN DÉTAILS

Context Establishment

- Risk Analysis Context
- Trends Evaluation
- Threat Assessment
- Synthesis of the trends and threats assessment
- Context of the risk management
- Definition of assessment criteria, acceptance and impact

Deliverable: Context Validation

Context Modelling

- Identification of assets, vulnerabilities and impact appreciation
- Synthesis of assets / impacts

Deliverable: Model Validation

Evaluation and treatment of risks

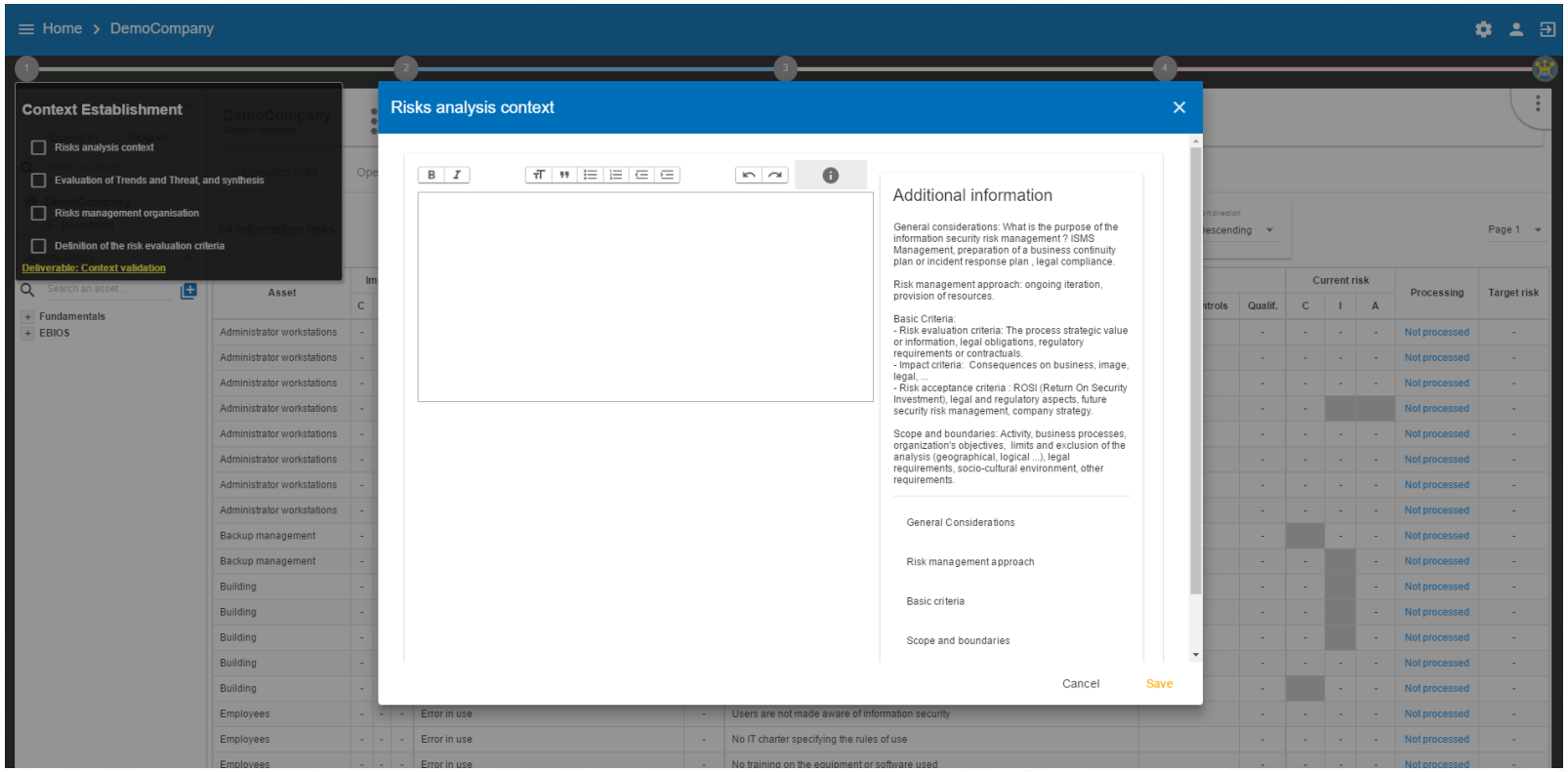
- Estimation, evaluation and risk treatment
- Management of plan for risk treatment

Deliverable: Final Report

Implementation and monitoring

- Management of the implementation plan for risk treatment

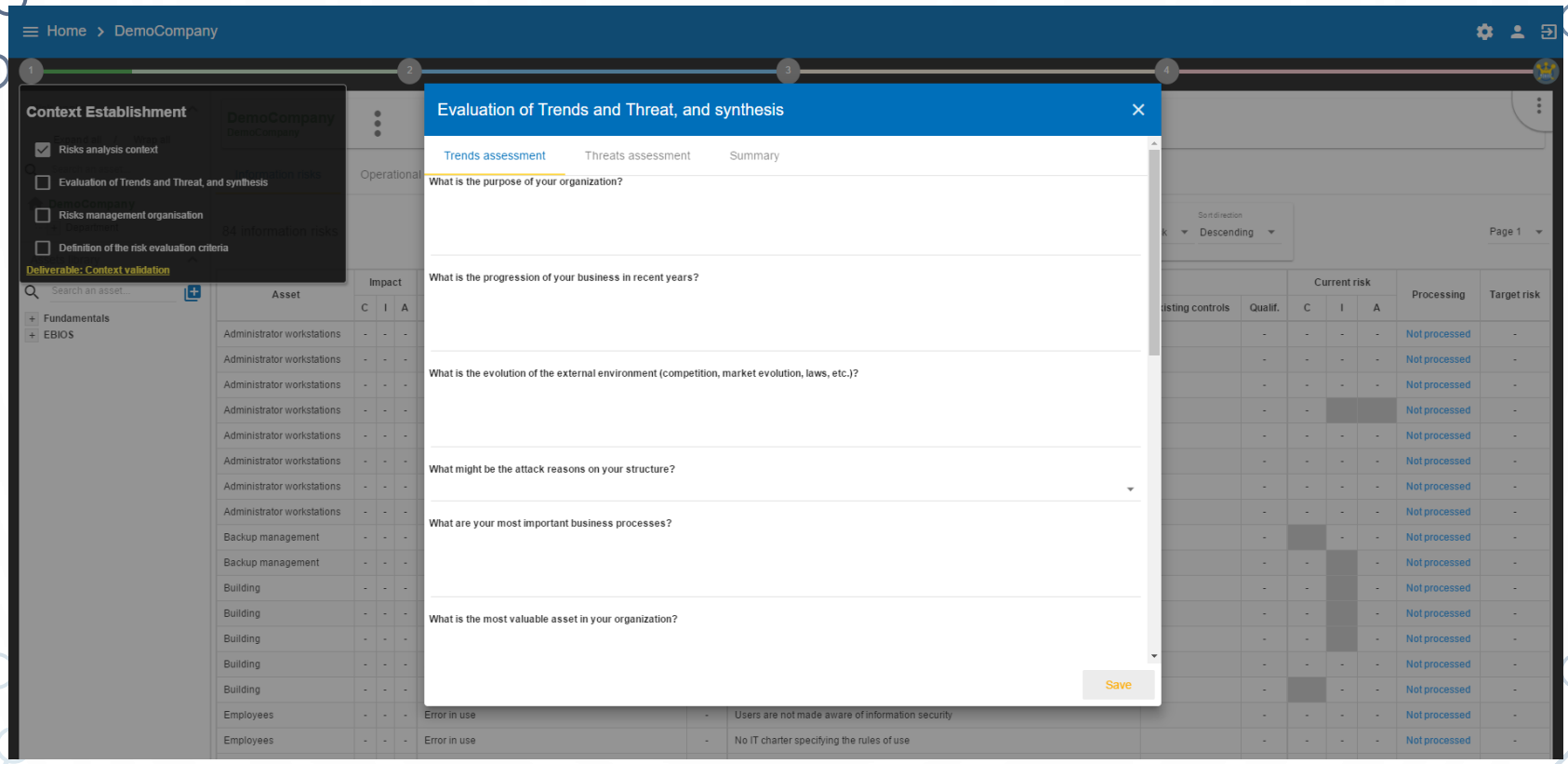
1.1 – CONTEXT OF THE RISK ANALYSIS



- Discovering the target organisation
- Links with ISO 27005:2011
  - Gereneral considerations : Chapter 7.1
  - Risk Management Approach : Chapter 7.2.1
  - Basic Criteria : Chapters 7.2.2, 7.2.3, 7.2.4
  - Targets and Limits : Chapter 7.3

DEMO

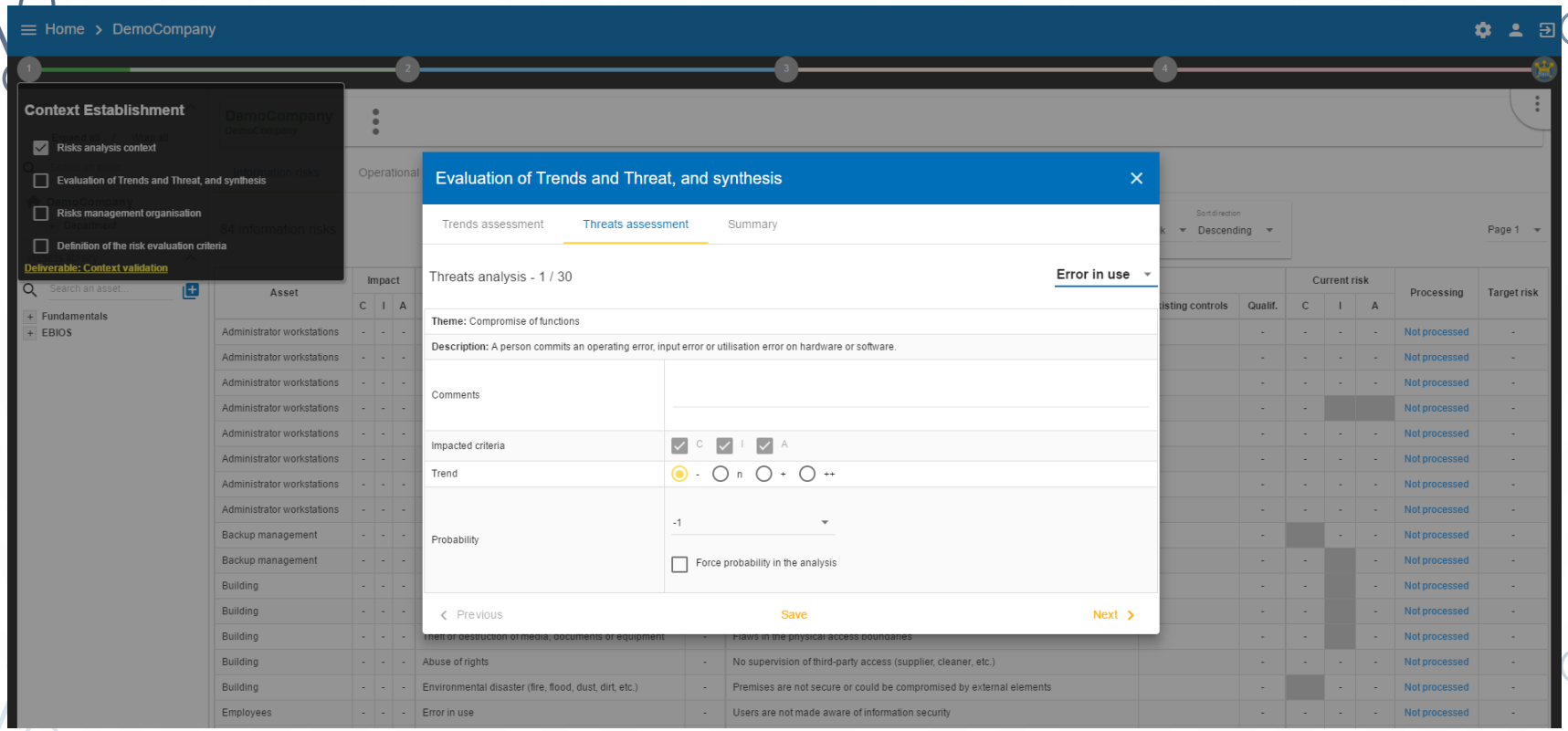
1.2 – EVALUATION OF TRENDS



- 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

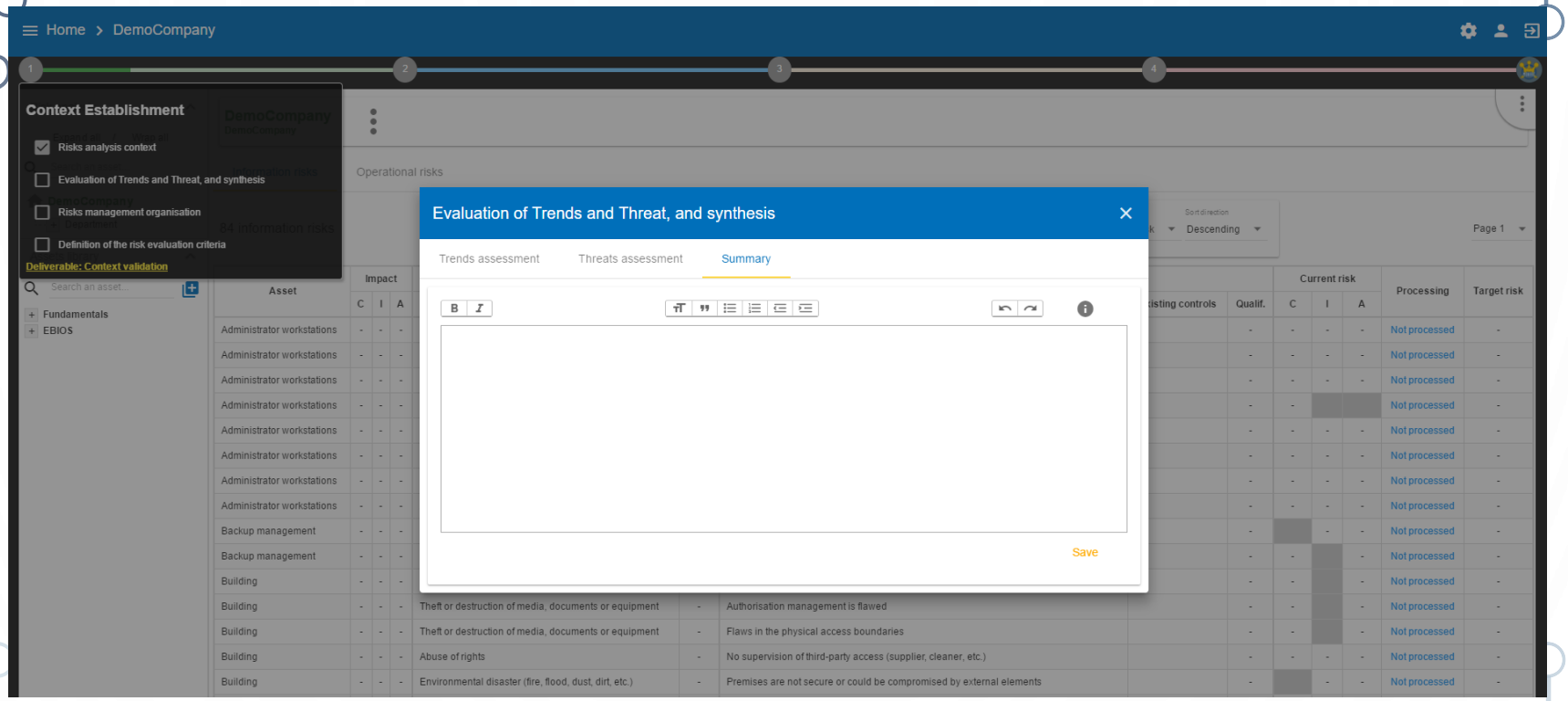
1.2 – EVALUATION OF THREATS



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

DEMO

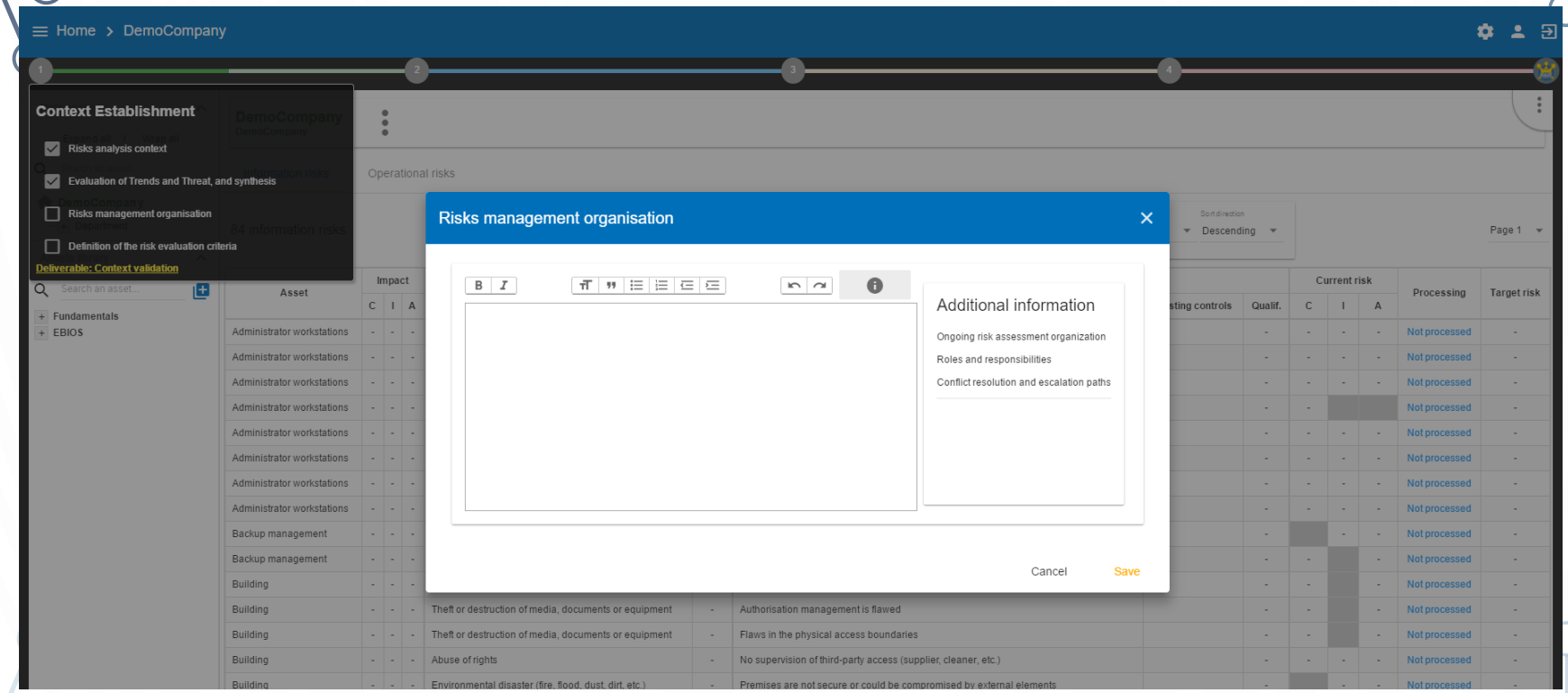
1.2 – SUMMARY



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

DEMO

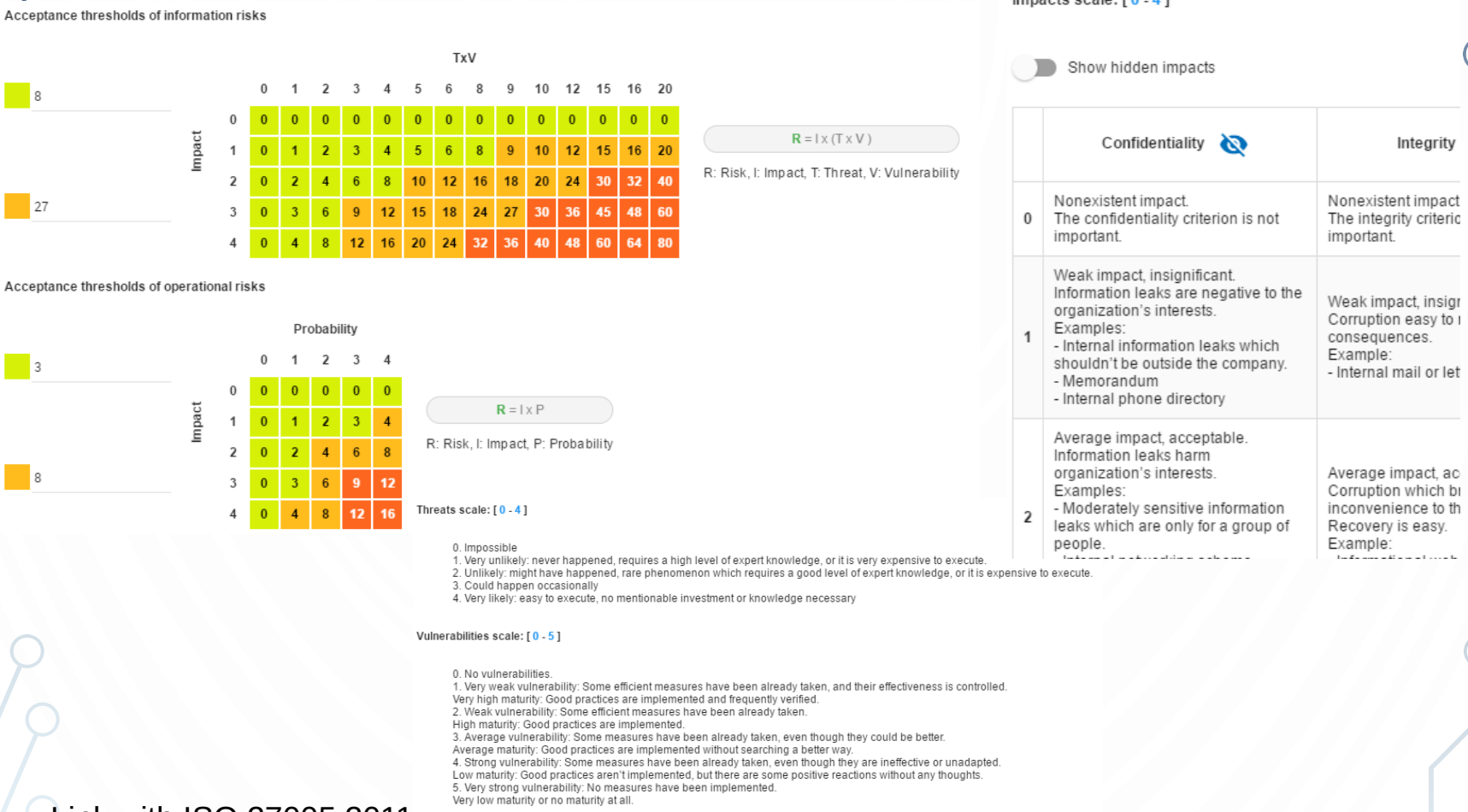
1.3 – ORGANISATION OF THE RISK MANAGEMENT



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

DEMO

1.4 – DEFINITION OF EVALUATION, ACCEPTANCE AND IMPACT CRITERIA



Acceptance thresholds of information risks

TxV

8

27

Impact \ 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 x (T x V)

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

Acceptance thresholds of operational risks

Probability

3

8

Impact \ Probability	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	6	8
3	0	3	6	9	12
4	0	4	8	12	16

R = I x 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.

Impacts scale: [0 - 4]

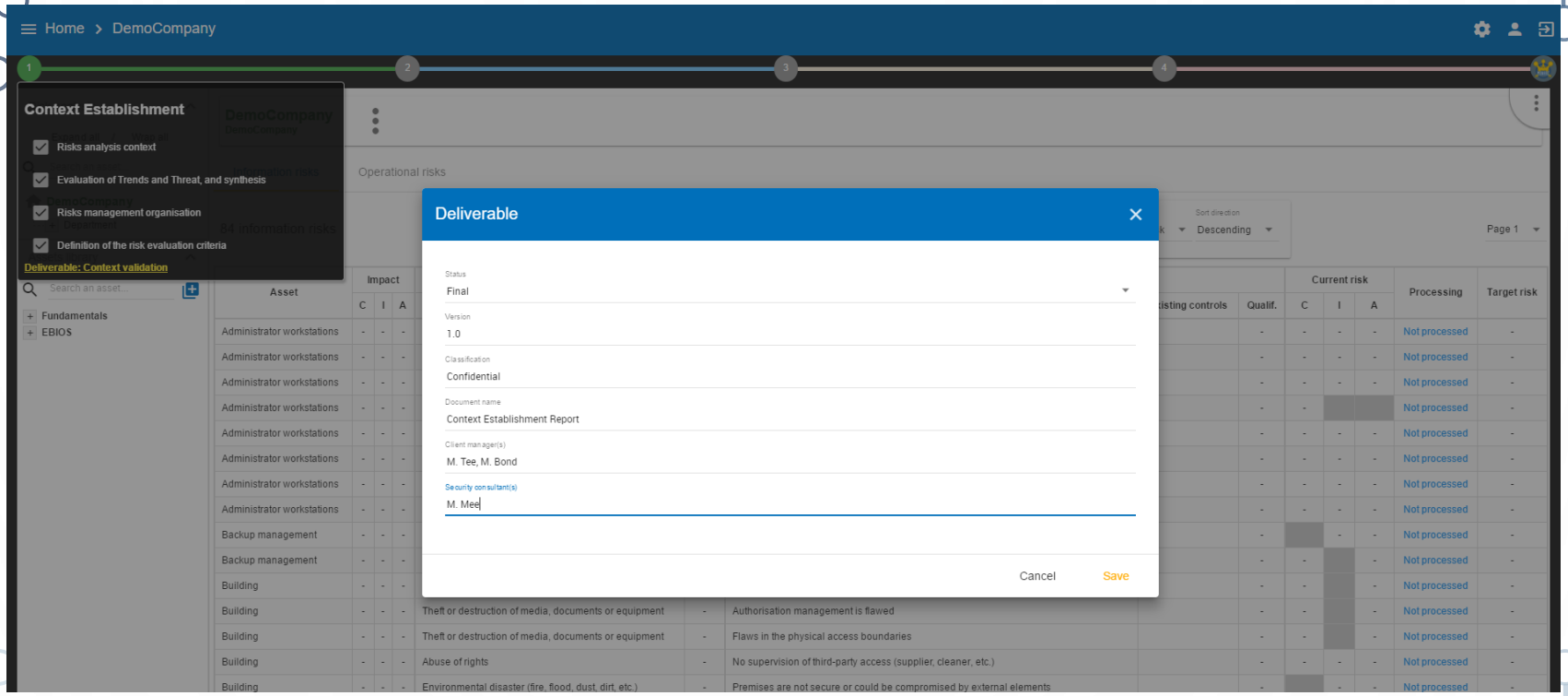
Show hidden impacts

	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 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 b inconvenience to th Recovery is easy. Example:

- Link with ISO 27005:2011
  - Organisation of risk management: Chapter 7.2,2, 7.2.3, 7.2.4

DEMO

1.5 – DELIVRABLE: CONTEXT VALIDATION



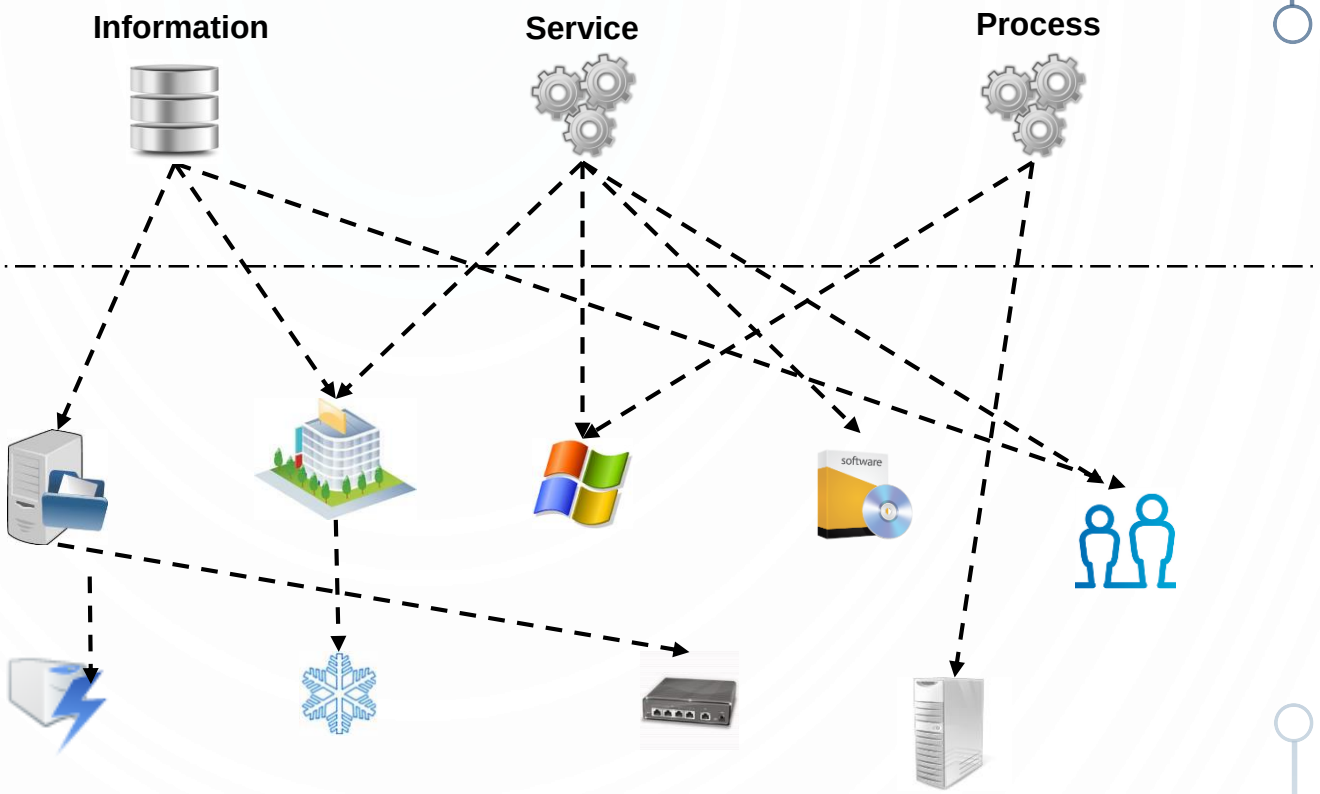
- Compile all the information collected during the context establishment
- Report is used to validate the collected information before the identification of risks starts.
- Export format: Microsoft Word

DEMO

2.1 – IDENTIFICATION OF ASSETS, VULNERABILITIES AND EVALUATION OF IMPACTS

Primary Assets
(Business)

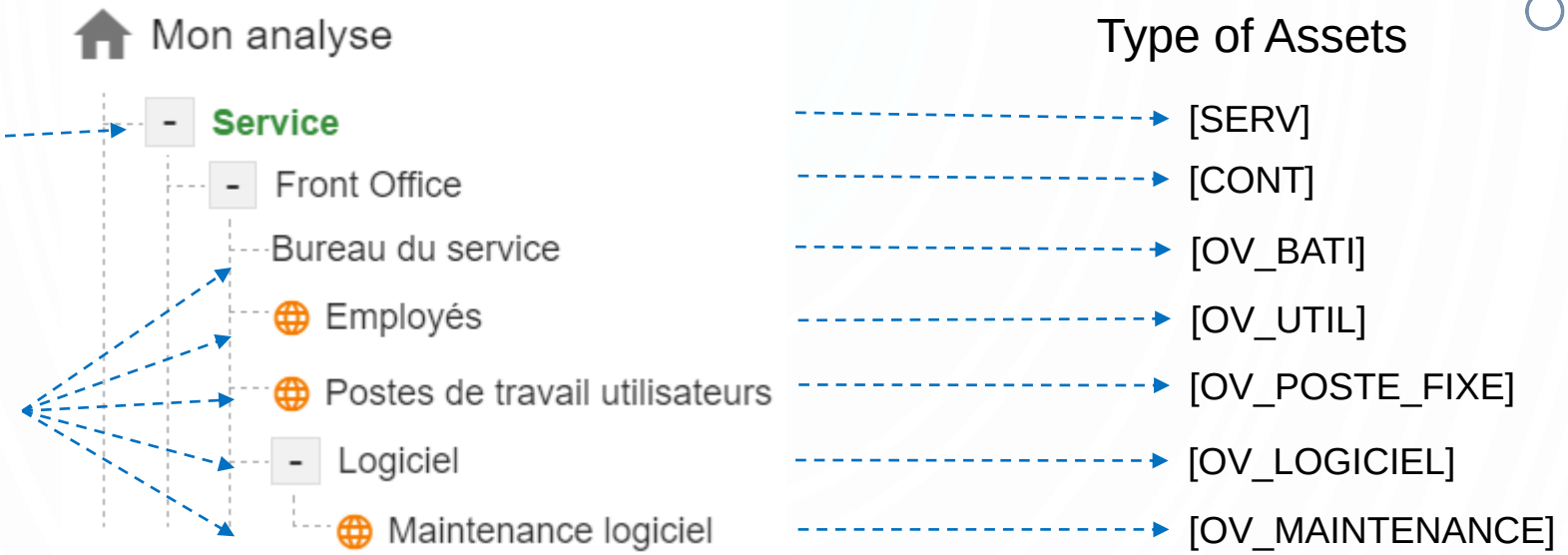
Secondary Assets
(Supporting)



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

FORMALISATION OF THE MODELLING

Hierarchy of Assets



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

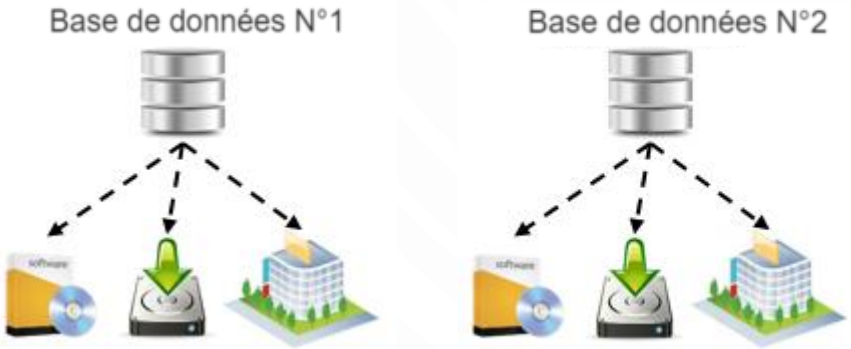
« GLOBAL » OR « LOCAL » ASSET

“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

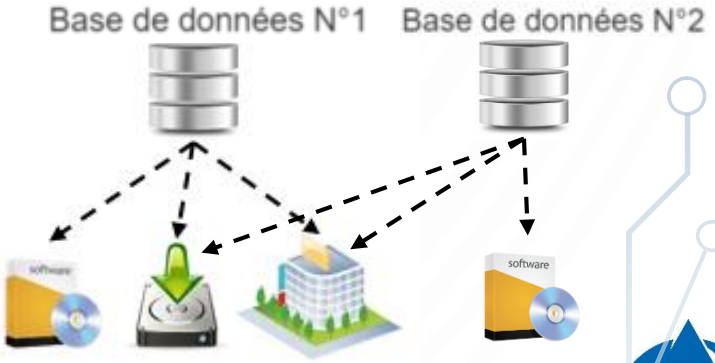


“Global”

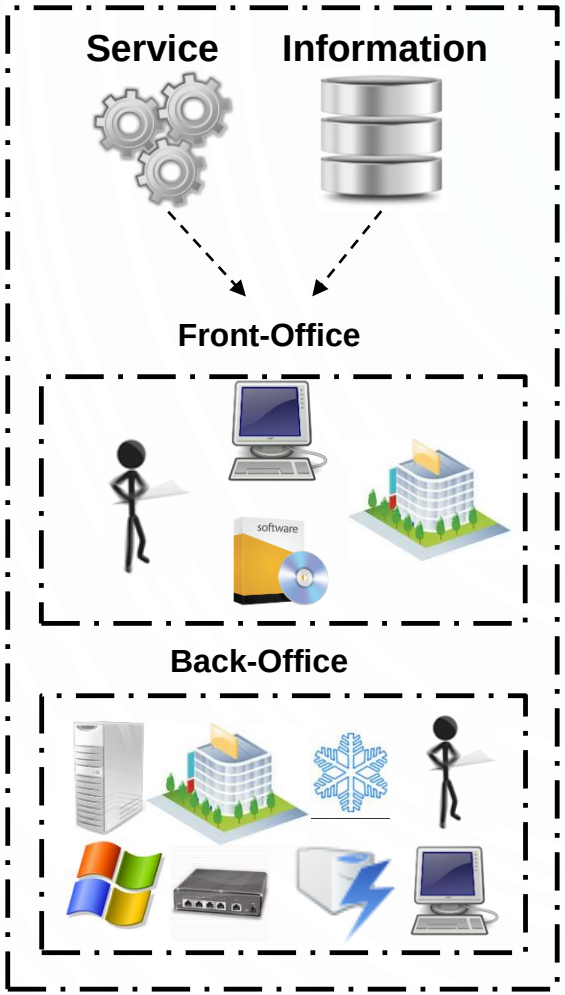
Mon analyse

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

21 risks

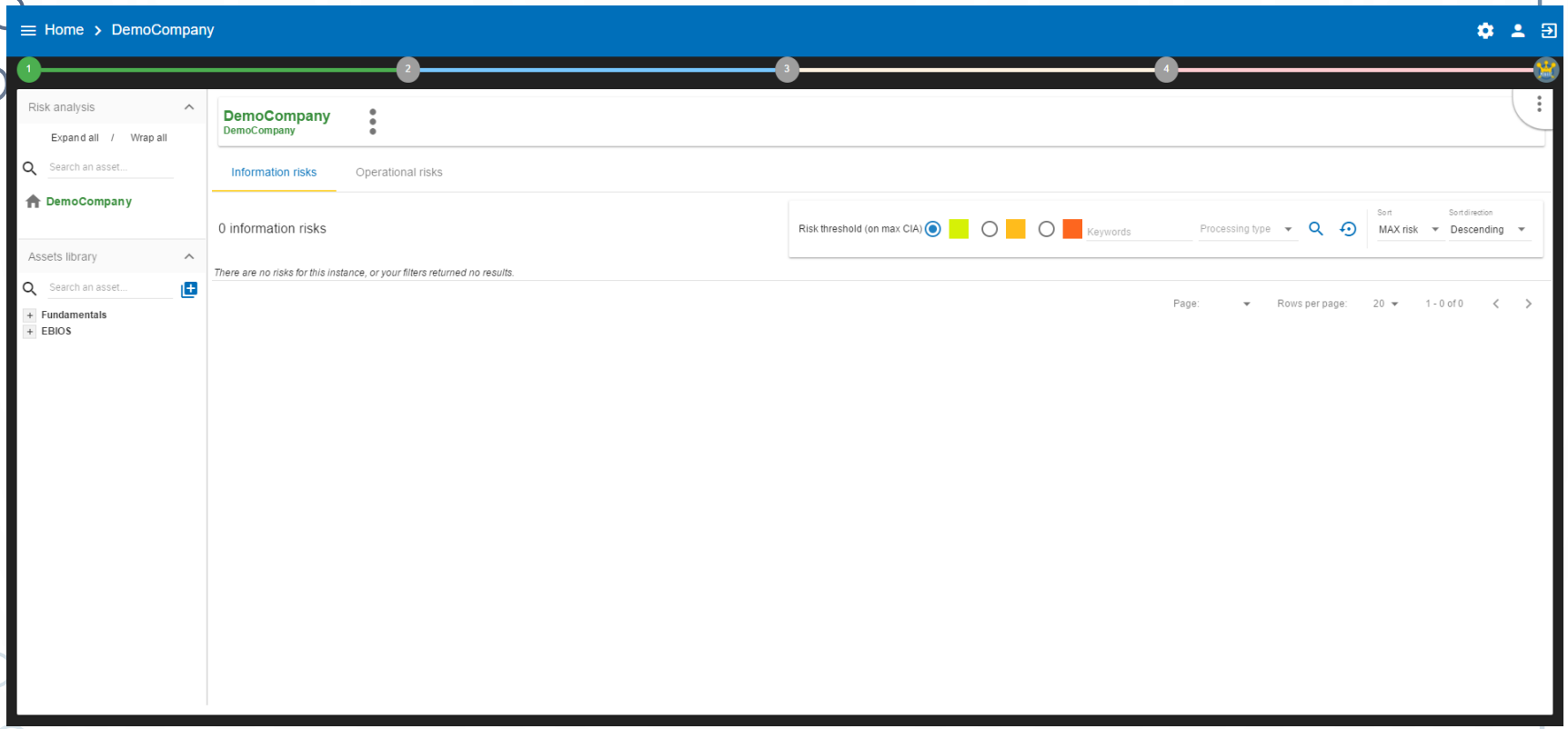


CASES MODELLING



- 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

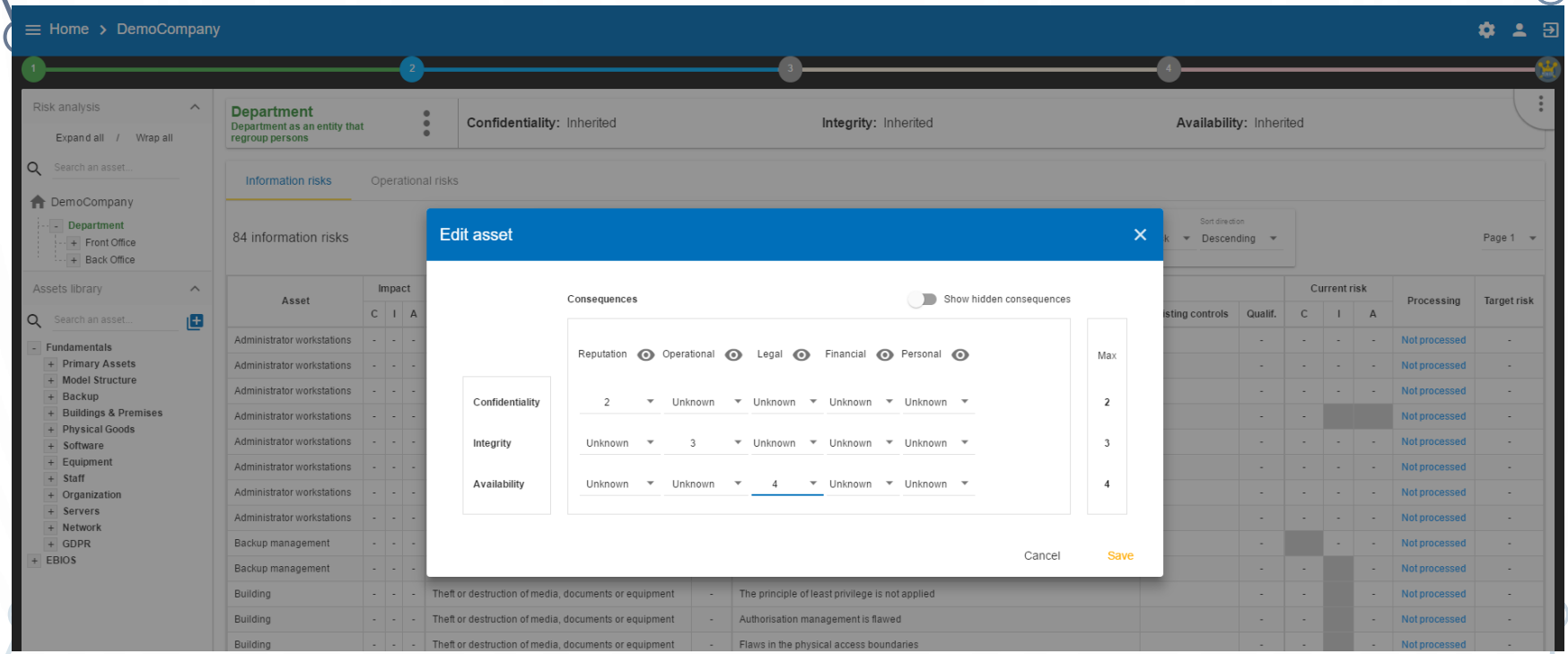
2.1 – IDENTIFICATION OF ASSETS, VULNERABILITIES AND IMPACTS



- 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

DEMO

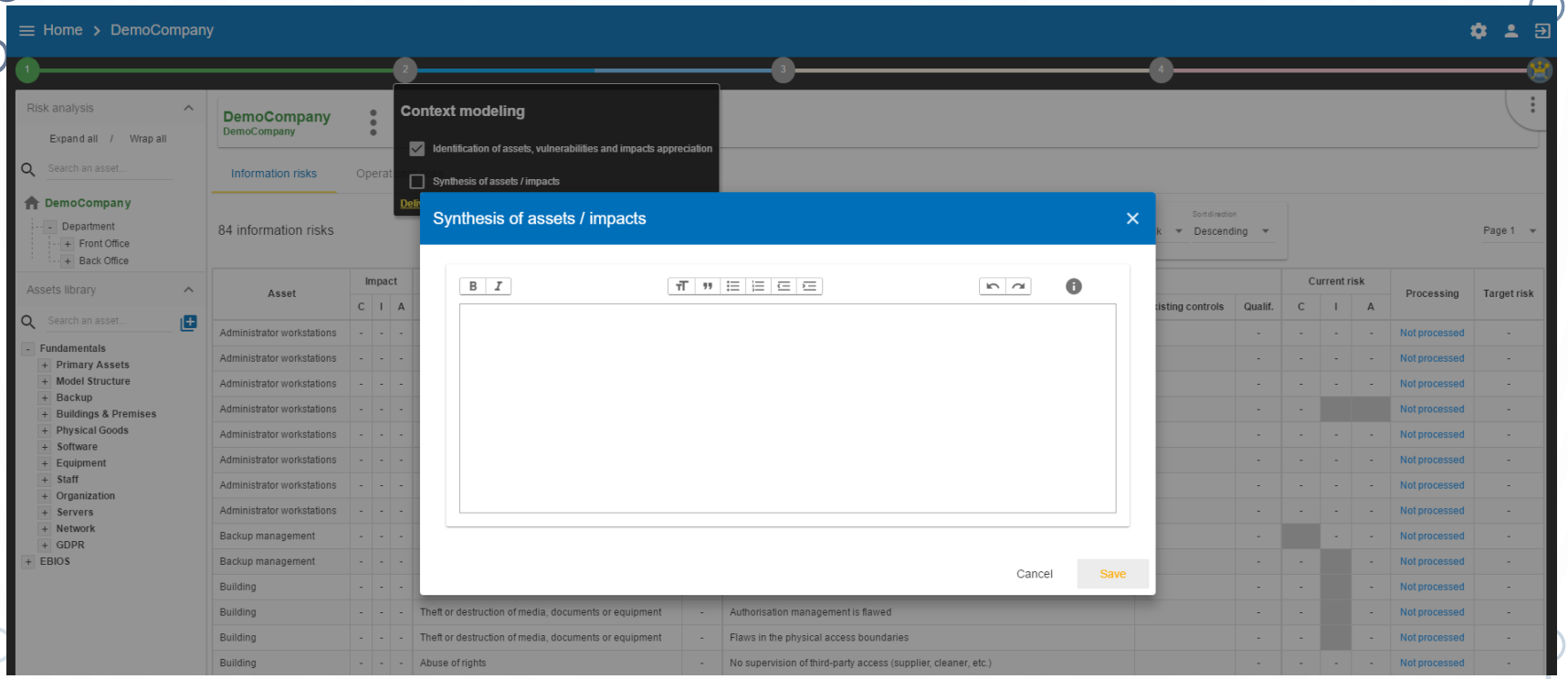
2.1 – IDENTIFICATION OF ASSETS, VULNERABILITIES AND IMPACTS



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

DEMO

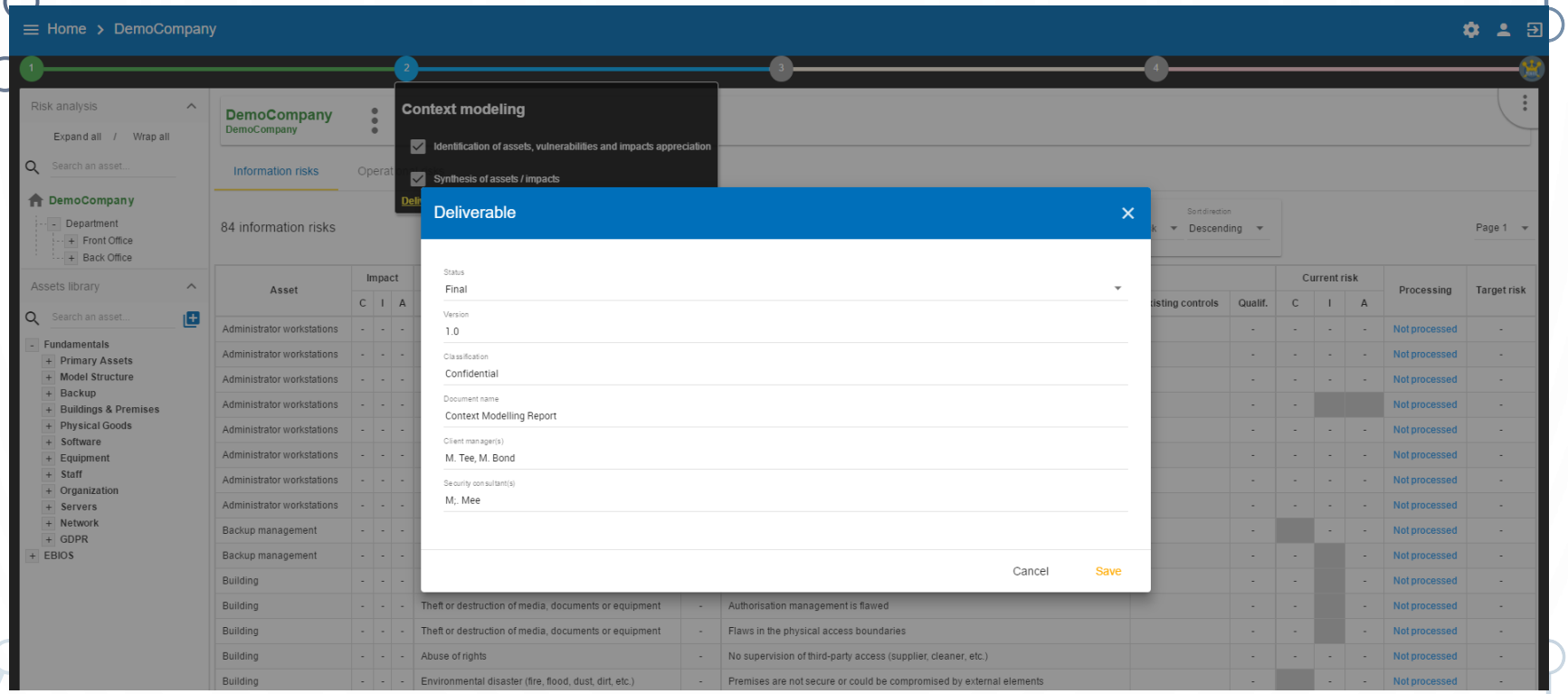
2.2 – SYNTHESIS OF ASSETS / IMPACTS



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

DEMO

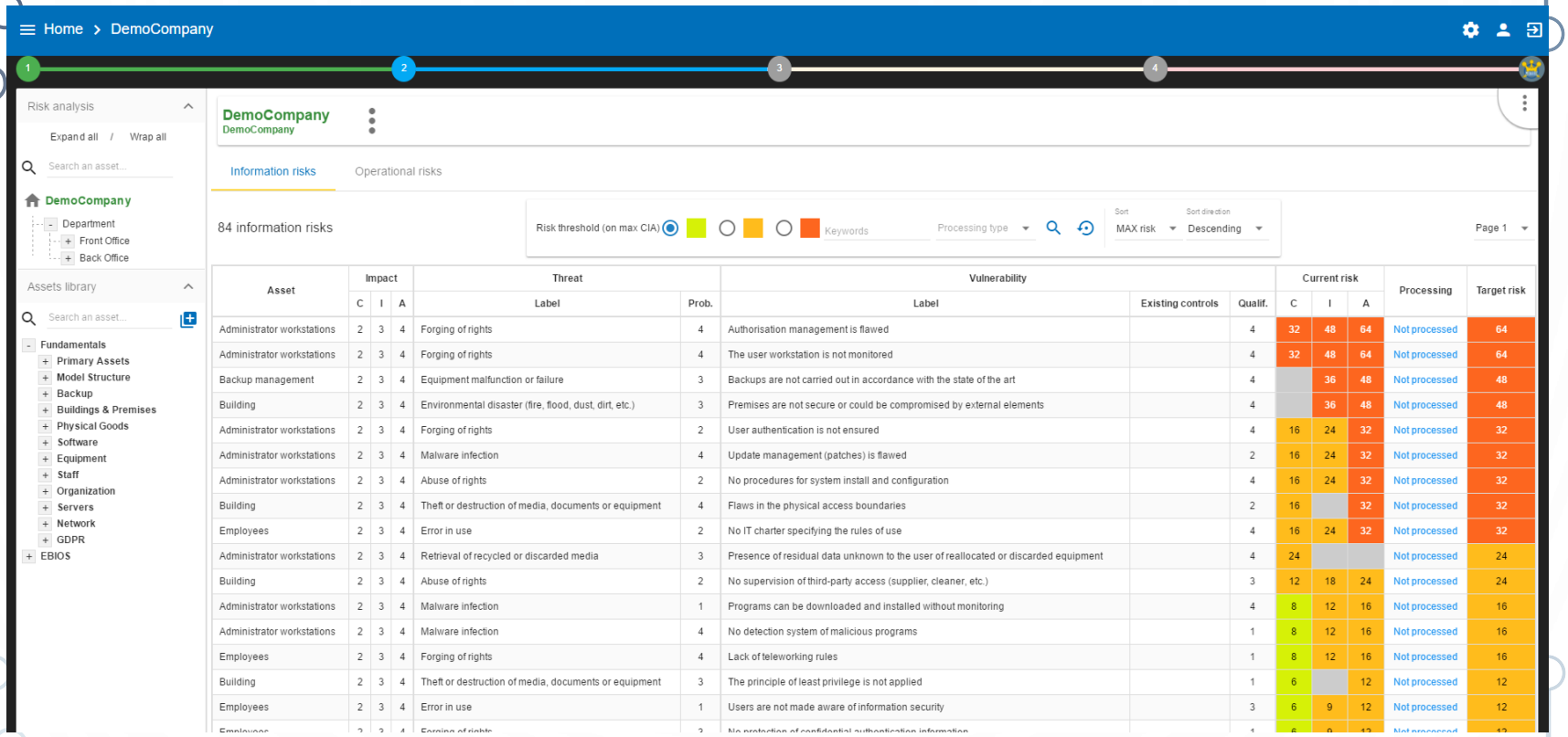
2.3 – DELIVRABLE: MODEL VALIDATION



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

DEMO

3.1 – ESTIMATION, EVALUATION AND RISK TRAITEMENT

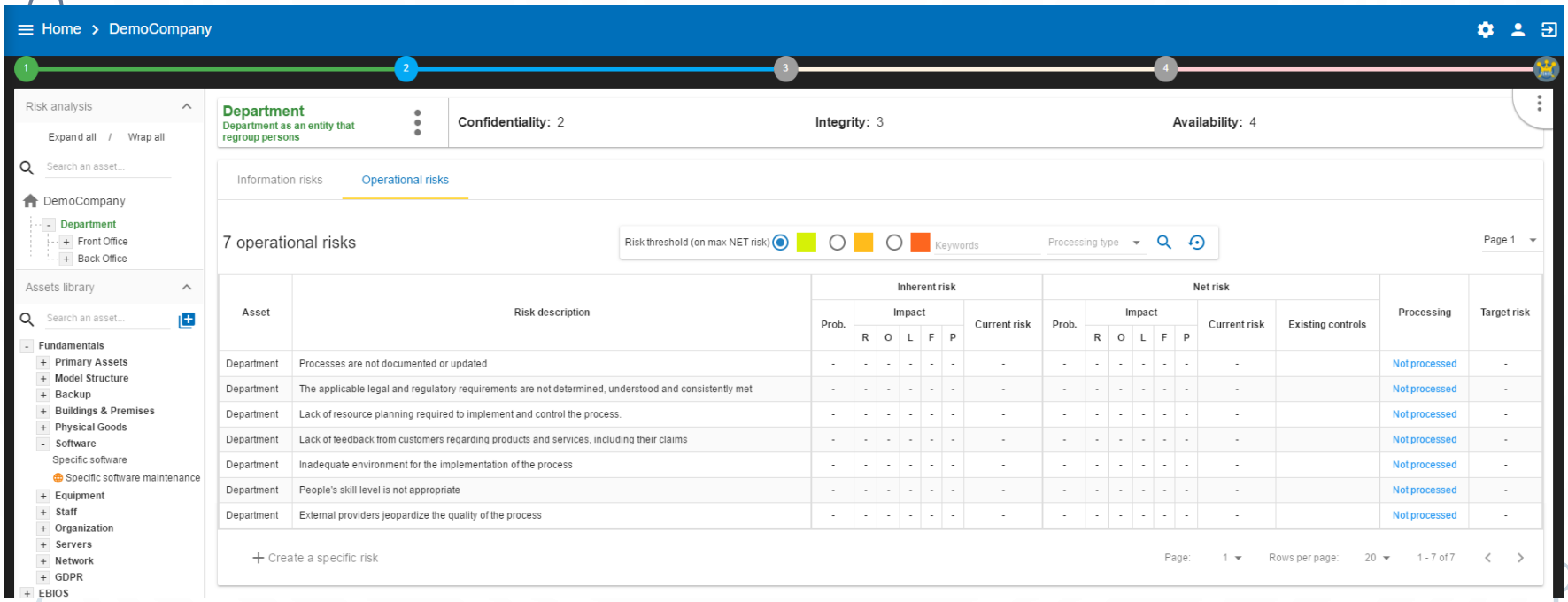


Asset	Impact			Threat		Vulnerability			Current risk			Processing	Target risk
	C	I	A	Label	Prob.	Label	Existing controls	Qualif.	C	I	A		
Administrator workstations	2	3	4	Forging of rights	4	Authorisation management is flawed		4	32	48	64	Not processed	64
Administrator workstations	2	3	4	Forging of rights	4	The user workstation is not monitored		4	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		4		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		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		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
Building	2	3	4	Theft or destruction of media, documents or equipment	3	The principle of least privilege is not applied		1	6		12	Not processed	12
Employees	2	3	4	Error in use	1	Users are not made aware of information security		3	6	9	12	Not processed	12

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

DEMO

3.1 – ESTIMATION, EVALUATION AND RISK TRAITEMENT

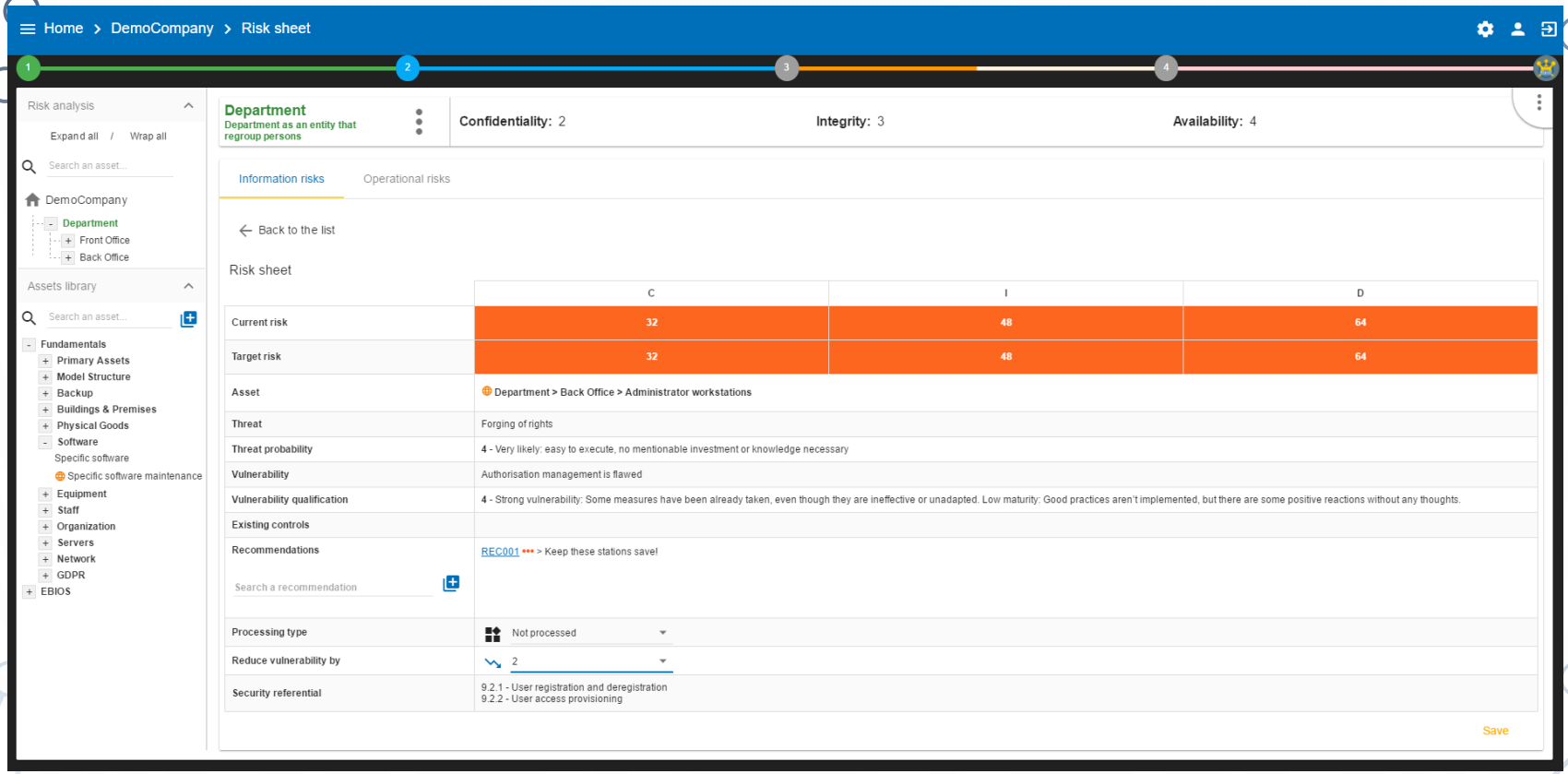


Asset	Risk description	Inherent risk							Net risk								Processing	Target risk
		Prob.	Impact					Current risk	Prob.	Impact					Current risk	Existing controls		
			R	O	L	F	P			R	O	L	F	P				
Department	Processes are not documented or updated	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not processed	-
Department	The applicable legal and regulatory requirements are not determined, understood and consistently met	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not processed	-
Department	Lack of resource planning required to implement and control the process.	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not processed	-
Department	Lack of feedback from customers regarding products and services, including their claims	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not processed	-
Department	Inadequate environment for the implementation of the process	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not processed	-
Department	People's skill level is not appropriate	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not processed	-
Department	External providers jeopardize the quality of the process	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Not processed	-

- Main View of MONARC
  - Evaluation of some operational risks

DEMO

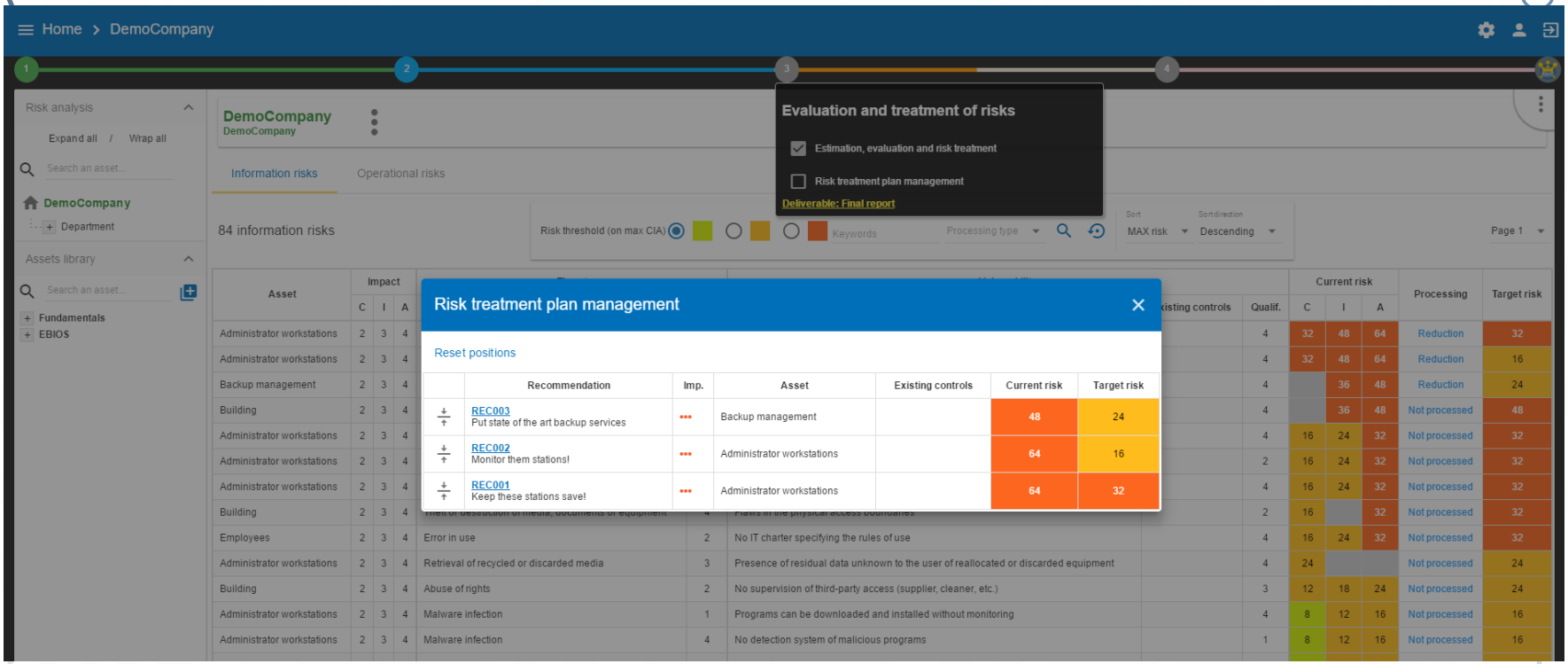
3.1 – ESTIMATION, EVALUATION AND RISK TRAITEMENT



- List of risks
- Creation of recommandations

DEMO

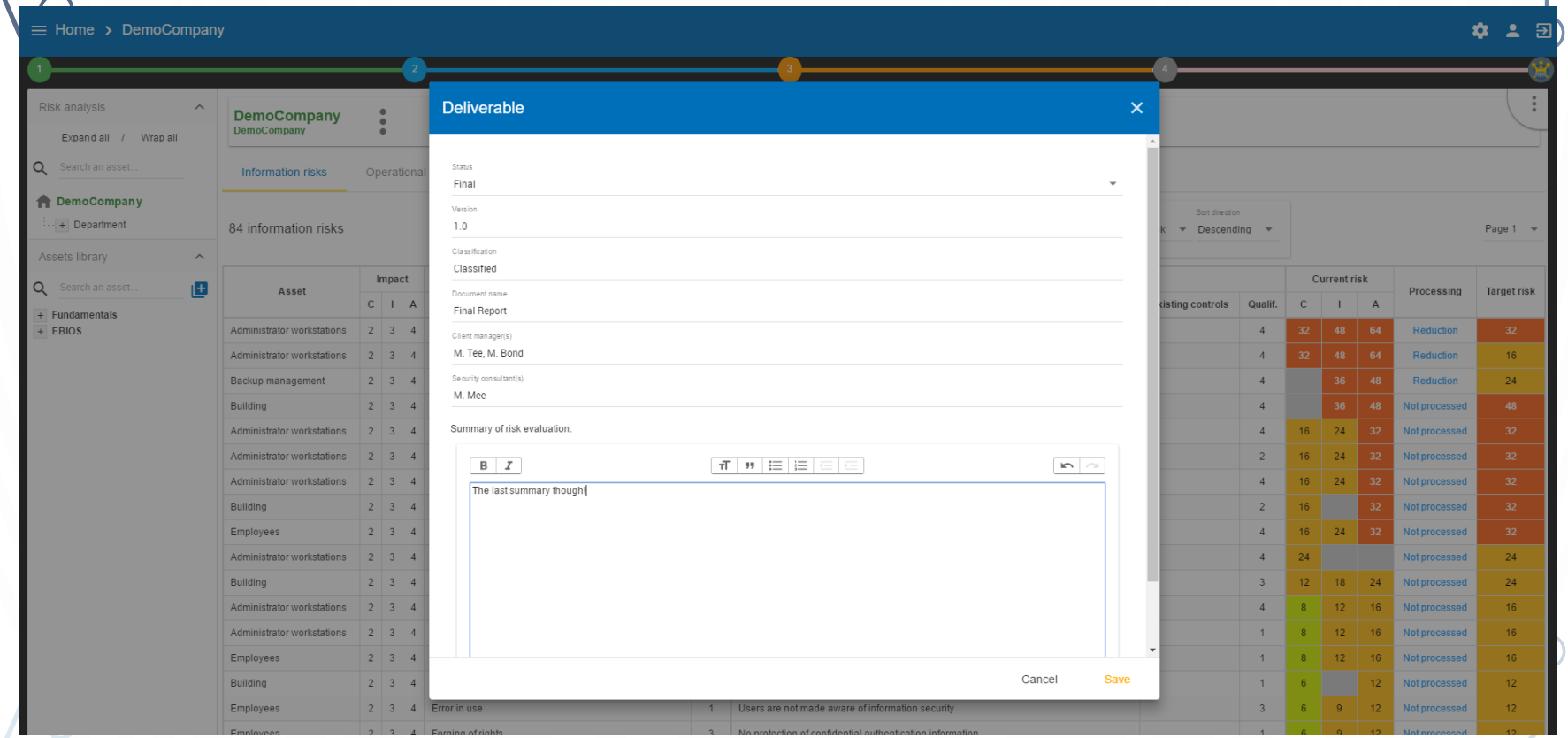
3.2 –MANAGEMENT OF PLAN FOR RISK TREATMENT



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

DEMO

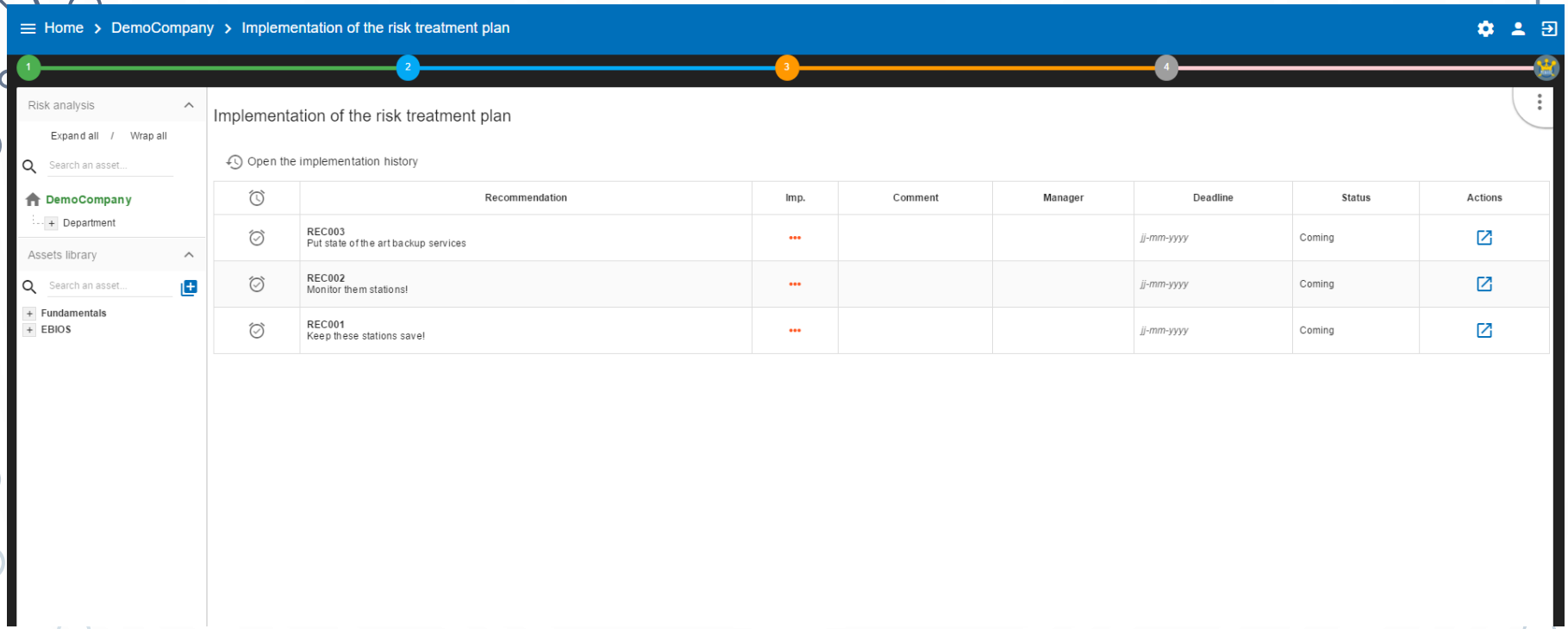
3.3 – DELIVRABLE: FINAL REPORT



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

DEMO

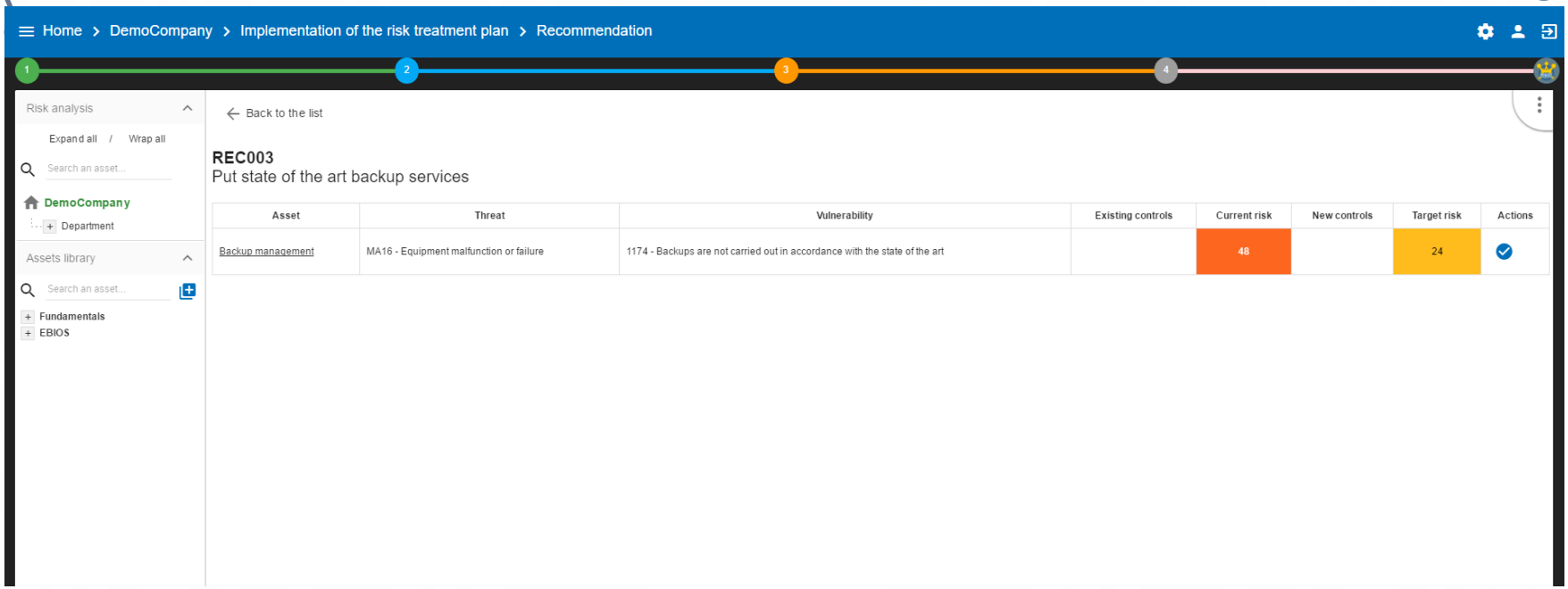
4.1 – MANAGEMENT OF THE IMPLMENETATION PLAN FOR RISK TREATMENT



- 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

DEMO

4.1 – MANAGEMENT OF THE IMPLMENETATION PLAN FOR RISK TREATMENT



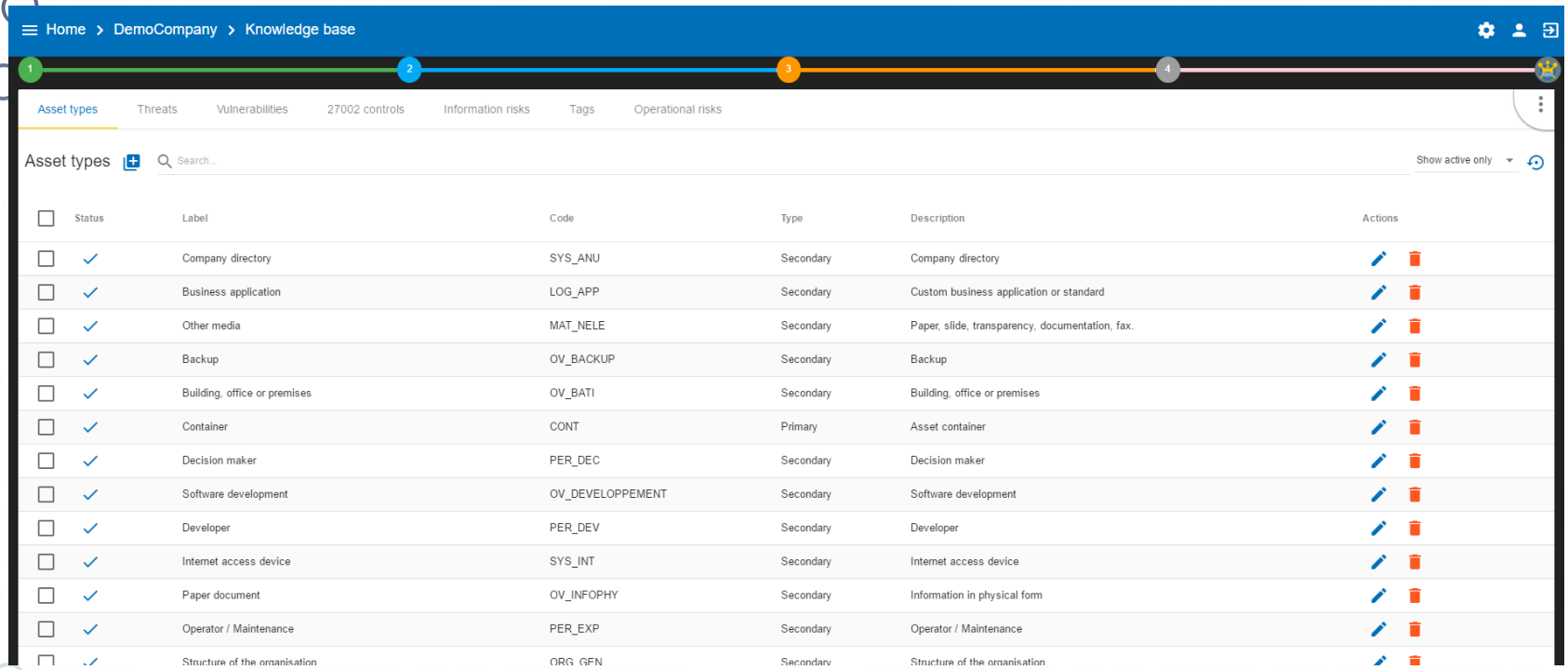
- Delegate a person in charge and fix deadlines for the implementation of each recommendation
- Validation risk by risk of their state change
- Change the value of the risk: the target risk becomes the actual risk

DEMO

AGENDA

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

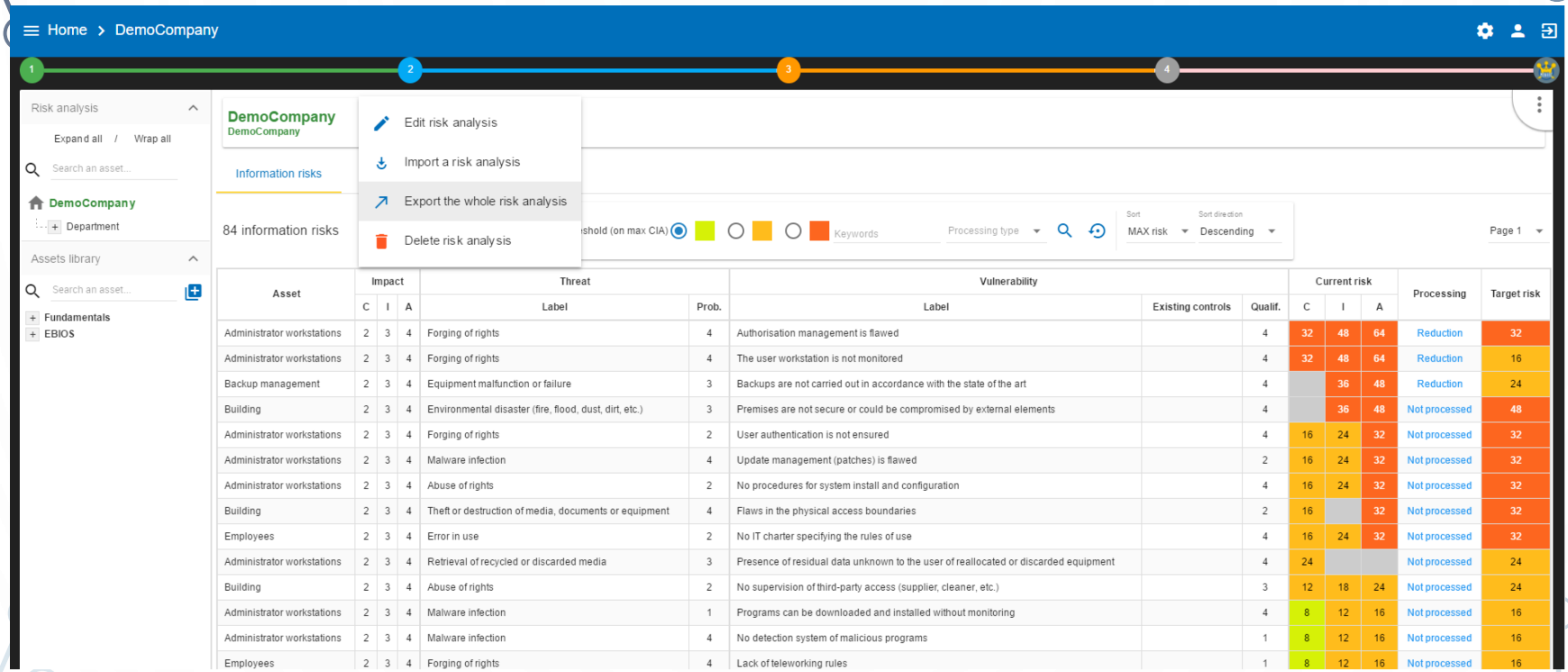
T&T: CREATION OF A RISK



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

T&T: IMPORT / EXPORT ASSETS



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		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	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		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