



**cases.lu**  
Secure. Innovate. Lead.

# **WORKSHOP MONARC**

## (MÉTHODE OPTIMISÉE D'ANALYSE DES RISQUES CASES)

FORMATION MONARC V2.0

*INFO@CASES.LU*

**SECURITY  
MADEIN.LU**





**cases.lu**  
Secure. Innovate. Lead.

# SECURITYMADEIN.LU



LE GOUVERNEMENT  
DU GRAND-DUCHÉ DE LUXEMBOURG



**Forme juridique: G.I.E (Groupement d'Intérêt Economique)**



**circl**

*Computer Incident  
Response Center  
Luxembourg*



**cases**

*Cyberworld Awareness  
and Security Enhancement  
Services*

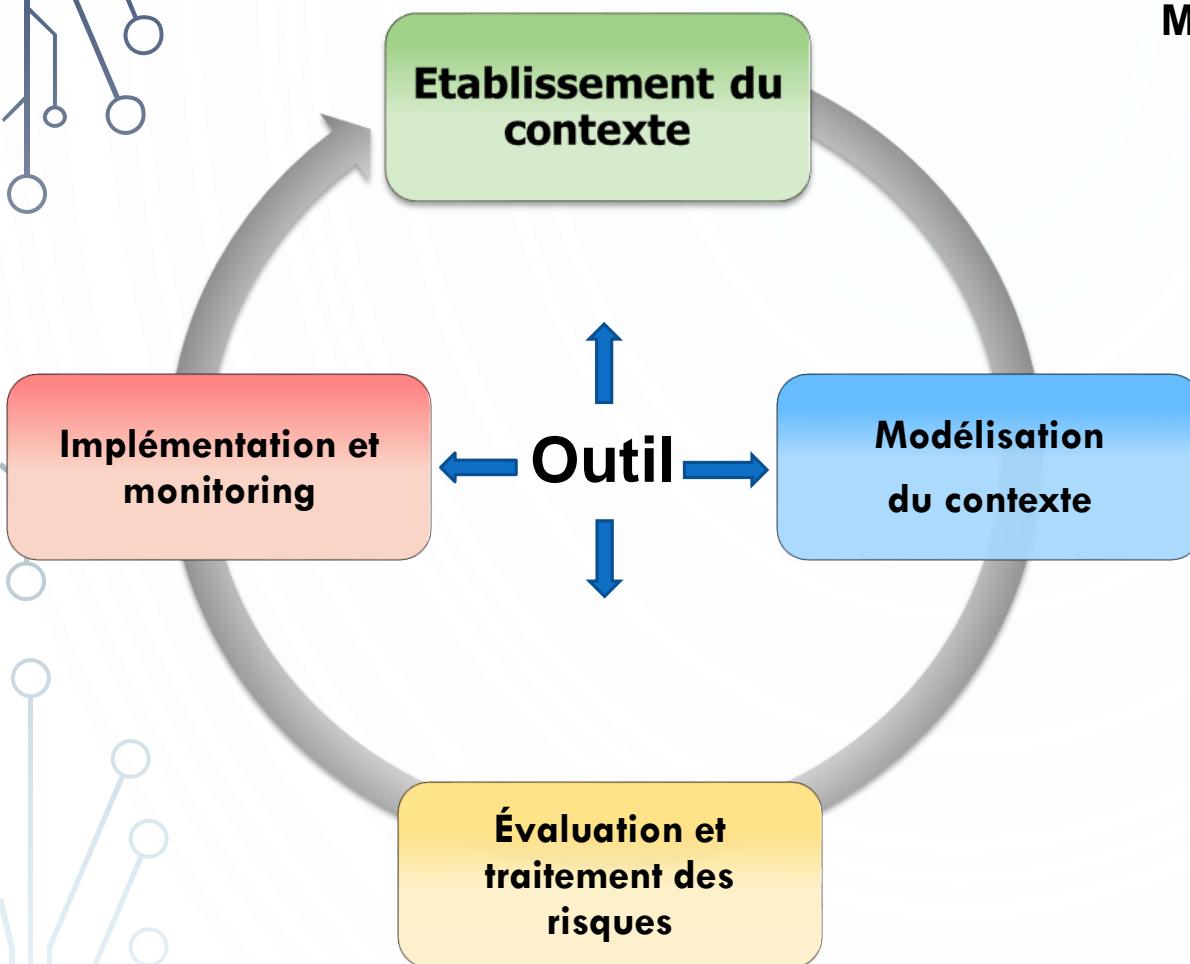
[www.securitymadein.lu](http://www.securitymadein.lu)  
[www.cases.lu](http://www.cases.lu)



# AGENDA

- ▶ **Qu'est-ce que MONARC ?**
- ▶ Découverte et utilisation de l'outil
- ▶ Déroulement de la méthode
- ▶ Trucs & Astuces

# MONARC : MÉTHODE OPTIMISÉE D'ANALYSE DES RISQUES CASES

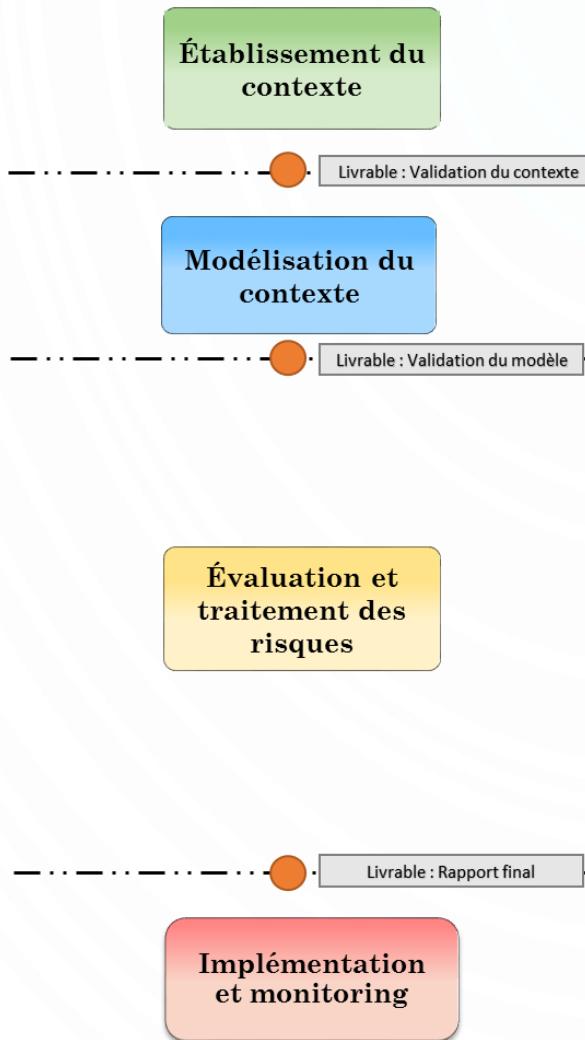


## Méthode d'analyse des risques

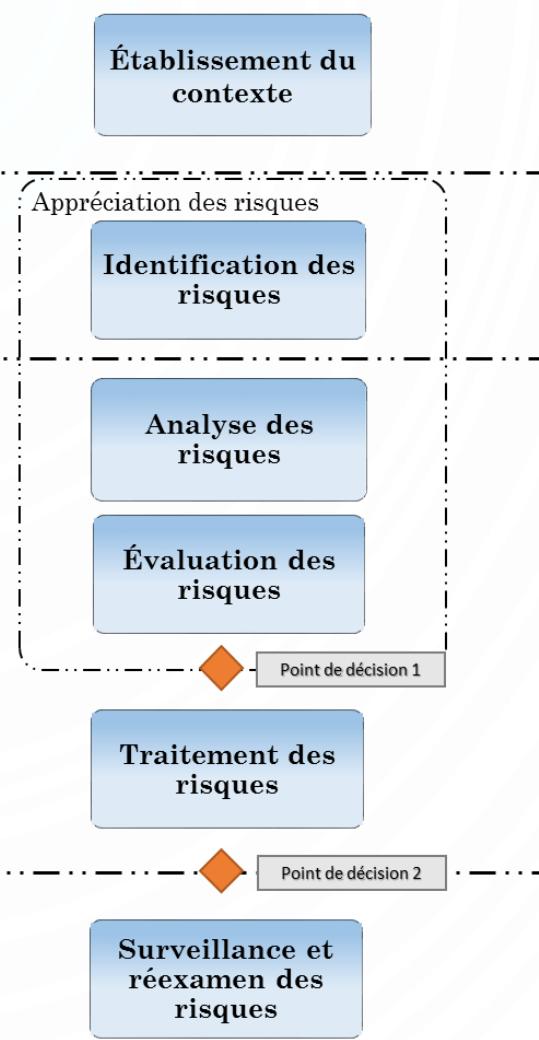
- Structurée
  - 1. ...
  - 2. ...
  - n. ...
- Itérative
  - Plan
  - Do
  - Check
  - Act
- Qualitative : Valeurs / conséquences
  - Réputation, Image
  - Opération
  - Légal
  - Financier
  - Personne (à la)
  - ...

# MONARC : LA MÉTHODE

## MONARC



## ISO/IEC 27005



# MONARC : À RETENIR

## Open source

[www.github.com/CASES-LU/MonarcAppFO](https://www.github.com/CASES-LU/MonarcAppFO)

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

## Gestion de risques

Risques de l'information ( $R = I \times M \times V$ )

Impact sur le CID

Actifs secondaires

Risques opérationnels ( $R = I \times P$ )

Impact sur le ROLFP

Brut/Net

Actifs primaires

## Partage des modèles de risques

## Optimisée (modèles, livrables, héritage, globalisation)

# AGENDA

- ▶ Qu'est-ce que MONARC ?
- ▶ **Découverte et utilisation de l'outil**
- ▶ Déroulement de la méthode
- ▶ Trucs & Astuces



cases.lu  
Secure. Innovate. Lead.

# PRINCIPALES FONCTIONNALITÉS

The screenshot displays the 'Mon analyse' dashboard of the cases.lu software. The top navigation bar shows 'Accueil > Mon analyse'. A horizontal progress bar at the top indicates four steps: 1. Analyse des risques (green), 2. (grey), 3. (yellow), and 4. (pink). The main content area is titled 'Mon analyse Analyse de risques'. It features two tabs: 'Risques de l'information' (selected) and 'Risques opérationnels'. Below these tabs, it shows '91 risques de l'information'. A search bar and filter options are available. The main view is a table with columns: Actif, Impact (C, I, D), Menace (Libellé, Prob.), Vulnérabilité (Libellé, Mesures en place, Qualif.), Risque actuel (C, I, D), Traitement, and Risque résiduel. The table lists various risks related to system administrators, such as 'Erreur d'utilisation' and 'Usurpation de droits', with corresponding descriptions and treatment status.

Actif	Impact			Menace		Vulnérabilité			Risque actuel			Traitement	Risque résiduel
	C	I	D	Libellé	Prob.	Libellé	Mesures en place	Qualif.	C	I	D		
Administrateur système	-	-	-	Erreur d'utilisation	-	Les utilisateurs ne sont pas sensibilisés à la sécurité de l'information	-	-	-	-	-	Non traité	-
Administrateur système	-	-	-	Erreur d'utilisation	-	Absence de charte informatique précisant les exigences d'utilisation	-	-	-	-	-	Non traité	-
Administrateur système	-	-	-	Erreur d'utilisation	-	Absence de formation sur les matériels ou logiciels utilisés	-	-	-	-	-	Non traité	-
Administrateur système	-	-	-	Usurpation de droits	-	Absence de protection d'informations secrètes d'authentification	-	-	-	-	-	Non traité	-
Administrateur	-	-	-	Usurpation de droits	-	Absence de règles encadrant le	-	-	-	-	-	Non traité	-

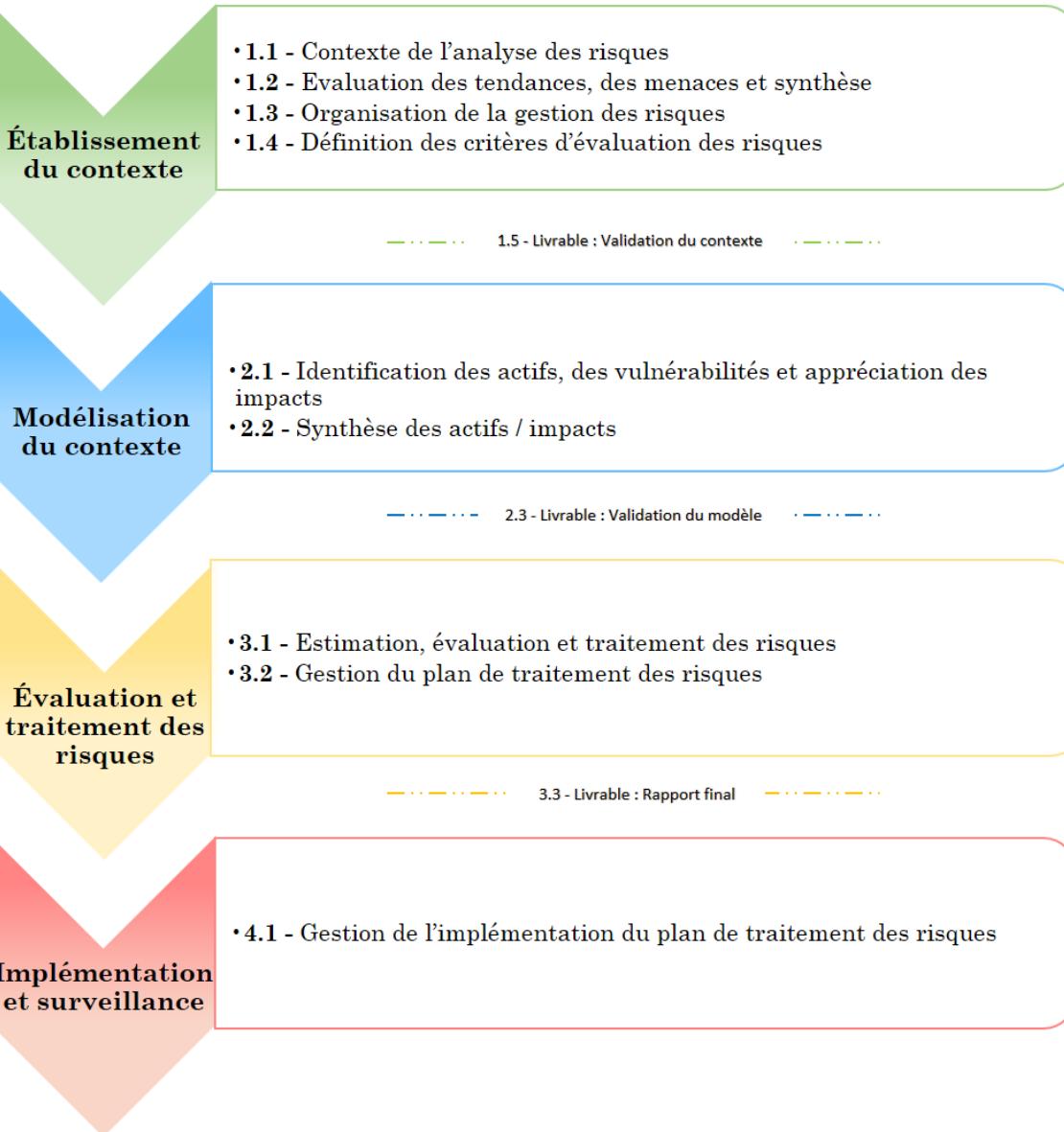
# AGENDA

- ▶ Qu'est-ce que MONARC ?
- ▶ Découverte et utilisation de l'outil
- ▶ **Déroulement de la méthode**
- ▶ Trucs & Astuces



**cases.lu**  
Secure. Innovate. Lead.

# MONARC : LA MÉTHODE EN DÉTAIL





cases.lu  
Secure. Innovate. Lead.

# 1.1 – CONTEXTE DE L'ANALYSE DES RISQUES

The screenshot shows the software's main dashboard with a sidebar on the left containing a navigation menu and a tree view of organizational assets. A central modal window titled "Contexte de l'analyse des risques" is open, displaying various sections of risk analysis context. The sections include:

- Informations supplémentaires
- Considérations générales : Reason pour lesquelles l'analyse est réalisée ? Gestion d'un ISMS, préparation plan de continuité, gestion des incidents, aspects légaux.
- Approche de la gestion des risques : Iterations en cours, choix des ressources
- Critères de bases :
  - Critères d'évaluation des risques : valeurs stratégiques processus ou informationnel, obligations légales, réglementaires ou contractuelles
  - Critères d'impact : Conséquences sur le business, temps, legal
  - Critère d'acceptation des risques : ROSI/Return On Security investment, lois et règlements, traitements futurs du risque, stratégie de l'entreprise
- Cibles et limites : Activité, processus à couvrir, objectif de l'organisation, limites et exclusion de l'analyse (géographique, logique...), contraintes légales, environnement socio-culturel, autres contraintes...
- Considérations générales
- Approche de la gestion des risques
- Critères de base
- Cibles et limites

At the bottom right of the modal are "Annuler" and "Sauvegarder" buttons.

- Phase de découverte de l'organisme cible
  - Parallèle avec ISO 27005:2011
    - Considérations générales
    - Approche de la gestion des risques
    - Critères de base
    - Cibles et limites
- : Chapitre 7.1  
: Chapitre 7.2.1  
: Chapitres 7.2.2, 7.2.3, 7.2.4  
: Chapitre 7.3

Démonstration



cases.lu  
Secure. Innovate. Lead.

# 1.2 – ÉVALUATION DES TENDANCES

The screenshot shows a software application window titled "Evaluation des tendances, des menaces et synthèse". The left sidebar is titled "Établissement du contexte" and includes a checklist with several items checked, such as "Contexte de l'analyse des risques" and "Evaluation des tendances, des menaces et synthèse". The main content area contains five questions with input fields:

- Quelle est la raison d'être de votre structure ?
- Quelle est l'évolution de votre activité de dernières années ?
- Quelle est l'évolution du contexte externe (concurrence, évolution marché, lois, etc.) ?
- Quels pourraient être les motifs d'attaque contre votre structure ?
- Quels sont vos processus métiers les plus importants ?
- Quel est l'actif ayant le plus de valeur dans votre structure ?
- Pour votre activité et vos données quel est le critère le plus important ?

A "Sauvegarder" (Save) button is located at the bottom right of the form. The background shows a blurred view of the "Mon analyse" dashboard with various data tables and filters.

- Kick-off meeting : Personnes clés (management, chefs de services, IT, Qualité ...)
- Questions larges pour découvrir le contexte
- Précise le scope et le focus de l'analyse
- Collecte de l'information

Démonstration



cases.lu  
Secure. Innovate. Lead.

# 1.2 – ÉVALUATION DES MENACES

The screenshot shows the cases.lu software interface. At the top, there's a navigation bar with 'Accueil > Mon analyse'. Below it is a progress bar with four steps: 1. Etablissement du contexte (Context establishment), 2. Mon analyse (My analysis), 3. Risques opérationnels (Operational risks), and 4. Risques stratégiques (Strategic risks). The main area is titled 'Evaluation des tendances, des menaces et synthèse' (Evaluation of trends, threats and synthesis). The 'Evaluation des menaces' tab is selected. The dialog box contains the following fields:

Thème	Description	Commentaires
Compromission des fonctions	Personne commettant une erreur de manipulation, de saisie, d'utilisation de matériels ou logiciels.	

Below this, there are sections for 'Critère impacté' (Impact criterion) with checkboxes for C, I, and D, and 'Tendances' (Trends) with radio buttons for -, n, +, and ++. There's also a 'Probabilité' (Probability) slider set to -1 and a checkbox for 'Forcer la probabilité dans l'analyse' (Force probability in analysis). At the bottom are buttons for 'Précédent' (Previous), 'Sauvegarder' (Save), and 'Suivant' (Next).

- Parcourir la plupart des menaces, faire parler le groupe, découvrir le contexte
- Collecter de l'information avant interviews face à face



cases.lu  
Secure. Innovate. Lead.

# 1.2 – RÉSUMÉ

The screenshot shows the software's main interface with a navigation bar at the top. The left sidebar contains a tree view of organizational assets under 'Fondamentaux'. A modal window titled 'Evaluation des tendances, des menaces et synthèse' is open, showing tabs for 'Evaluation des tendances', 'Evaluation des menaces', and 'Résumé' (Summary), with 'Résumé' selected. The summary section contains a rich text editor and a sidebar with additional information and a 'Sauvegarder' button.

- Résumé de l'information pertinente collectée pendant l'évaluation des tendances et des menaces.
- Ce texte permet d'étoffer le livrable.



cases.lu  
Secure. Innovate. Lead.

## 1.3 – ORGANISATION DE LA GESTION DES RISQUES

The screenshot shows a software application for risk management. At the top, there's a navigation bar with 'Accueil' and 'Mon analyse'. Below it is a progress bar with four steps: 1. Etablissement du contexte (Context establishment), 2. Mon analyse (My analysis), 3. Risques opérationnels (Operational risks), and 4. Mise en œuvre (Implementation). A dropdown menu for step 1 is open, showing several items under 'Établissement du contexte': 'Contexte de l'analyse des risques' (checked), 'Evaluation des tendances, des menaces et synthèse' (checked), 'Mon analyse' (checked), 'Organisation de la gestion des risques' (checked), and 'Définition des critères d'évaluation des risques' (unchecked). The main area displays a modal window titled 'Organisation de la gestion des risques' with a rich text editor on the left and a sidebar on the right containing sections like 'Informations supplémentaires', 'Organisation de la mission en cours', 'Rôles et responsabilités', and 'Résolution des conflits et escalation'. At the bottom of the modal are 'Annuler' and 'Sauvegarder' buttons.

- Complément d'information sur la gestion des risques dans l'organisme
- Parallèle avec ISO 27005:2011
  - Organisation de la gestion des risques : Chapitre 7.4

Démonstration

# 1.4 – DÉFINITION DES CRITÈRES D'ÉVALUATION, D'ACCEPTATION ET D'IMPACT

## Echelle des menaces : [ 0 - 4 ]

0. Impossible
1. Très improbable : jamais arrivé, nécessite d'un haut niveau d'expertise, ou très coûteux à mettre en œuvre.
2. Improbable : Peut être déjà survenu, phénomène rare ou nécessite d'un bon niveau d'expertise ou coûteux à mettre en œuvre.
3. Peut arriver de temps à autre.
4. Très probable: facile à mettre en œuvre, pas d'investissement ou d'expertise particulière.

## Echelle d'impacts : [ 0 - 4 ]

	Confidentialité 	Intégrité 	
0	Impact inexistant. Le critère de confidentialité n'est pas important.	Impact inexistant. Le critère d'intégrité n'est pas important.	Imp Le imp
1	Impact faible, négligeable La divulgation est défavorable aux intérêts de l'organisation Exemples : - Divulgation d'information interne ne devant pas sortir de l'organisme - Note de service - Annuaire téléphonique interne	Impact faible, négligeable Corruption facile à rectifier et sans grandes conséquences. Exemples : - Courrier interne, e-mail interne	Imp Ind enc pre
2	Impact moyen, acceptable La divulgation nuit aux intérêts de l'organisation Exemples : - Divulgation d'information moyennement sensible restreinte à un groupe de personnes - schéma de réseau interne - Documentation ou programme source non critique	Impact moyen, acceptable Corruption occasionnant une gêne modérée aux parties prenantes. Le rétablissement est facile. Exemples : - Site Internet informationnel	Imp Ind gén Ex - Di cor atte

## Echelle des vulnérabilités : [ 0 - 5 ]

0. Pas de vulnérabilité.
1. Vulnérabilité très faible : Des mesures efficaces sont en place, leurs efficacités sont contrôlées.  
Très bonne maturité : Les bonnes pratiques sont implémentées et périodiquement vérifiées.
2. Vulnérabilité faible : Des mesures efficaces sont en place.  
Bonne maturité : Les bonnes pratiques sont implémentées.
3. Vulnérabilité normale : Des mesures sont en place, elle peuvent encore être améliorées.  
Maturité moyenne : Les bonnes pratiques sont implémentées sans recherche d'amélioration.
4. Vulnérabilité élevée : Des mesures sont en place, mais elles sont peu efficaces ou inadaptées.  
Maturité faible : Les bonnes pratiques ne sont pas implémentées, pratiques primaires sans réflexion.
5. Vulnérabilité très élevée : aucune mesure en place.  
Maturité très faible - Aucune maturité.

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

R : Risque, I : Impact, M : Menace, V : Vulnérabilité

	MxV													
	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

- Parallèle avec ISO 27005:2011
  - Organisation de la gestion des risques : Chapitre 7.2.2, 7.2.3, 7.2.4



cases.lu  
Secure. Innovate. Lead.

# 1.5 – LIVRABLE : VALIDATION DU CONTEXTE

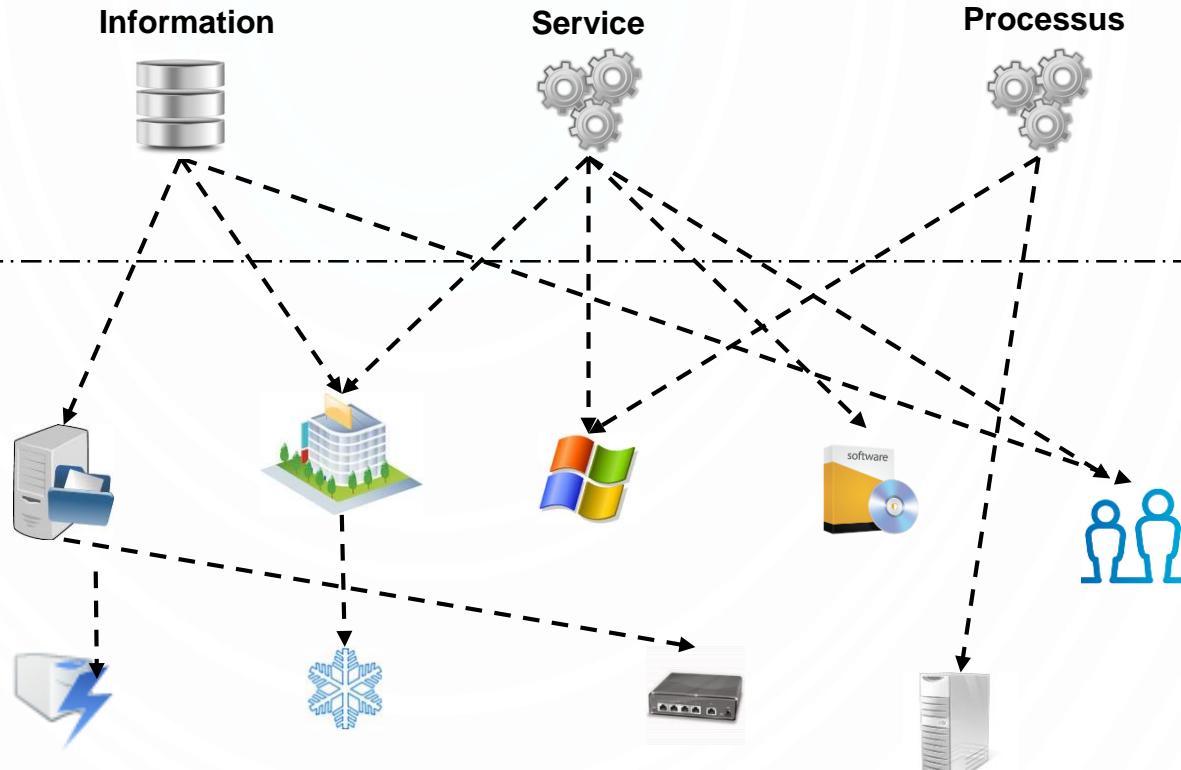
The screenshot shows the cases.lu software interface. On the left, there's a sidebar with a navigation menu and a search bar. The main area has a header 'Accueil > Mon analyse'. Below the header is a progress bar with four steps: 1. Etablissement du contexte (highlighted in green), 2. Identification des risques, 3. Analyse et priorisation, and 4. Planification et suivi. A sub-menu for step 1 is open, listing several risk analysis components with checkboxes, some of which are checked. The main content area is titled 'Livrable' and contains fields for 'Statut' (Final), 'Version' (1.0), 'Classification' (Confidentielle), 'Nom du document' (Rapport établissement du contexte), 'Responsable(s) client' (M. Thill), and 'Consultant(s) sécurité' (M. Muller). At the bottom of the 'Livrable' window are 'Annuler' and 'Sauvegarder' buttons. The background shows a grid of risk data with various filters and sorting options.

- Reprise de toutes les informations collectées et saisies lors de la phase d'établissement du contexte.
- Utilisé pour valider les informations avant de commencer l'identification des risques.
- Format de sortie : Microsoft Word

## 2.1 – IDENTIFICATION DES ACTIFS, DES VULNÉRABILITÉS ET ÉVALUATION DES IMPACTS

**Actifs primaires  
(Business)**

**Actifs secondaires  
(de support)**



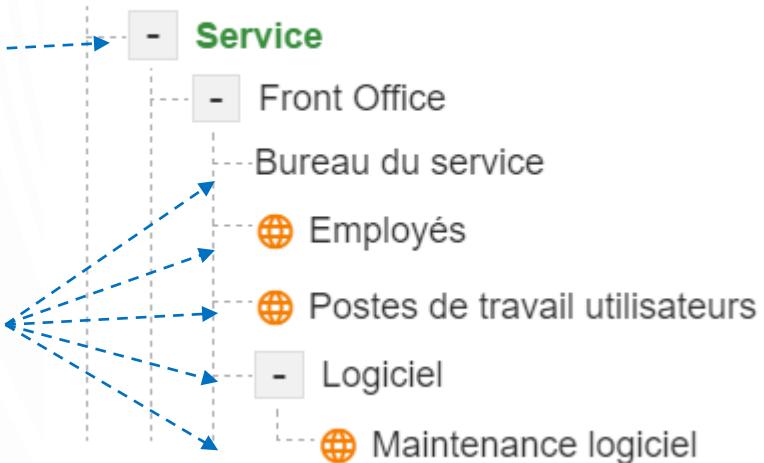
**Les risques cumulés des actifs de support remontent vers les actifs business  
par héritage des critères CID**

# FORMALISATION DE LA MODÉLISATION

## Hiérarchie des actifs

### Mon analyse

**Actif primaire**



**Actifs secondaires**

**Type d'actif**

- [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.

# ACTIF « GLOBAL » OU « LOCAL »

## “Local”

### Mon analyse

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

**30 risques**

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 risques**

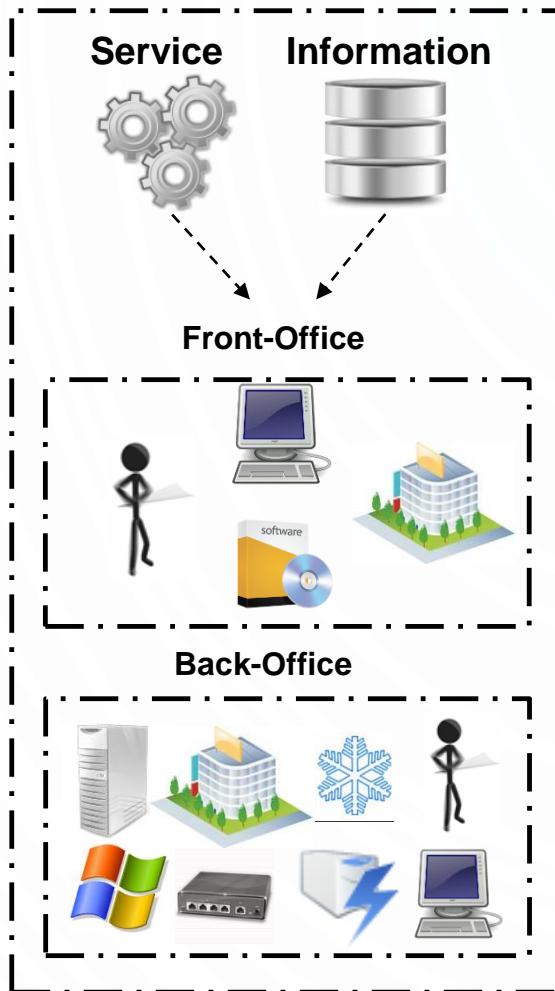
Base de données N°1    Base de données N°2





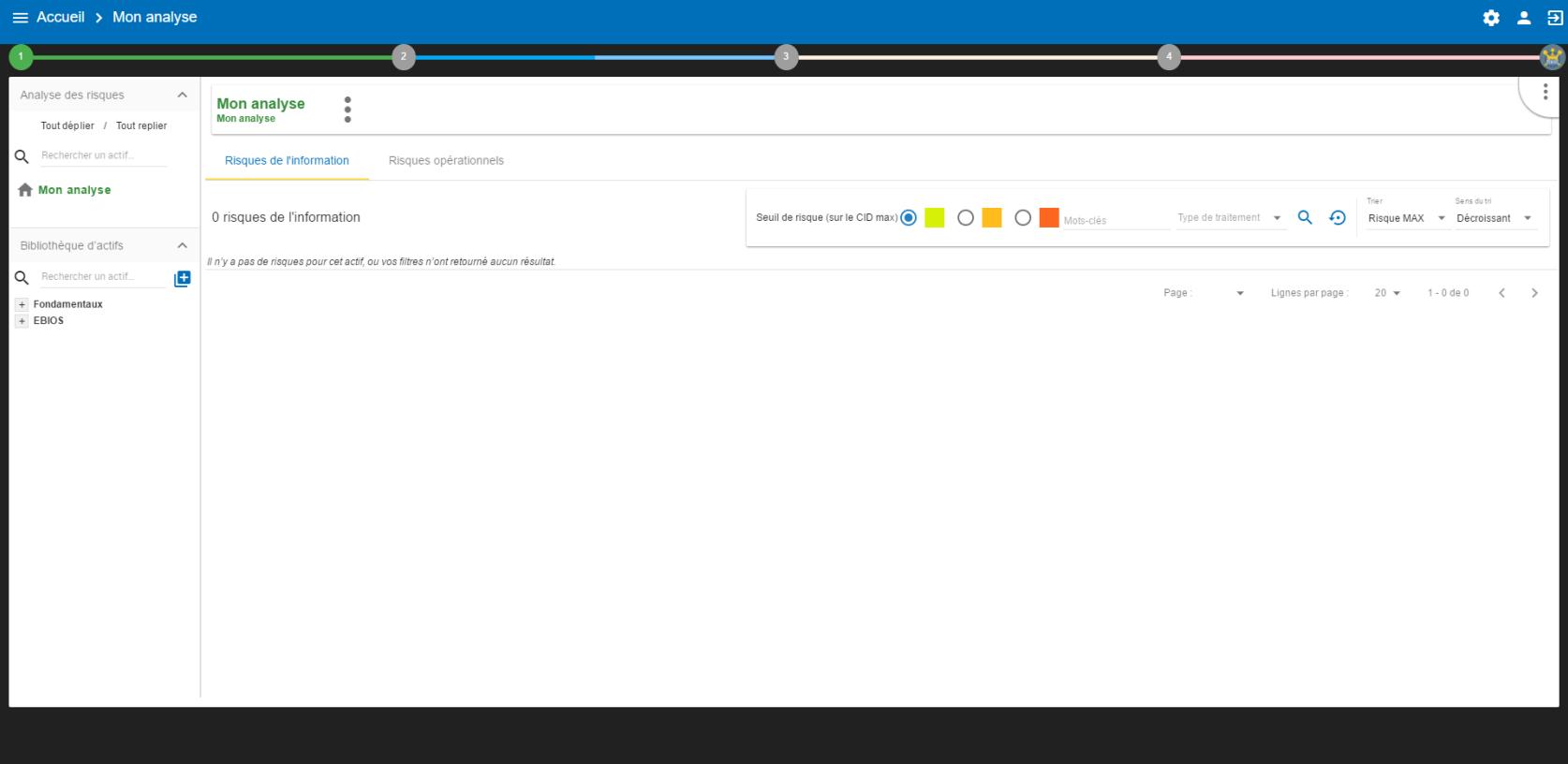
**cases.lu**  
Secure. Innovate. Lead.

# MODÉLISATION CASES



- **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 DES ACTIFS, DES VULNÉRABILITÉS ET APPRÉCIATION DES IMPACTS



The screenshot shows the MONARC software interface. At the top, there is a navigation bar with 'Accueil' and 'Mon analyse'. Below the navigation bar is a horizontal progress bar divided into four colored segments: green (1), blue (2), grey (3), and pink (4). The main area is titled 'Mon analyse' and contains tabs for 'Risques de l'information' (selected) and 'Risques opérationnels'. A message indicates '0 risques de l'information'. On the left, there is a sidebar with sections for 'Analyse des risques' (with 'Tout déplier / Tout replier' options), 'Rechercher un actif...', 'Mon analyse' (highlighted in green), 'Bibliothèque d'actifs' (with 'Rechercher un actif...' option), and 'Fondamentaux' (with 'EBIOS' option). On the right, there are filters for 'Seuil de risque (sur le CID max)' (with color-coded circles for green, yellow, orange, red, and 'Mots-clés'), 'Type de traitement' (with dropdowns for 'Trier' and 'Sens du tri'), and pagination controls ('Page : 1 - 0 de 0', 'Lignes par page : 20', 'Sens du tri : Risque MAX, Décroissant').

- Vue principale de MONARC
  - Création de modèle de risques
- Parallèle avec ISO 27005:2011
  - Identification des actifs : Chapitre 8.2.2
  - Identification des vulnérabilités : Chapitre 8.2.5

# 2.1 – IDENTIFICATION DES ACTIFS, DES VULNÉRABILITÉS ET APPRÉCIATION DES IMPACTS

Accueil > Mon analyse

1 2 3 4

**Service**  
Service en tant qu'entité regroupant un ensemble de personnes

Confidentialité : Hérité Intégrité : Hérité Disponibilité : Hérité

Risques de l'information Risques opérationnels

79 risques de l'information

Seuil de risque (sur le CID max) Mots-clés Type de traitement Risque MAX Sens du tri Décroissant Page 1

**Modifier l'actif**

Actif	Impact	Risque actuel					Traitement	Risque résiduel
		C	I	D	Qualif.	Max		
Administrateur système	- - -	-	-	-	-	-	Non traité	
Administrateur système	- - -	-	-	-	-	-	Non traité	
Administrateur système	- - -	-	-	-	-	-	Non traité	
Administrateur système	- - -	-	-	-	-	-	Non traité	
Administrateur système	- - -	-	-	-	-	-	Non traité	
Administrateur système	- - -	-	-	-	-	-	Non traité	
Bâtiment	- - -	-	-	-	-	-	Non traité	
Bâtiment	- - -	-	-	-	-	-	Non traité	
Bâtiment	- - -	-	-	-	-	-	Non traité	
Bâtiment	- - -	-	-	-	-	-	Non traité	
Bureau de service	- - -	-	-	-	-	-	Non traité	
Bureau de service	- - -	-	-	-	-	-	Non traité	
Bureau de service	- - -	-	-	-	-	-	Non traité	
Bureau de service	- - -	-	-	-	-	-	Non traité	
Bureau de service	- - -	-	-	-	-	-	Non traité	
Développements	- - -	-	-	-	-	-	Non traité	
Dysfonctionnement initial	- - -	-	-	-	-	-	Non traité	

**Conséquences**

Afficher les conséquences masquées

Réputation	Opérationnel	Légal	Financier	Personne	Max
Non renseigné	-1				
Non renseigné	-1				
Non renseigné	-1				

Annuler Sauvegarder

Vol ou destruction de supports, de documents ou de matériel

Le principe du moindre privilège n'est pas appliqué

La gestion des autorisations comporte des failles

Failles dans les périmètres d'accès physiques

Absence de vigilance lors d'une intervention d'un tiers (fournisseur, femme de ménage, etc.)

Les locaux ne sont pas sécurisés ou peuvent être compromis par des éléments externes

Absence d'identification des besoins en sécurité

- Vue principale de MONARC
  - Appréciation des impacts et des conséquences
- Parallèle avec ISO 27005:2011
  - Appréciation de conséquences : Chapitre 8.3.2



cases.lu  
Secure. Innovate. Lead.

## 2.2 – SYNTHÈSE DES ACTIFS / IMPACTS

The screenshot shows the cases.lu software interface. At the top, there's a navigation bar with 'Accueil' and 'Mon analyse'. Below it is a sidebar with sections like 'Analyse des risques', 'Mon analyse', 'Risques de l'information', 'Bibliothèque d'actifs', and 'Fondamentaux'. A main content area shows a progress bar with four steps: 1. Analyse des risques (green), 2. Mon analyse (blue), 3. Modélisation du contexte (grey), and 4. Synthèse des actifs / impacts (grey). Step 2 is currently active. A modal window titled 'Modélisation du contexte' is open, listing 'Identification des actifs, des vulnérabilités et appréciation des impacts' and 'Synthèse des actifs / impacts' with a checked checkbox. Below this is a 'Livrable : validation du modèle' section. Another modal window titled 'Synthèse des actifs / impacts' is also open, containing a rich text editor and an 'Informations supplémentaires' section with fields for 'Actifs primaires sélectionnés ?', 'Critères de sécurité relevant ?', 'Actifs de support principaux ?', and 'Particularité de la modélisation ?'. At the bottom of this modal are 'Annuler' and 'Sauvegarder' buttons.

- Contenu rédactionnel qui justifie le choix des actifs et des impacts
- Destiné à étoffer le livrable.



cases.lu  
Secure. Innovate. Lead.

## 2.3 – LIVRABLE : VALIDATION DU MODÈLE

The screenshot shows the cases.lu software interface. On the left, there's a navigation sidebar with sections like 'Analyses des risques', 'Mon analyse', and 'Bibliothèque d'actifs'. The main area has a progress bar at the top with four steps: 1. Analyse des risques (green), 2. Modélisation du contexte (blue), 3. Synthèse des actifs / impacts (grey), and 4. Livrable : validation du modèle (grey). Step 2 is currently active. A modal window titled 'Livrable' is open in the center, containing fields for 'Statut' (Final), 'Version' (1.0), 'Classification' (Confidentielle), 'Nom du document' (Validation modélisation du contexte), 'Responsable(s) client' (M. Thill), and 'Consultant(s) sécurité' (M. Muller). At the bottom right of the modal are 'Annuler' and 'Sauvegarder' buttons.

- Reprise des actifs primaires importants du modèle (Critères d'impacts fixés)
- Reprise synthèse des actifs.
- Format de sortie : Microsoft Word

# 3.1 – ESTIMATION, ÉVALUATION ET TRAITEMENT DES RISQUES

Accueil > Mon analyse

1 2 3 4

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

Mon analyse

- Service
  - Front Office
  - Bureau du service
  - Employés

Bibliothèque d'actifs

Rechercher un actif...

Fondamentaux
 

- Actifs primaires
- Structure modèle
- Backup
- Bâtiments & locaux
- Biens physiques
- Logiciels
- Materiel
- Organisation
- Personnel
- Serveurs
- Réseau

+ EBios

Mon analyse

Risques de l'information Risques opérationnels

Evaluation et traitement des risques

Estimation, évaluation et traitement des risques  
 Gestion du plan de traitement des risques

Livrable : rapport final

79 risques de l'information

Seuil de risque (sur le CID max)

Type de traitement

Trier Sens du tri

Risque MAX Décroissant

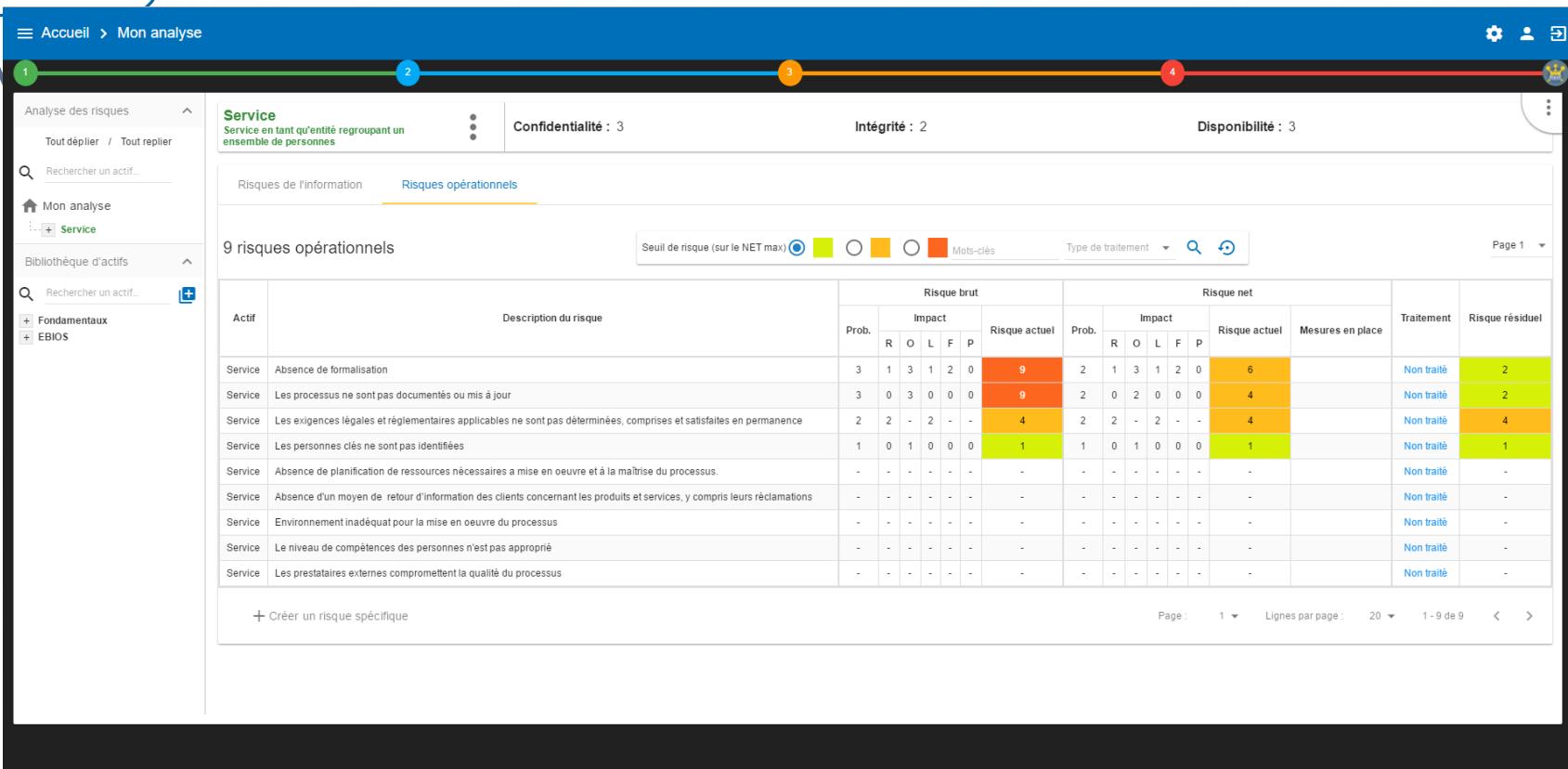
Page 1

Actif	Impact			Menace		Vulnérabilité			Risque actuel			Traitement	Risque résiduel
	C	I	D	Libellé	Prob.	Libellé	Mesures en place	Qualif.	C	I	D		
Organisation informatique	3	2	3	Usurpation de droits	4	Absence de contrôle périodique des autorisations d'accès logique		4	48	32	48	Non traité	48
Postes de travail admin	3	2	3	Infection par un malware	4	Possibilité de télécharger et d'installer des programmes sans contrôle		4	48	32	48	Non traité	48
Administrateur système	3	2	3	Erreur d'utilisation	3	Absence de charte informatique précisant les exigences d'utilisation		4	36	24	36	Non traité	36
Postes de travail admin	3	2	3	Abus de droits	3	Absence de procédure d'installation et de configuration		4	36	24	36	Non traité	36
Administrateur système	3	2	3	Erreur d'utilisation	3	Les utilisateurs ne sont pas sensibilisés à la sécurité de l'information		2	18	12	18	Non traité	18
Bureau du service	3	2	3	Vol ou destruction de supports, de documents ou de matériel	2	Le principe du moindre privilège n'est pas appliqué		3	18	12	18	Non traité	18
Postes de travail admin	3	2	3	Usurpation de droits	3	La gestion des autorisations comporte des failles		2	18	12	18	Non traité	18
Réseau & télécom	3	2	3	Écoute passive	3	Absence de cloisonnement des réseaux de communication		2	18			Non traité	18
Développements logiciels	3	2	3	Atteinte à la maintenabilité du système d'information	2	Absence de documentation à jour		2		12		Non traité	12
Gestion des backups	3	2	3	Vol ou destruction de supports, de documents ou de matériel	1	Les supports de backup ne sont pas entreposés dans un endroit adéquat		4	12	12		Non traité	12
Postes de travail utilisateurs	3	2	3	Infection par un malware	4	La gestion des mises à jour (patch) comporte des lacunes		1	12	8	12	Non traité	12
Postes de travail utilisateurs	3	2	3	Infection par un malware	4	Absence de système de détection des logiciels malveillants		1	12	8	12	Non traité	12
Développements logiciels	3	2	3	Infection par un malware	3	Absence de revue de code et tests d'intrusion		1	9	6	9	Non traité	9
Employés	3	2	3	Erreur d'utilisation	2	Les utilisateurs ne sont pas sensibilisés à la sécurité de l'information		1	6	4	6	Non traité	6
Employés	3	2	3	Usurpation de droits	2	Absence de protection d'informations secrètes d'authentification		1	6	4	6	Non traité	6
Organisation informatique	3	2	3	Divulgation d'information	2	Absence de règles de contrôle des entrées/sorties des matériels dans l'organisme		1	6			Non traité	6
Employés	3	2	3	Atteinte à la disponibilité du personnel	1	Non-redondance du personnel stratégique		1		3		Non traité	3
Gestion serveurs	3	2	3	Usurpation de droits	1	Possibilité d'administrer le système à distance		0	0	0	0	Non traité	0
Administrateur système	3	2	3	Erreur d'utilisation	-	Absence de formation sur les matériels ou logiciels utilisés		-	-	-	-	Non traité	-
Administrateur système	3	2	3	Usurpation de droits	-	Absence de protection d'informations secrètes d'authentification		-	-	-	-	Non traité	-

Page : 1 Lignes par page : 20 1 - 20 de 79

- Vue principale de MONARC
  - Évaluation de quelques risques de l'information

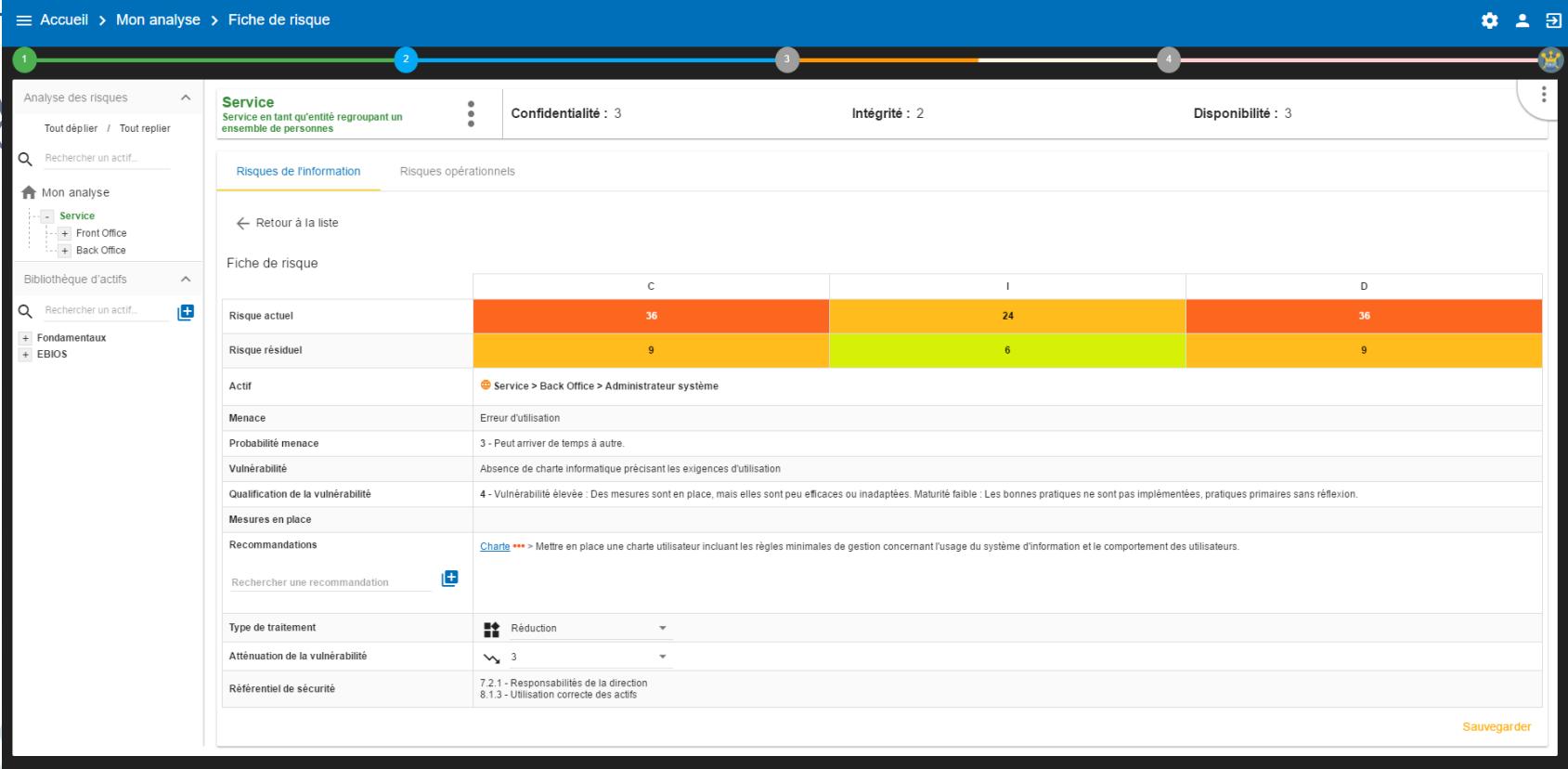
# 3.1 – ESTIMATION, ÉVALUATION ET TRAITEMENT DES RISQUES



The screenshot shows the MONARC software interface. At the top, there's a navigation bar with four colored segments (green, blue, orange, red) and a status bar indicating 'Service' (Confidentialité : 3, Intégrité : 2, Disponibilité : 3). Below the navigation bar is a search bar and a sidebar with various filters and categories like 'Analise des risques', 'Service', and 'Bibliothèque d'actifs'. The main area displays a table titled '9 risques opérationnels' with columns for 'Actif', 'Description du risque', 'Risque brut' (with sub-columns for Prob., Impact, and Risque actuel), 'Risque net' (with sub-columns for Impact, Risque actuel, and Mesures en place), 'Traitement', and 'Risque résiduel'. The table rows list various operational risks such as 'Absence de formalisation' and 'Les processus ne sont pas documentées ou mis à jour', each with its corresponding risk scores and treatment status.

- Vue principale de MONARC
  - Évaluation de quelques risques opérationnels

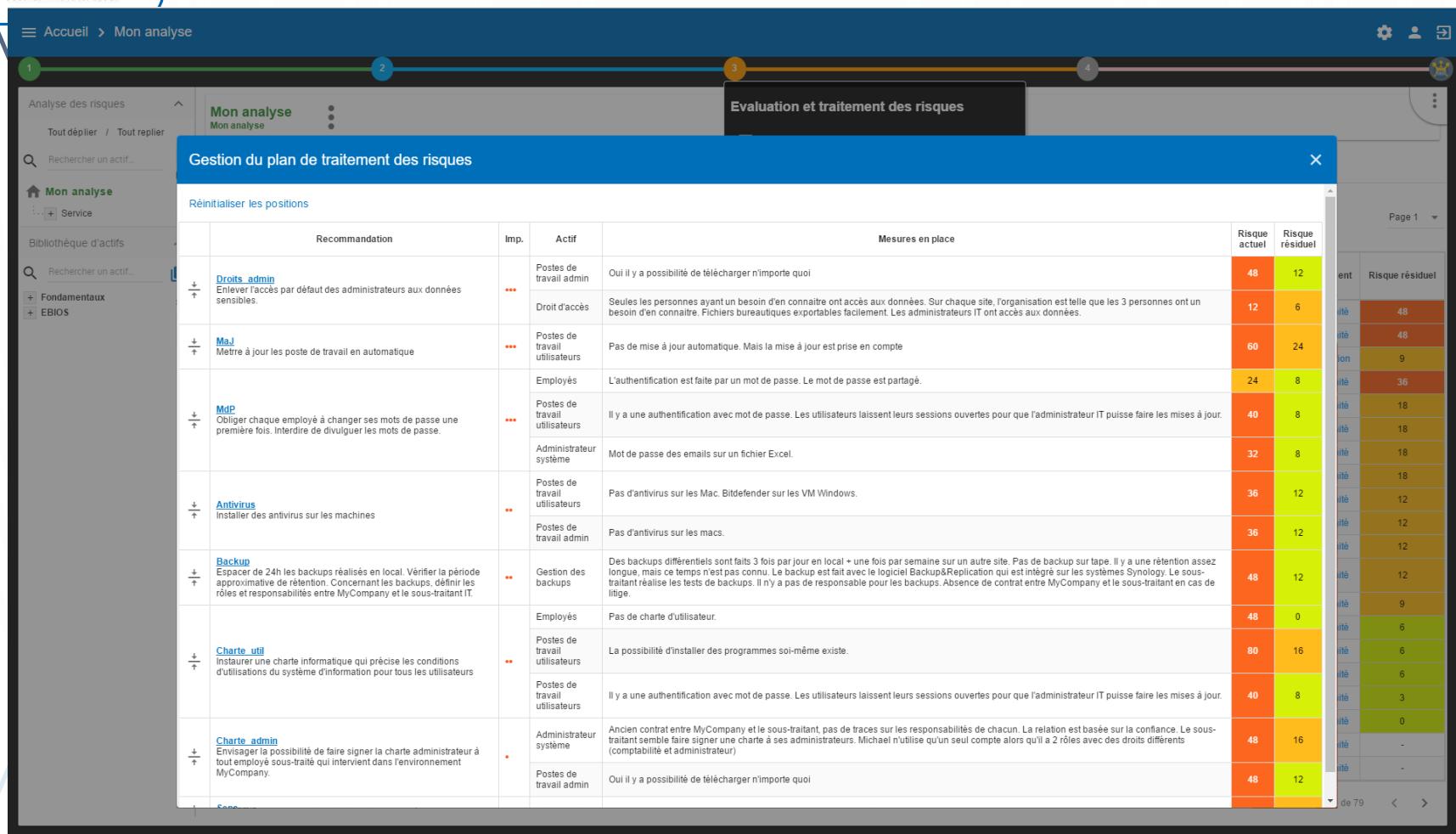
# 3.1 – ESTIMATION, ÉVALUATION ET TRAITEMENT DES RISQUES



The screenshot shows a risk sheet for a 'Service' asset. The top navigation bar includes 'Accueil', 'Mon analyse', 'Fiche de risque', and user icons. A progress bar at the top indicates steps 1 through 4. The main area displays service details ('Service: Service en tant qu'entité regroupant un ensemble de personnes'), risk scores ('Confidentialité : 3', 'Intégrité : 2', 'Disponibilité : 3'), and two tabs: 'Risques de l'information' (selected) and 'Risques opérationnels'. Below these are sections for 'Fiche de risque' (Risk Sheet), 'Risque actuel' (Actual Risk), 'Risque résiduel' (Residual Risk), 'Actif' (Asset), 'Menace' (Threat), 'Probabilité menace' (Threat Probability), 'Vulnérabilité' (Vulnerability), 'Qualification de la vulnérabilité' (Vulnerability Qualification), 'Mesures en place' (Measures in place), 'Recommandations' (Recommendations), 'Rechercher une recommandation' (Search recommendation), 'Type de traitement' (Treatment type), 'Atténuation de la vulnérabilité' (Mitigation of vulnerability), and 'Référentiel de sécurité' (Security reference). A large orange bar chart visualizes the risk levels across categories C, I, and D. A 'Sauvegarder' (Save) button is at the bottom right.

- Fiche de risque
- Création de recommandations

# 3.2 – GESTION DU PLAN DE TRAITEMENT DES RISQUES



The screenshot shows the software interface for risk analysis. At the top, there's a navigation bar with 'Accueil > Mon analyse'. Below it, a horizontal bar has four colored segments: green (1), blue (2), orange (3), and grey (4). The central part of the screen is titled 'Evaluation et traitement des risques' and contains a sub-section titled 'Gestion du plan de traitement des risques'. This section includes a 'Réinitialiser les positions' button and a table with columns: 'Recommandation', 'Imp.', 'Actif', 'Mesures en place', 'Risque actuel', and 'Risque résiduel'. The table lists various recommendations with their status (e.g., 'Droits admin', 'MaJ', 'Mdp', 'Antivirus', 'Backup', 'Charte util', 'Charte admin'). The 'Risque actuel' column uses a color-coded scale from red (high) to green (low), while the 'Risque résiduel' column uses a color-coded scale from red (high) to yellow (low). A sidebar on the left shows 'Mon analyse' and 'Bibliothèque d'actifs' sections.

Recommandation	Imp.	Actif	Mesures en place	Risque actuel	Risque résiduel
Droits admin Enlever l'accès par défaut des administrateurs aux données sensibles.	...	Postes de travail admin	Oui il y a possibilité de télécharger n'importe quoi	48	12
		Droit d'accès	Seules les personnes ayant un besoin d'en connaître ont accès aux données. Sur chaque site, l'organisation est telle que les 3 personnes ont un besoin d'en connaître. Fichiers bureautiques exportables facilement. Les administrateurs IT ont accès aux données.	12	6
MaJ Mettre à jour le poste de travail en automatique	...	Postes de travail utilisateurs	Pas de mise à jour automatique. Mais la mise à jour est prise en compte	60	24
		Employés	L'authentification est faite par un mot de passe. Le mot de passe est partagé.	24	8
Mdp Obliger chaque employé à changer ses mots de passe une première fois. Interdire de divulguer les mots de passe.	...	Postes de travail utilisateurs	Il y a une authentication avec mot de passe. Les utilisateurs laissent leurs sessions ouvertes pour que l'administrateur IT puisse faire les mises à jour.	40	8
		Administrateur système	Mot de passe des emails sur un fichier Excel.	32	8
Antivirus Installer des antivirus sur les machines	..	Postes de travail utilisateurs	Pas d'antivirus sur les Mac. Bitdefender sur les VM Windows.	36	12
		Postes de travail admin	Pas d'antivirus sur les macs.	36	12
Backup Espacer de 24h les backups réalisés en local. Vérifier la période approximative de rétention. Concernant les backups, définir les rôles et responsabilités entre MyCompany et le sous-traitant IT.	..	Gestion des backups	Des backups différentiels sont faits 3 fois par jour en local + une fois par semaine sur un autre site. Pas de backup sur tape. Il y a une rétention assez longue, mais ce temps n'est pas connu. Le backup est fait avec le logiciel Backup&Replication qui est intégré sur les systèmes Synology. Le sous-traitant réalise les tests de backups. Il n'y a pas de responsable pour les backups. Absence de contrat entre MyCompany et le sous-traitant en cas de litige.	48	12
		Employés	Pas de charte d'utilisateur.	48	0
Charte util Instaurer une charte informatique qui précise les conditions d'utilisations du système d'information pour tous les utilisateurs	..	Postes de travail utilisateurs	La possibilité d'installer des programmes soi-même existe.	80	16
		Postes de travail utilisateurs	Il y a une authentication avec mot de passe. Les utilisateurs laissent leurs sessions ouvertes pour que l'administrateur IT puisse faire les mises à jour.	40	8
Charte admin Envisager la possibilité de faire signer la charte administrateur à tout employé sous-traité qui intervient dans l'environnement MyCompany.	..	Administrateur système	Ancien contrat entre MyCompany et le sous-traitant, pas de traces sur les responsabilités de chacun. La relation est basée sur la confiance. Le sous-traitant semble faire signer une charte à ses administrateurs. Michael n'utilise qu'un seul compte alors qu'il a 2 rôles avec des droits différents (comptabilité et administrateur)	48	16
		Postes de travail admin	Oui il y a possibilité de télécharger n'importe quoi	48	12

- Liste de tous les risques faisant l'objet d'une recommandation
- Risques de l'information et risques opérationnels.



cases.lu  
Secure. Innovate. Lead.

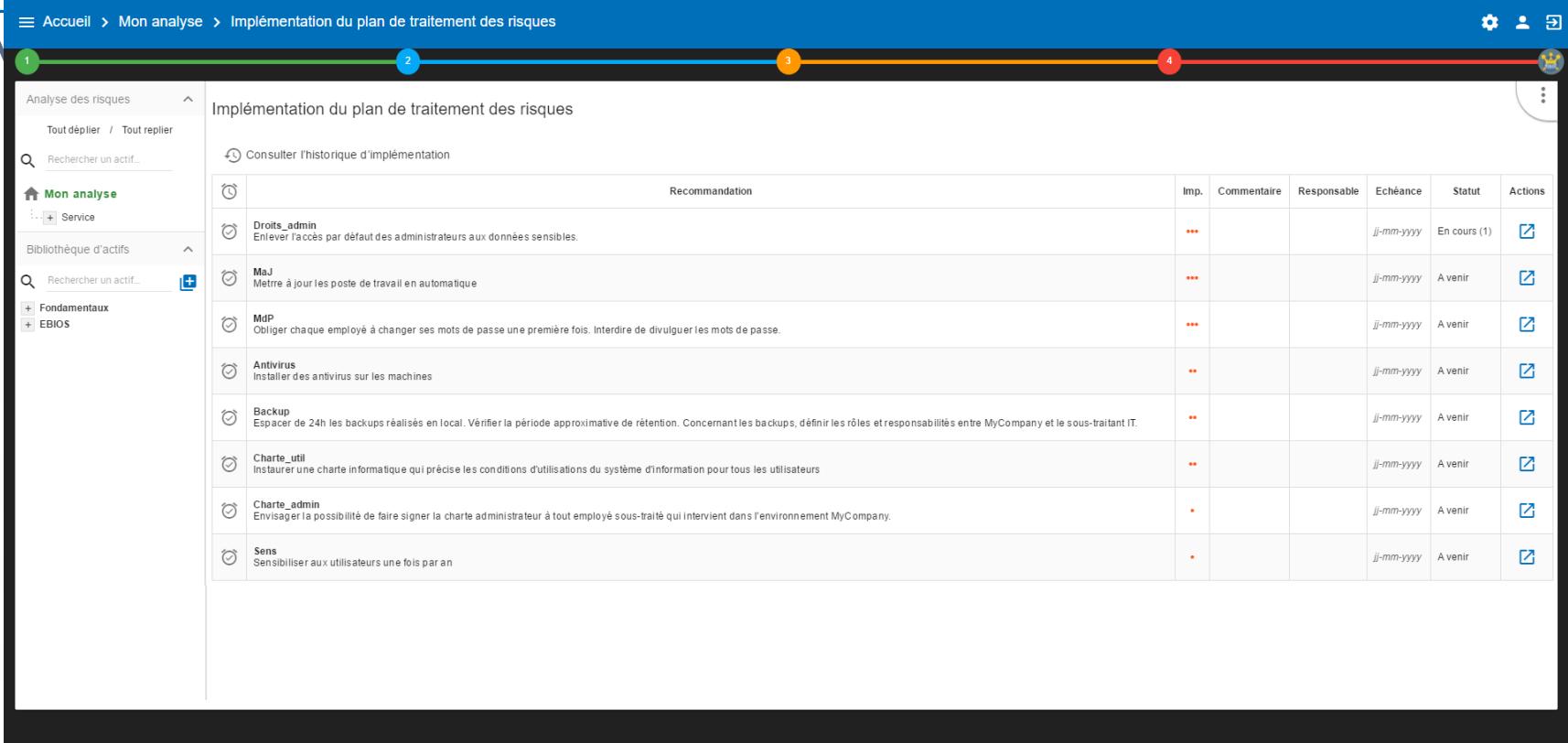
## 3.3 – LIVRABLE : RAPPORT FINAL

The screenshot shows the software's main dashboard with a navigation bar at the top. A central modal window titled "Livrable" is open, displaying risk analysis details. The modal includes fields for Status (Final), Version (1.0), Classification (Confidentielle), and Responsible(s) client (M. Thill). It also contains a "Synthèse de l'évaluation des risques:" section with a Microsoft Word document placeholder. At the bottom of the modal are "Annuler" and "Sauvegarder" buttons. The background shows a grid of risk data with columns for Mesures en place, Qualif., Impact (C, I, D), Treatment, and Risque résiduel. The grid rows show various risk items like "Usurpation de droits" and "Absence de protection d'informations secrètes d'authentification".

- Reprise exhaustive de toutes les informations collectées et saisies
- Possibilité de saisir un résumé de l'analyse.
- Format de sortie : Microsoft Word

Démonstration

# 4.1 – GESTION DE L'IMPLEMENTATION DES RECOMMANDATIONS



The screenshot shows the 'Implémentation du plan de traitement des risques' (Implementation of the risk treatment plan) section of the cases.lu platform. The interface includes a navigation bar at the top with 'Accueil > Mon analyse > Implémentation du plan de traitement des risques'. A progress bar at the top indicates the process flow from analysis to implementation.

The main area displays a table of recommendations:

	Recommandation	Imp.	Commentaire	Responsable	Echéance	Statut	Actions
1	Droits_admin Enlever l'accès par défaut des administrateurs aux données sensibles.	...			jj-mm-yyyy	En cours (1)	<input type="checkbox"/>
2	MoJ Mettre à jour les poste de travail en automatique	...			jj-mm-yyyy	A venir	<input type="checkbox"/>
3	MdP Obliger chaque employé à changer ses mots de passe une première fois. Interdire de divulguer les mots de passe.	...			jj-mm-yyyy	A venir	<input type="checkbox"/>
4	Antivirus Installer des antivirus sur les machines	..			jj-mm-yyyy	A venir	<input type="checkbox"/>
	Backup Espacez de 24h les backups réalisés en local. Vérifier la période approximative de rétention. Concernant les backups, définir les rôles et responsabilités entre MyCompany et le sous-traitant IT.	..			jj-mm-yyyy	A venir	<input type="checkbox"/>
	Charte_util Instaurer une charte informatique qui précise les conditions d'utilisations du système d'information pour tous les utilisateurs	..			jj-mm-yyyy	A venir	<input type="checkbox"/>
	Charte_admin Envisager la possibilité de faire signer la charte administrateur à tout employé sous-traité qui intervient dans l'environnement MyCompany.	.			jj-mm-yyyy	A venir	<input type="checkbox"/>
	Sens Sensibiliser aux utilisateurs une fois par an	.			jj-mm-yyyy	A venir	<input type="checkbox"/>

- Affection de responsables et délais pour la mise en place des recommandations



cases.lu  
Secure. Innovate. Lead.

# 4.1 – GESTION DE L'IMPLEMENTATION DES RECOMMANDATIONS

The screenshot shows a software interface for risk management. At the top, a navigation bar includes links for Accueil, Mon analyse, Implémentation du plan de traitement des risques, and Recommandation. A progress bar at the top right is divided into four colored segments: green (step 1), blue (step 2), orange (step 3), and red (step 4). The main content area displays a table titled 'Maj' (Update) with the sub-instruction 'Mettre à jour les poste de travail en automatique' (Automatically update workstations). The table has columns for Actif (Active), Menace (Threat), Vulnérabilité (Vulnerability), Mesures en place (Measures in place), Risque actuel (Current risk), Nouvelles mesures (New measures), Risque résiduel (Residual risk), and Actions (Actions). One row is shown: 'Postes de travail utilisateurs' (User workstations) under 'Actif', 'MDA13 - Infection par un malware' under 'Menace', '1178 - La gestion des mises à jour (patch) comporte des lacunes' under 'Vulnérabilité', 'Pas de mise à jour automatique. Mais la mise à jour est prise en compte' under 'Mesures en place', '60' under 'Risque actuel', '24' under 'Risque résiduel', and a checked checkbox under 'Actions'. On the left, there's a sidebar with sections for Analyse des risques, Mon analyse (selected), and Bibliothèque d'actifs.

- Validation risque par risque du changement d'état
- Changement valeur du risque : Risque visé devient risque actuel

# AGENDA

- ▶ Qu'est-ce que MONARC ?
- ▶ Découverte et utilisation de l'outil
- ▶ Déroulement de la méthode
- ▶ **Trucs & Astuces**



cases.lu

Secure. Innovate. Lead.

# CRÉATION D'UN NOUVEAU RISQUE

The screenshot shows the cases.lu software interface. At the top, there is a navigation bar with the following items: Accueil > Mon analyse > Base de connaissances. Below the navigation bar is a horizontal bar with four colored circles (green, blue, orange, red) and corresponding numbers (1, 2, 3, 4). The main area displays a table of asset types. The table has columns: Statut, Libellé (sorted by ascending order), Code, Type, Description, and Actions (with edit and delete icons). The data in the table is as follows:

Statut	Libellé	Type	Description	Actions
✓	Annuaire d'entreprise	Secondaire	Annuaire d'entreprise	[Edit] [Delete]
✓	Application métier	Secondaire	Application métier sur mesure ou standard	[Edit] [Delete]
✓	Autres supports	Secondaire	Documents, Fax, Lettre, BdC, information papier, etc.	[Edit] [Delete]
✓	Backup	Secondaire	Qualification des backups	[Edit] [Delete]
✓	Bâtiment, bureau ou local	Secondaire	Bâtiment, bureau ou local	[Edit] [Delete]
✓	Conteneur	Primaire	Conteneur d'actifs	[Edit] [Delete]
✓	Décisionnel	Secondaire	Décisionnel	[Edit] [Delete]
✓	Développements d'applications	Secondaire	Développements d'applications	[Edit] [Delete]
✓	Développeur	Secondaire	Développeur	[Edit] [Delete]
✓	Dispositif d'accès internet	Secondaire	Dispositif d'accès internet	[Edit] [Delete]
✓	Document papier	Secondaire	Information sous forme physique	[Edit] [Delete]
✓	Exploitant / Maintenance	Secondaire	Exploitant / Maintenance	[Edit] [Delete]
✓	Générale	Secondaire	Organisation générale de l'organisme	[Edit] [Delete]

1. Création d'un type d'actif
2. Création d'une menace
3. Création vulnérabilité
4. Association Actif / Menace / Vulnérabilité
5. Création actif dans la bibliothèque
6. Utilisation de l'actif dans l'analyse



cases.lu  
Secure. Innovate. Lead.

# IMPORT / EXPORT ACTIF

The screenshot shows the 'Mon analyse' section of the cases.lu software. The left sidebar has sections for 'Analyse des risques' (with 'Tout déplier / Tout replier' and 'Rechercher un actif...'), 'Mon analyse' (selected), 'Bibliothèque d'actifs' (with 'Rechercher un actif...', 'Fondamentaux', and 'EBIOS'), and a search bar. The main area has tabs for 'Mon analyse' (selected), 'Risques de l'information', and '79 risques de l'information'. It includes buttons for 'Modifier l'analyse des risques', 'Importer une analyse de risques', 'Exporter toute l'analyse des risques', and 'Supprimer l'analyse'. Below these are filters for 'Type de traitement', 'Tier', 'Sens du tri', 'Risque MAX', and 'Décroissant'. The main table displays 79 risks across columns for Actif, Impact (C, I, D), Menace (Libellé, Prob.), Vulnérabilité (Libellé, Mesures en place, Qualif.), Risk actuel (C, I, D), Traitement, and Risque résiduel. The table rows include various risk types such as 'Usurpation de droits', 'Infection par un malware', and 'Abus de droits', with corresponding scores and treatment status.

- Possibilité d'importer et d'exporter des actifs :
  - de la bibliothèque
  - de l'analyse, avec ou sans l'évaluation .

Démonstration