



**cases.lu**

Secure. Innovate. Lead.

# **WORKSHOP MONARC** **(MÉTHODE OPTIMISÉE D'ANALYSE DES** **RISQUES CASES)**

FORMATION MONARC V2.0

INFO@CASES.LU

**SECURITY**  
**MADEIN.LU**



# SECURITYMADEIN.LU



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



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*

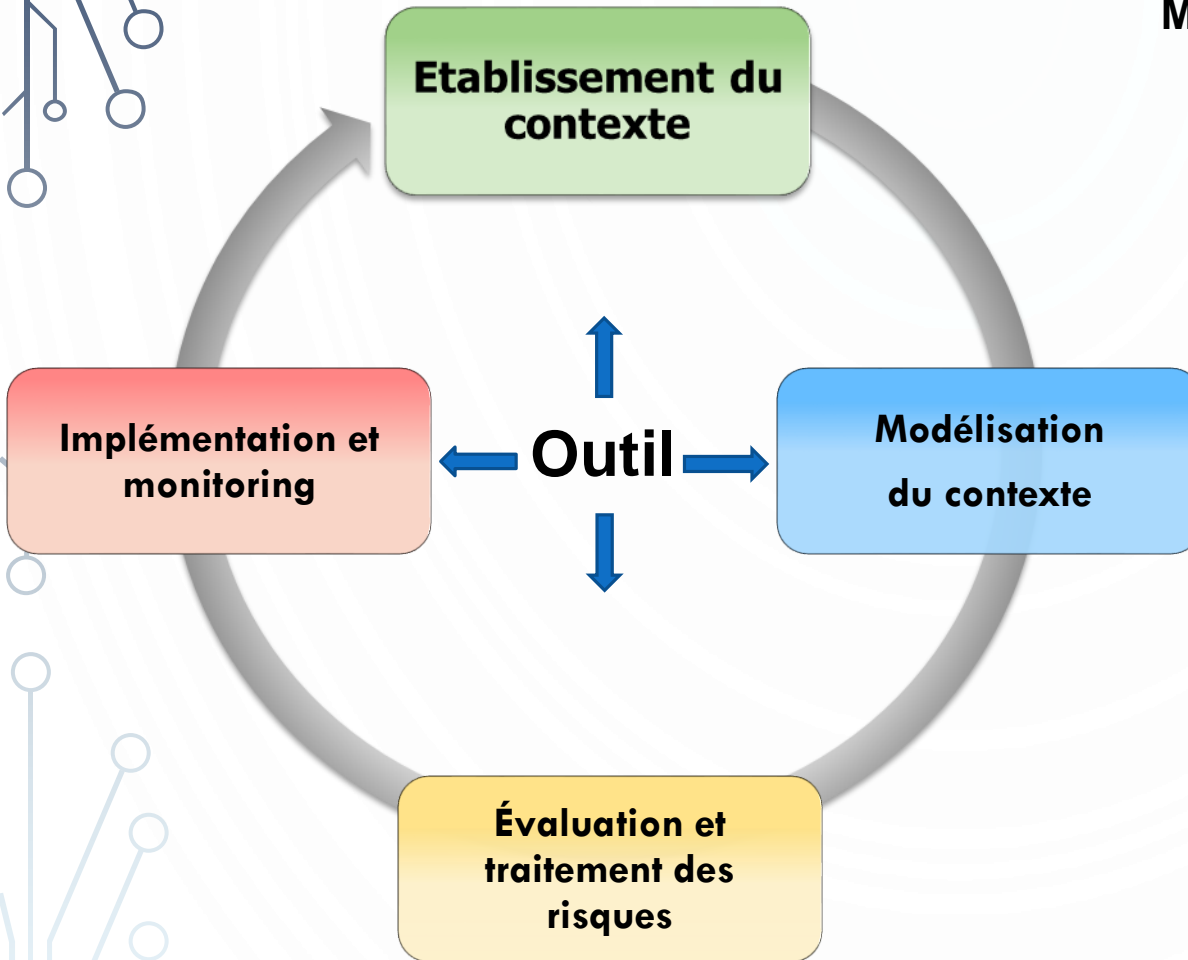
[www.securitymadein.lu](http://www.securitymadein.lu)  
[www.cases.lu](http://www.cases.lu)



# 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



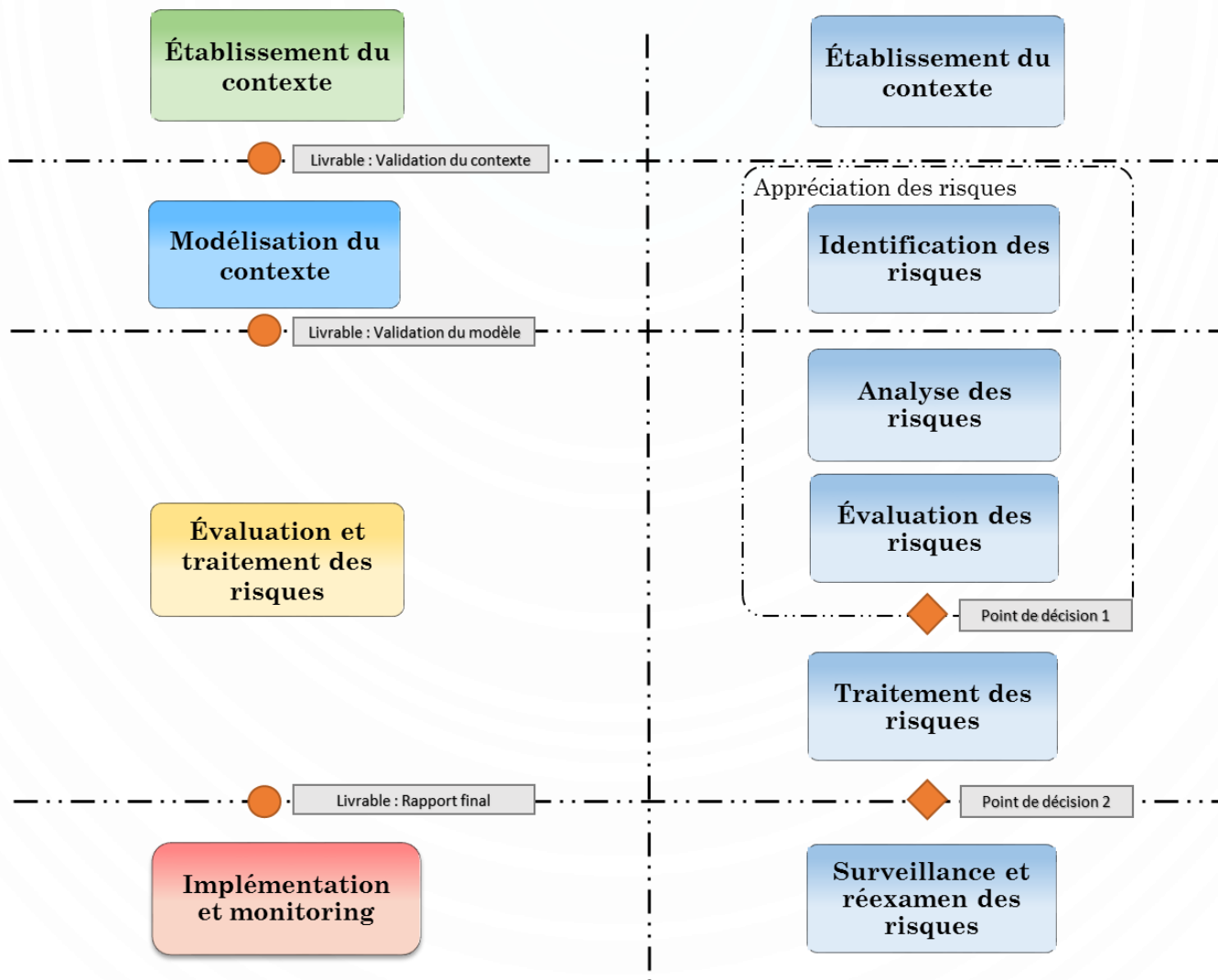
## Méthode d'analyse des risques

- **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

Accueil > Mon analyse

Mon analyse

+ Créer une analyse des risques

Copyright © 2012-2016 - securitymadein.lu - All rights reserved - Legal

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

Mon analyse

+ Service

Bibliothèque d'actifs

Rechercher un actif...

+ Fondamentaux

+ EBIOS

Mon analyse

Analyse de risques

Risques de l'information Risques opérationnels

91 risques de l'information

Seuil de risque (sur le CID max) ☒ ☐ ☐ ☐ ☐ Mots-clés 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		
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 système	-	-	-	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

## Établissement du contexte

- 1.1 - Contexte de l'analyse des risques
- 1.2 - Evaluation des tendances, des menaces et synthèse
- 1.3 - Organisation de la gestion des risques
- 1.4 - Définition des critères d'évaluation des risques

1.5 - Livrable : Validation du contexte

## Modélisation du contexte

- 2.1 - Identification des actifs, des vulnérabilités et appréciation des impacts
- 2.2 - Synthèse des actifs / impacts

2.3 - Livrable : Validation du modèle

## Évaluation et traitement des risques

- 3.1 - Estimation, évaluation et traitement des risques
- 3.2 - Gestion du plan de traitement des risques

3.3 - Livrable : Rapport final

## Implémentation et surveillance

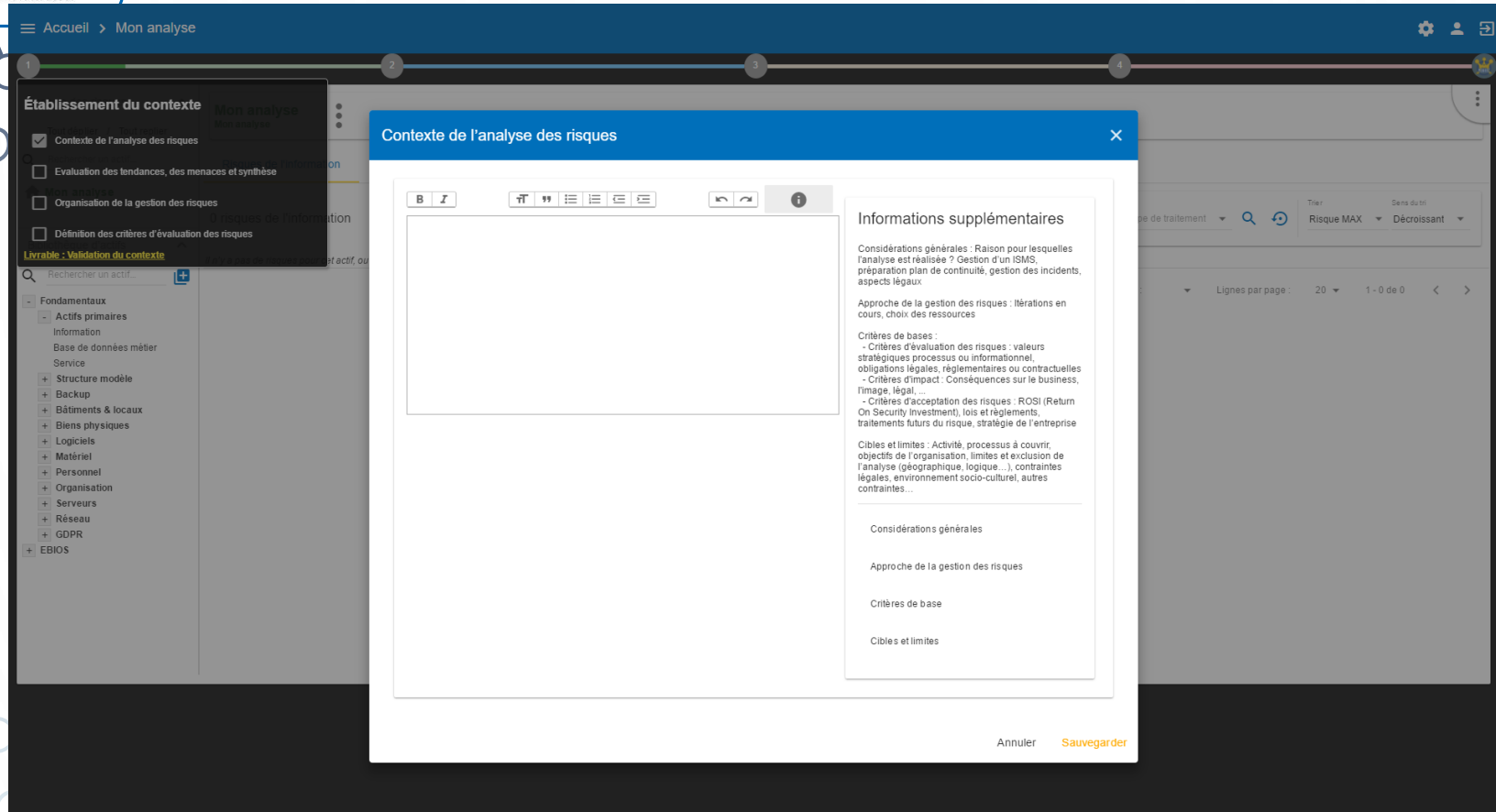
- 4.1 - Gestion de l'implémentation du plan de traitement des risques



**cases.lu**

Secure. Innovate. Lead.

# 1.1 – CONTEXTE DE L'ANALYSE DES RISQUES



- 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 displays the 'cases.lu' web application interface. The top navigation bar includes 'Accueil' and 'Mon analyse'. A sidebar on the left lists various modules under 'Fondamentaux', with 'Actifs primaires' expanded. The main content area is titled 'Evaluation des tendances, des menaces et synthèse' and contains a form with several questions in French. A 'Sauvegarder' button is visible at the bottom right of the form.

**Établissement du contexte**

- ☒ Contexte de l'analyse des risques
- ☒ Evaluation des tendances, des menaces et synthèse
- ☐ Organisation de la gestion des risques
- ☐ Définition des critères d'évaluation des risques

**Livrable : Validation du contexte**

Rechercher un actif...

**Fondamentaux**

- Actifs primaires
  - Information
  - Base de données métier
  - Service
  - + Structure modèle
  - + Backup
  - + Bâtiments & locaux
  - + Biens physiques
  - + Logiciels
  - + Matériel
  - + Personnel
  - + Organisation
  - + Serveurs
  - + Réseau
  - + GDPR
  - + EBIOS

**Evaluation des tendances, des menaces et synthèse**

Évaluation des tendances | Evaluation des menaces | Résumé

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 ?

Sauvegarder

- 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 displays the 'cases.lu' web application interface. The main navigation bar at the top shows 'Accueil > Mon analyse'. A sidebar on the left lists various categories under 'Fondamentaux', including 'Actifs primaires', 'Information', 'Base de données métier', 'Service', 'Structure modèle', 'Backup', 'Bâtiments & locaux', 'Biens physiques', 'Logiciels', 'Matériel', 'Personnel', 'Organisation', 'Serveurs', 'Réseau', 'GDPR', and 'EBIOS'. The main content area is titled 'Établissement du contexte' and includes a checklist for 'Contexte de l'analyse des risques', 'Evaluation des tendances, des menaces et synthèse', 'Organisation de la gestion des risques', and 'Définition des critères d'évaluation des risques'. A modal window titled 'Evaluation des tendances, des menaces et synthèse' is open, showing the 'Evaluation des menaces' tab. The modal contains a form for 'Analyse des menaces - 1 / 30' with fields for 'Thème', 'Description', 'Commentaires', 'Critère impacté', 'Tendances', and 'Probabilité'. The 'Tendances' field has a scale from -1 to ++. The 'Probabilité' field has a dropdown menu and a checkbox for 'Forcer la probabilité dans l'analyse'. The modal also includes navigation buttons for 'Précédent', 'Sauvegarder', and 'Suivant'.

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



**cases.lu**

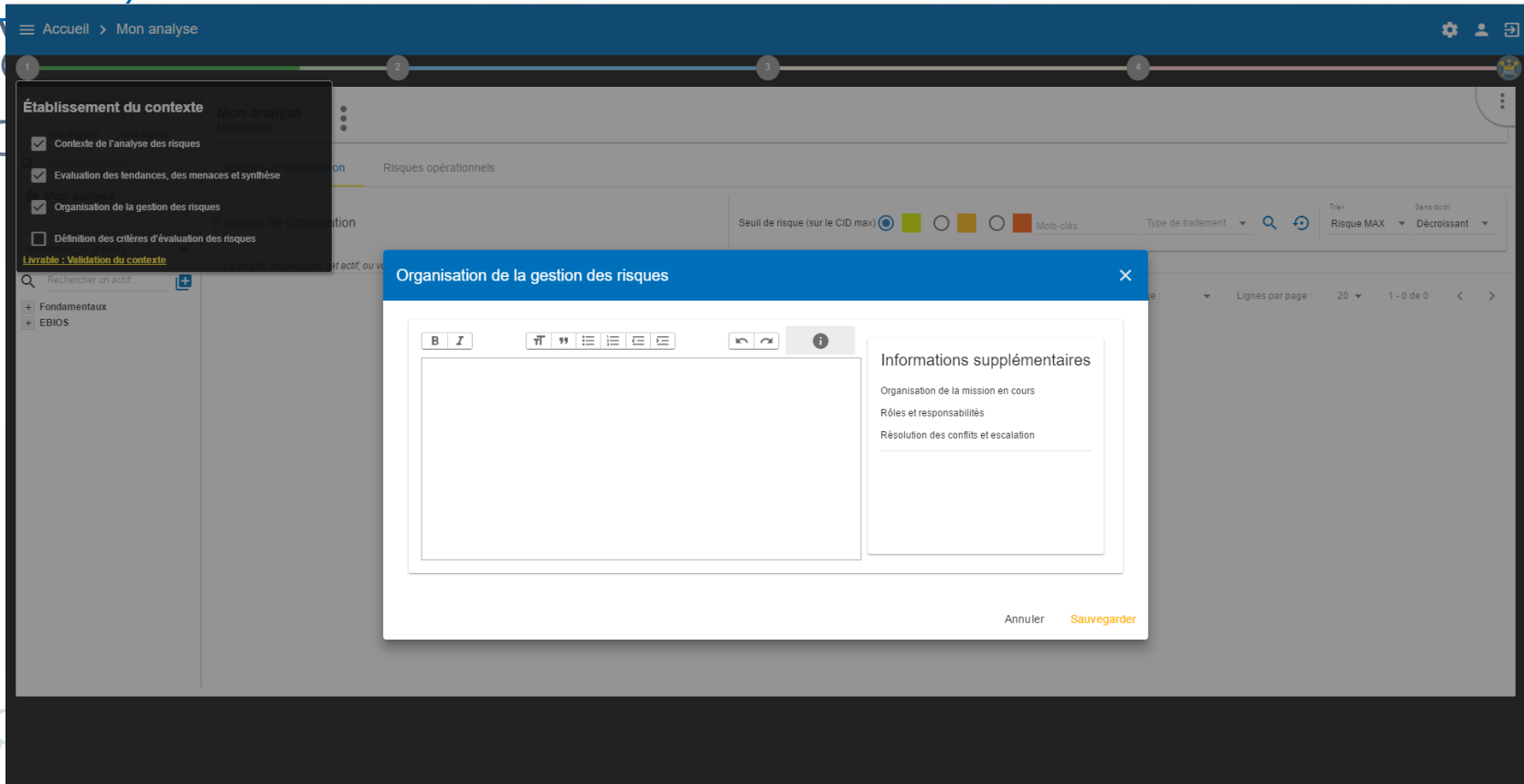
Secure. Innovate. Lead.

# 1.2 – RÉSUMÉ

The screenshot displays the 'cases.lu' web application interface. The top navigation bar includes 'Accueil' and 'Mon analyse'. A sidebar on the left lists various asset categories under 'Fondamentaux', such as 'Actifs primaires', 'Information', 'Base de données métier', 'Service', 'Structure modèle', 'Backup', 'Bâtiments & locaux', 'Biens physiques', 'Logiciels', 'Matériel', 'Personnel', 'Organisation', 'Serveurs', 'Réseau', 'GDPR', and 'EBIOS'. The main content area shows a progress bar with four steps. A modal window titled 'Evaluation des tendances, des menaces et synthèse' is open, with tabs for 'Évaluation des tendances', 'Évaluation des menaces', and 'Résumé'. The 'Résumé' tab is active, showing a text area for notes and a 'Sauvegarder' button. The background interface includes a search bar, a 'Seuil de risque' filter, and a 'Type de traitement' dropdown.

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

## 1.3 – ORGANISATION DE LA GESTION DES RISQUES



The screenshot displays the 'cases.lu' web application interface. The main menu at the top includes 'Accueil' and 'Mon analyse'. A sidebar on the left lists several tasks under 'Établissement du contexte': 'Contexte de l'analyse des risques', 'Evaluation des tendances, des menaces et synthèse', 'Organisation de la gestion des risques' (which is highlighted), and 'Définition des critères d'évaluation des risques'. The 'Livraison : Validation du contexte' section is also visible. The main content area shows a list of risks, with a filter for 'Seuil de risque (sur le CID max)' and a search bar. A modal dialog box titled 'Organisation de la gestion des risques' is open in the foreground. This dialog has a text editor on the left and a section titled 'Informations supplémentaires' on the right, which contains the following text: 'Organisation de la mission en cours', 'Rôles et responsabilités', and 'Résolution des conflits et escalation'. At the bottom of the dialog 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

# 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 : - Divulgence 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 : - Divulgence 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 gér Ex - D 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		
Impact	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 displays the 'cases.lu' web application interface. A modal window titled 'Livrable' (Deliverable) is open, showing the 'Validation du contexte' (Context Validation) form. The form contains the following fields:

- Statut: Final
- Version: 1.0
- Classification: Confidentielle
- Nom du document: Rapport établissement du contexte
- Responsable(s) client: M. Thill
- Consultant(s) sécurité: M. Muller

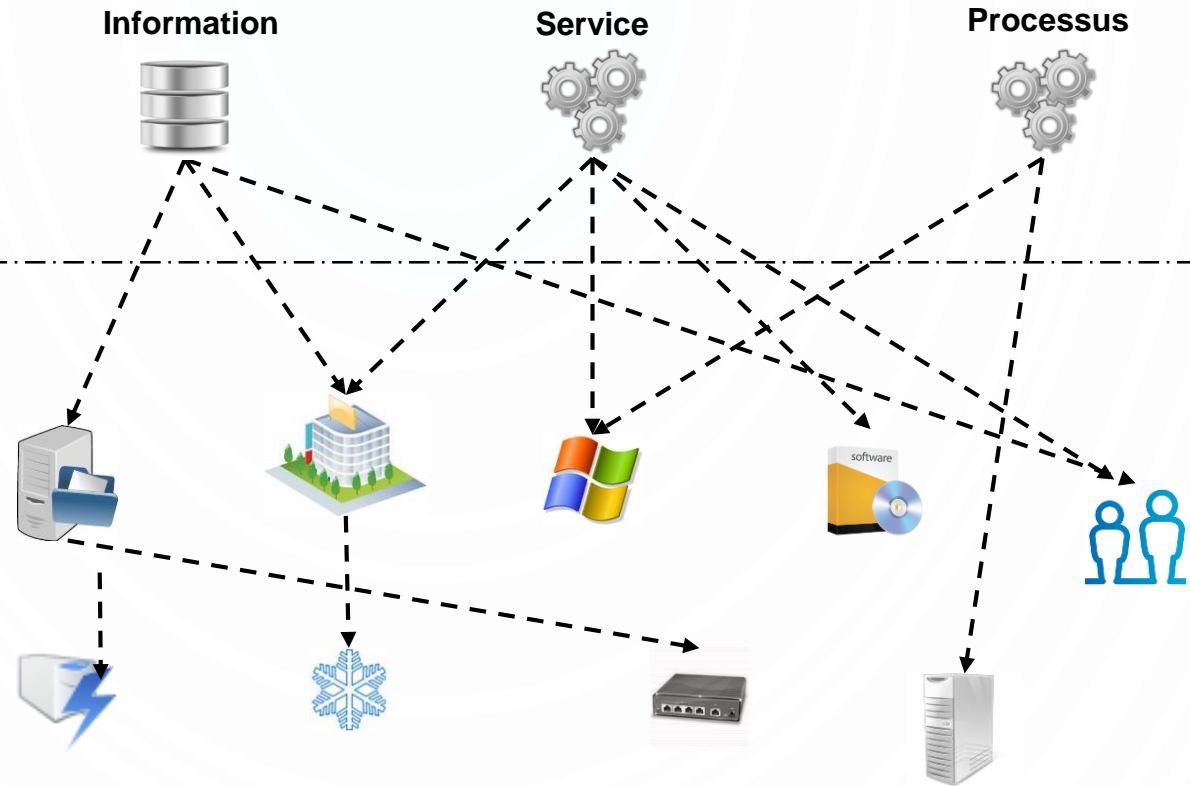
At the bottom of the modal, there are buttons for 'Annuler' (Cancel) and 'Sauvegarder' (Save). The background shows the application's navigation menu with options like 'Accueil', 'Mon analyse', and 'Risques opérationnels'. A sidebar on the left lists various risk categories, and a main panel on the right displays a list of risks with 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**

- **Service**

- Front Office

- Bureau du service

🌐 Employés

🌐 Postes de travail utilisateurs

- Logiciel

🌐 Maintenance logiciel

**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	Faibles 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

# 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**

**21 risques**

## “Global”

Mon analyse

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

Base de données N°1

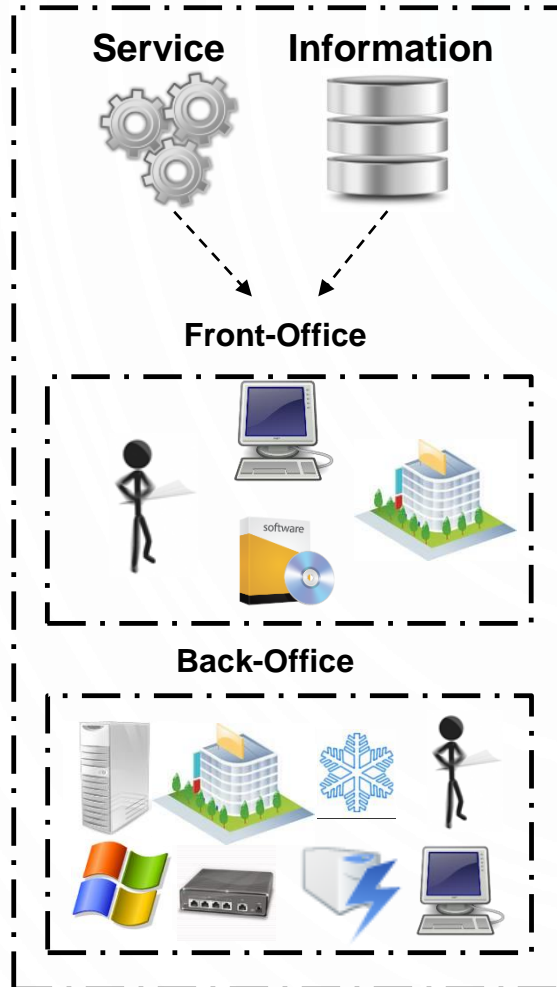
Base de données N°2



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

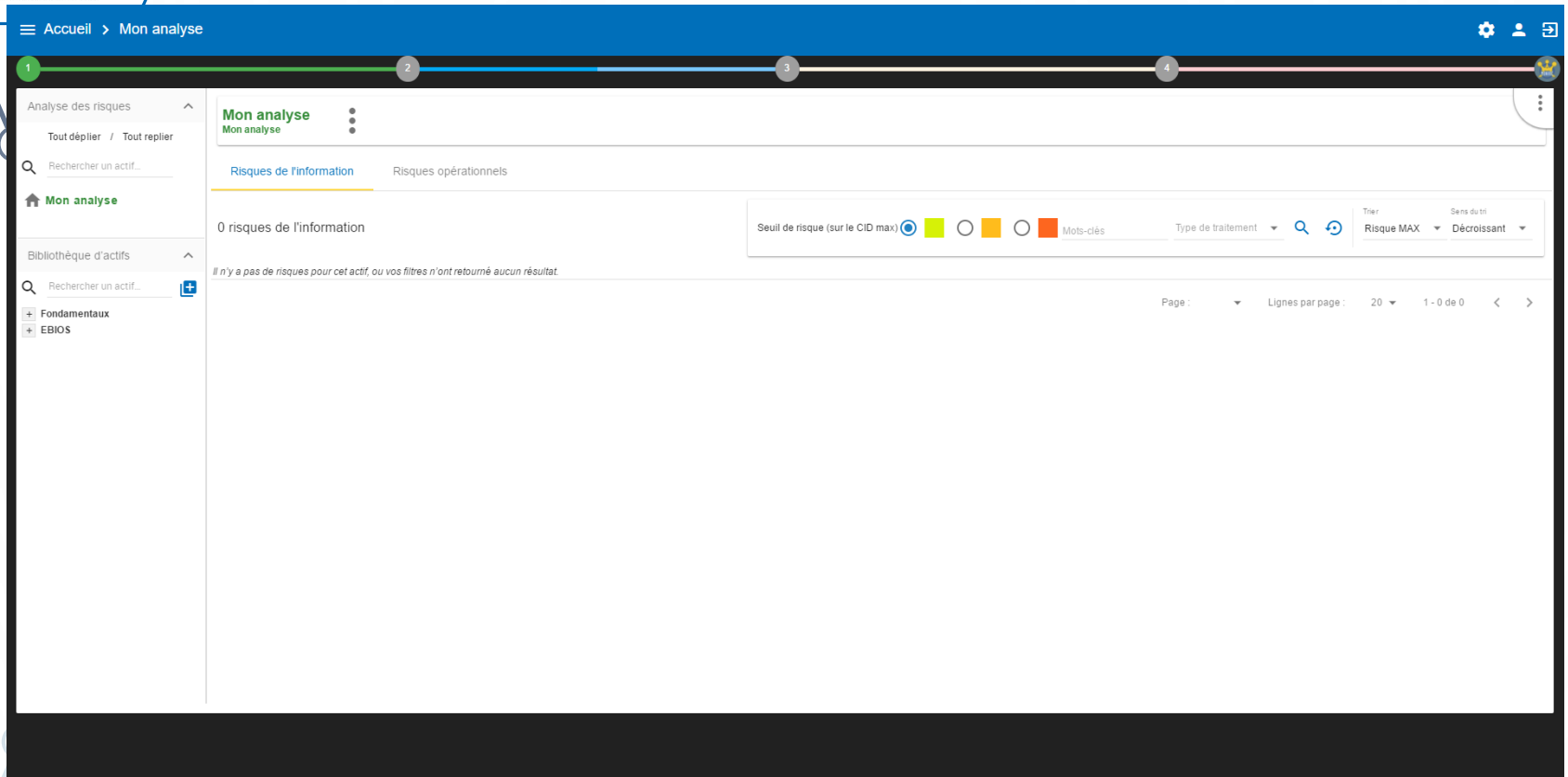


# MODÉLISATION CASES



- **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

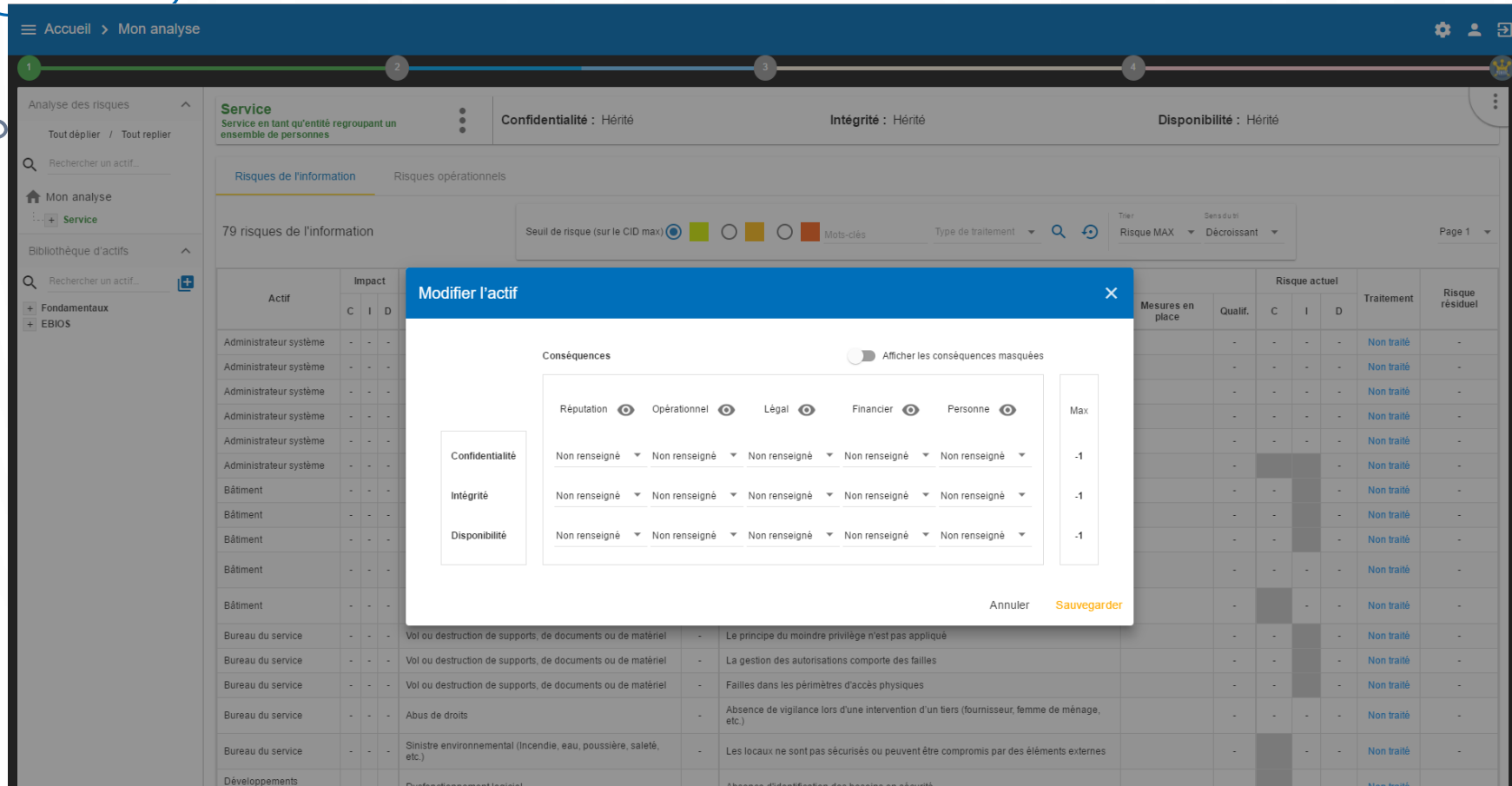
## 2.1 – IDENTIFICATION DES ACTIFS, DES VULNÉRABILITÉS ET APPRÉCIATION DES IMPACTS



- 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

**Démonstration**

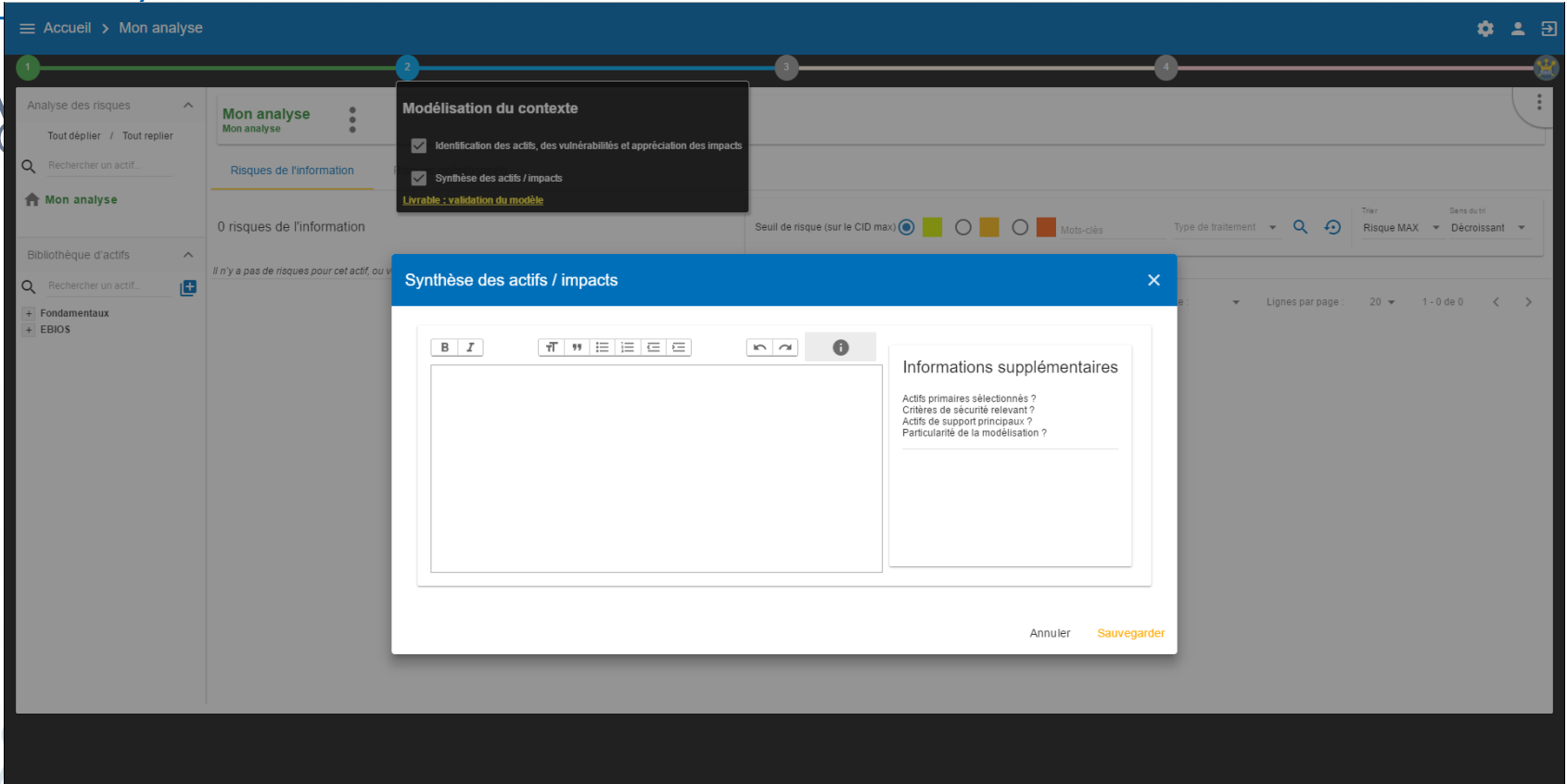
## 2.1 – IDENTIFICATION DES ACTIFS, DES VULNÉRABILITÉS ET APPRÉCIATION DES IMPACTS



The screenshot displays the MONARC risk analysis interface. The main window shows a list of risks under the 'Risques de l'information' tab. A modal dialog titled 'Modifier l'actif' is open, allowing the user to edit the consequences of a selected asset. The dialog includes a table for defining consequences across different domains: Confidentialité, Intégrité, and Disponibilité. Each domain has a 'Non renseigné' dropdown and a 'Max' value. The background interface shows a sidebar with navigation options like 'Analyse des risques', 'Mon analyse', and 'Bibliothèque d'actifs'. The main content area displays a table of risks with columns for 'Actif', 'Impact', 'Confidentialité', 'Intégrité', 'Disponibilité', 'Risque actuel', 'Traitement', and 'Risque résiduel'.

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

## 2.2 – SYNTHÈSE DES ACTIFS / IMPACTS

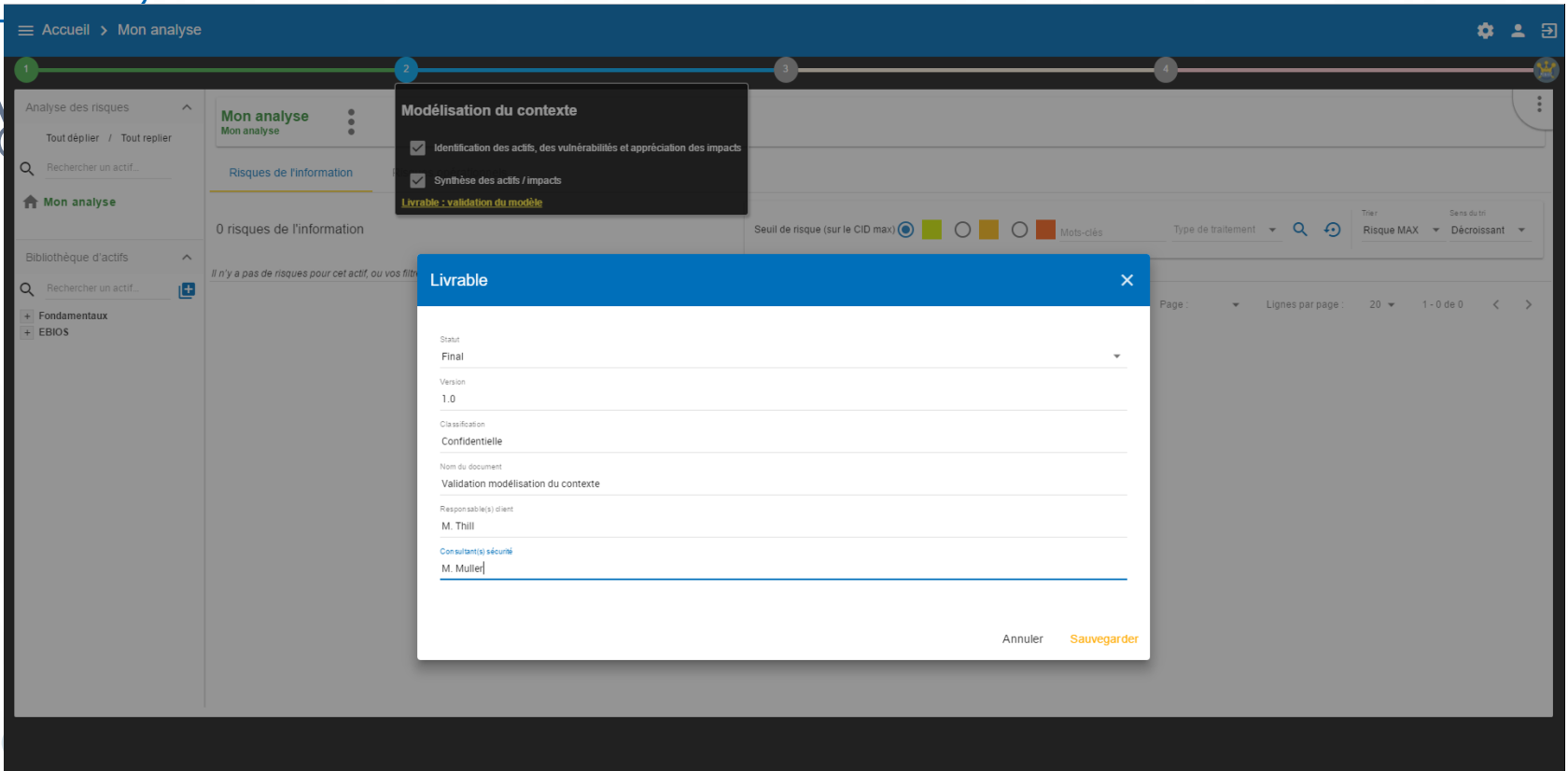


The screenshot displays the 'cases.lu' web application interface. The main navigation bar at the top shows 'Accueil' and 'Mon analyse'. The left sidebar contains 'Analyse des risques' and 'Bibliothèque d'actifs'. The central area is titled 'Mon analyse' and shows 'Risques de l'information' with '0 risques de l'information'. A modal window titled 'Synthèse des actifs / impacts' is open, featuring a text editor with bold and italic buttons, and a section for 'Informations supplémentaires' with a list of questions: 'Actifs primaires sélectionnés?', 'Critères de sécurité relevant?', 'Actifs de support principaux?', and 'Particularité de la modélisation?'. The modal also includes 'Annuler' and 'Sauvegarder' buttons. A smaller 'Modélisation du contexte' modal is also visible, with checkboxes for 'Identification des actifs, des vulnérabilités et appréciation des impacts' and 'Synthèse des actifs / impacts', and a note 'Livrable : validation du modèle'.

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



## 2.3 – LIVRABLE : VALIDATION DU MODÈLE



The screenshot displays the 'cases.lu' web application interface. The top navigation bar shows 'Accueil > Mon analyse'. The main content area is titled 'Mon analyse' and includes a sidebar with 'Analyse des risques' and 'Bibliothèque d'actifs'. The central panel shows 'Risques de l'information' with 0 risks listed. A modal window titled 'Modélisation du contexte' is open, showing two checked items: 'Identification des actifs, des vulnérabilités et appréciation des impacts' and 'Synthèse des actifs / impacts'. Below this, a 'Livable : validation du modèle' button is visible. A second modal window titled 'Livable' is open, containing a form with the following fields: '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). The form has 'Annuler' and 'Sauvegarder' buttons at the bottom right.

- 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

Matériel

Organisation

Personnel

Serveurs

Réseau

EBIOS

Mon analyse

Risques de l'information

Risques opérationnels

79 risques de l'information

Seuil de risque (sur le CID max)

Mots-clés

Type de traitement

Trier

Sans du tri

Risque MAX

Décroissant

Page 1

Evaluation et traitement des risques

☒ Estimation, évaluation et traitement des risques

☐ Gestion du plan de traitement des risques

Livrable : rapport final

Actif	Impact			Menace	Prob.	Vulnérabilité	Mesures en place	Qualif.	Risque actuel			Traitement	Risque résiduel
	C	I	D						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		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	Divulgaration 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

Accueil > Mon analyse

1 2 3 4

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

Mon analyse

Service

Bibliothèque d'actifs

Rechercher un actif...

Fondamentaux

EBIOS

Service

Service en tant qu'entité regroupant un ensemble de personnes

Confidentialité : 3

Intégrité : 2

Disponibilité : 3

Risques de l'information

Risques opérationnels

9 risques opérationnels

Seuil de risque (sur le NET max)

Mots-clés

Type de traitement

Page 1

Actif	Description du risque	Risque brut						Risque net						Mesures en place	Traitement	Risque résiduel		
		Prob.	Impact					Risque actuel	Prob.	Impact							Risque actuel	
			R	O	L	F	P			R	O	L	F	P				
Service	Absence de formalisation	3	1	3	1	2	0	9	2	1	3	1	2	0	6		Non traité	2
Service	Les processus ne sont pas documentés ou mis à jour	3	0	3	0	0	0	9	2	0	2	0	0	0	4		Non traité	2
Service	Les exigences légales et réglementaires applicables ne sont pas déterminées, comprises et satisfaites en permanence	2	2	-	2	-	-	4	2	2	-	2	-	-	4		Non traité	4
Service	Les personnes clés ne sont pas identifiées	1	0	1	0	0	0	1	1	0	1	0	0	0	1		Non traité	1
Service	Absence de planification de ressources nécessaires à mise en oeuvre et à la maîtrise du processus.	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Non traité	-
Service	Absence d'un moyen de retour d'information des clients concernant les produits et services, y compris leurs réclamations	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Non traité	-
Service	Environnement inadéquat pour la mise en oeuvre du processus	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Non traité	-
Service	Le niveau de compétences des personnes n'est pas approprié	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Non traité	-
Service	Les prestataires externes compromettent la qualité du processus	-	-	-	-	-	-	-	-	-	-	-	-	-	-		Non traité	-

+ Créer un risque spécifique

Page : 1 Lignes par page : 20 1 - 9 de 9

- Vue principale de MONARC
  - Évaluation de quelques risques opérationnels

# 3.1 – ESTIMATION, ÉVALUATION ET TRAITEMENT DES RISQUES

Accueil > Mon analyse > Fiche de risque

1 2 3 4

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

Mon analyse

- Service
- Front Office
- Back Office

Bibliothèque d'actifs

Rechercher un actif...

Fondamentaux

EBIOS

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

Confidentialité : 3

Intégrité : 2

Disponibilité : 3

Risques de l'information Risques opérationnels

Retour à la liste

Fiche de risque

	C	I	D
Risque actuel	36	24	36
Risque résiduel	9	6	9

Actif  
Service > Back Office > Administrateur système

Menace  
Erreur d'utilisation

Probabilité menace  
3 - Peut arriver de temps à autre.

Vulnérabilité  
Absence de charte informatique précisant les exigences d'utilisation

Qualification de la vulnérabilité  
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.

Mesures en place

Recommandations  
[Charte](#) > Mettre en place une charte utilisateur incluant les règles minimales de gestion concernant l'usage du système d'information et le comportement des utilisateurs.

Rechercher une recommandation

Type de traitement  
Réduction

Atténuation de la vulnérabilité  
3

Référentiel de sécurité  
7.2.1 - Responsabilités de la direction  
8.1.3 - Utilisation correcte des actifs

Sauvegarder

- Fiche de risque
- Création de recommandations

## 3.2 – GESTION DU PLAN DE TRAITEMENT DES RISQUES

Accueil > Mon analyse

Mon analyse

Evaluation et traitement des risques

Gestion du plan de traitement des risques

Réinitialiser les positions

	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 les 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
Mdp	Obliger chaque employé à changer ses mots de passe une première fois. Interdire de divulguer les mots de passe.	***	Employés	L'authentification est faite par un mot de passe. Le mot de passe est partagé.	24	8
			Postes de travail utilisateurs	Il y a une authentification avec mot de passe. Les utilisateurs laissent leurs sessions ouvertes pour que l'administrateur IT puisse faire les mises à jour.	40	8
Antivirus	Installer des antivirus sur les machines	**	Administrateur système	Mot de passe des emails sur un fichier Excel.	32	8
			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
Charte_util	Instaurer une charte informatique qui précise les conditions d'utilisations du système d'information pour tous les utilisateurs	**	Employés	Pas de charte d'utilisateur.	48	0
			Postes de travail utilisateurs	La possibilité d'installer des programmes soi-même existe.	80	16
			Postes de travail utilisateurs	Il y a une authentification 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

Accueil > Mon analyse

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

Mon analyse

Service

Bibliothèque d'actifs

Rechercher un actif...

Fondamentaux

EBIOS

Risques de l'information

79 risques de l'information

Actif	C	I	D
Organisation informatique	3	2	3
Postes de travail admin	3	2	3
Administrateur système	3	2	3
Postes de travail admin	3	2	3
Administrateur système	3	2	3
Bureau du service	3	2	3
Postes de travail admin	3	2	3
Réseau & télécom	3	2	3
Développements logiciels	3	2	3
Gestion des backups	3	2	3
Postes de travail utilisateurs	3	2	3
Postes de travail utilisateurs	3	2	3
Développements logiciels	3	2	3
Employés	3	2	3
Employés	3	2	3
Organisation informatique	3	2	3
Employés	3	2	3
Gestion serveurs	3	2	3
Administrateur système	3	2	3
Administrateur système	3	2	3

Statut: Final

Version: 1.0

Classification: Confidentielle

Nom du document: Rapport final

Responsable(s) client: M. Thili

Consultant(s) sécurité: M. Muller

Synthèse de l'évaluation des risques:

B I

Annuler Sauvegarder

Mesures en place	Qualif.	C	I	D	Traitement	Risque résiduel
	4	48	32	48	Non traité	48
	4	48	32	48	Non traité	48
	4	36	24	36	Réduction	9
	4	36	24	36	Non traité	36
	2	18	12	18	Non traité	18
	3	18		18	Non traité	18
	2	18	12	18	Non traité	18
	2	18		18	Non traité	18
	2	18		12	Non traité	12
	4	12		12	Non traité	12
	1	12	8	12	Non traité	12
	1	12	8	12	Non traité	12
	1	9	6	9	Non traité	9
	1	6	4	6	Non traité	6
	1	6	4	6	Non traité	6
	1	6		6	Non traité	6
	1			3	Non traité	3
	0	0	0	0	Non traité	0
	-	-	-	-	Non traité	-
	-	-	-	-	Non traité	-

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

- 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'IMPLÉMENTATION DES RECOMMANDATIONS

Accueil > Mon analyse > Implémentation du plan de traitement des risques

1 2 3 4

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

Mon analyse

Service

Bibliothèque d'actifs

Rechercher un actif...

Fondamentaux

EBIOS

Implémentation du plan de traitement des risques

Consulter l'historique d'implémentation

	Recommandation	Imp.	Commentaire	Responsable	Echéance	Statut	Actions
🕒	Droits_admin Enlever l'accès par défaut des administrateurs aux données sensibles.	...			jj-mm-yyyy	En cours (1)	🔗
🕒	Maj Mettre à jour les poste de travail en automatique	...			jj-mm-yyyy	A venir	🔗
🕒	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	🔗
🕒	Antivirus Installer des antivirus sur les machines	..			jj-mm-yyyy	A venir	🔗
🕒	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.	..			jj-mm-yyyy	A venir	🔗
🕒	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	🔗
🕒	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	🔗
🕒	Sens Sensibiliser aux utilisateurs une fois par an	.			jj-mm-yyyy	A venir	🔗

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

# 4.1 – GESTION DE L'IMPLÉMENTATION DES RECOMMANDATIONS

Accueil > Mon analyse > Implémentation du plan de traitement des risques > Recommandation

1 2 3 4

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

Mon analyse

Service

Bibliothèque d'actifs

Rechercher un actif...

Fondamentaux

EBIOS

← Retour à la liste

**MaJ**  
Mettre à jour les poste de travail en automatique

Actif	Menace	Vulnérabilité	Mesures en place	Risque actuel	Nouvelles mesures	Risque résiduel	Actions
<a href="#">Postes de travail utilisateurs</a>	MDA13 - Infection par un malware	1178 - La gestion des mises à jour (patch) comporte des lacunes	Pas de mise à jour automatique. Mais la mise à jour est prise en compte	60		24	✓

- 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

Accueil > Mon analyse > Base de connaissances

1 2 3 4

Type d'actifs Menaces Vulnérabilités Mesures 27002 Risques de l'information Tags Risques opérationnels

Type d'actifs  Rechercher... Afficher actifs uniquement

<input type="checkbox"/>	Statut	Libellé ↑	Code	Type	Description	Actions
<input type="checkbox"/>	✓	Annuaire d'entreprise	SYS_ANU	Secondaire	Annuaire d'entreprise	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Application métier	LOG_APP	Secondaire	Application métier sur mesure ou standard	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Autres supports	MAT_NELE	Secondaire	Documents, Fax, Lettre, BdC, information papier, etc.	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Backup	OV_BACKUP	Secondaire	Qualification des backups	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Bâtiment, bureau ou local	OV_BATI	Secondaire	Bâtiment, bureau ou local	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Conteneur	CONT	Primaire	Conteneur d'actifs	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Décisionnel	PER_DEC	Secondaire	Décisionnel	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Développements d'applications	OV_DEVELOPPEMENT	Secondaire	Développements d'applications	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Développeur	PER_DEV	Secondaire	Développeur	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Dispositif d'accès internet	SYS_INT	Secondaire	Dispositif d'accès internet	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Document papier	OV_INFOPHY	Secondaire	Information sous forme physique	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Exploitant / Maintenance	PER_EXP	Secondaire	Exploitant / Maintenance	<input type="button" value="✎"/> <input type="button" value="✖"/>
<input type="checkbox"/>	✓	Générale	ORG_GEN	Secondaire	Organisation générale de l'organisme	<input type="button" value="✎"/> <input type="button" value="✖"/>

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

**Démonstration**



# IMPORT / EXPORT ACTIF

Accueil > Mon analyse

1 2 3 4

Mon analyse  
Mon analyse

Risques de l'information

79 risques de l'information

Modifier l'analyse des risques  
Importer une analyse de risques  
Exporter toute l'analyse des risques  
Supprimer l'analyse

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

Actif	Impact			Menace	Prob.	Vulnérabilité	Mesures en place	Qualif.	Risque actuel			Traitement	Risque résiduel
	C	I	D						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
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		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
Administrateur système	3	2	3	Erreur d'utilisation	3	Absence de charte informatique précisant les exigences d'utilisation	after	1	9	6	9	Non traité	9
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	Divulgaration 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

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