****

**${DOCUMENT}**

**${COMPANY}**

**Sécurité de l'information - MONARC**

**Informations générales**

Version: ${VERSION}

État document: ${STATE}

Classification: ${CLASSIFICATION}

Société: ${COMPANY}

Nom du document: ${DOCUMENT}

Date: ${DATE}

Consultant(s) sécurité: ${SMILE}

Représentant(s) client: ${CLIENT}

**Résumé**

${SUMMARY\_EVAL\_RISK}

**Carte des risques actuels**

${CURRENT\_RISK\_MAP}

**Carte des risques résiduels**

${TARGET\_RISK\_MAP}

Table des matières

[1 Introduction 4](#_Toc102393843)

[1.1 Mise en contexte de l’analyse des risques 4](#_Toc102393844)

[1.2 Objectifs du document 4](#_Toc102393845)

[1.3 Références 4](#_Toc102393846)

[1.4 Acronymes/Glossaire 4](#_Toc102393847)

[1.5 Description de la « Méthode Optimisée d’Analyse des Risques CASES » (MONARC) 5](#_Toc102393848)

[2 Établissement du contexte 7](#_Toc102393849)

[2.1 Description du contexte 7](#_Toc102393850)

[2.2 Définition des critères d’évaluation du risque 7](#_Toc102393851)

[2.2.1 Risques de l’information 7](#_Toc102393852)

[2.2.1.1 Échelle d’impacts 7](#_Toc102393853)

[2.2.1.2 Échelle des menaces 7](#_Toc102393854)

[2.2.1.3 Échelle des vulnérabilités 7](#_Toc102393855)

[2.2.1.4 Seuils d’acceptation des risques 8](#_Toc102393856)

[2.2.2 Risques opérationnels 8](#_Toc102393857)

[2.2.2.1 Échelle d’impacts 8](#_Toc102393858)

[2.2.2.2 Echelle de vraisemblance 8](#_Toc102393859)

[2.2.2.3 Seuils d’acceptation des risques 8](#_Toc102393860)

[2.3 Évaluation des tendances et des menaces 9](#_Toc102393861)

[3 Modélisation du contexte 10](#_Toc102393862)

[3.1 Identification des actifs 10](#_Toc102393863)

[3.2 Identification des vulnérabilités 10](#_Toc102393864)

[3.3 Appréciation des conséquences 10](#_Toc102393865)

[4 Évaluation et traitement des risques 11](#_Toc102393866)

[4.1 Résumé de l’évaluation des risques 11](#_Toc102393867)

[4.1.1 Risques de l’information 11](#_Toc102393868)

[4.1.2 Risques opérationnels 11](#_Toc102393869)

[4.2 Traitement des risques 12](#_Toc102393870)

[4.2.1 Type de traitement 12](#_Toc102393871)

[4.2.2 Plan de traitement 12](#_Toc102393872)

[Annexe A : Interview et collecte de l’information 13](#_Toc102393873)

[Annexe B : Évaluation des tendances 14](#_Toc102393874)

[Annexe C : Évaluation des menaces 15](#_Toc102393875)

[Annexe D : Contexte des actifs 16](#_Toc102393876)

[Annexe E : Propriétaires des risques 17](#_Toc102393877)

[Annexe F : Notes et remarques du consultant 18](#_Toc102393878)

[Risques de l’information 18](#_Toc102393879)

[Risques opérationnels 19](#_Toc102393880)

# Introduction

## Mise en contexte de l’analyse des risques

${CONTEXT\_ANA\_RISK}

## Objectifs du document

Ce document résume la méthode et expose les résultats de l'analyse de risques menée avec MONARC dans l’environnement du client. MONARC est influencée par la norme internationale ISO 27005:2011.

Les résultats ainsi obtenus visent à identifier les risques majeurs, à appréhender le niveau de sécurité en place et à fournir des recommandations pour l’établissement des mesures de sécurité. Il est entendu par les parties que les recommandations ne sont ni exclusives ni exhaustives.

La liste des risques détectés est basée sur les informations fournies par le Client et/ou ses représentants sans aucune recherche de preuves. L’analyse issue de cette appréciation ne peut engager Luxembourg House of Cybersecurity pour toute omission ou erreur qui seraient due à toute personne impliquée ou des tiers.

## Références

1. ISO/IEC 27005 (2011), Gestion des risques liés à la sécurité de l'information.
2. <http://www.iso.org/iso/fr/catalogue_detail?csnumber=56742>. La norme ISO 27005 explique en détail comment conduire l'appréciation des risques et le traitement des risques, dans le cadre de la sécurité de l'information

## Acronymes/Glossaire

**Actif**:Tout élément représentant de la valeur pour l'établissement.

**Confidentialité** : Propriété d'une information de ne pas être disponible ou divulguée à des individus, entités ou processus non autorisés.

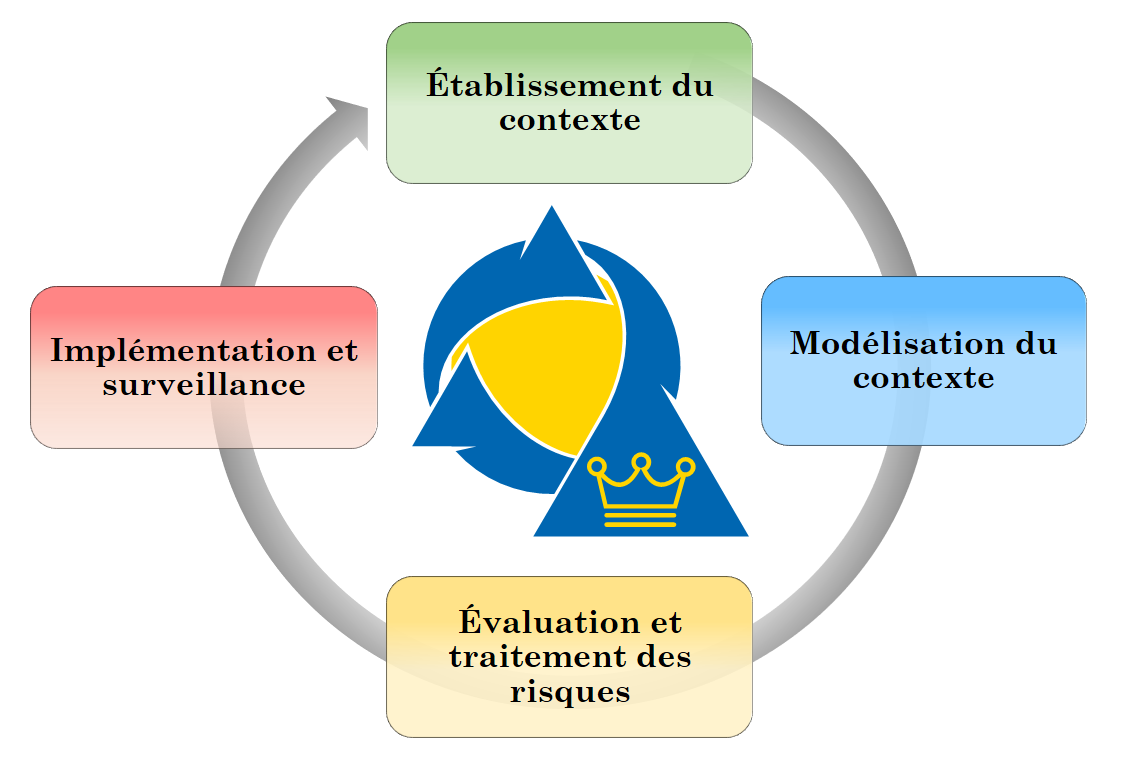
**Disponibilité** : Propriété d'être accessible et utilisable à la demande d'une entité autorisée.

**Intégrité** : Propriété de préservation de l'exactitude et de la complétude d'un bien.

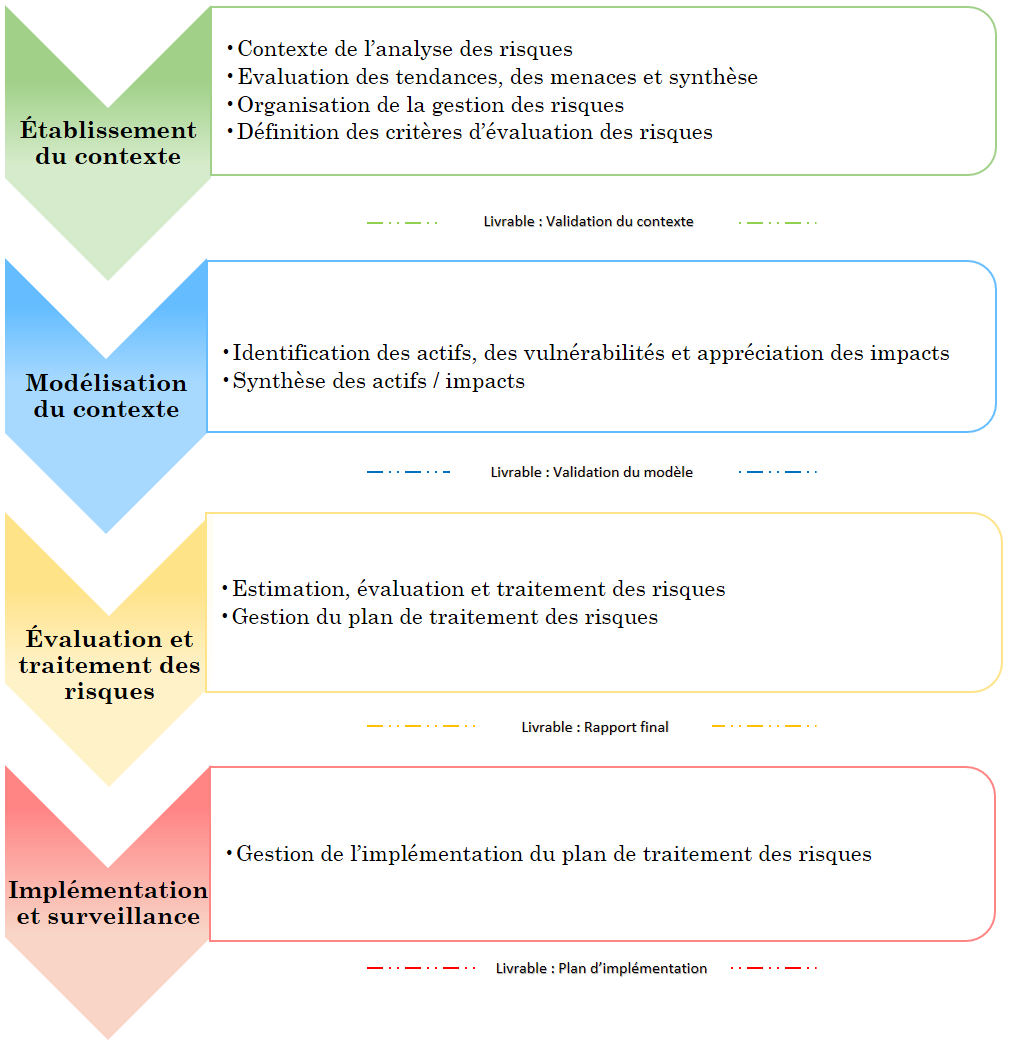
**MONARC** : Méthode Optimisée d’Analyse des Risques CASES.

## Description de la « Méthode Optimisée d’Analyse des Risques CASES » (MONARC)

La méthode d’analyse des risques MONARC est composée de 4 phases :



Plus précisément :



MONARC simplifie la gestion des risques en proposant une solution de gestion des risques, et même de gouvernance de la sécurité de l’information, basée sur l’état de l’art du domaine. Elle permet de réaliser en peu de temps une analyse à partir de modèles existants et personnalisables, tout en restant conforme avec la norme internationale ISO/IEC 27005:2011.

MONARC s’appuie sur une bibliothèque de modèles de risques proposant des objets composés de scénarios de risques par actifs ou groupes d’actifs. Cette approche facilite la gestion des risques les plus courants et permet de gagner en objectivité ainsi qu’en efficacité. MONARC étant complètement itérative, ces résultats peuvent être approfondis et ajustés à la maturité de chaque organisation en augmentant la granularité des scénarios de risques.

**Établissement du contexte**

Cette 1ère étape vise à faire le point sur le contexte, les enjeux et les priorités propres à l’entreprise ou l’organisation qui désire analyser ses risques.

Il s’agit d’identifier notamment les activités essentielles et les processus critiques de l’entreprise, afin d’orienter l’analyse des risques vers les éléments les plus importants. Pour ce faire, un kick-off meeting est organisé avec les membres du management et les personnes clés. L’objectif est de savoir ce qui fait vivre l’entreprise et ce qui pourrait la détruire, d’identifier les processus-clés, les menaces internes et externes, les vulnérabilités organisationnelles, techniques et humaines.

**Modélisation du contexte**

Cette phase comprend la modélisation des arbres d’objets. Les actifs ont été définis dans la phase précédente. Ils doivent maintenant être détaillés et formalisés dans un schéma qui représente leurs interdépendances.

Les impacts sont définis au niveau des actifs primaires (services ou informations). Les actifs secondaires héritent de l’impact de l’actif primaire auquel ils sont rattachés (arbre d’objets).

Il est possible de modifier manuellement les impacts au niveau des actifs secondaires.

**Évaluation et traitement des risques**

L’évaluation consiste à chiffrer les menaces, les vulnérabilités et les impacts pour calculer les risques.

Pour ce faire, il est nécessaire d’avoir des informations de qualité sur la vraisemblance exacte des menaces, l’aisance d’exploitation des vulnérabilités et les impacts potentiels… D’où l’intérêt de se fier à des métriques qui ont été validées par des experts.

Lorsque l’évaluation des risques identifie un risque supérieur au niveau acceptable (grille d’acceptation des risques), des mesures de traitement de ce risque doivent être mises en place pour réduire le risque à un niveau acceptable.

**Implémentation et surveillance**

Lorsque le premier traitement des risques a été réalisé, il faut entrer dans une phase de gestion continue de la sécurité avec un suivi et un contrôle récurrent des mesures de sécurité, afin de pouvoir améliorer celles-ci de façon durable.

Cette 4ème phase permet aussi d’optimiser continuellement la sécurité en augmentant la granularité des objets utilisés respectivement en élargissant l’étendue de l’analyse des risques.

# Établissement du contexte

## Description du contexte

${CONTEXT\_GEST\_RISK}

## Définition des critères d’évaluation du risque

### Risques de l’information

### Échelle d’impacts

La table ci-dessous représente l’échelle d’impact et des conséquences que peut avoir un risque sur l’établissement. 0 n’étant pas d’impact, donc il n'a pas de risque.

${SCALE\_IMPACT}

### Échelle des menaces

La table ci-dessous représente l’échelle de probabilité de survenance d’une menace.

${SCALE\_THREAT}

### Échelle des vulnérabilités

La table ci-dessous représente l’échelle de vulnérabilité de l’actif considéré. La qualification de la vulnérabilité prend en compte les mesures de sécurité en place.

${SCALE\_VULN}

### Seuils d’acceptation des risques

La table ci-dessous représente la table de calcul des risques. Les couleurs sont à titre indicatif et devront être acceptées et/ou modifiées par le conseil d'administration / comité de direction.

Rouge  : Risque inacceptable devant être traité

Orange  : Risque moyen qui selon le cas devrait ou non, être traité

Vert  : Risque faible ne nécessitant aucune action

${TABLE\_RISKS}

### Risques opérationnels

### Échelle d’impacts

${OP\_RISKS\_SCALE\_IMPACT}

### Echelle de vraisemblance

${OP\_RISKS\_SCALE\_LIKELIHOOD}

### Seuils d’acceptation des risques

${TABLE\_OP\_RISKS}

## Évaluation des tendances et des menaces

${SYNTH\_EVAL\_THREAT}

La table ci-dessous représente les menaces qui ont fait l’objet d’une attention particulière.

${TABLE\_THREATS}

# Modélisation du contexte

## Identification des actifs

${SYNTH\_ACTIF}

## Identification des vulnérabilités

L’utilisation de la modélisation de MONARC et de ses objets permet d’identifier les vulnérabilités avec une granularité suffisante pour cette itération d’analyse des risques.

Il reste toutefois à la discrétion des consultants de créer de nouveaux risques contextuels qu’ils pourraient découvrir pendant la mission.

## Appréciation des conséquences

La table ci-dessous représente la table des impacts pour les actifs essentiels de ${COMPANY}. Pour un gain de temps, tous les actifs secondaires qui entreront dans la modélisation des actifs essentiels vont hériter de ces impacts par défauts, mais pourront être raffinés manuellement.

${IMPACTS\_APPRECIATION}

# Évaluation et traitement des risques

Le résultat de la collecte des informations, des encodages et des évaluations diverses sont traités dans l’outil MONARC et sont à disposition du client. Une partie de ces informations se trouvent également dans l’annexe de ce document.

La suite de ce chapitre présente les résultats et recommandations qui finalisent cette analyse des risques.

## Résumé de l’évaluation des risques

${SUMMARY\_EVAL\_RISK}

### Risques de l’information

${DISTRIB\_EVAL\_RISK}

${GRAPH\_EVAL\_RISK}

### Risques opérationnels

${DISTRIB\_EVAL\_OP\_RISK}

${GRAPH\_EVAL\_OP\_RISK}

## 

## Traitement des risques

### Type de traitement

${RISKS\_KIND\_OF\_TREATMENT}

### Plan de traitement

Le tableau suivant contient les recommandations principales issues de l’analyse des risques et du plan de traitement des risques. L’évaluation ainsi que la formulation des recommandations respectent l’échelle suivante :

●●● : Recommandation prioritaire.

●● : Recommandation qui requiert une action dédiée pour remédier à une vulnérabilité ou à une bonne pratique qui fait défaut.

● : Indication utile pour la sécurité, conseil.

Risques de l’information

${RISKS\_RECO\_FULL}

Risques opérationnels

${OPRISKS\_RECO\_FULL}

# Annexe A : Interview et collecte de l’information

La collecte des informations ayant permis de mener l’analyse s’est opérée au travers d’entretiens avec les personnes clés du métier et les responsables techniques.

Nous remercions les personnes suivantes pour leur contribution active lors des entretiens et visites menés dans le cadre de notre mission répertoriés ci-dessous :

${TABLE\_INTERVIEW}

# Annexe B : Évaluation des tendances

${TABLE\_EVAL\_TEND}

# Annexe C : Évaluation des menaces

${TABLE\_THREATS\_FULL}

# Annexe D : Contexte des actifs

${TABLE\_ASSET\_CONTEXT}

# Annexe E : Propriétaires des risques

${TABLE\_RISK\_OWNERS}

# Annexe F : Notes et remarques du consultant

## Risques de l’information

${TABLE\_AUDIT\_INSTANCES}

## Risques opérationnels

${TABLE\_AUDIT\_RISKS\_OP}