



**CASES**  
LUXEMBOURG

# **MONARC**

**Méthode optimisée d'analyse des risques CASES**

**Quick Start**

**v1.0**

---

## Table des matières

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
1.1	OBJECTIF DU DOCUMENT .....	3
1.2	AUTRES DOCUMENTS À VENIR .....	3
1.3	AVERTISSEMENT DE COMPATIBILITÉ .....	3
1.4	SYNTAXE UTILISÉE DANS LE DOCUMENT .....	3
1.5	SYNTAXE UTILISÉE DANS MONARC .....	3
<b>2</b>	<b>ACCUEIL .....</b>	<b>4</b>
2.1	ÉCRAN DE PREMIÈRE CONNEXION .....	4
2.2	CRÉATION DE LA PREMIÈRE ANALYSE.....	4
2.3	DESCRIPTION DE LA VUE PRINCIPALE.....	5
<b>3</b>	<b>ANALYSE SIMPLIFIÉE .....</b>	<b>6</b>
3.1	IDENTIFICATION DES RISQUES (MODÉLISATION PAR DÉFAUT) .....	6
3.2	MISE À JOUR DES IMPACTS ET CONSÉQUENCES .....	7
3.3	ÉVALUATION D'UN RISQUE.....	8
3.4	TRAITEMENT D'UN RISQUE .....	9
3.5	GESTION DU PLAN DE TRAITEMENT .....	10

# 1 Introduction

## 1.1 Objectif du document

Ce document a pour objectif d'aider la prise en main rapide de MONARC. Il explique les principales fonctionnalités de l'outil et les étapes à parcourir pour traiter un risque avec les paramètres par défaut.

## 1.2 Autres documents à venir

« MONARC\_Doc-Outil » : Documentation complète de l'outil.

« MONARC\_Doc-Méthode » : Documentation complète de la méthode.

## 1.3 Avertissement de compatibilité

L'application MONARC est optimisée pour « Chrome ». Dans un premier temps, veuillez ne pas utiliser « Internet Explorer ».

## 1.4 Syntaxe utilisée dans le document

**1** : Tous les chiffres en blanc sur fond rouge sont utilisés sur des copies de vues pour fournir des explications supplémentaires. Les explications se trouvent toujours après la vue avec la numérotation correspondante : « 1) », etc.

*Italique* : Toutes les phrases exprimées en italiques sont des conseils d'utilisation.

## 1.5 Syntaxe utilisée dans MONARC

⋮ : Représente toujours l'appel d'un menu.

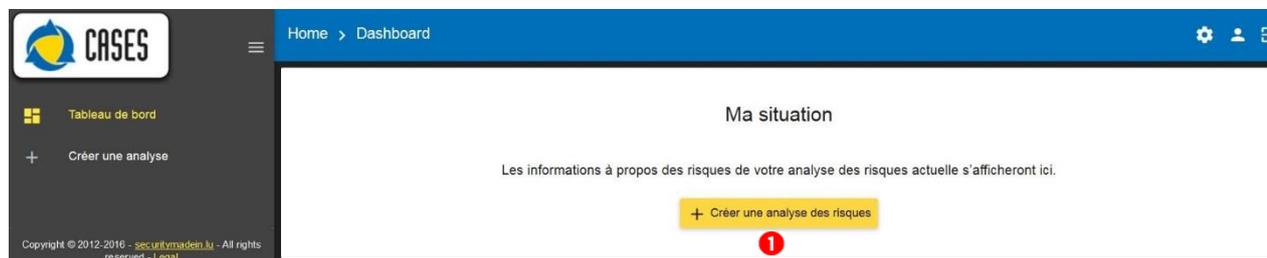
⊕ : Création / ajout de quelque chose en contexte (actifs, recommandations, etc.).

☞ : La plupart des champs de MONARC affichent une information complémentaire, lorsque la souris est laissée quelques instants immobiles dessus.

## 2 Accueil

### 2.1 Écran de première connexion

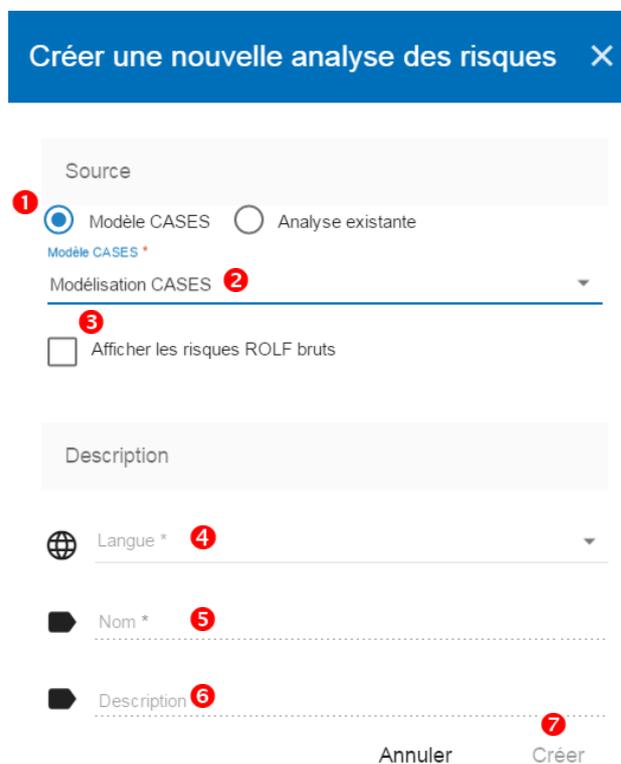
Lors de la première connexion, l'écran suivant apparaît :



- 1) Cliquer sur « Créer une analyse des risques »

### 2.2 Création de la première analyse

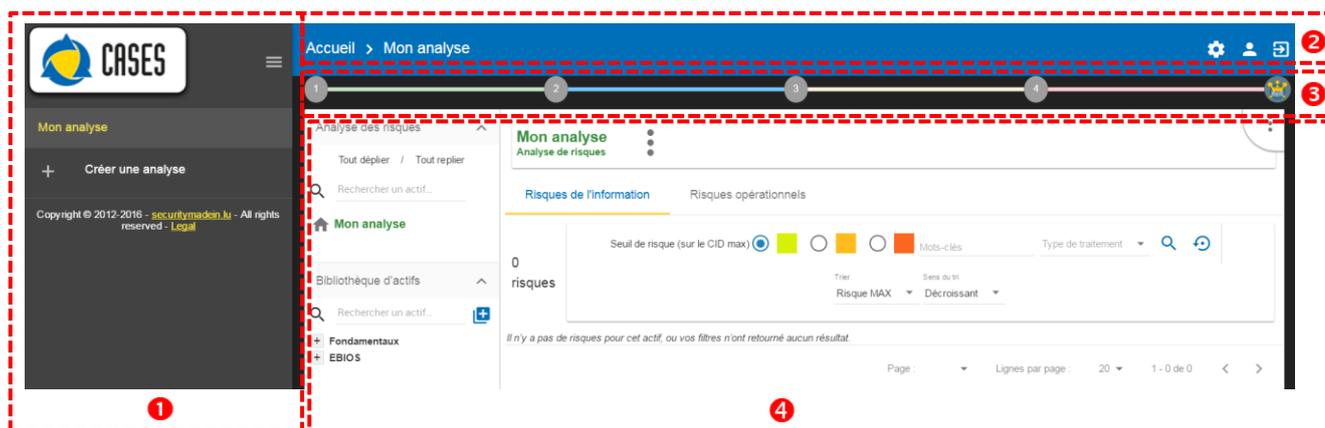
Après avoir cliqué sur « Créer une analyse des risques », le pop-up suivant apparaît :

The screenshot shows a blue pop-up window titled 'Créer une nouvelle analyse des risques' with a close button (X). The form contains several fields and options:

- Source:** Two radio buttons: 'Modèle CASES' (selected, marked with a red circle 1) and 'Analyse existante'.
- Modélisation CASES:** A dropdown menu showing 'Modèle CASES' (marked with a red circle 2).
- Afficher les risques ROLF bruts:** A checkbox (marked with a red circle 3) that is currently unchecked.
- Description:** A section with three fields:
  - Langue \*:** A dropdown menu (marked with a red circle 4).
  - Nom \*:** A text input field (marked with a red circle 5).
  - Description:** A text input field (marked with a red circle 6).
- Buttons:** 'Annuler' and 'Créer' (marked with a red circle 7) at the bottom right.

- 1) Sélectionner l'option « Modèle CASES »
- 2) Il existe au moins deux choix. Sélectionner « Modèle société générique », c'est le modèle par défaut mis à disposition par l'éditeur de MONARC. Il propose des bases de connaissances suffisantes pour démarrer une analyse.
- 3) Affiche les risques bruts dans la table des risques opérationnels. Cette option n'est pas d'importance dans un premier temps.
- 4) Sélectionner votre langue de préférence pour cette nouvelle analyse.
- 5) Donner un nom à votre analyse, par exemple « Mon analyse ».
- 6) Champ optionnel, qui permet de décrire plus en détail votre analyse.
- 7) Si tous les champs obligatoires sont renseignés, cliquer sur « Créer »

## 2.3 Description de la vue principale



1. Liste des analyses : Permet de créer, modifier, supprimer et sélectionner les analyses. Une fois l'analyse sélectionnée, le tableau de bord peut s'escamoter pour optimiser l'espace horizontal en cliquant sur le symbole ☰.
2. Fil d'Ariane et gestion de l'environnement client, droits et informations des utilisateurs.
3. Accès aux étapes de la méthode en cliquant sur les chiffres de 1 à 4.
4. Zone contextuelle de travail dans les analyses.

### 3 Analyse simplifiée

#### 3.1 Identification des risques (Modélisation par défaut)

Il s'agit d'utiliser les actifs de la bibliothèque pour les placer dans l'analyse.

Si l'analyse des risques ne contient aucun actif, suivre les instructions suivantes, sinon passer au chapitre suivant.

MONARC propose par défaut, un principe de structuration dans lequel, il faut placer les actifs primaires (Business) sur la racine de l'analyse, puis en dessous les actifs de supports. Afin de simplifier cette étape, deux groupes d'actifs ont été créés :

- 1) Front-Office : Ce regroupement d'actifs, propose une identification des risques courants que l'on retrouve du côté des utilisateurs pour un service « Ressources Humaines » par exemple (risques liés au bureau, aux ordinateurs, aux applications, aux dossiers physiques, etc.).
- 2) Back-Office : Ce regroupement d'actifs, propose une identification des risques transversaux dans l'organisme liés à l'informatique et à l'organisation en général.



Cliquer sur les « + » et les « - » pour respectivement déplier et plier les catégories de la bibliothèque.

1. Dans la catégorie « Actifs primaires » se trouve l'actif « Service »
  - a. Cliquer sur « Service », puis, en maintenant le bouton gauche de la souris enfoncé, déplacer l'actif dans la zone de l'analyse juste au-dessus (Glisser-Déposer).
2. Dans la catégorie « Structure modèle » se trouve les actifs « Front Office » et « Back Office »
  - a. Cliquer sur « Front Office », puis, en maintenant le bouton gauche de la souris enfoncé, déplacer l'actif sur le « Service » qui se trouve maintenant dans la zone de l'analyse.
  - b. Cliquer sur « Back Office », puis, en maintenant le bouton gauche de la souris enfoncé, déplacer l'actif sur le « Service » qui se trouve maintenant dans la zone de l'analyse.

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 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 télétravail			-	-	-	-	Non traité	-
Administrateur système	-	-	-	Atteinte à la disponibilité du personnel	-	Non-redondance du personnel stratégique			-	-	-	-	Non traité	-

- 1) L'analyse des risques propose maintenant un modèle pour le « service ».

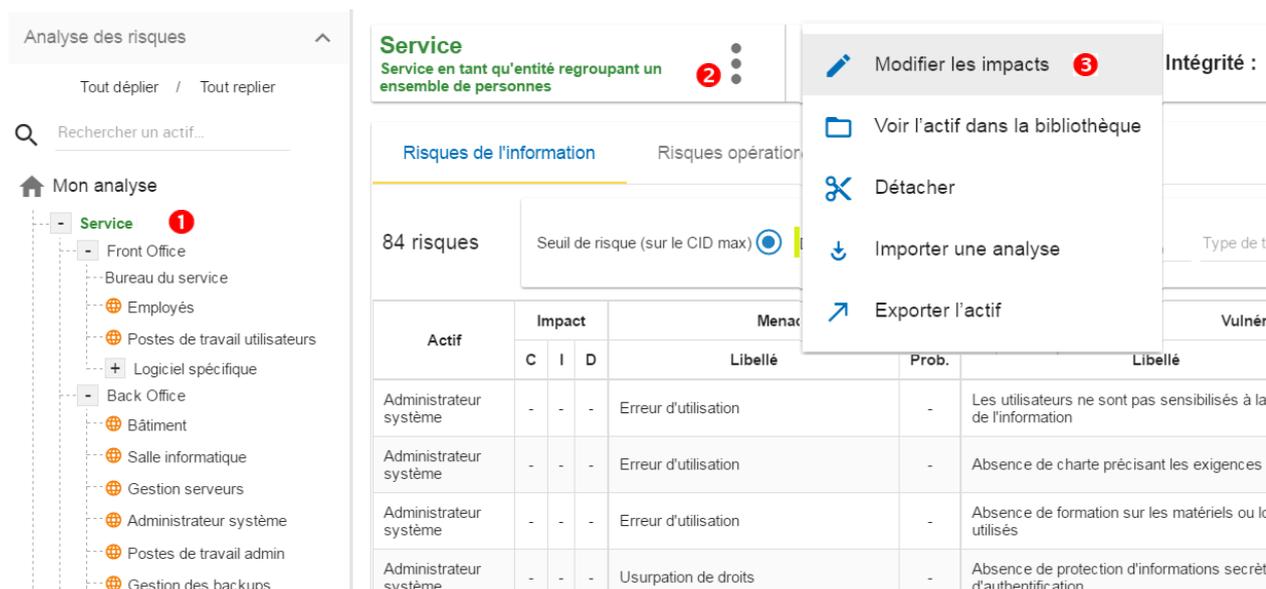
- 2) Le « Front Office » propose une identification par défaut des risques cotés utilisateurs.
- 3) Le « Back Office » propose une identification par défaut des risques, coté IT et organisation.
- 4) Nombre total de risques du modèle, 84 en l'occurrence.

Note : Les risques identifiés par défaut sont les risques couramment rencontrés et supposés importants, ils n'ont pas la prétention d'être exhaustifs.

### 3.2 Mise à jour des impacts et conséquences

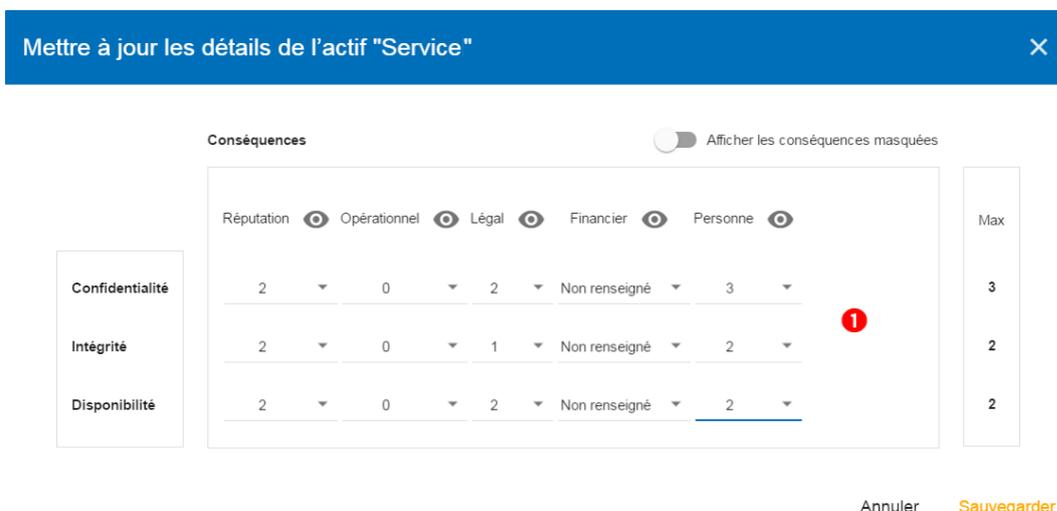
Il s'agit de définir au niveau des actifs primaires, les impacts et les conséquences que peuvent provoquer la réalisation des risques du modèle.

Dans le cas de notre analyse, il s'agit de « Service »



- 1) Cliquer sur l'actif primaire de l'analyse « Service »
- 2) Cliquer sur le symbole pour faire apparaître le menu contextuel de l'actif
- 3) Cliquer sur « Modifier les impacts »

Le pop-up ci-dessous apparaît :



La consultation des échelles d'impacts se fait par le menu en haut à droite de l'écran. En laissant la souris sur les chiffres, le libellé apparaît après 1 seconde.

Le raisonnement à suivre est le suivant : lorsqu'un des critères C (confidentialité), I (intégrité) ou D (disponibilité) est affecté, il faut se poser la question : quelles sont les conséquences sur l'organisme, et notamment sur son ROLFP, c'est-à-dire sa « Réputation », son « Opération », son « Légal », ses « Finances » ou l'impact à la « Personne » (au sens des données à caractère personnel).

Dans le cas de la figure ci-dessus, le « 3 » (sur 5) d'impact sur la confidentialité, s'explique par la valeur maximum ROLFP concernant la confidentialité. Exemple, « 3 » est la conséquence pour la personne, en cas de divulgation de son dossier personnel.

### 3.3 Évaluation d'un risque

Actif	Impact			Menace		Vulnérabilité			Risque actuel			Traitement	Risque résiduel
	C	I	D	Libellé	Prob.	Libellé	Mesures en place	Qualif.	C	I	D		
Administrateur système	3	2	2	Erreur d'utilisation	-	Les utilisateurs ne sont pas sensibilisés à la sécurité de l'information	-	-	-	-	-	Non traité	-
Administrateur système	3	2	2	Erreur d'utilisation	-	Absence de charte précisant les exigences d'utilisation	-	-	-	-	-	Non traité	-

- 1) Cliquer sur un actif secondaire, par exemple « Bâtiment ».
- 2) Les critères CID qui ont été affectés au « Service » sont hérités par défaut et ne sont plus à renseigner.
- 3) La menace : « Vol destruction de supports, de documents ou de matériels » est une menace physique qui exprime la crainte de se faire voler ou détruire un actif.
- 4) Il s'agit ici d'estimer la probabilité sur une échelle de 1 à 4 que la menace se réalise. Prenons par exemple, le cas d'une très grosse entreprise ou cette menace est au-delà de la moyenne, donc « 3 ».
- 5) La vulnérabilité : « Le principe du moindre privilège n'est pas appliqué ». Les principes de sécurité recherchés ici sont de savoir qui a les droits d'accès et si ceux-ci sont en rapport avec les fonctions des personnes en présence.
- 6) Mesure en place : Décrire ici, de façon factuelle les mesures sécurité en place concernant cette vulnérabilité ou plus largement le risque en question. Prenons, par exemple un second cas défavorable, par exemple un hôpital où l'on considère le bâtiment comme une zone publique.
- 7) Par rapport à la mesure en place (point 6 ci-dessus), la vulnérabilité est maximum donc « 5 » sur l'échelle de 5.

En laissant la souris sur la plupart des champs, une bulle d'aide apparaît après 1 seconde.

Tous les paramètres permettant de calculer le risque sont présents, le risque actuel est donc calculé sur les valeurs CID, dépendantes directement de la menace.

Actif	Impact			Menace		Vulnérabilité			Risque actuel			Traitement	Risque résiduel
	C	I	D	Libellé	Prob.	Libellé	Mesures en place	Qualif.	C	I	D		
Bâtiment	3	2	2	Vol ou destruction de supports, de documents ou de matériel	3	Le principe du moindre privilège n'est pas appliqué	Le bâtiment est accessible par tous les visiteurs, sans aucun contrôle d'accès.	5	45	30	30	Non traité	-

- 1) Cliquer sur « Non traité » pour appeler la vue de traitement des risques.

### 3.4 Traitement d'un risque

Le traitement du risque consiste à proposer un des 4 types de traitement, sachant que la plupart du temps le traitement consiste à réduire le risque en affectant une mesure de sécurité, ou d'accepter les risques faibles.

Confidentialité : 3 (hérité)    Intégrité : 2 (hérité)    Disponibilité : 2 (hérité)

← Retour à la liste

Fiche de risque

	C	I	D
Risque actuel	45		30
Risque résiduel	45		30

Actif: Service RH > Back Office > Bâtiment

Menace: Vol ou destruction de supports, de documents ou de matériel

Probabilité menace: 3 - Peut arriver de temps à autre

Vulnérabilité: Le principe du moindre privilège n'est pas appliqué

Qualification de la vulnérabilité: 5 - Vulnérabilité très élevée : aucune mesure en place.

Mesures en place: Le bâtiment est accessible par tous les visiteurs, sans aucun contrôle d'accès.

Recommandations: 1

Type de traitement: Non traité 2

Atténuation de la vulnérabilité: 0 3

Référentiel de sécurité: 11.1.2 - Contrôles physiques des accès

Sauvegarder

- 1) Créer une recommandation
- 2) Définir le type traitement (selon ISO/IEC 27005)
- 3) Apprécier la valeur réductrice du risque, afin de définir le risque résiduel

Analyse des risques

Tout déplier / Tout replier

Rechercher un actif...

My analyse 4

- Service
  - Back Office
    - Bâtiment
      - Salle informatique
      - Gestion serveurs
      - Administrateur système
      - Postes de travail admin
      - Gestion des backups
      - Réseau & télécom
      - Organisation informatique
      - Développements logiciels
    - Front Office

Bibliothèque d'actifs

- Fondamentaux
  - Actifs primaires
  - Structure modélée
  - Backup
  - Bâtiments & locaux
  - Biens physiques
  - Logiciels
  - Matériel
  - Organisation
  - Personnel
  - Réseau

Confidentialité : 3 (hérité)    Intégrité : 2 (hérité)    Disponibilité : 2 (hérité)

← Retour à la liste

Fiche de risque

	C	I	D
Risque actuel	45		30
Risque résiduel	18		12

Actif: Service RH > Back Office > Bâtiment

Menace: Vol ou destruction de supports, de documents ou de matériel

Probabilité menace: 3 - Peut arriver de temps à autre

Vulnérabilité: Le principe du moindre privilège n'est pas appliqué

Qualification de la vulnérabilité: 5 - Vulnérabilité très élevée : aucune mesure en place.

Mesures en place: Le bâtiment est accessible par tous les visiteurs, sans aucun contrôle d'accès.

Recommandations: Ctrl\_accès \*\*\* -> Déplacer la réception à l'entrée du bâtiment principal pour vérifier chaque personne entrante

Type de traitement: Réduction

Atténuation de la vulnérabilité: 3

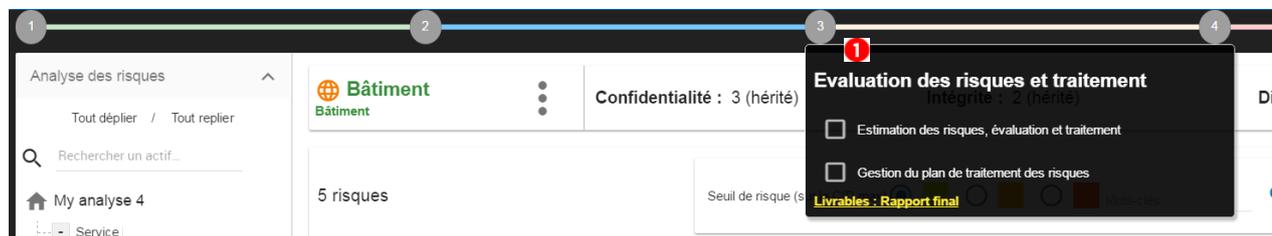
Référentiel de sécurité: 11.1.2 - Contrôles physiques des accès

Sauvegarder 1

- 1) Une fois la recommandation créée et la fiche risque validée, le risque est traité.

### 3.5 Gestion du plan de traitement

Le plan de traitement des risques ne se compose que d'un risque, mais lorsque tous les risques seront évalués, nous y retrouverons toutes les recommandations des risques de l'information et des risques opérationnels.



- 1) L'appel du popup se fait en cliquant sur la 3<sup>ème</sup> étape de la méthode et « Gestion du plan de traitement des risques »

Gestion du plan de traitement des risques						
Réinitialiser les positions						
	Recommandation	Imp.	Type d'actifs	Mesures en place	Risque actuel	Risque résiduel
↓ ↑	<a href="#">Ctrl accès</a> Déplacer la réception à l'entrée du bâtiment principal pour vérifier chaque personne entrante	***	Bâtiment	Le bâtiment est accessible par tous les visiteurs, sans aucun contrôle d'accès.	45	18

Un rapport final d'analyse des risques peut être généré en cliquant sur la 3<sup>ème</sup> étape de la méthode et « Livrable : Rapport final ».

Note : Le livrable n'est vraiment relevant que lorsque la méthode MONARC a été complètement déroulée et que toutes les informations ont été renseignées.