

**MONARC**

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

**Documentation de l’outil**

**v1.0**

Table des matières

[1 Introduction 4](#_Toc476055557)

[1.1 Objectif du document 4](#_Toc476055558)

[1.2 Avertissement de compatibilité 4](#_Toc476055559)

[1.3 Syntaxe utilisée dans le document 4](#_Toc476055560)

[1.4 Syntaxe utilisée dans MONARC 4](#_Toc476055561)

[2 Accueil 5](#_Toc476055562)

[2.1 Tableau de bord 5](#_Toc476055563)

[2.2 Créer une analyse 5](#_Toc476055564)

[2.3 Vue principale de gestion des analyses 6](#_Toc476055565)

[3 Administration de l’environnement client 7](#_Toc476055566)

[3.1 Administration des utilisateurs 7](#_Toc476055567)

[3.1.1 Liste des utilisateurs 7](#_Toc476055568)

[3.1.2 Droits et informations des utilisateurs 8](#_Toc476055569)

[3.2 Gestion du compte de l’utilisateur en cours 8](#_Toc476055570)

[4 Gestion des analyses 9](#_Toc476055571)

[4.1 Appels étapes de la méthode 9](#_Toc476055572)

[4.2 Bibliothèque 10](#_Toc476055573)

[4.2.1 Organisation des actifs 10](#_Toc476055574)

[4.2.2 Gestion d’un actif 10](#_Toc476055575)

[4.2.3 Créer un actif 12](#_Toc476055576)

[4.2.4 Modifier un actif 13](#_Toc476055577)

[4.2.5 Importer un actif 13](#_Toc476055578)

[4.2.6 Exporter un actif 15](#_Toc476055579)

[4.3 Risques de l’information 15](#_Toc476055580)

[4.3.1 Table des risques 15](#_Toc476055581)

[4.3.2 Fiche risque de l’information 17](#_Toc476055582)

[4.3.3 Ajout risque supplémentaire 18](#_Toc476055583)

[4.3.4 Menu contextuel 19](#_Toc476055584)

[4.3.5 Mise à jour des impacts et conséquences 19](#_Toc476055585)

[4.4 Risques opérationnels 20](#_Toc476055586)

[4.4.1 Table des risques 20](#_Toc476055587)

[4.4.2 Fiche risque opérationnel 21](#_Toc476055588)

[4.4.3 Ajout risque supplémentaire 22](#_Toc476055589)

[5 Échelles d’évaluation 23](#_Toc476055590)

[5.1 Échelles d’impact 23](#_Toc476055591)

[5.2 Échelles des menaces 24](#_Toc476055592)

[5.3 Gestion des vulnérabilités 24](#_Toc476055593)

[5.4 Gestion des seuils d’acceptation des risques opérationnels 24](#_Toc476055594)

[6 Gestion bases de connaissances 25](#_Toc476055595)

[6.1 Types d’actifs 25](#_Toc476055596)

[6.2 Menaces 26](#_Toc476055597)

[6.3 Vulnérabilités 26](#_Toc476055598)

[6.4 Mesures 27002 26](#_Toc476055599)

[6.5 Risques 26](#_Toc476055600)

[6.6 Tags (Risques opérationnels) 26](#_Toc476055601)

[6.7 Risques opérationnels 26](#_Toc476055602)

[7 Gestion des interviews 27](#_Toc476055603)

[8 Snapshots 28](#_Toc476055604)

[9 Gestion de l’implémentation du plan de traitement 29](#_Toc476055605)

# fond_doc2fond_doc2fond_doc2Introduction

## Objectif du document

Ce document a pour objectif d’expliquer de façon exhaustive, toutes les options de l’outil MONARC.

## Avertissement de compatibilité

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

## Syntaxe utilisée dans le document

 : 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.

## Syntaxe utilisée dans MONARC

 : Représente toujours l’appel d’un menu.



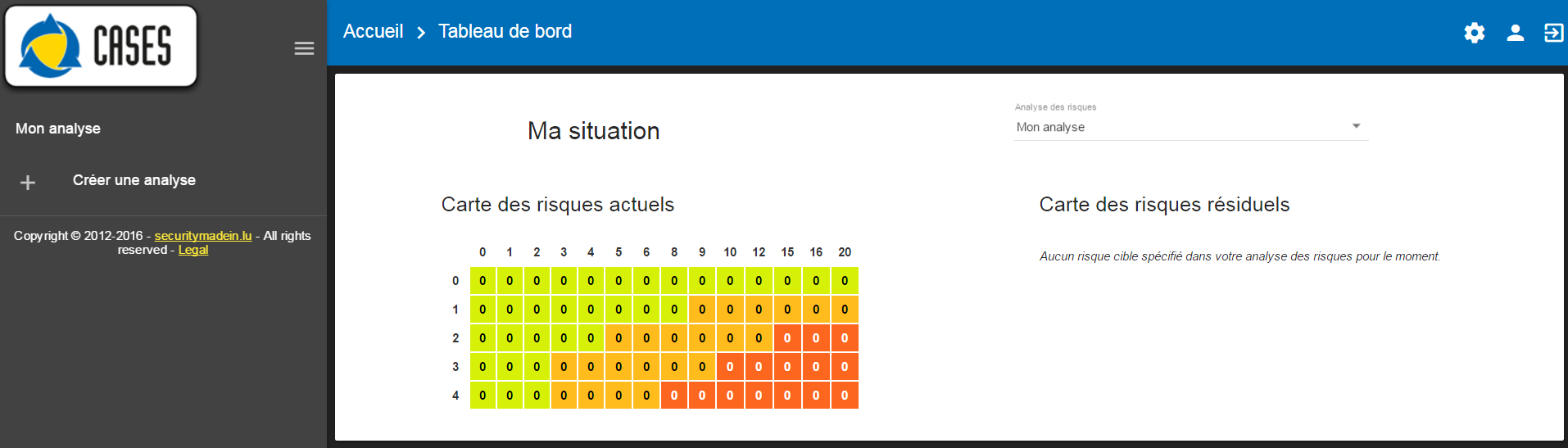
: Création / ajout de quelque chose en contexte (actifs, recommandations, etc.).

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

# Accueil

## Tableau de bord

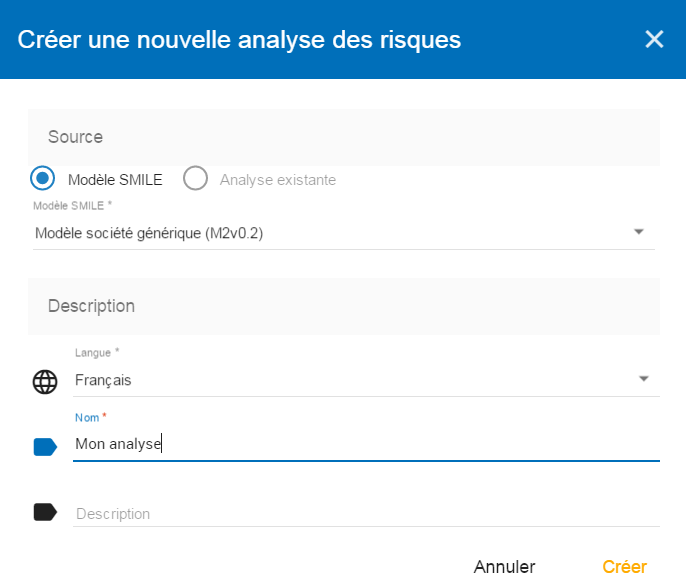
Directement après l’authentification de l’utilisateur, la vue ci-dessous apparaît. Elle peut toutefois être légèrement différente, s’il n’y a pas encore d’analyse créée ou s’il y en a déjà plusieurs et selon l’état d’avancement de celles-ci.



1. Graphique présentant les statistiques de la dernière analyse modifiée.
2. Liste des analyses existantes. Dans ce cas, il n’y en a qu’une. Cliquer sur l’analyse de votre choix pour la sélectionner (suite voir chapitre 2.3)
3. Cliquer pour créer une nouvelle analyse. (suite voir chapitre 2.2).
4. File d’Ariane, permettant une navigation plus aisée
5. Administration de l’environnement client. Cliquer pour respectivement « Gérer le compte », « Gérer les utilisateurs » ou « Se déconnecter » (suite voir chapitre 3).

## Créer une analyse

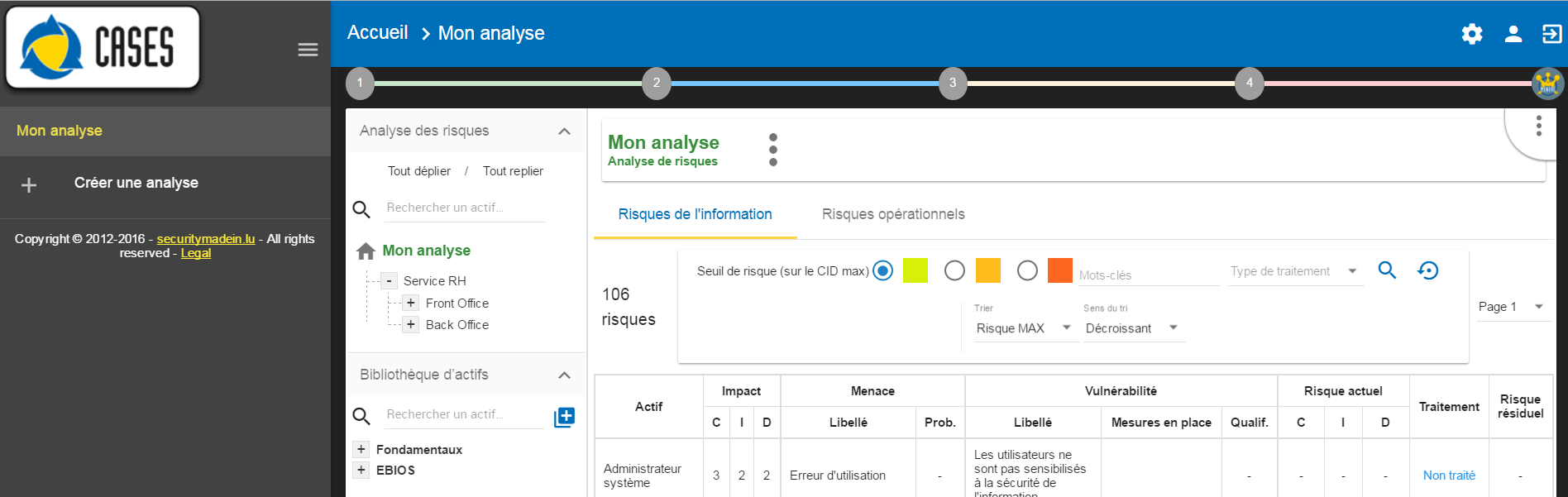
Après avoir cliqué sur « Créer une analyse des risques », le pop-up suivant apparaît :



1. La création d’une analyse se fait toujours à partir d’un modèle existant. Il existe deux choix pour cela :
   1. « Modèle CASES » : Propose les modèles disponibles dans les bases de connaissances. Cette option possède au moins deux choix, « 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. C’est par défaut cette option qu’il faut utiliser, pour démarrer une nouvelle analyse. Il existe également le choix « Modèle vierge » qui est un modèle complètement vide. Ce modèle « Bac à sable » est généralement utilisé de façon temporaire pour tester le contenu d’un fichier xml d’import.
   2. « Analyse existante » va dupliquer une analyse de votre choix présente dans votre environnement.
2. Selon l’option a) ou b) choisie ci-dessus, sélectionner la source de départ.
3. Sélectionner la langue de préférence pour cette nouvelle analyse. MONARC ne propose que les langues effectivement disponibles dans la source choisie.
4. Donner un nom à votre analyse.
5. Champ optionnel, qui permet de décrire plus en détail votre analyse.
6. Si tous les champs obligatoires sont renseignés, cliquer sur « Créer »

Une fois créé, l’analyse est sélectionnée par défaut.

## Vue principale de gestion des analyses



*Une fois l’analyse sélectionnée, le tableau de bord peut s’escamoter pour optimiser l’espace horizontal, en cliquant sur le symbole* *.*

# Administration de l’environnement client

Il existe deux profils :

* Administrateur : Droits de créer, modifier et supprimer des utilisateurs. Un administrateur n’a pas les droits d’accès sur les analyses (mais, il peut se les donner).
* Utilisateurs : Droits d’accès sur les analyses.

Par analyse des risques, il existe 3 types de droits :

* Aucun droit d’accès (pas même lecture).
* Lecture seule.
* Lecture et écriture.

Vue des menus lorsque l’on est administrateur :



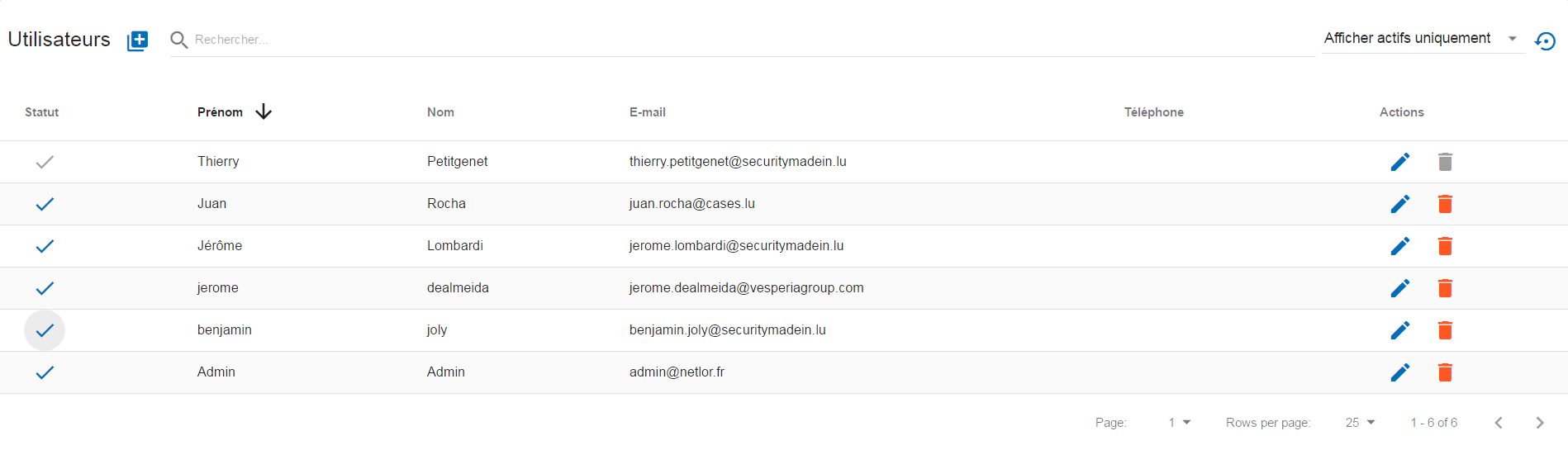
Vue des menus lorsque l’on est utilisateur :



1. Administration des utilisateurs (suite chapitre 3.1)
2. Gestion du compte de l’utilisateur en cours (suite chapitre 3.2)
3. Déconnexion (fermeture de la session MONARC)

## Administration des utilisateurs

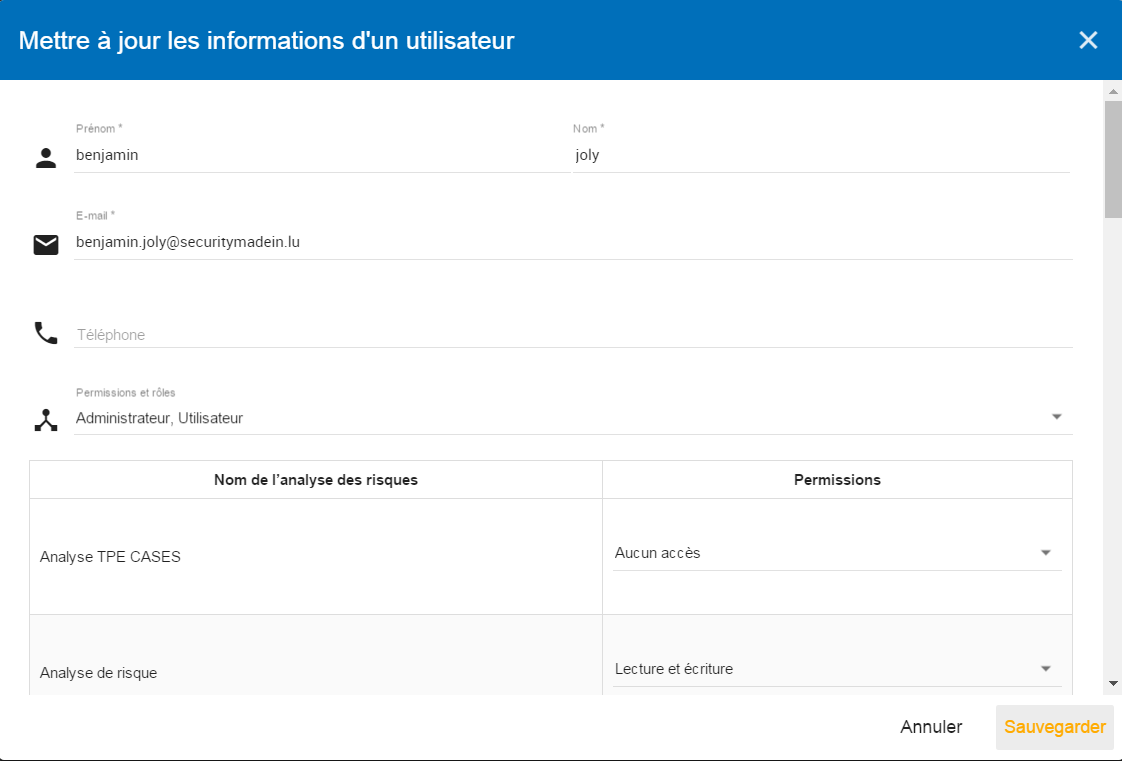
### Liste des utilisateurs



1. Créer un utilisateur ou un administrateur
2. Statut : Activation ou désactivation des comptes
3. Informations sur la personne
4. Éditer les informations d’une personne
5. Supprimer une personne

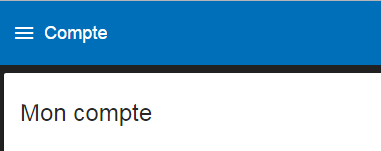
### Droits et informations des utilisateurs

Après avoir cliqué sur l’icône «  », l’écran suivant apparaît :



1. Informations générales.
2. Sélection type de profils « Administrateur » ou « Utilisateur ».
3. Gestion des droits de l’utilisateur par analyse.

## Gestion du compte de l’utilisateur en cours

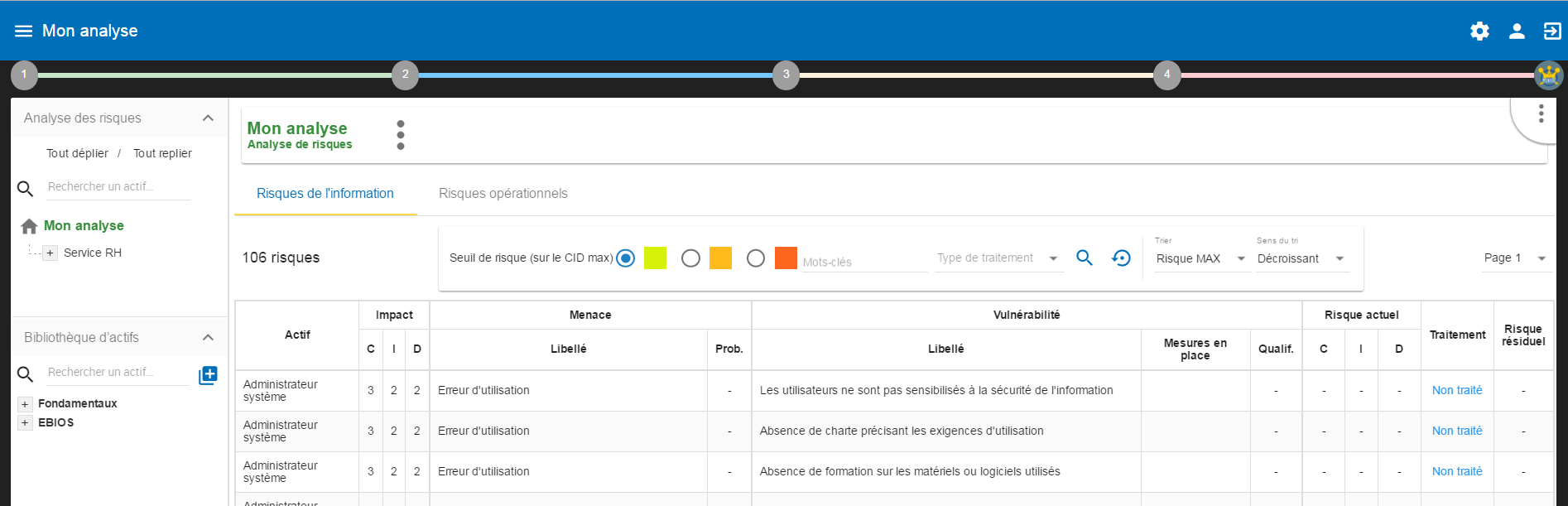


Cette vue permet de :

* Gérer les informations générales concernant l’utilisateur
* Changer le mot de passe. Une complexité de mot de passe est requise.
* Changer la langue de consultation. Cette action ne change que la langue des interfaces, les informations propres aux données des analyses restent dans la langue d’origine)
* Gérer les informations générales concernant l’entité (compte MONARC).

# Gestion des analyses

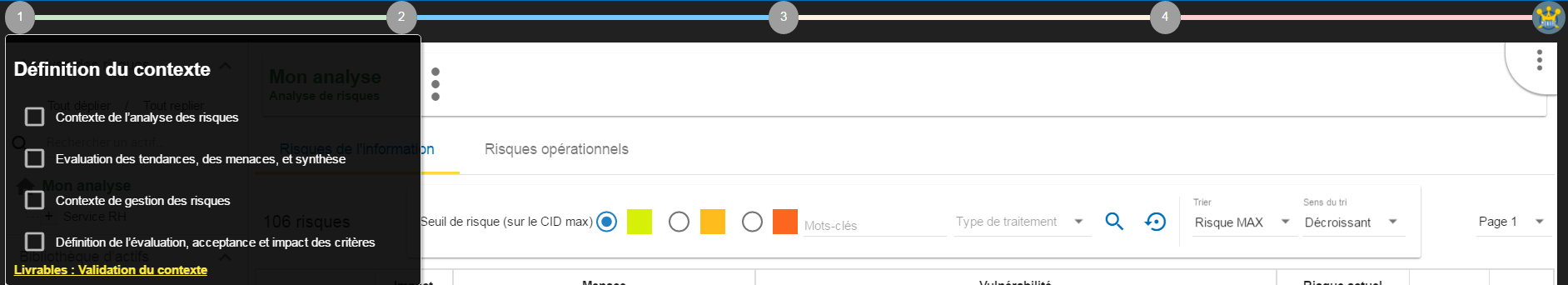
La vue principale de l’analyse se compose de 4 parties distinctes.

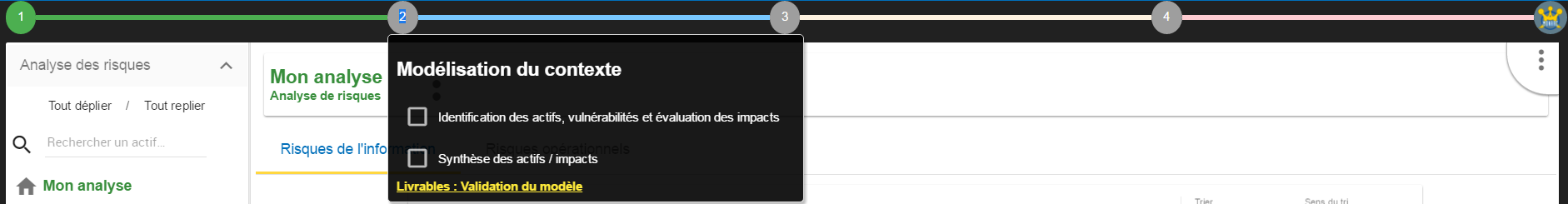


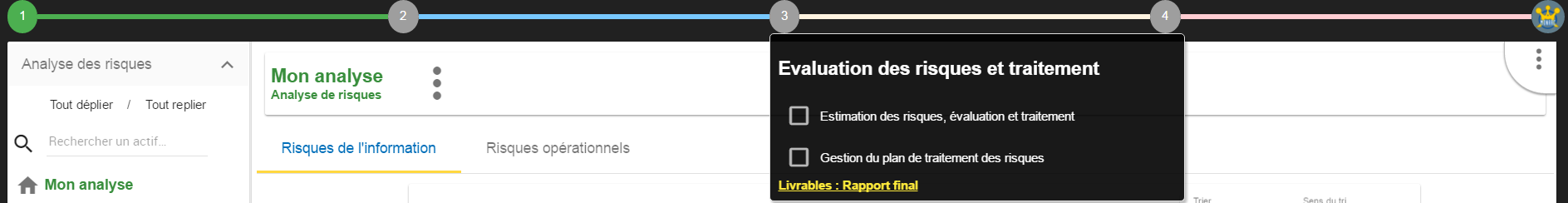
1. Accès aux étapes de la méthode : Cliquer sur les chiffres de 1 à 4 pour accéder aux menus qui permettent de suivre la méthode pas à pas (suite chapitre 4.1).
2. Zone « Bibliothèque d’actifs » : Stockage des actifs. Il faut utiliser la fonction « Glisser-Déposer » pour placer ces actifs dans l’analyse juste au-dessus (suite chapitre 4.2).
3. Zone « Analyse des risques » : permet de structurer hiérarchiquement les actifs de l’analyse en utilisant la fonction « Glisser-Déposer » (maintenir le bouton gauche de la souris enfoncé pour déplacer un actif). (suite chapitres 4.3 et 4.4)
4. Zone contextuelle de travail dans les analyses : en fonction des actifs et des parties actives de l’analyse, cette zone contient contextuellement les éléments de travail.

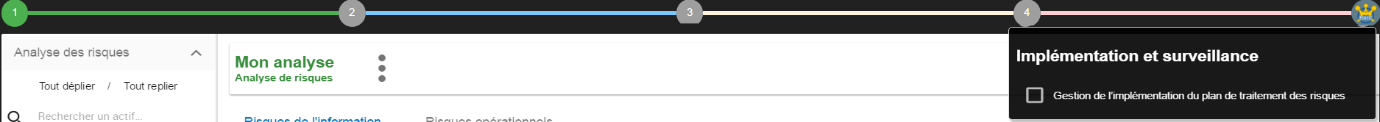
## Appels étapes de la méthode

En cliquant, sur les chiffres de 1 à 4, un menu contextuel apparaît.









1. Cocher les cases permet de faire évoluer l’état d’avancement de la méthode
2. Cliquer sur le libellé, appel du sous-écran contextuel de gestion

## Bibliothèque

### Organisation des actifs

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

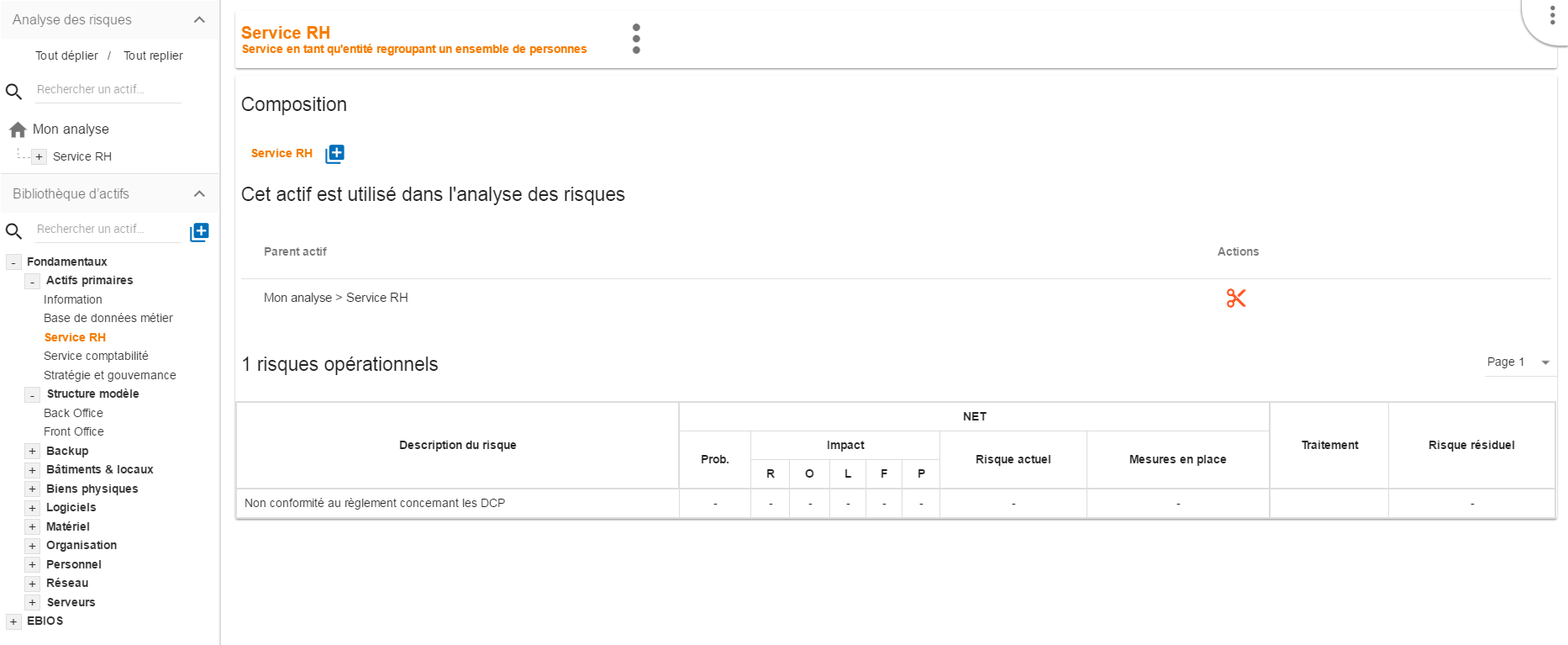
|  |  |
| --- | --- |
|  | 1. Zone de recherche pour trouver rapidement un actif. 2. Bouton pour créer / importer un actif (suite chapitre 4.2.3) 3. Niveau racine de la bibliothèque. Il y en a généralement deux :    1. « Fondamentaux » : Contient tous les actifs par défaut proposés par CASES. »   « EBIOS » : Contient les actifs inspirés par EBIOS. Ce sont des actifs contenant des modèles de risques non optimisés.   1. Conteneur secondaire permettant de classer les actifs par types logiques 2. Niveau actifs : Ce sont les actifs qu’il faut « Glisser-Déposer » dans l’analyse |

### Gestion d’un actif

Les informations sur chaque actif sont différentes en fonction de leur type : « Primaire » ou « Secondaire ». Cette notion est expliquée en détail au chapitre 6.1 « Types d’actifs ».

#### Actif primaire

Cliquer sur un actif primaire de la bibliothèque, généralement classé dans « Fondamentaux \ Actifs Primaires ».



1. Appel menu contextuel de gestion de l’actif (détails au chapitre 4.2.2.3).
2. Ajouter un actif déjà existant dans la structure, créant ainsi un actif composé. Il n’y a pas de limite dans l’arborescence des actifs.
3. Indication si cet actif est actuellement utilisé dans l’analyse. Dans ce cas, on le retrouve à la racine de l’analyse.
4. Possibilité de détacher l’actif de l’analyse. *Attention détacher complètement un actif de l’analyse va supprimer toute son évaluation.*
5. Table des risques opérationnels éventuellement associés à l’actif. Un actif primaire ne peut pas posséder de risques de l’information. La modification de la table des risques opérationnels se fait à partir de la base de connaissances.

#### Actif secondaire

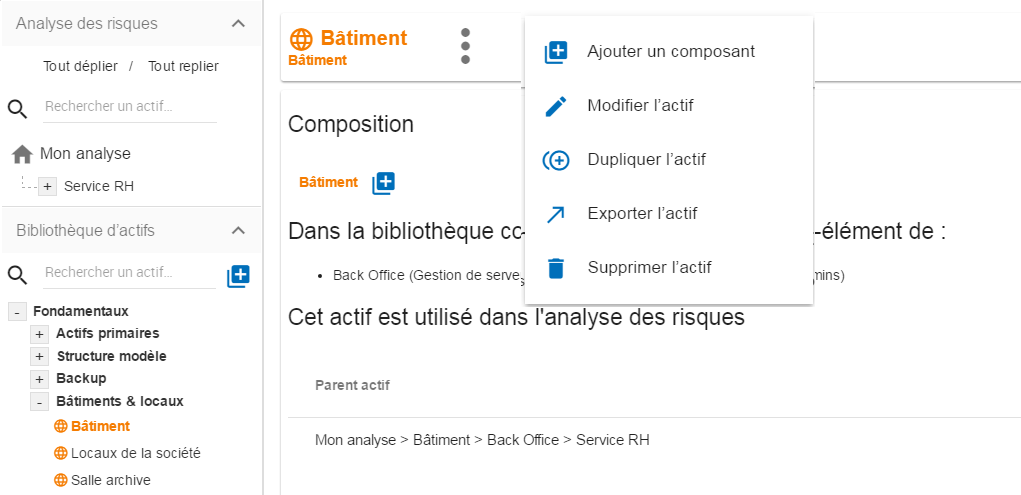
Cliquer sur un actif secondaire de la bibliothèque, par exemple sur « Bâtiment » classé dans « Fondamentaux \ Bâtiments & locaux ».



1. Appel menu contextuel de gestion de l’actif (détails au chapitre 4.2.2.3).
2. Ajouter un actif déjà existant dans la structure, créant ainsi un actif composé. Il n’y a pas de limite dans l’arborescence des actifs.
3. Indication si l’actif fait déjà partie de la composition d’un autre actif. Dans cas, c’est déjà un sous-élément de l’actif « Back Office »
4. Indication si cet actif est actuellement utilisé dans l’analyse. Dans ce cas, on le retrouve au 3ème niveau de la racine de l’analyse.
5. Possibilité de détacher l’actif de l’analyse. *Attention détacher complètement un actif de l’analyse va supprimer toute son évaluation.*
6. Table des risques de l’information associés à l’actif. Inversement aux actifs primaires, les actifs de supports ne peuvent que posséder des risques de l’information. La modification de la table des risques se fait à partir de la base de connaissances.

#### Menu contextuel

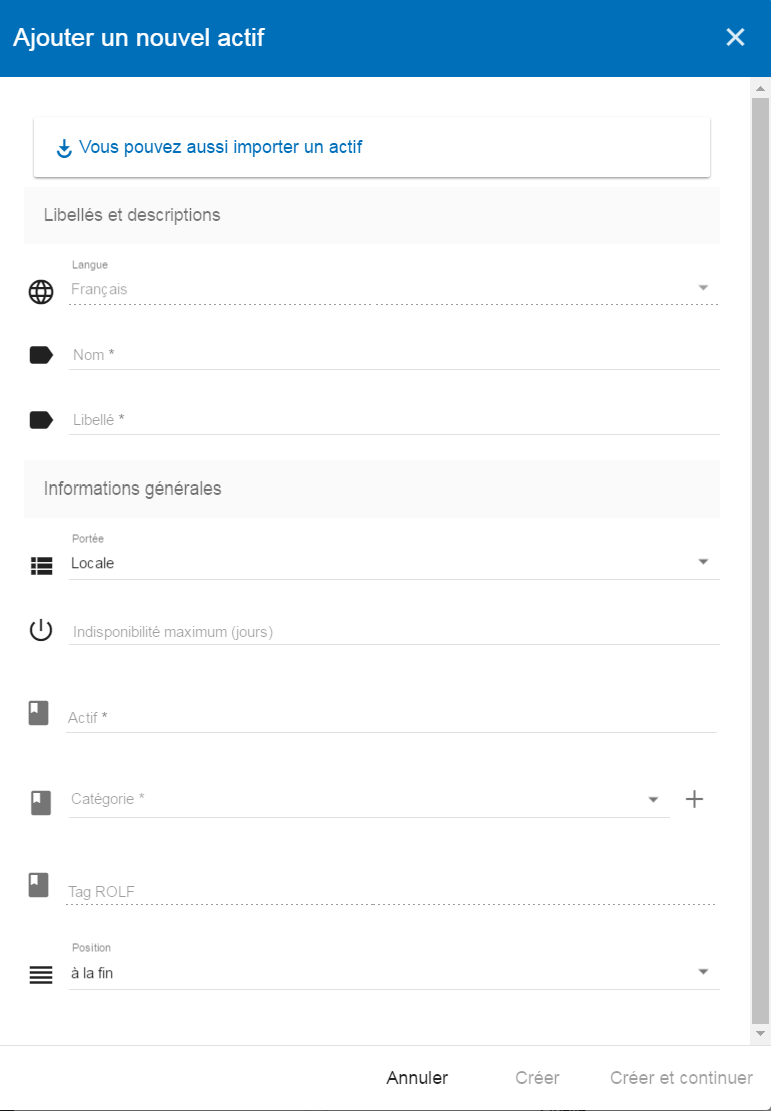
En cliquant sur l’icône «   », le menu contextuel suivant apparaît. Quel que soit le type d’actif de la bibliothèque, le menu est le même.



1. Ajoute un actif déjà existant dans la structure, créant ainsi un actif composé.
2. Lance le pop-up qui permet de modifier la plupart des paramètres d’un actif (suite chapitre 4.2.4).
3. Créé une copie de l’actif nommée « Nom (copie #1) », qu’il suffit de renommer ensuite avec l’option « Modifier un actif ».
4. Lance le pop-up d’export des actifs (suite chapitre 4.2.6).
5. Supprime un actif. Attention, cette action est définitive, même si l’actif est utilisé dans l’analyse.

### Créer un actif

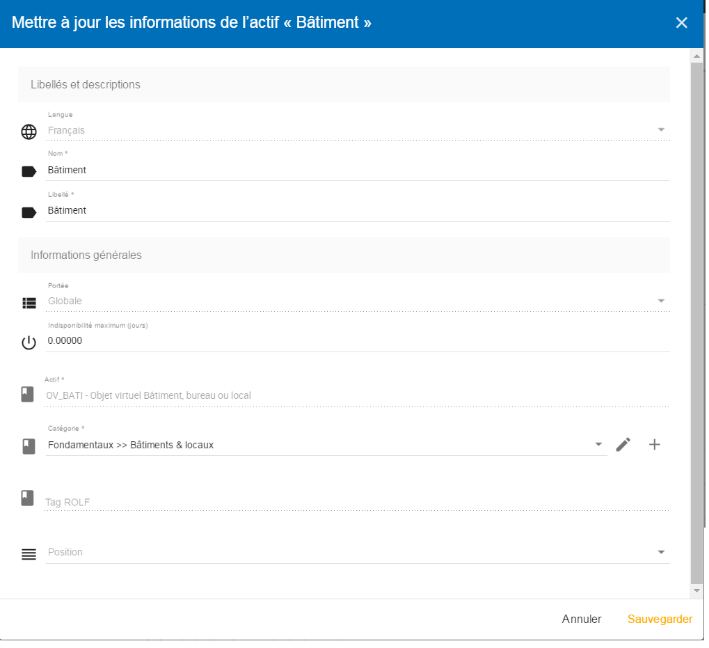
Dans la bibliothèque, après avoir cliqué sur « Ajouter un actif », le pop-up suivant apparaît :



1. Pour créer un actif, il est également possible de l’importer (suite chapitre 4.2.5).
2. Sélection de la langue : Cette option n’est pas utilisable, la langue par défaut de l’analyse est imposée.
3. Nom de l’actif : Ce nom doit être unique pour l’analyse.
4. Libellé de l’actif : C’est un complément de description, il est affiché dans la bulle d’aide lorsque la souris est positionnée sans bouger sur l’actif.
5. Portée de l’actif, deux choix possibles :
   1. Locale : les risques identifiés de l’actif sont à évaluer à chaque fois que ce dernier est présent dans l’analyse. *Un actif primaire est généralement à portée locale.*
   2. Globale : les risques identifiés de l’actif ne sont à évaluer qu’une seule fois pour toute l’analyse. Cette option est à utiliser surtout pour les actifs de support, dès qu’ils sont repris dans plusieurs actifs primaires. Exemple, la salle informatique, le bâtiment principal : une fois les risques évalués seul l’impact provenant de l’actif primaire peut faire changer le niveau de risque.
6. Information facultative indiquant le délai d’indisponibilité au-delà duquel l’impact sur l’organisme devient important ou plus. La collecte de cette information permet de comparer les exigences métiers (actifs primaires) avec la résilience de l’ensemble des actifs de support.
7. Sélection du type d’actif : C’est lui qui détermine la nature de l’actif et donc le modèle de risque qui lui est associé.
8. Sélection de la catégorie, c’est-à-dire l’endroit dans la bibliothèque où l’actif sera stocké, ou bien création « + » d’une nouvelle catégorie.
9. Pour les actifs primaires uniquement, le « Groupe risque opérationnel » permet d’associer à l’actif des risques opérationnels par défaut.
10. Permet d’ordonner les actifs dans la catégorie sélectionnée.

### Modifier un actif

L’appel est effectué à partir du menu contextuel lorsqu’un objet de la bibliothèque est sélectionné. Le pop-up suivant apparaît :

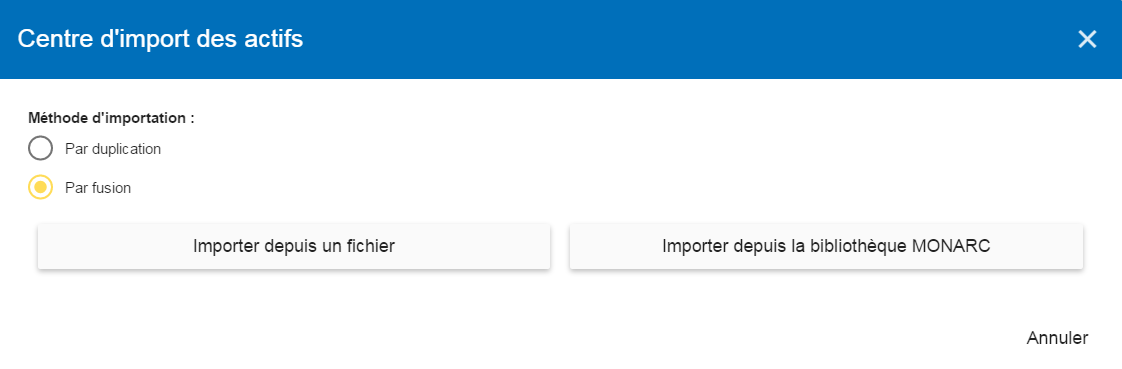


Pour l’explication de l’ensemble des champs pouvant être modifiée, voir le paragraphe 4.2.3 « Créer un actif ». Pour des raisons techniques, la modification ne permet pas de modifier :

* La sélection de la langue
* La portée « Locale » et « Globale » d’un actif.
* Le groupe de risques opérationnels

### Importer un actif

Ce pop-up est accessible à partir du pop-up « Ajouter un nouvel actif ».



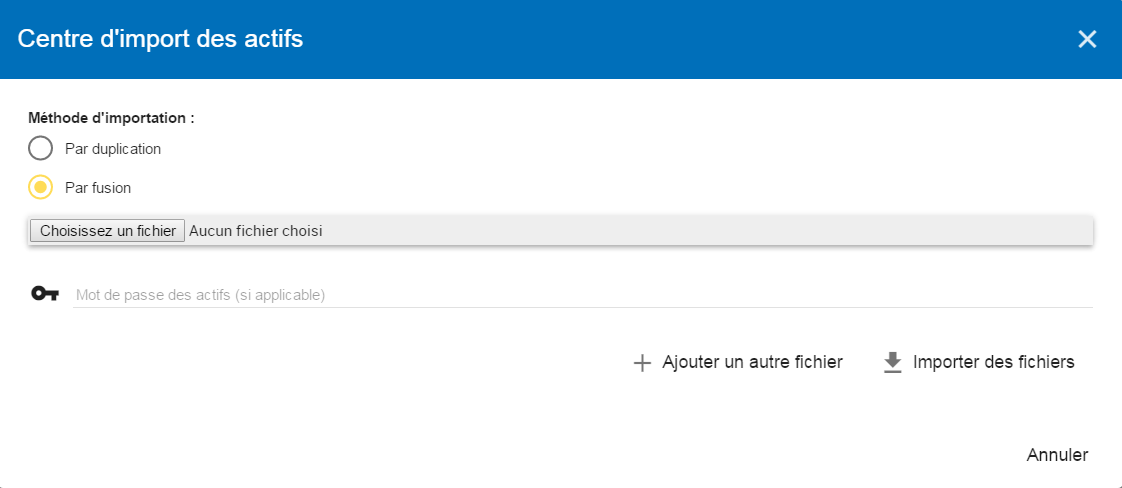
1. Le principe d’importation impose que l’objet importé reste dans la catégorie dans laquelle il se trouve. Deux méthodes d’importation sont alors possibles :
   1. « Par duplication » : lors de l’import, si un objet du même nom existe, alors il sera dupliqué et le nom sera suffixer «  - Imp #n ».
   2. « Par fusion » : lors de l’import, si un objet du même nom existe, alors il sera remplacé. Dans ce cas, seul le modèle de risques associé sera modifié.

*L’import d’objet d’origine non contrôlée peut être destructif pour l’analyse en cours. Il est fortement conseillé de créer un Snapshot avant l’import, ou d’utiliser une analyse vide « Bac à sable ».*

1. « Importer depuis un fichier » : permet d’échanger des actifs d’un environnement à l’autre (suite voir chapitre 4.2.5.1).
2. « Importer depuis la bibliothèque MONARC » ": Cette option n’est pas disponible dans le cas d’une une version « Stand Alone » de MONARC (suite voir chapitre 4.2.5.2).

#### Importer un actif depuis un fichier

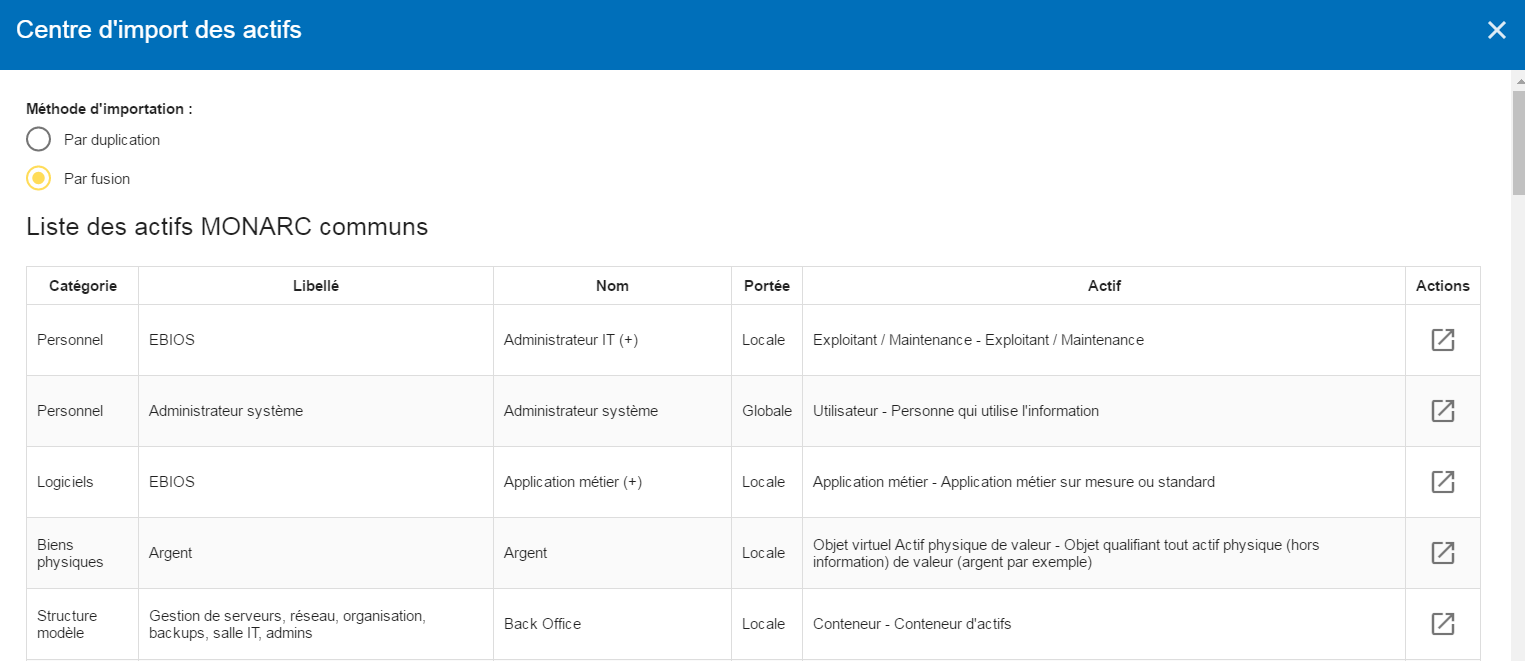
Le pop-up apparaît après avoir cliqué sur l’option « Importer depuis un fichier » du centre d’import des actifs.



1. Accède aux répertoires de l’ordinateur pour pointer sur un fichier.
2. Mots de passe : Si à l’export du fichier sélectionné, un mot de passe a été utilisé pour chiffrer ce dernier, il faut l’entrer ici.
3. Lance l’import du fichier

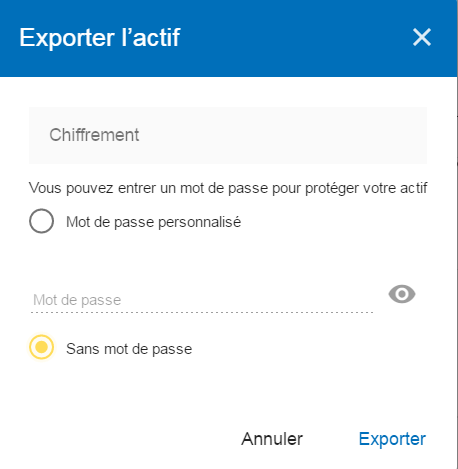
#### Importer depuis la bibliothèque MONARC

Le pop-up apparaît après avoir cliqué sur l’option « Importer depuis un fichier » du centre d’import des actifs.

****

1. Tableau des actifs disponible se trouvant dans la base commune
2. Action : lancement de la procédure d’import pour l’actif correspondant.

### Exporter un actif

****

1. Possibilité de chiffrer le fichier généré avec un mot de passe symétrique qui sera nécessaire lors de l’import.

## Risques de l’information

### Table des risques

En sélectionnant le haut de l’analyse ou un actif de l’arborescence, la table des risques apparaît.

****

1. Il existe deux tables de risques distinctes
   1. La table des risques de l’information basée sur les critères CID.
   2. La table des risques opérationnels basée sur les conséquences ROLFP

Il existe deux règles métiers pour gérer l’affichage :

1. Seuls les actifs de supports peuvent posséder des risques de l’information.
2. Seuls les actifs primaires peuvent posséder des risques opérationnels.

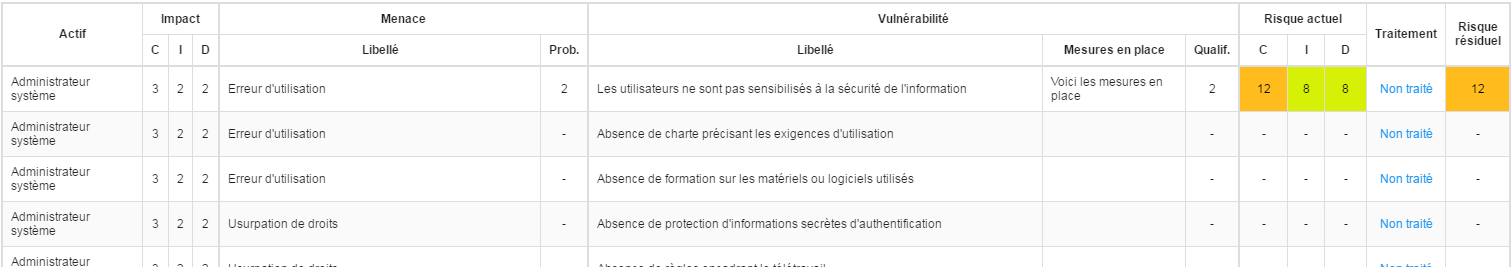
Selon l’actif en cours de sélection l’affichage peut donc changer :

* Dans le cas d’un actif primaire :
  + Il peut exister des risques opérationnels
  + La table des risques de l’information est composée de tous les risques des actifs de support qui le compose.
* Dans le cas d’un actif de support :
  + La table des risques de l’information est composée de tous les risques de l’actif de support sélectionné.
  + La table des risques opérationnels n’existe pas.
* Dans le cas où c’est la racine de l’analyse qui est sélectionnée :
  + La table des risques de l’information est composée de tous les risques des actifs de support qui composent l’analyse.
  + La table des risques opérationnels est composée de tous les risques des actifs primaires qui composent l’analyse.



1. L’actif primaire « Service RH » est sélectionné dans l’analyse.
2. Affichage des impacts CID du « service RH ».
3. Onglet « Risques de l’information » sélectionné.
4. L’actif « Service RH » est composé d’actifs de support qui fournissent en tout 106 risques (dans cet exemple).
5. Possibilité de ne sélectionner que certains risques, selon le seuil d’acceptation des risques.
6. Possibilité de trier sur la plupart des colonnes de la table.
7. Sélection de la page dans la liste de résultats



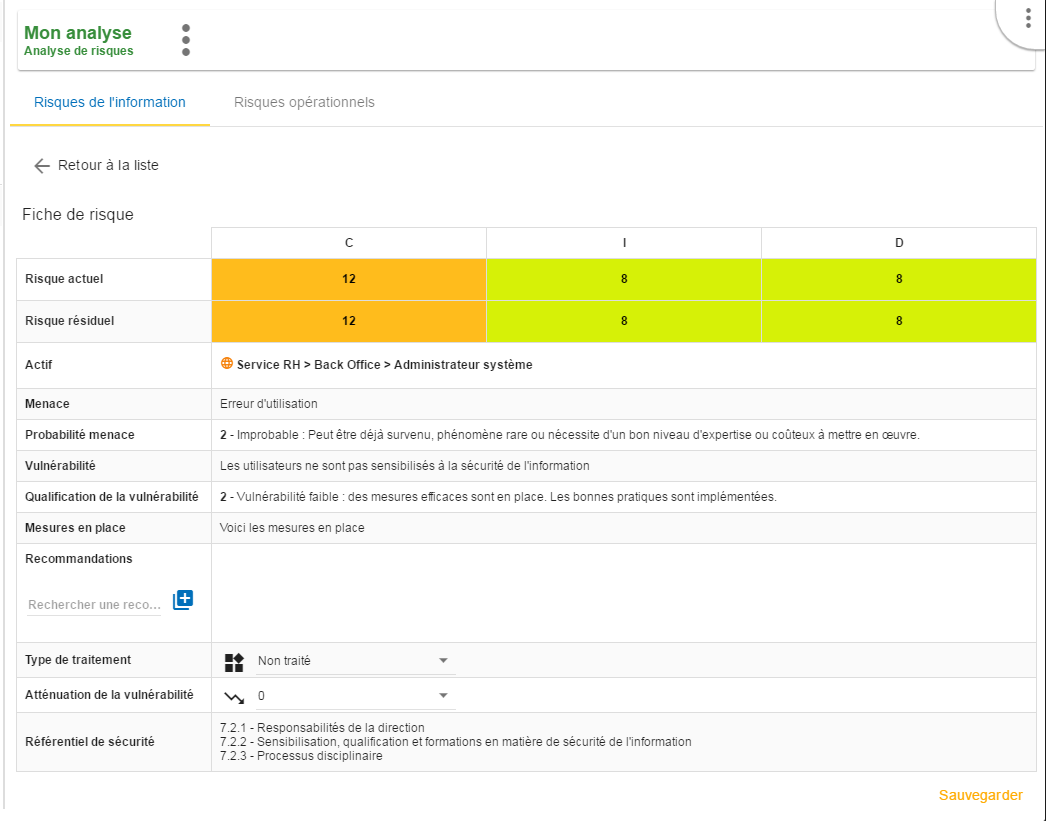


1. Actif concerné par l’évaluation
2. Les critères CID qui ont été affectés au « Service RH » sont hérités par défaut par les actifs de support.
3. Libellé de la menace.
4. Probabilité de la menace (échelles d’évaluation, voir chapitre 5).
5. Libellé de la vulnérabilité.
6. Mesure en place : Décrire ici, de façon factuelle les mesures de sécurité en place concernant la vulnérabilité ou plus largement le risque en question.
7. Évaluation de la mesure en place pour déterminer le niveau de vulnérabilité (échelles d’évaluation, voir chapitre 5).
8. Valeur du risque calculé en fonction de la formule de calcul du risque. Les couleurs dépendent de la grille d’acceptation des risques (Grille d’acceptation des risques, voir chapitre 5).
9. Indication si le risque est traité et lien vers la fiche risque (suite voir chapitre 4.3.2).
10. Valeur du risque résiduel. Dans le cas de la figure ci-dessus, le risque résiduel est égal au risque max, parce qu’il n’est pas encore traité.

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

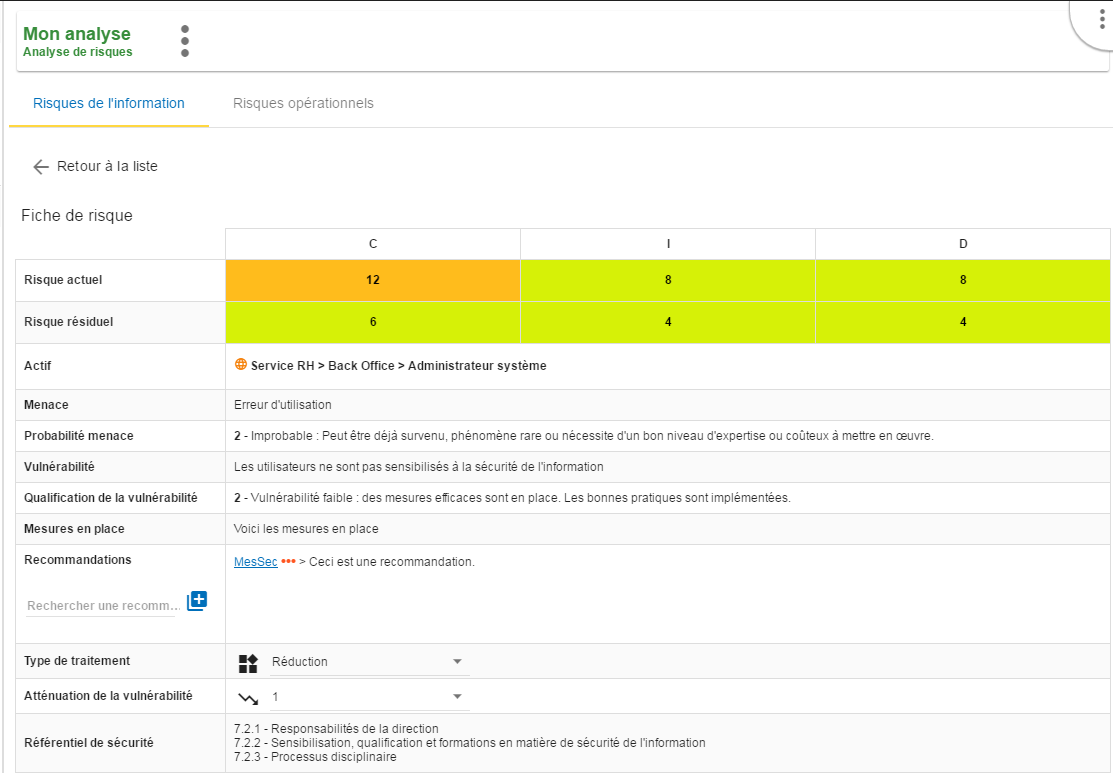
### Fiche risque de l’information

La fiche risque s’affiche lorsque l’on clique sur le lien « Traitement » de la table des risques de l’information.

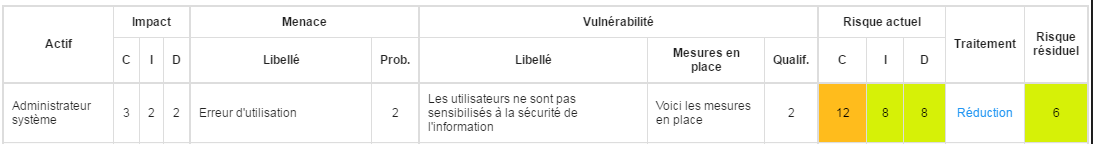


1. Bouton de retour à la table des risques.
2. Valeurs du risque pour les critères CID (non encore traité dans l’exemple).
3. Rappel des paramètres de la table des risques.
4. Bouton de création/Affectation d’une ou plusieurs mesures de sécurité.
5. Sélection du type de traitement du risque, les 4 valeurs ont leurs sources d’ISO/IEC 27005 :
   1. Réduction
   2. Refusé
   3. Accepté
   4. Partagé
6. Choix d’une valeur de réduction du risque, plus la mesure recommandée est efficace, plus la valeur de réduction est grande.
7. Proposition de mesures de sécurité provenant de référentiels divers.
8. Sauvegarde de la fiche pour calculer le risque résiduel.

La figure ci-dessus montre la fiche risque après traitement du risque et validation.

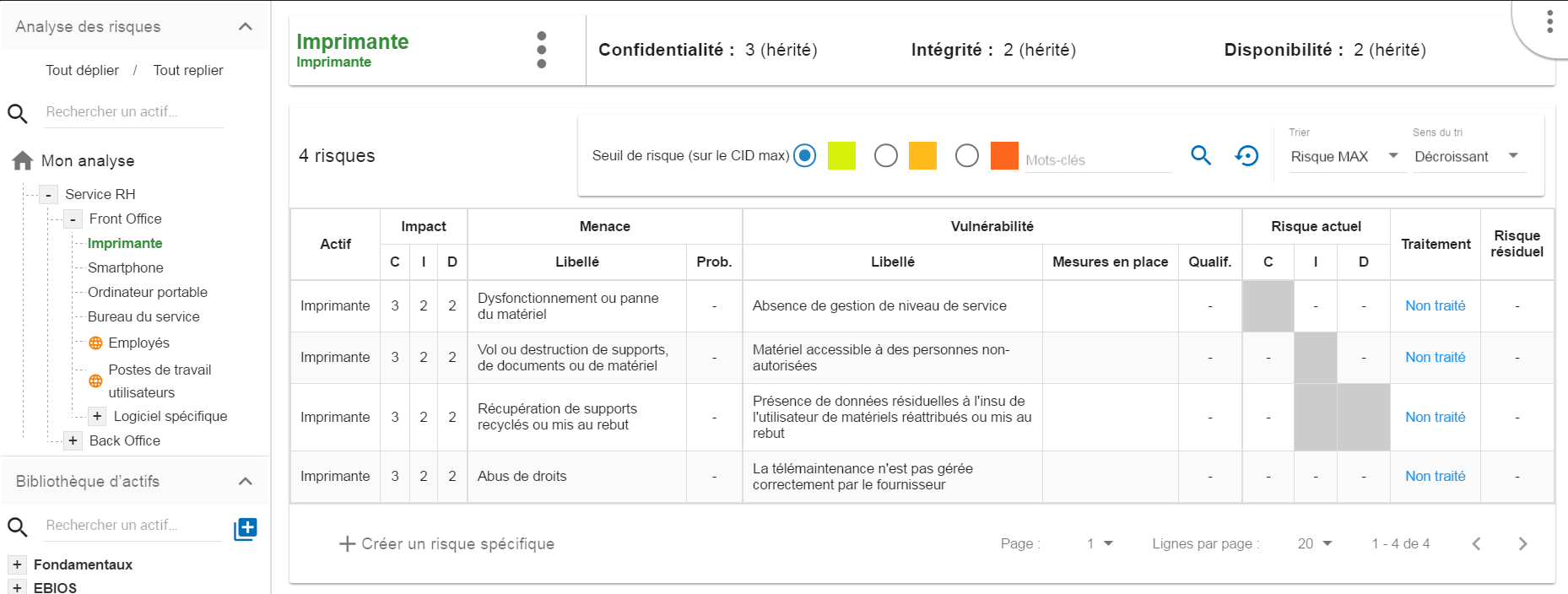


La table des risques devient :



### Ajout risque supplémentaire

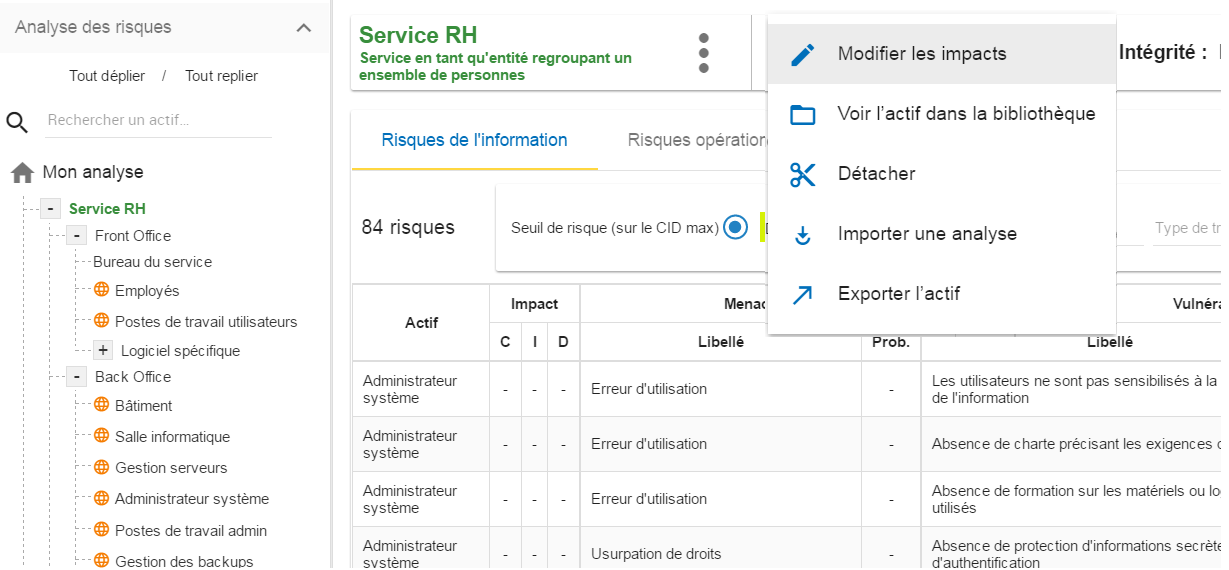
Lorsqu’un actif est sélectionné dans l’analyse



1. Cliquer pour créer un risque spécifique : Un pop-up apparaît et permet d’associer à l’actif courant, un couple Menace/Vulnérabilité. La menace et la vulnérabilité doivent exister au préalable.

### Menu contextuel

En cliquant sur les 3 points, le menu contextuel apparaît :

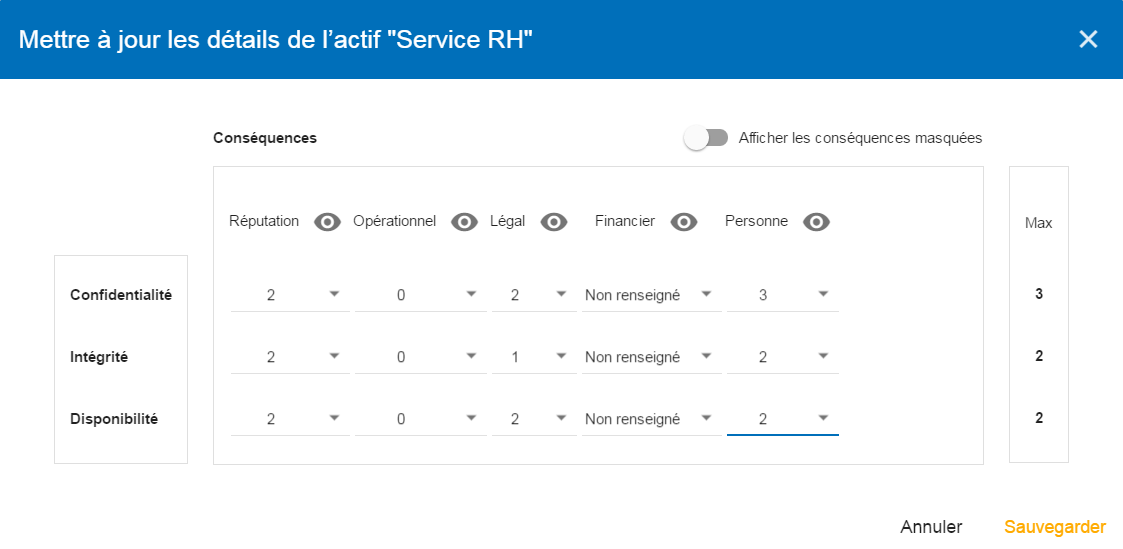


1. Affiche la vue de modification des impacts et conséquences (suite voir chapitre 4.3.5).
2. Affiche l’actif depuis la bibliothèque, ce qui permet d’avoir un autre menu contextuel qui permet les modifications de l’actif.
3. Détacher permet d’enlever un actif de l’analyse des risques. *Attention cette action peut entrainer la perte des évaluations des risques pour cet actif et ses enfants.*
4. Permet d’importer une analyse, à partir de l’endroit pointé par l’actif sélectionné de l’analyse. L’import fonctionne exactement comme l’import d’un actif, voir chapitre 4.2.5).
5. Permet d’exporter une analyse, à partir de l’endroit pointé par l’actif sélectionné de l’analyse. L’export fonctionne exactement comme l’import d’un actif, voir chapitre 4.2.6).

### 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.

Le pop-up ci-dessous apparaît :



*La consultation des échelles d’impacts se fait par le menu en haut à droite de l’écran.*

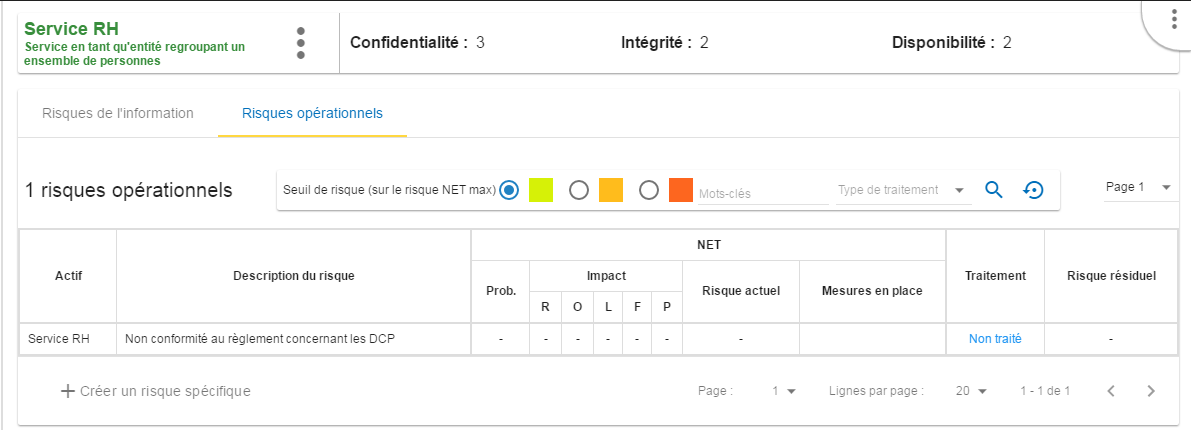
*En laissant la souris sur les chiffres, le libellé apparaît après 1 seconde.*

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.

## Risques opérationnels

### Table des risques

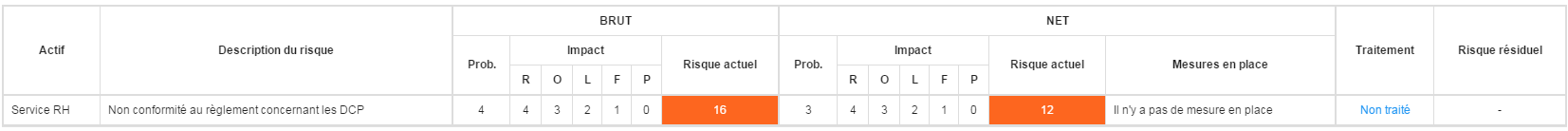


1. L’actif primaire « Service RH » est sélectionné dans l’analyse.
2. Onglet « Risques opérationnels » sélectionné.
3. L’actif « Service RH » ne possède qu’un seul risque opérationnel.
4. Possibilité de ne sélectionner que certains risques, selon le seuil d’acceptation des risques.
5. Possibilité de trier sur la plupart des colonnes de la table.
6. Sélection de la page dans la liste de résultats.

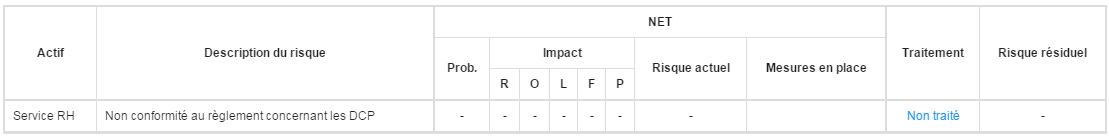
Selon l’option choisie, la table des risques opérationnels peut afficher ou non les risques bruts, c’est-à-dire les risques tels qu’ils impacteraient l’organisme sans aucune mesure de sécurité.

Certaine société n’utilise pas cette option, donc pour gagner de l’espace horizontal, la partie risques bruts est escamotée.





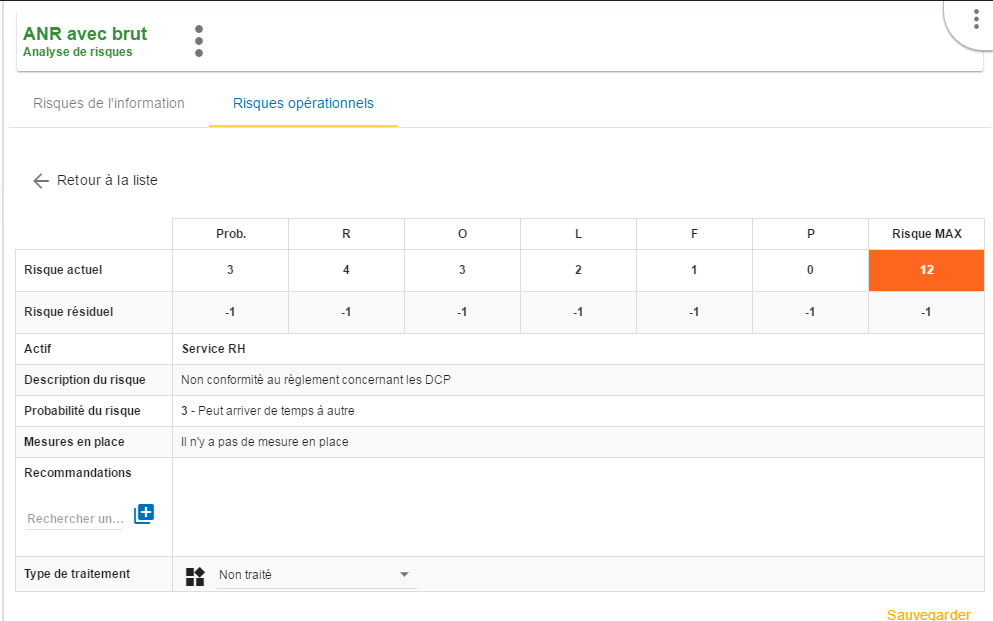




1. Actif concerné par l’évaluation
2. Description du risque
3. Le risque opérationnel brut est calculé à partir des deux paramètres « Probabilité » du scénario de risque, multiplié par l’impact sur le ROLFP (voir échelles d’évaluation au chapitre 5). Le risque actuel, représente la valeur maximum de la probabilité sur les valeurs d’impacts ROLFP renseignées.
4. Le risque NET représente le risque avec les mesures en place actuellement. Le calcul est le même que pour les risques bruts.
5. Mesure en place : Décrire ici, de façon factuelle les mesures sécurité en place concernant le risque en question.
6. Indication si le risque est traité et lien vers la fiche risque (suite voir chapitre 4.4.2).
7. Valeur du risque résiduel. Dans le cas de la figure ci-dessus, le risque résiduel est égal au risque max, parce qu’il n’est pas encore traité.

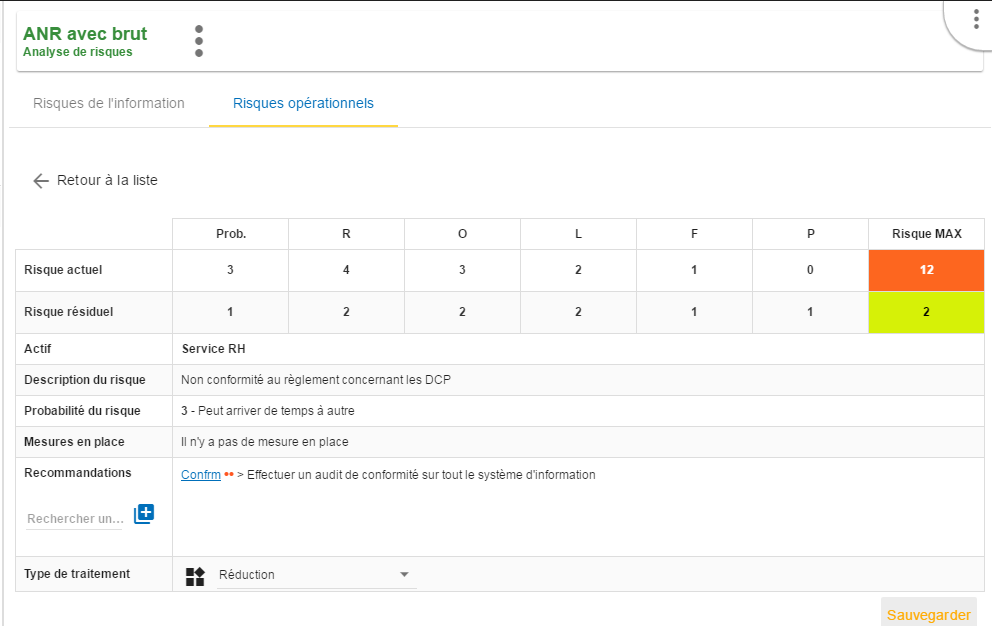
### Fiche risque opérationnel

La fiche risque s’affiche lorsque l’on clique sur le lien « Traitement » de la table des risques de l’information.



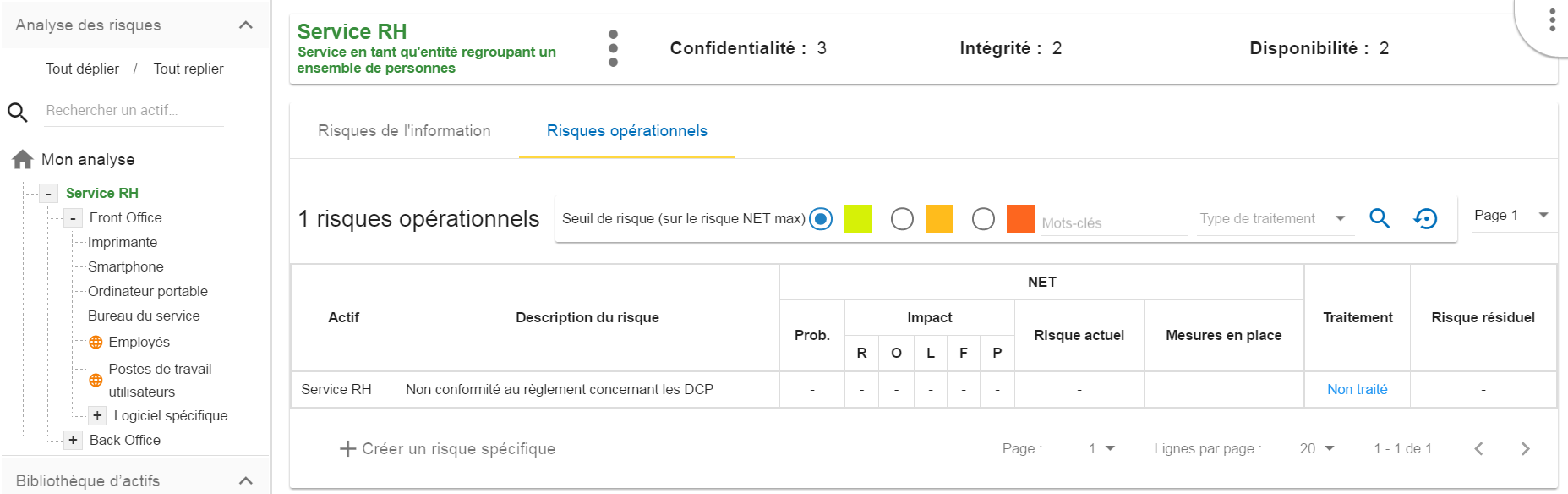
1. Bouton de retour à la table des risques.
2. Valeurs du risque actuel pour les critères ROLFP.
3. Valeurs du risque résiduel pour les critères ROLFP (non encore traité). Ces valeurs doivent être ajustées en fonction de la recommandation et des mesures qui seront mises en place.
4. Rappel des paramètres de la table des risques.
5. Bouton de création/Affectation d’une ou plusieurs mesures de sécurité.
6. Sélection du type de traitement du risque, Les 4 valeurs sont tirées d’ISO/IEC 27005 :
   1. Réduction (modification)
   2. Refusé
   3. Accepté
   4. Partagé
7. Sauvegarde de la fiche pour calculer le risque résiduel.

Une fois la validation effectuée, le risque est traité :



### Ajout risque supplémentaire

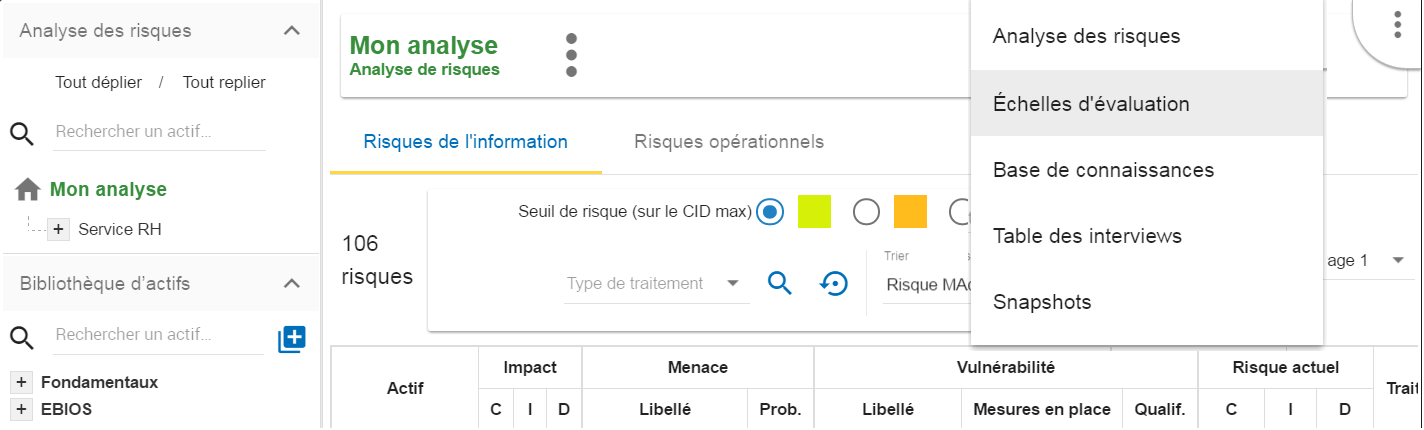
Lorsqu’un actif est sélectionné dans l’analyse

1. Cliquer pour créer un risque spécifique : Un pop-up apparaît et permet d’associer à l’actif courant, un nouveau risque. Si le risque n’existe pas, il peut être créé à la volée.

# Échelles d’évaluation

Le menu est toujours accessible à partir de la vue principale de MONARC :



1. Appel du menu
2. Appel de la vue de gestion des échelles d’évaluation

La vue « Échelles d'évaluations » reprend à la suite :

1. L’échelle d’impact
2. L’échelle des menaces
3. L’échelle de vulnérabilités
4. La gestion des seuils d’acceptation des risques de l’information
5. La gestion des seuils d’acceptation des risques opérationnels

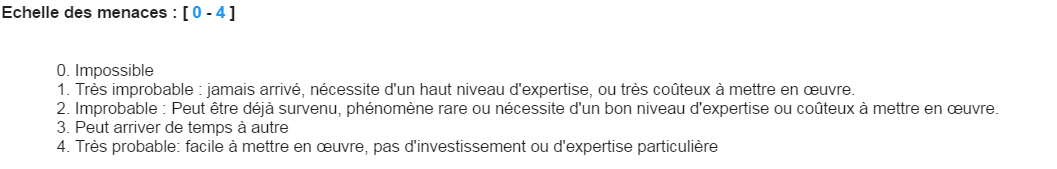
**Note** : Toutes les échelles sont modifiables et les échelons personnalisables. Toutefois, il n’est plus autorisé de modifier les échelles dès qu’une évaluation a été encodée.

## Échelles d’impact



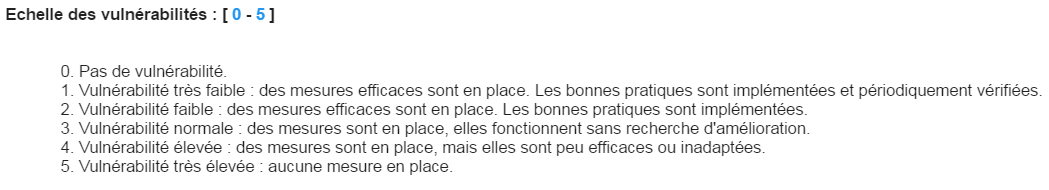
1. Cliquer pour modifier le nombre d’échelons.
2. Cliquer pour « Afficher ou Masquer » les critères non utilisés de l’analyse.
3. Cliquer sur le symbole  pour masquer une colonne inutilisée.
4. Cliquer pour ajouter un nouveau critère d’impact.
5. Cliquer pour éditer les libellés de chaque échelon (la gestion est telle une table Excel, en cliquant sur un libellé, il est possible de l’éditer, en cliquant sur un autre, le premier se sauvegarde automatiquement et ainsi de suite).

## Échelles des menaces



1. Cliquer pour modifier le nombre d’échelons
2. Cliquer pour éditer les libellés de chaque échelon (Gestion idem échelle impact).

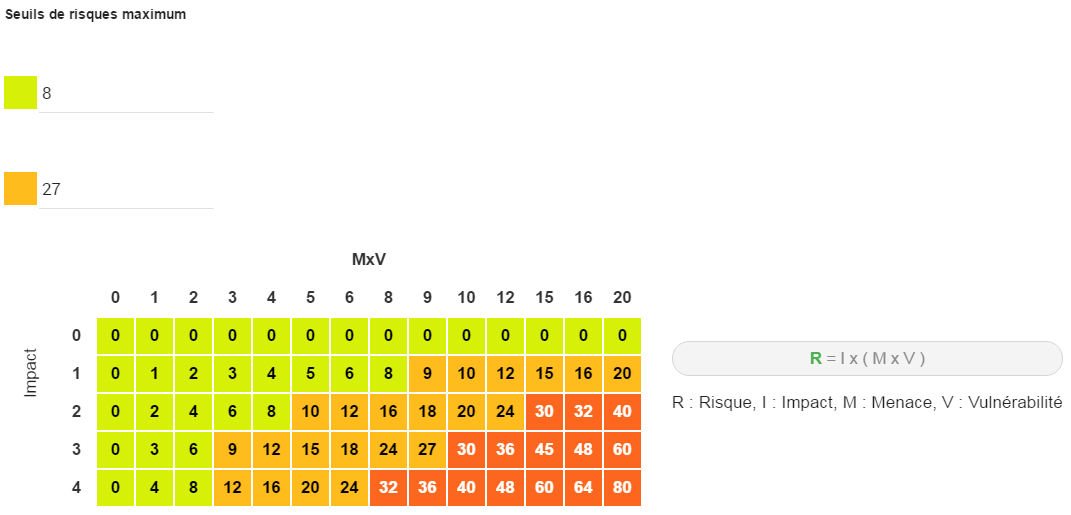
## Gestion des vulnérabilités



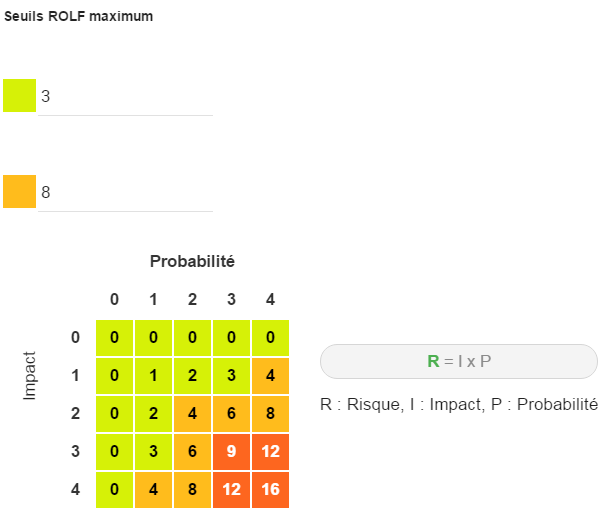
1. Cliquer pour modifier le nombre d’échelons
2. Cliquer pour éditer les libellés de chaque échelon (Gestion idem échelle impact).

## Gestion des seuils d’acceptation des risques opérationnels

Pour les risques de l’information :



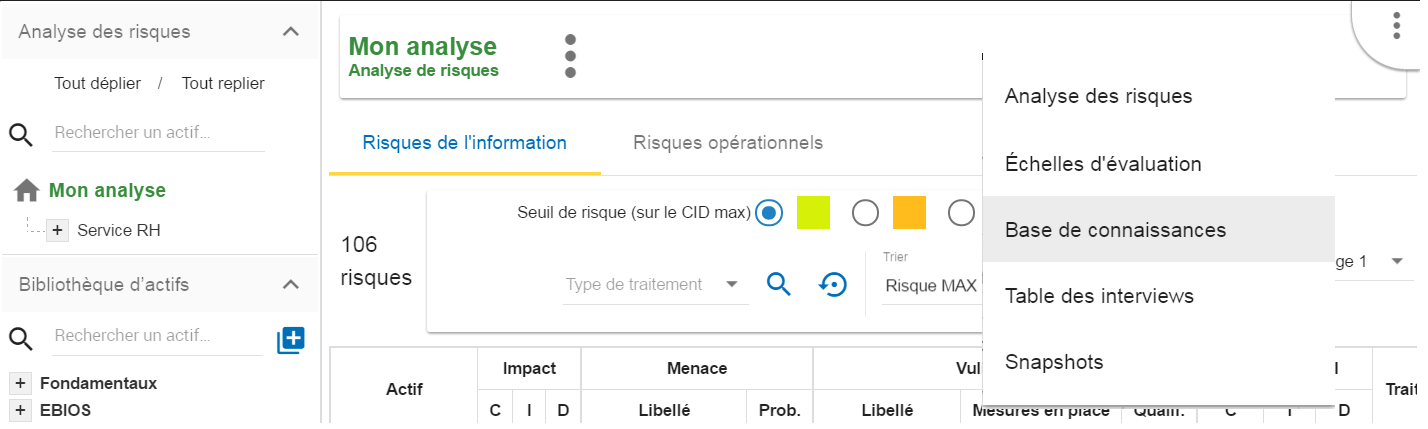
Pour les risques opérationnels :



1. Modification des valeurs de seuils. La table juste au-dessous se met à jour directement, ainsi que toutes les tables de risques de l’analyse.

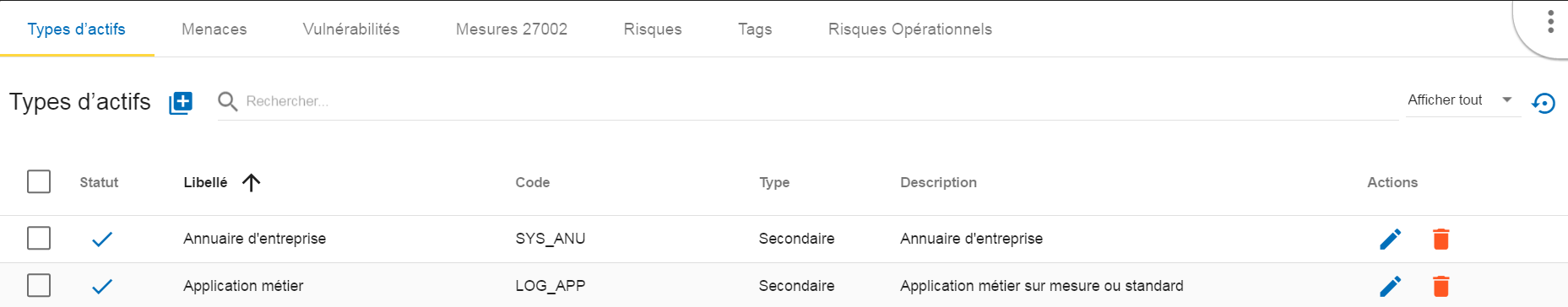
# Gestion bases de connaissances

Le menu est toujours accessible à partir de la vue principale de MONARC :



1. Appel du menu
2. Appel de la vue de gestion des échelles d’évaluation

Tous les paramètres se gèrent avec la même vue de gestion :



1. Sélection de l’onglet de paramètres désiré
2. Ajout d’un paramètre en fonction de l’onglet actif. Fais apparaître un pop-up demandant des informations contextuelles.
3. Recherche d’un paramètre
4. Sélection d’un paramètre (pour suppression)
5. Édition / suppression de paramètre actif.

De façon générale, tous les paramètres possèdent un code, un libellé et une description

* Le code permet de catégoriser le paramètre
* Le libellé est celui qui s’affiche dans toutes les vues de MONARC
* La description est le libellé qui s’affiche généralement dans la bulle d’aide.

## Types d’actifs

Il existe deux types d’actifs :

* Les actifs primaires ou business : Ils représentent généralement sans être exhaustif, des services internes ou externes, des processus ou de l’information. Ce sont eux que l’on place à la racine de l’analyse et qui déclineront leurs impacts sur les autres actifs. *Les conteneurs utilisés pour organiser visuellement l’analyse sont déclarés en tant qu’actif primaire (exemple Back Office).*
* Les actifs secondaires ou de supports : Ce sont les actifs sur lesquels on associe des risques, ils servent ainsi à décrire le profil de risques des actifs primaires.

## Menaces

Les paramètres essentiels des menaces des menaces sont l’association avec les critères CID. Il est important lors de la création d’une nouvelle menace de bien spécifier ces critères, parce qu’ils vont conditionner les tables de risques.

Exemple : L’écoute passive (écouter, regarder sans rien toucher) est par exemple une menace qui n’affecte que le critère de confidentialité.

Les menaces possèdent des catégories pour pouvoir générer des statistiques.

## Vulnérabilités

Les vulnérabilités doivent décrire de façon négative le contexte de risque. Plus la vulnérabilité est grande, moins les mesures en place sont existantes ou efficaces. La vulnérabilité est inverse à la maturité.

Exemple : « Absence d'identification des biens sensibles » : Vulnérabilité faible si les biens sensibles sont identifiés et inversement la vulnérabilité est grande, s’ils ne le sont pas.

La description de la vulnérabilité est très importante, parce qu’elle apparaît dans la table des risques comme un complément de description qui permet d’aider le spécialiste en sécurité à affiner son questionnaire ou les points précis qui sont cherchés par rapport à un risque.

## Mesures 27002

C’est le référentiel qui est utilisé par défaut pour aider à proposer des mesures de sécurité au regard d’un risque spécifique.

## Risques

Cette table est le cœur de la base de connaissances de MONARC. C’est ici que l’on fait les associations entre le « Type d’actif », la « Menace » et la « Vulnérabilité ». C’est l’association des risques inhérents à chaque actif qui seront proposés par défaut lorsque le modèle de risque est créé.

À chaque association qui peut être assimilée à un scénario de risque, il est possible d’associer de 1 à 3 mesures de sécurité provenant d’ISO27002 (guide de bonnes pratiques en matière de sécurité de l’information).

Seuls les actifs de supports sont proposés pour une association Menace/Vulnérabilité.

## Tags (Risques opérationnels)

Les tags représentent une catégorisation des risques opérationnels. C’est un regroupement logique des risques qui pourra être ensuite associé à des actifs primaires.

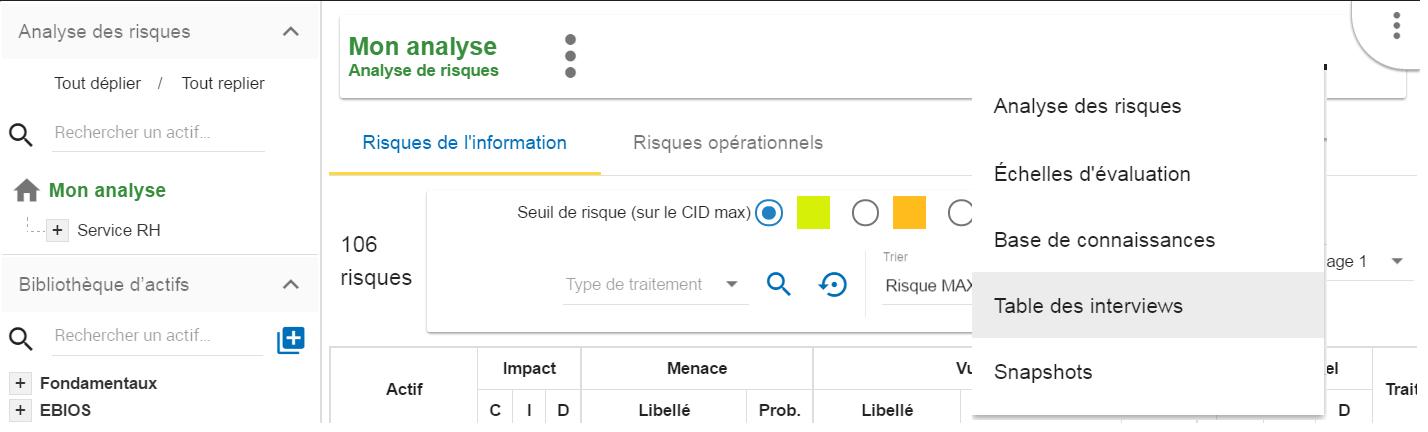
## Risques opérationnels

C’est une liste de risques créés par défaut ou ajoutés spécifiquement. Chaque risque peut être associé à zéro ou plusieurs tags, ce qui permet lorsque l’on dépose un actif dans l’analyse de proposer des risques par défaut, comme pour les risques de l’information.

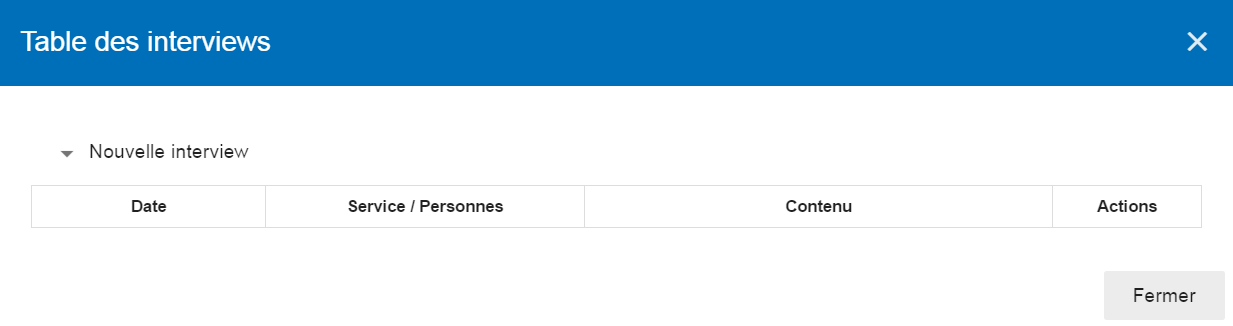
# Gestion des interviews

La table des interviews permet lors d’une analyse des risques de lister dans le rapport final, les différents interviews qui ont été nécessaires pour collecter l’information. Des informations telles que dates, personnes interviewées peuvent être saisies pour obtenir un rapport exhaustif.

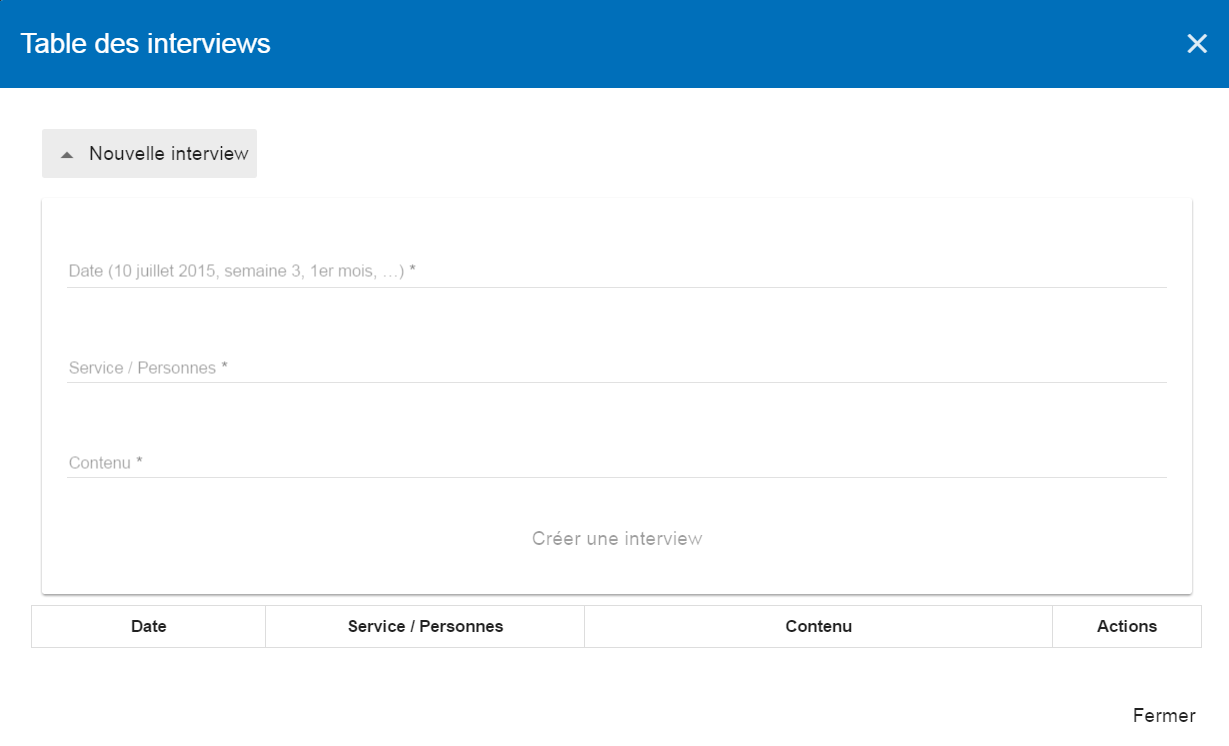
Le menu est toujours accessible à partir de la vue principale de MONARC :



1. Appel du menu
2. Appel de la vue de gestion des échelles d’évaluation



1. Clique pour encoder un nouvel interview

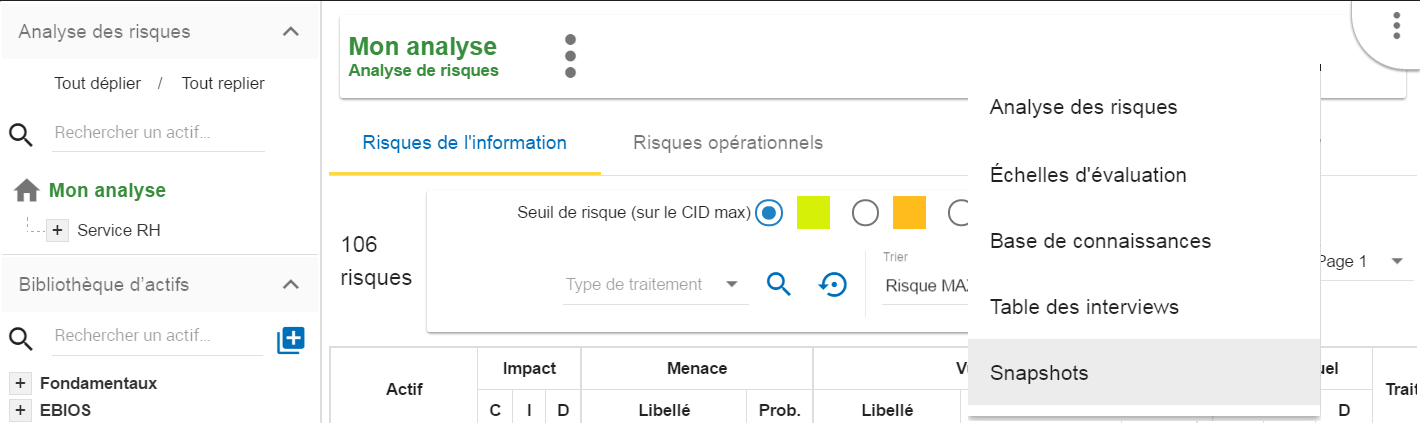


1. Information à saisir : date, noms des personnes et éventuellement les sujets abordés.

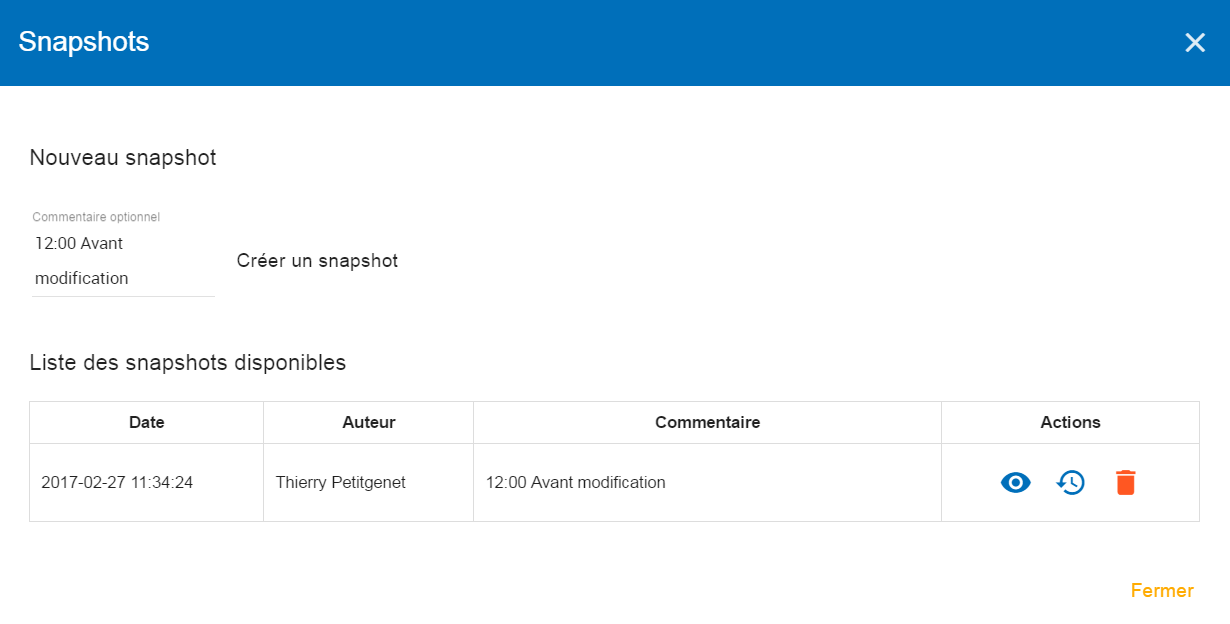
# Snapshots

Les Snapshots permettent de créer une sauvegarde d’une analyse complète. *C’est une fonction à utiliser régulièrement pendant le déroulement, avant et après de grands changements, car c’est le seul moyen de revenir en arrière dans les modifications.*

Le menu est toujours accessible à partir de la vue principale de MONARC :

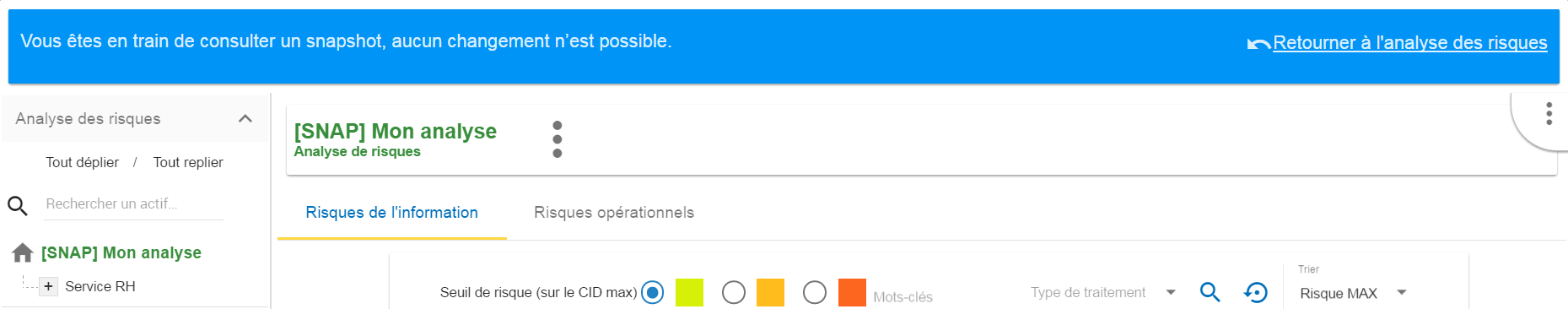


Le pop-up suivant apparaît :



1. « Créer un Snapshot » : Possibilité de saisir un commentaire permettant de contextualiser le Snapshot.
2. Actions possibles :
   1. Voir un Snapshop
   2. Restaurer un Snapshot. Attention cette option va écraser l’analyse en cours.
   3. Détruire un Snapshot.

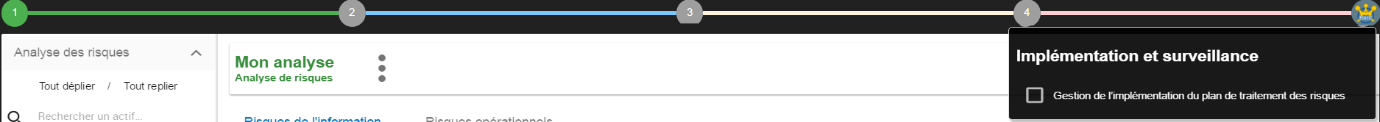
Lors de la consultation d’un Snapshot, aucune modification n’est possible, et la barre bleue comme montrée ci-dessus s’affiche :



1. Cliquer sur le bouton, pour revenir en mode fonctionnement normal.

# Gestion de l’implémentation du plan de traitement

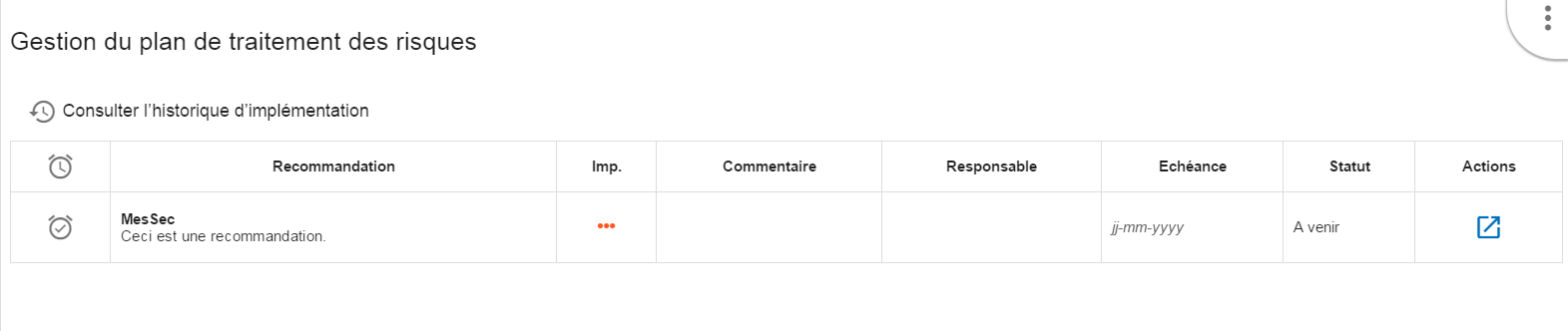
En cliquant, sur le chiffre 4 de la barre de méthode, le menu suivant apparaît :



Cette vue va au-delà de la norme ISO/IEC 27005, parce qu’elle permet de gérer le suivi de l’implémentation des mesures.

La version actuelle est en Beta, elle est développée mais en attente de retour des utilisateurs pour amélioration.

En cliquant sur le lien « Gestion de l’implémentation du plan de traitement des risques » la vue suivante apparaît, elle liste toutes les recommandations faites de l’analyse.

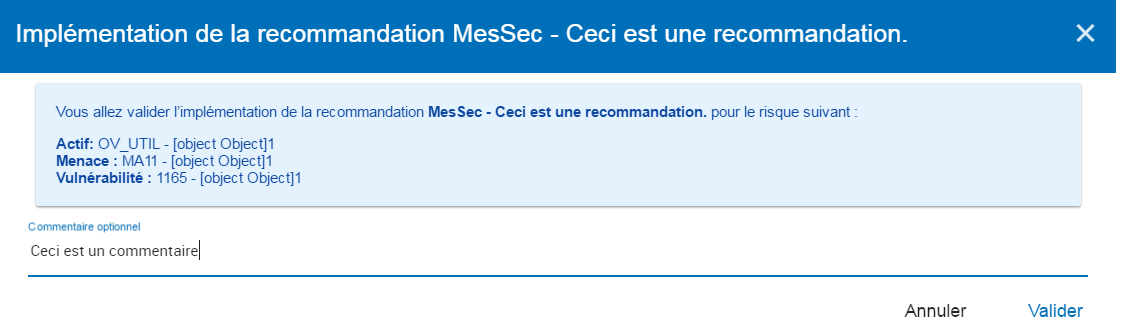


1. Nom de la recommandation
2. Commentaire sur la recommandation
3. Responsable de la mise en place de la recommandation
4. Échéance de mise en place de la recommandation
5. Etat de l’implémentation
6. Lorsque la recommandation a été implémentée, cliquer sur action va lancer le processus de mise à jour des risques (suite ci-dessous)

Cette vue, liste tous les risques qui sont dépendant de la recommandation. Ensuite, pour chaque risque les informations suivantes sont renseignées :



1. Diverses informations concernant le risque
2. Encoder la nouvelle constatation, telle que les choses sont après la mise à jour de la recommandation
3. Lance le pop-up validation de la mise à jour ci-après



Après validation, le risque visé devient le risque actuel, la recommandation est supprimée du risque concerné.

Toutes les validations sont historiées et peuvent être consultées :



1. Cliquer pour consulter l’historique des recommandations échues

