

**MONARC**

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

**Documentation de la méthode**

**v1.0**

Table des matières

[1 Introduction 3](#_Toc476055471)

[1.1 Objectif du document 3](#_Toc476055472)

[1.2 Avertissement de compatibilité 3](#_Toc476055473)

[1.3 Syntaxe utilisée dans le document 3](#_Toc476055474)

[1.4 Syntaxe utilisée dans MONARC 3](#_Toc476055475)

[2 Méthode MONARC 4](#_Toc476055476)

[2.1 Méthode itérative 4](#_Toc476055477)

[2.2 Méthode « Qualitative » 5](#_Toc476055478)

[2.3 Méthode largement inspirée d’ISO/IEC 27005 5](#_Toc476055479)

[2.4 Accès aux écrans méthodologiques 6](#_Toc476055480)

[2.5 Définition du contexte d’analyse des risques 6](#_Toc476055481)

[3 Définition du contexte d’analyse des risques 7](#_Toc476055482)

[3.1 Contexte de l’analyse des risques 7](#_Toc476055483)

[3.2 Evaluation des tendances, des menaces et synthèse 8](#_Toc476055484)

[3.2.1 Évaluations des tendances 8](#_Toc476055485)

[3.2.2 Évaluations des menaces 8](#_Toc476055486)

[3.2.3 Résumé des évaluations 9](#_Toc476055487)

[3.3 Contexte de gestion des risques 9](#_Toc476055488)

[3.4 Définition des critères d'évaluation, d'acceptation et d'impact 10](#_Toc476055489)

[3.4.1 Échelle d’impacts 10](#_Toc476055490)

[3.4.2 Échelles des menaces 11](#_Toc476055491)

[3.4.3 Gestion des vulnérabilités 11](#_Toc476055492)

[3.4.4 Gestion des seuils d’acceptation 11](#_Toc476055493)

[3.5 Livrable : Validation du contexte 12](#_Toc476055494)

[4 Modélisation du contexte 13](#_Toc476055495)

[4.1 Identification des actifs, vulnérabilités 13](#_Toc476055496)

[4.2 Évaluation des impacts et conséquences 13](#_Toc476055497)

[4.3 Synthèse des actifs / impacts 14](#_Toc476055498)

[4.4 Livrable : Validation du contexte 15](#_Toc476055499)

[5 Évaluation et traitement des risques 16](#_Toc476055500)

[5.1 Évaluation et traitement des risques 16](#_Toc476055501)

[5.1.1 Évaluation des probabilités de menaces 16](#_Toc476055502)

[5.1.2 Évaluation des vulnérabilités 16](#_Toc476055503)

[5.1.3 Traitement des risques 16](#_Toc476055504)

[5.2 Gestion du plan de traitement 16](#_Toc476055505)

[5.3 Livrable : Rapport final 17](#_Toc476055506)

[6 Implémentation et surveillance 18](#_Toc476055507)



# fond_doc2fond_doc2fond_doc2Introduction

## Objectif du document

Ce document a pour objectif d’expliquer le déroulement de la méthode MONARC à travers les étapes proposées par l’outil.

## 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.).

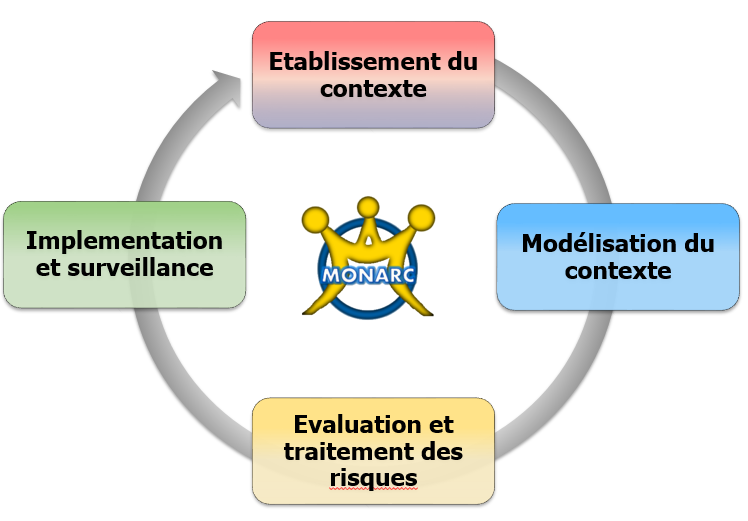
: La plupart des champs de MONARC affichent une information complémentaire, lorsque la souris est laissée quelques instants immobiles dessus.

# Méthode MONARC

MONARC est une méthode itérative « Qualitative » d’analyse des risques en quatre phases, très largement inspirée d’ISO/IEC 27005.

## Méthode itérative

MONARC est une méthode itérative qui permet de progresser pragmatiquement dans la gestion des risques. Cette approche, conseillée par ISO 27005 permet de se restreindre d’abord à l’essentiel, puis de procéder à des itérations successives pour élargir la cible ou l’approfondir à des dimensions plus techniques. Les modèles de risques optimisés fournis de base avec l’outil permettent cette gestion.



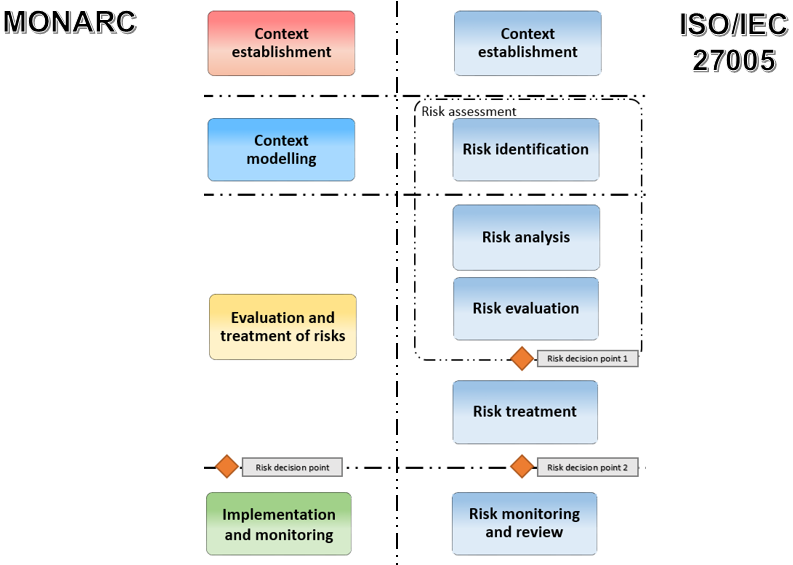
1. **Établissement du contexte** : Définition de la cible d’analyse des risques, découverte et description du contexte, définition des critères d’analyses des risques et de la structure de l’approche des risques.
2. **Modélisation du contexte** : Phase de construction du modèle de risques. Après avoir identifié les actifs primaires, il suffit de les décomposer en actifs de supports de façon hiérarchique. Les actifs les plus usuels sont présents dans la base de connaissance de MONARC et donc une identification par défaut des risques est proposée. Cette identification est peut être suffisante dans une première itération de risques, mais il est à la charge de l’expert en sécurité de rendre le modèle exhaustif.
3. **Évaluation et traitement des risques** : L’évaluation des risques consiste à déterminer les niveaux de menaces et de vulnérabilités du contexte traité. Le traitement des risques consiste à proposer des mesures de sécurité qui vont tendre à baisser les grands risques à des niveaux acceptables, ainsi qu’à accepter les risques faibles.
4. **Implémentation et surveillance** : La version actuelle de MONARC, propose en version Beta des vues de suivies de l’implémentation des recommandations. La surveillance consiste à vérifier périodiquement les changements significatifs du contexte d’analyse des risques, mais également tout changement significatif à l’extérieur du contexte et qui suggèreraient de refaire une itération d’analyse.

## Méthode « Qualitative »

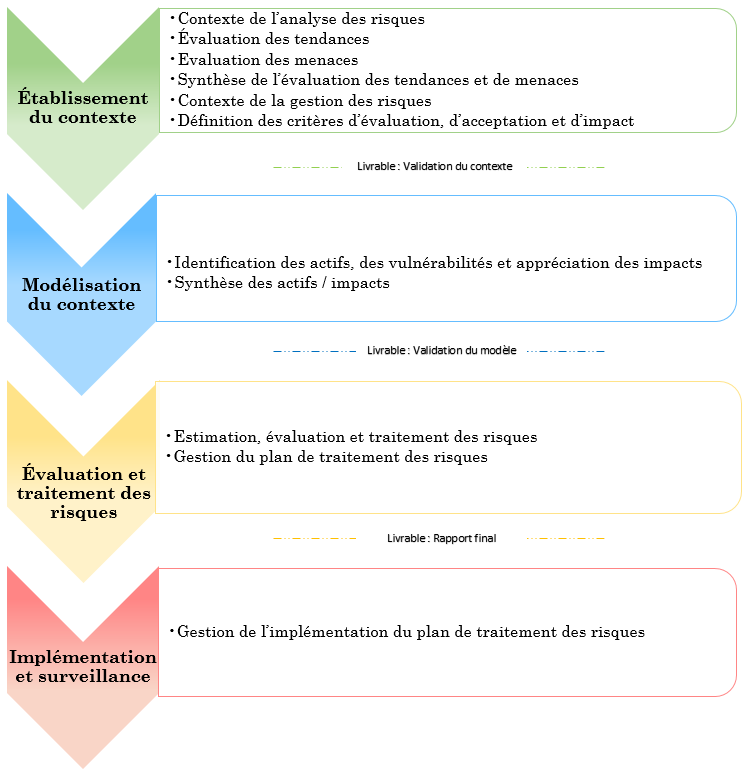
MONARC est une méthode « Qualitative », c’est-à-dire que les paramètres du risque sont exprimés sur des échelles numériques contextuelles qui permettent de hiérarchiser les risques. Cette approche est préconisée par ISO/IEC 27005 parce qu’elle est plus simple à appréhender, surtout pour des critères non tangibles d’impact et de conséquences comme la « Réputation », l’« Image », la « Légalité », etc.

## Méthode largement inspirée d’ISO/IEC 27005

La figure ci-dessous montre le parallèle entre ISO/IEC 27005 et MONARC.



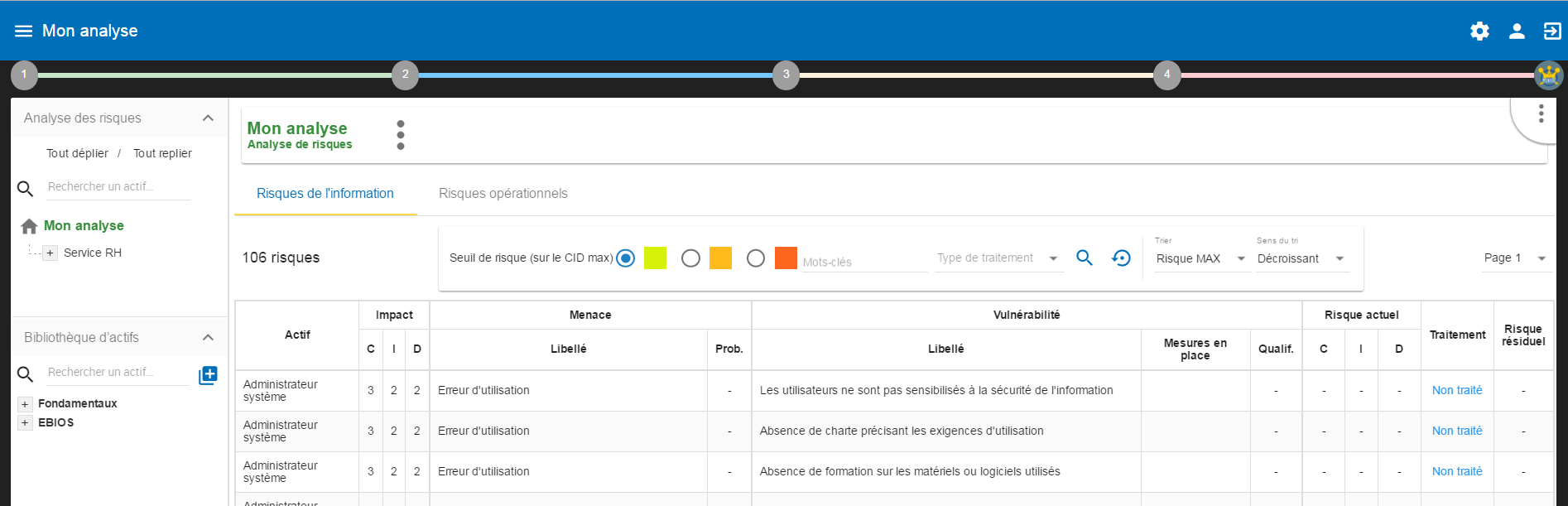
Les sous-étapes proposées par la méthode vont également dans le sens d’ISO/IEC 27005 :



## Accès aux écrans méthodologiques

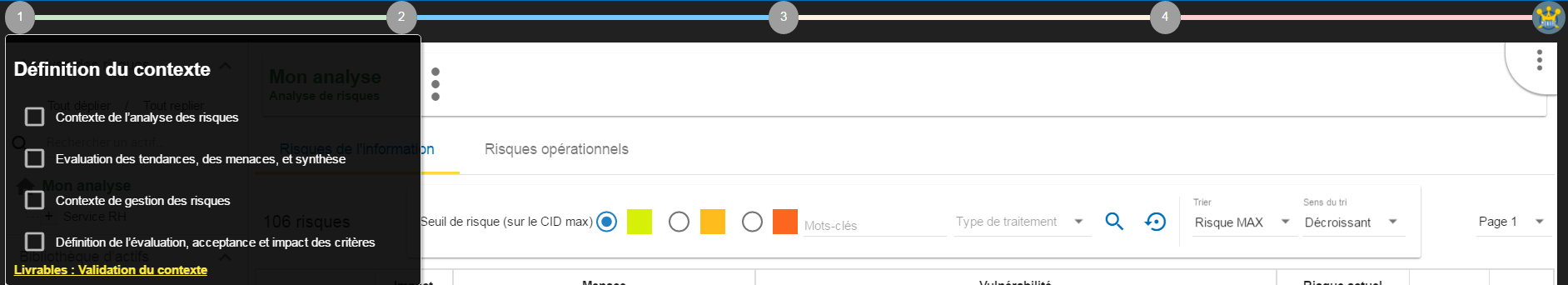
L’accès aux vues des étapes de la méthode se fait en cliquant sur les numéros de 1 à 4 qui se trouvent sous le fil d’Ariane de la vue principale MONARC.

Les processus d’ISO/IEC 27005 sont mis en œuvre à travers les vues.



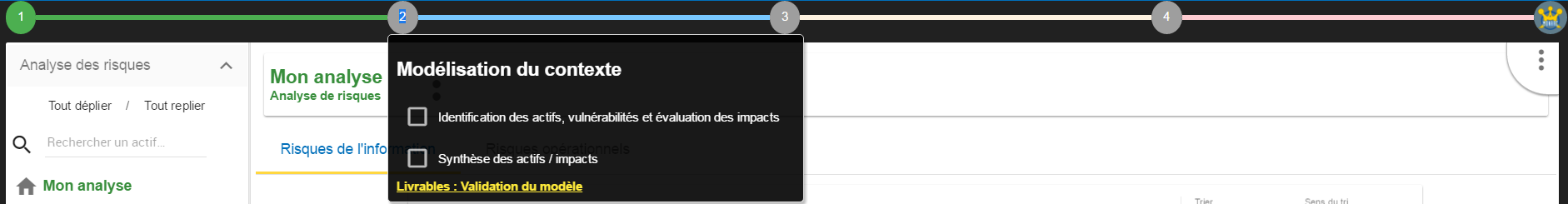
## Définition du contexte d’analyse des risques

En cliquant, sur le chiffre 1, le menu suivant apparaît :

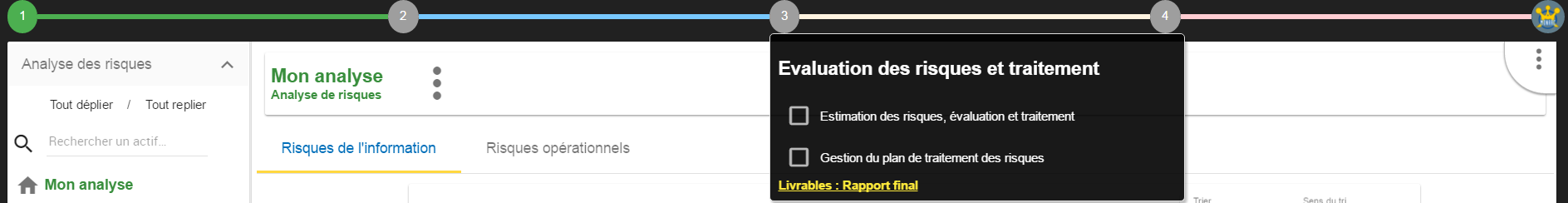


1. Cocher les cases permet de faire évoluer l’état d’avancement de la méthode
2. Cliquer sur le libellé appel le sous-écran contextuel de gestion

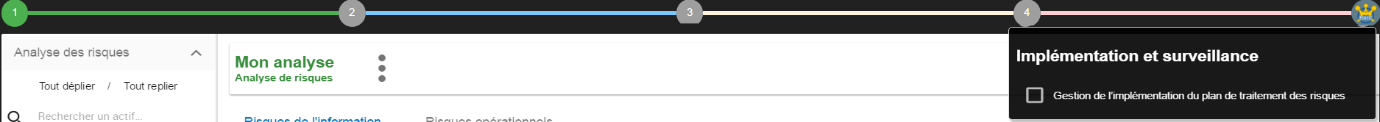
En cliquant, sur le chiffre 2, le menu suivant apparaît :



En cliquant, sur le chiffre 3, le menu suivant apparaît :

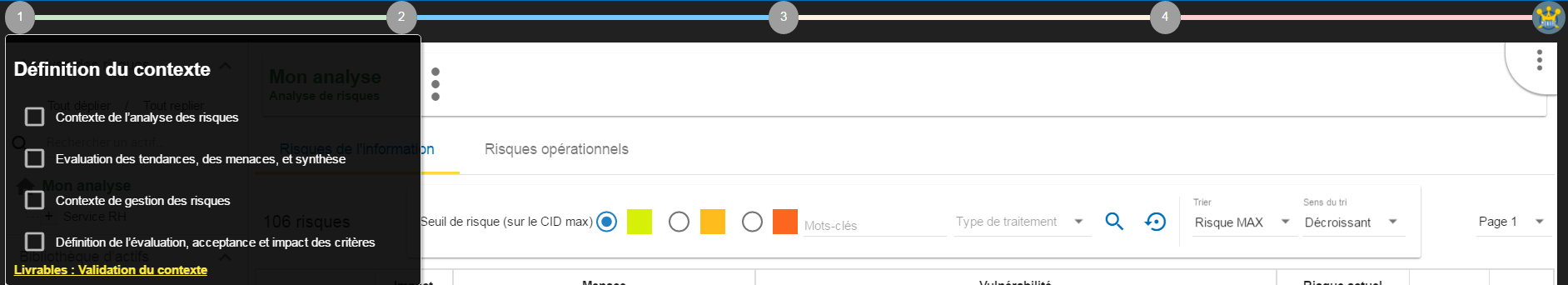


En cliquant, sur le chiffre 4, le menu suivant apparaît :



# Définition du contexte d’analyse des risques

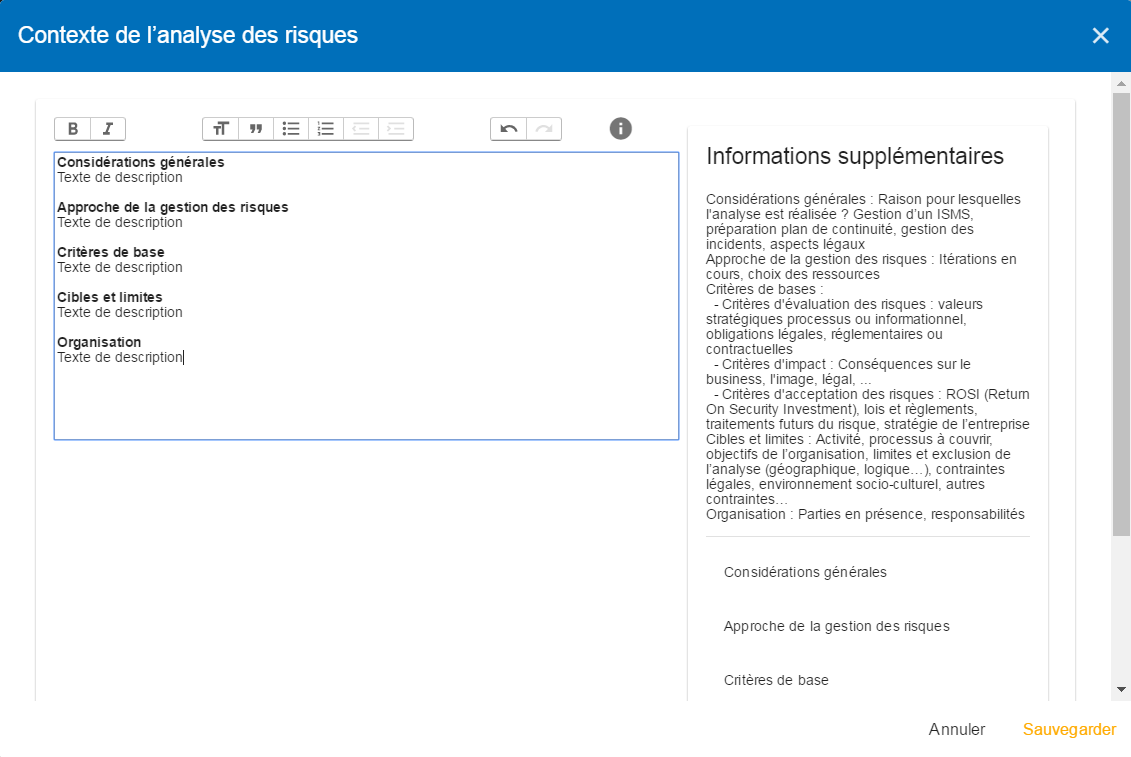
En cliquant, sur le chiffre 1, le menu suivant apparaît :



1. Liens vers les pop-up de gestion contextuels, voir chapitres suivants
2. Cases à cocher, indiquant que l’étape sélectionnée est terminée. Cette information optionnelle sert à montrer l’avancement du projet d’analyse de risques et à afficher le graphique de représentation des risques du tableau de bord.
3. Lien qui permet de générer le livrable de « Validation du contexte ». Dans une mission de consultance par exemple, il peut être utile de le faire valider par le client.

## Contexte de l’analyse des risques

Cette vue offre des fonctionnalités d’encodage et de formatage du texte, permettant ainsi de contextualiser la cible d’analyse des risques avec des textes bien formatés qui seront repris dans les livrables.



1. Accès aux fonctionnalités de formatage du texte (Bold, Italique, paragraphe, taille de texte, etc.). *La qualité de l’encodage conditionne directement la qualité du livrable.*
2. Permet d’afficher ou d’effacer la zone d’aide .
3. Zone d’aide sur le contenu qui est préconisé de saisir (suite voir ci-dessous).
4. Chapitres préconisés par ISO27005. Cliquer sur le libellé le place automatiquement dans la zone de saisie.

**Préconisation sur le contenu**

Les chapitres cités ci-dessous font référence à ISO/IEC 27005 :2011

**Considérations générales :** Voir chapitre 7.1

**Approche de la gestion des risques :** Voir chapitre 7.2.1

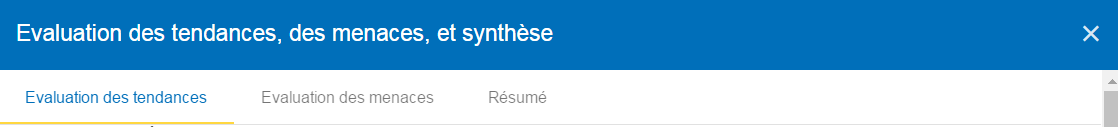
**Critères de base :** Voir chapitres 7.2.2, 7.2.3, 7.2.4

**Cibles et limites :** Voir chapitre 7.3

Ces préconisations ne sont bien entendues qu’indicatives et toute information précisant le contexte est bonne à saisir.

## Evaluation des tendances, des menaces et synthèse

Cette étape est partagée en 3 parties distinctes qui structurent la collecte des données nécessaires pour bien comprendre le contexte à analyser. Il est conseillé d’animer un groupe de 5 à 10 personnes (selon organisme) qui rassemble des membres de la direction, l’informatique, le service de gestion des risques (s’il existe), des chefs de service ou des personnes à fonction clé.



1. Évaluations des tendances : MONARC propose une série de questions qui permettent de découvrir le contexte d’un point de vue très global (suite voir chapitre 3.2.1).
2. Évaluation des menaces : Permet de revoir les menaces de façon très généraliste et éventuellement de les évaluer par défaut dans le futur modèle (suite voir chapitre 3.2.2).
3. Résumé textuel des points importants retenus lors des étapes 1 et 2 (suite voir chapitre 3.2.3).

### Évaluations des tendances

L’évaluation des tendances propose une série de questions qui permettent de découvrir le contexte d’un point de vue très global. Ces questions permettent de mettre le focus sur la sélection des actifs importants qu’il faut considérer dans l’analyse, les critères de sécurités, ainsi que quelques points sur les motifs d’attaque et le contexte extérieur de la cible.

La liste n’est pas exhaustive, des questions de votre choix peuvent être ajoutées en fin de page.

### Évaluations des menaces

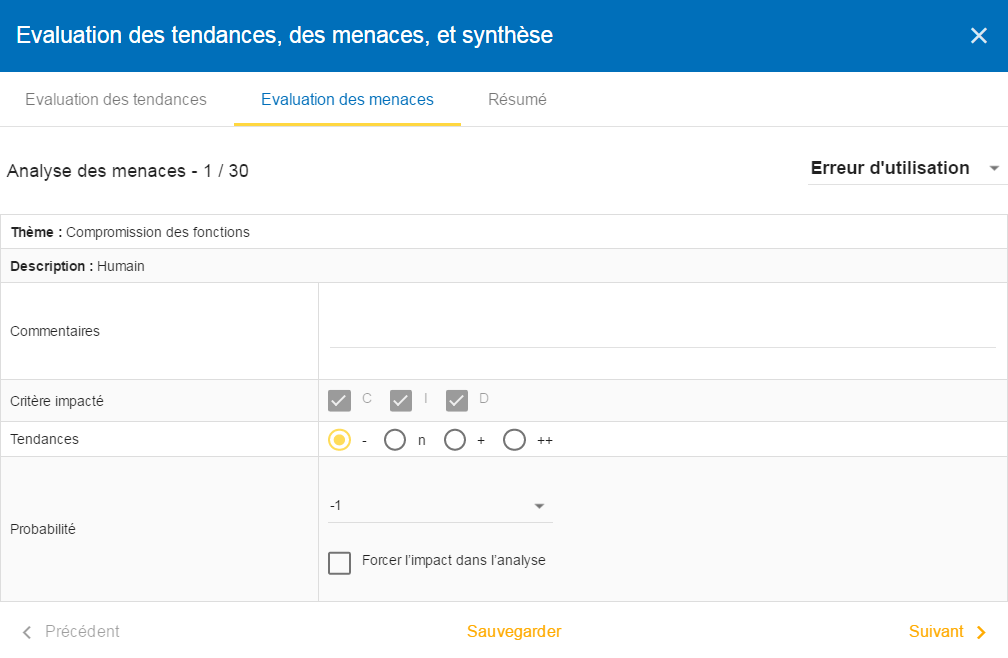
L’évaluation des menaces, tout comme l’évaluation des tendances est un meeting réunissant des personnes clés de l’organisme.

L’objectif est de parcourir la plupart des menaces en collectant l’information sur le passé et les remarques générales qui émanent du groupe.

Le principe c’est d’obtenir un consensus sur la probabilité de la menace sur une échelle facile à interpréter :

* Plutôt moins : Jamais arrivé, vraiment pas probable
* Normal : Pas de position ferme, pas d’avis
* Plutôt + : Déjà arrivé
* Plutôt ++ : Déjà arrivé plusieurs fois

C’est l’expert en sécurité qui transforme le consensus en une valeur de probabilité de 1 à n qui sera utilisée dans le modèle.

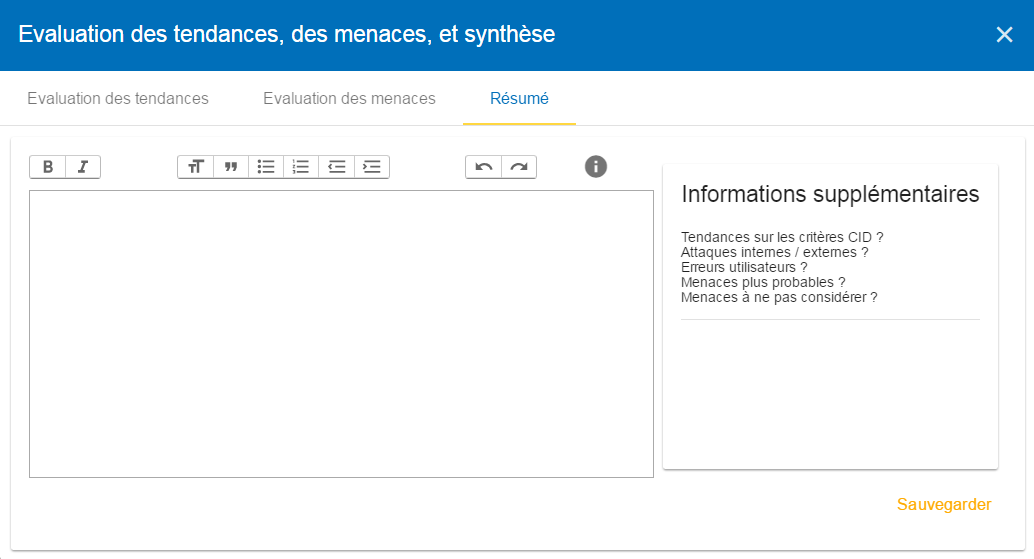


1. Cliquer sur l’onglet « Évaluation des menaces ».
2. Libellé de la menace.
3. Information sur la menace.
4. Commentaire à encoder, collecte de l’information du groupe de personnes.
5. Information sur les critères de sécurité impactés par la menace.
6. Choix de la tendance, obtenu par consensus du groupe.
7. Sélection de la probabilité déduite du point  par l’expert en sécurité.
8. Possibilité par la suite de forcer les menaces du modèle (après qu’il soit construit).
9. Sauvegarde des informations et navigations dans les menaces.

### Résumé des évaluations

Comme pour le contexte d’analyse des risques, cette vue permet de résumer l’information pertinente collectée pendant l’évaluation des tendances et des menaces.

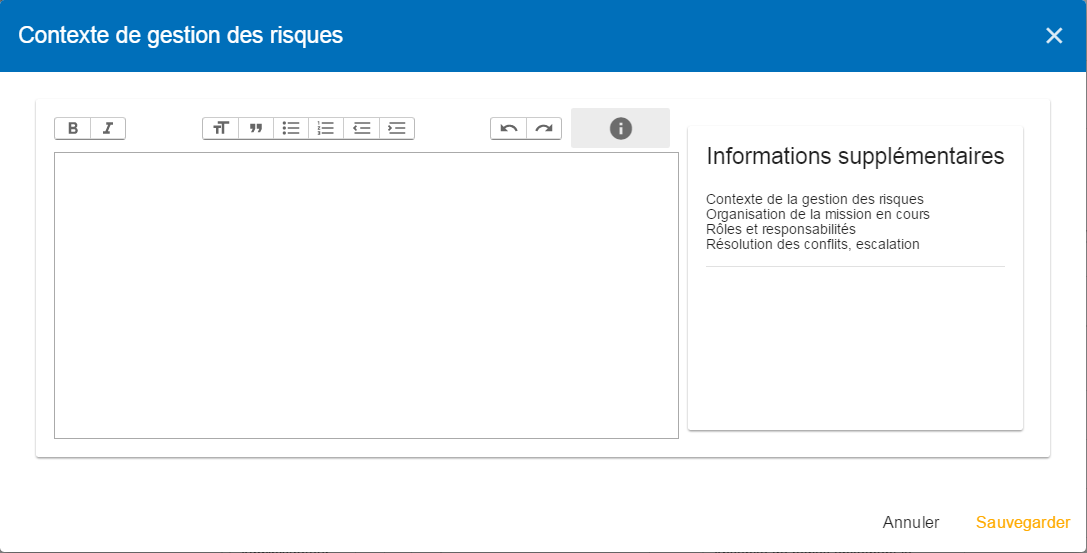
Ce texte permet d’étoffer le livrable.



## Contexte de gestion des risques

Cette vue permet d’encoder les informations sur le contexte de la gestion des risques, par exemple ce qui concerne les rôles et responsabilités, les parties prenantes, etc.

Pour plus d’information, se référer au chapitre 7.4, d’ISO/IEC 27005 :2011



## Définition des critères d'évaluation, d'acceptation et d'impact

Il s’agit ici de personnaliser toutes les échelles et critères d’impact et de conséquence.

MONARC propose des valeurs par défaut qui peuvent être personnalisées au contexte. 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.

### Échelle d’impacts



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).

Par défaut, l’échelle d’impact et de conséquence reprend les critères suivants :

* C : Confidentialité
* I : Intégrité
* D : Disponibilité
* R : Réputation
* O : Opération
* L : Légal
* F : Financier
* P : Personne (impact à la)

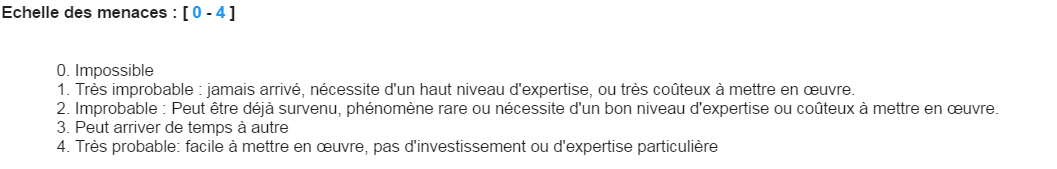
Il est possible d’ajouter des conséquences personnalisées, mais pas de critères d’impact.

Les mêmes échelles sont utilisées pour traiter les risques de l’information et les risques opérationnels, il y a juste une différence d’interprétation. :

* Les risques de l’information sont évalués sur les critères CID en prenant en compte les conséquences ROLFP.
* Les risques opérationnels sont directement évalués sur les critères ROLFP

### Échelles des menaces

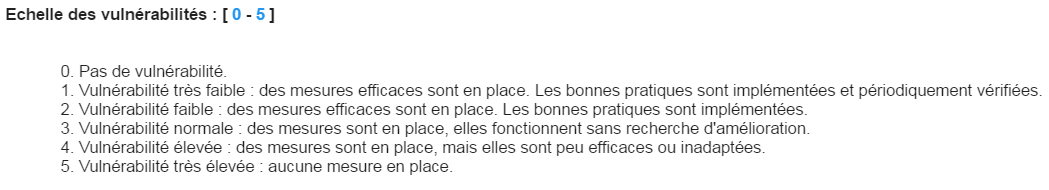
L’échelle des menaces est utilisée que pour calculer les risques de l’information et les probabilités de scénarios des risques opérationnels



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

### Gestion des vulnérabilités

L’échelle des vulnérabilités n’est utilisée que pour calculer les risques de l’information.



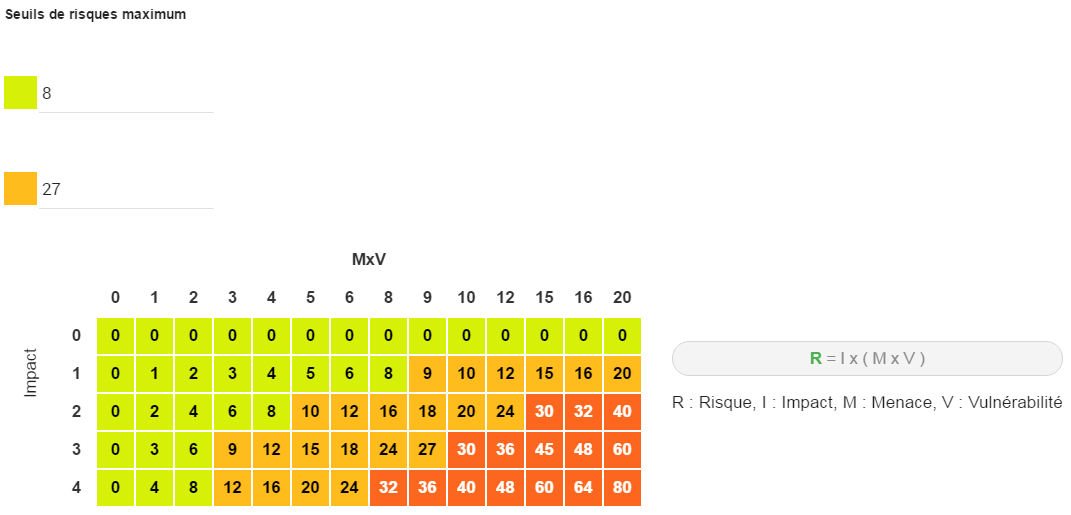
1. Cliquer pour modifier le nombre d’échelons
2. Cliquer pour éditer les libellés de chaque échelon (Gestion idem échelle impact).

### Gestion des seuils d’acceptation

Il existe deux tables distinctes pour les seuils d’acceptation, parce que les risques opérationnels et les risques de l’information ne sont pas calculés sur les mêmes critères.

Pour les risques de l’information, le calcul est fait sur 3 critères :

 (Impact x Menace x Vulnérabilité)

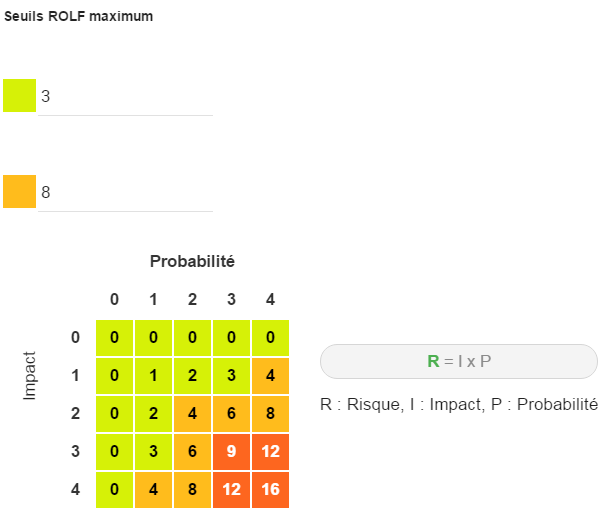


Pour les risques opérationnels le calcul est fait sur 2 critères :

 (Impact x Probabilité)

La « Probabilité » utilise l’échelle de menace, c’est en réalité la vraisemblance du scénario exprimé par le risque.

 :



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.

## Livrable : Validation du contexte

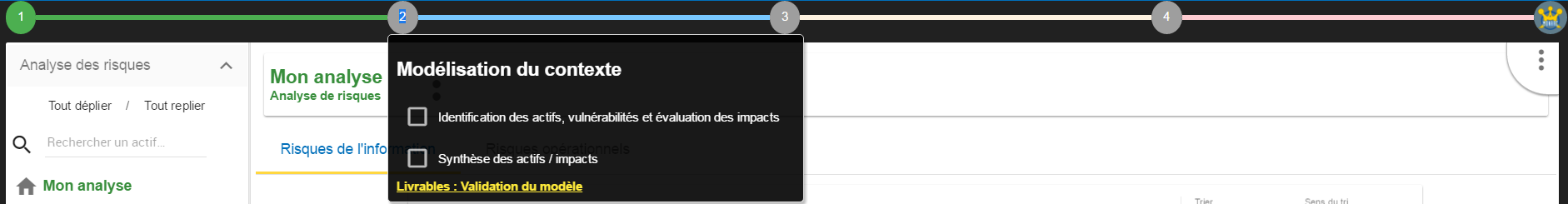
Ce livrable reprend toutes les informations collectées et saisies lors de la phase d’établissement du contexte. Il peut être utilisé pour valider les informations par le client, avant de commencer l’identification des risques.

Un formulaire est à remplir. Lorsque l’on clique sur « Sauvegarde », un fichier au format Word est généré.



# Modélisation du contexte

En cliquant, sur le chiffre 2, le menu suivant apparaît :



## Identification des actifs, vulnérabilités

Le clique sur le lien appelle la vue principale de MONARC.

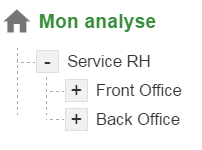
L’objectif est de créer le modèle de risques à partir des actifs de la bibliothèque.

Le principe de modélisation propose de placer sur la racine de l’analyse les actifs primaires, puis de placer en dessous les actifs de support qui les composent.

La phase d’établissement du contexte a permis de découvrir les actifs primaires qui vont faire l’objet de l’analyse. Il est déjà possible qu’à ce stade de l’analyse, certains actifs secondaires soient déjà connus.

Par défaut, MONARC propose une structuration « Front Office », « Back office », mais ce n’est pas une obligation. Il est important que la construction du modèle suive une logique contextuelle, les actifs et termes cités doivent utiliser la terminologie de l’organisme, et pour ce faire, il ne faut pas hésiter à renommer les actifs proposés par défaut de la bibliothèque.

**Principe de la structuration « Front Office », « Back office »**



* Le « Front Office » représente le côté « utilisateur », par exemple dans le cas d’un service « Ressources Humaines » nous allons y trouver les employés et l’ensemble du système d’information qui leur est accessible (Bureau, poste de travail, matériels divers, logiciel, personnes, etc.).
* Le « Back Office » représente le côté informatique et organisationnel de l’organisme qui sont communs (bâtiment, data centre, réseau, administrateurs, règles communes, etc.).

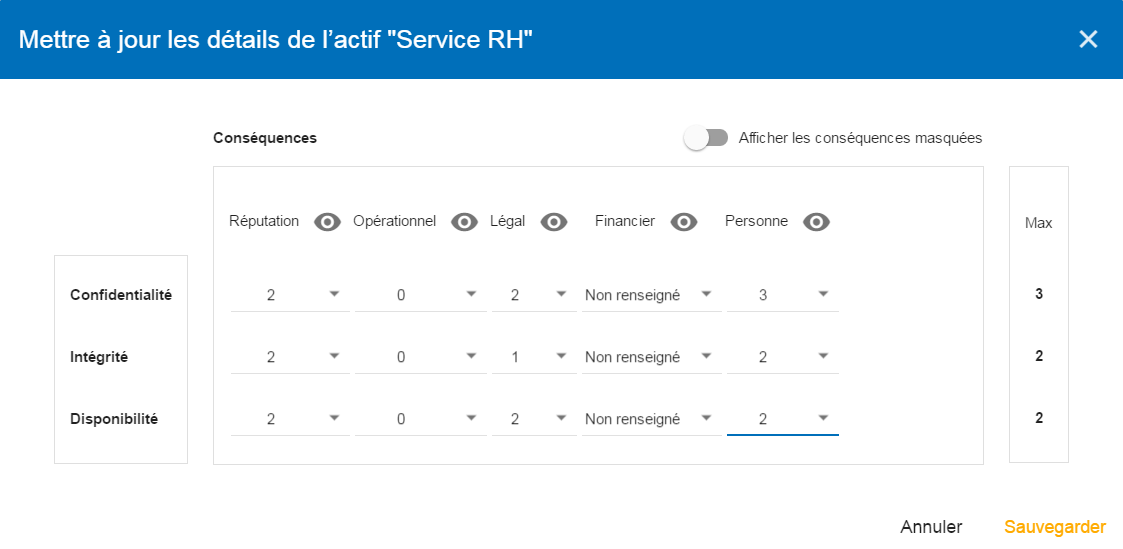
## Évaluation des impacts et conséquences

Il faut définir pour chaque actif primaire les impacts et conséquences qui pourraient s’appliquer, si les risques présents dans le modèle se réalisaient. Par défaut, tous les actifs de supports vont hériter de ces impacts, mais il est toujours possible de les redéfinir.

Lorsque l’actif primaire est un service, alors, le C (Confidentialité) et le I (Intégrité) concernent l’information la plus sensible de ce service. Le D (Disponibilité) concerne le service et l’information, en partant du principe que si l’information est indisponible, le service l’est également.

Lorsque l’actif primaire est l’information, il n’y a pas d’ambiguïté sur les critères CID, ils concernent tous l’information.

Dans certains cas plus rares, si le « C » associé à un service exprime la confidentialité du mode opératoire (ex. procédé de fabrication), il suffit d’exprimer distinctement les actifs dans le modèle en un actif informationnel et un service.

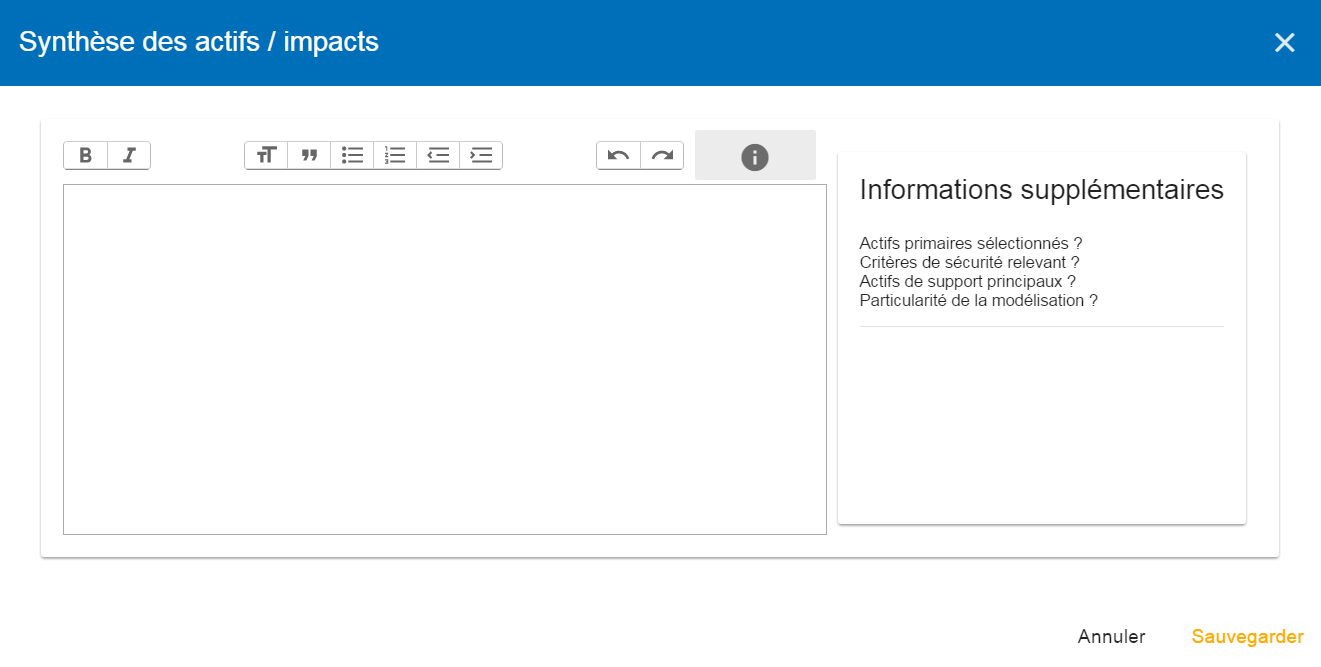


La valeur des critères CID est déduite automatiquement en fonction des conséquences ROLFP ou autres qui leur ont été associés (valeur maximum).

Exemple : Dans le cas de la figure ci-dessus, le « 3 » d’impact sur la confidentialité, s’explique par la valeur maximum ROLFP concernant la confidentialité qui est dans ce cas « 3 » en conséquence pour la personne.

## Synthèse des actifs / impacts

La synthèse des actifs permet de fournir un contenu rédactionnel qui justifie le choix des actifs et des impacts à destination du livrable.



## Livrable : Validation du contexte

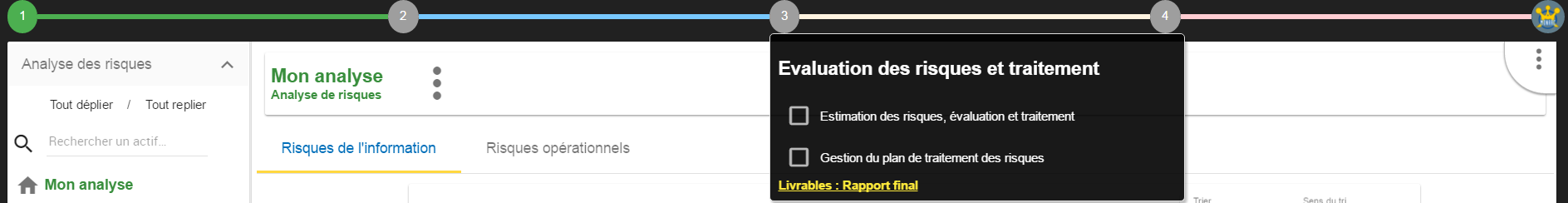
Ce livrable reprend tous les actifs primaires importants du modèle, c’est-à-dire ceux sur lesquels des impacts sont renseignés, ainsi que la synthèse des actifs.

Un formulaire est à remplir. Lorsque l’on clique sur « Sauvegarde », un fichier au format Word est généré.



# Évaluation et traitement des risques

En cliquant, sur le chiffre 3, le menu suivant apparaît :



Le clique sur le lien appelle la vue principale de MONARC.

## Évaluation et traitement des risques

La phase précédente a permis de renseigner les critères d’impacts, il reste maintenant à évaluer les menaces et les vulnérabilités pour pouvoir calculer les niveaux de risques.

### Évaluation des probabilités de menaces

Dans le cas où l’évaluation des menaces faite pendant l’établissement du contexte a renseigné des probabilités, il faut revenir à cet écran pour forcer toutes les menaces du modèle.

Ensuite, lors du passage en revue des risques du modèle, les valeurs par défaut peuvent toutes être révisées unitairement.

### Évaluation des vulnérabilités

Les niveaux de vulnérabilités dépendent directement des mesures de sécurité en place. Afin de justifier chaque valeur, il est nécessaire de décrire de façon factuelle toutes ces mesures.

### Traitement des risques

Le traitement des risques dans MONARC consiste comme dans ISO/IEC 27005, à prendre une décision de type de traitement et non pas d’implémenter la mesure.

Il existe 4 façons pour traiter un risque :

1. Accepter : Le risque est accepté tel quel. Aucune action supplémentaire ne sera lancée.
2. Modifier / Réduire : Des mesures sont mises en place pour réduire le risque à un niveau acceptable. La force de réduction est alors évaluée afin de pouvoir calculer le risque résiduel.
3. Partager / Refuser : cas des assurances par exemple. Ce type de traitement est particulier, parce qu’il tend à réduire l’impact du risque et non pas la vulnérabilité. Le risque résiduel ne peut pas être calculé.
4. Refuser : La cause du risque est éliminée, après traitement le risque ne doit plus exister.

## Gestion du plan de traitement

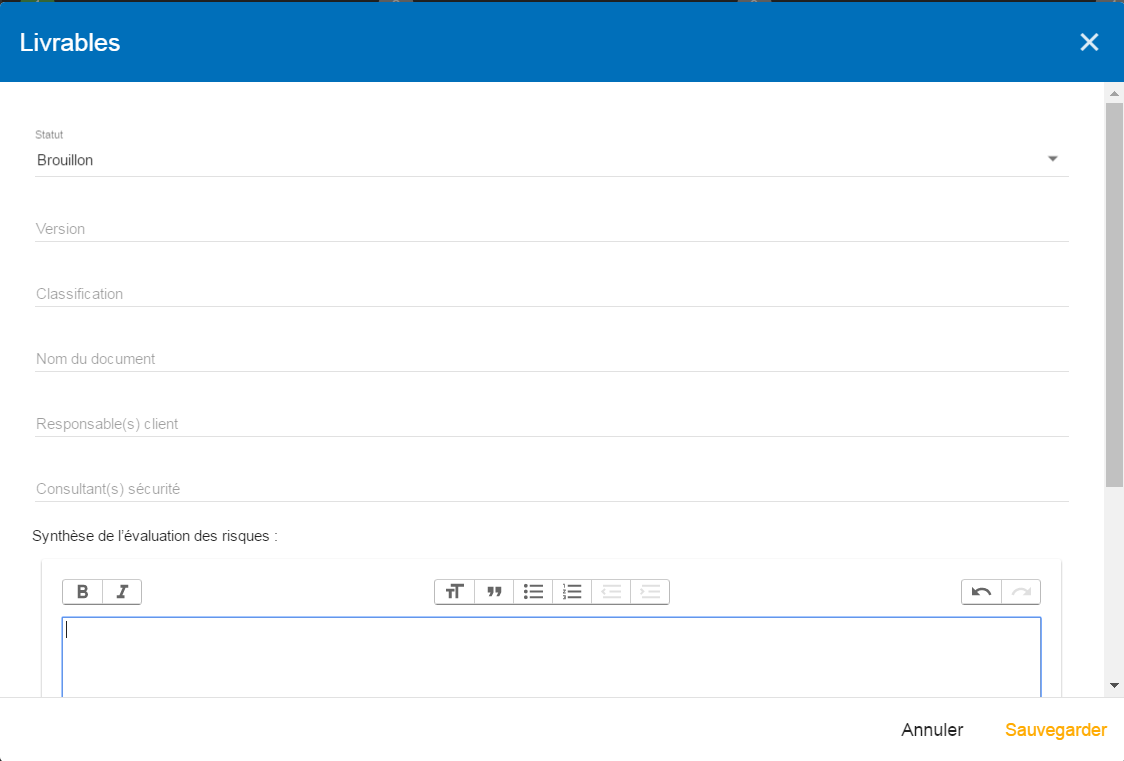
Tous les risques faisant l’objet d’un des 4 traitements décrits ci-dessus sont inscrits dans le plan de traitement des risques, que ce soit les risques de l’information ou les risques opérationnels.

La formule de calcul n’est pas la même pour les deux types de risques, c’est donc les seuils d’acceptation des risques qui donne l’ordre des risques. Toutefois, il est possible de réordonner l’ordre du plan de traitement des risques avant de générer le livrable final.

## Livrable : Rapport final

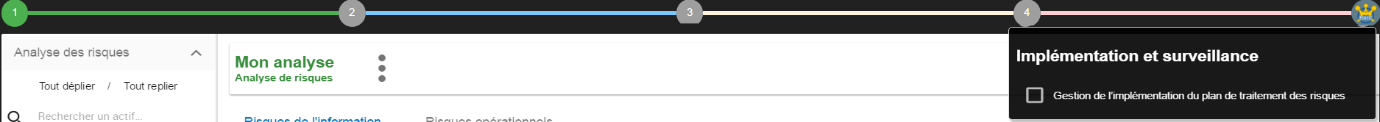
Le livrable reprend de façon exhaustive toutes les informations collectées et saisies dans MONARC, y compris les informations contenues dans les deux précédents livrables.

Un formulaire est à remplir. Il est possible d’y ajouter un résumé de l’analyse qui s’ajoute aux 5 premiers risques du plan de traitement. Lorsque l’on clique sur « Sauvegarde », un fichier au format Word est généré.



# Implémentation et surveillance

En cliquant, sur le chiffre 4, 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.

Le séquencement des actions est le suivant :

* Un responsable et un délai sont définis pour chaque recommandation.
* Lorsque la recommandation a été complètement implémentée, une validation est demandée pour chaque risque traité par la recommandation en question.
* Pour chaque risque, le nouvel état est documenté et les valeurs de risques résiduels deviennent le risque actuel.

Et ainsi de suite pour chaque recommandation.