LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

Guide utilisateurs – Réalisation d'une analyse de risques avec l'outil MONARC

HCPN/ANSSI

11 juillet 2025: Version 1.2

Table des matières

1 Introduction

1.1 Objectif

Ce guide a pour objectif d'accompagner les utilisateurs dans la réalisation d'une analyse de risques, à travers les différentes phases prévues par l'outil MONARC. Il s'adresse principalement aux ministères, administrations et services de l'État.

Il s'appuie sur une méthodologie de gestion des risques et un modèle qui comprend une bibliothèque d'actifs, définis afin de permettre aux entités de l'Etat de réaliser une analyse de risques comprenant les éléments appropriés et proportionnés à leurs enjeux de sécurité.

1.2 Terminologies

Nom	Définition
SI (Système d'Information)	Composé de l'ensemble des ressources organisées pour permettre la collecte, le stockage, le traitement et la distribution de l'information quelle que soit la forme sous laquelle elle est exploitée (ex : électronique, imprimée, etc.). Cela inclut les moyens humains, techniques et organisationnels.
Conformité	Respect des lois, réglementations, directives et spécifications pertinentes pour l'entité, telles que le RGPD (Règlement Général sur la Protection des Données), NIS2, etc.
NIS2	Directive européenne visant à assurer un niveau commun élevé de cybersécurité des réseaux et des systèmes d'information en Europe et à renforcer la résilience des infrastructures informatiques face aux cyberattaques. Elle établit des mesures pour la gestion des risques de cybersécurité et la notification des incidents, ainsi que des règles sur la coopération, le partage d'informations, la supervision et l'application de la loi.
Menace	Cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme.
Vulnérabilité	Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.
Risque	Perte, dommage ou destruction potentielle d'un actif par suite de l'exploitation d'une vulnérabilité par une menace.
Risque résiduel	Risque subsistant après le traitement du risque.
Mesure de sécurité	Un contrôle de sécurité permettant d'atténuer les risques en réduisant les vulnérabilités. Elle assure la protection des actifs.
Impact	La conséquence ou l'effet d'un événement se produisant, impactant la confidentialité des données, l'intégrité des données, la disponibilité des données, la réputation, la performance opérationnelle, etc. d'une entité.
Confidentialité	Propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés.
Intégrité	Propriété d'exactitude et de complétude.
Disponibilité	Propriété d'être accessible et utilisable à la demande par une entité autorisée.

SERIMA (Security Risk MAnagement)	Une plateforme mise à disposition par l'ILR permettant, entre autres fonctionnalités, de réaliser des analyses de risques standardisées.
ILR (Institut Luxembourgeois de Régulation)	L'autorité chargée de la régulation économique des réseaux et services de communications électroniques, du transport et la distribution d'électricité et de gaz, des services postaux, du réseau ferroviaire et des redevances aéroportuaires. Autorité compétente entre autres en charge de la supervision des entités concernées par la directive NIS2 de tous les secteurs sauf le secteur bancaire et les infrastructures de marchés financiers.

1.3 Public ciblé

Le présent guide s'adresse principalement aux entités de l'État, ainsi qu'à toute autre partie prenante impliquée dans la gestion et la réalisation des analyses de risques de sécurité de l'information. Ce guide a été conçu pour tous les utilisateurs de tous niveaux de maîtrise en analyse de risques.

1.4 Contexte et objectifs

L'objectif principal de ce guide est de faciliter l'identification des risques de sécurité de l'information potentiels auxquels une entité est exposée. Cela permettra de définir les mesures de sécurité appropriées pour les atténuer et d'optimiser l'approche de la gestion des risques.

La directive NIS 2 impose des exigences plus strictes en matière de gestion des risques de sécurité de l'information, et de réponse aux incidents de cybersécurité.

En particulier, elle met l'accent sur **une évaluation systématique des risques et des mesures de sécurité appropriées :** les entités devront démontrer qu'elles disposent d'une méthodologie robuste pour identifier, évaluer et gérer les risques liés à la sécurité de l'information.

1.5 Prérequis

Pour que les entités puissent se familiariser avec les fonctionnalités de la plateforme MONARC, il est recommandé de suivre les sessions de formation organisées par le LHC et l'ILR.

Le LHC met à disposition des ressources pour les sessions de formation passées et un lien vers les formations à venir. Pour plus d'informations, il est recommandé de consulter MONARC trainings (lhc.lu). Un guide d'utilisation est par ailleurs mis à disposition des utilisateurs de la plateforme MONARC. Il est conseillé de le consulter en cliquant sur 'User Guide (MONARC.lu)'.

Par ailleurs, les formations organisées par l'ILR sont également annoncées sur leur site.

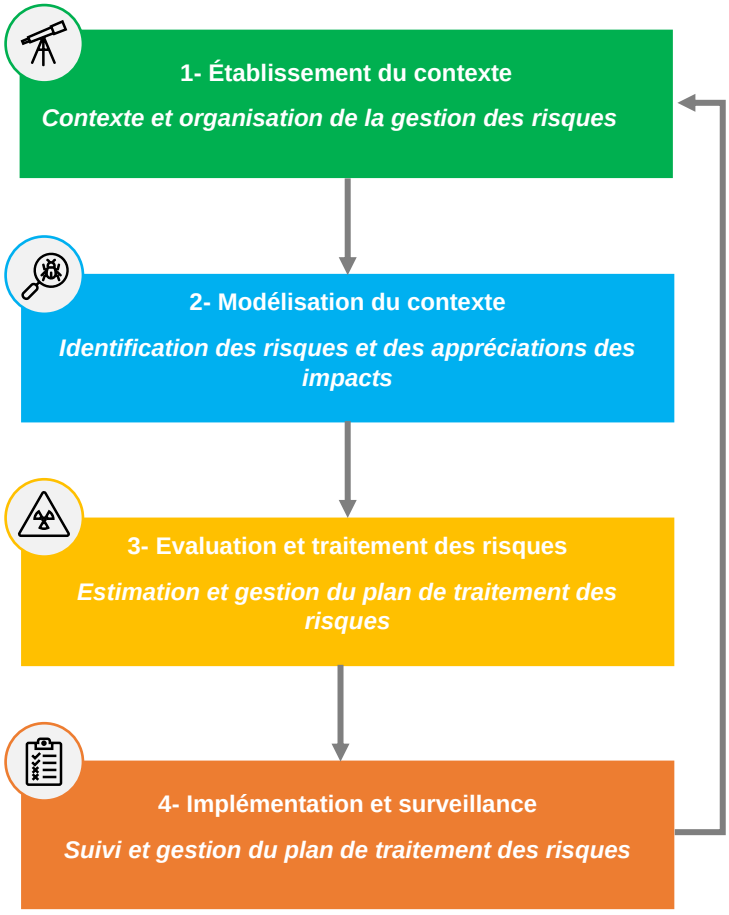
1.6 Support et contact HCPN/ANSSI

Pour toute demande d'assistance et de support concernant l'utilisation de l'outil MONARC et les différentes catégories du modèle défini, il est recommandé de contacter le HCPN/ANSSI, par exemple par courriel en utilisant l'adresse info@anssi.etat.lu.

2 Guide de gestion de risques HCPN

2.1 Méthodologie d'analyse de risques MONARC

MONARC est basé sur une méthodologie d'analyse de risques avec plusieurs phases clés, permettant d'identifier, d'évaluer et de traiter les risques, comme indiqué ci-dessous :



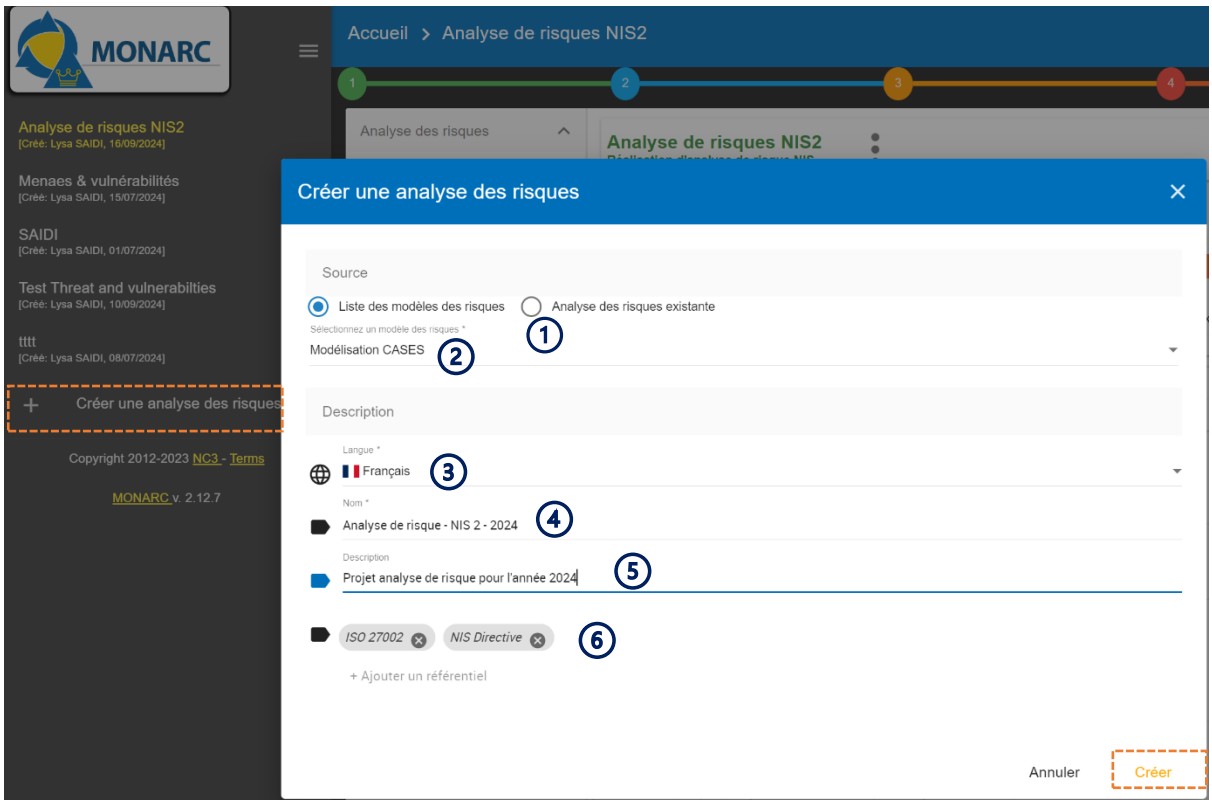
Méthodologie analyse de risques MONARC

Avant de procéder à la réalisation de l'analyse de risques, il est nécessaire de créer un projet sur MONARC, en suivant les étapes suivantes :

- Pour commencer, il suffit de choisir l'option "Ajouter une nouvelle analyse de risques".
- Une nouvelle fenêtre permettant la création d'un projet d'analyse de risques s'affiche. Afin de le créer, il est nécessaire de préciser :
    1. La source de l'analyse de risques, basée sur un modèle existant, avec deux options possibles :
        - ✓ Utiliser les modèles définis (par le HCPN/ANSSI) dans la base de connaissance MONARC.
        - ✓ Utiliser une analyse de risques préalablement réalisée dans l'outil MONARC, permettant ainsi sa duplication.
    2. Le choix du modèle recommandé est celui défini par le "HCPN/ANSSI" dont le nom est "Modélisation HCPN-ANSSI ".
    3. Le choix de la langue de l'analyse de risques parmi le français et l'anglais.

4. L'attribution d'un nom à l'analyse de risques à réaliser.
5. L'ajout d'une description de l'analyse de risques.
6. Le choix des référentiels de sécurité qui peuvent être utilisés lors de la définition d'un plan d'action pour le traitement des risques.

Lors de la création du projet, il est fortement recommandé de sélectionner les référentiels de sécurité ISO 27002. Cela permettra de définir des recommandations aux risques qui seront identifiés plus facilement.



Une fois ces étapes effectuées, il suffit de cliquer sur "Créer" pour que le projet soit créé.

Figure 1: création projet analyse de risques

***Les étapes 5 et 6* sont optionnelles**, mais il est recommandé de les compléter lors de la création du projet d'analyse de risque.

2.2 Description des phases analyse de risques

2.2.1 Phase 1 : établissement du contexte

La phase d'établissement du contexte est une étape essentielle lors d'une analyse de risques, comme elle permet d'identifier son contexte et ses objectifs.

2.2.1.1 Contexte de l'analyse des risques

Cette étape permet la description du contexte de l'analyse de risques et le cadre dans lequel elle sera réalisée, en tenant compte de plusieurs éléments clés permettant d'assurer son alignement avec les besoins et les objectifs de chacune des entités, tels que :

- Les raisons pour lesquelles elle est effectuée (ex : conformité, sécurité, etc.).
- L'approche choisie (nombre d'itérations, ressources allouées au projet comme les équipes ou outils, etc.) et méthodologies choisies).
- Les objectifs et les limites du projet (ex : contraintes légales, limites budgétaires, processus ou systèmes à couvrir dans l'évaluation, etc.).

Dans MONARC, cette étape peut être effectuée en cliquant sur "***Contexte de l'analyse des risques***" qui apparaît lorsque la phase "**1**" est sélectionnée, comme montré ci-dessous :

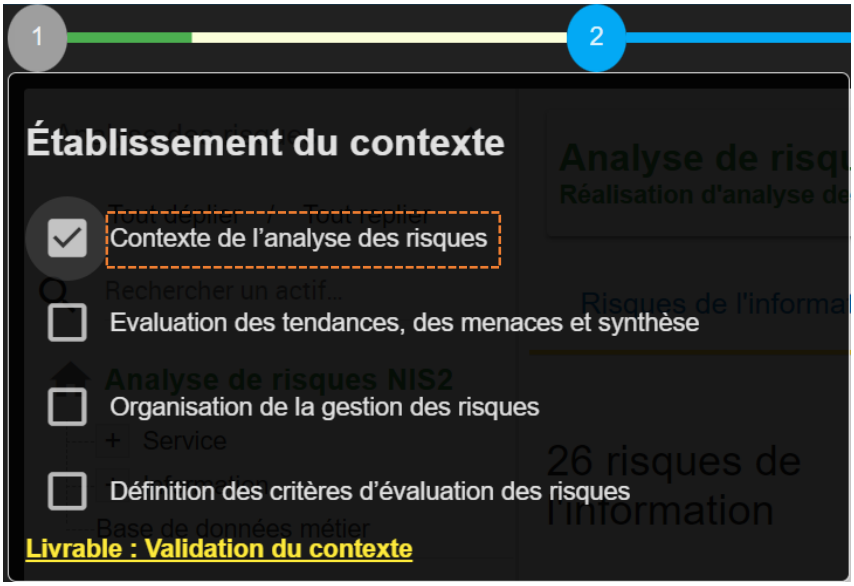


Figure 2: étape définition contexte analyse de risques MONARC

2.2.1.2 Définition des critères d'évaluation des risques

La phase d'établissement de contexte permet également de définir les critères d'évaluation des risques en fixant les échelles pour les impacts CIA (Confidentialité, intégrité et disponibilité) et les conséquences, les menaces et vulnérabilités, ainsi que le seuil d'acceptation des risques.

Dans MONARC, cette étape sera complétée en cliquant sur "**Définition des critères d'évaluation des risques**" qui apparaît lorsque la phase "**1**" est sélectionnée, comme montré ci-dessous :

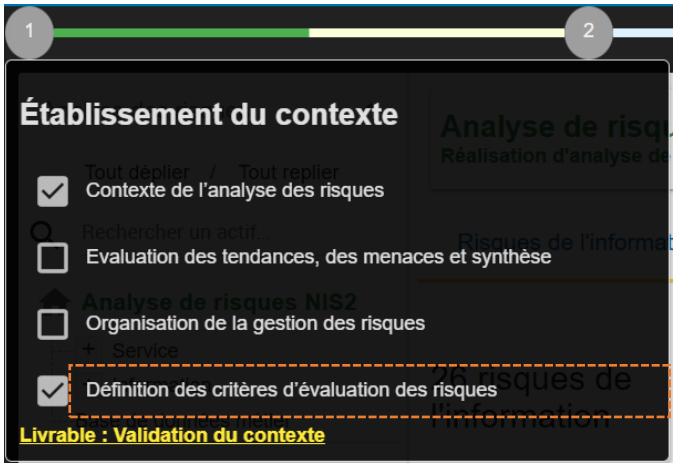


Figure 3: étape définition des critères d'évaluation des risques MONARC

Les critères d'évaluation des risques préalablement définis ne devraient pas être changés ou modifiés lors de la réalisation de l'analyse de risques.

Pour les Tips concernant la phase 1 de cette méthodologie, il est recommandé de faire référence à la section « ***Tips/FAQ – Tips établissement contexte*** » de ce guide utilisateur.

2.2.1.3 Evaluation des tendances, des menaces et synthèse

Cette étape consiste à l'évaluation des tendances et des menaces, en tenant compte d'un certain nombre de facteurs. Parmi ces éléments figurent les actifs, les processus métiers critiques, les réglementations auxquelles l'entité est soumise, incidents et cyberattaques passées, etc.

- **Evaluation des tendances**

Afin d'évaluer les tendances, un ensemble de questions est préalablement établi. Il suffit de répondre à celles qui semblent pertinentes et utiles pour l'analyse de risques.

Si des questions ne figurent pas dans la liste proposée, il est alors possible d'ajouter d'autres en cliquant sur « **Ajouter une question** » qui apparait en bas de la fenêtre, comme indiqué ci-dessous :

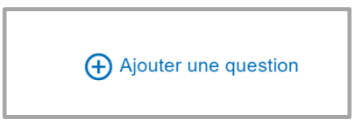


Figure 4: évaluation des tendances

➢ ***Evaluation des menaces***

Cette étape permet d'évaluer la tendance de toutes les menaces définies dans la base de connaissance MONARC pour le modèle défini par le HCPN et sélectionné lors de la création du projet d'analyse de risques.

Pour évaluer toutes les menaces, il suffit de cliquer sur « Sauvegarder » ou sur « Suivant » pour sauvegarder et passer aux menaces suivantes.

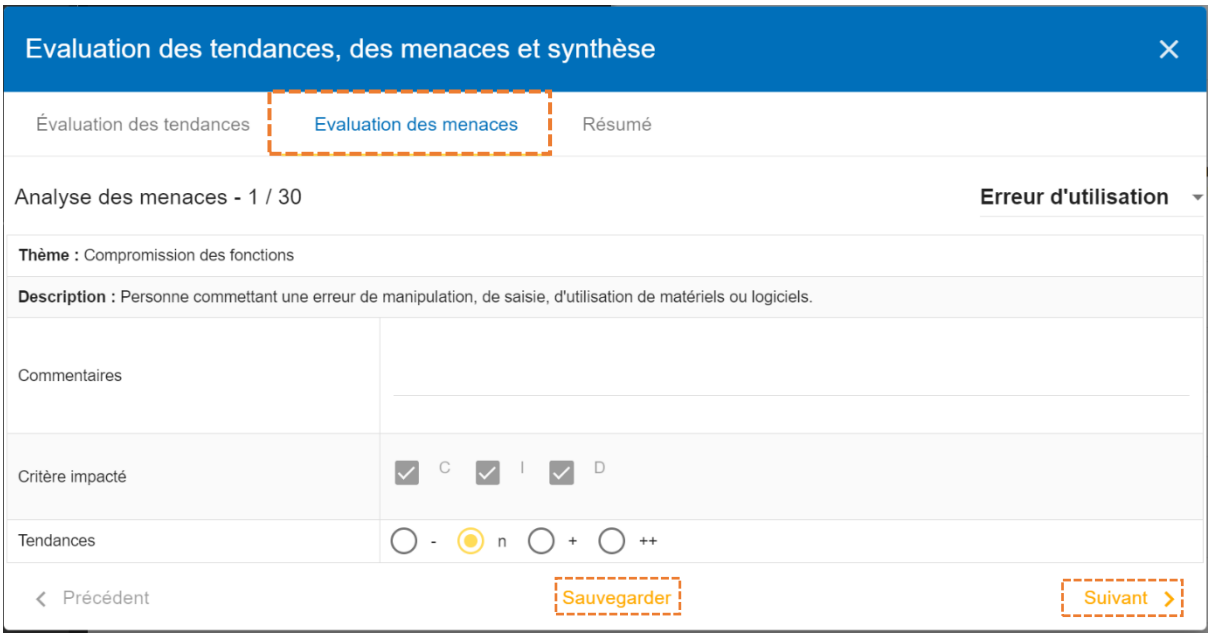


Figure 5: évaluation des menaces

Pour réaliser l'étape en cours, il convient de cocher "**Définition des critères d'évaluation des risques**", afin de pouvoir estimer correctement les probabilités.

➢ ***Synthèse***

Une fois l'évaluation des tendances et des menaces effectuées, un résumé peut être établi, incluant des informations pertinentes telles que les attaques internes/externes, les erreurs des utilisateurs, les menaces les plus probables, les menaces à ne pas considérer, etc.

Dans MONARC, l'ensemble de ces étapes peuvent être effectuées en cliquant sur "**Evaluation des tendances, des menaces et synthèse**" qui apparaît lorsque la phase "**1**" est sélectionnée, comme montré ci-dessous :

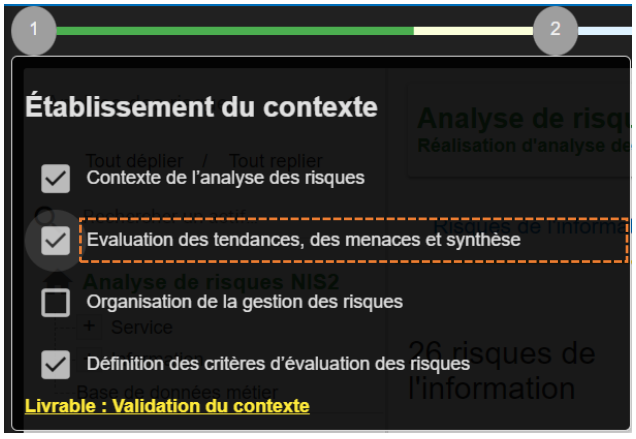


Figure 6: étape évaluation des tendances, des menaces et synthèse MONARC

2.2.1.4 Organisation de la gestion des risques

Cette étape prévoit la description des rôles et responsabilités des différentes parties impliquées dans la réalisation de l'analyse de risques, ainsi que l'organisation de la mission en cours, afin d'assurer une séparation des tâches efficace. Une fois la description est complétée, il suffit de la sauvegarder.

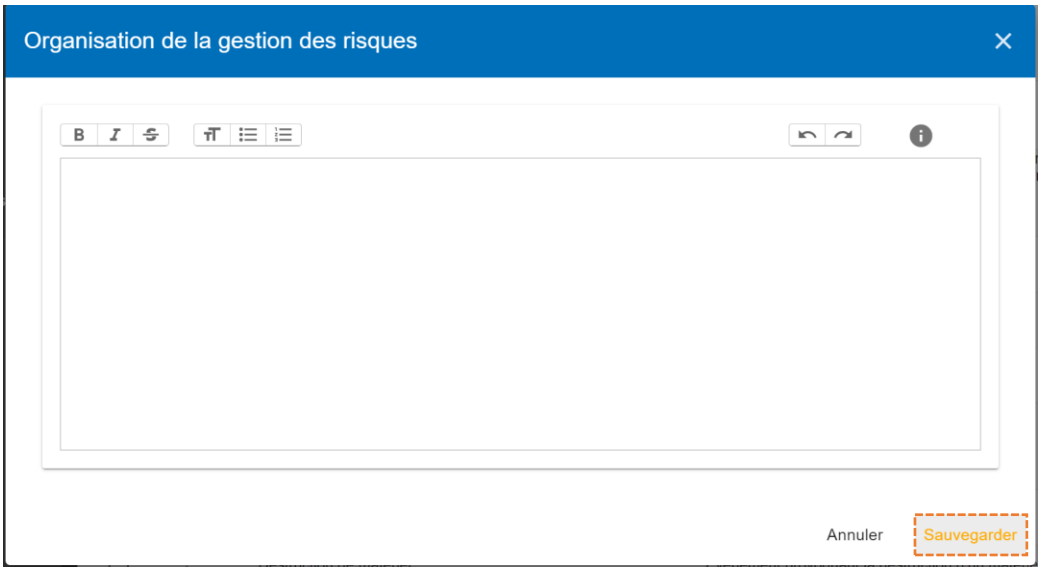


Figure 7: description organisation de la gestion des risques MONARC

Dans MONARC, cette étape sera complétée en cliquant sur "**organisation de la gestion des risques**" qui apparaît lorsque la phase "**1**" est sélectionnée, comme montré ci-dessous :

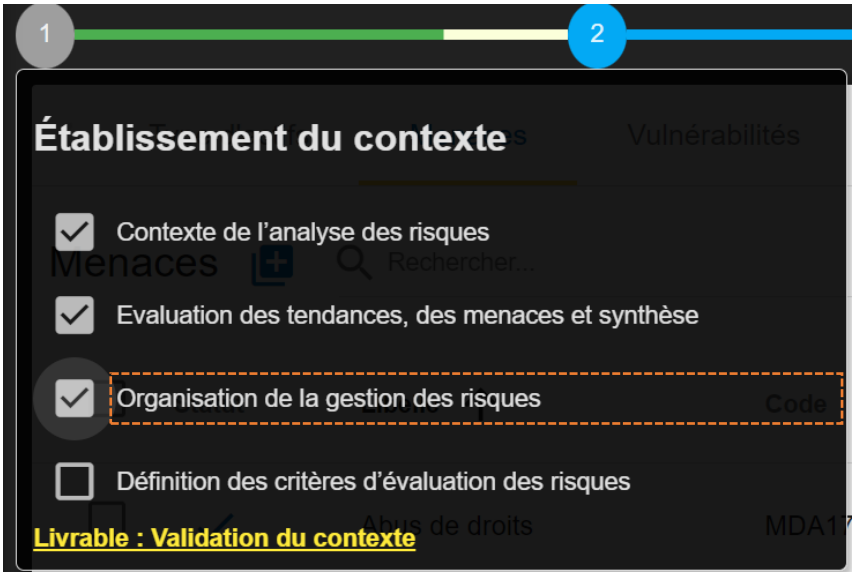


Figure 8: étape organisation de la gestion des risques MONARC

2.2.2 Phase 2 : Modélisation du contexte

L'identification des risques est une phase fondamentale lors de l'analyse de risques, elle se décline en plusieurs étapes, détaillées dans ce qui suit :

2.2.2.1 Identification des actifs, des vulnérabilités et appréciation des impacts

Identification des actifs

Pour identifier les risques de chaque entité de l'État, il est important de définir en premier lieu les actifs essentiels pour l'entité, qu'ils soient matériels (ex : serveurs, équipements informatiques, réseau et infrastructure, etc.) ou immatériels (ex : données, processus et procédures, etc.). Il existe deux types d'actifs :

- Actif primaire : c'est l'ensemble des services, processus internes ou les informations de l'entité. Ils représentent la base de l'analyse des risques et leur impact sera hérité par les actifs sur lesquels ils s'appuient.

  Trois actifs primaires sont définis dans la plateforme MONARC, ces actifs devraient être utilisés et considérés lors d'identification des actifs.

Figure 9: Actifs primaires définis dans MONARC

S'il est nécessaire d'avoir différents actifs primaires du même type***, il est possible de dupliquer l'actif en question autant de fois que nécessaire, puis les renommer selon les besoins.*** Il suffit ensuite de faire glisser les actifs vers l'analyse de risques créée, comme indiqué ci-dessous :

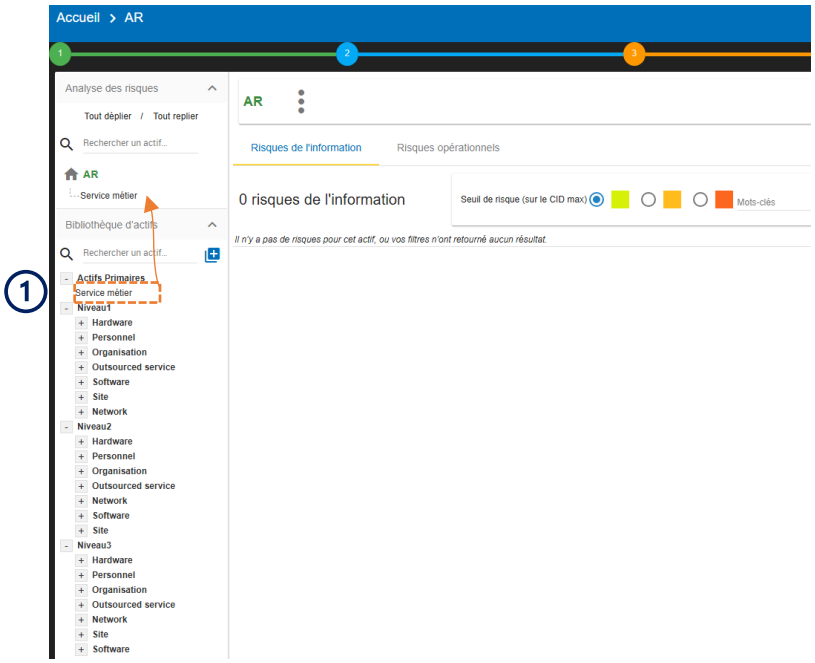


Figure 10: ajout d'un actif au projet d'analyse de risques

Étapes duplication d'un actif

Afin de le dupliquer un actif dans la plateforme MONARC, il est recommandé de suivre les étapes suivantes :

- D'abord, il convient de le sélectionner l'actif à dupliquer, une fois les informations connexes affichées, il suffit de cliquer sur les trois points situés en haut à gauche pour afficher la liste des actions qui peuvent être effectuées sur l'actif, comme indiqué ci-dessous :

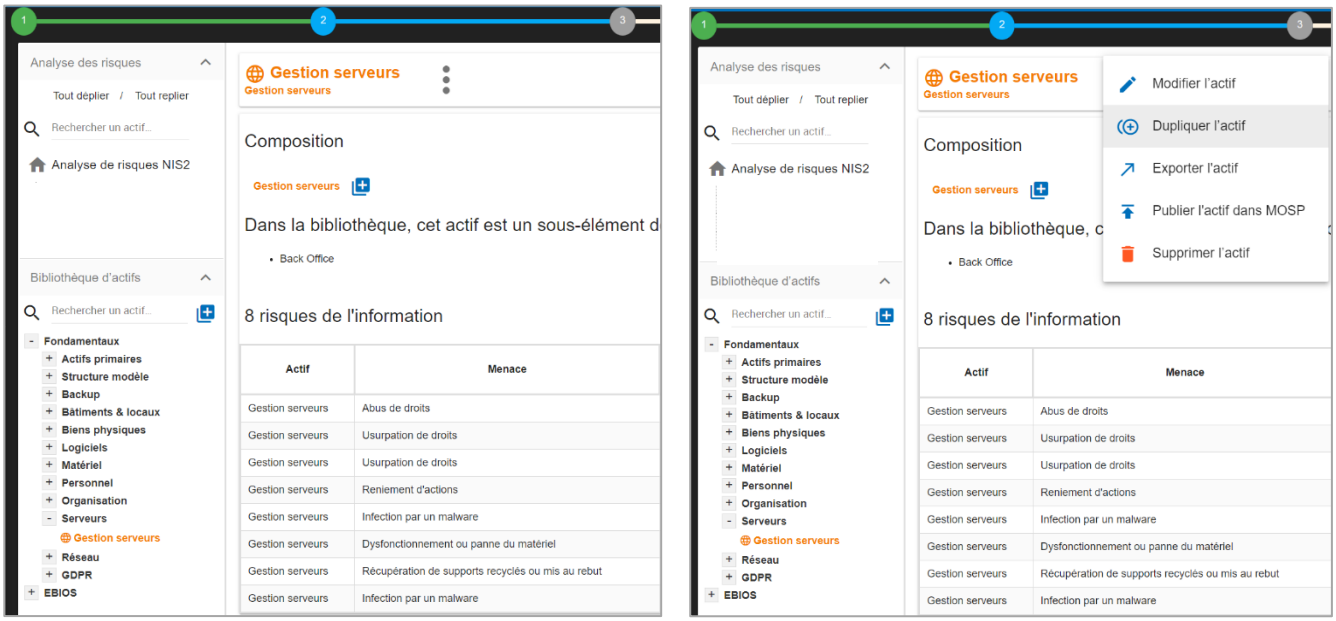


Figure 11: choix de l'actif et l'option de duplication

- Une fois l'étape précédente effectuée, il suffit de cliquer sur "Dupliquer l'actif" pour qu'il soit immédiatement dupliqué.

- Pour le renommer, la sélection de "Modifier l'actif" permet de le renommer à la suite du clic sur les trois points situés en haut à gauche. Une fois renommé, il convient de sauvegarder les modifications effectuées.

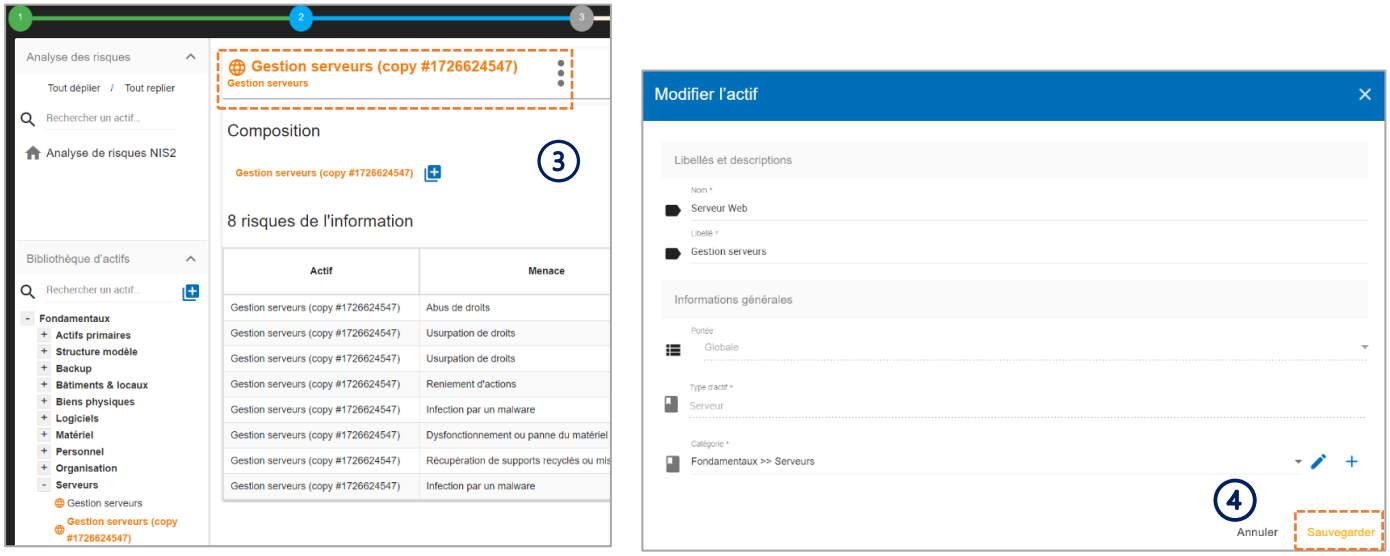


Figure 12: Modification de l'actif dupliqué

- Actif de support : ce sont les actifs qui supportent les actifs primaires. Ils peuvent être des équipements, des applications et logiciels, des réseaux, des ressources humaines, etc. Les risques (menaces et vulnérabilités) sont associés à ces actifs.

Concernant les actifs de support, le HCPN a défini un modèle d'actifs basés sur 3 catégories :

- Catégorie « Niveau 1 » : nombre limité d'actifs de supports et de risques
- Catégorie « Niveau 2 » : nombre modéré d'actifs de supports et de risques
- Catégorie « Niveau 3 » : nombre élevé d'actifs de supports et de risques

Pour plus de détails sur l'ensemble des actifs définis pour les différentes catégories, il est recommandé de se référer au lien suivant dans la section ***"Annexes - Répartition des Actifs".***

Dans le cadre des analyses de risques, les entités peuvent, si nécessaire, utiliser des actifs issus des différentes catégories définies (Niveau 1, Niveau 2, Niveau 3). Cependant, il convient de rester raisonnable lors de la sélection des actifs, en particulier s'il s'agit d'une première analyse de risques, et si les ressources dont dispose l'entité sont limitées.

Duplication et renommage des actifs de supports

Les actifs de supports peuvent être choisis parmi ceux qui ont été définis selon la catégorie appropriée à l'entité. Par ailleurs, s'il est nécessaire d'avoir le même actif mais pour différents composants, MONARC offre la possibilité de le dupliquer et de le renommer en fonction des besoins en suivant la procédure de duplication précédente.

Les administrations publiques utilisent régulièrement des produits ou services fournis par des prestataires étatiques tels que le CTIE. Conformément à la directive NIS2, la responsabilité en matière de cybersécurité reste entièrement portée par chaque entité. Cela signifie que chaque administration doit évaluer les risques liés à sa propre dépendance vis-à-vis de ces services.

L'objectif lors des premières années, pour les services externalisés, est principalement de bien de comprendre comment une interruption ou une défaillance de ces services pourrait impacter les activités de l'entité elle-même, sans attendre que le prestataire ne fournisse une analyse de risques spécifique.

Puis, dans un deuxième temps, de réévaluer les mesures de sécurité mises en œuvre par le prestataire.

Dans le cadre de vos premières analyses de risques avec l'outil MONARC, nous vous recommandons ainsi de vous concentrer prioritairement sur les risques liés à votre périmètre direct de responsabilité, y compris ceux découlant de vos dépendances externes.

Par exemple :

- Pour un équipement hardware hébergé ou géré par un prestataire, évaluez le risque pour vos opérations en cas d'indisponibilité ou de défaut de maintenance.
- Pour une application métier exploitée par un prestataire étatique, analysez les conséquences pour vos processus si le service est interrompu, dégradé, ou exposé à une faille non corrigée rapidement.

En pratique, vous pouvez facilement identifier si un actif de support est fourni par le CTIE (postes de travail, serveurs de fichiers, réseau RACINE, etc.) en consultant la colonne I « Actif(s) de support potentiellement concerné(s) par un service offert par le CTIE » du fichier « Modèle d'actifs de support du HCPN.

Identification des risques

Une fois les actifs primaires et de support identifiés et ajoutés au projet créé sur la plateforme MONARC, un ensemble de risques (menaces et vulnérabilités) seront alors associés aux actifs de support, tel qu'indiqué ci-dessous :

Exemple : menaces et vulnérabilités d'un « Serveur Web ».

Actif	Impact C	Impact I	Impact D	Menace Libellé	Menace Prob.	Vulnérabilité Libellé	Vulnérabilité Mesures en place	Vulnérabilité Qualif.	Risque actuel C	Risque actuel I	Risque actuel D	Traitement	Risque résiduel
Serveur Web	3	2	2	Dysfonctionnement ou panne du matériel	-	Absence de gestion de niveau de service		-		-	-	Non traité	-
Serveur Web	3	2	2	Usurpation de droits	-	Possibilité d'administrer le système à distance		-	-	-	-	Non traité	-
Serveur Web	3	2	2	Usurpation de droits	-	Failles dans la gestion ou l'utilisation dans les comptes à privilèges		-	-	-	-	Non traité	-

Figure 134 : Menaces et vulnérabilités associées au serveur Web

La volumétrie et le niveau de granularité des vulnérabilités est aligné avec chaque type de catégorie défini, afin de permettre une analyse plus fine des risques selon la taille, les ressources et la complexité de l'infrastructure pour chaque entité.

Héritage des risques pour les catégories d'actifs

Les risques associés aux actifs dont la catégorie est « Niveau 1 » ou « Niveau 2 » seront hérités par ceux dont la catégorie est plus détaillée et granulaire (« Niveau 2 » ou « Niveau 3 »).

Exemple : actif de support "Application métier logiciel"

Le tableau ci-dessous montre que les risques identifiés pour l'actif de support "Application métier/Logiciel" sont bien hérités et repris dans la catégorie « Niveau 2 ». Les risques de la catégorie « Niveau 2 » sont également hérités dans la catégorie « Niveau 1 » (Ils ne figurent pas dans ce tableau).

ID Actif	Actif de support	Type d'actif	ID Menace	Menace	ID Vulnérabilité	Vulnérabilité
Niveau 1						
C1-SFT-01	Application métier/Logiciel	Software	MDA17	Abus de droits	ISO-VLN-28	Mauvaise allocation des droits d'accès logiques
			MDA13	Infection par un malware	CUS-VLN-37	Absence de mise en place de règles de sécurité de base pour application/logiciel
			MA15	Dysfonctionnement logiciel	ISO-VLN-32	Utilisation d'une version obsolète
Niveau 2						

C2-SFT-01	Application métier/Logiciel+	Software	MDA13	Infection par un malware	CUS-VLN-37	Absence de mise en place de règles de sécurité de base pour application/logiciel
			MA15	Dysfonctionnement logiciel	ISO-VLN-32	Utilisation d'une version obsolète
			MDA17	Abus de droits	ISO-VLN-28	Mauvaise allocation des droits d'accès logiques
			CUS-TH13	Exploitation de faille	CUS-VLN-76	Absence de mise à jour et de correctifs réguliers
			CUS-TH21	Interruption des services	CUS-VLN-78	Absence de procédure de maintenance et de rollback
			MA11	Erreur d'utilisation	70	Absence de documentation explicite sur les systèmes applicatifs

Risques catégorie « Niveau 1 »

Risques catégorie « Niveau 2 »

Tableau 1: héritage des risques d'application métier/logiciel par type de catégories

Appréciation des impacts

Après l'identification des actifs primaires et des risques potentiels pour chaque entité, l'étape suivante consiste à évaluer chaque actif primaire en fonction de son impact sur les critères de sécurité de l'information (confidentialité des données (C), intégrité des données (I) et disponibilité des données (D)) ainsi que les différentes conséquences sur l'entité en question (ROLFP).

Cette évaluation consiste à déterminer les conséquences potentielles d'une compromission de chaque actif sur les différents critères, sur une échelle définie.

ROLFP

- **R**: Réputation
- **O**: Opérationnel
- **L**: Légal
- **F**: Financier
- **P**: Personne

Afin de définir les impacts sur MONARC, il suffit de suivre les étapes suivantes :

1. D'abord, il est nécessaire de sélectionner l'actif primaire pour lequel l'évaluation des impacts CIA (Confidentialité, Intégrité, Disponibilité) sera effectuée.

   Ensuite, il est nécessaire de sélectionner les trois points pour afficher les options relatives aux actifs. Cela permettra d'accéder à des fonctionnalités telles que l'évaluation des impacts CIA associés à l'actif.

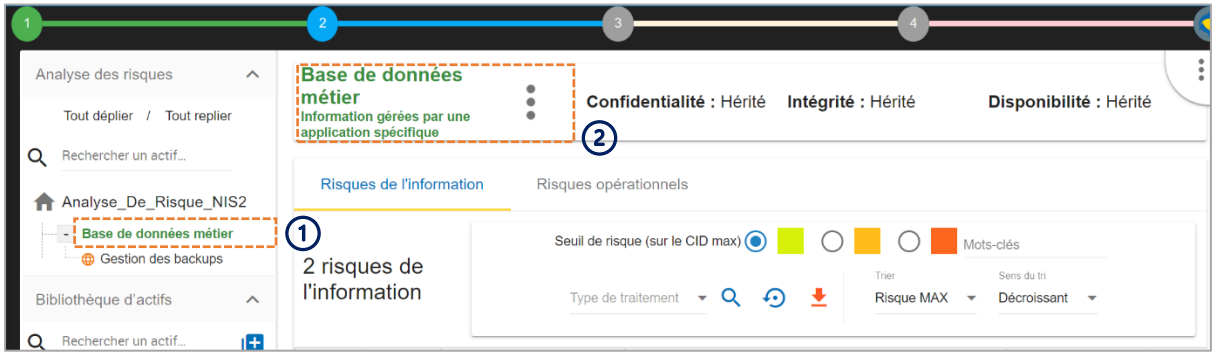


Figure 15 : sélection de l'actif primaire

2. Une fois l'étape précédente réalisée, il convient de choisir "Modifier les impacts" parmi la liste des options qui s'affichera.

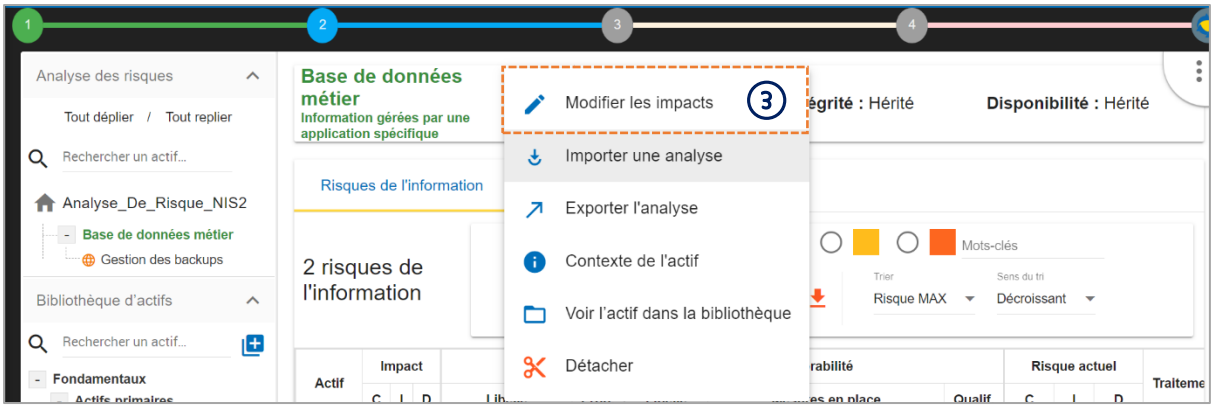


Figure 146 : sélection de l'option modification d'impact pour l'actif primaire

3. Une fois la matrice d'évaluation d'impact pour chaque critère CIA affichée, il est important d'évaluer le niveau d'impact en fonction des conséquences définies.

   La valeur d'impact pour chaque critère CIA correspond à la valeur maximale parmi les différents types de conséquences évaluées (ROLFP). Cela représente la criticité la plus élevée de l'actif et indique le domaine dans lequel une compromission pourrait entraîner les conséquences les plus importantes.

   Une fois la définition d'impact complétée, il convient de sauvegarder les modifications effectuées.

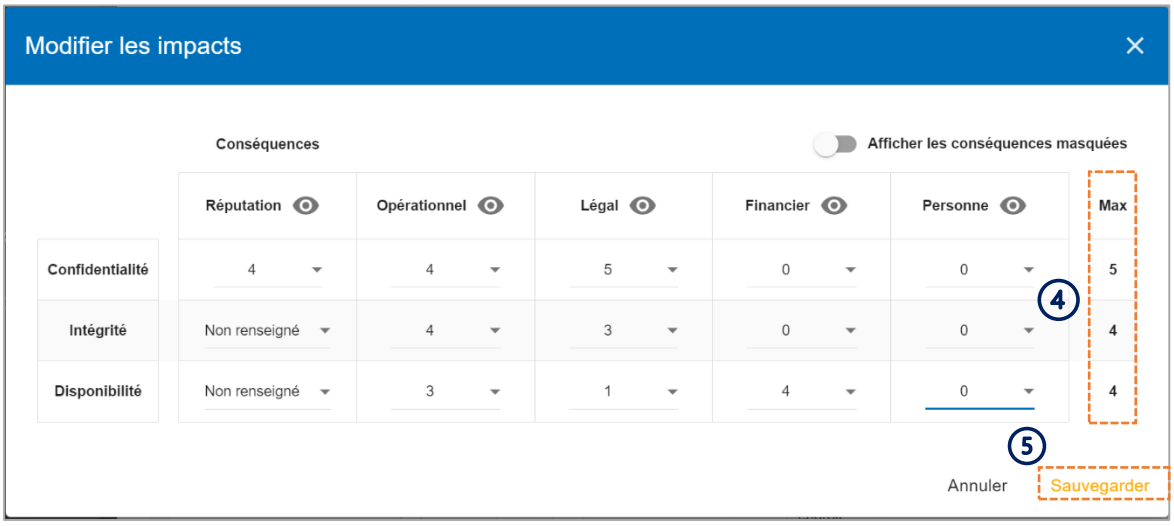


Figure 1715: évaluation et choix d'impact maximal

Héritage des impacts :

Grâce à la notion d'héritage sur MONARC, les mêmes niveaux d'impact définis pour les actifs primaires seront également appliqués aux actifs qui les supportent (les actifs de support).

Par exemple, dans la figure ci-dessous, l'actif « Serveur de stockage » supporte l'actif primaire » Base de données métier« , pour lequel les impacts ont été évalués précédemment (***cf : Appréciation des impacts***). Celui-ci a automatiquement hérité des mêmes niveaux d'impact.

Figure 18 : héritage des impacts CIA pour les actifs de support

Les impacts CIA (Confidentialité, Intégrité, Disponibilité) sont liés et associés aux actifs primaires identifiés lors d'une analyse de risques.

Dans la plateforme MONARC, l'étape d'identification des actifs, menaces et vulnérabilités peut être réalisée en cliquant sur "**Identification des actifs, vulnérabilités et appréciation des impacts**", qui s'affichera en double-cliquant sur "**2**", comme indiqué ci-dessous :

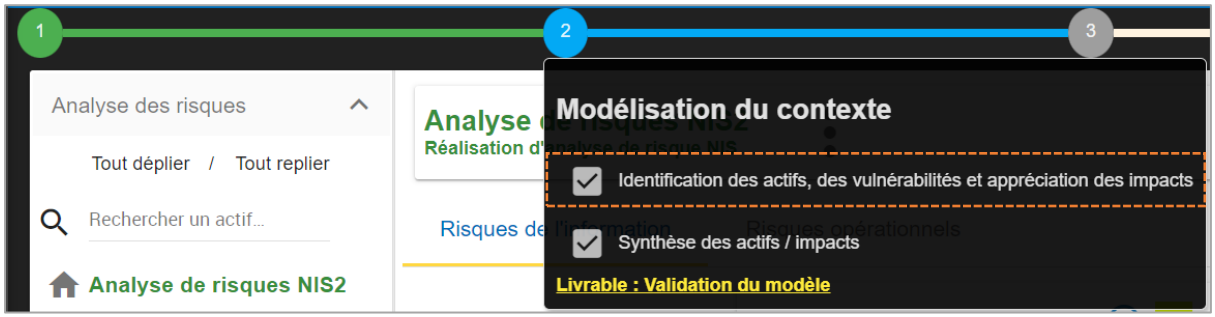


Figure 19: étape identification des actifs, vulnérabilités et appréciation des impacts dans MONARC

2.2.2.2 Synthèse des actifs/impacts

Cette étape synthétise quelques éléments importants relatifs à la phase d'identification des actifs et des risques qui y sont liés, comme la liste des actifs primaires et supports sélectionnés, etc.

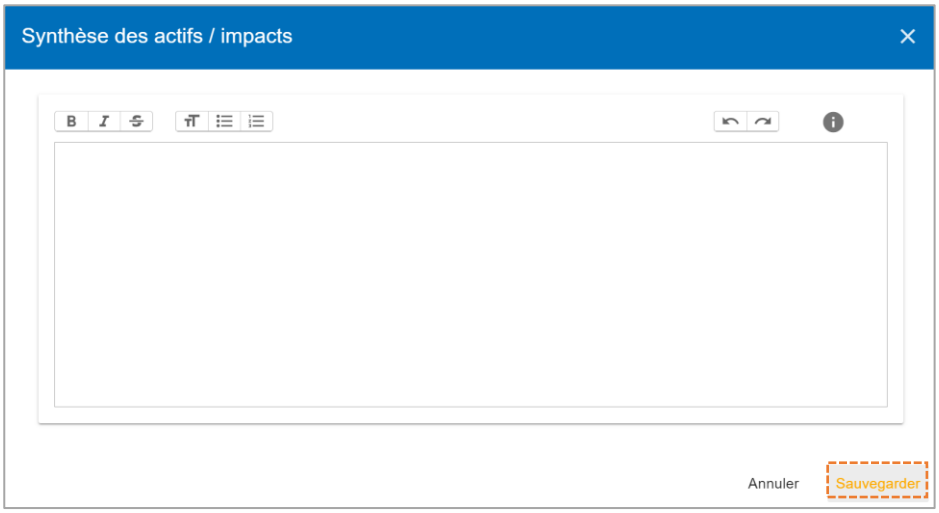


Figure 16: résumé des actifs et des impacts

Cette étape peut être réalisée en cliquant sur « **synthèse des actifs/Impacts** », qui s'affichera en double-cliquant sur "**2**", comme suit :

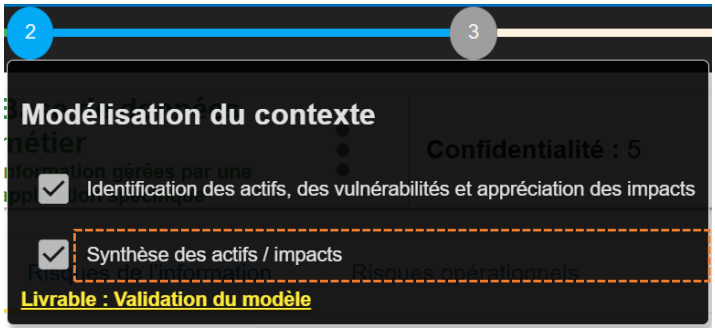


Figure 17: étape synthèse des actifs/impacts dans MONARC

2.2.3 Phase 3 : Evaluation et traitement des risques

Une fois l'étape "2" est complétée, il est nécessaire d'évaluer les risques identifiés.

2.2.3.1 Estimation, évaluation, et traitement du risque

Pour cette étape, il convient de définir la qualification de chaque vulnérabilité en tenant compte de la maturité des mesures de sécurité mises en place par l'entité.

Pour justifier du niveau de vulnérabilité choisi, il est nécessaire d'indiquer dans le champ « Mesures en place » les mesures de sécurité déjà implémentées.

L'estimation de la probabilité d'exploitation des vulnérabilités dépendant directement de l'efficacité des contrôles existants. Ainsi, des questions avec les contrôles à avoir en place pour chaque vulnérabilité ont été ajoutées à la plateforme MONARC.

Afin de visualiser les questions, il suffit de placer le curseur sur chacune des vulnérabilités.

Ensuite, il convient de définir la probabilité des menaces et leur capacité à exploiter les vulnérabilités identifiées en considérant les mesures de sécurité déjà mises en place par l'entité.

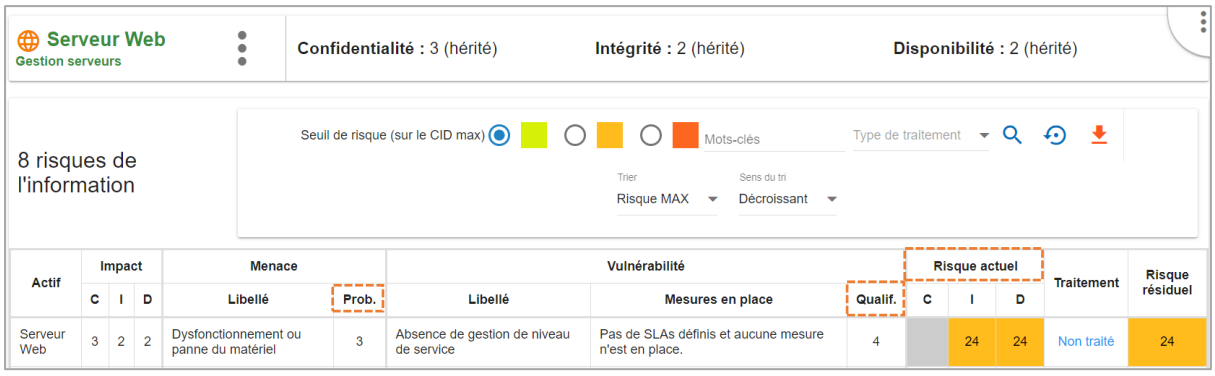
Une fois la probabilité d'une menace et la qualification de la vulnérabilité définie, le niveau de risque actuel est automatiquement calculé dans MONARC en tenant compte de ces éléments, ainsi que du niveau d'impact, qui constitue un composant clé dans l'évaluation du risque.

Le niveau de risque est calculé et évalué suivant la formule ci-dessous :

Niveau de risque = impact x (menace x vulnérabilité)

Probabilité du risque

Ci-dessous un exemple d'évaluation d'un risque dans MONARC pour l'actif de support "Serveur Web" :



Actif	Impact			Menace		Vulnérabilité			Risque actuel			Traitement	Risque résiduel
	C	I	D	Libellé	Prob.	Libellé	Mesures en place	Qualif.	C	I	D		
Serveur Web	3	2	2	Dysfonctionnement ou panne du matériel	3	Absence de gestion de niveau de service	Pas de SLAs définis et aucune mesure n'est en place.	4		24	24	Non traité	24

Figure 18: évaluation du risque lié à l'actif serveur

Les risques de non-conformité aux lois et règlements auxquels l'entité est soumise ***doivent être considérés et évalués, indépendamment de la catégorie*** d'actif choisie et utilisée.

Traitement de risques

Identification d'une option de traitement de risques

Après l'évaluation des risques identifiés pour une entité, plusieurs options de traitement des risques peuvent être envisagées, comme défini ci-dessous **:**

Option de traitement	Description
Refusé	Suspension de toute activité à l'origine du risque qui entraînerait une perte potentielle, permettant ainsi de l'éliminer.
Accepté	Le risque peut être accepté. Cela est particulièrement possible lorsque le risque se situe dans les limites de tolérance définies par l'entité. Un risque peut également être accepté lorsqu'il n'est pas possible de le transférer, de le traiter ou de le refuser.
Réduction	La mise en œuvre de contrôles et de mesures de sécurité pour réduire la probabilité et/ou l'impact du risque.
Partagé	Transférer ou partager un risque avec d'autres entités par le biais d'une assurance ou d'un contrat externe.

Tableau 2: options traitement de risques

Pour chaque risque évalué, il convient de lui associer l'une des options de traitement définies dans le tableau ci-dessus.

Critères de traitement de risques

Le traitement des risques prend en compte plusieurs critères, dont l'impact de chaque risque et l'appétit au risque défini par l'entité, ainsi que la criticité des actifs.

Si les risques évalués sont associés à des actifs gérés par une entité et que certains doivent être réduits, il est alors essentiel de définir pour chacun un ensemble de recommandations (plan d'action) et de les intégrer dans MONARC.

Si certains actifs sont gérés par les fournisseurs (p. ex. : le CTIE), il convient de choisir l'option de traitement du risque « Partagé ».

Acceptation de risques

Les risques devraient être acceptés selon les critères et les exigences d'acceptation adoptés par l'entité.

Si l'acceptation de certains risques fait l'objet d'une exception, celle-ci devrait être documentée, approuvée par les parties prenantes appropriées et périodiquement réévaluée.

Choix de l'option de traitement de risques MONARC

Pour choisir l'option de traitement d'un risque sur MONARC, il suffit de suivre les étapes suivantes :

1. D'abord, il convient de double-cliquer sur « Non traité » dans la colonne "Traitement'' pour chaque risque identifié, afin d'accéder aux options de traitement de risques et de définir les mesures de traitement à mettre en place pour l'atténuer.

Figure 19: accès aux options de traitement de risques

2. Ensuite, il est nécessaire de choisir l'option de traitement la plus appropriée pour chaque risque, en sélectionnant une option dans la liste déroulante des options de traitement disponibles.

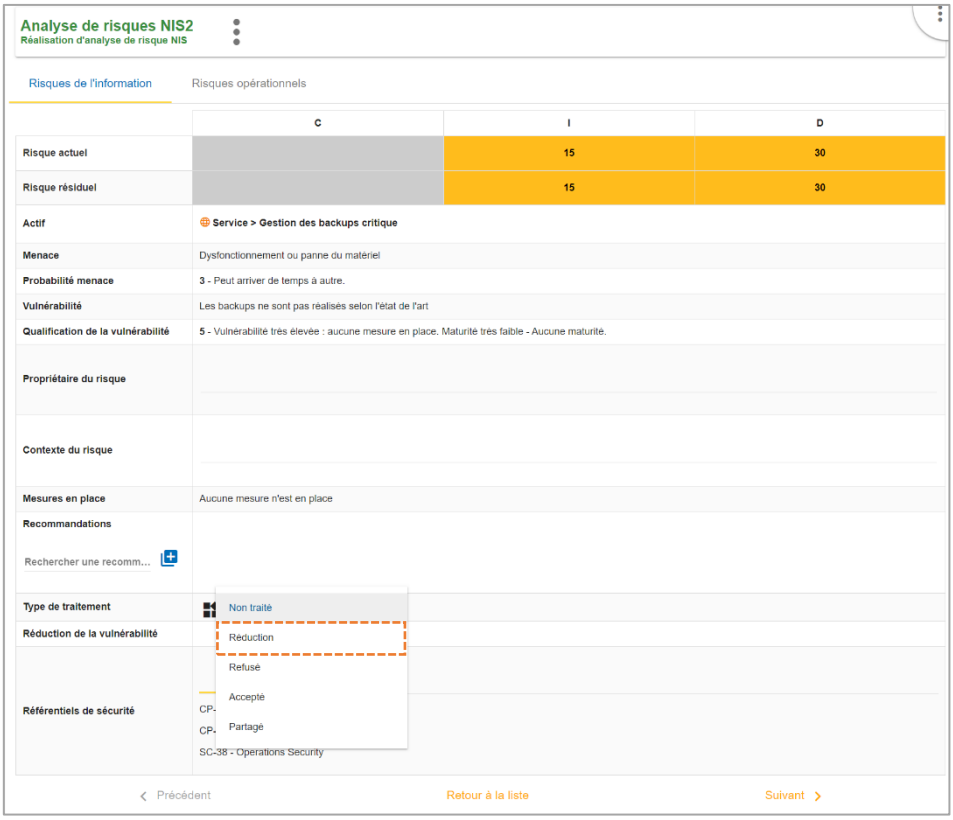


Figure 20: choix option traitement de risque

3. Une fois l'option sélectionnée, il est important de définir la nouvelle qualification de la vulnérabilité, atteinte une fois les recommandations mises en place, afin de réduire le niveau de risque en fonction de l'option de traitement choisi.

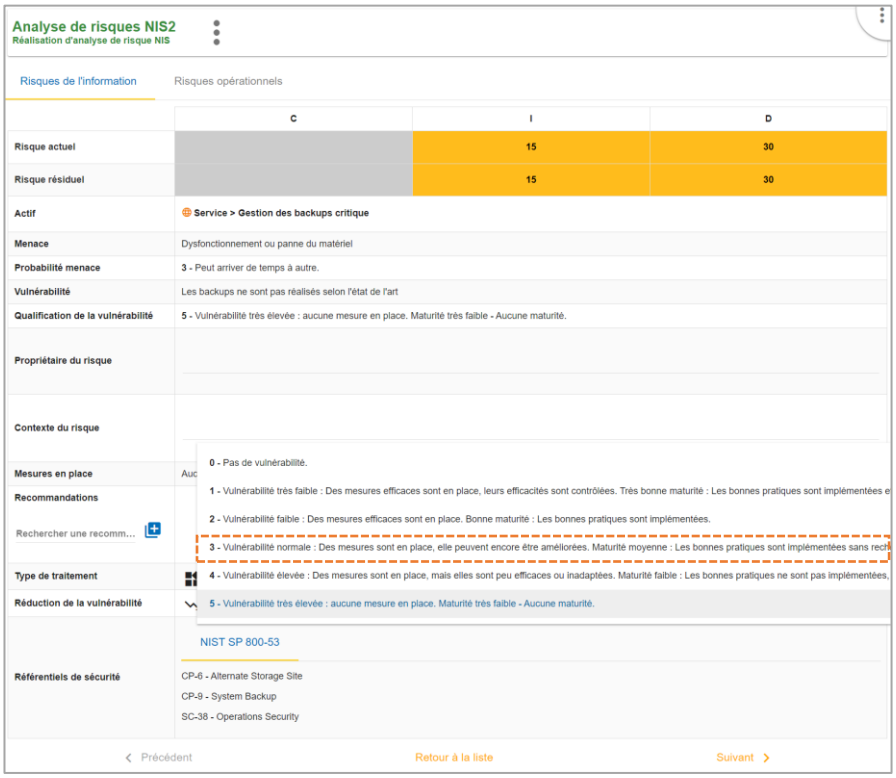


Figure 21: Réduire niveau de vulnérabilité

4. À la suite de la réduction de la vulnérabilité, le niveau de risque résiduel sera également diminué. La différence entre le risque initial et le risque résiduel sera affichée et calculée automatiquement, comme indiqué ci-dessous :

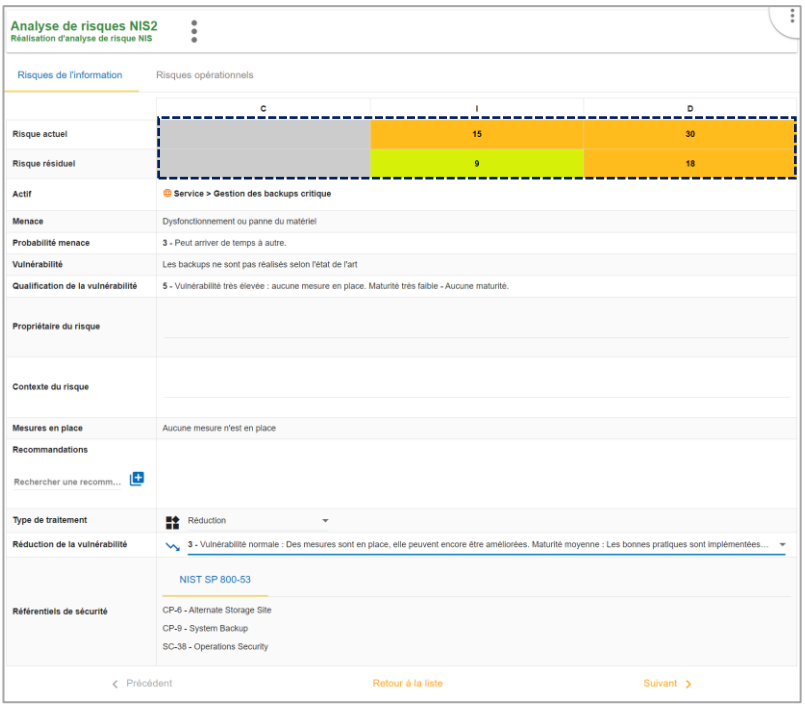


Figure 22: Calcul automatique du risque résiduel

Dans le cas où l'option de traitement de risques à choisir est la réduction, il est alors nécessaire de définir les mesures de traitement visant à diminuer le niveau de vulnérabilité et le niveau de risques actuel.

Il existe deux méthodes pour définir les recommandations : elles peuvent être sélectionnées à partir d'une liste prédéfinie ou créées en fonction des risques et du besoin.

Méthode 1 : Sélection d'une recommandation :

Afin de sélectionner une recommandation, il est nécessaire de suivre les étapes suivantes :

- Il est possible d'effectuer une recherche par mot clé dans la barre de recherche située dans la section « Recommandation » (ex : service).

  La liste de toutes les recommandations déjà définies contenant le mot clé s'affichera, comme indiqué ci-dessous :

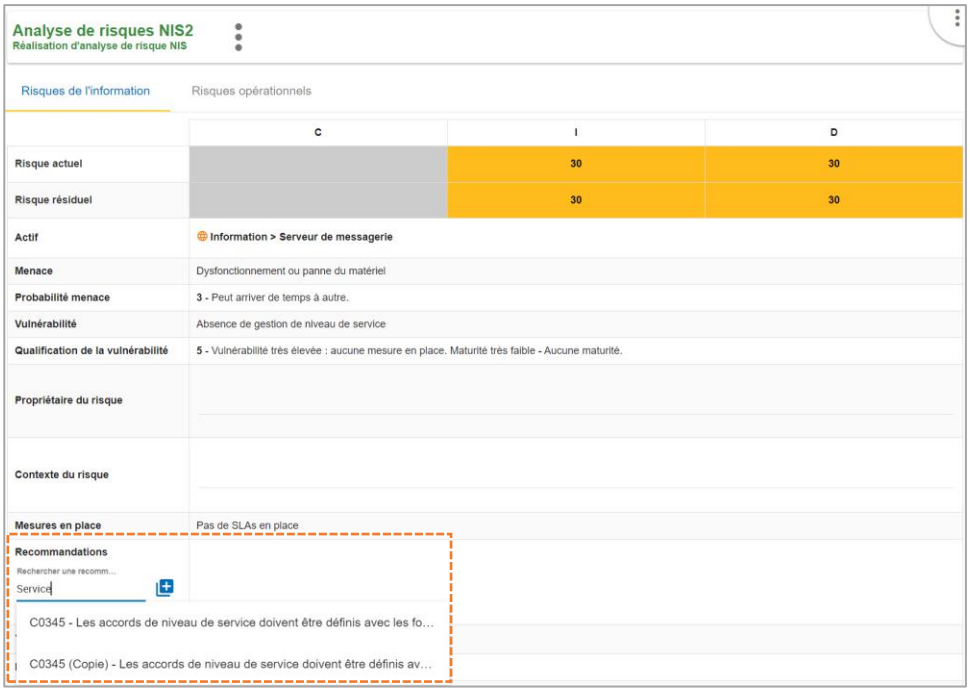


Figure 27 : Rechercher une recommandation avec mot-clé

- Une fois la recommandation sélectionnée, elle sera automatiquement liée et associée au risque.

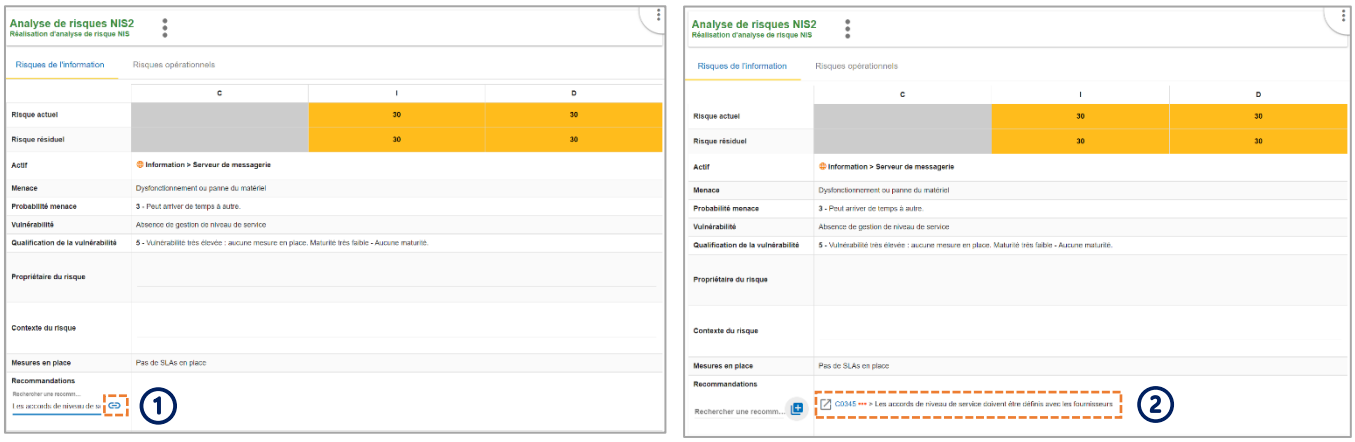


Figure 28 : Association d'une recommandation à un risque

Méthode 2 : création d'une recommandation

Afin d'ajouter une nouvelle recommandation, il est important de suivre les étapes suivantes :

- D'abord, il convient de cliquer sur "**+**'' dans la section " Recommandations''.

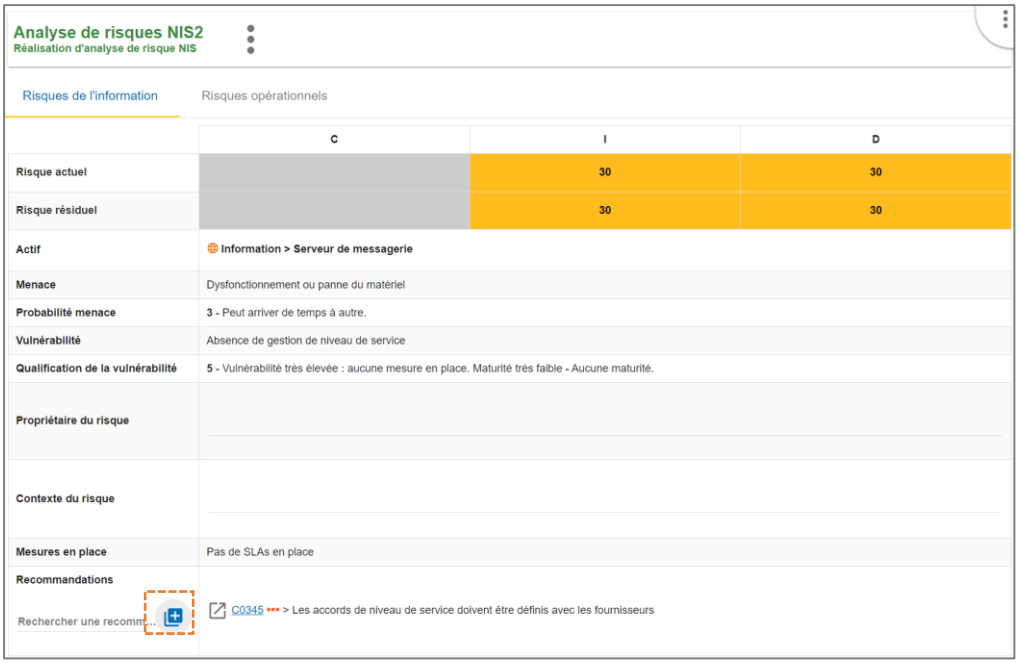


Figure 29 : Création d'une nouvelle recommandation

- Ensuite, tous les champs présents dans la fenêtre d'ajout devraient être complétés. Il est important de cliquer sur ''**+**'' afin d'ajouter la recommandation puis choisir l'option ''Crée''.

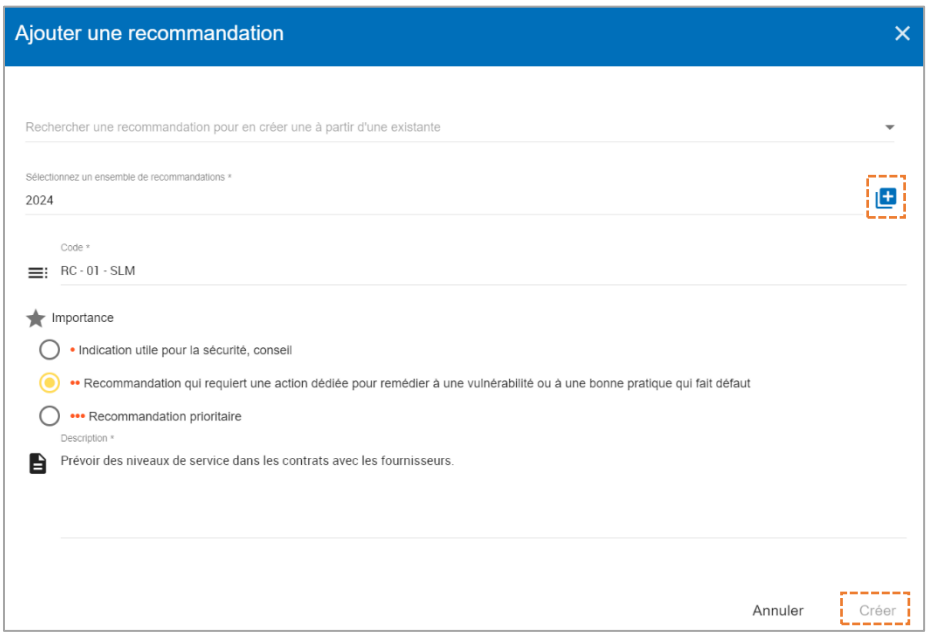


Figure 23: Ajout de la recommandation au risque

La recommandation créée sera automatiquement associée au risque en question et intégrée dans le plan de traitement défini sur MONARC

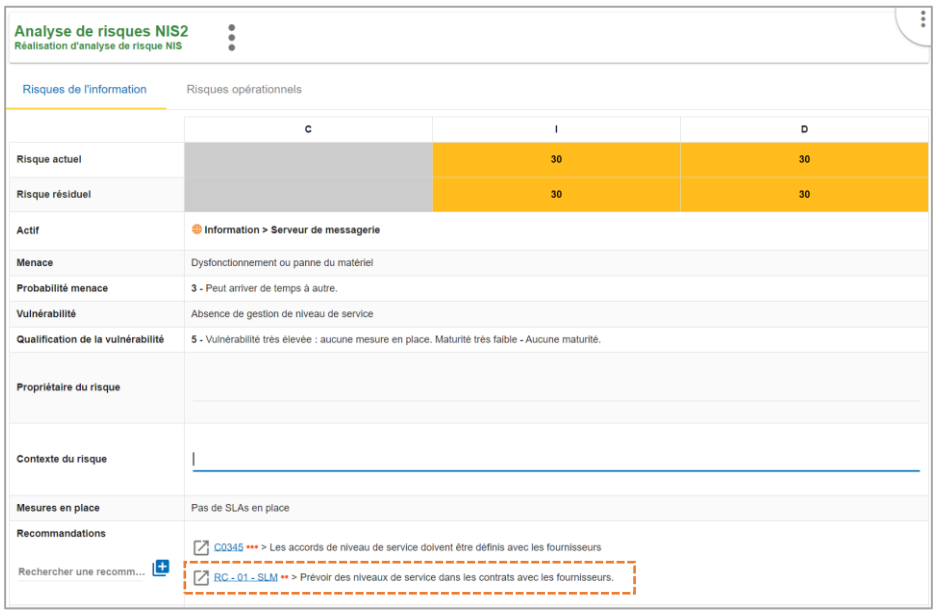
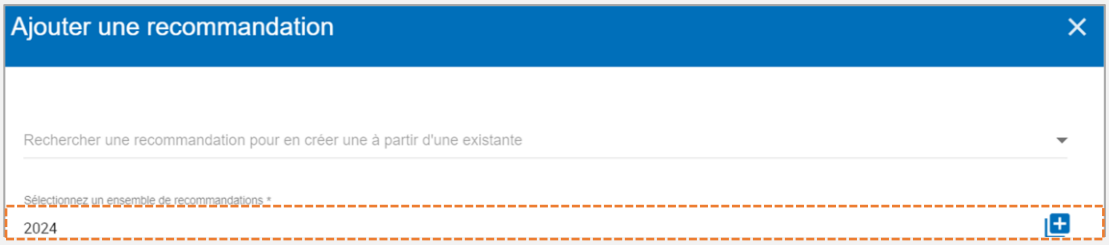


Figure 24: association de la recommandation au risque

- Pour évaluer les autres risques, il suffit de cliquer sur "Retour à la liste" afin d'avoir l'ensemble des risques identifiés. Si tous les risques ont déjà été évalués, il est possible de choisir "Suivant". Cette option permet de définir les options de traitement et les recommandations spécifiques à chaque risque évalué.

Lors de la création d'une recommandation, il est conseillé d'ajouter l'année en court dans le champ ''Sélectionnez un ensemble de recommandations'' afin d'identifier facilement l'ensemble des recommandations définies pour chaque année.



Risque résiduel

Après avoir traité un risque, le risque résiduel devrait être réévalué et son acceptabilité validée selon le niveau d'acceptation de risques défini.

Figure 25: Calcul du risque résiduel suivant l'option de traitement choisie

Dans la plateforme MONARC, cette étape peut être réalisée en cliquant sur "**Estimation, évaluation et traitement des risques**", qui s'affichera en double-cliquant sur "**3**", comme indiqué ci-dessous :

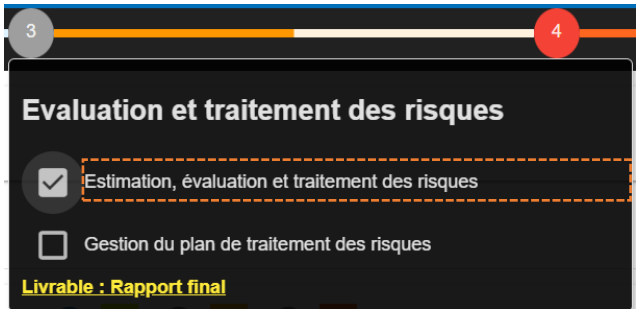


Figure 26: étape estimation, évaluation et traitement des risques dans MONARC

2.2.3.2 Gestion du plan traitement de risques

Une fois l'étape 2 réalisée, un plan de traitement sera créé automatiquement sur MONARC, contenant toutes les recommandations définies pour l'ensemble des risques évalués. La priorité des recommandations peut être ajustée en fonction de leur importance et du niveau de risques auquel elles sont associées.

Figure 27: Ajout automatique des recommandations au plan de traitement

Dans la plateforme MONARC, cette étape peut être réalisée en cliquant sur "**Gestion du plan de traitement des risques**", qui s'affichera en double-cliquant sur "**3**", comme indiqué ci-dessous :

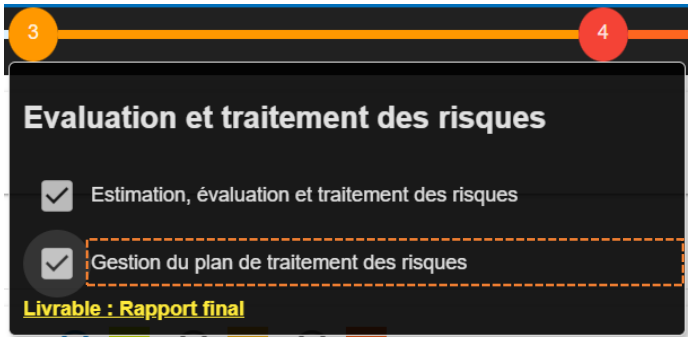


Figure 28: étape gestion du plan de traitement des risques dans MONARC

2.2.4 Phase 4 : implémentation et surveillance

Une fois les recommandations définies pour réduire les risques, il est important de veiller à ce qu'elles soient suivies avec les personnes responsables de leur implémentation. Cela permet de garantir qu'elles sont effectivement mises en place.

Il est important de définir un responsable et un niveau d'importance pour chaque recommandation et fixer des échéances.

Il est possible de consulter l'historique d'implémentation et les informations relatives aux actions.

Figure 29: Suivi et implémentation du plan de traitement

Le suivi des recommandations peut être réalisé sur MONARC en cliquant sur "**Gestion de l'implémentation du plan de traitement des risques**", qui s'affichera en double-cliquant sur "**4**", comme indiqué ci-dessous :

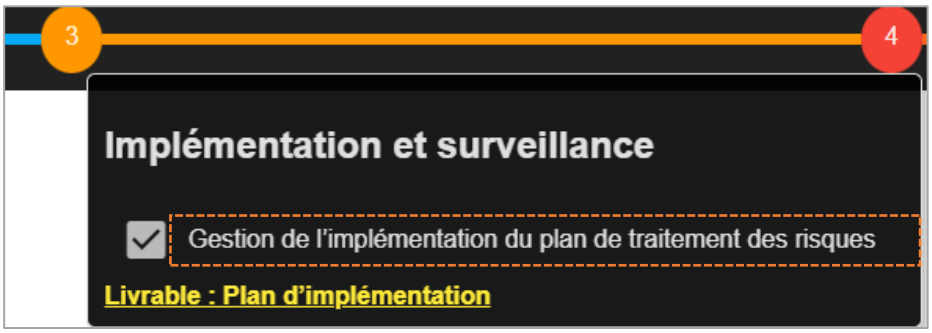


Figure 37: étape gestion et implémentation du plan de traitement des risques

3 Tips/FAQ

3.1 Tips établissement de contexte

3.1.1 Étapes de changement des échelles

Si la modification des échelles pour les critères d'évaluation des risques est autorisée, il est alors possible de procéder comme suit :

1. Pour chaque critère, il est possible de faire un double clic sur le niveau d'échelle maximum et de l'incrémenter en fonction des besoins.

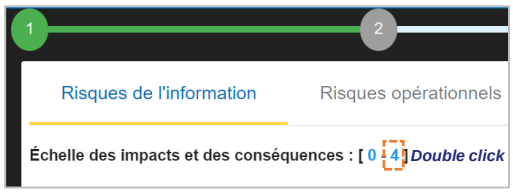


Figure 38 : sélection du niveau maximum de l'échelle

2. Une fois l'étape précédente réalisée, il convient d'ajouter les descriptions nécessaires pour les lignes ajoutées en fonction des critères mis à jour (ex : Impact CIA, vulnérabilités, etc.), comme indiqué ci-dessous :

	Impacts		
	Confidentialité	Intégrité	Disponibilité
0	Impact inexistant. Le critère de confidentialité n'est pas important.	Impact inexistant. Le critère d'intégrité n'est pas important.	Impact inexistant. Le critère de disponibilité n'est pas important.
1	Impact faible, négligeable La divulgation est défavorable aux intérêts de l'organisation Exemples : - Divulgation d'information interne ne devant pas sortir de l'organisme - Note de service - Annuaire téléphonique interne	Impact faible, négligeable Corruption facile à rectifier et sans grandes conséquences. Exemples : - Courrier interne, e-mail interne	Impact faible, négligeable Indisponibilité gênante, mais pas encore préjudiciable pour les parties prenantes
2	Impact moyen, acceptable La divulgation nuit aux intérêts de l'organisation Exemples : - Divulgation d'information moyennement sensible restreinte à un groupe de personnes - schéma de réseau interne - Documentation ou programme source non critique	Impact moyen, acceptable Corruption occasionnant une gêne modérée aux parties prenantes. Le rétablissement est facile. Exemples : - Site Internet informationnel	Impact moyen, acceptable Indisponibilité occasionnant une gêne modérée aux parties prenantes. Exemples : - Délais maximums considérés comme insupportables pas encore atteints
3	Impact sérieux, difficilement supportable La divulgation nuit gravement aux intérêts de l'organisation Exemples : - Divulgation d'information confidentielle - Secret bancaire - Données à caractère personnelles sensibles - Incidents de sécurité	Impact sérieux, difficilement supportable Corruption occasionnant une gêne considérable aux parties prenantes. Exemples : - Confusion entre parties prenantes	Impact sérieux, difficilement supportable Indisponibilité occasionnant une gêne considérable aux parties prenantes. Exemples : - Atteinte des délais maximums considérés comme insupportables
4	Impact très sérieux, insupportable La divulgation nuit de façon quasi insurmontable aux intérêts de l'organisation. Exemples : - Divulgation d'information secrète ou très sensible - Information classifiée par la loi (EU, OTAN, nationale, etc.)	Impact très sérieux, insupportable Corruption non recouvrable débouchant sur une indisponibilité définitive	Impact très sérieux, insupportable Indisponibilité demandant un très gros effort de rétablissement, voire définitif. Exemples : - Large dépassement des délais maximums considérés comme insupportables
5			

Figure 39 : Ajout de descriptions pour les différents critères

3.1.2 Informations sur contexte/Synthèse/Organisation de l'analyse de risques

Pour plus d'informations sur le contexte d'analyse de risques et son organisation, il est recommandé de cliquer sur l'icône d'information afin d'avoir des détails supplémentaires relatifs à ces étapes. Cela permettra d'avoir un contexte détaillé et exhaustif pour l'analyse de risques à réaliser.

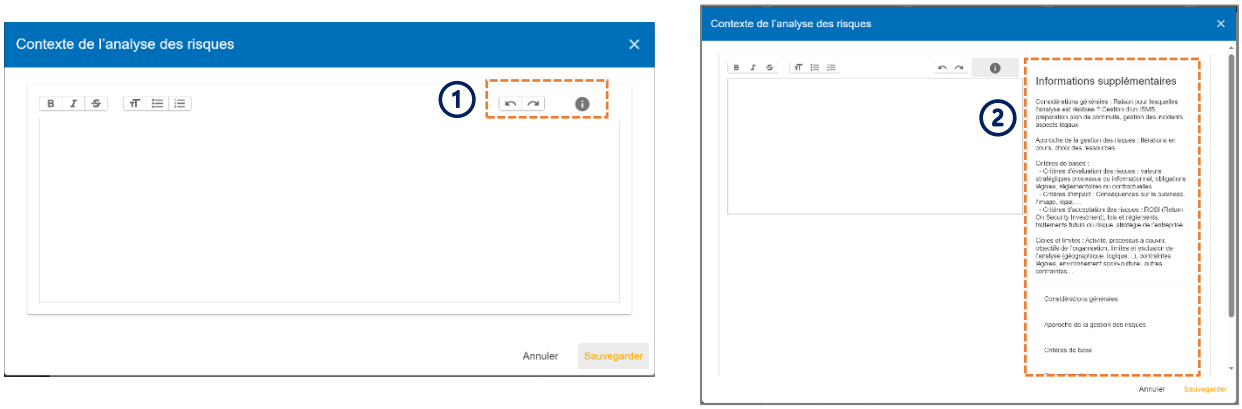


Figure 40 : Affichage des informations supplémentaires

4 Annexes

4.1 Liste des actifs de support

Pour plus de détails sur les actifs de support définis pour chaque catégorie, il est recommandé de se référer au tableau ci-dessous :

Actif de support	Type d'actif	Niveau 1	Niveau 2	Niveau 3	Exemple actif
Serveurs	Hardware	X	X	X	Serveur de fichier, serveur de messagerie
Equipement utilisateur	Hardware	X			Laptops, Smartphone
Utilisateur	Personnel	X	X	X	
Organisation informatique	Organisation	X	X	X	Gestion infrastructure réseau, stockage, etc.
Service externalisé	Outsourced service	X	X	X	Alimentation, eau, etc..
Application métier/Logiciel	Software	X	X	X	Gestion personnel, gestion de paie, gestion de documents etc.
Messagerie	Software	X	X	X	
Infrastructure Physique	Site	X	X		Bâtiments/Locaux, Salle de serveurs, Salle des archives, Système de sécurité physique
Média amovible	Hardware	X	X	X	USB, disque dur externe
Réseau et télécommunication	Network	X	X		Internet, réseau Wifi
Outils communication	Software	X	X	X	Teams, outil gestion de projet et collaboration, etc.
Equipement Réseau	Hardware	X	X	X	Routeur, Switch, etc.
Poste de travail+	Hardware		X	X	Laptops, Ordinateur fixe
Smartphone+	Hardware		X	X	
Intranet+	Network		X	X	

Actif de support	Type d'actif	Niveau 1	Niveau 2	Niveau 3	Exemple actif
Imprimante+	Hardware		X	X	
Firewall+	Hardware		X	X	
Administrateur+	Personnel		X	X	
Equipement personnel (BYOD)+	Hardware		X	X	PC, tablette, smartphone, etc.
Fournisseurs+	Outsourced service		X	X	
Salle de serveurs++	Site			X	
Proxy++	Hardware			X	
Datacenter++	Hardware			X	
Base de données++	Software			X	
Système de supervision++	Software			X	
Système d'exploitation++	Software			X	Windows, Mac, Linux, etc.
Document numérique/papier++	Hardware			X	
Développeur++	Personnel			X	
Salle des archives++	Site			X	
Système de sécurité physique++	Software			X	Caméra, badge, biométrie, alarme, etc.
VPN++	Network			X	
Poste de travail admin ++	Hardware			X	
Outils de développement ++	Software			X	IDE (ex : Visual studio), environnement, etc..
Internet++	Network			X	
Réseau Wifi++	Network			X	
Serveur Web++	Hardware			X	

Actif de support	Type d'actif	Niveau 1	Niveau 2	Niveau 3	Exemple actif
Développements logiciels++	Organisation			X	
Backup++	Organisation			X	système de backup, audit, politique/processus, etc.
Système monitoring de la sécurité++	Organisation			X	Antivirus sur poste de travail et serveurs, EDR

Tableau 3: liste des actifs de support par type de catégorie

4.2 Répartition des Actifs

Le tableau ci-dessous permet d'illustrer la répartition des actifs à travers les trois catégories définies :

Asset Type	Actif « Niveau 1 »	Actif « Niveau 2 »	Actif « Niveau 3 »
Hardware	Serveurs	Serveurs+	Serveurs++ Serveur Web++
	Equipement utilisateur	Poste de travail+	Poste de travail++ Poste de travail admin++
		Smartphone+	Smartphone++
		Equipement personnel (BYOD)+	Equipement personnel (BYOD)++
	Média amovible	Média amovible+	Média amovible++ Document numérique/papier++
	Equipement Réseau	Equipement Réseau+	Equipement Réseau++ Proxy++
		Firewall+	Firewall++
Software	Application métier/Logiciel	Application métier/Logiciel+	Application métier/Logiciel++ Base de données++ Système d'exploitation++ Outils de développement ++
	Messagerie	Messagerie+	Messagerie++
	Outils communication	Outils communication+	Outils communication++
Personnel	Utilisateur	Utilisateur+	Utilisateur++ Développeur++
		Administrateur+	Administrateur++

Asset Type	Actif « Niveau 1 »	Actif « Niveau 2 »	Actif « Niveau 3 »
Information Security Governance	Organisation informatique	Organisation informatique+	Organisation informatique++ Développements logiciels++ Backup++
Outsourced Services	Service externalisé	Service externalisé+	Service externalisé++
		Fournisseurs+	Fournisseurs++
Network	Réseau et télécommunication	Réseau et télécommunication+	Internet++ Réseau Wifi++ VPN++
		Intranet+	Intranet++
Site	Infrastructure Physique	Infrastructure Physique+	Salle de serveurs++ Salle des archives++ Datacenter++
System	(System)	(System)	Système de supervision++ Système de sécurité physique++ Système monitoring de la sécurité++