Gestion des risques

**1. Objet**

**1.1 Finalité**

**1.2 Domaine d'application**

**1.3 Glossaire**

**2. Responsabilité**

**3. Documents**

**4. Exigences des normes**

**4.1 Exigences de la norme ISO 31000 version 2018**

**4.2 Exigences de la norme ISO 27001 version 2022**

**5. Déroulement**

**5.1 Planification**

**5.1.1 Généralités**

**5.1.2 Ressources**

**5.1.3 Communication interne**

**5.1.4 Communication externe**

**5.2 Contexte**

**5.3 Identification**

**5.4 Analyse**

**5.5 Évaluation**

**5.6 Traitement**

**5.7 Surveillance**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2023 |
| **Page** | **Changement** | **Date** |

**1. Objet**

**1.1 Finalité**

La présente procédure a pour objet de définir les règles d’identification, d’analyse, d’évaluation et de réduction des risques. L’objectif est d’augmenter la performance globale de l’organisation en se concentrant sur son cœur de métier et non sur les situations d’urgence.

**1.2 Domaine d'application**

Nous n’oublions pas que le risque zéro n’existe pas et que toute activité inclut des risques liés à :

* la sécurité de l’information
* la sécurité des processus
* la satisfaction du client
* la maîtrise des documents
* l’analyse de données
* la compétence du personnel (formation inadéquate)
* la dégradation de l’image de l’organisation

Les enjeux externes et internes pertinents pour le SMSI et les actions face aux risques identifiés et opportunités d’améliorations trouvées sont pris en compte.

**1.3 Glossaire**

SMSI – système de management de la sécurité de l’information

Risque – vraisemblance d’apparition d’une menace ou d’une opportunité

AMDEC - analyse des modes de défaillance, de leurs effets et de leur criticité.

**2. Responsabilité**

La direction à son plus haut niveau a la responsabilité de veiller à la stricte application de cette procédure conformément à la politique de gestion des risques de l’organisation. Tout chef de projet, comme pilote du risque, est responsable de la gestion des risques de son produit ou processus. Chaque département de l’organisation contribue au traitement (à la réduction) des risques identifiés.

**3. Documents**

Registre des incidents

Liste des risques

Plan de traitement des risques

Plan d’atteinte des objectifs

**4. Exigences des normes**

**4.1 Exigences de la norme ISO 31000 version 2019**

§ 6.4 Appréciation du risque

§ 6.5 Traitement du risque

**4.2 Exigences de la norme ISO 27001 version 2022**

§ 6.1 Actions face aux risques

§ 6.2 Objectifs

§ 8.1 Planification et maîtrise

§ 8.2 Appréciation des risques

§ 8.3 Traitement des risques

**5. Déroulement**

**5.1 Planification**

**5.1.1 Généralités**

L’implication de la direction est une condition incontournable pour le succès du projet de gestion des risques.

Sur la base des informations et documents existants, la planification du projet est mise en route. Le processus de gestion des risques fait partie du système de management global de l’organisation et est adapté à nos spécificités.

Les objectifs annuels d’identification, d’analyse, d’évaluation et de traitement des risques sont fixés. Les personnes responsables, les rôles et les délais sont établis, enregistrés et communiqués (cf. Plan de traitement des risques).

Une évaluation de la conformité des processus de notre organisation aux exigences légales applicables est réalisée par le responsable sécurité de l’information.

**5.1.2 Ressources**

La direction planifie et assure les ressources nécessaires à chaque étape des activités liées à la gestion des risques.

La formation, les connaissances, les compétences et l’expérience du personnel sont déterminantes.

Dans les ressources sont incluses les méthodes, le processus, la documentation et les équipements utilisés.

**5.1.3 Communication interne**

La communication et la concertation en interne des informations sur les activités de gestion des risques sont enregistrées dans les rapports internes.

## Les rapports aident le personnel à comprendre l’appréciation et le traitement des risques.

Pour chaque risque identifié comme non acceptable une mesure de maîtrise est choisie (cf. Plan d’atteinte des objectifs).

**5.1.4 Communication externe**

## La communication et la concertation en externe des informations sur les activités de gestion des risques sont enregistrées dans les rapports externes avec la participation active des parties intéressées (retour d’information, consultation, plan d’urgence).

**5.2 Contexte**

Pour établir le contexte externe, avant tout, nous prenons en compte la satisfaction des exigences des parties intéressées externes.

Pour établir le contexte interne nous prenons en compte surtout la stratégie et notre culture d’entreprise, la politique, les objectifs de gestion des risques, les aptitudes et perceptions du personnel.

Les ressources nécessaires sont établies et assurées (cf. paragraphe 5.1.2).

Les activités du processus « gérer les risques » sont déterminées (cf. paragraphes 5.3 à 5.7).

Les critères de risque sont déterminés :

* types de causes
* types de conséquences
* méthode de mesures
* vraisemblance (probabilité) d’apparition des effets
* niveau du risque acceptable
* combinaison de plusieurs risques

**5.3 Identification**

La liste de tous les risques identifiés (potentiels et réels) est enregistrée et mise à jour au moins deux fois par an (cf. le fichier Liste des risques).

La participation active de tous est indispensable car c’est le personnel sur le terrain qui connaît le mieux les situations réelles et potentiellement dangereuses.

Cette liste est le résultat du travail de l’équipe pluridisciplinaire ayant passée en revue les sources, causes, impacts, effets et conséquences des risques pouvant apparaitre dans notre organisation.

**5.4 Analyse**

Déterminer les causes et les conséquences des risques nous permet de rassembler les données nécessaires pour évaluer les risques (cf. paragraphe 5.5) et prendre les décisions de traitement des risques (cf. paragraphe 5.6).

Une méthode d’analyse des risques utilisée est l’AMDEC – analyse des modes de défaillance, de leurs effets et de leur criticité. Cette analyse nous permet d’identifier et d’évaluer les défaillances potentielles et d’éliminer ou réduire les risques associés avec des actions appropriées. L’AMDEC est utilisée par le département sécurité de l’information pour analyser les risques aux différents niveaux de l’organisation.

Nous utilisons le tableau suivant pour déterminer la vraisemblance d’apparition d’un risque :

|  |  |  |
| --- | --- | --- |
| Vraisemblance d’apparition (A) | | |
|  | Détection | Fréquence |
| 1 | Improbable | N’est jamais arrivé |
| 2 | Très faible | Une fois par an |
| 3 | Faible | Quelques fois par an |
| 4 | Probable | Une fois par mois |
| 5 | Forte | Une fois par semaine |

Nous utilisons le tableau suivant pour déterminer la gravité des impacts d’un risque :

|  |  |  |
| --- | --- | --- |
| Gravité des impacts (I) | | |
|  | **Degré** | Impact |
| 1 | **Minimal** | Négligeable |
| 2 | **Mineur** | Faible |
| 3 | **Modéré** | Modéré |
| 4 | **Majeur** | Elevé |
| 5 | **Sévère** | Critique |

Chaque risque est quantifié quant à sa vraisemblance d’apparition (A) et la gravité des impacts (I) qu’il peut exercer. Le niveau de risque (N) est le résultat de la multiplication de l’apparition par l’impact :

N = A x I

Dans certains cas on peut ajouter des facteurs comme le temps d’exposition au danger (risque multiplié) et la difficulté de détection du risque.

**5.5 Évaluation**

Nous classons les risques d’après leur niveau en trois catégories (cf. figure niveau des risques) :

* **acceptables (1 ÷ 4) - vert**
* **inacceptables (5 ÷ 9) - jaune**
* **intolérables (10 ÷ 25) -** rouge

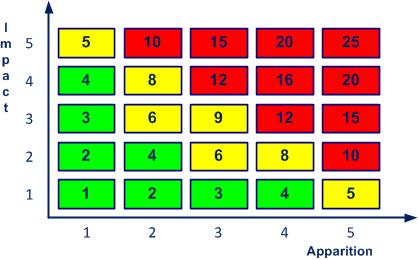


Figure niveau des risques

Cela nous permet de prendre des décisions sur la priorité et la mise en place des mesures de maîtrise pour traiter les risques (cf. paragraphe 5.6).

Les conséquences financières jouent un rôle important dans l'évaluation des risques et la décision de mise en place des actions.

L'évaluation des risques nous permet de déterminer quand un risque est acceptable et peut être toléré par le pilote du risque (niveau de 1 à 4). Selon l’importance du risque, les moyens de maîtrise existants restent inchangés.

Pour un niveau de risque inacceptable (niveau de 5 à 9) nous cherchons des opportunités de maîtrise équilibrées avec des coûts raisonnables et réalistes (rapport bénéfice/risque).

Quand le niveau de risque est intolérable (niveau supérieur à 10) le traitement du risque est incontournable, quel que soit son coût.

Les mesures de maîtrise pour traiter les risques inacceptables et intolérables respectent les exigences légales applicables auxquelles notre organisation a souscrit.

L’évaluation des risques repose sur :

* la revue des données
* le rapport bénéfice/risque
* la participation des parties intéressées
* la prise en compte du pire cas (limites extrêmes)

**5.6 Traitement**

Quand les risques potentiels ou réels sont inacceptables ou intolérables ils sont réduits, évités ou transférés.

La priorité des actions est menée sur les risques avec le niveau le plus élevé.

Quand la source du risque est identifiée nos efforts sont dirigés vers l’élimination de la source.

Le traitement des risques est évalué en vérifiant si les risques résiduels sont tolérables et en passant en revue l’efficacité des mesures de maîtrise.

Une comparaison est réalisée sur l’impact financier de la mise en place et la non mise en place de chaque mesure de maîtrise. Après cette analyse des coûts, les mesures de maîtrise sont sélectionnées et les responsabilités sont attribuées.

Les actions de traitement des risques sont régulières et sont décrites dans les plans de traitement. Chaque plan est enregistré, daté, vérifié et validé par la personne désignée par la direction (cf. descriptions de fonction).

Une combinaison de plusieurs options de traitement des risques est souvent utilisée.

La communication et la concertation avec les parties intéressées lors du choix des options de traitement d’un risque est une garantie qu’un nouveau risque ne va pas être créé suite au traitement de l’ancien risque.

**5.7 Surveillance**

Le but est de vérifier la pertinence de l’analyse, l’efficacité des moyens de maîtrises mis en place et le niveau des risques résiduels.

Les personnes responsables des risques (cf. descriptions de fonction) assurent régulièrement la surveillance.

Les retours d’information (incidents, réclamations, résultats des actions correctives) sont la base de données pour piloter l’amélioration continue, cf. le Registre des incidents.

Les enregistrements de la surveillance sont conservés dans les rapports et sont un élément d’entrée de la revue de direction.

Les données obtenues après la vente des produits nous permettent :

* d’identifier de nouveaux risques comme utilisation non-prévue
* d’actualiser l’analyse, l’évaluation et le traitement des risques
* d’actualiser le rapport bénéfice/risque
* d’améliorer le processus de gestion des risques