RISK ASSESSMENT &

RISK TREATMENT

*Connaissez les risques pour votre entreprise...*

Document : Historique

**Historique des versions du document**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Dates** | **Modifié par** | **Articles modifiés (V +1)** |
| **xxx** | **xxx** | **xxx** | **xxx** |
| **…** |  |  |  |

**Historique des validations**

|  |  |  |
| --- | --- | --- |
| **Nom** | **Fonction** | **Date de la validation par le plus haut niveau de direction** |
| **xxx** | **xxx** | **xxx** |
| **…** |  |  |

Le présent document s’applique à compter du **[date].**

Ce document est conservé comme suit :

1. Sur papier, aux endroits suivants : **[Indiquer les lieux]**.
2. Sous forme numérique aux endroits suivants : **[localisation sur l’intranet, par exemple]**.

Le titulaire de ce document est [fonction]. Il vérifie au moins 1 fois par an si des mises à jour sont nécessaires

TABLE DES MATIERES

[Document : Historique 2](#_Toc57732449)

[Historique des versions du document 2](#_Toc57732450)

[Historique des validations 2](#_Toc57732451)

[Chapitre I. Objectif du document 4](#_Toc57732452)

[Chapitre II. **RISK ASSESSMENT** 5](#_Toc57732454)

[Étape 0 : Placez un pilote dans l'avion 6](#_Toc57732456)

[2.1 Identifier les risques 7](#_Toc57732457)

[Étape 1 : Identifiez les types de ressources 7](#_Toc57732458)

[Étape 2 : Identifiez les ressources pertinentes 7](#_Toc57732459)

[Étape 3 : Déterminez qui est le « resource owner » . 7](#_Toc57732460)

[2.2 Analyser les risques 8](#_Toc57732461)

[Étape 4 : Identifiez les menaces 8](#_Toc57732462)

[Étape 5 : Identifiez les vulnérabilités 8](#_Toc57732463)

[Étape 6 : Identifiez les points de contrôle 8](#_Toc57732464)

[Étape 7 : Déterminez qui est le « Risk owner » 9](#_Toc57732465)

[2.3 Évaluer les risques 10](#_Toc57732466)

[Étape 8 : Déterminez l’impact éventuel 10](#_Toc57732467)

[Étape 9 : Déterminez la probabilité 11](#_Toc57732468)

[Étape 10 : Déterminez le niveau de risque 11](#_Toc57732469)

[Chapitre III. **RISK TREATMENT** 13](#_Toc57732470)

[Étape 1 : Collectez les informations sur les risques à traiter 14](#_Toc57732472)

[Étape 2 : Gérer les risques 14](#_Toc57732473)

[Étape 3 : Déterminez le risque résiduel 14](#_Toc57732474)

[Chapitre IV. Vocabulaire 16](#_Toc57732475)

[Chapitre V. Annexes 18](#_Toc57732476)

[**5.1.** **Annexe 1 : Tableau Impact Score - éditable** 18](#_Toc57732477)

[**5.2.** **Annexe 2 : Tableau score de probabilité - éditable** 19](#_Toc57732478)

[**5.3.** **Annexe 3 : Tableau Score risque - éditable** 20](#_Toc57732479)

**Chapitre I.**Objectif du document

**Chaque entreprise est différente** : selon le secteur, ses activités spécifiques, ses clients, ses fournisseurs … Ces différences entraînent également **des vulnérabilités et des risques spécifiques**.

Autant que possible, il est important, de connaître **vos risques au préalable**, afin de pouvoir déterminer les mesures préventives (avant tout incident) et curatives (pendant un incident) nécessaires en vue de vous assurer que votre entreprise puisse continuer à fonctionner au mieux même en cas d’urgence.

Ce document vous aide, en quelques étapes, à identifier, analyser et **évaluer vos risques ( Chapitre II. Risk Assessment)** et ensuite à **prendre les mesures nécessaires pour les traiter (Chapitre III. Risk Treatment).**

N’oubliez pas que les risques évoluent constamment et que votre entreprise doit donc également continuer à s’adapter. Veillez à **actualiser régulièrement** (au moins une fois par an) votre « Risk Assessment » (Évaluation des risques) et votre « Risk Treatment » (Gestion des risques) et à faire de ces plans un processus itératif (répétitif). Soyez rassuré : la « première fois » demande beaucoup de travail, ce sera ensuite beaucoup plus rapide !

### Que faut-il entrendre par « Risque » ?

Le risque est la possibilité qu’une menace

(interne ou externe) tire profit d'une

vulnérabilité (une erreur, un point sensible) dans votre entreprise et vous cause des

dommages (impact).

Chapitre II.   
RISK ASSESSMENT

Un Risk Assessment comporte 3 volets :

1. **Identifier** les risques (étapes 1 - 3)
2. **Analyse**r les risques (étapes 4 - 7)
3. **Evaluer** les risques (étapes 8 - 10)

Dès que le Risk Assessment est terminé, il s'agit de traiter les risques (voir Chapitre III. Risk Treatment (Gestion des risques)).

Utilisez ce document avec le   
« tableau Risk Assessment » que vous trouverez dans le toolkit.

### Comment réaliser un Risk Assessment ?

### Étape 0 : Placez un pilote dans l'avion

* Le Risk Assessment est coordonné par **[fonction]**.

Il est préférable que la direction de l’entreprise désigne **une seule personne (leader)** pour assurer la gestion de l’ensemble du Risk Assessment même si une équipe peut soutenir cette personne. Le gestionnaire du Risk Assessment **coordonne et consulte** le cas échéant les services internes concernés et **rapporte** régulièrement à la direction de l’entreprise.

* L'identification des menaces et vulnérabilités est réalisée, en collaboration avec le gestionnaire du Risk Assessment par les gestionnaires des ressources (Resource owner).
* L'évaluation de l'impact et de la probabilité est réalisée par le gestionnaire de risques. (Risk owners).

*Rem. : dans les petites entreprises, la direction réalise parfois elle-même le Risk Assessment. Pensez également à inventorier vos procédures existantes : certaines d’entre elles pourront vous aider à remplir le fichier Excel « Risk Assessment ».*

## 2.1 Identifier les risques

À l’aide du document « *Template Risk Assessment table.xlsx »*, nous établissons une **liste des principaux "assets**" également appelés **"ressources"** (ou actifs) au sein de votre entreprise et nous attribuons à chacun d’entre eux un « owner » (gestionnaire).

Étape 1 : Identifiez les types de ressources

**Remplissez la colonne B du tableau Risk Assessment.**

La première étape consiste à répertorier **toutes les « ressources » importantes** de l’entreprise. Il s’agit d’éléments - de nature matérielle ou immatérielle – qui s’avèrent précieux pour votre entreprise et son fonctionnement. **Sélectionnez les catégories pertinentes dans le menu déroulant de la colonne B** ou ajoutez des catégories supplémentaires via l’onglet 2. Pour vous aider, les catégories suivantes sont déjà prévues dans l’onglet :

1. Personnes (travailleurs, direction…)
2. Infrastructure (bureau, entrepôts…)
3. Technologie (ordinateurs, lignes téléphoniques…)
4. Informations et documentation   
   (back-ups, archives…)
5. Tiers (fournisseurs, clients...)

N’hésitez pas à ajouter des catégories spécifiques à la situation de votre entreprise.

Étape 2 : Identifiez les ressources pertinentes

**Remplissez la colonne C du tableau Risk Assessment.**

Dans la colonne C, spécifiez par catégorie **les « ressources » importantes pour votre entreprise.** Pour ce faire, utilisez à nouveau le menu déroulant ou ajoutez des catégories supplémentaires via l’onglet 2.

*Par exemple : dans les types de sources (B), vous avez sélectionné la source « Technologie ». Le menu déroulant de la colonne C vous propose différentes sources, parmi lesquelles vous sélectionnez par exemple « Serveurs ».*

Étape 3 : Déterminez qui est le « resource owner » (Gestionnaire de la ressource).

**Complétez la colonne D du tableau Risk Assessment.**

Un « Resource owner » (gestionnaire de la ressource) est **la personne en charge de la gestion quotidienne** de cette ressource.

*Par exemple, si vous avez sélectionné la source « serveurs » (colonne C) dans la catégorie « Technologie » (colonne B), vous pouvez à présent désigner dans la colonne « Resource owner » (D) un membre du département IT possédant les compétences adéquates et qui gère quotidiennement les serveurs (par ex compte administrateur IT).*

## 2.2 Analyser les risques

Maintenant que tous les assets ou « ressources » sont connus, vous pouvez identifier les menaces (étape 4) et les vulnérabilités (étape 5) qui y sont associées, réfléchir aux procédures (étape 6) existantes au sein de votre entreprise et aux « risk owners » (étape 7) responsables de leur gestion.

Étape 4 : Identifiez les menaces

**Remplissez la colonne du tableau Risk Assessment.**

Les menaces peuvent avoir différentes causes, par exemple les éléments naturels (inondation, incendie, tempête…) ou des hackers, des terroristes, de l’espionnage industriel…

Attention : une même ressource peut faire l’objet de plusieurs menaces ! *Ainsi, dans l’exemple, les serveurs peuvent être menacés non seulement par une inondation, mais aussi par un incendie, par des hackers…*

Les étapes suivantes (vulnérabilités, procédures existantes, impact…) peuvent être fort différentes. Utilisez donc une nouvelle ligne et essayez de ne pas tout ajouter ensemble !

Via le menu déroulant, vous pouvez déjà sélectionner plusieurs exemples. Vous pouvez bien sûr à nouveau ajouter vos propres éléments, via l’onglet 3 au bas du document.

Étape 5 : Identifiez les vulnérabilités

**Remplissez la colonne F du tableau Risk Assessment.**

Via le menu déroulant, vous pouvez accéder à une liste des vulnérabilités éventuelles. Vous pouvez également ajouter vos propres éléments, via l’onglet 4 au bas du document.

*Par exemple : vos serveurs peuvent se trouver dans une zone inondable et être situés sous le niveau de l’eau. Vous pouvez sélectionner « site sensible aux catastrophes naturelles ».*

Étape 6 : Identifiez les points de contrôle

**Remplissez si possible la colonne G du tableau Risk Assessment.**

Chaque fois qu’un risque est identifié, il doit être traité (Risk Treatment). Chaque décision de traitement peut constituer un point de contrôle.

*Par exemple : vous pouvez avoir prévu une « procédure en cas d’inondation » spécifique, comportant un point spécifique relatif à vos serveurs.*

*Par exemple : vous avez transféré vos risques relatifs aux services cloud à une partie externe. Vous ne vous en chargez donc pas personnellement. Votre point de contrôle consiste donc ici à vérifier régulièrement que tout fonctionne toujours comme souhaité et que votre fournisseur cloud répond aux exigences stipulées dans le contrat que vous avez conclu ensemble (disponibilité, qualité…)*

La colonne G ne propose pas de menu déroulant, car le choix des contrôles dépend de la gestion.

Étape 7 : Déterminez qui est le « Risk owner »

**Remplissez la colonne H du tableau Risk Assessment.**

Pour chaque risque, désignez une personne au sein de l’entreprise **compétente pour la gestion de ce risque.** Attention : bien que, dans les organisations de petite taille, le Resource Owner et le Risk Owner puissent être une seule et même personne, ce n’est pas toujours le cas !

*Exemple : le « Resource owner » des serveurs peut être un membre du département IT qui dispose des compétences privilégiées (compte de gestionnaire) et qui gère quotidiennement les serveurs. Par contre, le « Risk owner» est p. ex. le responsable du département IT qui est capable d’identifier de manière transversale les risques, ou qui pourrait offrir une formation spécifique au « propriétaire de la ressource », ou encore qui pourrait proposer à la direction d’améliorer la sécurité, etc.*

## 2.3 Évaluer les risques

Il s’agit à présent d’évaluer les risques, c’est-à-dire d’estimer l’impact que le risque pourrait avoir, s’il survenait, sur votre entreprise (étape 8) et d’estimer la probabilité que le risque survienne (étape 9).

Sur cette base, le niveau de risque est automatiquement calculé (étape 10) et réparti dans des catégories focus qui vous aident à vous concentrer sur les principaux risques. Les matrices proposées sont toujours indicatives et peuvent être adaptées aux besoins de l’organisation (voir annexes)

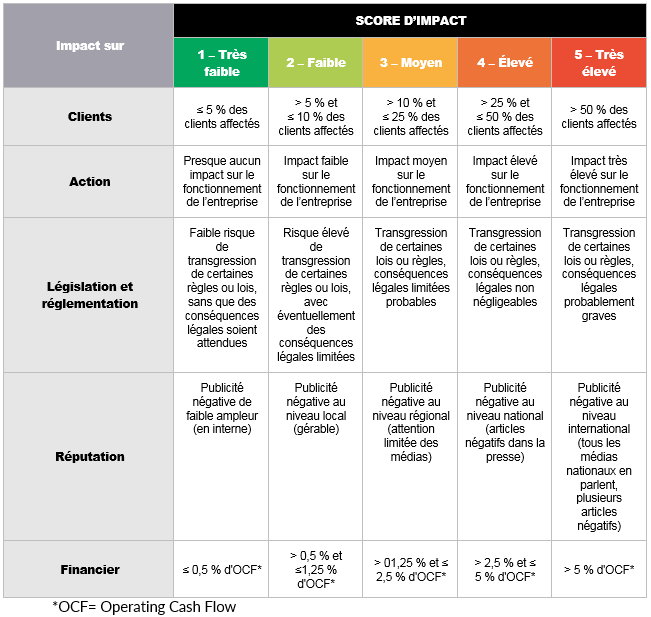
Étape 8 : Déterminez l’impact éventuel

**Remplissez les colonnes I à M**

Évaluez l’impact sur chaque aspect selon le tableau ci-dessus, de 1 (très faible) à 5 (très élevé).

* Colonne I : impact sur vos clients
* Colonne J : impact sur vos activités principales
* Colonne K : conséquences pour vos obligations légales
* Colonne L : influence sur la réputation de votre entreprise
* Colonne M : conséquences financières pour votre entreprise

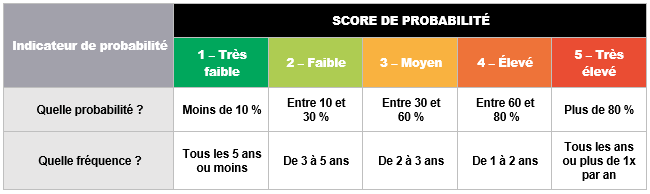
L’**impact total** est automatiquement calculé dans la **colonne N** sur base de la moyenne des scores des colonnes I à M. Le tableau ci-après vous propose une grille de lecture, vous pouvez modifier les critères via le tableau figurant en annexe (Chapitre V, 5.1 Annexe 1).



Étape 9 : Déterminez la probabilité

**Remplissez la colonne O du tableau Risk Assessment.**

La gravité, mais aussi la probabilité **qu’un problème déterminé survienne réellement** doivent être évaluées le mieux possible afin de déterminer l'« acceptabilité » du risque. Le tableau ci-dessous vous aide à attribuer **un score** à cette probabilité, **entre 1 (très faible) et 5 (très élevé).**

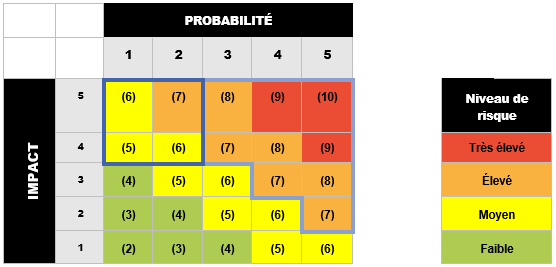
Le tableau ci-après vous propose une grille de lecture, vous pouvez modifier les critères via le tableau figurant en annexe (Chapitre V, 5.2 Annexe 2).

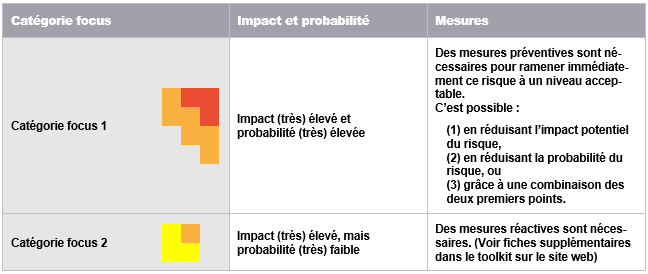
Étape 10 : **DÉTERMINEZ LE NIVEAU DE RISQUE**

**Les scores sont automatiquement calculés dans la colonne P du tableau Risk Assessment.**

La combinaison du score d’impact et du score de probabilité vous indique si un risque est « acceptable » ou non. Cela **déterminera comment vous devez gérer chacun de ces risques**. La matrice ci-dessous en offre une restitution visuelle.

Le tableau ci-après vous propose une grille de lecture, vous pouvez modifier les critères via le tableau figurant en annexe (Chapitre V, 5.3 Annexe 3).



Les risques **inacceptables** **doivent être traités en priorité**. Nous portons une attention particulière sur les 2 catégories de risques les plus élevés regroupés en 2 "catégories focus" :

Tous les autres risques peuvent être qualifiés d’acceptables, à moins que vous n’en décidiez autrement en tant qu’entreprise.

**Les catégories focus sont automatiquement calculées dans la colonne Q du tableau Risk Assessment.**

**ATTENTION : Un Risk Assessment est un processus itératif (répétitif) !**

Vous devez maintenant traiter les (principaux) risques identifiés (voir chapitre 3 : Risk Treatment), puis régulièrement adapter vos Risk Assessment et Risk Treatment**.**

**Faites-le au moins une fois par an** et toujours dans les cas suivants :

* Changements importants au sein de l’entreprise ;
* Changements importants dans l’environnement (in)direct de l’entreprise ;
* Changements importants d’ordre technologique (nouveau logiciel, nouvelles machines) ;
* Grands changements dans le personnel ;
* Changements législatifs importants (p. ex. RGPD) ;
* Changements des objectifs de l’entreprise ;
* Leçons tirées d’un indicent ou d’une crise ;
* Leçons tirées d’un test ;
* Etc.

# Chapitre III. RISK TREATMENT

## Gérer les risques

Le Risk Treatment est un processus au cours duquel votre entreprise précise comment elle va gérer ses risques :

1. **Accepter** le risque
2. **Réduire** le risque
3. **Transférer** le risque
4. **Éviter** le risque

Notez tous les risques importants pour l’entreprise dans le document « Tableau Risk Treatment ». Vous avez ensuite le choix entre un ou plusieurs traitements :

1. **Accepter** le risque : la direction peut considérer certains risques comme acceptables, p. ex. en cas de dommages (impact) négligeables. Toutefois, ce qui est considéré comme « acceptable » ou non doit être clairement identifié ;
2. **Réduire** le risque : réduire l’impact ou la probabilité des risques en prenant des mesures afin d’éviter et/ou de gérer ces risques ;
3. **Transférer** le risque : p. ex. en souscrivant une assurance spécifique ou p. ex. en sous-traitant certains services à des tiers (p. ex. services cloud) ;
4. **Éviter** le risque : si un risque est élevé, mais si les mesures permettant de le réduire ou de le transférer sont trop coûteuses ou trop complexes, il peut être décidé d’éviter le risque en choisissant de ne pas/plus exercer l’activité qui lui est associée.

Il est parfaitement possible qu’un certain niveau de risque subsiste même après un Risk Treatment : il s’agit du *risque résiduel*.

Déterminez **comment votre entreprise abordera concrètement ses risques en commençant par les risques relevant des deux catégories focus (1 et 2)** c'est à dire en commençant par les risques les plus élevés.

**utilisez ce chapitre avec le fichier**   
« risk treatment table.xlsx » que vous trouverez dans le toolkit.

Sur la base du Risk Assessment précédemment réalisé, établissez **un Risk Treatment en 3 étapes**.

Étape 1 : Collectez les informations sur les risques à traiter

Lors de cette phase, l’objectif consiste à recueillir des informations sur le risque initial qui doit être abordé. Il s’agit donc du risque **AVANT** exécution d’un (nouveau) traitement. **Tous les risques de niveau ÉLEVÉ à TRÈS ÉLEVÉ** doivent passer par la phase de Risk Treatment. Remarque : la direction de l’entreprise peut décider d’inclure également les risques dotés d’un score inférieur.

**Remplissez les colonnes B à K. Vous pouvez simplement reprendre ces données telles que mentionnées dans le document « Risk Assessment Table.xlsx ». Soyez rassuré : le plus gros du travail est déjà fait, remplir le tableau Risk Treatment sera beaucoup plus rapide !**

|  |  |  |
| --- | --- | --- |
| Colonne  Risk Assessment |  | Colonne  Risk Treatment |
| C | 🡺 | B |
| D | 🡺 | C |
| E | 🡺 | D |
| F | 🡺 | E |
| G | 🡺 | F |
| H | 🡺 | G |
| N | 🡺 | H |
| O | 🡺 | I |
| P | 🡺 | J |
| Q | 🡺 | K |

Étape 2 : Gérer les risques

La prochaine étape consiste, pour chaque risque, à **déterminer comment votre organisation va le gérer**.

Pour chaque risque, sélectionnez une option dans le menu déroulant de la colonne L :

* Accepter un risque
* Réduire un risque
* Transférer un risque
* Éviter un risque

Ajoutez ensuite dans la colonne M une **brève explication** du choix opéré et faites si possible référence à des documents corroborant cette décision, p. ex. un rapport du comité de direction ou un contrat d’assurance couvrant ce risque.

**Remplissez les colonnes L et M du tableau Risk Treatment**

Étape 3 : Déterminez le risque résiduel

**APRÈS** que votre entreprise ait pris des mesures pour traiter les risques, il reste encore dans certains cas un **« risque résiduel ». Vous pouvez à nouveau l’évaluer** selon la même technique.

Les tableaux des étapes 8 à 10 incluses du Risk Assessment peuvent vous y aider.

Les mesures ont-elles réduit l’impact sur votre entreprise ? La probabilité est-elle moindre ?

**Remplissez les colonnes N (Impact 2) et O (Probabilité 2) du tableau Risk Treatment. Les valeurs des colonnes P (= Risque 2) et Q (Focus 2) sont automatiquement calculées.**

*Conseil : réévaluez ce document au moins 1x par an afin de veiller à ce que les mesures prises continuent à répondre à la situation actualisée.*

# Chapitre IV. Vocabulaire

| Terme | Définition |
| --- | --- |
| Impact | Résultat d’un événement qui influence les objectifs de l’entreprise |
| Menace | Tout événement prévisible ou imprévisible susceptible d’affecter les actifs de l’entreprise. Les menaces peuvent être d’origine naturelle (incendie, inondation...), humaine (erreur, dommage intentionnel...) |
| Niveau de risque | Importance d’un risque ou d’une combinaison de risques, mesurée au moyen de la combinaison de l’impact (ou conséquence) et de la probabilité. |
| Probabilité | Le risque qu’un événement survienne |
| Propriétaire du risque | Personne ou entité compétente pour gérer un risque. |
| Ressources | L’ensemble des actifs, personnes, compétences, informations (électroniques ou non), technologies (installations et appareils inclus), bâtiments et stocks dont une organisation doit pouvoir disposer pour pouvoir travailler et atteindre son objectif. |
| Resource owner (propriétaire de la ressource) | Personne ou entité compétente pour gérer les ressources. Il s’agit souvent de la direction elle-même ou d’une personne désignée par la direction à laquelle elle rapporte régulièrement. |
| Risk Assessment (Évaluation du risque) | Processus global rassemblant l’identification, l’analyse et l’évaluation des risques |
| Risk Treatment (Gestion du risque) | Efforts fournis par une organisation pour maîtriser les risques. |
| Risque | Élément susceptible d’avoir un effet incertain sur des objectifs.  Remarque 1 : Un effet est un écart par rapport à ce qui est attendu – il peut être tant positif que négatif.  Remarque 2 : Les objectifs peuvent avoir différents aspects (financiers, axés sur la santé, la sécurité et l’environnement) et peuvent être d’application à différents niveaux (stratégiques, au niveau de l’organisation, projet, produit et processus).  Remarque 3 : Le risque est souvent caractérisé par des événements et des conséquences potentiels, ou par une combinaison d’entre eux.  Remarque 4 : Le risque est souvent exprimé sous la forme d’une combinaison des conséquences d’un événement (y compris des changements de circonstances) et du risque qu’elles surviennent. |
| Risque résiduel | Le risque qui subsiste après Risk Treatment |
| Vulnérabilité | La vulnérabilité est le maillon faible d’une possession ou d’un groupe de possessions pouvant être exploité par un ou plusieurs dangers menaçants (erreur de développement, installation erronée) |

Chapitre V. Annexes

## 5.1. Annexe 1 : Tableau Impact Score - éditable

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impact sur | Score d’impact | | | | |
| 1 – Très faible | 2 – Faible | 3 – Moyen | 4 – Élevé | 5 – Très élevé |
| Clients | ≤ 5 % des clients affectés | > 5 % et ≤ 10 % des clients affectés | > 10 % et ≤ 25 % des clients affectés | > 25 % et ≤ 50 % des clients affectés | > 50 % des clients affectés |
| Action | Presque aucun impact sur le fonctionnement de l’entreprise | Impact faible sur le fonctionnement de l’entreprise | Impact moyen sur le fonctionnement de l’entreprise | Impact élevé sur le fonctionnement de l’entreprise | Impact très élevé sur le fonctionnement de l’entreprise |
| Législation et réglementation | Faible risque de transgression de certaines règles ou lois, sans que des conséquences légales soient attendues | Risque élevé de transgression de certaines règles ou lois, avec éventuellement des conséquences légales limitées | Transgression de certaines lois ou règles, conséquences légales limitées probables | Transgression de certaines lois ou règles, conséquences légales non négligeables | Transgression de certaines lois ou règles, conséquences légales probablement graves |
| Réputation | Publicité négative de faible ampleur (en interne) | Publicité négative au niveau local (gérable) | Publicité négative au niveau régional (attention limitée des médias) | Publicité négative au niveau national (articles négatifs dans la presse) | Publicité négative au niveau international (tous les médias nationaux en parlent, plusieurs articles négatifs) |
| Financier | ≤ 0,5 % d'OCF\* | > 0,5 % et ≤1,25 % d'OCF\* | > 01,25 % et ≤ 2,5 % d'OCF\* | > 2,5 % et ≤ 5 % d'OCF\* | > 5 % d'OCF\* |

\*OCF= Operating Cash Flow

5.2. Annexe 2 : Tableau score de probabilité - éditable

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Indicateur de probabilité | Score de probabilité | | | | |
| 1 – Très faible | 2 – Faible | 3 – Moyen | 4 – Élevé | 5 – Très élevé |
| Quelle probabilité ? | Moins de 10 % | Entre 10 et 30 % | Entre 30 et 60 % | Entre 60 et  80 % | Plus de 80 % |
| Quelle fréquence ? | Tous les 5 ans  ou moins | De 3 à 5 ans | De 2 à 3 ans | De 1 à 2 ans | Tous les ans ou plus de 1x par an |

5.3. Annexe 3 : Tableau Score risque - éditable

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | PROBABILITÉ | | | | |  |  |
|  |  | 1 | 2 | 3 | 4 | 5 |  | of risk |
| **IMPACT** | 5 | (6) | (7) | (8) | (9) | (10) |  | Niveau de risque | |
| 4 | (5) | (6) | (7) | (8) | (9) |  | Très élevé | |
| 3 | (4) | (5) | (6) | (7) | (8) |  | Élevé | |
| 2 | (3) | (4) | (5) | (6) | (7) |  | Moyen | |
| 1 | (2) | (3) | (4) | (5) | (6) |  | Faible | |

|  |  |  |  |
| --- | --- | --- | --- |
| Catégorie focus |  | Impact et probabilité | Mesures |
| Catégorie focus 1 | |  |  |  | | --- | --- | --- | |  |  |  | |  |  |  | |  |  |  | |  |  |  | | Impact (très) élevé et  probabilité (très) élevée | Des mesures préventives sont nécessaires pour ramener immédiatement ce risque à un niveau acceptable.  C’est possible :  (1) en réduisant l’impact potentiel du risque,  (2) en réduisant la probabilité du risque, ou  (3) grâce à une combinaison des deux premiers points. |
| Catégorie focus 2 | |  |  | | --- | --- | |  |  | |  |  | | Impact (très) élevé, mais  probabilité (très) faible | Des mesures réactives sont nécessaires. (Voir fiches supplémentaires dans le toolkit sur le site web) |