Fiche méthodologique
GOUVERNANCE

Pour livrable attendu
CARTOGRAPHIE DES RISQUES

Bonnes Pratiques de référence
9-28-31-32-33-48-49

SOMMAIRE

L'OBJECTIF

Rappel de l'objectif à atteindre :

- **Quoi ? l'objet :**

La Gestion des Risques a pour objectifs :

- D'identifier les risques relatifs aux activités de l'entité,
- De les caractériser,
- De construire et de mettre en œuvre les parades nécessaires :
  - Actions de prévention pour réduire la probabilité d'apparition,
  - Actions d'atténuation pour réduire les conséquences négatives en cas de survenance du risque considéré.
- La Cartographie des risques est l'outil de la Gestion des Risques. C'est le document dans lequel sont identifiés, évalués et hiérarchisés les risques auxquels l'organisme doit faire face.
- De manière générale, la cartographie des risques permet d'une part d'avoir une vue globale et exhaustive des risques auxquels l'organisme est confronté tant à l'interne qu'à l'externe et d'autre part de définir des stratégies formelles afin de les gérer. Elle sert donc de base à la gestion des risques au sein de l'organisation, et en particulier, elle peut être utilisée comme point de départ à la structuration du dispositif de contrôle interne.

- **Pour Qui ? à qui s'adresse ce livrable :**

L'équipe de direction élue et salariée.
Toute personne qui sera en charge de maitriser un ou plusieurs risques.

- **Comment est-ce mis à disposition ?**

Une communication interne est élaborée.

Cela assure pour l'ensemble des équipes (bénévoles, volontaires et salariés) une connaissance des parades de maîtrise des risques et une implication dans leurs mises en œuvre (BP48).

Les partenaires externes de l'organisation sont informés des grandes lignes de sa politique de gestion des risques (BP49).

LE POURQUOI

- **Rappel des obligations légales (si applicable)**

En vertu de la loi Sapin II, du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, les entreprises d'au moins 500 salariés et ayant un chiffre d'affaire supérieur à 100 millions d'euros doivent disposer d' « Une cartographie des risques prenant la forme d'une documentation régulièrement actualisée et destinée à identifier, analyser et hiérarchiser les risques d'exposition de la société à des sollicitations externes aux fins de corruption, en fonction notamment des secteurs d'activités et des zones géographiques dans lesquels la société exerce son activité »

Note : le Document Unique d'Evaluation des Risques (DUER), est un document obligatoire à tenir par les entreprises qui embauchent du personnel salarié, quel que soit le nombre d'employés. L'évaluation des risques professionnels (EvRP) consiste à identifier les risques auxquels sont soumis les salariés d'un établissement, en vue de mettre en place des actions de prévention pertinentes couvrant les dimensions techniques, humaines et organisationnelles. Cette démarche de prévention en santé et sécurité au travail L'EvRP est une démarche dont les résultats sont formalisés dans le DUER. Le guide n'est pas mieux disant que le droit social sur ce point (voir BP 38).

.

COMMENT PROCEDER

Proposition de méthodologie :

- **Préalable**

Un **risque est un évènement incertain susceptible de se produire** et pouvant avoir, en cas d'apparition, des conséquences néfastes pour toute structure organisée, sur :

- l'atteinte des objectifs stratégiques,
- les actifs clefs,
- le bon déroulement de ses activités et missions sociales,
- les résultats financiers de l'organisme,
- son image auprès du public ou des bailleurs.

Il est important lors de l'identification des risques de faire la différence entre risque et dysfonctionnement.

- Un risque est par définition un évènement futur et incertain aux conséquences négatives. **L'organisme ne maîtrise pas la survenance de cet évènement**.

- Un dysfonctionnement est un évènement interne qui s'est déjà produit. C'est donc un problème actuel auquel il faut trouver et mettre en œuvre une solution pour le supprimer et améliorer ainsi le fonctionnement de l'organisme. **L'organisme sait maîtriser la non-survenance de cet évènement.**

Seuls les risques doivent être conservés dans la cartographie des risques. Les dysfonctionnements n'y ont pas leur place. Ils doivent rejoindre la liste des actions à mettre en place pour les supprimer.

Exemple de risque :

Changement de fiscalité pour le mécénat d'entreprises, entrainant la perte de financeurs et donc des difficultés financières importantes.

Exemple de dysfonctionnement :

Perte de donateurs qui n'ont pas obtenu leur reçu fiscal dans les temps, suite à de mauvais traitements dans la base de données donateurs.

- # Etape 1 : Identification des risques

EN AMONT

La réflexion de l'identification et l'évaluation des risques est une approche collective. Il faut donc :

- définir les acteurs de cette réflexion
- définir la méthode d'animation

On pourra envisager un brainstorming en plénière ou bien du travail en sous-groupes par spécialités (finance, RH, communication, informatique, etc.)

Afin de préparer au mieux la réunion de réflexion sur les risques, les personnes de l'organisme qui participeront à cette réflexion devront, avant la première réunion, trouver un peu de temps pour identifier les principaux risques déjà connus dans leur zone de responsabilité ou d'action.

IDENTIFICATION DES RISQUES

L'approche proposée consiste à travailler par domaines de risques et éventuellement sous-domaines. Le tableau ci-dessous peut servir de base :

Domaines de risques	Sous domaines
Stratégique	**- risques pays** **- concurrence** **- partenaires / prestataires** **- acquisitions/fusions/investissements** **- évolutions réglementaires** **- etc**
Financier	**-trésorerie/liquidité** **-taux d'intérêt** **-taux de change** **- ressources** **- fiscalité**
Conformité	**-veille réglementaire** **- RGPD** **- règlements spécifiques** **- autorités administratives**
Opérationnels	**- défaillance fournisseur/prestataire** **- risques opérationnels (à définir)** **- projets (coûts, délais, qualité)** **- sinistre** **- RH (erreur humaine, risque social, expatriés, ...)** **- personnes clés**
Informatique et cyber	**- disponibilité du service** **- intégrité des données** **- confidentialité de l'information**
Image/réputation	**- éthique non respectée** **- détournement de la marque** **- communication non maîtrisée**
Sanitaire	**- disponibilité des salariés et bénévole** **- interdiction totale ou partielle d'ouverture** **- pertes de partenaires, adhérents** **- pertes de financement**

Pour bien identifier un risque : Demandez-vous « Qu'est-ce qui pourrait m'arriver » ? ou bien « De quoi ai-je peur ? »

Pour bien formuler le risque pensez, dans la mesure du possible, à prendre en compte les trois éléments suivants :

1- La cause de l'événement

2- L'événement à proprement parler

3- Les conséquences sur l'organisation.

Exemple :

Evènement redouté	Cause	Conséquence
Perte de données sur le serveur central	Intrusion malveillante externe	Incapacité à reconstituer le listing des donateurs

Cette approche a 3 avantages :

- Le risque est identifié sans ambiguïté.
- La cause du risque permettra d'évaluer sa probabilité d'apparition
- Les conséquences permettront d'évaluer sa gravité

RECOMMANDATION :

- Se limiter aux risques "réalistes"
- Ne pas essayer d'être exhaustif (c'est impossible)

• Etape 2 : Validation des risques

COMMENT : séances de relecture.

Cette étape est importante. Elle permet de :

- S'assurer de la pertinence et de la justesse des formulations de risques.
- Supprimer de la liste les risques qui n'en seraient pas (les dysfonctionnements de l'organisation)

• Etape 3 : Évaluation et Hiérarchisation

QUOI : deux critères sont proposés pour « peser » le risque :

La probabilité de survenance,
L'impact en cas de survenance

Le niveau de Criticité du Risque est alors déduit : Criticité = Probabilité x Impact

Il existe différentes échelles de notation pour l'évaluation tant de la probabilité de survenance que de l'impact. Vous pouvez ainsi retenir :

- un système de notation à trois niveaux (3-élevé, 2-moyen, 1-faible)

OU

- un système à cinq niveaux (5-très élevé, 4-élevé, 3-moyen, 2-faible, 1-très faible).

Le choix du type de notation à utiliser dépend du niveau de détail souhaité dans l'analyse.

Il est aussi utile de se donner des critères pour guider la notation. Par exemple :

Pour la probabilité d'apparition :

1	de la connaissance des personnes consultées on a jamais vu ça.
2	On ne sait pas, on doute
3	Jamais vu, mais on pense que cela est possible
4	déjà vu une fois par certains
5	de la connaissance des personnes consultées tous ont vu au moins une fois

Pour la gravité :

1	aucune incidence sur le fonctionnement
2	incidences gérables en interne
3	incidences visibles à l'extérieur de l'organisme
4	des impacts visibles du grand public
5	les actions sont remises en cause, très visible du grand public

En général les impacts sont soit financiers, soit sur le fonctionnement, soit sur l'image de marque (réputation). Il peut être intéressant de définir 3 tables et retenir pour chaque risque le critère le plus important. Une proposition plus complète est à retrouver dans l'exemple fournit avec la fiche.

Il faut aussi définir si l'évaluation du risque sera réalisée sur le risque BRUT ou le risque NET.

Le **RISQUE BRUT** s'évalue indépendamment des parades déjà en place. C'est un risque intrinsèque.

Le **RISQUE NET** s'évalue en prenant en compte les parades déjà en place. C'est un risque résiduel qui dépend de l'efficacité estimée des parades existantes.

Il est recommandé de travailler à partir du risque BRUT et ainsi de faire figurer dans la cartographie des risques, les parades déjà en place. Elles feront ainsi naturellement partie du dispositif de gestion de risques.

• Etape. 4 : Traitements

La première décision à prendre est de décider le **seuil de criticité** nécessitant une attention.

- Tous les risques dont la criticité est en dessous de ce seuil seront considérés comme des risques assumés, donc sans parade à envisager (sauf si elles sont évidentes).

- Pour les risques dont la criticité est supérieure au seuil défini, des parades doivent être imaginées.

Les parades sont de deux types :

- La **Prévention** qui consiste à réduire la probabilité que l'événement redouté nous impacte. Cette méthode permet donc de diminuer la probabilité d'occurrence du risque en diminuant ou supprimant certains des facteurs de risque.

- L'**Atténuation** qui consiste à diminuer les conséquences potentielles de l'événement. Cette méthode permet donc de minimiser l'impact de l'événement lorsque l'on ne peut agir sur le facteur de risque lui-même, mais que l'on peut agir sur ses conséquences.

A noter que l'on peut aussi envisager de transférer le risque à une autre entité ou un prestataire spécialisé. C'est par exemple le cas des risques informatiques, pour lesquels les parades demandent des compétences très spécifiques et très pointues.

Dans ce cas, on devra cependant évaluer le risque résiduel et s'il est encore considéré comme élevé, imaginer des parades complémentaires pouvant être mises en œuvre localement. Par exemple des règles de bonne utilisation des mots de passe, des séances de sensibilisation aux risques, ….

Exemple de parade de type prévention :

Evènement redouté	cause	Parade préventive
Risque de détournement de fonds	Par l'émission de fausses commandes/factures	Séparation des fonctions engagement/paiement/comptabilisation
Perte de contenu internet	Cyber attaque	Hébergeur apportant un niveau de garantie compatible avec la sensibilité du contenu

Exemple de parade de type atténuation :

Evènement redouté	cause	Parade d'atténuation
Perte de données sensibles	Attaque malveillante du serveur	Procédure de sauvegarde périodique et sécurisée
Rumeur sur des dysfonctionnements internes du CA	Personne interne ou externe mal intentionnée	Communication interne Communiqué de presse
Absence prolongée et soudaine d'une personne clef	Accident	Manuel de procédures précis et personnes back-up définies sur les tâches sensibles

- **Etape. 5 : Finalisation de la cartographie**

Lorsque toutes les parades sont imaginées, il reste 3 éléments à compléter ligne à ligne dans le tableau.

1 – Définir la personne en charge de la mise en place de la parade.

2 – Définir le délai de mise œuvre.

3 – Indiquer si les parades doivent être intégrées dans le dispositif de contrôle interne (nouvelles règles à mettre en place et à intégrer dans les procédures opérationnelles).

Enfin, pour toutes les parades de type PCA (continuité d'activité en mode dégradé), définir le processus de gestion de crise et lancer la rédaction des procédures nécessaires pour chaque scénario envisagé (cf BP33) .

Au vu des parades envisagées, il peut être intéressant d'imaginer le risque résiduel et de le faire figurer en fin de tableau. Lors des mises à jour annuelles de la cartographie, ce risque résiduel sera alors régulièrement re-estimé en fonction de l'efficacité opérationnelle des parades et du dispositif de contrôle interne.

Le risque résiduel peut être associé à un indicateur de suivi de l'efficacité des parades. Par exemple, si la mesure préventive est de nature « formation », l'indicateur de suivi sera élaboré à partir de la comptabilisation des actions de formation.

LES FACTEURS DE SUCCÉS

Proposition de méthodologie :

1. Les prérequis :

Un comité de pilotage :

- Qui explique l'intérêt de la démarche,
- Qui identifie les participants,
- Qui se tient informé de l'avancement.

2. L'implication des acteurs :

Une implication de tous : la démarche d'analyse des risques concerne toutes les directions/ activités.
Désignation d'un animateur responsable.

3. Le choix des contributeurs :

La Gestion des Risques est une activité permanente des responsables des familles de risques.
Il faut donc des contributeurs pour chaque famille.

4. Le processus de validation :

La cartographie des risques fait l'objet d'une présentation en séance de l'organe collégial d'administration pour information et validation.

La communication interne sur la gestion des risques existe et est largement diffusée.

LES CRITÈRES DE QUALITÉ du Livrable Cartographie des Risques

La cartographie des risques est un des livrables du dossier nécessaire à la labellisation IDEAS.

Les grandes familles de risques sont présentes.

Les risques sont correctement formulés pour éviter tout malentendu.

La pesée des risques est effective.

Les responsables sont identifiés.

Les parades sont clairement documentées et pour celles qui sont à développer, une date de réalisation est indiquée.

Une procédure gestion de crise a été préparée pour le cas de survenance de risques pouvant engager la réputation de l'entité (cf focus thématique Gestion de crise).

Le comité spécialisé en charge de vérifier la qualité du contrôle interne (le comité d'audit), doit s'assurer régulièrement de l'actualité de la cartographie des risques (cf fiche de mission du comité d'audit).

La cartographie des risques a fait l'objet d'une présentation et d'une validation par l'OCA.

LES BONNES PRATIQUES DE REFERENCE

UN DISPOSITIF DE CONTROLE INTERNE STRUCTURE - G 2.2

Un dispositif de contrôle interne adapté, défini par l'organe collégial d'administration et audité par un comité spécialisé.

Bonne Pratique 9 : L'organe collégial d'administration définit un dispositif de contrôle interne :
- En cohérence avec les délégations de pouvoirs données,

- Et ayant pour mission de lui donner une assurance raisonnable que :

- Les activités sont menées dans le respect de ses valeurs et de sa mission sociale,
- **Les risques identifiés sont globalement maîtrisés**.

UN PLAN STRATÉGIQUE À MOYEN TERME

Un plan stratégique à moyen terme (3 – 5 ans).

Bonne Pratique 28 : Existence d'un document de planification stratégique.
Découlant du projet associatif, il s'organise en référence à la vision, la mission et les valeurs formulées dans le projet afin de tendre à sa réalisation,

- explicitant le modèle socio-économique sur lequel repose l'entité,
- incluant les thèmes de Responsabilité Sociétale et la référence aux objectifs de développement durable sur lesquels l'entité choisit de s'engager,
- **tenant compte des risques stratégiques, sectoriels et environnementaux propres à l'entité,**
- définissant des objectifs stratégiques, il les décline en projets opérationnels pour leur réalisation,
- il est établi en connaissance des attentes des parties prenantes pour :
  - l'identification des besoins,
  - l'élaboration (ou l'amélioration) des actions et les modalités de mise en œuvre,
  - initier la démarche de mesure d'impact.

UNE METHODOLOGIE ADAPTEE - G 5.1

Recensement et évaluation au moyen d'une cartographie périodiquement actualisée

Bonne Pratique 31 : L'entité élabore collaborativement et met à jour la liste des principaux risques auxquels elle est confrontée à court et moyen terme. Elle en évalue la criticité en termes d'impact et de probabilité. Lorsqu'aucun changement n'est intervenu, la mise à jour est effectuée au minimum tous les 3 ans.

ELABORATION D'UNE PROCEDURE DE GESTION DE CRISE - G 5.2

Politique active de prévention ou de maitrise des risques validée et suivie par l'organe collégial d'administration

Bonne Pratique 32 : L'entité met en œuvre les plans d'actions, les procédures internes et les contrôles aptes à prévenir les principaux risques identifiés et à en réduire leurs impacts.

Bonne Pratique 33 : L'entité élabore des **scénarii de gestion de crise** sur les risques majeurs auxquels elle est particulièrement exposée, et qui le nécessitent. Ils incluent **si nécessaire un volet « communication de crise ».**

UNE COMMUNICATION AUX PARTIES PRENANTES - G 8.1

La politique de gestion des risques fait l'objet :

- d'une communication interne

Bonne Pratique 48 : Une communication interne adaptée permet à l'ensemble des équipes (bénévoles, volontaires, salariés) d'être informé des actions de maîtrise des risques mises en œuvre avec leur concours.

- et d'une communication externe aux partenaires

Bonne Pratique 49 : Les partenaires de l'association sont informés des grandes lignes de sa politique de gestion des risques.