

CARTOGRAPHIE DES RISQUES DE L'ENTITE ET MATRICE DES RISQUES DE L'AUDITEUR.

La cartographie des risques d'une entité :

Le risque peut être défini comme tout événement dont la survenance porte atteinte à la capacité d'une structure à atteindre ses objectifs.

On distingue traditionnellement :

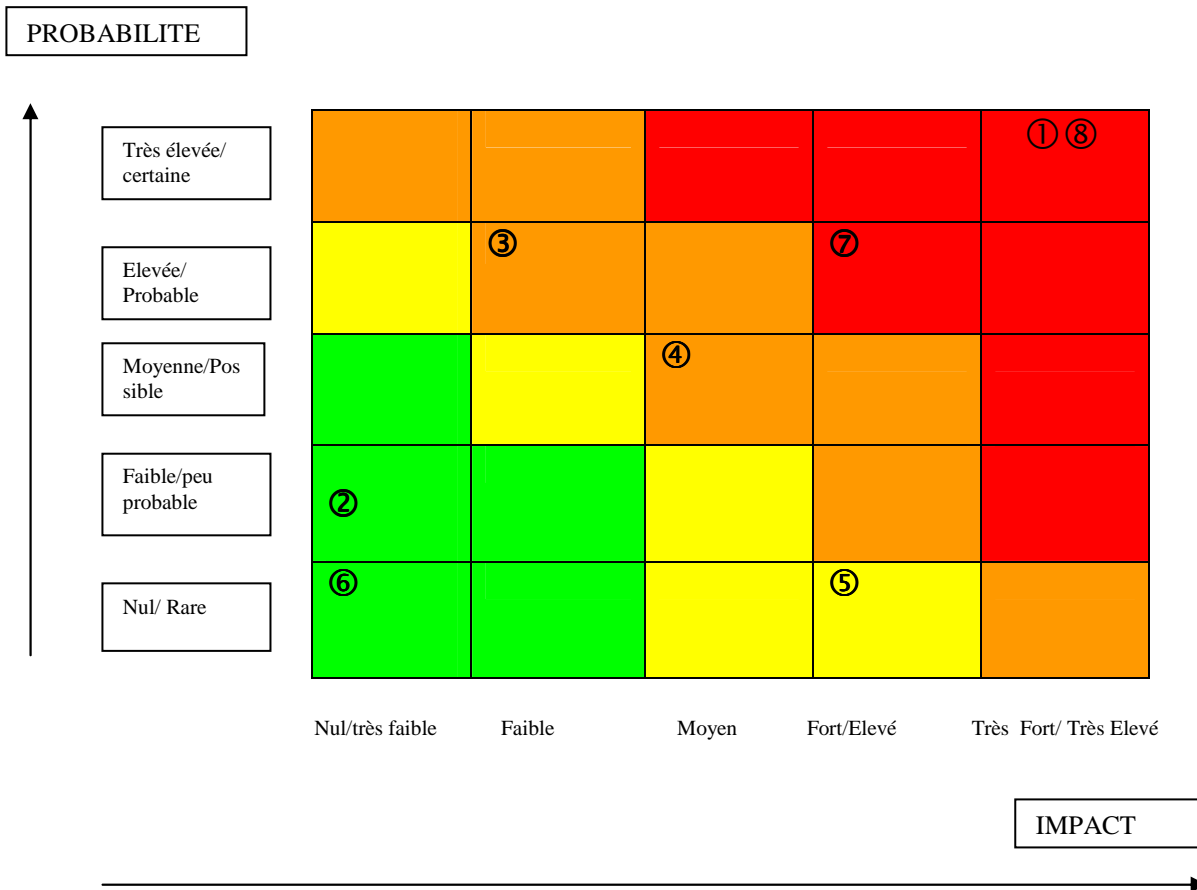
- le risque inhérent : c'est le risque théorique lié à l'activité. On peut aussi le définir comme le risque initial, avant toute mesure de maîtrise (contrôle interne) ;
- le risque résiduel : c'est le risque subsistant après la mise en œuvre de dispositifs de maîtrise (contrôle interne). Il convient de rappeler que des mesures de maîtrise des risques peuvent exister indépendamment d'un dispositif de contrôle interne formalisé.

Un risque se caractérise par sa probabilité de survenance et par son impact, en cas de réalisation. Pour chaque facteur, on peut évaluer un niveau selon une échelle de trois valeurs (faible, moyen, fort ou 1, 2, 3). Il existe également des modèles à 4 niveaux (faible, moyen ou modéré, fort, critique) ou à 5 niveaux (très faible ou nul, faible, modéré, fort, critique). Tout dépend de la capacité de la structure à mesurer la probabilité de survenance du risque, ce qui est facile pour certains domaines tels que les domaines opérationnels à condition de mettre en place un dispositif de mesure (% d'erreurs, % de réclamations, % de rejets par le comptable, % de factures donnant lieu à des intérêts de retards, % de blocages d'opérations par le système informatique, % d'incidents déclarés par les services ou enregistrés par les SI, taux d'indisponibilité des SI etc.). Pour certains domaines, où le risque est plus « qualitatif », l'évaluation de la probabilité revêt une part de subjectivité.

Dans les structures dotées de dispositifs de maîtrise des risques formalisés et organisés, il existe une cartographie des risques.

La construction d'une cartographie des risques est une démarche complexe, qui peut se décomposer en trois étapes :

- l'identification des risques, conduite généralement par processus d'activité. C'est ce que nous faisons dans notre tableau. Nous travaillons sur le processus « ressources humaines » que nous avons décomposé en sous-processus de pilotage, de gestion opérationnelle et en procédures (recrutement, affectation-mutation...) ;
- l'évaluation du risque selon les deux facteurs de probabilité et d'impact en distinguant entre le risque inhérent et le risque résiduel : on peut dans ce cadre réaliser un tableau des risques en faisant figurer le risque inhérent, le dispositif de maîtrise des risques existant, le risque résiduel : on parlera alors **de matrice des risques** ;
- la représentation du portefeuille des risques dans une **cartographie des risques**. Les différents risques identifiés sont généralement reportés sur un repère orthonormé, ce qui permet de disposer d'une représentation immédiate des risques majeurs ou critiques. On peut réaliser une cartographie des risques inhérents et une cartographie des risques résiduels. Le plus souvent, il n'existe qu'une cartographie des risques résiduels.



L'intérêt d'une cartographie des risques est de servir de base à la définition d'un plan d'action pour maîtriser ou réduire les risques les plus importants.

On considère généralement que les risques critiques sont du domaine de la gouvernance, les risques moyens de celui de l'encadrement opérationnel et les risques de non qualité (faible impact et probabilité assez élevée) de la responsabilité des agents de premier niveau.

La matrice des risques de l'auditeur :

L'auditeur construit dans la phase de prise de connaissance de l'entité qu'il va auditer une matrice des risques, qu'il va alimenter au fur et à mesure de ses travaux, c'est-à-dire un tableau dans lequel il va faire figurer :

- le risque inhérent à l'activité selon un référentiel de risques qui peut être
 - o soit une production externe à l'entité :
 - pour les aspects comptables, les référentiels de contrôle interne comptable développés par la DGFIP,
 - pour les aspects budgétaires, ceux développés par la MACIB à la direction du Budget),
 - pour les RH et les SI, ceux qui résulteront des GT du CHAI...
 - o soit une production interne : sa propre cartographie des risques...

- le risque de contrôle : c'est-à-dire le risque qu'il n'y ait pas de dispositif de maîtrise du risque (ex : des contrôles de cohérence dans une application informatique, un mécanisme de validation hiérarchique en chaîne papier ou en chaîne documentaire, un dispositif d'accès à la réglementation, un recueil de procédures, une veille réglementaire, des actions de formation ...). ou que le dispositif prévu ne soit pas mis en place ou ne soit pas efficace. Les travaux d'audit vont permettre d'établir ce point.
- le risque résiduel tel que l'auditeur peut l'évaluer au regard des dispositifs recensés et des tests de permanence réalisés.

Pour les risques côtés forts ou moyens, il indiquera dans une colonne spécifique la nature les travaux d'audit qu'il va entreprendre et au fur et à mesure de leur exécution, les références des documents correspondants (comptes-rendus d'entretien, tests). On peut aussi prévoir des travaux sur des risques faibles soit parce qu'il s'agit d'un thème obligatoire (attention particulière du ministre par exemple), soit parce que l'on entend vérifier que le risque est maîtrisé (particulièrement, lorsque des éléments conjoncturels modifient l'environnement de contrôle).

Au terme de ces travaux, il requalifiera le risque soit pour confirmer sa cotation initiale, soit pour la modifier en fonction des travaux réalisés. Tout risque confirmé donnera lieu à un constat assorti d'une recommandation. La matrice ainsi complétée doit permettre de suivre le déroulement de l'audit.

Nous établirons des matrices pour les sous-processus RH que nous sélectionnerons.

Une matrice des risques se présente généralement de la manière suivante.

EXEMPLE DE MATRICE DES RISQUES (AUDITEUR)

Objectifs des domaines ou des activités	Nature du risque inhérent	Éléments d'évaluation du risque (facteurs identifiés lors de la phase de prise de connaissance)	Cotation du risque inhérent	Dispositif de contrôle attendu (cadre théorique)	Dispositif de maîtrise des risques existant ou prévu par l'entité (plan d'action)	Niveau de mise en œuvre du dispositif de maîtrise des risques	Référence des fiches de tests de permanence et des entretiens	Niveau d'efficacité du dispositif de maîtrise des risques	Cotation du niveau de risque de contrôle	Cotation du risque résiduel	Référence des fiches de tests détaillés	Références FRAP et recommandations
Activité 1												
Activité 2												

Cette matrice est très proche de celle qui a été réalisée pour les audits comptables et financiers, processus « commande publique ». Elle comporte une colonne supplémentaire « éléments d'évaluation du risque » car en l'absence de référentiel pré-déterminé, c'est l'auditeur qui va déterminer les éléments qui le conduisent à estimer le niveau de risque. Moins le risque se prête à une mesure quantitative et plus cette colonne est importante.