## Qu’est-ce qu’un risque pour une entreprise ?

Le risque en entreprise désigne **l’évènement qui peut survenir et avoir un impact sur sa rentabilité ou sa pérennité.**

 Par exemple :

* Des erreurs de prévisions ou de gestion ;
* Des menaces qui se réalisent ;
* La survenance d’aléas défavorables.

Le risque se mesure par son **degré de probabilité et par les conséquences humaines et financières** qu’il génère pour la structure. Les risques peuvent ensuite être :

* Acceptés ;
* Transférés, par exemple sur un assureur ;
* Diminués ;
* Éliminés.

Pour lutter contre le risque en entreprise, il convient d’établir une[cartographie des risques](https://trustpair.fr/blog/une-cartographie-elaboree-pour-gerer-les-risques-tiers/) et de mettre en place un processus de management des risques (PMR). Ces opérations seront pilotées par :

* La direction générale
* Les directions opérationnelles, notamment la direction des affaires financières, très exposée
* Un risque manager
* https://trustpair.fr/

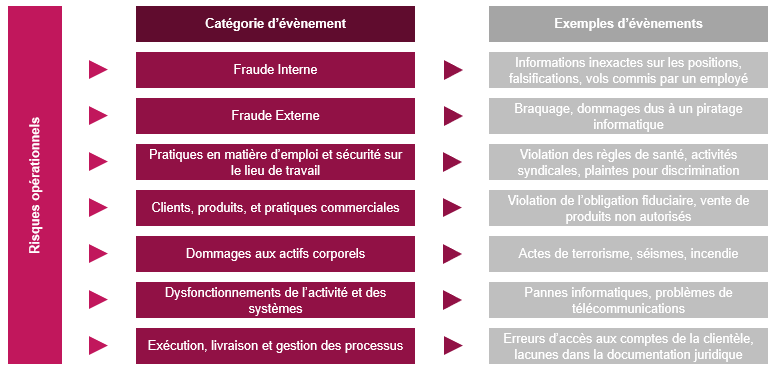
Gestion du risque opérationnel

**Définition :**

Le risque opérationnel pour les établissements financiers est le risque de pertes directes ou indirectes dues à une inadéquation ou à une défaillance des procédures de l'établissement, de son personnel, des systèmes internes, des risques externes ou émergents. [Wikipédia](https://fr.wikipedia.org/wiki/Risque_op%C3%A9rationnel_(%C3%A9tablissement_financier))

**L'accord de Bâle II classe les risques opérationnels en 7 catégories**

**Différentes :**



#### **Les différents**[**risques opérationnels**](https://trustpair.fr/blog/gestion-risques-tiers-mode-demploi-webinar-trustpair-redbridge/)

Ils comprennent notamment :

* **Le risque de capital humain** : la sécurité et la santé au travail, la perte de la culture d’entreprise, la formation insuffisante du personnel, les conflits sociaux, les difficultés de recrutement… ;
* [**Les risques cyber**](https://trustpair.fr/blog/gestion-risques-cybersecurite/): parmi les plus redoutés des dirigeants d’entreprise, ils comprennent notamment le ransomware, le piratage de données, la panne du système informatique… Un logiciel comme Trust pair permet de lutter contre la fraude au virement bancaire, grâce au [nettoyage continu de la base des données tiers et fournisseurs](https://trustpair.fr/solutions/nettoyage-base-tiers/) ;
* **L’interruption d’activité** liée à un facteur interne (défaut sur la chaîne d’approvisionnement, par exemple) ou externe (catastrophe climatique qui entraîne la destruction des équipements) trustpair.fr

### **Indicateurs de risques opérationnels : rôle et exemples**

Les indicateurs de suivi des risques opérationnels servent à surveiller et estimer la probabilité et l'impact des risques opérationnels au sein d'une entreprise (banque, assurances, etc.).

Ce sont des indicateurs-clés (souvent des bases de données), qui permettent de détecter des signes avant-coureurs et de mettre en place des plans d'action préventifs.

Voici quelques exemples d'indicateurs de suivi des risques opérationnels :

* La détermination du profil des risques opérationnels en fonction des lignes de métier.
* Le pourcentage d'erreurs humaines.
* Le temps de résolution des différents problèmes.
* La probabilité d'occurrence des risques (là aussi, selon les lignes de métier).
* Le taux de récidive d'un même problème.
* L'évaluation des pertes financières.
* Etc. www.capital.fr

**Comment maîtriser les risques opérationnels ?**

**La maîtrise du risque opérationnel est un processus continu et complexe qui vise à réduire les probabilités d'occurrence et les impacts des risques opérationnels sur une entreprise. Voici quelques étapes clés pour maîtriser le risque opérationnel :**

**1. Identification des Risques :**

* **Analyse des Processus : Examinez en détail les processus métier pour identifier les points faibles, les erreurs potentielles et les risques inhérents.**
* **Évaluation des Scénarios : Passez en revue les scénarios qui pourraient conduire à des pertes opérationnelles, y compris les erreurs humaines, les défaillances des systèmes, la fraude, etc.**

**2. Évaluation et Quantification des Risques :**

* **Analyse Quantitative : Utilisez des modèles statistiques pour estimer les pertes potentielles en fonction de scénarios de risques.**
* **Analyse Qualitative : Évaluez la probabilité et l'impact des risques en vous basant sur l'expertise et l'expérience des gestionnaires de risques.**

**3. Contrôles et Mitigation :**

* **Mise en Place de Contrôles Internes : Développez et mettez en œuvre des procédures et des contrôles pour réduire les risques identifiés, comme des vérifications croisées, des autorisations spécifiques, des limites de transaction, etc.**
* **Politiques et Procédures : Élaborez des politiques claires et des procédures opérationnelles détaillées pour assurer que les processus sont suivis de manière cohérente et conforme aux normes de l'entreprise.**

**4. Formation et Sensibilisation :**

* **Formation des Employés : Sensibilisez et formez les employés aux risques opérationnels, en les rendant conscients des pratiques à suivre pour les minimiser.**
* **Culture de Gestion des Risques : Promouvez une culture d'entreprise axée sur la gestion des risques, où chaque employé comprend son rôle dans la minimisation des risques opérationnels.**

**5. Surveillance et Reporting :**

* **Surveillance Continue : Utilisez des indicateurs clés de risque (KRI) pour surveiller en temps réel ou périodiquement l'exposition aux risques.**
* **Rapports de Gestion : Élaborez et partagez des rapports réguliers sur les risques opérationnels pour informer la direction et les parties prenantes des niveaux de risque et des mesures prises pour les atténuer.**

**6. Gestion des Incidents :**

* **Plan de Continuité des Activités (PCA) : Établissez des plans pour maintenir les opérations en cas d'interruption majeure, tels que des plans de reprise après sinistre.**
* **Gestion des Crises : Prévoyez des plans pour gérer les crises opérationnelles de manière efficace, en désignant des équipes et des procédures spécifiques.**

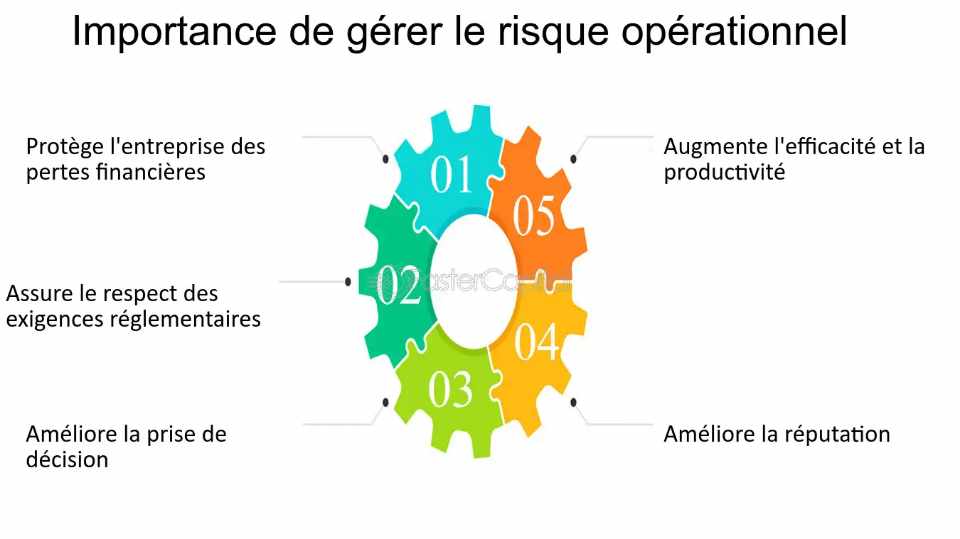
**7. Révision et Amélioration Continue :**

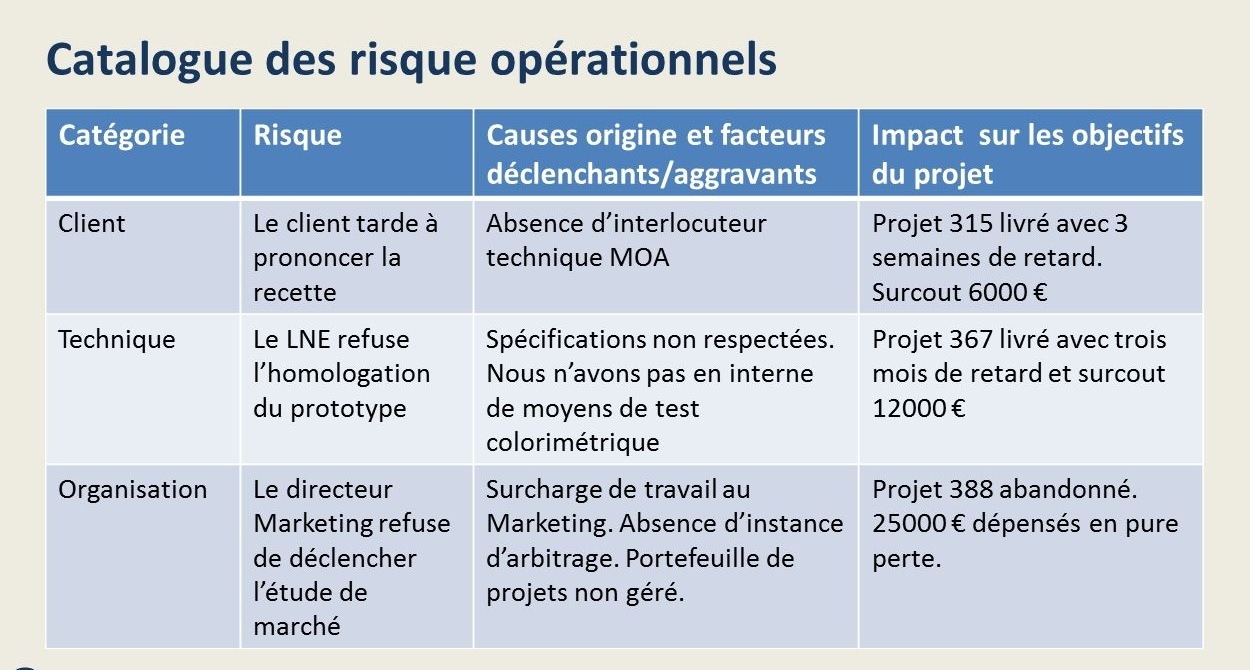
* **Révision Régulière : Évaluez régulièrement l'efficacité des mesures de contrôle et d'atténuation des risques, en identifiant les domaines d'amélioration.**
* **Adaptation aux Changements : Ajustez le dispositif de gestion des risques en fonction des évolutions de l'entreprise, de son environnement réglementaire, technologique et économique.**

**8. Audit et Vérification :**

* **Audits Internes et Externes : Effectuez des audits pour vérifier l'efficacité des mesures de contrôle et pour assurer la conformité aux normes et réglementations.**

**9. Utilisation de la Technologie : Outils de Gestion des Risques : Utilisez des logiciels et des outils spécialisés pour suivre et gérer les risques opérationnels de manière plus efficace. ChatGPT**





**ANALYSE DU RISQUE: AXES CAUSES ET CONSEQUENCES :**

**Le risque opérationnel est un type de risque qui résulte de la perte potentielle due à des processus internes, des personnes, des systèmes ou des événements externes autres que les risques de marché ou de crédit. Voici quelques causes et conséquences du risque opérationnel :**

**Causes du Risque Opérationnel :**

1. **Erreurs Humaines : Les actions incorrectes, les mauvaises décisions ou les manquements des employés peuvent entraîner des pertes opérationnelles.**
2. **Défaillances des Systèmes : Les défaillances des systèmes informatiques, des équipements ou des processus automatisés peuvent causer des perturbations et des pertes financières.**
3. **Fraude et Malversations : Les activités frauduleuses, telles que la fraude comptable, la corruption ou le vol, représentent un risque opérationnel majeur.**
4. **Catastrophes Naturelles et Événements Externes : Les catastrophes naturelles, les crises politiques, les pandémies et autres événements imprévus peuvent perturber les opérations d'une entreprise.**
5. **Non-conformité Réglementaire : Ne pas respecter les réglementations en vigueur peut entraîner des amendes, des sanctions et des pertes financières importantes.**
6. **Complexité des Opérations : Les opérations complexes peuvent être plus difficiles à gérer et peuvent conduire à des erreurs et des pertes.**

**Conséquences du Risque Opérationnel :**

1. **Pertes Financières : La conséquence la plus directe est la perte financière pour l'entreprise, résultant des événements opérationnels.**
2. **Réputation Endommagée : Les incidents opérationnels, en particulier ceux liés à la fraude ou à la non-conformité, peuvent ternir la réputation de l'entreprise et affecter sa crédibilité auprès des clients et des investisseurs.**
3. **Amendes et Pénalités : Les non-conformités réglementaires peuvent entraîner des amendes et des pénalités financières significatives.**
4. **Baisse de la Productivité : Les interruptions opérationnelles peuvent entraîner une baisse de la productivité, en particulier si des systèmes critiques sont hors service.**
5. **Coûts de Réparation : Après un incident opérationnel, l'entreprise peut devoir engager des coûts importants pour réparer les dommages et prévenir de futurs incidents.**
6. **Perte de Clients : Une mauvaise gestion des risques opérationnels peut conduire à une perte de confiance des clients, les incitant à se tourner vers des concurrents plus fiables.**
7. **Impact sur le Capital : Les pertes financières importantes peuvent réduire les fonds propres de l'entreprise, affectant sa capacité à investir et à se développer.**

**ChatGPT**

**LES LEVIERS DE MAITRISE DES RISQUES :**

**Plusieurs stratégies s’offrent aux propriétaires des risques pour appréhender les risques opérationnels quels qu’ils soient. La détermination de l’attitude à avoir face aux risques nécessite la définition, même non encore formalisée, de l’appétence au risque. Il existe 4 types de réponses face aux risques :**

1. **L’acceptation : le couple risque/ rentabilité justifie la prise de risque, l’espérance de gain est largement superieure aux risques encourus**
2. **La réduction :**

* **Prévention : on évite l’occurrence, en agissant sur le DMR EX : contrôle des dossiers de souscription / d’adhésion**
* **Protection : on limite l’impact, en agissant sur les conséquence EX : Mise en place d’un PCA**
* **Transfert : on transfert contractuellement une partie de l’activité et donc la maitrise du risque a un tiers ( délégation de gestion, externalisation).Le risque est toutefois conservé par l’entreprise**

1. **Le financement :**

* **Rétention (franchise de l’assurance, provision …..)**
* **Transfert (assurances, captives, ART) EX : responsabilité civile professionnelle fraude/ perte d’exploitation**

1. **L’évitement : refus de l’intégralité du risque : abandon de l’activité**

[**https://obsmetiers.rcp-pro.fr**](https://obsmetiers.rcp-pro.fr)