**Gestion des risques**

Motuc entreprise

Table des matières

[1. Le risque 4](#_Toc36472144)

[1.1 Définition d’un risque 4](#_Toc36472145)

[1.2 Définition de la gestion des risques 4](#_Toc36472146)

[1.3 Les différents types de risques 4](#_Toc36472147)

[1.4 Gestion des risques 5](#_Toc36472148)

# Le risque

## 1.1 Définition d’un risque

Le **risque** est la possibilité de survenue d'un événement indésirable, la probabilité d'occurrence d'un péril probable ou d'un aléa.

Lorsque l’on parle de risque dans une entreprise comme chez Motuc, il est souvent associé à la gestion des risques. Une entreprise comme Motuc ne veut être confronter au moins de risque possible pour avoir une certaine stabilité qui permettra une bonne gestion des projets en cours et ceux à venir.

## 1.2 Définition de la gestion des risques

La gestion des risques, ou management du risque (risk management), est la discipline qui s'attache à identifier, évaluer et prioriser les risques relatifs aux activités d'une organisation, quelles que soient la nature ou l'origine de ces risques, pour les traiter méthodiquement de manière coordonnée et économique, de manière à réduire et contrôler la probabilité des événements redoutés, et réduire l'impact éventuel de ces événements.

## 1.3 Les différents types de risques

Les risques propres à la gestion du projet : mauvaise organisation (les rôles ne sont pas clairement identifiés, plusieurs personnes sont affectées à la même tâche, implication insuffisante de l’équipe et/ou du client) ou encore d’un mauvais choix de personne (un chef de projet inexpérimenté pour un projet important ou à risque par exemple).

Les risques juridiques : concernent tous les intervenants auxquels vous êtes liés contractuellement. Typiquement, il peut s’agir d’un fournisseur qui n’est pas capable de tenir ses engagements en termes de livraison de matériel ou de logiciels ou d’un cotraitant ou sous-traitant qui ne peut finalement pas fournir les ressources humaines convenues.

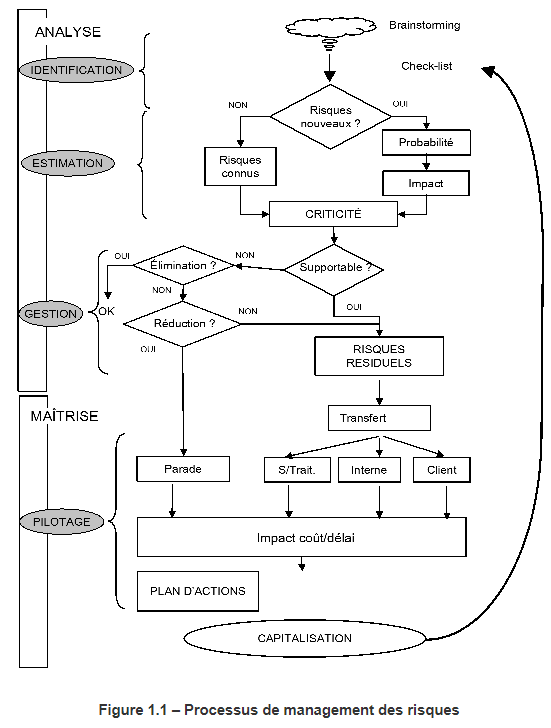
Les risques concernant le respect du planning : mauvaise estimation de la durée d’exécution des tâches en amont. Les dérapages sur le déroulement du planning peuvent d’ailleurs être liés à d’autres risques (techniques, humains…).

Les risques humains : gestion des ressources humaines du projet. Ils prennent notamment en compte les maladies, voire les décès, de certains intervenants clés du projet, la réaffectation de ressources à d’autres projets (et donc la diminution de la capacité de réalisation de l’équipe courante) ou encore le manque de compétences de l’équipe nécessitant éventuellement des formations.

Les risques techniques : liés aux langages de programmation, technologies et logiciels choisis pour le projet, mais qui ne sont pas encore maîtrisés par l’ensemble de l’équipe. Les risques concernent aussi bien la lenteur de réalisation des tâches que les erreurs en termes d’architecture pouvant être commises à cause d’une connaissance insuffisante du domaine concerné.

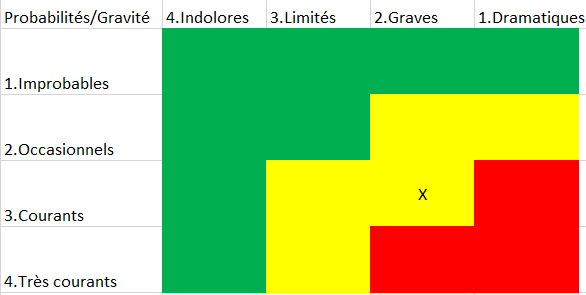
## 1.4 Gestion des risques

Il y a différents outils et méthodes pour gérer les risques en entreprises. Le premier que nous allons utiliser pour répondre à cette période de crise ça sera ceci :



Ceci est une des méthodes pour répondre à notre problématique qui est d’analyser les différents risques que l’entreprise pourrait subir. Comme vous pouvez le voir, il se découpe en deux parties, la première partie qui est l’analyse du risque et ensuite la maîtrise de celui-ci qui nous permettra de savoir quoi faire.

Puis il y a le taux de criticité des risques. Pour ceci il y a une matrice qui est simple à comprendre et facile à mettre en place.



Ici nous avons un risque qui sera donc grave et courant, il faudra donc le traiter priorité. Voici un exemple de matrice que nous allons utiliser tout au long de ce dossier pour mettre en évidence les ordres de priorités de l’entreprise concernant la gestion des risques.

# Les risques connus

## 2.1 Risques concernant les mesures de sécurité existantes

Vous nous avez indiquez que vous exigez de conserver un serveur servant de RCD sur chaque site pour minimiser d’éventuelles coupures WAN. Ceci est un très bon choix de votre part, ça permettra une continuité des services de votre entreprise. En revanche, nous devons vous mettre en garde, plus il y a de serveurs plus il y a de risques d’intrusion dans votre SI même si votre choix est le bon, nous préférions vous l’indiquez.



Dans le dossier que vous nous avez envoyer, il est écrit : « Les salles hébergeant les serveurs des magasins sont fermées à clé. Seul le directeur du magasin possède la clé de la salle. » Ceci est une bonne sécurité mais est-elle suffisante ? Le directeur pourrait égarer ou se faire voler la clé des serveurs et ne pas s’en rendre compte avant plusieurs jours. Cela pourrait engendrer des conséquences dramatiques pour l’entreprise comme la perte de toute les données clients, ou simplement le vole de ces données mais par chance, cela est peu probable.

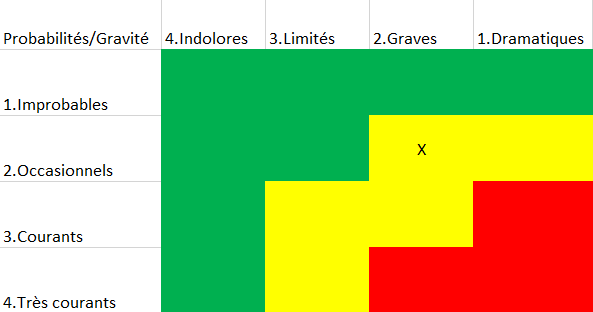


Par conséquent, pour ce risque nous vous proposons une doublé sécurité, comme une première porte avec un code digital à entrer qui changerai chaque semaine, puis une autre porte avec votre clé.

Au niveau du bâtiment nous n’avons pas vu d’information concernant la sécurité des bureaux de la direction ou du service informatique. Du coup, nous préférons vous indiquez qu’il faudrait fermer ces bureaux à partir du moment où ces bureaux sont vides pour éviter une intrusion et un piratage des données cruciales pour l’entreprise. C’est une des premières causes de piratage de données en informatique.



Vous nous avez notifier que vous n’aviez mis aucune mesure en place pour assurer la non-répudiation, nous pensons que dans votre entreprise il serait bon de le faire. Quand nous observons les dysfonctionnements survenus, il est indiqué qu’une personne malveillante à utiliser l’identité du responsable réapprovisionnement. C’est pour cela que nous vous conseillons de mettre en place la non-répudiation dans votre entreprise.



## Risques concernant les dysfonctionnements

Les des dysfonctionnements votre entreprises à souvent fait appels à des sociétés extérieur pour résoudre vos problèmes, lors des ces interventions, ces sociétés ont pu introduire ce fameux ransomware dans vos serveurs. Si cela ne vient pas de ça, il est fort possible que cela pour arrive un jour, ce qui dramatiques pour votre entreprise.



Fort heureusement ceci n’arrive très rarement car la société qui ferai ce genre d’action risque de grosse conséquence pénale. Mais pour votre sécurité, nous vous conseillions d’installer des caméras si cela n’est pas déjà fait et d’avoir un service de Log sur vos serveurs et de savoir comment les interpréter. Nous faisons confiance à votre service informatique pour gérer ceci.