**Gestion des risques**

Motuc entreprise

Table des figures :

[Figure 1: Schema management des risques 5](#_Toc36564011)

[Figure 2: Exemple criticité du risque 6](#_Toc36564012)

[Figure 3: Criticité réplication des serveurs 7](#_Toc36564013)

[Figure 4: Criticité porte salle serveur 7](#_Toc36564014)

[Figure 5: Criticité fermeture des bureaux 8](#_Toc36564015)

[Figure 6: Criticité non-répudiation 8](#_Toc36564016)

[Figure 7: Criticité société exterieur 9](#_Toc36564017)

[Figure 8: Criticité phishing 10](#_Toc36564018)

[Figure 9: Criticité ambiance entreprise 10](#_Toc36564019)

[Figure 10: Criticité catastrophe naturel 11](#_Toc36564020)

[Figure 11: Criticité concurent stratégie 12](#_Toc36564021)

[Figure 12: Criticité attaque guerre / terroriste 13](#_Toc36564022)

[Figure 13: Criticité manifestation 14](#_Toc36564023)

Table des matières

[1. Le risque 4](#_Toc36555205)

[1.1 Définition d’un risque 4](#_Toc36555206)

[1.2 Définition de la gestion des risques 4](#_Toc36555207)

[1.3 Les différents types de risques 4](#_Toc36555208)

[1.4 Gestion des risques 5](#_Toc36555209)

[2. Les risques connus 6](#_Toc36555210)

[2.1 Risques concernant les mesures de sécurité existantes 6](#_Toc36555211)

[2.2 Risques concernant les dysfonctionnements 8](#_Toc36555212)

[3. Risque commun général 11](#_Toc36555213)

# 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 :

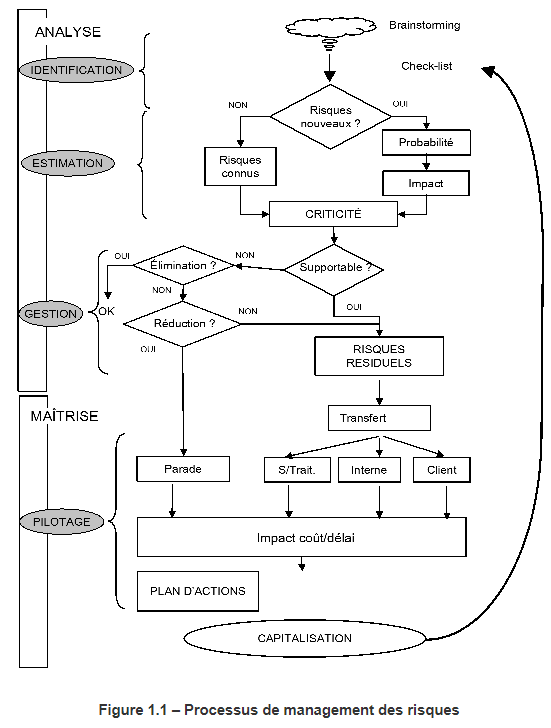


Figure 1: Schema management des risques

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.

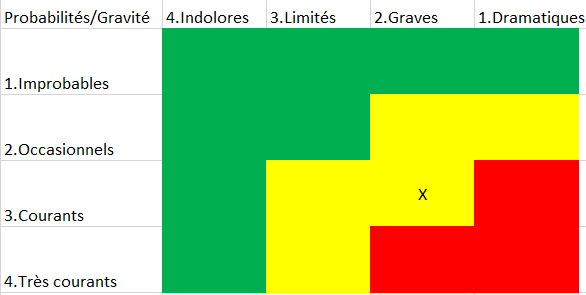


Figure 2: Exemple criticité du risque

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.



Figure 3: Criticité réplication des serveurs

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 vol de ces données mais par chance, cela est peu probable.



Figure 4: Criticité porte salle serveur

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.



Figure 5: Criticité fermeture des bureaux

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.

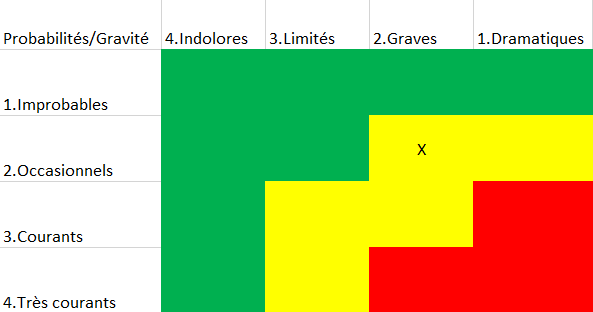


Figure 6: Criticité non-répudiation

## 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.



Figure 7: Criticité société exterieur

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.

Nous avons remarqué que vous avez été victime de phishing sur l’ordinateur du directeur d’un magasin du nord est lors du rapport des dysfonctionnement. Cela peut avoir des conséquences assez graves si depuis cet ordinateur il a accès à des données capitales. Le phishing est la méthode la plus répandue pour le vol de donnée et la plus facile à mettre en place pour des pirates.



Figure 8: Criticité phishing

Nous savons que vous avez déjà fait des formations sur la sécurité informatique en générale mais nous pensons qu’une formation sur le phishing en particulier pour toutes les personnes ayant accès à des données importante serait une priorité pour votre entreprise.

Vous nous dites qu’il y a une ambiance tendue entre le directeur de la plateforme commerciale et les responsables des services. Vous faites appel à nous pour identifier les risques envisageables alors je vous mets en garde, il est possible que les responsables des services donnent des informations au concurrents comme vous nous l’avez signalé.

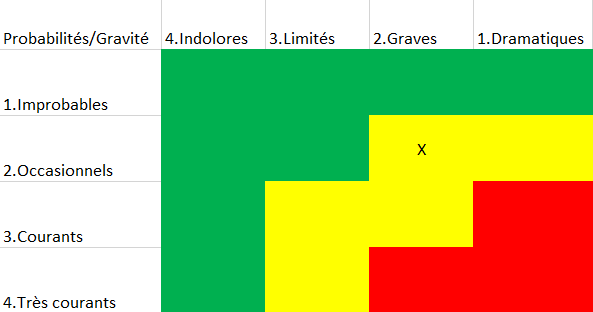


Figure 9: Criticité ambiance entreprise

L’espionnage est très courant, il faudra faire attention lors de vos futurs recrutements. Nous vous conseillons de bien vérifier leurs références.

# Risque commun général

Dans cette partie nous allons vous parlez des risques communs à d’autres entreprises qui pourrait vous impacter vous aussi. Comme vous le savez, il y a des risques que nous ne pouvons pas contrôler comme les risques de catastrophes naturelles, certes ces événements sont rares mais pas inenvisageable.



Figure 10: Criticité catastrophe naturel

Dans votre cas, nous n’avons pas d’informations concernant la gestion de vos données, et la gestion de vos sites où sont vos serveurs. Mais il serait préférable d’avoir une sauvegarde de vos données dans le cloud sur des plateformes spécialisées dans le stockage de données qui sont protéger contre ce genre d’événement naturel car vos données seront stockées avec redondance ce qui permettra sur sécurité accrue. Si vous le souhaitez vous pouvez aussi faire de la redondance de donnée sur vos différents serveurs ce qui ne fera que renforcer la sécurité de vos données.

Vous nous faites part qu’il y a un nouveau concurrent sur le marché, ce n’est pas forcément une nouvelle négative, la concurrence peut avoir du bon, cela va pouvoir vous aidez à avoir une nouvelle vision de votre marché, votre concurrent ne peut avoir la même stratégie que vous. Mais faites attention à ne pas vous laisser dépasser, cela est déjà arriver à un grand nombre d’entreprise de se reposer sur son marché et que son marché s’écroule pour une raison diverse.

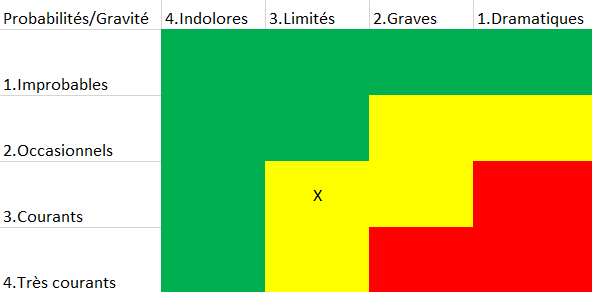


Figure 11: Criticité concurrent stratégie

C’est pour cela que nous vous conseillions de bien observer ce que fait votre concurrent pour pouvoir contrer sa stratégie et de continuer à faire évoluer votre entreprise en prenant en compte vos concurrents.

## Risque concernant les magasins

En sachant que vous êtes une chaine de magasin, vous devez savoir qu’il peut y avoir plusieurs types de risque concernant vos magasins. Le premier se serai en cas de guerre, ou d’attaque terroriste proche de vos magasins, cela est un événement très rare mais il obligera le magasin à fermer.



Figure 12: Criticité attaque guerre / terroriste

Vous allez ensuite devoir investir dans le marketing pour remettre en avant votre entreprise et continuer à faire parler de vous.

Ensuite il peut y avoir des risques de manifestations par forcement contre votre entreprise mais comme vous avez pu le voir l’année dernière lors de la manifestation des gilets jaune, il y a eu de nombreuses entreprises qui ont subi de grosse perte de chiffre d’affaire. Cela arrive de plus en plus souvent il va falloir faire attention à cela.

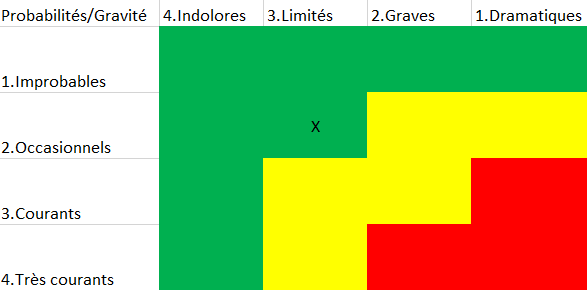


Figure 13: Criticité manifestation

Nous vous proposons comme solution des assurances contre ce genre d’événement ou avoir une trésorerie nécessaire pour payer vos employés pendant plusieurs semaines sans avoir de chiffre d’affaire. Pour certains risques il n’y a pas de solution efficace comme ici.

# Conclusion

La gestion des risques implique la mise en place de processus, de méthodes et d'outils afin de traiter les conséquences des événements que nous avons identifiés comme représentant des menaces importantes pour votre entreprise. Cela pourrait être aussi simple que de mettre de côté des réserves financières afin de faciliter les problèmes de trésorerie s'ils surviennent ou de garantir une sauvegarde informatique efficace et des procédures de soutien des TI pour traiter une panne des systèmes.

Les programmes traitant des menaces identifiées au cours de l'évaluation des risques sont souvent appelés les plans de continuité des opérations. Ils indiquent ce que vous devez faire si un événement donné survient, par exemple si un incendie détruit votre bureau. Vous ne pouvez éviter tous les risques, mais les plans de continuité des opérations peuvent minimiser la perturbation de votre activité.

Les évaluations des risques changeront de pair avec la croissance de votre entreprise ou en raison de changements internes ou externes. Cela signifie que les processus que vous avez mis en place pour gérer les risques de votre entreprise doivent être revus périodiquement. De telles révisions identifieront les améliorations à apporter aux processus et peuvent également indiquer le fait qu'un processus ne soit plus nécessaire.

Il existe quatre façons de traiter ou de gérer chaque risque que vous avez identifié. Vous pouvez :

* L’accepter
* Le transférer
* Le diminuer
* L'éliminer

Par exemple, vous pourriez décider d'accepter un risque, car le coût relié à son élimination complète est trop élevé. Vous pourriez décider de transférer le risque, ce qui est habituellement effectué avec une assurance. Ou vous pourriez être en mesure de diminuer le risque en introduisant de nouvelles mesures de sécurité ou l'éliminer complètement en changeant la façon dont vous produisez le produit.

Lorsque vous aurez évalué et accepté les mesures et les procédures visant à diminuer le risque, ces mesures doivent être mises en place.