**Gestion des risques**

Motuc entreprise

Table des figures :

[Figure 1: Schema management des risques 6](#_Toc36735875)

[Figure 2: Exemple criticité du risque 7](#_Toc36735876)

[Figure 3: Criticité réplication des serveurs 7](#_Toc36735877)

[Figure 4: Criticité porte salle serveur 8](#_Toc36735878)

[Figure 5: Criticité fermeture des bureaux 9](#_Toc36735879)

[Figure 6: Criticité non-répudiation 9](#_Toc36735880)

[Figure 7: Criticité société extérieure 10](#_Toc36735881)

[Figure 8: Criticité phishing 10](#_Toc36735882)

[Figure 9: Criticité ambiance entreprise 11](#_Toc36735883)

[Figure 10: Criticité catastrophe naturelle 12](#_Toc36735884)

[Figure 11: Criticité concurrent stratégie 12](#_Toc36735885)

[Figure 12: Criticité attaque guerre / terroriste 13](#_Toc36735886)

[Figure 13: Criticité manifestation 14](#_Toc36735887)

Table des matières

[1. Le risque 5](#_Toc36735900)

[1.1 Définition d’un risque 5](#_Toc36735901)

[1.2 Définition de la gestion des risques 5](#_Toc36735902)

[1.3 Les différents types de risques 5](#_Toc36735903)

[1.4 Gestion des risques 6](#_Toc36735904)

[2. Les risques connus 7](#_Toc36735905)

[2.1 Risques concernant les mesures de sécurité existantes 7](#_Toc36735906)

[2.2 Risques concernant les dysfonctionnements 10](#_Toc36735907)

[3. Risque commun général 12](#_Toc36735908)

[4. Risque concernant les magasins 13](#_Toc36735909)

[Conclusion 15](#_Toc36735910)

# Le risque

## 1.1 Définition d’un risque

Le **risque** est la possibilité que survienne 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 Motuc, il est souvent associé à la gestion des risques. Une entreprise comme Motuc veut être confrontée au minimum de risques possibles pour garantir une stabilité optimale, et permettre une bonne gestion des projets en cours et 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, pour réduire et contrôler la probabilité des événements redoutés, et minimiser 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

Parmi les différents outils et méthodes pour gérer les risques en entreprises, nous utiliserons d’abord la suivante :

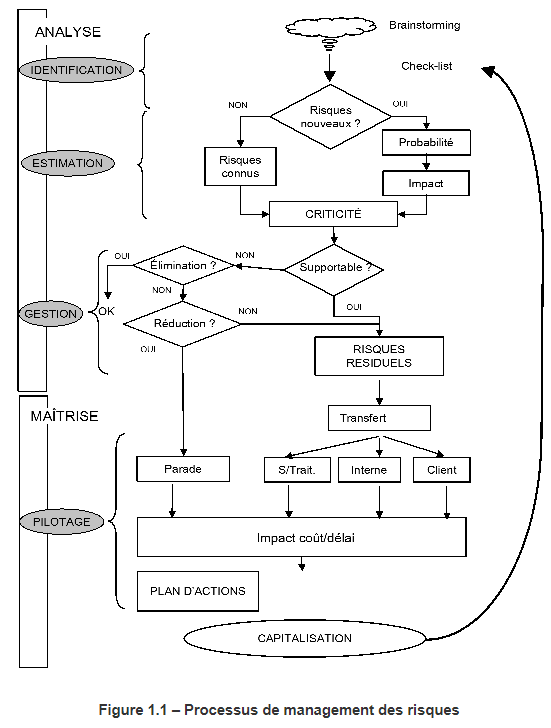


Figure 1: Schema management des risques

Cette méthode permet de répondre à la problématique, qui est d’analyser les différents risques que l’entreprise pourrait subir. Il se découpe en deux parties : l’analyse du risque et la maîtrise de celui-ci qui permet d’adapter la conduite à adopter face à ce risque.

Le taux de criticité des risques doit ensuite être analysé. La matrice suivante est simple à comprendre et facile à mettre en place.

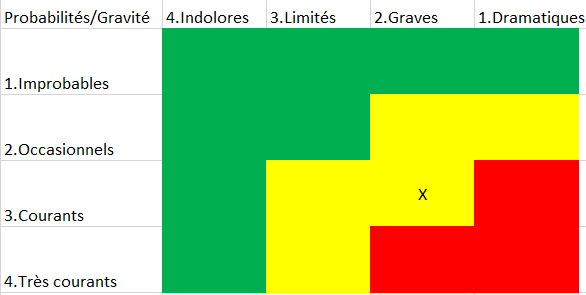


Figure 2: Exemple criticité du risque

Dans l’exemple ci-dessus, le risque est grave et courant, il faudra donc le traiter en priorité. C’est à l’aide de cette matrice que nous allons mettre en évidence les priorités de l’entreprise concernant la gestion des divers risques auxquels elle est confrontée.

# 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. C’est une très bonne décision, qui permettra une continuité des services de votre entreprise. En revanche, il est bon de rappeler que le risque d’intrusion dans le SI est proportionnel au nombre de serveurs.



Figure 3: Criticité réplication des serveurs

Les salles hébergeant les serveurs des magasins sont fermées à clé et seul le directeur du magasin possède cette clé. C’est une bonne précaution mais elle crée d’autres vulnérabilités. 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. Il est peu probable que cela arrive, mais des mesures supplémentaires devraient être mises en place.



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.

Aucune information ne nous est fournie quant à la sécurité des bureaux de la direction ou du service informatique. Nous recommendons donc de fermer ces bureaux quand ils 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. Aussi, chaque utilisateur doit prendre l’habitude de verrouiller son poste quand il le quitte, même pour quelques instants.



Figure 5: Criticité fermeture des bureaux

Comme aucune mesure n’est en place pour assurer la non-répudiation dans l’entreprise, nous pensons qu’il serait bon de le faire rapidement. Quand on analyse les dysfonctionnements survenus, on s’aperçoit que l’identité du responsable réapprovisionnement à été utilisée par une personne malveillante. C’est pour cela que nous vous conseillons de mettre en place la non-répudiation dans votre entreprise.

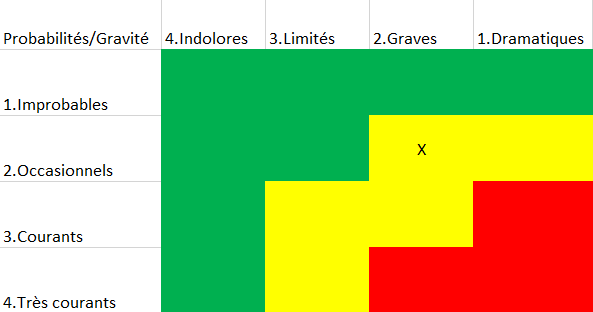


Figure 6: Criticité non-répudiation

## Risques concernant les dysfonctionnements

Lors de dysfonctionnements passés, MOTUC à souvent fait appel à des sociétés extérieures pour résoudre les problèmes. Lors de ces interventions, il est possible que l’un de ces sociétés ait pu introduire ce ransomware dans les serveurs. Si cela ne vient pas de ça, il est possible que cela puisse arriver un jour, avec des conséquences dramatiques pour l’entreprise.



Figure 7: Criticité société extérieure

Fort heureusement, c’est un scénario peu probable, car la société qui ferai ce genre d’action risque de grosses conséquences pénales. 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.

Il est fait état d’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, et cette tension en est un, il est possible que les responsables des services donnent des informations au concurrents comme vous nous l’avez signalé.

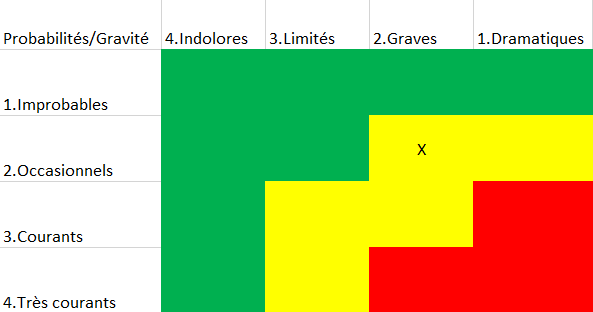


Figure 9: Criticité ambiance entreprise

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. Ces événements sont de moins en moins rares et doivent donc être envisagés.



Figure 10: Criticité catastrophe naturelle

Dans le cas de MOTUC, nous n’avons pas d’informations concernant la gestion des données, et la gestion des sites ayant des serveurs. Il serait préférable d’avoir une sauvegarde des données dans le cloud sur des plateformes spécialisées dans le stockage de données qui sont protégées contre ce genre d’événements naturels. Des données stockées avec redondance permettent une sécurité accrue. Il est aussi possible de faire de la redondance sur les serveurs physiques de l’entreprise sans faire appel au cloud, ce qui augmenterait aussi nettement la sécurité des données.

Vous nous faites part qu’il y a un nouveau concurrent sur le marché, ce qui 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 peut ne pas 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.

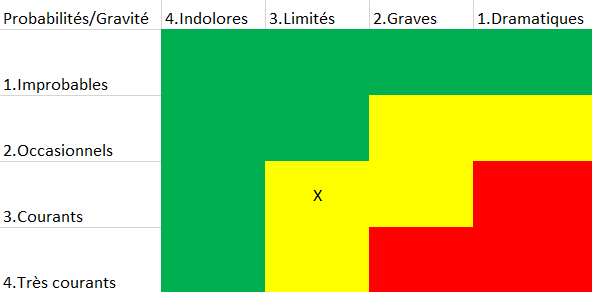


Figure 11: Criticité concurrent stratégie

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 magasins, vous devez savoir qu’il peut y avoir plusieurs types de risques concernant vos magasins. Le premier serait une guerre, attaque terroriste ou conflit local proche de vos magasins, des évènements rares, mais dont la probabilité ne cesse d’augmenter en France et en occident. Les conséquences en serait évidement dramatiques.



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.

Les manifestations sont aussi un risque pour le magasin même si celui-ci n’est pas visé. Des exemples récents illustrent bien le pouvoir destructeur que peut avoir une manifestation pour les commerces sur son trajet.

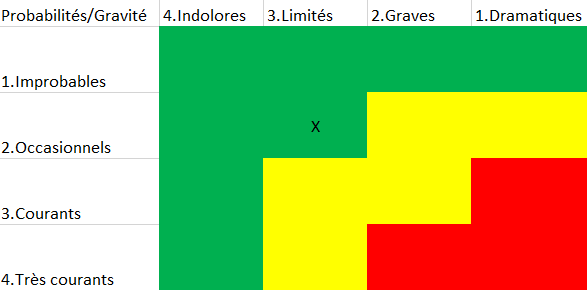


Figure 13: Criticité manifestation

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.