ANALYSE DES RISQUES ET MANAGENEMENT DES RISQUES

Introduction :

Le management des risques est un processus qui permet au Business Manager d'équilibrer les coûts économiques et opérationnels et faire du profit dans les possibilités des missions, tout en protégeant les processus businness qui supporte les objectifs de l'entreprise.

Le senior management a pour mission d'assurer que l'entreprise est capable d'accomplir sa mission. Mais cependant, plusieurs organisations ont de très petits budgets sécurité, d'où le besoin pour le management d'avoir un processus lui permettant de déterminer les dépenses qui seront faites et de façon stratégique.

Pour cela, plusieurs questions sont généralement posées dans une analyse de risque, qui est une étape importante du management des risques.

1. **Pourquoi doit-on réaliser une analyse des risques** ?
   - ✓ C'est important de le faire car, étant l'étape la plus importante du management des risques, elle permet à l'entreprise de décider de son avenir.

2. **Quand doit-on réaliser une analyse des risques** ?
   - ✓ Elle doit se faire chaque fois que l'argent ou une ressource doit être utilisé. Par exemple, elle doit se faire avant le démarrage d'une tache, d'un projet ou d'un cycle de développement dans une organisation.

3. **Qui doit conduire une analyse des risques** ?
   - ✓ Elle doit inclure les experts internes à l'organisation, car ils sont mieux placés pour comprendre les processus business de l'entreprise.

4. **En combien de temps une analyse des risques doit-elle se faire** ?
   - ✓ Elle doit se faire rapidement, avec le minimum d'impact sur les employés. Elle se fait généralement en jours, pas en semaine, ni en mois.

5. **Qu'est une analyse des risques peut analyser**?
   - ✓ Elle peut être utilisé pour revoir des taches, des projets et des idées, permettant ainsi de savoir par exemple si un nouveau contrôle doit être implémenté ou non.

6. **Quelles informations le résultat d'une analyse des risques peut fournir à l'organisation** ?

- ✓ Il permet à l'organisation d'examiner toutes les ressources concernées, de définir les priorités entre les niveaux de vulnérabilités et d'appliquer les contrôles adéquats.

7. **Qui devrait revoir le résultat d'une analyse des risques** ?
   - ✓ Etant donné que celui-ci est généralement classé top secret dans l'organisation, sa révision ne peut être faite que par le sponsor ou par ceux mandaté par le sponsor.

8. **Comment le succès d'une analyse des risques est – il mesuré** ?
   - ✓ Une façon de mesurer le résultat d'une analyse des risques est d'évaluer le nombre de fois que l'on est revenu sur une décision prise en se basant sur ce résultat.

Le management des risques doit être totalement intégré au « **System Development Life Cycle** » (SDLC) de l'organisation.

Le processus SDLC comporte les phases suivantes :

1. **Analyse**
2. **Design**
3. **Construction**
4. **Test**
5. **Maintenance**

Les activités du management des risques

1. **Analyse** : permet d'identifier les risques et besoins de sécurité
2. **Design** : permet de produire une architecture en fonction des besoins précédemment identifiés.
3. **Development** : permet de créer ou d'implémenter les contrôles de sécurité et contre-mesure pour satisfaire aux besoins exprimés.
4. **Test** : permet de tester les contrôles et de s'assurer que les décisions prises en fonction de ceux-ci réduisent effectivement les risques identifiées à un niveau acceptable.
5. **Maintenance** : permet de réexaminer les contrôles lorsqu'il ya un changement, une mise à jour ou une irrégularité.

Le management des risques est la responsabilité du management de l'entreprise. Chaque groupe a un rôle différent et ces rôles supportent les différentes activités de l'entreprise. Les différents rôles généralement retrouvés dans les organisations sont les suivantes :

◊ **Senior Management** : Son rôle est d'assurer que toutes les ressources nécessaires sont déployées et mises en œuvre pour atteindre les objectifs business. Il doit prendre en compte le résultat de l'analyse des risques.

◊ **Chief Information Security Officer :** Il est responsable du plan de sécurité de l'entreprise incluant toutes les composantes. Ses prises de décision doivent prendre en compte le management des risques.

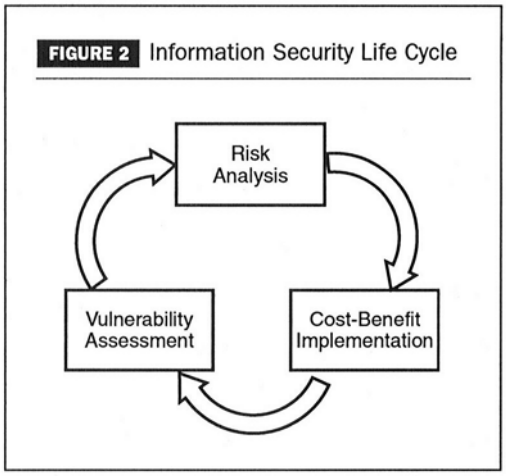
◊ **System and Information Owner :** Son rôle est de s'assurer que les contrôles mise en place permettent d'avoir l'intégrité, la confidentialité et la disponibilité de l'information dont la gestion lui est assignée.

◊ **Business Manager :** Il est responsable de toutes les décisions prises dans l'entreprise, y garantie un bénéfice essentiel et assure l'atteinte des objectifs business de l'organisation, tout en se basant sur les résultats de l'analyse des risques.

◊ **Information Security Manager :** Il est le responsable du programme de sécurité de l'organisation.

CYCLE DE VIE DE LA SECURITE DE L'INFORMATION

1. Risk analysis
2. Cost-Benefit Implementation
3. Vulnerability Assessment.



Le cycle de vie de la sécurité de l'information démarre avec une analyse des risques « **Risk Analysis** » qui permet d'identifier les risques qu'encouru par le business. Cette étape

permet par exemple au management de s'assurer les dépenses réalisées sont nécessaire à l'atteinte des objectifs de l'entreprise par rapport à sa stratégie globale.

L'étape suivante « **Cost-Benefit Implementation** » détermine les contrôles qui aideront à mitiger les risques à un niveau acceptable.

A la suite de l'implémentation de ces contrôles, il est nécessaire de réaliser une évaluation des vulnérabilités, ceci pour tester les contrôles et contre-mesures afin de s'assurer de leur efficacité.

PROCESSUS D'ANALYSE DES RISQUES

L'analyse des risques a trois livrables :

- L'identification des menaces
- L'établissement d'un niveau de risque en déterminant la probabilité qu'une menace arrive et son impact.
- L'identification des contrôles et contres mesures qui peuvent réduire le risque à niveau acceptable.

Pour obtenir ses livrables, il est nécessaire d'exécuter six étapes dans le processus d'analyses des risques qui est une partie du management des risques. Les six étapes sont les suivantes :

- **Définition des actifs** : La première étape dans le processus la ou les ressources qui seront analysées. Pour cela des techniques telles que les questionnaires, les interviews sur site, la revue de la documentation et les outils vérifications.
- **Identification des menaces :** Cette étape consiste à identifier les menaces, créer une liste complète et les classer par catégories (Menaces naturelles, Humaines, Environnementales). Les méthodes utilisées ici sont le développement des listes de contrôles, l'examen de l'historique des données et le brainstorming.
- **Détermination de la probabilité des menaces** : Cette étape consiste à déterminer pour chaque menace, la probabilité qu'elle arrive.
- **Détermination l'impact de la menace** : cette étape consiste pour chaque menace de déterminer l'impact qu'elle aura sur le business si celle-ci survenait.
- **Identification des contrôles et contre mesures** : Cette étape consiste à identifier les contrôles et contre-mesure permettant de réduire les risque à un niveau acceptable.
- **Documentation de l'analyse des risques :** Cette étape consiste à documenter le résultat de l'analyse des risques sous un format standard et sous forme d'état livré au propriétaire des actifs.

MITIGATION DU RISQUE

C'est une méthodologie systématique utilisé par les seniors managements pour réduire le risque des organisations. Les méthodes les plus connus de mitigation des risques sont les suivantes :

1. **Hypothèse de Risque** : cette méthode consiste à déterminer si la meilleure décision business est d'accepter le risque potentiel et de continuer l'exploitation.
2. **Allègement du Risque :** cette méthode consiste au senior management d'approuvé les contrôles et contre-mesure à mettre en place pour réduire les risques.
3. **Evitement du risque :** cette méthode consiste de choisir délibérément d'éviter le risque en éliminant le processus qui pourrait causer le risque.
4. **Limitation du risque :** cette méthode consiste à limiter le risque en implémentant les contrôles qui minimise l'impact déficitaire de la menace.
5. **Planification du risque :** cette méthode consiste à décider de manager les risques en développant une architecture qui fait ressortir les priorités, implémente et maintient les contrôles.
6. **Transfert du risque :** cette méthode consiste à transférer le risque en utilisant d'autres options pour compenser les pertes (Ex : les polices d'assurance).

LES CATEGORIES DE CONTROLE

Dans l'architecture de la sécurité de l'information, il y a quatre couches de contrôle. Nous :

1. L'évitement
2. L'assurance
3. La détection
4. La récupération / la reprise

Il est aussi possible de créer un ensemble de contrôle liée à l'entreprise tel que :

1. **Les contrôles d'opération** (Backup, plan de reprise, analyses des risques, contrôle antivirus, dépendance d'interface, maintenance, « service-level agreement », Gestion du changement, l'analyse de l'impact du business).
2. **Les contrôles d'application** (Contrôle des applications, Teste de réception, Entrainement, promotion aux procédures du produit, stratégie corrective).
3. **Les contrôles de sécurité** (Politique, entrainement, révision, classification des actifs, management du support, sensibilisation de sécurité, contrôle d'accès).
4. **Les contrôles système** (Gestion du changement, audit des logs système).
5. **Les contrôles physiques** (Sécurité physique).

COST-BENEFIT ANALYSIS

Cette étape est conduite par l'organisation après avoir réalisé une étude de faisabilité et de l'efficacité de tous les contrôles identifiés. Ce processus est réalisé pour déterminer l'impact de l'implémentation de chaque nouveauté ou de la mise en œuvre du contrôle et déterminer aussi l'impact de la non implémentation des dits contrôles.

Les coûts d'implémentation de cette analyse prennent en compte les éléments suivants :

- Les couts inclus les dépense initial pour le matériel et le logiciel
- La réduction de l'efficacité opérationnelle
- Implémentation des politiques et procédures additionnelles pour supporter les nouveaux contrôles.
- Les coûts d'embauche du staff additionnel, au minimum la formation du staff existant.
- Les coûts d'éducation du support du personnel pour maintenir l'efficacité des contrôles.