Analyse des risques : méthode simplifiée

1. Définir ce qui a de la valeur

En fonction de l'organisation, définir ce qui a de la valeur pour le métier. Comme on réalise une analyse des risques orientées SI, il serait logique que l'attention soit portée sur de l'information.

P.ex.
- dans une entreprise réalisant de la comptabilité : les bilans comptables.
- dans un hôpital : les dossiers médicaux des patients.

2. Proposer une échelle des conséquences

P.ex. Celle-ci-dessous est tirée de la méthode Ebios.

Derrière la colonne « conséquences » se cache la notion d'impact : financier, image, juridique, …
C'est, au regard de ces impacts que le métier pourra déterminer le niveau de conséquence/de gravité d'un évènement (cf. point 3). < ! > c'est bien au métier de décider < ! >

ÉCHELLE	CONSÉQUENCES
G4 CRITIQUE	Incapacité pour la société d'assurer tout ou partie de son activité, avec d'éventuels impacts graves sur la sécurité des personnes et des biens. La société ne surmontera vraisemblablement pas la situation (sa survie est menacée).
G3 GRAVE	Forte dégradation des performances de l'activité, avec d'éventuels impacts significatifs sur la sécurité des personnes et des biens. La société surmontera la situation avec de sérieuses difficultés (fonctionnement en mode très dégradé).
G2 SIGNIFICATIVE	Dégradation des performances de l'activité sans impact sur la sécurité des personnes et des biens. La société surmontera la situation malgré quelques difficultés (fonctionnement en mode dégradé).
G1 MINEURE	Aucun impact opérationnel ni sur les performances de l'activité ni sur la sécurité des personnes et des biens. La société surmontera la situation sans trop de difficultés (consommation des marges).

3. Définir ce qui « fait peur » et à quel point « ça fait peur »

- Pour définir ce qui fait peur, il faut mettre en lien « ce qui a de la valeur » et les grands objectifs de la sécurité.
  P.ex.
  - Je crains que le dossier médical d'un patient soit altéré (Intégrité),
  - Je crains que les bilans comptables de mes clients soient effacés (Disponibilité),
  - …
- Pour définir « à quel point ça fait peur », j'utilise l'échelle de gravité.

Je synthétise (p.ex. dans un tableau)

Evènements	Gravité/Impacts/Conséquences
Je crains que le dossier médical d'un patient soit altéré.	3

4. Définir la probabilité des évènements craints

En se basant sur les mesures de sécurité déjà en place et sur l'état du SI, définir la probabilité de réalisation de l'évènement « foireux ». Pour cette étape, le regard d'un expert technique du SI sera certainement utile.

P.ex. la probabilité de perdre une information diminue si on dispose de backup.

Il faut bien comprendre qu'une mesure de sécurité n'influence pas la gravité (ou les conséquences) d'un risque (un évènement craint) mais bien sa probabilité de concrétisation en un évènement craint. Il faut donc se méfier des abus de langage et des paroles du genre « ce n'est pas grave, on a un backup… ».

Cette distinction est plus facile à comprendre si on introduit la notion de criticité :

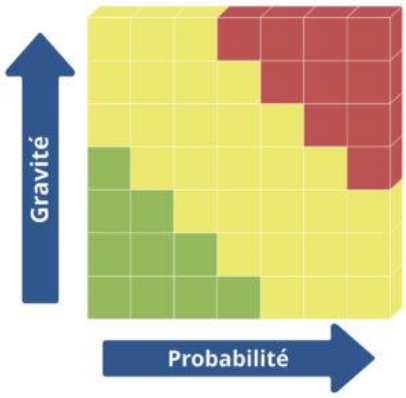
Criticité = Probabilité X Gravité

Cette notion se traduira par la matrice de criticité des risques (cf. étape 5).

5. Construire la matrice de criticité des risques

Placer les risques dans une matrice XY avec :

- X = Probabilité
- Y = Gravité



6. Gérer les risques

En fonction de la stratégie de gestion des risques de l'organisation, proposer des mesures de sécurité pour ramener les risques dans une zone « acceptable ».

Le plan de gestion du risque doit mettre en lumière les mesures envisagées, les délais, les budgets alloués, les responsables techniques,…