CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Gérer ses risques avec la norme ISO 27005 et MEHARI

Comment passer des ambiguïtés de la norme aux spécifications fonctionnelles d'une méthode

Gérer les risques : pourquoi ?

Objectifs cités dans la norme ISO/IEC 27005 :

En introduction , au chapitre 1 – Domaine d'application :

- La présente Norme internationale … est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion de risque.

Gérer les risques : pourquoi ?

Objectifs cités dans la norme ISO/IEC 27005 :

Dans les considérations générales (par 7.1) :

- Il est essentiel de déterminer l'objectif de la gestion du risque en sécurité de l'information puisqu'il influence l'ensemble du processus … L'objectif peut être :
  - une réponse aux exigences d'un SMSI,
  - la conformité avec la loi et la preuve de la mise en œuvre du devoir de précaution,
  - la préparation d'un plan de continuité de l'activité,
  - la préparation d'un plan de réponse aux incidents,
  - la description des exigences en matière de sécurité de l'information pour un produit, un service ou un mécanisme

Gérer les risques : pourquoi ?

Objectifs réaffirmés de MEHARI avec la version 2010 :

Les objectifs fondamentaux d'une gestion … des risques auxquels l'entreprise ou l'organisation est exposée, sont :

- Identifier tous les risques auxquels l'entreprise est exposée.
- Quantifier le niveau de chaque risque.
- Prendre, pour chaque risque considéré comme inadmissible, des mesures pour que le niveau de ce risque soit ramené à un niveau acceptable.
- …

Gérer les risques : pourquoi ?

Objectifs réaffirmés de MEHARI avec la version 2010 :

Les objectifs fondamentaux d'une gestion … des risques auxquels l'entreprise ou l'organisation est exposée, sont :

- …
- Mettre en place, comme outil de pilotage, un suivi permanent des risques et de leur niveau.
- S'assurer que chaque risque, pris individuellement, est bien pris en charge et a fait l'objet d'une décision d'acceptation, de réduction, d'évitement ou de transfert.

Gérer les risques : comment ?

L'objectif de MEHARI de gestion directe, et individualisée si nécessaire, des risques nécessite des spécifications particulières et complémentaires, pour :

- L'identification des risques
- L'estimation des risques
- La gestion des risques

L'identification des risques

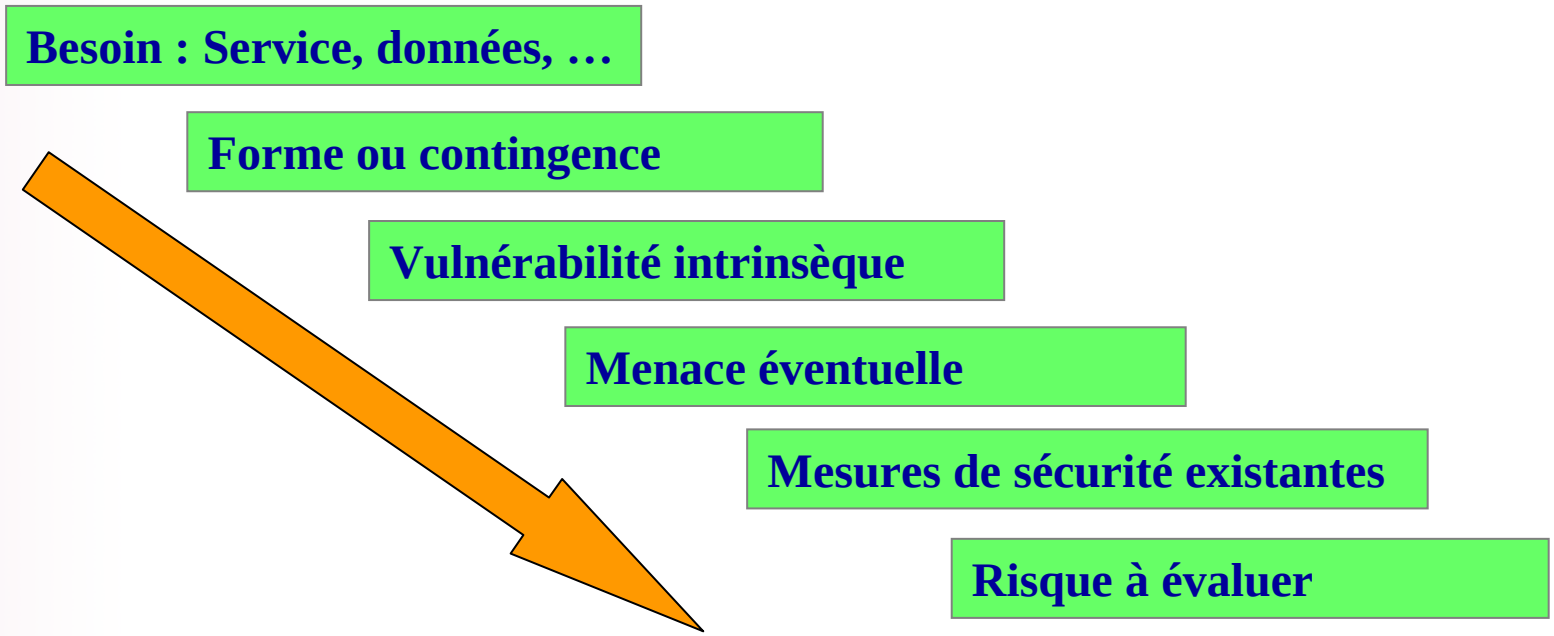
Les étapes prévues par la norme ISO 27005 sont :

- L'identification des actifs
- L'identification des menaces
- L'identification des mesures de sécurité existantes
- L'identification des vulnérabilités
- L'identification des conséquences

… et la norme précise, en introduction, que ces activités peuvent être effectuées dans un ordre différent selon la méthodologie appliquée.

L'identification des risques

MEHARI 2010 précise le processus d'identification des risques selon le schéma suivant :



L'identification des risques

Définitions complémentaires nécessaires :

Les actifs

Pour garantir que tous les risques seront identifiés, MEHARI 2010 part de la notion de « besoin de l'activité ».

Ce besoin peut revêtir trois formes :

- Un besoin de services
- Un besoin d'informations (ou données) nécessaires à l'accomplissement des services
- Un besoin de conformité (des processus et comportements) à un référentiel (éthique, réglementaire, légal, etc.)

La recherche exhaustive de ces besoins permet d'identifier les actifs « primaires » de l'entreprise ou de l'organisme

L'identification des risques

Définitions complémentaires nécessaires

Les actifs

Pour garantir que tous les risques seront identifiés, MEHARI 2010 précise comment ces besoins ou actifs primaires se matérialisent :

- Sous quelles formes ou sur quels supports
- En dépendant de quelles contingences

La recherche exhaustive de ces matérialisations permet d'identifier les actifs « secondaires » pour chaque type d'actif primaire

L'identification des risques

Définitions complémentaires nécessaires

Les vulnérabilités

La définition donnée à ce terme par l'ISO 27000 est la suivante :

« Faille dans un **actif** ou dans une **mesure de sécurité** qui peut être exploitée par une **menace** ».

Les deux aspects de cette définition sont de nature totalement différente.

L'identification des risques

Définitions complémentaires nécessaires

Les vulnérabilités

Pour garantir que tous les risques seront identifiés, MEHARI 2010 précise ces deux notions :

- **Vulnérabilité intrinsèque** : caractéristique intrinsèque d'un actif pouvant être le point d'application d'une menace
- **Vulnérabilité contextuelle** : faille dans un dispositif de sécurité pouvant être exploitée par une menace

L'identification des risques doit s'appuyer sur la recherche des vulnérabilités intrinsèques

L'identification des risques

Définitions complémentaires nécessaires

Les menaces

Pour pouvoir estimer les risques, la description de la menace doit comprendre tous ses éléments caractéristiques.

MEHARI 2010 précise ce que doit comprendre cette description :

- **L'événement déclencheur** et son caractère volontaire ou accidentel
- **L'acteur** déclenchant cet événement
- **Les circonstances** dans lesquelles survient cet événement

L'identification des risques doit s'appuyer sur une recherche de l'ensemble de ces éléments

L'estimation des risques

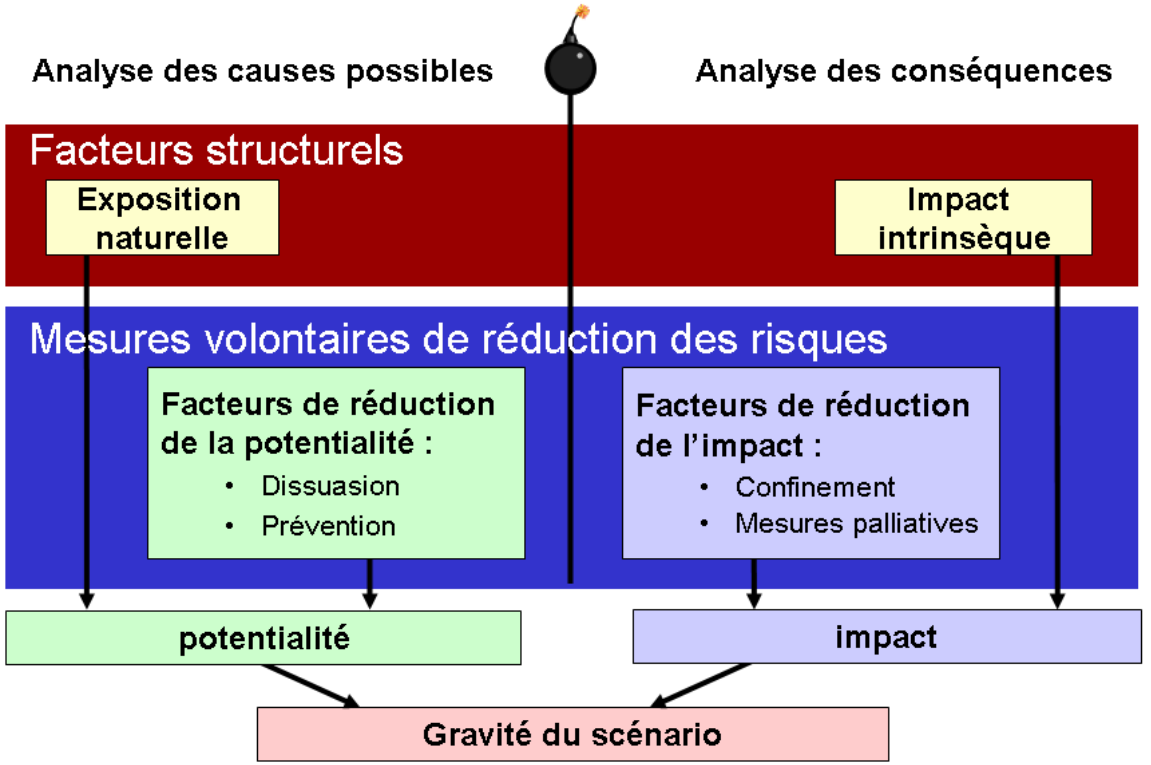
L'estimation des risques nécessite un modèle de risque et ce modèle doit être adapté à l'objectif fixé pour la gestion des risques.

Les objectifs de MEHARI (en tant que méthode de gestion de risques) impose un modèle qui tienne compte :

- **Des facteurs structurels** liés à l'activité et au contexte de l'entreprise
- **Des mesures de sécurité mises en œuvre**
- **De la qualité de ces mesures**

L'estimation des risques

Le modèle de risque MEHARI est conforme depuis l'origine à cette spécification et n'évolue que très peu : transfert du risque reporté en phase de traitement.



La gestion des risques

La gestion directe et individualisée des risques doit s'appuyer sur le modèle de risque et impose en outre que l'on sache fixer des objectifs en termes de :

- Services de sécurité à améliorer
- Niveaux de qualité cibles pour ces services

et que l'on sache mesurer l'atteinte des objectifs.

Ceci est difficilement envisageable sans une base de connaissance comprenant une base d'audit des services de sécurité.

Conclusion

L'ensemble des considérations développées à partir des objectifs complémentaires fixés (par MEHARI) pour la gestion des risques conduit à des principes fondamentaux et des spécifications fonctionnelles.

Ces principes et spécifications sont documentés et justifiés dans la version 2010 de MEHARI.

Merci de votre attention