***1.1.1 Notion de risques informatiques***

Les organismes :

Origine IFACI (institut Français de l’Audit et du Contrôle Interne)

* Risque : possibilité que se produise un évènement qui aura un impact sur la réalisation des objectifs.

Il se mesure en termes de conséquences et probabilités

* Cartographie des risques : positionnement des risques majeurs selon différents axes tels que :

• L’impact potentiel

• La probabilité de survenance.

• Le niveau actuel de maîtrise des risques

La prise en compte des risques au niveau des entreprises et en fonction des compétences des différentes personnes n’est pas toujours la même.

D’où la charte informatique pour les obligations et les droits de l’utilisateur.

***1.1.2 Approches du management par les risques***

Matériel : serveur, pc, surcharge, routeur, matériel réseau, alimentation, virus sur matériel

Logiciel : pare feu, OS, antivirus, paramétrage logiciel

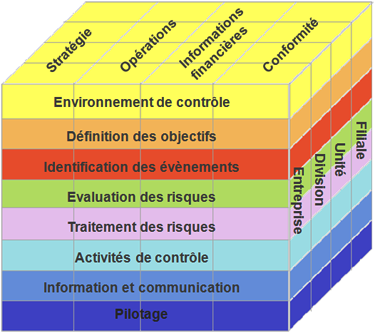
Humain : visiteurs, utilisateurs

Autres : catastrophes naturelles, incendies, inondations…

Cette approche de risques est apparue à la fin des années 1950 aux USA.

Au départ, cette notion de risque vient d’une limitation aux contrats d’assurance.

* Gouvernement d’entreprise et obligation de contrôle des risques.
* COSCO II : C’est un cube qui visualise la gestion du risque en 3D, du point de vue des objectifs de l’entreprise tel que le contrôle interne et les composantes de la gestion du risque à l’échelle de l’entreprise



Dans Risk IT (Information Technology) de ISACA (Information Systems Audit and Control Association) :

Le risque informatique est désigné comme un risque métier qui est associé à l’utilisation de l’informatique :

-L’utilisation

-La possession

-L’exploitation

-L’implication

-L’influence

-L’adoption de l’informatique dans une organisation

Exemples et lien risques métiers :

-Interruption des activités d’une entreprise en raison d’une indisponibilité du SI :

. Panne d’un composant du réseau (par exemple un routeur)

. Incendie de la salle machine

. Intrusion d’un pirate et destruction des bases de données.

. Plan de secours n’ayant pas suivi les évolutions récentes des systèmes.

* **L’incendie :**

• Non-respect des normes : protection passive, détection, propagation, extinction

* **Les dégâts des eaux :**

• L’environnement du bâtiment (naturel, eau courante, stagnante, terrain, climat )

• Artificiel (canalisations, réservoirs)

• Dispositifs de climatisation

• Condensation

• Entretiens inadéquats

* **Les accès :**

• Perturbations et désordres occasionnés par du personnel extérieur au service informatique

• Le vol : support de données, matériels

• Le sabotage

• L’attentat

* **La fiabilité technique et énergétique :**

• La panne ou déficience électrique

• Le conditionnement de l’air

• Pièce défectueuse (fusible par exemple)

• L’incapacité du personnel informatique à localiser l’origine d’une panne

Les risques matériels et logiciels :

* Le matériel et la maintenance :

• Le non-respect des délais de livraison

• Livraison non conforme

• L’indisponibilité du matériel

• La fiabilité du matériel

• Panne lors d’une phase critique de production

• Restitution des données incorrectes

* Les logiciels de base et la maintenance

• Perte d’exploitation pour livraison tardive

• Non-Conformité

• Logiciel obsolète ne supportant pas de nouvelles technologies

• La non-disponibilité du logiciel

• Le manque de fiabilité

• Les dysfonctionnements liés au virus

* L’absence de systèmes de secours