ANALYSE DES RISQUES II

Introduction

- La gestion des risques est définie par l'ISO comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.
- But:

1. Améliorer la sécurisation des systèmes d'information.
2. Justifier le budget alloué à la sécurisation du système d'information.
3. Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Definitions

- il existe plus de 200 méthodes de gestion des risques.
- l'ISO définit un risque par la combinaison de la probabilité d'un événement et de ses conséquences.
- l'équation du risque :

RISQUE = MENACE * VULNÉRABILITÉ * IMPACT

Définitions

- RISQUE = MENACE * VULNÉRABILITÉ * IMPACT
- Menace: la source du risque, c'est l'attaque possible d'un élément dangereux pour les assets. C'est l'agent responsable du risque.
- Vulnérabilité: est la caractéristique d'un asset constituant une faiblesse ou une faille au regard de la sécurité.
- Impact: représente la conséquence du risque sur l'organisme et ses objectifs,
  - L'impact peut, quant à lui, être qualifié en termes de niveau de sévérité.

Définitions

- La gravité est l'estimation de la hauteur des effets d'un événement redouté ou d'un risque ; elle représente ses conséquences ;
- La vraisemblance est l'estimation de la possibilité qu'un événement redouté, un scénario de menace ou un risque, se produit ; elle représente sa force d'occurrence ;
- Exemple
  - La vraisemblance qu'une personne non autorisée entre dans la salle machine pour lancer une commande sur la console est basse si un dispositif contrôle l'accès à la salle (lecteur de badge, sas, caméra, etc.). La vraisemblance sera nettement plus haute si rien ne protège la salle machine.

Difficultés courantes de l'appréciation des risques

Commencer l'appréciation

- Si l'entreprise n'avait encore jamais effectué d'appréciation des risques, le premier travail consiste à choisir une méthode.
- Le responsable du projet a l'embarras du choix.
- Il est illusoire d'espérer trouver du premier coup une méthode d'appréciation des risques, applicable telle quelle, avec les bons critères de risque, la bonne typologie d'actifs, les bonnes définitions de niveaux de risque et la bonne formule de calcul.

Inventaire des actifs

- Qu'est-ce qu'un actif d'information ?
- Exemples d'éléments pouvant être considérés comme actifs d'information : les données du client, les documents, les serveurs, les logiciels, la salle machine.

Inventaire des actifs
-Différents niveaux d'actifs:

- **Actif primaire:** toute information ayant de la valeur pour le SI, indépendamment de son support.

  - Exemple : actif primaire
  - Les actifs primaires le plus souvent répertoriés sont : le fichier client, les méthodes industrielles, les principaux services fournis aux clients, le savoir-faire de l'entreprise, etc.

Inventaire des actifs
-Différents niveaux d'actifs: suite

- **Actif secondaire**(actifs support): on s'intéresse au support de l'information. Il peut s'agir de logiciels, de fichiers, d'équipements système ou réseau, de documentations (papier ou électronique), de locaux où se déroulent les activités sensibles, etc.

Inventaire des actifs
-Différents niveaux d'actifs: suite

Exemple : actifs primaires et actifs support:

- Considérons une caisse de retraite dont le cœur de métier est le calcul et le paiement de la retraite complémentaire de ses allocataires. Elle fournit aussi des services tels que des bourses d'études pour les enfants des cotisants, des voyages à coût réduit et tous types de petits services secondaires.
- Lors de l'appréciation des risques, deux niveaux d'actifs peuvent être décidés :

Inventaire des actifs
-Différents niveaux d'actifs: suite

- **1. Actifs primaires :** paie des employés, bourses d'études pour les fils des cotisants, service de voyages, liquidation de retraite, paiement des échéances pour les allocataires. Les actifs primaires « liquidation de retraite » et « paiement des échéances » ont une importance capitale pour la caisse de retraite. Ils seront donc décomposés en actifs plus détaillés. Quant aux autres, ils ne nécessitent pas un niveau plus fin car ils ne sont pas capitaux pour la survie de la caisse de retraites.
- **2. Actifs support** liés aux actifs primaires « liquidation de retraite » et « paiement des échéances » :

  – codes sources des programmes de liquidation de retraite et de paiement des échéances ;

  – procédures d'exploitation de ces programmes ;

  – base de données centrale des allocataires dans le mainframe ;

  – mainframe et imprimante système ;

  – personnel du service « liquidation » et du service « paiement des échéances » ;

  – ingénieur système ;

  – opérateurs du mainframe.

Valoriser les actifs

- Une étape importante dans l'appréciation des risques consiste à donner une valeur à chaque actif, de cette valeur dépendra le niveau de risque et, donc, les moyens qui seront déployés pour le protéger.

Valoriser les actifs (suite)

- Exemple de critères de valorisation des actifs

Niveau	Confidentialité	Intégrité	Disponibilité
0	Aucune conséquence	Aucune conséquence	Aucune contrainte
1	Perte < un jour de CA	Perte < un jour de CA	Remise à disposition en deux semaines
2	Perte < une semaine de CA	Perte < une semaine de CA	Remise à disposition en une semaine
3	Perte < un mois de CA	Perte < un mois de CA	Remise à disposition en 48 heures
4	Perte > un mois de CA	Perte > un mois de CA	Remise à disposition dans la journée

Valoriser les actifs (suite)

- Exemple: valorisation de l'actifs ***catalogue*** et de l'actif ***fichier clients, et leur c***onfrontation aux critères du tableau
- **1. Catalogue (0,1,4) :**

la note 0 signifie que la perte de confidentialité du catalogue a été valorisée à zéro, c'est-à-dire qu'elle n'a « aucune conséquence ». C'est bien normal puisque par nature, le catalogue a vocation à être public. La note d'intégrité a été mise à 1. Cela signifie que si une erreur survient dans le catalogue, cela aura pour conséquence une perte financière inférieure à un jour de chiffre d'affaires (CA). Enfin, la note de 4 pour la disponibilité montre que le catalogue doit être remis en ligne dans la journée.

Valoriser les actifs (suite)

- Exemple: valorisation de l'actifs ***catalogue*** et de l'actif ***fichier clients, et leur c***onfrontation aux critères du tableau
- 2. Fichier clients (4,2,2) : la valeur de confidentialité a été estimée à 4 car le fichier client est le capital incorporel de l'entreprise. Sa divulgation conduit à des pertes pouvant dépasser un mois de chiffre d'affaires. Un problème d'intégrité aura pour conséquence la perte d'une semaine de chiffre d'affaires. Enfin, si jamais un incident rend indisponible le fichier client, cette perte de disponibilité sera supportable pendant une semaine.

Estimer le risque

- Il faut tenir compte de la vraisemblance du risque Celle-ci peut être mesurée par une note, par une probabilité ou par niveaux (nul, faible, moyen, élevé)
- Exemple : formule de calcul de niveau de risque
  - La façon la plus simple pour définir le niveau de risque consiste à retenir le maximum des trois composantes de la valeur de l'actif (confidentialité, intégrité, disponibilité), puis à le multiplier par la vraisemblance.)
  - Risque = Max (Confidentialité, Intégrité, Disponibilité) × Vraisemblance

Estimer le risque (suite)

- Application aux actifs de l'exemple précédent (catalogue et fichier client) :

– si la menace de divulgation du catalogue a une vraisemblance de 3, le risque associé sera valorisé de la façon suivante :

$$\text{Max } (0,1,4) \times 3 = 12 \text{ ;}$$

– si la menace de divulgation du fichier client est estimée à 2, le risque associé sera valorisé de la façon suivante :

$$\text{Max } (4,2,2) \times 2 = 8.$$

Mesures de sécurité

- Considérer les actifs seuls, en faisant abstraction de leur environnement?
- Considérer les actifs en tenant compte de leur environnement?
- Exemple : serveur web d'une agence de voyage sur Internet
  - Considérons un site web qui fournit un service de réservations de voyages sur Internet. Cet actif est valorisé de la façon suivante : serveur web (2,4,4). En effet, une perte d'intégrité du serveur ou une indisponibilité du service peuvent avoir des conséquences catastrophiques.
  - Si nous considérons le serveur web indépendamment de son milieu, la vraisemblance d'une attaque du serveur (par exemple par déni de service) est très élevée. Elle sera évaluée à 5 (sur une échelle de 5).
  - En revanche, si nous tenons compte du fait que le serveur est protégé par un garde-barrière, que son système d'exploitation a déjà été sécurisé et qu'un relais applicatif se charge de filtrer toutes les requêtes HTTP malveillantes, cela diminue considérablement la vraisemblance d'une attaque. Aussi la note sera-t-elle portée à 2.

Étude de cas d'appréciation de risques (TD)

- Exemple simplifié d'appréciation des risques

Actif	Responsable	Valorisation			Vulnérabilités	Menaces	Vraisem-blance	Risque
		C	I	D				
Serveur web de vente par correspon-dance	DSI	2	4	4	Système non à jour	Exploitation d'une vulnérabilité connue	3	
					Pas de filtrage d'URL	Injection SQL et XSS	2	
Ordinateur portable du commercial	Responsable Service commercial	4	1	1	Équipement léger et peu encombrant	Vol	3	

Étude de cas d'appréciation de risques (TD)

- Quels sont les actifs traités dans ce tableau?
- Quel est le type de chacun?
- La valorisation de l'actif serveur web, dépend-t-elle des vulnérabilités et des menaces?
- Mesurer le risque pour chaque menace.
- Quel est le paramètre qui fait varier le niveau de risque entre une menace et une autre ?

Actifs primaires vs secondaires

- Plusieurs Actifs Secondaires sont associés à un même Actif Primaire
- Valeur de l'Actif secondaire= Valeur de l'Actif Primaire associé

Valeur d'un Actif

- Disponibilité : Quelles seraient les conséquences en cas d'indisponibilité ?
- Confidentialité : Quelles seraient les conséquences en cas de divulgation ?
- Intégrité : Quelles seraient les conséquences en cas de perte d'intégrité ?
  - 1 -> négligeables : les effets sont indécelables
  - 2 -> faibles : les effets affectent des éléments de confort
  - 3 -> significatifs : les effets affaiblissent la performance
  - 4 -> élevés : les effets affectent toute l'unité
  - 5 -> critiques : les effets mettent en danger les missions de l'unité

Vraisemblance (1)

- la Vraisemblance d'une Menace sur un actif s'évalue en fonction de la Probabilité d'Occurrence de la Menace (POM) et de la Facilité d'Exploitation de la Vulnérabilité (FEV).

Vraisemblance de la Menace = POM + FEV – 1

Vraisemblance (2)

- La POM étant valorisée sur 3 niveaux
  - 1: Faible,
  - 2: Moyen,
  - 3: Forte
- La FEV étant valorisée sur 3 niveaux
  - 3: Facile,
  - 2: Moyen,
  - 1:Difficile

La Vraisemblance de la Menace est valorisée de 1 à 5

Le Niveau de Risque est valorisé de 1 à 25

Niveau Risque = Valeur de l'Actif * Vraisemblance de la Menace

Valeur de l'Actif=max(C,I,D)

Traitement du Risque (1)

- Pour chaque Menace qui pèse sur un actif à travers une vulnérabilité donnée, en fonction du niveau de risque calculé, on détermine alors s'il faut traiter le risque
  - Inutile,
  - Envisageable,
  - Nécessaire,
  - Obligatoire
- Quel type de traitement du risque adopter ?
  - Accepter -> Ne rien changer !
  - Diminuer -> Engager des actions pour réduire le risque
  - Transférer -> Engager des actions pour déplacer le risque
  - Eviter -> Refuser le risque !

(A)ccepter
(D)iminuer = réduire
(T)ransférer
(E)viter = refuser

Traitement du Risque (2)

- Pour les niveaux de risque compris entre :
  - 1 à 5 : traitement inutile => A
  - 6 à 11 : traitement envisageable => A,D,T ou E ?
  - 12 à 19 : traitement nécessaire => A,D,T ou E ?
  - 20 à 25 : traitement obligatoire => A,D,T ou E ?

Traitement du Risque (3)

- Pour chaque Menace si l'analyse de risque conclue:
  - Accepter le risque -> Aucune action à prévoir
  - Diminuer le risque -> Choisir une mesure dans la norme 27001
  - Transférer le risque -> Déplacer la responsabilité du risque sur un tiers
  - Eviter le risque -> Supprimer l'Actif, Arrêter le service !

Techniques et outils en matière de transfert des risques

- « transfert des risques » signifie les manières d'éviter d'avoir à payer pour les erreurs associées aux activités et produits contrôlés par des tiers (partenaires d'affaires, sous-traitants, fournisseurs, etc.). L'idée est de faire en sorte que la partie la mieux équipée pour contrôler les risques assume la responsabilité. Le but est également de s'assurer que ces tiers aient la capacité financière de payer.
- Les outils principaux en matière de transfert des risques incluent notamment :
- Certificat d'assurance (CA). confirme quelle couverture est en vigueur au moment de son émission, ainsi que sa date d'expiration. (Une mise à jour des certificats doit être demandée chaque année, avant leur expiration.)
- Entente de non-responsabilité. Ce document est à l'effet qu'une partie ne tiendra pas l'autre partie responsable, sous certaines circonstances particulières. Par exemple, un peintre, embauché par le propriétaire d'un bâtiment, fournit à ce dernier une entente de non-responsabilité. Le peintre renverse de la peinture sur une automobile à proximité. Le document prévoit que le peintre, et non pas le propriétaire du bâtiment, sera responsable des dommages.)