Cours Gestion des Risques

Les différentes méthodologies ou normes

- 200 méthodologies existantes
  - Sectorielles ou globales
  - 80 % obsolètes ou non maintenues
- En France:
  - MEHARI, produite par le CLUSIF
  - EBIOS, produite par l'ANSSI
  - ISO27005, produite par l'ISO

Définition

La gestion du risque SSI consiste à coordonner, de manière continue, les activités visant à diriger et piloter un organisme vis-à-vis des risques. Elle inclut l'appréciation, le traitement, l'acceptation et la communication relative aux risques SSI.

Définition

- L'appréciation des risques SSI représente l'ensemble du processus d'analyse (mise en évidence des composantes) et d'évaluation du risque (estimation de leur importance).
- L'appréciation consiste tout d'abord à décrire le contexte: l'organisme, le système d'information (SI), les éléments essentiels à protéger (informations, fonctions...), les entités sur lesquelles ils reposent, les enjeux liés au SI, les contraintes à prendre en compte...

Définition

- Les besoins de sécurité des éléments essentiels doivent être ensuite être exprimés (couramment en termes disponibilité, d'intégrité et de confidentialité).
- Les menaces pesant sur le SI doivent être identifiées et caractérisées en terme d'opportunité (représentant l'incertitude de ces menaces)
-

Définition

- Les risques doivent enfin être déterminés en confrontant les menaces aux besoins de sécurité.
-

Définition

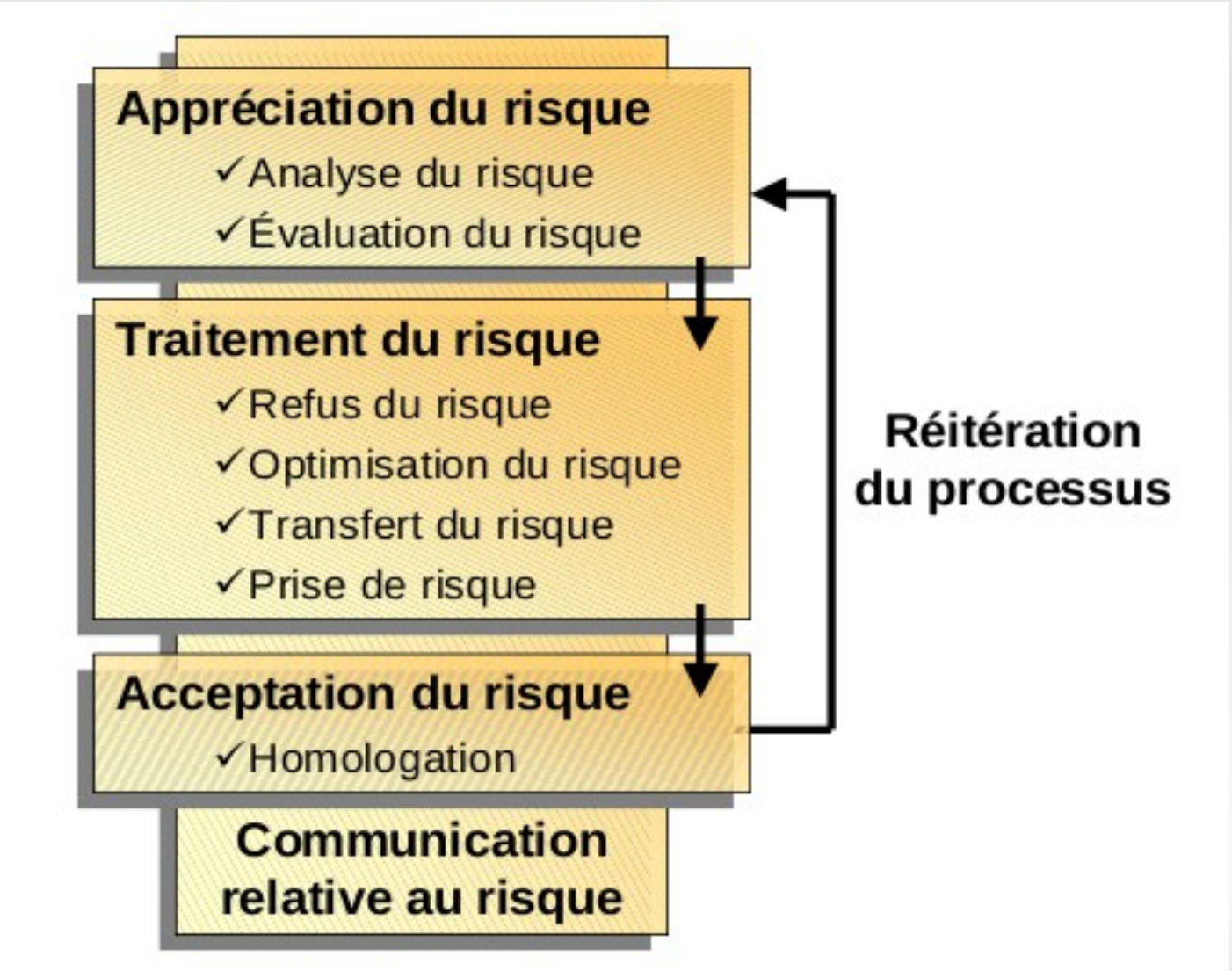
- Le traitement des risques représente le processus de sélection et de mise en oeuvre des mesures visant un refus, une optimisation, un transfert ou une prise de risque.
- Il consiste à identifier les objectifs de sécurité en déterminant le mode de traitement (refus,optimisation, transfert ou prise de risque) et en tenant compte des éléments du contexte.
-

Définition

- Puis détermination d'exigences de sécurité satisfaisant les objectifs de sécurité identifiés et décrivant la manière de traiter les risques (dissuasion, protection, détection, récupération, restauration, compensation...)
- Enfin les mesures de sécurité, techniques ou non, spécifiées par les exigences de sécurité peuvent être mises en oeuvre.
-

Définition

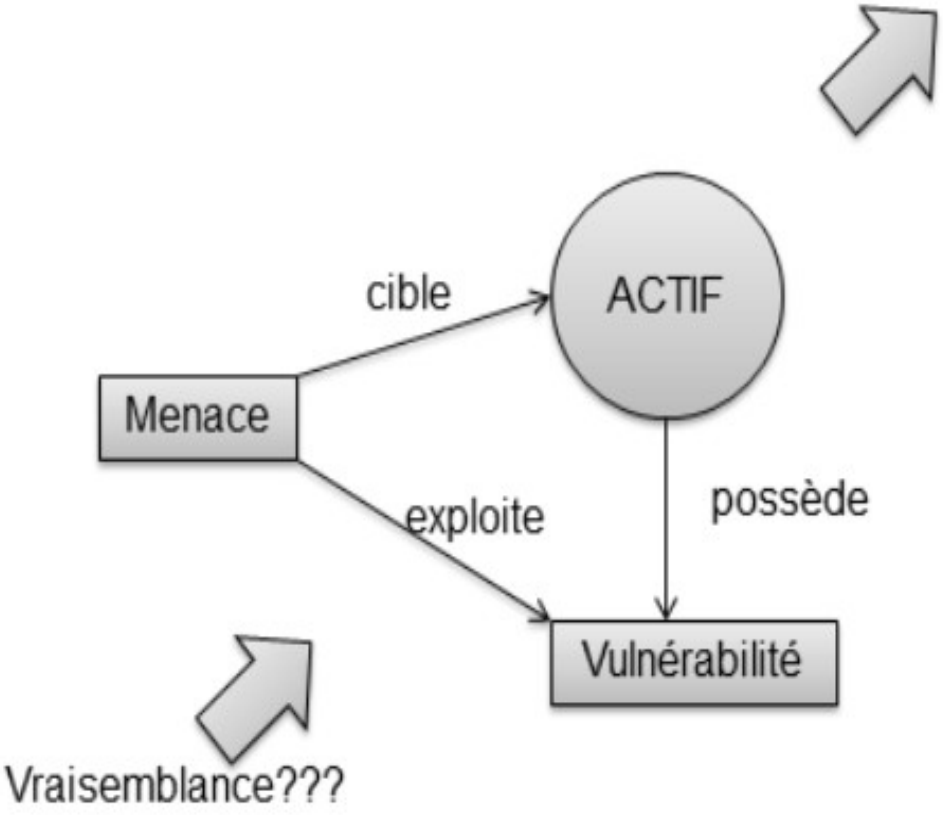
- L'acceptation des risques SSI représente la décision d'accepter les risques traités.
- La communication relative aux risques SSi répresente l'échange ou le partage d'informations concernant les risques.


Appréciation du risque
✓Analyse du risque
✓Évaluation du risque
Traitement du risque
✓Refus du risque
✓Optimisation du risque
✓Transfert du risque
✓Prise de risque
Acceptation du risque
✓Homologation
Communication relative au risque
Réitération du processus

Risque?

- Le risque de sécurité des systèmes d'information est une combinaison d'une menace et des pertes qu'elle peut engendrer (ANSSI)
- Ou
- Probabilité qu'une menace puisse exploiter une vulnérabilité d'un actif ou d'un groupe d'actifs et cause un impact non négligeable sur l'organisation ou ses activités (ISO27005)

Risque?



Impacts:

Disponibilité (Ex: données inaccessibles)
Intégrité (Ex: données ont été modifiées)
Confidentialité (Ex: données ont été rendues publiques)

Conséquences:

Juridiques, légales, sur l'activité business, l'image et la réputation...

Risque?

- Deux notions fondamentales
  - Incertitude
  - dommage

Concepts

- Actif:
  - Tout ce qui a une valeur pour l'organisme
    - Donc qui nécessite une protection
  - Typologie des actifs
    - Actifs primordiaux
      - Processus
      - Information
    - Actifs de support
      - Logiciel
      - Matériel
      - Réseau
      - Personnes
      - Sites: Organisation

Concepts

- Actif: Exemples
  - Logiciel: OS
  - Logiciel: messagerie
  - Matériel: serveur
  - Personne: ingénieur
  - Site: Salle Machine
  - Processus: processus de production
  - Information: liste des clients
  - Logiciel: Fichier client

Concepts

- Propriétaire:
  - Un propriétaire est associé à chaque actif
  - Responsable de l'actif en termes de:
    - Production
    - Développement
    - Maintenance
    - Utilisation
    - Sécurité (suivi des actions)
  - Ne possède pas nécessairement les droits de propriété sur l'actif
  - C'est la personne de choix pour valoriser l'actif

Exercice

L'entreprise Senokaze, engagé dans les énergies nouvelles fabrique des éoliennes de toutes tailles.

Elle est en concurrence avec le groupe EnergySol spécialisé en panneaux solaires et qui souhaite se lancer sur le marché de l'éolien.

Senokaze est composé des services suivants:

R&D

Production

Commercial

Administratif

Juridique

Les ingénieurs R&D travaillent sur les données les plus sensibles de l'entreprise. Les commerciaux utilisent des ordinateurs portables contenant les documentations commerciales et le fichier client.

L'ensemble de la gestion administrative est réalisée au siège.

Exercice

La gestion de risque porte sur le processus de création de nouveaux produits.

Les ingénieurs R&D développent des nouvelles technologies innovantes et des nouveaux produits basés sur ces technologies.

Les données R&D sont présentes sur les serveurs du service R&D et sur les ordinateurs portables des ingénieurs.

Les ingénieurs sont amenés à voyager pour travailler avec des équipes étrangères.

Ils utilisent tous types de connexions réseau (salon aéroport, hôtel, réseaux partenaires, hotspots…) pour accèder à leur messagerie (IMAP).

Exercice

Pour chacun des actifs suivants, décider s'il faut le retenir ou l'exclure et justifier votre réponse

Schémas de nouveaux produits

Documentation commerciales

Messages electroniques

Système d'exploitation

Application de calcul et modélisation 3D

Navigateur

Disque dur de l'ordinateur portable

Batterie

Fichier client

Ordinateur portable

Serveur

Application de base de données

Exercice

- Déterminer le propriétaire pour chaque actif retenu

Concepts

- Valoriser un actif
  - Actif = élément qui a de la valeur pour l'organisme
    - Essentiel donc de le valoriser
  - Comment?
    - Définir des critères de valorisation de l'actif
      - Et une échelle de de valorisation
  - Puis identifier la valeur par:
    - Entretien avec le propriétaire
    - Entretien avec les personnes qui interagissent avec l'actif

Concepts

- Valoriser un actif (suite)
  - Méthodes
    - Qualitatives – exemples: critique, importante, moyenne, faible
    - Quantitives -exemples: valeurs numériques basées sur des données
  - $Valeur_{actif} = f(\text{différentes valeurs}_{actif}\ \text{obtenues})$

Concepts

- Valeur de l'actif
  - Estimation de la valeur monétaire
    - Achat
    - Remplacement
    - Ré-élaboration
    - Perte de DIC
  - Valeur $_{actif}$ = ⅄ (différentes valeurs $_{actif}$ obtenues)
    - Ou
  - Valeur $_{actif}$ = MAX(différentes valeurs $_{actifs}$ obtenues)

Exercice

Pour les actifs retenus à l'exercice 1, identifier leur valeur selon les 3 critères de sécurité.

Valeur	Disponibilité	Intégrité	Confidentialité
1 Négligeable	Indisponibilité >1 semaine	Pas de besoin	Public
2 Faible	Indisponibilité d'une semaine	Intégrité conseillé	Accessible à un concurrent
3 Moyenne	Indisponibilité de 3 jours	Intégrité nécessaire	Accessible à toute l'entreprise
4 Elevée	Indisponibilité d'1 jour	Intégrité importante	Confidentiel
5 Critique	Indisponibilité intolérable	Intégrité parfaite	Secret

Concepts

- Menace:
  - Cause potentielle d'un incident qui peut engendrer des dommages à un système ou une organisation
  - Caractérisé par
    - Origine: délibérérée, accidentelle et/ou environnementale
    - Type: Dommage physique, événement naturel, compromission d'information...
    - Source: Pirate, terroriste, espion, personne interne...
    - Motivation de la source: curiosité, égo, gain financier

Concepts

- Vulnérabilité:
  - Faiblesse d'un actif (ou d'une mesure de sécurité) qui peut être exploitée par une menace
  - Caractéristique intrinséque d'un actif
    - Un actif possède une vulnérabilité
    - Une menace exploite une vulnérabilité
  - Attention:
    - Vulnérabilité sans menace n'implique pas d'impact sur l'actif
    - Impact si exploitation de la vulnérabilité par une menace

Exercice: menace ou vulnérabilité?

- Lignes de communication non protégées
- Erreur de l'équipe opérationnelle
- Défaut de maintenance
- Erreur d'utilisation
- Politique de mot de passe faible
- Transfert du mot de passe en clair
- Absences de mises à jour de sécurité
- Infection virale
- Jeu de règles de filtrage IP laxiste
- Corruption de données
- Présence en zone inondable
- Crue
- Abus de droit
- Absence de procédure de gestion du changement
- Portabilité
- Incendie

Exercice: menace ou vulnérabilité?

- Lignes de communication non protégées: V
- Erreur de l'équipe opérationnelle: M
- Défaut de maintenance: V
- Erreur d'utilisation: M
- Politique de mot de passe faible: V
- Transfert du mot de passe en clair: V
- Absences de mises à jour de sécurité: V
- Infection virale: M
- Jeu de règles de filtrage IP laxiste: V
- Corruption de données: M
- Présence en zone inondable: V
- Crue: M
- Espionnage: M
- Abus de droit: M
- Absence de procédure de gestion du changement: V
- Portabilité: V
- Incendie: M

Concepts

- Pour chacun des actifs retenus:
  - Identifier une ou plusieurs menaces
  - Identifier ou une plusieurs vulnérabilités

Concepts

- Mesures de sécurité
  - Moyen de gestion du risque comme des
    - Politiques
    - Procédures
    - Guides
    - Pratiques
  - de nature
    - Administrative ou réglementaire
    - Technique
    - organisationnelle

Concepts

- Exemples:
  - Coordination de la sécurité de l'information
  - Inclure la sécurité dans les accords avec les tiers
  - Sensibilisation et formation en SSI
  - Maintenance du matériel
  - Mesures contre les codes malveillants
  - Réexamen des droits d'accès utilisateur
  - Séparation des réseaux
  - Validation des données d'entrée d'une application

Concepts

- Identification des mesures existantes
  - Eviter du travail ou des coûts non nécessaires
  - Identifier des vulnérabilités
    - Intrinséques aux mesures
    - Ou liés à un mauvais fonctionnement des mesures
  - Estimer les effets des mesures de sécurité
    - Pour supprimer, éventuellement, les mesures inefficaces

Concepts

- Incident de sécurité
  - Evénement de sécurité de l'information
    - Occurrence identifiée de l'état d'un système, service ou réseau indiquant
      - Infraction à la politique de sécurité de l'information
      - Dysfonctionnement d'une mesure de sécurité
      - Situation inconnue relative à la sécurité de l'information
  - Incident de sécurité de l'information
    - Un ou une série d'événements de sécurité de l'information ayant une forte probabilité d'affecter le métier et de menacer la sécurité de l'information.

Question

- Comment réunir tous ces concepts dans un même schéma mental?

Réponse

- Réalisation du risque formulée sous forme de **scénarios d'incident**
- Relie au sein d'un événement
  - Actif(s) concerné(s)
  - Menace
  - Une ou plusieurs vulnérabilités
  -
  - Impacts en CID
  - Conséquences sur le processus métier, le projet, l'organisme...

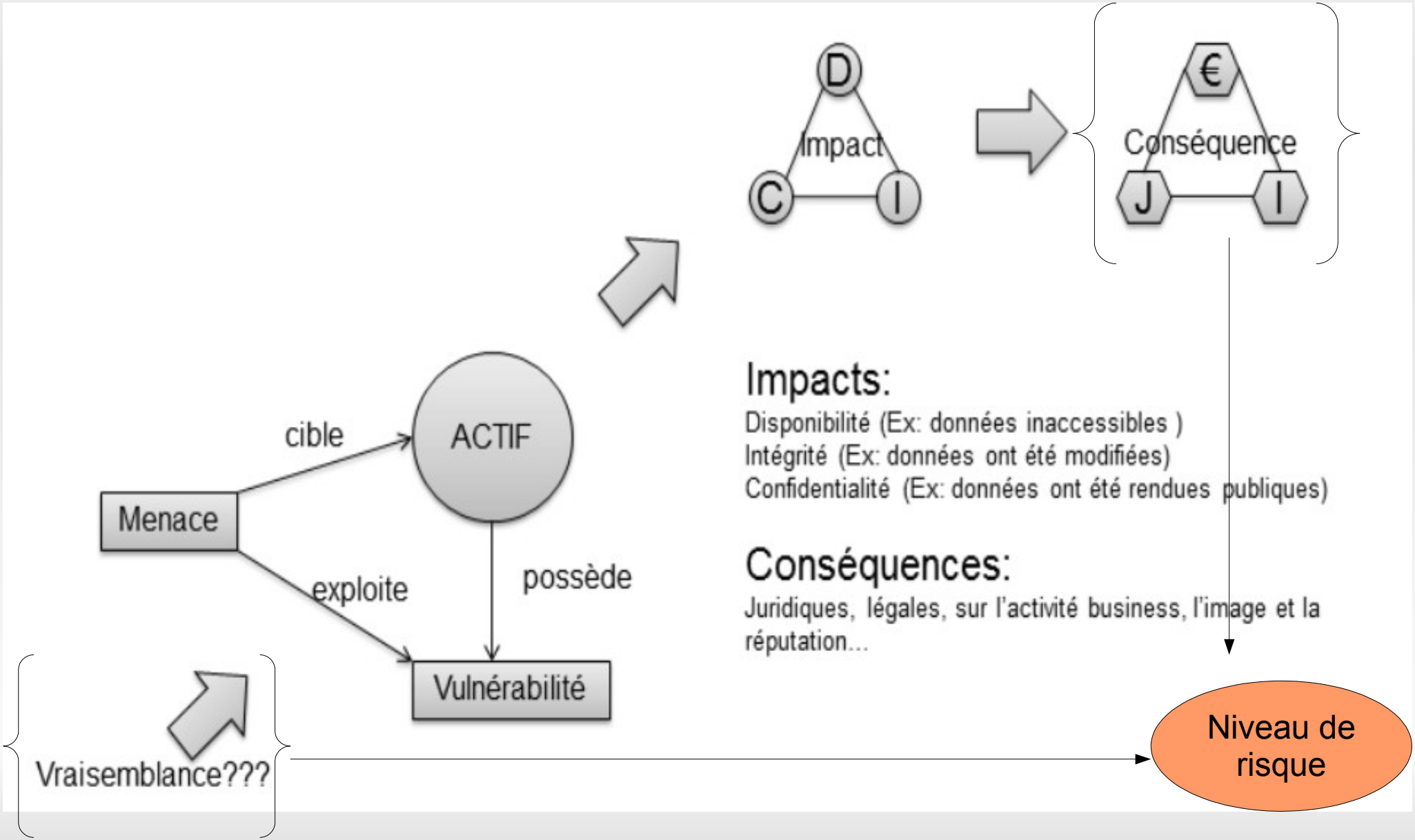
Exemple de scénario

- La salle machine principale, présente en zone inondable, est remplie d'eau suite à une crue. L'ensemble des serveurs et équipements réseau présents dans la salle sont rendus inutilisables et donc indisponibles. Les équipes métier ne sont plus en mesure de travailler. Les conséquences sont une perte financière et d'activité.

Exercice

- Pour les trois trios ”actifs, menaces, vulnérabilités” suivants
  - OS/Usurpation de droits/Vulnérabilités logicielle connues
  - Message électronique/Espionnage/Communication en clair
  - Base de données R&D/Corruption de données/Erreur de programmation
- Rédiger les scénarios d'incident

Estimation du niveau de risque



Niveau de risque

- Estimé à partir de
  - Estimation des conséquences
  - Vraisemblance des scénarios d'incident
  -
- S'appuie sur des approches
  - Qualititatives et/ou Quantitatives
  -
- Risque= f(conséquence, vraisemblance)

Apréciation des conséquences

- Peut prendre en compte
  - Valeur de l'actif
  - Impact d'une perte de DIC
  - Etudes et données statistiques
- Peut prendre la forme
  - Valeur monétaire
  - Qualification: faible, forte, importante...

Appréciation de la vraisemblance d'un scénario d'incident

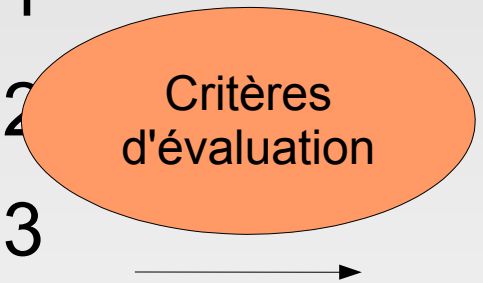
- Se base sur
  - Probabilité d'occurence des menaces
  - Difficulté d'exploitation des vulnérabilités
- Peut prendre en compte
  - Expérience
  - Données statistiques
  - Motivation et ressources des sources de menaces
  - Facteurs géographiques
  - Mesures de sécurité déjà mises en place

Exercice

- Proposer les échelles d'estimation
  - **Vraisemblance** des scénarios d'incident
  - **Conséquence** des scénarios d'incident
- Estimer, pour chaque scénario d'incident de la question précédente
  - Vraisemblance
  - Conséquence
- Proposer une méthode d'estimation du **niveau de risque**
- Estimer, pour chaque scénario d'incident de la question précédente

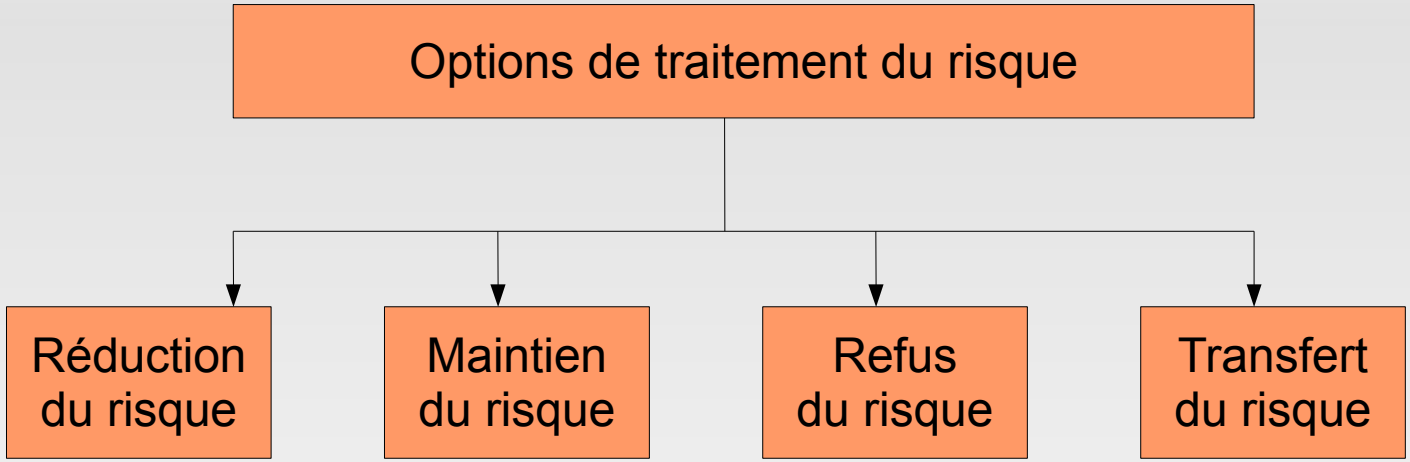
Evaluation du risque

- Liste des risques estimés
  - Risque 1
  - Risque 2
  - Risque 3
  - …
  - Risque N



- Liste des risques évalués
  - Risque 2
  - Risque 1
  - ...
- NON RETENUS
  - Risque3
  - ...

Traitement du risque



Traitement du risque

- Réduction du risque
  - Appliquer des mesures de sécurité
- Maintien du risque
  - Ne rien faire vis à vis du risque
- Refus du risque
  - Eliminer l'activité ou la situation qui engendre des risques
- Transfert du risque
  - Transférer le risque à un tiers pouvant gérer de manière plus efficace l'activité ou la situation

Risque résiduel

- Risque résiduel = risque qui perdure après traitement
- Réduction de risque
  - Risque résiduel < risque initial
- Maintien du risque
  - Risque résiduel = risque initial
- Refus du risque
  - Risque résiduel = 0
- Transfert du risque
  - Dépend du transfert

Traitement et risque induit

- Mettre en place une mesure de sécurité
- Transférer un risque à un tiers
- Peut créer de nouveaux risques
  - ➔ **Le risque induit**
- Exemple:
  - Espionnage d'information confidentielles circulant sur le réseau
  - Mise en place du chiffrement de données
  - Risque induit: Perte de la clé permettant le déchiffrement

Acceptation du risque

- Prendre une décision pour tous les risques résiduels
- Accepté
- Non accepté
  - Retour vers une étape précédente