POLYTECHNIQUE
MONTRÉAL

UNIVERSITÉ
D'INGÉNIERIE

INF8085 : Cybersécurité
Séance 2 : Analyse et gestion des risques

Frédéric Cuppens

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Contenu du cours

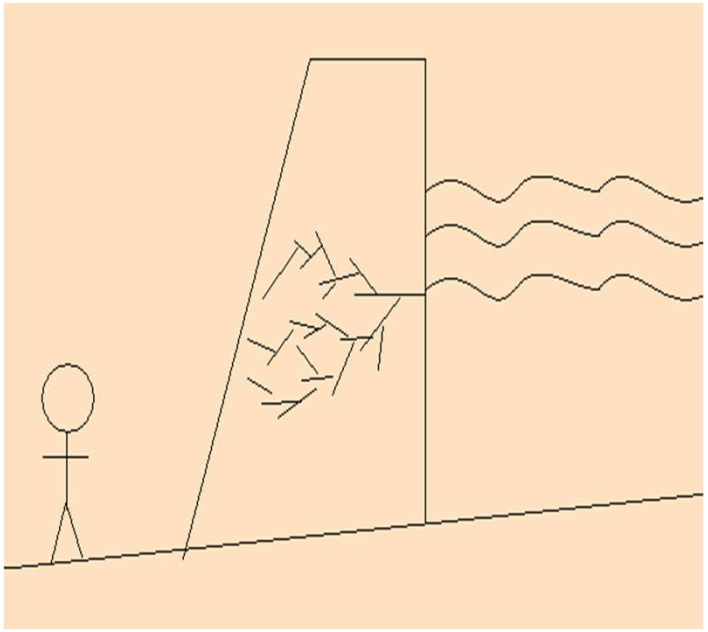
- Concept de menace
- Concept de vulnérabilité
- Concept de risque
- Evaluation des risques
- Réduction des risques
- Analyse de risques
- Méthodes d'analyse des risques

Objectifs de la SSI

- Empêcher l'exploitation de failles (vulnérabilités) contre le système d'information par des acteurs malveillants (menace)

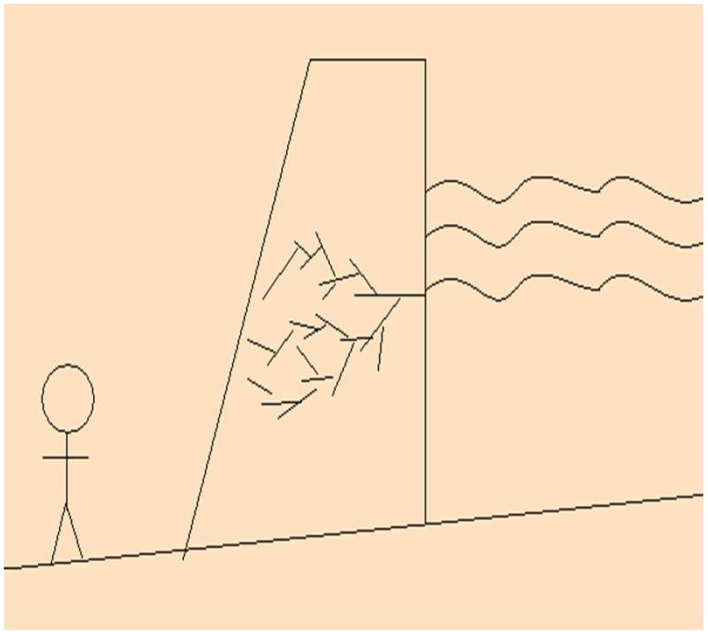
Menace

- Bien
  - Objet/personne ayant de la valeur
- Acteur/agent de menace
  - Objet/personne/entité qui met un bien à risque
- Scenario
  - Séquence d'évènement menant à la perte partielle ou totale de la valeur d'un bien



Attaque

- Concrétisation de la menace
  - Acteur + Scenario
  - « Une méthode (COMMENT)
    par laquelle un acteur particulier (QUI)
    entreprend une action (QUOI)
    pour faire subir un dommage à un bien
    (POURQUOI) »



La menace en sécurité informatique

- Quel type de menaces ?
  - Accidentelles (acteur inconscient ou absence d'acteur)
    - Catastrophes naturelles (« acts of God »)
      - feu, inondation, …
    - Actes humains involontaires
      - mauvaise entrée de données, erreur de frappe, de configuration, …
    - Performance imprévue des systèmes
      - Erreur de conception dans le logiciel ou le matériel
      - Erreur de fonctionnement dans le matériel

☚ Sûreté

  - Malveillantes ou Délibérées (acteur conscient)
    - Attaque de déni de service (atteinte à la disponibilité)
    - Vol d'informations (atteinte à la confidentialité)
    - Modification non-autorisée des systèmes (atteinte à l'intégrité)
    - …

☚ Sécurité

La menace en sécurité informatique

- Qui sont les « acteurs » ?
  - Catastrophes naturelles
  - Pirate/Hackers
    - "Script kiddies"
    - « Black hat » (et White Hat)
    - Professionnels
  - Concurrents
  - États étrangers
  - Crime organisé
  - Groupe terroriste
  - Compagnie de marketing

☚ Externe

  - Ceux à qui vous faites confiance…

☚ Interne

Vulnérabilité

- Vulnérabilité
  - Faille qui offre l'opportunité de porter un dommage à un bien
- Scénario
  - Exploitation d'une vulnérabilité par un acteur pour causer un impact
- Probabilité
  - Que la menace soit réalisée (dans une période de temps donné)
- Impact
  - Perte ou dommage à un bien

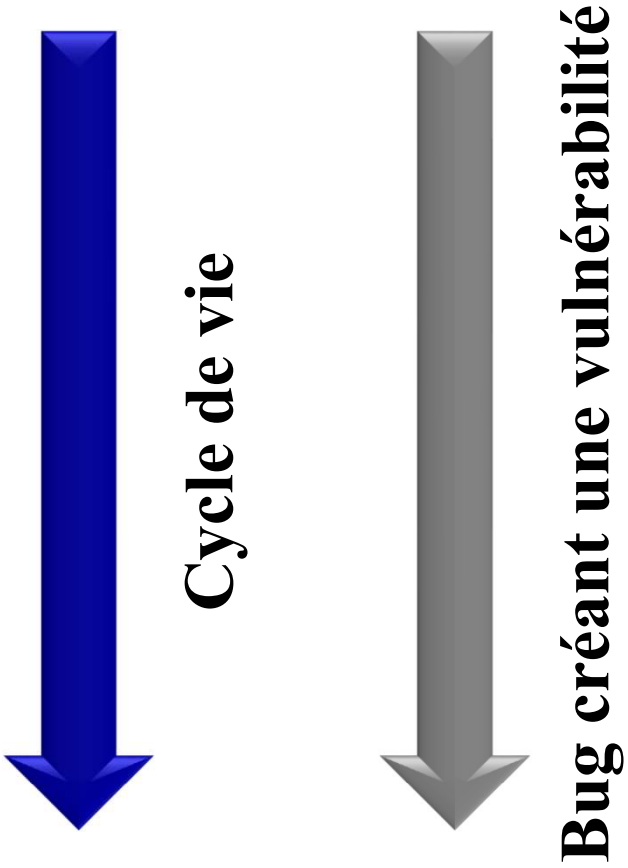
Vulnérabilité - exemple

- Biens
  - Barrage et Vies humaines
- Vulnérabilités
  - Faiblesse du barrage et
  - Usure de la vanne ou
  - Vulnérabilité logicielle de la vanne
- Menace
  - Panne accidentelle de la vanne ou
  - Attaque terroriste
- Risque
  - Rupture du barrage et
  - Perte de vies humaines

Vulnérabilité informatique

- Vulnérabilité = Faille
  - Causée par une erreur = bug

- Conception
- Implémentation
- Installation / Configuration
- Exploitation
- Mise à jour / Maintenance
- Suppression / Destruction



Vulnérabilité informatique Security vs. Safety

- Partie vulnérabilité
  - Pas de différence significative entre sécurité informatique et sureté de fonctionnement
- C'est la partie menace qui diffère
  - Menace accidentelle pour la sureté de fonctionnement
  - Menace délibérée pour la sécurité informatique
- Conséquence très importante pour évaluer les risques

Risque

- Définition qualitative
  - La prise en compte d'une exposition à un danger, un préjudice ou autre événement dommageable, inhérent à une situation ou une activité
  - Un risque correspond à la combinaison d'une vulnérabilité et d'une menace

Risque

- Définition quantitative

Risque = probabilité * impact
= espérance de perte

Il faut être conscient du niveau de risque avant de prendre une décision

- Le risque est inhérent à l'activité
  - Il est impossible de l'éliminer
  - On peut le « gérer » par
    - Réduction
    - Transfert
    - Acceptation
    - Arrêt de l'activité

Risque – « Reality Check »

- Il y a un risque s'il y a un enjeu réel relié au bien
  - Même si une vulnérabilité (scénario) et un acteur existent
    - Pas d'impact ➔ pas de risque
- Il y a un risque si un scénario a une chance de se réaliser
  - Même si une vulnérabilité existe
    - Pas d'acteur ➔ Pas de risque
  - Même s'il y a un acteur,
    - Pas de vulnérabilité ➔ pas de scénario ➔ pas de risque
- Mais comment gérer/estimer les risques potentiels ?
  - Vulnérabilité non encore identifiée
  - Menace non encore identifiée

Risque

- Le risque informatique s'apparente à
  - une loterie où on ne peut pas ~~perdre~~ gagner !

$$E = P \times I$$

Espérance de perte

Probabilité d'incident

Impact d'un incident

Risque

- Comment évaluer le risque
  - Impact
    - sous le contrôle du propriétaire du système à protéger
    - « facile » à évaluer
  - Probabilité
    - Risques naturels
      - Valeurs connues (statistiques, actuariat, historique de catastrophes, etc.)
      - Probabilité expérimentale ou fréquentielle
    - Risques délibérés
      - Acteur conscient et intelligent
      - Pas événement aléatoire

☛ Comment évaluer le risque délibéré ?

Probabilité des risques délibérés

- Capacité
  - Savoir/connaissances ou accès au savoir
  - Outils
  - Ressources humaines
  - Argent
- Opportunité
  - Espace : avoir accès physique
  - Connectivité : existence d'un lien physique et logique
  - Temps : être « là » au bon moment
- Motivation
  - « À qui profite le crime ? » (Qui)
  - Que gagne l'attaquant ? (Quoi)
  - Combien gagne t-il ? (Combien)

*probabilité = capacité * opportunité * motivation*

Probabilité des risques délibérés

*probabilité = capacité * opportunité * motivation*

- On obtient une mesure subjective
  - Repose sur l'expertise
  - Deux experts différents peuvent donner une évaluation différente
  - Contrairement à une probabilité fréquentielle qui peut être mesurée expérimentalement
- Il ne s'agit donc pas d'une valeur « absolue »
  - Une valeur de 0,5 de la probabilité ne veut rien dire
  - Mais cette valeur peut être utilisée pour faire des comparaisons
    - Une valeur de 0,6 représente une « probabilité » plus grande qu'une valeur de 0,4

Évaluation et choix de contremesures

- Contremesure : Définition
  - Objet (ou processus) qui réduit le risque associé à une menace sur un bien

Évaluation et choix de contremesures

- Réduction du risque
  - Motivation et impact ne changent pas
  - Réévaluation de capacité et opportunité => risque résiduel
  - réduction = risque initial (sans contremesures) – risque résiduel (après application efficace)
- Coût total
  - Coût d'installation (achat, installation, configuration)
  - Coût d'opération (licences, personnel supplémentaire)
  - Impact sur la performance des systèmes
  - Convivialité du système
  - Impact sur le processus d'affaires
  - Introduction de nouveaux risques …

Concepts et principes d'opération

- Efficacité des contremesures
  - Sensibilisation du personnel
  - Utilisation réelle des contrôles disponibles
  - Recouvrement des contrôles
  - Vérification administrative

- Principe de l'efficacité
  - Pour que les contremesures soient effectives, elles doivent être utilisés
  - Pour qu'elles soient utilisées, elles doivent être perçues comme étant faciles d'usage, et appropriées aux situations particulières

Évaluation et choix – Principes fondamentaux

- Principe du point le plus faible
  - Une personne cherchant à pénétrer un système utilisera tous les moyens possibles de pénétration, mais pas nécessairement le plus évident ou celui bénéficiant de la défense la plus solide

- Principe de la protection adéquate (Gestion du risque)
  - La durée de la protection doit correspondre à la période pendant laquelle l'importance et la valeur sont présentes, et pas plus
  - Le niveau et le coût de la protection doivent correspondre à l'importance et à la valeur de ce qu'on veut protéger

☛ Choisir la contremesure avec le meilleur rapport « qualité » (réduction de risque) vs. « prix » (coût total)

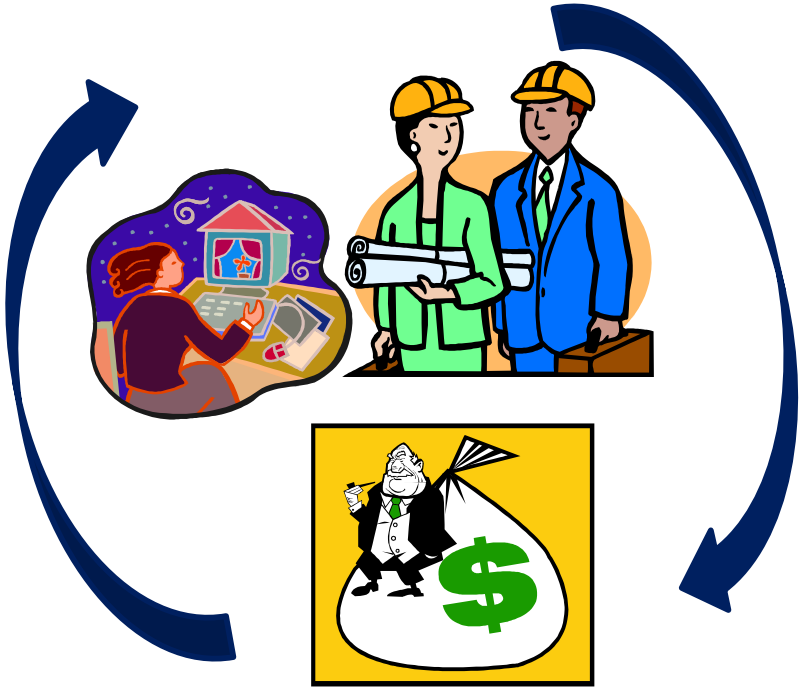
Moyens de protection - Types

- Exemples de contre-mesures
  - Chiffrement des données
  - Contrôles au niveau des logiciels
    - Programmés
    - Partie du système d'exploitation
    - Contrôle du développement des logiciels
  - Contrôles du matériel
    - Contrôle de l'accès au matériel: identification et authentification
    - Contrôles physiques: serrures, caméras de sécurité, gardiens, etc…
  - Procédures
    - Qui est autorisé à faire quoi?
    - Changements périodiques des mots de passe
    - Prise de copies de sécurité
    - Formation et administration

Politique de sécurité

Méthodologie d'analyse de risque

1. Identifier la menace
   - Qui ou quoi ?
   - Comment (vulnérabilités) ?
2. Évaluer les risques
   - Probabilité
   - Impact
3. Considérer les mesures de protection par rapport au risque
   - Efficacité (risque résiduel)
   - Coût
   - Difficulté d'utilisation
4. Mettre en place et opérer les mesures protections
   - Modification et/ou installation
   - Changer les politiques
   - Éduquer les utilisateurs
5. Retourner à 1…



Analyse de risque - Acteurs et responsabilités

- Responsable de sécurité informatique
  - Capacité et Opportunité
    - En analysant
      - Architecture des systèmes existants
      - Vulnérabilités connues et possible des systèmes
      - La nature technique de la menace

        Outils existants

        Techniques et méthode d'attaques (Scénario=comment)
  - Probabilité des risques accidentels humains

Analyse de risque - Acteurs et responsabilités

- « Stakeholders »
  - Description de la menace (quoi)
  - Motivation (qui)
    - Identification des acteurs : compétiteurs, opposants, etc.
    - Analyse d'objectifs et intentions des acteurs : « qu'est-ce qu'ils ont à gagner ? »
  - Impact (et alors)
    - « Combien ça coûterait si… »
    - Relié à la "valeur du remboursement" en assurances
    - Relié au concept d'exposition au risque en comptabilité

Analyse de risque - Acteurs et responsabilités

- Spécialiste en risque ou en sécurité générale
  - Probabilité de risque accidentel naturel

Analyse de risque

- Évaluer l'impact
  - Classification des actifs (les biens à protéger)
  - Échelle semi-objective
  - Chiffrage des impacts sur les « objectifs d'affaires »

- Le gestionnaire responsable du processus (propriétaire du système ou « stakeholder » en anglais) est la source de la classification puisqu'il est l'utilisateur du système
  - Ex. : le directeur de la paie est le propriétaire du système informatique qui génère la paie
  - Ex. : le directeur TI est le propriétaire du système informatique qui gère le VPN

Analyse de risque

- Exemple d'échelle de cotation d'impact
- Échelle arbitraire (aurait pu être différente)
- Toujours conserver la même échelle pour comparer

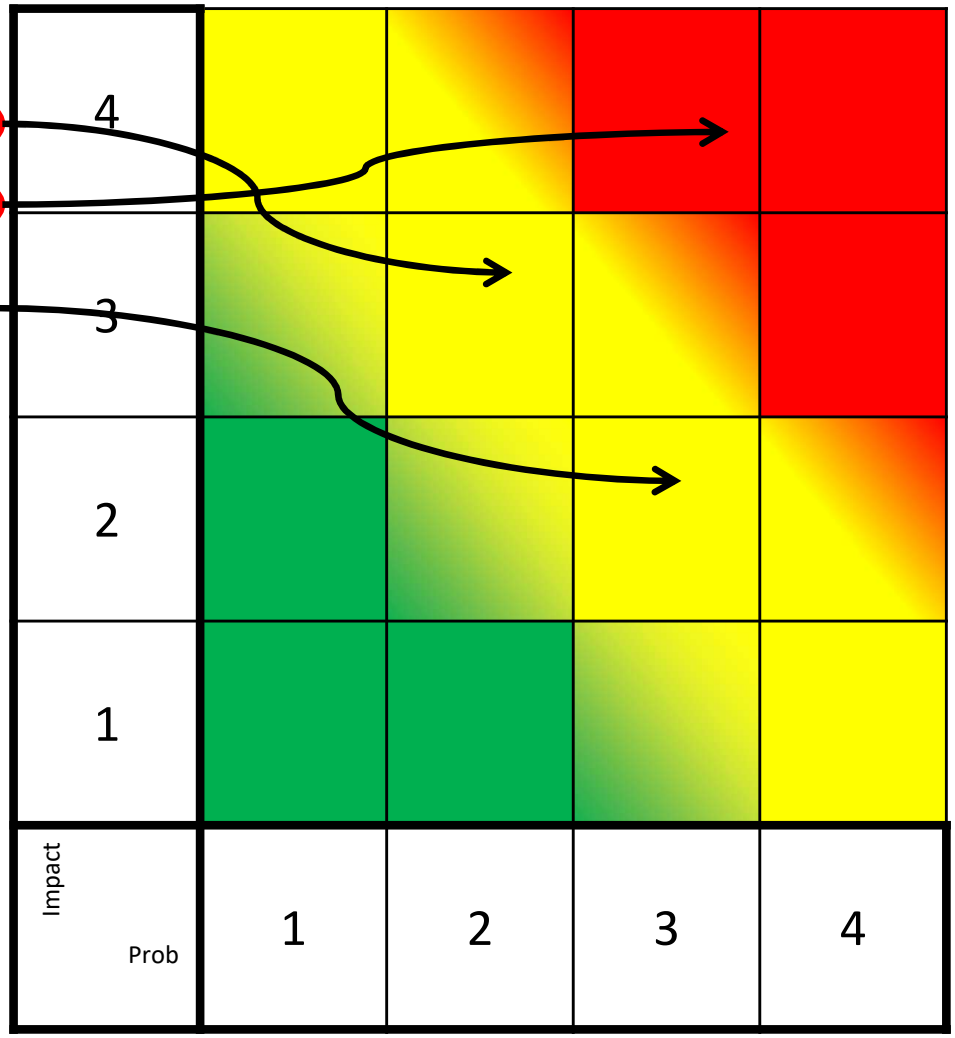
Cote	Disponibilité/Intégrité	Confidentialité
1	Mineur : courte perte de disponibilité, petite perte monétaire, pertes de peu de données, etc. (NON CRITIQUE)	Mineur : aucun impact relié si dévoilée à une tierce partie non autorisée (SANS CLASSIFICATION)
2	Moyen: perte de disponibilité de quelques heures, perte monétaire moyenne, pertes de données peu dommageables etc. (CRITIQUE)	Moyen: impact grave si dévoilée à un tierce partie non autorisée (CONFIDENTIEL)
3	Majeur : arrêts de plusieurs jours, pertes monétaires de plusieurs mois, pertes d'un large volume de données, etc. (TRÈS CRITIQUE)	Majeur: impact très grave si dévoilée à une tierce partie non autorisée (SECRET)
4	Catastrophique: arrêt indéfini, perte de millions de dollars, etc. (VITAL; « MISSION CRITICAL »)	Catastrophique: impact extrêmement grave si dévoilée a une tierce partie non autorisée (TRÈS SECRET)

Analyse de risque

- Évaluer la probabilité
  - Échelle objective pour les aléas (ex. : tables actuarielles)
  - Échelle subjective pour les risques délibérés
  - Chiffre les probabilités d'observer un impact dans un scénario précis

Analyse de risque

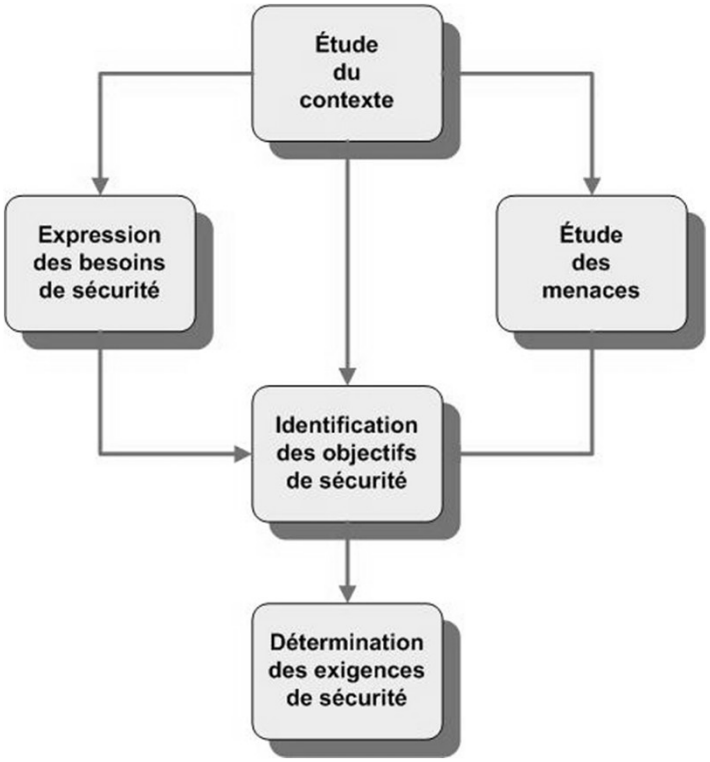
Scénario	C	M	O	P	I
Scénario 1	1	3	2	2	3
Scénario 2	4	3	3	3.3	4
Scénario 3	3	2	4	3	2
…					



- Ici, on a utilisé la moyenne pour calculer P
- On aurait pu prendre autre chose (médiane, moyenne pondérée, maximum, etc.)
- L'important c'est d'être consistent pour pouvoir comparer !

Méthodes d'analyse de risque

- Exemples de méthodes d'analyse de risques
  - Méhari Méthode harmonisée d'analyse des risques (MEHARI)
    - CLUSIF (Club de la sécurité de l'information français)
    - CLUSIQ (Québec)
- EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) (France)
  - Supportée par l'ANSSI
    - (Agence Nationale de la Sécurité des Systèmes d'Information)
    - Evolution EBIOS RM (Risk Manager)



Méthodes d'analyse de risque

- Autres méthodes d'analyse de risques
  - CRAMM (Royaume-Uni)
    - Établir les objectifs de sécurité
    - Analyser les risques
    - Identification et sélection de contrôles
  - Octave (Etats-Unis)
    - Operationally critical threat, asset, and vulnerability evaluation
  - FAIR
    - Factor Analysis of Information Risk
    - Méthode reposant sur un taxonomie des facteurs de risques
  - RiskIT/COBIT
  - …

Normes ISO 27000

- Panorama des normes ISO 27000
- Famille de normes internationales de sécurité de l'information
- Principales normes

27001	• Systèmes de gestion de la sécurité de l'information
27002	• Code de bonnes pratiques
27004	• Mesures de gestion de la sécurité
27005	• Gestion des risques
27035	• Gestion des incidents de sécurité
27037	• Traitement des preuves numériques *(forensics)*
…	• …

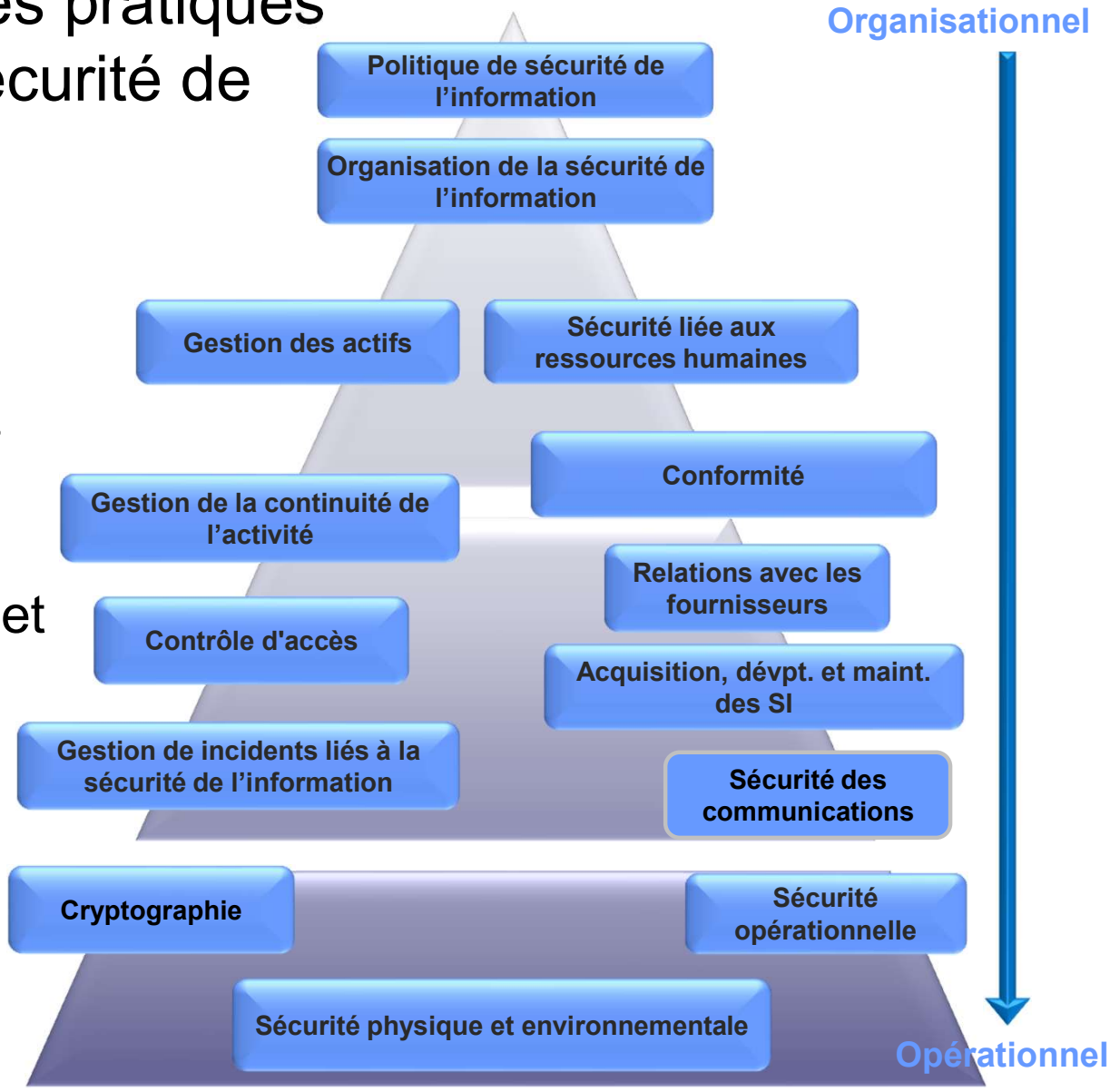
Normes ISO 27000

- ISO 27001 : Système de Management de la Sécurité de l'Information
  - Certification ISO 27001 délivrée par un organisme certificateur accrédité
    - Démarche calquée sur ISO 9000 (Plan / Do / Check / Act)
    - Audit qui garantit que l'organisation a appliqué les exigences de la norme
    - Certification valable 3 ans, chaque année un audit de contrôle est effectué
    - Certification exigée pour accéder à certains contrats
      - Exemple : organisme payeur d'aides agricoles européennes
    - Pas de niveau minimum de sécurité à atteindre
      - Une entreprise peut donc être certifiée ISO 27001 tout en ayant défini un périmètre réduit et une politique de sécurité peu stricte

Normes ISO 27000

- 27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information

- Approche globale de la sécurité des S.I.
- Composée de 114 mesures de sécurité réparties en 14 chapitres couvrant les domaines organisationnels et techniques
- Référentiel de mise en œuvre
  - « Check-list » en cas d'audit



Normes ISO 27000

- 27002 : Code de bonnes pratiques pour la gestion de la sécurité de l'information
- Exemples de mesures du chapitre « Contrôle d'accès »
  - L'accès aux fichiers/répertoires doit être restreint conformément aux politiques de contrôle d'accès
    - Seuls les professeurs autorisés doivent pouvoir accéder à un répertoire contenant les épreuves des futurs examens/concours
  - Les propriétaires de l'information doivent vérifier les droits d'accès à intervalles réguliers
    - Le responsable des concours doit contrôler les droits d'accès au répertoire contenant les épreuves des futurs examens/concours pour s'assurer qu'il n'y a pas d'étudiants qui auraient été rajoutés
- Exemple de mesures du chapitre « Sécurité opérationnelle »
  - L'installation et la configuration de logiciels doivent être encadrés
    - Seuls les administrateurs doivent pouvoir installés un logiciel sur un poste
  - Des sauvegardes doivent êtres régulièrement effectuées et testées
    - Un espace de sauvegarde des données peut être mis à disposition des utilisateurs

Normes ISO 27000

- 27005 : Gestion des risques
- La norme 27005 présente une démarche
  - Donne les lignes directrices relatives à la gestion des risques de sécurité
- Avantages
  - Utilisable seule
  - Plusieurs méthodes sont compatibles IS0 27005
    - Exemple : EBIOS RM
  - Méthode générique, peut être utilisée en toutes circonstances
- Limites
  - C'est plus une démarche qu'une vraie méthode
    - L'organisation doit définir sa propre approche
  - Tendance à l'exhaustivité
  - Accumulation de mesures techniques sans cohérence d'ensemble

Questions ?

Frédéric Cuppens