1. Établissement du contexte

a. Comprendre l’organisation

- Étude de l’organisme : Identifier l’objectif, l’activité, les missions, les valeurs et les stratégies de l’organisation.
- Gouvernance : Structure, politiques, ressources, flux d’informations, relations avec les parties prenantes, culture, contrats.

b. Contexte externe

- Environnement externe (réglementations, exigences légales, attentes des parties prenantes).

c. Contexte interne

- Culture, processus, structure, stratégie, ressources internes.

d. Détermination des exigences

- Identifier les objectifs de gestion des risques (conformité, continuité, analyse de produits/services).

e. Gouvernance des risques

- Intégrer la gestion des risques dans l’organisation, attribuer les rôles et responsabilités, nommer un manager des risques, allouer les ressources nécessaires.

f. Politique de gestion des risques

- Définir les objectifs, le cadre, l’engagement de la direction, la surveillance et l’amélioration continue.

2. Identification du risque

a. Identification des actifs

- Repérer les actifs essentiels (informations, équipements, etc.) et leurs propriétaires.

b. Identification des menaces

- Recueillir les menaces potentielles auprès de différentes sources (internes/externes, experts, catalogues de menaces).

c. Identification des mesures existantes

- Lister les mesures de sécurité déjà en place et évaluer leur efficacité.

d. Identification des vulnérabilités

- Détecter les failles exploitables par les menaces (via audits, scans, questionnaires, etc.).
- Utilisation du score CVSS pour évaluer la gravité des vulnérabilités.

e. Identification des conséquences

- Évaluer les effets potentiels (positifs ou négatifs) sur les objectifs de l'organisation.

3. Analyse des risques

a. Méthodologie

- Analyse qualitative (rapide, générale) ou quantitative (précise, chiffrée), ou combinaison des deux.

b. Appréciation de la vraisemblance

- Évaluer la probabilité d'occurrence des menaces et la facilité d'exploitation des vulnérabilités.

c. Estimation du niveau de risque

- Croiser la probabilité et l'impact pour estimer le niveau de risque (matrice de risque).

4. Évaluation des risques

a. Prise de décision

- Décider des actions à entreprendre selon le niveau de risque (priorisation).

b. Critères d’évaluation

- Probabilité : Très probable à très peu probable (échelle de 1 à 5).
- Impact : Négligeable à grave (échelle de 1 à 5).

c. Matrice d’évaluation

- Utiliser une matrice pour prioriser les risques selon leur gravité.

5. Exemple de cas pratique

- Situation : Un chercheur utilise un ordinateur portable contenant des données sensibles, protégé seulement par un mot de passe simple, lors de déplacements à l’étranger.
- Analyse : Identifier les actifs, les mesures existantes, les vulnérabilités, puis évaluer et prioriser les risques.

seance5

1. Identification des actifs

Dans le contexte de la sécurité des systèmes informatiques, les actifs à protéger sont :

- Données (informations sensibles, bases de données, documents confidentiels)
- Systèmes informatiques (serveurs, postes de travail, réseaux)
- Applications (logiciels métiers, outils de communication)
- Infrastructure physique (locaux, équipements réseau, dispositifs de stockage)
- Utilisateurs (employés, partenaires, clients)
- Processus métiers (procédures critiques, flux de travail)

2. Identification des mesures existantes

Le document distingue plusieurs types de mesures de sécurité déjà en place :

a. Nature des mesures

- Dissuasives : découragent les attaques (ex : caméras, affichage de politiques)
- Préventives : empêchent les incidents (ex : pare-feu, politiques d’accès, alarmes)
- Détectives : détectent les incidents (ex : SIEM, IDS/IPS, vidéosurveillance)

- Correctives : limitent l’impact après un incident (ex : sauvegardes, plans de reprise)

b. Catégories de mesures

- Techniques : firewalls, chiffrement, antivirus, segmentation réseau, gestion des correctifs
- Administratives/Managériales : politiques de sécurité, gestion des accès, sensibilisation, audits
- Physiques/Opérationnelles : serrures, contrôle d’accès physique, vidéosurveillance, alarmes

3. Identification des vulnérabilités

Les vulnérabilités sont des faiblesses qui peuvent être exploitées par des menaces. Exemples :

- Mots de passe faibles ou mal gérés
- Absence de chiffrement des données sensibles
- Logiciels non mis à jour (failles non corrigées)
- Manque de formation des utilisateurs
- Accès physique non contrôlé
- Politiques de sécurité inadaptées ou non appliquées
- Réseaux non segmentés
- Absence de surveillance ou de détection d’intrusion

4. Évaluation et priorisation des risques

a. Méthodologie

- Analyse qualitative : évaluation subjective de la probabilité et de l’impact
- Analyse quantitative : chiffrage des pertes potentielles

b. Critères d’évaluation

- Probabilité : fréquence d’occurrence d’un incident
- Impact : gravité des conséquences (financières, réputationnelles, opérationnelles)

c. Exemples de risques et priorisation

Risque identifié	Probabilité	Impact	Niveau de risque	Priorité
Fuite de données sensibles (ex : vol de données)	Élevée	Très grave	Critique	1
Infection par malware (ex : ransomware)	Moyenne	Grave	Élevé	2
Intrusion physique (ex : vol d'équipement)	Faible	Grave	Moyen	3
Perte de données (ex : absence de sauvegarde)	Moyenne	Grave	Élevé	2
Non-conformité réglementaire	Faible	Très grave	Moyen	3

5. Traitement des risques

Quatre options principales :

- Réduction : mettre en place des mesures pour diminuer le risque (ex : renforcer les mots de passe, former les utilisateurs)
- Maintien (acceptation) : accepter le risque s'il est jugé acceptable
- Refus : éviter l'activité à risque
- Partage (transfert) : transférer le risque (ex : assurance cyber)

Le choix dépend du coût, des bénéfices attendus et des contraintes (budgétaires, humaines, techniques).

6. Surveillance et amélioration continue

- Surveillance permanente des risques, des menaces et des vulnérabilités (veille, alertes, audits)
- Révision régulière des mesures et des plans de gestion
- Communication : informer et impliquer les parties prenantes, constituer un comité de gestion des risques

7. Résumé des contrôles de sécurité

- Administratifs : politiques, sensibilisation, gestion des accès
- Techniques : pare-feu, chiffrement, antivirus, segmentation réseau
- Physiques : serrures, vidéosurveillance, contrôle d'accès

Chaque contrôle peut être :

- Préventif
- Détectif
- Correctif
- Dissuasif

1. Identification des actifs

- Information : disponibilité, intégrité, confidentialité
- Systèmes informatiques : données, applications, infrastructures
- Organisation : image de marque, opérations, employés

2. Identification des mesures existantes

- Gouvernance de la sécurité de l'information :
    - Processus décisionnels
    - Définition des rôles et responsabilités
    - Respect des lois et exigences réglementaires
    - Cadres de gouvernance (ISO 27000, NIST CSF, CIS Controls)
- Mesures techniques :
    - Outils de scan de réseau (Nmap, Zenmap, Spiceworks)
    - Chiffrement (Bitlocker, FireVault)
    - Analyse de sécurité (Qualys Browser Check, OpenVAS, Microsoft Baseline Security Analyzer)

        - Sauvegarde (Windows Backup, Apple Time Machine, Amanda Network Backup, Bacula)

3. Identification des vulnérabilités

- Techniques :
    - Logiciels non mis à jour
    - Mauvaise configuration des systèmes
    - Absence de chiffrement
- Organisationnelles :
    - Manque de sensibilisation des employés
    - Absence de politiques de sécurité claires
    - Non-conformité réglementaire (Loi 25)

4. Évaluation et priorisation des risques

- Risques :
    - Atteinte à la disponibilité, l'intégrité ou la confidentialité de l'information
    - Non-respect des exigences légales (Loi 25)
    - Cyberattaques (malware, phishing, etc.)
- Priorisation :
    - Basée sur la gestion des risques (identifier, évaluer, planifier, minimiser)
    - Utilisation des cadres de gouvernance pour améliorer la posture de sécurité

5. Cadres de gouvernance

- ISO 27000 :
    - ISO/IEC 27001 (SMSI)
    - ISO/IEC 27002 (conseils pour l'implémentation)
    - ISO 27005 (évaluation des risques)
- NIST CSF (Cybersecurity Framework) :
    - Fonctions : Govern, Identify, Protect, Detect, Respond, Recover
    - Profils organisationnels : adapter et prioriser les résultats en matière de cybersécurité
- CIS Controls :
    - Mesures de sécurité hiérarchisées
    - Phases : connaître son environnement, protéger les actifs, préparer son organisation

6. Loi 25

- Objectifs :
    - Renforcer la protection de la vie privée
    - Favoriser la transparence
    - Responsabiliser les entreprises
- Exigences :
    - Obtention du consentement
    - Droit à la portabilité des données
    - Droit à l'oubli
- Conformité :
    - Évaluation initiale
    - Mise en conformité
    - Nomination d'un responsable de la protection des renseignements personnels
    - Évaluation des Facteurs Relatifs à la Vie Privée (EFVP)