# 5.02 - Analyse de risque et bonnes pratiques en cybersécurité (CIEL)

**Durée approximative :** ***4h***

**Eléments du référentiel adressé :**

- ***U4 - Etude et conception de réseaux informatiques***
  - ***R1 : Accompagnement du client***
    - ***C04 : Analyser un système informatique***
      - ***Acteurs de l'écosystème réglementaire, normatif et de référence des bonnes pratiques***
      - ***Méthodologies d'analyse de risque***
      - ***Méthodologie de recherche et d'analyse de documentation, y compris en anglais***

- ***U6 - Valorisation de la donnée et cybersécurité***
  - ***D5 : Audit de l'installation ou du système***
    - ***C03 : Gérer un projet***
      - ***Moyens, outils et méthodes permettant d'effectuer une veille technologique***
    - ***C10 : Exploiter un réseau informatique***
      - ***Usage et documents réglementaires, normatifs adoptés au sein de l'entreprise et du secteur de la sécurité des systèmes d'information***

## I. Les recommandations et bonnes pratiques

Suite au TP de l'introduction, les étudiants doivent avoir téléchargé les guides de bonnes pratique et en avoir un résumé assez clair.

Lien de téléchargements :

- EXT - anssi : règles d'or
- EXT - anssi : bonnes pratiques

Il peut être bon d'afficher les fiches de synthèse dans la classe.

Pour chaque point suivant, expliquer avec des exemple et leur demander une analyse de risque basique :

1. Mots de passe forts uniques (brute force, attaque par dictionnaire, fuite de donnée, ...)
2. Garder les systèmes à jour (failles, zeroday, ...)
3. Effectuer des sauvegardes régulières, si possible offline et externalisées (incendie, cryptolocker, ...)
4. Réfléchir avant de cliquer (l'attaquant crée une situation d'urgence pour nous berner)

# II. Analyse de risque cybersécurité

## 2.1 La norme ISO27001

Présenter rapidement la norme ISO 27001, son historique et son but en s'appuyant sur : EXT - Wikipedia : iso 27005

## 2.2 La méthode EBIOS

Que cela soit pour un audit de sécurité ou pour une analyse interne, il est important de savoir évaluer correctement le risque sécu et qualifier le niveau de menace.

S'appuyer sur les documents de l'anssi pour organiser les ateliers : EXT - anssi : Methode ebios

> **TP** : dérouler les ateliers présentés dans le document de l'anssi et le mettre en parallèle avec le projet à venir.

# III. Les outils de veille

Présentation des outils de veille et des bulletins CERT-FR. Lecture d'un ou deux exemple.

Explication de la nécessité de disposer d'outils de veille technologique, notamment les flux RSS de l'anssi et de la cnil.

Etendre cette veille aux aspect technologiques, ne pas négliger les réseaux style LinkedIn ou des agrégateurs d'actualité.

- Flux RSS anssi : https://www.cert.ssi.gouv.fr/feed/
- Flux RSS CNIL : https://www.cnil.fr/fr/rss.xml

> **Conseil** : il sera utile plus tard de mettre en place ces flux dans GLPI par exemple.

> **TP** : mise en place de flux RSS sur teams ou discord.

---

*Supports de cours associés :*

- Sécurité - Analyse de risque (méthode Ebios)

*Ressources associées :*

- *Solidité mots de passe (2025)*
- *Evaluation des risques cybersécurité*
- *Méthodologie - Méthode PDCA*

---

Revision #1
Created 2026-07-17 13:12:02 UTC by Olivier
Updated 2026-07-17 13:12:04 UTC by Olivier