Fiche de Révision - Chapitre 1 : Normes et Bonnes Pratiques (Concepts de Base)

Ce chapitre introduit les concepts fondamentaux liés aux normes et bonnes pratiques informatiques.

- **Définitions Clés :**

1. **Service IT** : Ensemble organisé de ressources (humaines, technologiques, financières) qui fournissent de la valeur à un client (interne ou externe), souvent sous forme de résultat ou de capacité.

   Exemple : Service de messagerie électronique, de sauvegarde des données.

2. **Processus** : Suite d'activités corrélées ou interactives qui transforment des entrées en sorties dans un but précis.

   Exemple : Processus de gestion des incidents, processus de changement.

3. **Politique IT** : Document de haut niveau définissant les intentions et orientations formelles de la direction en matière de sécurité, qualité ou gestion des services.

4. **Risque** : Événement potentiel qui pourrait impacter la confidentialité, l'intégrité ou la disponibilité des services et informations de l'organisation.

   Géré par le SMSI (ISO 27001) et un pilier de la gouvernance I&T selon COBIT (objectif EDM03). Le niveau de risque acceptable est déterminé par la direction.

5. **Norme** : Document officiel, élaboré par un organisme reconnu (ISO, AFNOR), qui définit des exigences claires, mesurables et certifiables.

- Objectif : Assurer la conformité, l'harmonisation et la confiance.
- Exemple : ISO/CEI 27001 (exigences pour un SMSI). Les normes ne sont pas des lois, mais peuvent être obligatoires par contrat ou recommandées par la réglementation.
- Fondements : Consensus, bonne pratique éprouvée, amélioration continue, réduction du risque, interopérabilité et cohérence, transparence et traçabilité.

6. **Bonne Pratique** : Ensemble structuré d'activités ou de méthodes utilisées de manière répétée pour atteindre un objectif.

- Objectif : Appliquer des méthodes éprouvées pour améliorer la performance et la cohérence.
- Exemple : ITIL (gestion des services IT), COBIT (gouvernance IT).

- **Distinction entre Norme et Bonne Pratique:**

1 - Normes (ex: ISO 27001, 20000) :

Nature : Contraignante, certifiable.

Objectif : Conformité, audit.

Portée : Générale, applicable à toute organisation.

Origine : Organismes de normalisation.

2 - Bonnes Pratiques (ex: ITIL, COBIT, SCRUM) :

Nature : Recommandée, adaptable.

Objectif : Efficience, amélioration continue.

Portée : Spécifique, flexible.

Origine : Expériences et expertises.

Fiche de Révision - Chapitre 2 : ISO 27001

Ce chapitre se concentre sur la norme ISO 27001 relative au Système de Management de la Sécurité de l'Information (SMSI).

- **Fondamentaux de la norme ISO 27001:**

  - Familles de normes ISO 27001:

    - ISO/IEC 27000: Vue d'ensemble et vocabulaire.

    - ISO/IEC 27001: Norme principale, spécifie quoi faire pour sécuriser les informations (exigences pour un SMSI).

    - ISO/IEC 27002: Détaille comment appliquer les mesures listées dans l'ISO 27001 (code de bonnes pratiques).

    - ISO/IEC 27003: Lignes directrices pour la mise en œuvre du SMSI.

    - ISO/IEC 27004: Aide à mesurer la performance de la sécurité (indicateurs, métriques).

    - ISO/IEC 27005: Explique comment identifier et gérer les risques informatiques.

    - Autres normes spécifiques (27006, 27007, 27017, 27018, 27019, 27701).

  - Qu'est-ce qu'un système de management ?

    Ensemble d'éléments corrélés ou interactifs d'un organisme visant à établir des politiques, des objectifs et des processus permettant d'atteindre ces objectifs. Il combine processus, ressources, outils et main-d'œuvre.

  - Avantages d'un SMSI conforme à ISO/IEC 27001:

    - Sécurité de l'information.

    - Réponse efficace aux menaces.

    - Bonne gouvernance et culture.

    - Réduction des coûts liés à la sécurité.

    - Conformité avec d'autres lois et réglementations.

  - Structure de la norme ISO/IEC 27001:2022 (Cycle d'amélioration continue):

    - Article 4: Contexte de l'organisation.

    - Article 5: Leadership.

    - Article 6: Planification.

    - Article 7: Supports.

    - Article 8: Fonctionnement.

    - Article 9: Évaluation de la performance.

    - Article 10: Amélioration.

- Annexe A: Référencement des mesures de sécurité de l'information (93 mesures dans la version 2022, non exhaustives).

- **Concepts Clés de la Sécurité de l'Information** :
  - Information : Données porteuses de sens.
  - Actif : Élément ou entité ayant une valeur potentielle ou réelle pour une organisation (actifs virtuels, physiques, personnels, organisationnels).
  - Sécurité de l'Information : Protection de la vie privée, de l'intégrité et de la disponibilité de l'information. Elle couvre toutes les formes d'informations (imprimées, transmises, conversées).
  - Confidentialité : Propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés.

    Assurer la confidentialité : Authentification multifactorielle, politique d'accès aux données, contrôles d'accès, chiffrement.
  - Intégrité : Propriété d'exactitude et de complétude.

    Assurer l'intégrité : Informations non modifiées/corrompues, modifications autorisées seulement, données précises/cohérentes/fiables/protégées.
  - Disponibilité : Propriété d'être accessible et utilisable à la demande par une entité autorisée (à la demande, au moment voulu, à l'endroit voulu, à la personne qui en fait la demande).

    Garantir la disponibilité : Maintenir et améliorer les infrastructures physiques, sauvegardes, gestion des incidents, procédures de contrôle d'utilisation des systèmes.
  - Vulnérabilité : Faille dans un actif ou une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.
  - Menace : Cause potentielle d'un incident lié à la sécurité de l'information qui peut entraîner des dommages ou porter préjudice à un organisme. Une menace exploite une vulnérabilité.

    Exemples : Feux, eau, coupures d'alimentation, défaillances techniques, terrorisme, erreur d'utilisation, piratage, virus, vol, etc.
  - Risque lié à la sécurité de l'information : Possibilité qu'un événement impacte les opérations, les actifs, les personnes, entraînant une perte d'accès, d'utilisation, de divulgation, de perturbation, de modification ou de destruction non autorisée.

- **Classification des mesures de sécurité:**
  - Par Type:
    - **Mesures Techniques** : Liées à l'utilisation de mesures techniques (pare-feu, systèmes d'alarme, caméras de surveillance, IDS).
    - **Mesures Administratives** : Liées à la structure organisationnelle (séparation des tâches, rotations de postes, descriptions de postes, processus d'approbation).
    - **Mesures Légales** : Liées à l'application d'une législation, d'exigences réglementaires ou d'obligations contractuelles.
    - **Mesures Managériales** : Liées à la gestion du personnel (formation des employés, revues de direction, audits internes).
  - Par Fonction:
    - **Mesures Préventives** : Visent à éviter ou à prévenir l'apparition des risques.
    - **Mesures Détectives** : Visent à rechercher, détecter et identifier les risques.
    - **Mesures Correctives** : Visent à réduire les risques identifiés et à prévenir leur réapparition.

Fiche de Révision - Chapitre 3 : Initiation à ITIL 4

Ce chapitre fournit une introduction aux concepts fondamentaux d'ITIL 4 pour la gestion des services informatiques.

- **Introduction à ITIL :**
  - ITIL (Information Technology Infrastructure Library) : Référentiel international de bonnes pratiques pour la gestion des services informatiques (ITSM).
  - Objectif : Fournir une structure aux organisations pour livrer de la valeur aux clients en contrôlant les coûts et les risques, et en favorisant l'innovation.
  - ITIL 4 : Dernière version, adaptée à la transformation numérique, à l'agilité, à DevOps et à l'automatisation.
- **Rappels de quelques définitions:**
  - Service : Moyen d'apporter de la valeur en facilitant l'obtention de résultats souhaités par le client, sans qu'il ait à gérer les coûts ou les risques spécifiques.
  - Valeur : Bénéfices perçus par les parties prenantes (ex: réduction de coûts, gain de temps, amélioration de la qualité).
  - Produit : Combinaison de ressources organisationnelles offertes pour fournir un ou plusieurs services.
  - Offre de service : Description formelle d'un ou plusieurs services basés sur un ou plusieurs produits.
  - Service provider / consumer : Une même organisation peut être à la fois fournisseur et consommateur.
- **Principes Directeurs ITIL** : Ces principes guident toute décision et action dans l'adoption d'ITIL 4, assurant cohérence, adaptation, efficacité et simplicité.

1. Se concentrer sur la valeur : Toujours penser à l'utilité pour le client.
2. Partir de l'existant : Ne jamais repartir de zéro, valoriser les acquis.
3. Progresser par itérations avec retour d'expérience : Avancer étape par étape.
4. Collaborer et promouvoir la visibilité : Travailler ensemble et assurer la transparence.
5. Penser et travailler de manière holistique : Considérer l'ensemble du système, pas seulement les parties isolées.
6. Garder la simplicité et la praticité : Éviter la complexité inutile.
7. Optimiser et automatiser : Améliorer en continu et utiliser la technologie quand cela est approprié.

- **Système de Valeur des Services (SVS) ITIL:**

  Modèle opérationnel qui décrit comment tous les composants et activités d'une organisation travaillent ensemble pour créer de la valeur.

  - Composants clés du SVS:
    - Opportunité/Demande
    - Principes Directeurs
    - Gouvernance : Évaluation, orientation et suivi des actions d'une organisation.
    - Chaîne de Valeur des Services (SVC) : Modèle opérationnel qui définit les activités clés nécessaires pour répondre à une demande et co-créer de la valeur.
    - Activités de la SVC : Planifier, Améliorer, Engager, Concevoir et Transférer, Obtenir/Construire, Livrer et Supporter.
    - Pratiques ITIL : Ensemble de ressources organisationnelles conçues pour exécuter un travail ou atteindre un objectif. (ex: Gestion des incidents, Gestion des problèmes, Gestion des changements).
    - Amélioration Continue : Activité récurrente menée à tous les niveaux de l'organisation pour garantir l'alignement des pratiques et services avec les attentes des parties prenantes.

- **Modèle ITIL d'Amélioration Continue**:
  - Quelle est la vision ?
  - Où en sommes-nous ?
  - Où voulons-nous aller ?
  - Comment y parvenir ?
  - Agir.
  - Mesurer et évaluer.
  - Itérer.