Méthodologie d’audit des systèmes d'information

1. Audit de la Gouvernance et de l'Organisation

L'objectif est de vérifier si la DSI est alignée avec la stratégie de l'entreprise et si les responsabilités sont clairement définies.

- **Alignement Stratégique :** Existe-t-il un Schéma Directeur Informatique ? Les projets IT répondent-ils à des besoins métiers réels ?
- **Séparation des tâches (SoD - Segregation of Duties) :** Un administrateur système ne doit pas être celui qui valide ses propres accès ou qui audite les logs. On vérifie l'absence de conflits d'intérêts techniques.
- **Gestion des Prestataires (SLA) :** Analyse des contrats avec les tiers (Cloud, infogérance). Les engagements de service (temps de rétablissement en cas de panne) sont-ils mesurés et respectés ?
- **Indicateurs (KPI) :** La direction dispose-t-elle de tableaux de bord pour piloter le budget, la performance et les risques IT ?

---

2. Audit de l'Exploitation et de la Maintenance

C'est le "moteur" du SI. L'auditeur vérifie ici la stabilité et la pérennité des opérations quotidiennes.

- **Gestion des Changements (Change Management) :** * Toute modification (mise à jour, nouveau serveur) doit suivre un flux : **Demande → Test (Recette) → Approbation → Mise en production**.
    - *Point d'audit :* Vérifier si des changements ont été faits directement en production sans test préalable.
- **Gestion des Incidents et Problèmes :** Analyse du "Helpdesk". Les incidents récurrents sont-ils identifiés comme des "problèmes" pour en traiter la cause racine ?
- **Sauvegardes et Restauration :** * La règle du **3-2-1** est-elle appliquée (3 copies, 2 supports différents, 1 hors site) ?
    - *Test crucial :* L'auditeur demande une preuve de **test de restauration récent**. Une sauvegarde non testée est considérée comme inexistante.

---

3. Audit du Cycle de Vie des Applications (Développement)

Que l'entreprise développe en interne ou achète des solutions, le processus doit être sécurisé.

- **Méthodologie de Projet :** Utilisation de cycles en V ou de méthodes Agiles avec des jalons de validation clairs.
- **Sécurité par conception (Security by Design) :** Les exigences de sécurité sont-elles définies dès le début du projet ou ajoutées à la fin comme un "patch" ?

- **Gestion du code source :** Utilisation d'outils de versioning (Git) et revue de code pour détecter des portes dérobées ou des erreurs critiques.
- **Environnements étanches :** Séparation stricte entre les données de Développement, de Test et de Production (interdiction d'utiliser de vraies données clients pour les tests).

---

4. Audit de la Continuité d'Activité (PCA / PRA)

En cas de sinistre majeur (incendie, ransomware), l'entreprise peut-elle survivre ?

- **BIA (Business Impact Analysis) :** Les processus critiques ont-ils été identifiés ?
- **RTO / RPO :**
    - **RTO (Recovery Time Objective) :** Durée maximale d'interruption admissible.
    - **RPO (Recovery Point Objective) :** Perte de données maximale admissible (ex: 4h de travail).
- **Tests de secours :** Existe-t-il un rapport de test annuel simulant une bascule sur un site secondaire ?

---

5. Guide d'Exécution : Les Tests d'Audit (Exemples)

Pour chaque domaine, l'auditeur doit collecter des preuves irréfutables :

Objet de l'audit	Test à réaliser	Preuve attendue
Accès Utilisateurs	Tirage aléatoire de 10 départs récents de l'entreprise.	Logs de désactivation des comptes sous 24h.
Intégrité des Données	Comparaison entre la base de données de production et les rapports financiers.	Cohérence des montants et des dates.
Sécurité Physique	Tentative d'entrée dans le local serveur sans badge ou en "tailgating".	Rapport d'anomalie ou déclenchement alarme.
Obsolescence	Inventaire des versions d'OS (Windows, Linux).	Liste des systèmes en "Fin de vie" (End of Life).

Synthèse du Rapport d'Audit SI

Le rapport final doit toujours inclure une **Matrice de Maturité** (échelle de 1 à 5) pour chaque domaine :

1. **Initial :** Processus ad hoc, désorganisé.
2. **Reproductible :** Processus défini mais dépendant des individus.
3. **Défini :** Processus documenté et standardisé.

4. **Géré :** Processus mesuré et contrôlé.
5. **Optimisé :** Amélioration continue automatique.