

# Notion de risques : Chap.9.a: Part 1 : Audit de sécurité

lundi 28 octobre 2024

## III. Audit de Sécurité

### A. Concepts et Objectifs de l'Audit

### B. Méthodologies d'Audit de Sécurité

### C. Normes et cadres de référence (ISO 27001, NIST, etc.)

### D. Références

#### #### Objectifs

- Comprendre les principes et les méthodologies de l'audit de sécurité informatique.
- Apprendre à planifier, exécuter et rapporter un audit de sécurité.

### A. Introduction aux Audit de Sécurité Informatique

- Définition de l'audit de sécurité : \*\* Un audit en cybersécurité est un processus méthodique d'évaluation et de vérification des mesures de sécurité mises en place dans un système informatique, un réseau ou une organisation
- Objectifs de l'audit de sécurité : \*\* C'est d'identifier les failles de sécurité, les vulnérabilités et les risques potentiels, ainsi que de recommander des mesures correctives pour renforcer la sécurité et réduire les risques.
- Importance de l'audit dans la gestion des risques informatiques : \*\* Dans un environnement où les **cybermenaces** sont de plus en plus sophistiquées, l'audit de sécurité informatique joue un rôle crucial dans la gestion des risques informatiques. En identifiant les vulnérabilités et en évaluant les pratiques de sécurité, il permet de prévenir les incidents de sécurité et de renforcer la résilience des systèmes d'information.

### B. Méthodologies d'Audit de Sécurité

#### B.1. \*\*Méthodologies d'Audit : Approche Top-Down/Approche Bottom-Up : 2 approches complémentaires

##### Approche Top-Down :

- Dans une approche top-down, on **cherche à traverser le SI**, à se mettre dans un contexte de hacking.
- Cette approche sert à évaluer le SI dans son ensemble avant de se concentrer sur des aspects plus spécifiques.
- L'utilisation d'outils de pentest (test d'intrusion) est en effet une méthode courante dans une approche top-down. Ces outils permettent de simuler des attaques réelles contre un système ou un réseau, fournissant ainsi une évaluation globale de la sécurité en identifiant les vulnérabilités et les failles potentielles.

##### Approche Bottom-Up :

- À l'inverse, dans une approche bottom-up, on commence par examiner les détails ou les éléments spécifiques avant de remonter vers les aspects plus généraux.
- Cette approche consiste à **examiner les configurations de sécurité des systèmes** de façon individuelle, leurs vulnérabilités spécifiques, ou les incidents passés (des journaux d'audit), avant de tirer des conclusions sur la politique et les procédures de sécurité spécifiques de l'organisation, afin d'identifier les lacunes et les opportunités d'amélioration au niveau opérationnel.
- L'utilisation de méthodes et de normes peut être une composante clé de l'approche bottom-

up. Ces normes fournissent un cadre détaillé pour évaluer et améliorer la sécurité de l'information à tous les niveaux de l'organisation, en fournissant des lignes directrices spécifiques pour la mise en œuvre de contrôles de sécurité. L'utilisation des normes ISO, telles que l'ISO/CEI 27001 peut servir de cadre.

En pratique, une combinaison des deux approches peut être utilisée pour obtenir une vue complète et équilibrée de la sécurité du SI.

En résumé, l'approche top-down met l'accent sur une évaluation globale de la sécurité, souvent en simulant des attaques réelles ou en évaluant l'expérience utilisateur, tandis que l'approche bottom-up se concentre sur l'analyse détaillée des normes, des politiques et des pratiques opérationnelles pour identifier les problèmes spécifiques et les zones d'amélioration.

## B.2. **Méthodologies d'Audit : Audit Interne/Audit Externe**

### **Audit interne :**

- L'objectif principal de l'audit interne est d'évaluer l'efficacité, la pertinence et la conformité des politiques, procédures et contrôles de sécurité de l'organisation.
- L'audit interne est réalisé par des membres de l'organisation elle-même ou par des consultants externes mandatés par l'organisation, mais agissant en tant qu'entité indépendante de l'opérationnel.
- **Le personnel interne est partiellement informé ou totalement informé selon l'objectif visé.**

#### **1. **Audit en boîte blanche :****

- **Objectifs :** L'objectif principal est d'évaluer en profondeur les politiques, procédures et contrôles de sécurité de l'organisation en utilisant une connaissance approfondie des détails internes.
- **Conduite de l'audit :** L'audit en boîte blanche est mené en interne par des membres de l'organisation ou par des consultants externes mandatés par l'organisation, mais agissant en tant qu'entité indépendante de l'opérationnel.
- **Organisation :** **Les membres de l'équipe d'audit ont accès aux détails internes du système, y compris le code source, l'architecture réseau, etc.**
- **Méthodologie :** Les auditeurs peuvent utiliser des outils de sécurité informatique, des analyses de vulnérabilités et des techniques d'inspection approfondie pour évaluer la sécurité de l'organisation.

#### **2. **Audit en boîte grise :****

- **Objectifs :** L'objectif est de réaliser des évaluations plus réalistes en combinant des éléments d'audits en boîte blanche et en boîte noire.
- **Conduite de l'audit :** L'audit en boîte grise est également mené en interne par des membres de l'organisation ou des consultants externes, mais avec un niveau de connaissance limité sur le système.
- **Organisation :** **Les auditeurs ont un certain niveau de connaissance sur le système, mais pas un accès complet aux détails internes.**
- **Méthodologie :** Les auditeurs utilisent une approche mixte qui peut inclure des tests de pénétration externes, des évaluations de la résilience aux attaques et des analyses de conformité.

#### **3. **Audit de conformité :****

- **Objectifs :** L'objectif principal est de vérifier la conformité aux normes et réglementations

internes de l'organisation, il peut également servir à préparer l'organisation à des audits de certification.

- **Conduite de l'audit :** Les audits de conformité internes sont menés en interne par des membres de l'organisation ou par des auditeurs externes.

- **Organisation :** L'objectif est d'évaluer si l'organisation respecte les normes, les réglementations et les politiques de sécurité internes établies par l'entreprise.

- **Méthodologie :** Les auditeurs utilisent des listes de contrôle, des entretiens avec le personnel et des analyses documentaires pour évaluer la conformité.

### Audit Externe :

- L'objectif principal de l'audit externe est de fournir une évaluation objective et impartiale de l'attitude de l'organisation face aux enjeux de la sécurité.
- L'audit externe est mandaté par la direction de l'organisation et est généralement mené par des tiers indépendants, tels que des cabinets d'audit spécialisés en cybersécurité.
- **Le personnel interne peut être non informé, partiellement informé ou totalement informé selon l'objectif visé.**

#### 1. **Test de pénétration (pentest) = Audit en boîte noire :**

- **Objectifs :** L'objectif est de simuler une attaque externe contre l'organisation pour évaluer sa résistance aux menaces.

- **Conduite de l'audit :** Les tests de pénétration sont généralement menés par des tiers externes, tels que des consultants en sécurité, mandatés par l'organisation.

- **Organisation :** **Les auditeurs n'ont pas d'accès aux détails internes du système et agissent comme des attaquants externes.**

- **Méthodologie :** Les auditeurs utilisent des techniques d'attaque réalistes, telles que des scans de vulnérabilités, des tests de phishing et des tentatives d'exploitation de failles pour évaluer la sécurité de l'organisation.

#### 2. **Audit en boîte grise :**

- **Objectifs :** L'objectif est de simuler une attaque externe contre l'organisation pour évaluer sa résistance aux menaces et de combiner des éléments d'audits en boîte blanche.

- **Conduite de l'audit :** Les tests de pénétration sont généralement menés par des tiers externes tout en associant les équipes internes, permettant un niveau de connaissance limité du SI.

- **Organisation :** **Les auditeurs peuvent avoir un certain niveau de connaissance d'éléments du SI (cible potentielle), mais pas un accès complet aux détails internes du SI.**

- **Méthodologie :** Approche mixte : Approche boîte noire et analyses de conformité.

### B.3. **Processus d'audit (planification, exécution, rapport)**

Le processus d'audit de sécurité informatique comprend plusieurs étapes clés, notamment la planification de l'audit, l'exécution des tests et des enquêtes, et la rédaction du rapport final. Chaque étape est cruciale pour assurer l'efficacité de l'audit et la pertinence des recommandations.

#### **Cadre général du processus des audits :**

Les audits internes sont des évaluations périodiques des politiques, procédures et contrôles de sécurité d'une organisation, menées par des membres internes de l'organisation ou des consultants externes mandatés par celle-ci. Le processus d'audit interne comprend généralement les étapes

suivantes :

### 1. **\*\*Planification de l'audit :\*\***

- Définition des objectifs spécifiques de l'audit en fonction des besoins de l'organisation.
- Détermination de la portée de l'audit en identifiant les systèmes, processus ou domaines spécifiques à évaluer.
- Allocation des ressources nécessaires, telles que le personnel qualifié, les outils d'audit et le budget.
- Élaboration d'un plan d'audit détaillé comprenant les activités à entreprendre, les responsabilités des membres de l'équipe d'audit, le calendrier et les critères d'évaluation.

### 2. **\*\*Exécution de l'audit :\*\***

- Collecte d'informations sur les systèmes informatiques, les politiques de sécurité, les processus opérationnels, etc.
- Évaluation des contrôles de sécurité existants pour vérifier leur conformité aux politiques et normes établies et leur capacité à atténuer les risques.
- Analyse des vulnérabilités pour identifier les failles de sécurité potentielles dans les systèmes et les processus.

### 3. **\*\*Rapport d'audit :\*\***

- Documentation détaillée des résultats de l'audit, y compris les constatations, observations et recommandations.
- Présentation des conclusions aux parties prenantes avec une explication claire des résultats et des recommandations.
- Formulation de recommandations spécifiques pour remédier aux lacunes de sécurité identifiées et améliorer la posture de sécurité globale.

## C. Normes et cadres de référence (ISO 27001, NIST, etc.)

Les normes et cadres de référence fournissent des lignes directrices et des meilleures pratiques pour réaliser des audits de sécurité informatique. Parmi les plus utilisés, on trouve l'ISO 27001 pour la gestion de la sécurité de l'information et les publications du NIST (National Institute of Standards and Technology) pour les recommandations en matière de sécurité (USA).

### C.1. ISO 27001 (Norme ISO/IEC 27001)\*\* :

- L'ISO 27001 est une norme internationale qui spécifie les exigences pour établir, mettre en œuvre, tenir à jour et améliorer un **Système de Management de la Sécurité de l'Information (SMSI)** au sein d'une organisation.
- Elle fournit un cadre complet pour identifier, évaluer et traiter les risques liés à la sécurité de l'information, tout en garantissant la confidentialité, l'intégrité et la disponibilité des données.
- L'ISO 27001 repose sur une approche de gestion des risques, où les organisations doivent identifier les risques de sécurité de l'information auxquels elles sont confrontées, évaluer leur impact et leur probabilité, puis mettre en œuvre des mesures de sécurité appropriées pour les atténuer.

### 1. **\*\*Domaine d'application :\*\***

- La norme ISO 27001 spécifie les exigences pour établir, mettre en œuvre, tenir à jour et améliorer

un système de management de la sécurité de l'information (SMSI) au sein d'une organisation.

- Elle s'applique à toutes les organisations, quel que soit leur type, leur taille ou leur secteur d'activité, qui cherchent à protéger les informations sensibles et à gérer les risques liés à la sécurité de l'information.

## 2. **\*\*Références normatives : \*\***

- La norme ISO 27001 fait référence à plusieurs autres normes et documents connexes qui peuvent être utilisés pour compléter les exigences de la norme, notamment :

- ISO/IEC 27002: Code de bonnes pratiques pour le management de la sécurité de l'information.
- ISO/IEC 27003: Guide d'implémentation de l'ISO 27001.
- ISO/IEC 27004: Lignes directrices pour la mesure des résultats du management de la sécurité de l'information.
- **ISO/IEC 27005**: Gestion des risques liés à la sécurité de l'information.
- ISO/IEC 27007: Lignes directrices pour l'audit de systèmes de management de la sécurité de l'information.

### C.2. Code de bonnes pratiques pour le management de la sécurité de l'information (ISO 27002, ITIL, etc.)

Avant de se conférer à répondre aux exigences d'une norme, telle que la **norme ISO 27002**, il convient pour les personnes chargées du système d'information d'appliquer des mesures de sécurité organisationnelle, de sécurité applicables aux personnes, de sécurité physique et de sécurité technologique. S'inspirer des **référentiels ITIL** peut-être une source de cadrage de la démarche. Ce cadrage permet de s'inscrire dans **une démarche d'exécution de l'audit** sans être dans une démarche normée.

#### **A) Mesures de sécurité organisationnelles**

##### 1. **\*\*Politique de sécurité de l'information : \*\***

- Élaboration et communication d'une politique de sécurité de l'information qui définit les objectifs, les responsabilités et les exigences en matière de sécurité au sein de l'organisation.

##### 2. **\*\*Gestion des actifs : \*\***

- Identification, classification et gestion des actifs informationnels de l'organisation, y compris les données, les systèmes, les équipements et les ressources connexes.

##### 3. **\*\*Conformité : \*\***

- Assurer la conformité aux lois, réglementations, normes et politiques internes en matière de sécurité de l'information, ainsi que la gestion des risques liés à la non-conformité.

- => **Complète les Processus Organisationnels du "Chapitre 2 : Les éléments de la sécurité"**
  - [Notion de risques : Chap.2 : Les éléments de la sécurité](#)

#### **B) Mesures de sécurité applicables aux personnes**

##### 4. **\*\*Sécurité des ressources humaines : \*\***

- Gestion des ressources humaines en matière de sécurité de l'information, y compris les processus

de recrutement, de formation, de sensibilisation et de gestion des incidents liés aux employés.

- => **Complète les Menaces/sensibilisation/Formation du "Chapitre 7 : Sécurité humaine"**
  - Notion de risques : Chap.7 : Sécurité humaine

### **C) Mesures de sécurité physique**

#### **5. \*\*Sécurité physique et environnementale : \*\***

- Mise en place de mesures de sécurité physiques et environnementales pour protéger les locaux, les équipements et les ressources contre les menaces physiques telles que le vol, les incendies et les catastrophes naturelles.

- => **Complète les Menaces et Mesures à la sécurité physique** du "Chapitre 3 : Sécurité physique"
  - Notion de risques : Chap.3 : Sécurité physique

### **D) Mesures de sécurité technologiques**

#### **6. \*\*Gestion des configurations**

- La gestion des configurations implique d'identifier les éléments informatiques, de contrôler les modifications apportées à ces éléments, et de tenir un enregistrement des configurations et des versions. Son objectif est d'assurer l'intégrité et la sécurité des systèmes en garantissant une gestion structurée et documentée des changements.

#### **7. \*\*Accès aux systèmes et aux données : \*\***

- Contrôle de l'accès aux systèmes et aux données par le biais de politiques, de procédures et de mécanismes techniques tels que l'authentification, l'autorisation et la gestion des droits d'accès.

#### **8. \*\*Cryptographie : \*\***

- Utilisation de techniques de cryptographie pour protéger les données sensibles, les communications et les transactions contre les accès non autorisés et les altérations.

#### **9. \*\*Gestion des opérations : \*\***

- Gestion des opérations informatiques et des communications, y compris la surveillance des activités, la protection contre les logiciels malveillants, la sauvegarde des données et la gestion des incidents.

#### **10. \*\*Contrôle d'accès : \*\***

- Mise en place de contrôles d'accès appropriés pour garantir que seules les personnes autorisées peuvent accéder aux informations et aux systèmes, et que cet accès est accordé en fonction des besoins et des privilèges des utilisateurs.

#### **11. \*\*Sécurité des systèmes d'information : \*\***

- Mise en place de mesures de sécurité techniques pour protéger les systèmes d'information contre les menaces telles que les failles de sécurité, les vulnérabilités et les attaques informatiques.

#### **12. \*\*Gestion des incidents de sécurité : \*\***

- Élaboration et mise en œuvre d'un processus de gestion des incidents de sécurité pour détecter, signaler, enquêter et répondre aux incidents de sécurité de manière efficace et opportune.

#### 13. **\*\*Gestion de la continuité d'activité : \*\***

- Planification et préparation de mesures pour assurer la continuité des activités en cas d'incident majeur ou de catastrophe, afin de minimiser les perturbations et de garantir la reprise des opérations critiques.

#### 14. **\*\*Gestion des changements**

- La gestion des changements est un processus méthodique permettant de planifier, d'implémenter et de contrôler les modifications au sein des systèmes informatiques d'une organisation. Son objectif est de minimiser les risques et les perturbations opérationnelles tout en maximisant les avantages des changements proposés.

- => S'applique aux "Chapitre 4, 5, 6 et 8"

## D. Sources

- [En quoi consiste un audit de sécurité informatique ? - Axido]( <https://www.axido.fr/securite-it/audit-securite-informatique/>)

#### **- Autres Sources de référentiel normatif : \*\***

**\*\*NIST Cybersecurity Framework (CSF) \*\* :**

- Le Cadre de cybersécurité du NIST est un ensemble de meilleures pratiques, de normes et de directives pour aider les organisations à gérer et à réduire leurs risques en matière de cybersécurité.

- Normes USA : National Institute of Standards and Technology (NIST)

**\*\*COBIT (Control Objectives for Information and Related Technologies) \*\* :**

- COBIT est un cadre de gouvernance et de gestion des technologies de l'information (TI) développé par l'ISACA (Association de contrôle et d'audit des systèmes d'information).

- Normes USA

**\*\*PCI DSS (Payment Card Industry Data Security Standard) \*\* :**

- Le PCI DSS est une norme de sécurité des données développée par le Conseil des normes de sécurité (PCI SSC) pour assurer la sécurité des informations de paiement des cartes de crédit et de débit.

#### **Sources d'informations :**

- [Audit de sécurité — Wikipédia](#) : Explique les grandes lignes d'un audit de sécurité

- [Comment réaliser un audit de sécurité informatique ? - Appvizer]( <https://www.appvizer.fr/magazine/services-informatiques/securite-informatique/audit-de-securite-informatique>)

- [Audit de sécurité informatique - Diagnostiquez et analyser votre SI - OCI]( <https://www.oci.fr/sublimez-votre-it/securite-informatique/audit-de-securite/>)

- [Comment faire un audit de sécurité informatique ? - IPE]( <https://www.ipe.fr/comment-faire-un-audit-de-securite-informatique/>)

- [Audit de sécurité : les différents Audits et Pentest | Certilience]( <https://www.certilience.fr/nos-metiers/audit-de-securite-pentest/>)
- [Que faut-il vérifier dans un audit de sécurité informatique ? - ITAIA]( <https://www.itaia.fr/audit-securite-points-importants/>)