## Qu'est-ce que l'ISO/IEC 27001 ?

**ISO/IEC 27001** est une norme internationale de référence pour la **gestion de la sécurité de l'information**. Elle définit un *Système de Management de la Sécurité de l'Information (SMSI)* permettant aux organisations de protéger efficacement leurs données sensibles contre les risques de perte, vol, altération ou accès non autorisé.

**Objectifs principaux :**

- Assurer la **confidentialité**, l'**intégrité** et la **disponibilité** de l'information.
- Identifier et évaluer les risques liés à la sécurité de l'information.
- Mettre en place des contrôles adaptés pour réduire ces risques.
- Instaurer une démarche d'**amélioration continue**.

**Éléments clés de la norme :**

- **Contexte organisationnel :** analyse des besoins, des parties prenantes et du périmètre du SMSI.
- **Leadership :** implication de la direction et définition des responsabilités.
- **Planification :** gestion des risques et opportunités.
- **Support :** ressources, compétences, sensibilisation et communication.
- **Exploitation :** mise en œuvre des mesures de sécurité.
- **Évaluation :** audits internes, suivi des performances, revue de direction.
- **Amélioration continue :** actions correctives et évolutives.

**Exemple d'application en entreprise :**

- Mise en place d'une politique de sécurité informatique.
- Contrôle des accès aux systèmes critiques.
- Gestion des incidents de sécurité et plan de continuité d'activité.

**Avantage :** l'obtention de la certification ISO/IEC 27001 démontre la maturité et la fiabilité d'une organisation en matière de cybersécurité, renforçant la confiance des clients et partenaires.

Qu'est-ce que l'ISO/IEC 27005 ?

**ISO/IEC 27005** est une norme internationale qui fournit des lignes directrices pour la **gestion des risques liés à la sécurité de l'information**. Elle est conçue pour accompagner la mise en œuvre d'un **SMSI (Système de Management de la Sécurité de l'Information)** conformément à la norme **ISO/IEC 27001**.

**Objectifs principaux :**

- Identifier, analyser et évaluer les risques de sécurité de l'information.
- Déterminer les mesures de sécurité adaptées pour réduire les risques.
- Fournir un cadre méthodologique pour la prise de décision.
- Soutenir l'amélioration continue du SMSI.

**Étapes clés de la gestion des risques selon ISO/IEC 27005 :**

1. **Établissement du contexte** : définir le périmètre et les critères d'évaluation des risques.
2. **Identification des risques** : recenser les actifs, menaces et vulnérabilités.
3. **Analyse des risques** : estimer la vraisemblance et l'impact des incidents.
4. **Évaluation des risques** : prioriser les risques selon leur criticité.
5. **Traitement des risques** : définir et mettre en œuvre des mesures de sécurité.
6. **Acceptation et communication des risques** : décision par la direction.
7. **Surveillance et réexamen** : mise à jour régulière en fonction des évolutions.

**Lien avec ISO/IEC 27001 :**

- ISO/IEC 27001 définit les exigences pour établir un SMSI.
- ISO/IEC 27005 fournit la méthodologie pratique pour gérer les risques sur lesquels repose le SMSI.

**Exemple concret :** Dans une entreprise, ISO/IEC 27005 peut servir à évaluer le risque de fuite de données via une clé USB non chiffrée, puis recommander comme traitement l'*interdiction technique des ports USB* ou le *chiffrement obligatoire*.

Qu'est-ce que l'ITIL ?

**ITIL (Information Technology Infrastructure Library)** est un *ensemble de bonnes pratiques* pour la **gestion des services informatiques (ITSM – IT Service Management)**. Il fournit un cadre méthodologique permettant aux organisations de concevoir, délivrer, exploiter et améliorer leurs services informatiques en alignement avec les besoins métiers.

**Objectifs principaux :**

- Améliorer la **qualité des services informatiques**.
- Optimiser les **coûts et ressources** liés aux services IT.
- Assurer une meilleure **satisfaction des utilisateurs et clients**.
- Instaurer une démarche d'**amélioration continue**.

**Composantes clés d'ITIL (version 4) :**

- **Principes directeurs** : orientation valeur, collaboration, simplicité, optimisation et automatisation.
- **Système de valeur des services (SVS)** : vision globale intégrant gouvernance, pratiques et amélioration continue.
- **Pratiques ITIL** (anciennement processus) : gestion des incidents, gestion des changements, gestion des niveaux de service, gestion des actifs, etc.
- **Chaîne de valeur des services** : activités qui transforment la demande en valeur pour le client.

**Exemple concret en entreprise :**

- Mise en place d'un *helpdesk* centralisé pour gérer les incidents utilisateurs.
- Processus structuré de gestion des changements afin de réduire les risques lors des mises en production.
- Suivi des SLA (Service Level Agreements) pour mesurer la qualité des services fournis.

**Avantage :** ITIL n'est pas une norme mais un *référentiel de bonnes pratiques* : chaque organisation peut l'adapter à son contexte pour structurer son service informatique et créer de la valeur.