**ISO/IEC 27001** est une norme internationale publiée par l’**Organisation internationale de normalisation (ISO)** et la **Commission électrotechnique internationale (IEC)**. Elle spécifie les exigences pour établir, mettre en œuvre, maintenir et améliorer un **système de management de la sécurité de l'information** (SMSI ou ISMS en anglais – *Information Security Management System*).

**🎯 Objectif principal :**

Assurer la **confidentialité**, **intégrité** et **disponibilité** des informations dans une organisation, en identifiant les risques et en les traitant de manière systématique.

**📚 Principaux éléments d’ISO 27001 :**

1. **Évaluation des risques :** Identifier et analyser les menaces sur les actifs informationnels.
2. **Mesures de sécurité :** Mettre en place des **contrôles** pour réduire les risques (voir annexe A avec 93 contrôles regroupés en 4 thèmes selon la version 2022).
3. **Politique de sécurité :** Rédaction et communication des règles de sécurité dans l’entreprise.
4. **Amélioration continue :** Basée sur le cycle **PDCA** (Plan, Do, Check, Act).

**🔐 Exemples de domaines couverts :**

* Contrôle d’accès
* Sécurité physique
* Sécurité des communications
* Cryptographie
* Sécurité des fournisseurs
* Gestion des incidents
* Continuité d’activité

**✅ Certification :**

Une organisation peut se faire **certifier ISO 27001** par un organisme accrédité, ce qui prouve à ses clients, partenaires ou régulateurs qu'elle gère la sécurité de l'information de manière sérieuse et contrôlée.

**ISO/IEC 27002** est une norme complémentaire à **ISO/IEC 27001**. Elle **n’est pas certifiable**, mais elle fournit des **lignes directrices détaillées** pour la mise en œuvre des **contrôles de sécurité** listés dans l’annexe A d’ISO 27001.

### 🔍 ****Différence ISO 27001 vs 27002 :****

| **ISO 27001** | **ISO 27002** |
| --- | --- |
| Norme certifiable | Norme non certifiable |
| Spécifie les exigences d’un SMSI | Fournit des lignes directrices pour les contrôles |
| Orientation “quoi faire” | Orientation “comment faire” |

### 📚 ****Contenu d'ISO 27002:2022 (dernière version)****

La version 2022 a restructuré les contrôles autour de **4 grands thèmes** (au lieu de 14 dans la version 2013), avec un total de **93 contrôles** :

#### 🔹 1. **Organizational controls** (Contrôles organisationnels – 37)

Exemples :

* Politique de sécurité
* Rôles et responsabilités de la sécurité
* Classification de l'information
* Continuité d'activité

#### 🔹 2. **People controls** (Contrôles liés aux personnes – 8)

Exemples :

* Sensibilisation à la sécurité
* Confidentialité des employés
* Procédures de départ

#### 🔹 3. **Physical controls** (Contrôles physiques – 14)

Exemples :

* Sécurité des locaux
* Contrôle d’accès physique
* Protection contre les incendies

#### 🔹 4. **Technological controls** (Contrôles technologiques – 34)

Exemples :

* Contrôle d’accès logique
* Cryptographie
* Sécurité réseau
* Sécurité des applications

### 🆕 Nouveautés ISO 27002:2022

* **Attributs des contrôles** : Chaque contrôle est accompagné de métadonnées (type de menace, propriété de sécurité visée, etc.) pour aider à la sélection/adaptation.
* **Réduction du nombre de contrôles** : Fusion/simplification par rapport à la version précédente.

### 🎯 Utilité :

* Sert de **guide pratique** pour implémenter la sécurité selon ISO 27001.
* Utile pour les **responsables SSI, RSSI, DSI, auditeurs** ou consultants sécurité.

**ISO/IEC 27005** est la norme dédiée à la **gestion des risques liés à la sécurité de l'information** dans le cadre d’un SMSI (Système de Management de la Sécurité de l'Information), comme défini dans **ISO 27001**.

**🎯 Objectif de la norme ISO 27005**

Fournir une **méthodologie complète** pour identifier, analyser, évaluer, traiter, surveiller et revoir les **risques liés à l'information**.

Elle soutient directement ISO 27001, notamment pour répondre aux exigences des clauses 6.1.2 et 6.1.3 (analyse et traitement des risques).

**🛠️ Structure générale du processus de gestion des risques ISO 27005**

1. **Contexte** :
   * Définir les objectifs métier
   * Identifier les actifs informationnels
   * Déterminer les parties prenantes et les critères de risque
2. **Identification des risques** :
   * Identifier les actifs
   * Identifier les menaces et vulnérabilités
   * Identifier les conséquences
3. **Analyse des risques** :
   * Estimer la **probabilité** et l’**impact**
   * Calculer le **niveau de risque**
4. **Évaluation des risques** :
   * Comparer les niveaux de risque avec les **critères d’acceptabilité**
   * Décider quels risques nécessitent un traitement
5. **Traitement des risques** :
   * Accepter, éviter, transférer ou atténuer le risque
   * Sélectionner des **mesures de sécurité** appropriées (souvent tirées d’ISO 27002)
6. **Acceptation des risques**
7. **Communication et consultation**
8. **Surveillance et révision**

**🔄 Méthodes compatibles**

ISO 27005 **n’impose pas** une méthode unique, mais peut s’appuyer sur :

* **EBIOS** (France)
* **MEHARI**
* **OCTAVE**
* **FAIR**
* **ISO 31000** (cadre générique de gestion des risques)

**📌 Exemple de risque traité :**

* **Actif :** Base de données clients
* **Menace :** Piratage
* **Vulnérabilité :** Mots de passe faibles
* **Impact :** Fuite de données, sanctions RGPD
* **Mesure ISO 27002 :** Authentification forte