Normes en sécurité de l'information (27001 27002 27005) AFNOR – ISO - CEN

Paul Richy

ISO

- Créée en 1947
  - 175 pays environ – **1 voix par pays** – L'**AFNOR** est le **représentant français** - Environ **275 Comités Techniques** et plus de **26OOO normes**
  - Une norme passe par différents stades
    - NNWIP New Work Item Proposal
    - WD Working Draft
    - CD Committee Draft
    - DIS/FDIS Draft (Final) International Standard
  - Le dernier vote exige moins de 25% de votes négatifs (**consensus**)
  - Une norme est révisée tous les 5 ans et la révision demande en général 3 ou 4 ans

ISO

- **Quelques Comités Techniques importants**
  - **JTC 1** – Secrétariat USA- **Technologies de l'information** – Plus de **3500 normes**. Parmi ses Sous-Comités, le **SC 27** est en charge de **la sécurité de l'information, de la cybersécurité et de la protection de la vie privée** et le **SC 42** traite de **l'intelligence artificielle et du Big Data**
  - **TC 20** – Secrétariat USA - **Aéronautique et espace** près de **700 normes**
  - **TC 22** – Secrétariat France - **Véhicules routiers** plus de **1000 normes**
  - **TC 34** – Secrétariat France – **Produits alimentaires** plus de **900 normes**
  - **TC 292** – Secrétariat Suède - **Sécurité et résilience** plus de **60 normes**

AFNOR

- Créée en 1926
  - Membre français de l'ISO
    - Niveau mondial ISO
    - Niveau européen CEN (Comité Européen de Normalisation) créé en 1961 – 33 membres – UE, 3 pays de l'AELE (Suisse, Norvège, Islande), Turquie et Macédoine du Nord
  - Participation **ouverte à tous** - Cotisation basée sur le CA de l'entreprise et sur le rôle exercé au sein de la structure AFNOR
  - La **CN Cyber** est le miroir français du JTC 1 /SC 27 en charge de **la sécurité de l'information, de la cybersécurité et de la protection de la vie privée**
  - Chaque Comité Technique **se réunit 2 fois par an**. Les réunions, autrefois en présentiel, sont **passées en mode hybride** depuis la pandémie

ISO/CEI 27001

- **Norme de management parue en 2005**
  - Elle définit la notion d'**ISMS** (Information Security Management System), encourage l'adoption d'une approche **processus** dans une perspective d'**amélioration continue**
  - Elle est orientée vers l'évaluation de **conformité** et la **certification** via la **DdA** (Déclaration d'Applicabilité)
  - Révisée en 2013 puis en 2022. Dans ce dernier cas, la révision correspond à la simple prise en compte de la nouvelle version de l'ISO/CEI 27002 parue la même année
  - L'**Annexe A** (objectifs des mesures et mesures tirées de l'ISO/CEI 27002) est d'**application obligatoire**
  - Cette norme permet aussi la **certification de personnes** (**Lead Auditor** 27001, **Lead Implementor** 27003 et **Information Security Risk Manager** (ISO/CEI 27005)

ISO/CEI 27002

- **Norme technique parue en 2005**

  - Trois versions :
    2005 11 chapitres et 133 mesures
    2013 14 chapitres et 114 mesures
    2022 4 chapitres et 93 mesures

  - Dans la version actuelle, les 4 chapitres distinguent :
    Mesures **organisationnelles** (37 dont 3 nouvelles)
    Mesures liées aux **personnes** (8, aucune nouvelle)
    Contrôles **physiques** (14, 1 nouveau)
    Mesures **technologiques** (34 dont 5 nouvelles)

ISO/CEI 27002

- **Norme technique parue en 2005**
  - Dans la version actuelle, la notion d'**attributs** apparaît avec **5 thèmes** proposés

    Type de mesure (Prévention, Détection, Correction)
    Propriété en sécurité de l''information (critères DIC)
    Concepts de **cybersécurité** (approche NIST issue du **Security Framework :** Identifier, Protéger, Détecter, Répondre, Restaurer)
    Capacité opérationnelle (15 attributs proposés)
    Domaines de sécurité (Gouvernance et écosystème, Protection, Défense, Résilience)

ISO/CEI 27005

- **Norme parue en 2005, révisée en 2011 puis en 2018**
  La version actuelle est parue en 2022

  - La norme traite de la **gestion du risque en sécurité de l'information**

  - Elle permet de **valider la conformité de méthodes** d'analyse des risques en sécurité de l'information

  - L'annexe A de la version 2022 valide l'approche **EBIOS Risk Manager**

Compléments

- **27001** study period pour préparer révision
- **27002** study period pour préparer révision
- **27005** study period pour préparer révision
- Cas du **TC 292** (**Sécurité et résilience**). Il n'y a pas d'approche en analyse de risques par scénarios mais par BIA (Business Impact Analysis)
- Cas du **JTC 1 SC 42** (**Intelligence artificielle et big data**). Problèmes pour l'analyse de risques et pour les données personnelles
- Evolution des conditions de **réunion** pour les commissions de normalisation, **hybride** donc **moins de présentiel**