Club 27001

La norme ISO 27002

Elisabeth Manca
Hervé Schauer

HS2
Hervé Schauer Sécurité

Plan

- La norme ISO 27002:2022
  - Présentation
  - La nouvelle structure de la norme et des mesures
- Les mesures de sécurité de la norme ISO 27002
  - Classement
  - Exemples d'évolution des mesures

- ISO/IEC 27002:2022
  - *Information security, cybersecurity and privacy protection — Information security controls*
    - Rappels de la version 27002:2013 : *Code of practice for information security controls*
  - *Volumétrie*
    - *Nombre total de pages : 164*
    - *Notes préliminaires, vocabulaires et bibliographie*
      - ➔ *19 pages*
        - *Liste des mesures de sécurité*
          - ➔ *122 pages*
  - *Annexe A : synthèse des attributs pour développer leurs usages*
  - *Annexe B pour aider à la correspondance des mesures de la précédente version*

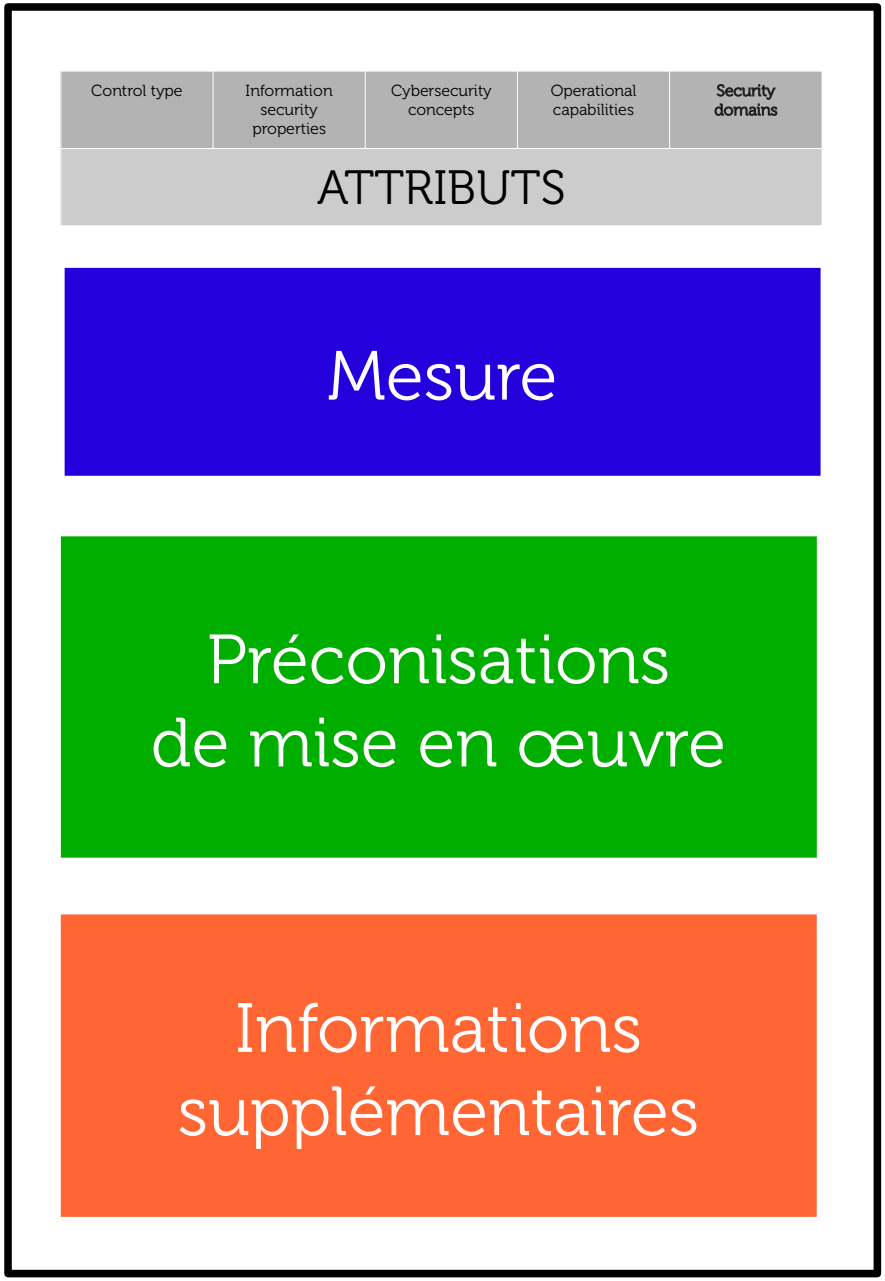
Rappel : ISO 27002:2013

Ce qui est présent dans l'annexe A de l'actuelle 27001 :

- 14 chapitres
- 35 objectifs de sécurité (*control objectives*)
- 114 mesures de sécurité (*security controls*)

Nouvelle structure de chaque mesure

- Tableau des attributs
- Énoncé de la mesure de sécurité
- Recommandations pour l'implémentation de la mesure
  - **Pas toujours applicables**
- Explications sur le guide d'implémentation
  - Aspects complémentaires
  - Autres facteurs à prendre en compte
  - Lien avec d'autres mesures



La révision de la norme ISO27002

- Réorganisation des mesures selon 4 thèmes :
  - §5 : Organizational controls (37)
  - §6 : People controls (8)
  - §7 : Physical controls (14)
  - §8 : Technological controls (34)

    –> **93 mesures,**

- Suppression d'une mesure (Removal of assets)
- L'identifiant de la mesure est sur 2 nombres séparés d'un point au lieu de 3 :
  - Le numéro du chapitre
  - Le numéro dans le chapitre
  - Il n'y a plus d'identifiant d'objectif

La révision de la norme ISO27002

Recombinaison-fusion de mesures pour 22 sujets

- Policies for information security
- Information security in project management
- User endpoint devices
- Inventory of information and other associated assets
- Acceptable use of information and other associated assets
- Information transfer
- Storage media
- Access control
- Authentication information
- Access rights
- Monitoring, review and change management of supplier services
- Information security during disruption
- Identification of legal, statutory, regulatory and contractual requirements
- Compliance with policies and standards for information security
- Information security event reporting
- Management of technical vulnerabilities
- Logging
- Installation of software on operational systems
- Application security requirements
- Security testing in development and acceptance
- Separation of development, test and production environments
- Change management

La révision de la norme ISO27002

- Ajout de 11 mesures :
  - 5.7 Threat intelligence
  - 5.23 Information security for use of cloud services
  - 5.30 ICT readiness for business continuity
  - 7.4 Physical security monitoring
  - 8.9 Configuration management
  - 8.10 Information deletion
  - 8.11 Data masking
  - 8.12 Data leakage prevention
  - 8.16 Monitoring activities
  - 8.23 Web filtering
  - 8.28 Secure coding

La révision de la norme ISO27002

- Ajout d'attributs pour chaque mesure (1/2) :
  - **Control types** : à quel moment du risque la mesure agit :
    - Preventive : avant,
    - Detective : pendant,
    - Corrective : après
  - **Information security properties** : sur quel critère de sécurité, la mesure agit (disponibilité, intégrité et/ou confidentialité)
  - **Cybersecurity concepts** : en lien avec les concepts du cycle de vie de la Cybersécurité (ISO/IEC TS 27110) similaire au framework du NIST :
    - Identify, Protect, Detect, Respond and Recover.

La révision de la norme ISO27002

- Ajout d'attributs pour chaque mesure (2/2) :
  - **Operational capabilities** : capacités opérationnelles du point de vue de l'implémenteur en lien avec les 14 précédents chapitres :
    - Governance, Asset management, Information protection, Human resource security, Physical security, System and network security, Application security, Secure configuration, Identity and access management, Threat and vulnerability management, Continuity, Supplier relationships security, Legal and compliance, Information security event management and Information security assurance
  - **Security domains** : en lien avec un domaine de la sécurité de l'information :
    - Governance and Ecosystem, Protection, Defence and Resilience

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Eco-system #Resilience

Choix de mesures de sécurité

- Choisir la mesure de sécurité qui permet de réduire le risque
  - En agissant sur la vulnérabilité ou la menace : #PREVENTIVE
  - En surveillant le risque et en agissant lorsqu'il se produit : #DETECTIVE
  - En préparant la réaction après l'incident : #CORRECTIVE
- En fonction de l'actif et/ou du risque
  - Plusieurs articles et objectifs peuvent entrer en jeu
  - Plusieurs mesures peuvent être nécessaires
- Prendre en considération
  - Le PDCA
  - L'organisation
  - Les aspects techniques

Choix de mesures de sécurité

- Exemple de mesure de sécurité (1 pour 1)
  - 7.11 (ex 11.2.2) Supporting utilities
    - *Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.*
    - *Purpose :*
      - To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection

Listes de mesures de sécurité §5

Politiques pour la sécurité de l'information(5.1)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Eco-system #Resilience

- *Fusion 5.1.1 et 5.1.2*
- Définir, Formaliser, approuver, publier, communiquer et réviser :
- Ensemble de politiques de sécurité :
  - Prennent en compte la stratégie, les exigences légales et contractuelles, les menaces
  - Contiennent la définition de la sécurité de l'information, les objectifs et principes applicables, les responsabilités et les règles de contournement éventuelles
  - Exemples de thèmes : Contrôle d'accès, classification de l'information, sécurité physique, sauvegardes, transfert d'information, protection contre les logiciels malfaisants, gestion des vulnérabilités techniques, gestion des tiers, etc.
- Revue des politiques *(intégrée en une seule mesure)*
  - A intervalles réguliers et planifiés ou lors de changements significatifs
  - Revalidations régulières par le management

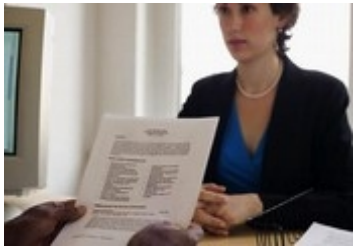
Relation avec les fournisseurs (ex §15)

- Sécurité de l'information dans les relations avec les fournisseurs(5.19 ex 15.1.1)
- Prise en compte de la sécurité dans les accords conclus avec les fournisseurs(5.20 ex 15.1.2)
- Gestion dans la sécruité de l'information pour la supply-chain en technologie de l'information et de la communication(5.21 ex 15.1.3)
- Surveillance et réexamen des services rendus par les fournisseurs et la gestion des changements(5.22 ex 15.1.2 & 15.2.2)
- + **Sécurité de l'information pour l'usage des services Cloud** (5.23)

Listes de mesures de sécurité §6

Sécurité liée aux ressources humaines (6 ex §7)

- **Le début du chapitre 6 reprend le chapitre 7 (1 pour 1)**
- Avant le recrutement
  - Sélection (6.1 ex 7.1.1)
    - Vérifications avant embauches (CV, Diplôme, casier)
  - Conditions d'embauche (6.2 ex 7.1.2)
    - Contrats, NDA, engagements



- Pendant la durée du contrat
  - Responsabilités de la direction (5.4 ex 7.2.1)
  - Sensibilisation, qualification et formations en matière de sécurité de l'information (6.3 ex 7.2.2)
  - Processus disciplinaire (6.4 ex 7.2.3)
- Fin ou modification du contrat
  - Responsabilités en fin de contrat (6.5 ex 7.3.1)

- NDA (6.6 ex 13.2.4)
- Travail à distance (6.7 ex 6.2.2)
- Signalement des évènements de sécurité (intègre les failles) (6.8 ex 16.1.2 & 16.1.3)

Listes de mesures de sécurité §7

Sécurité physique (7 ex §11)

- Sécurité des locaux
  - Périmètre de sécurité physique (7.1 ex 11.1.1)
  - Contrôles Physiques des accès (7.2 ex 11.1.2 & 11.1.6)
    - Intègre l'ancienne mesure : Zones de livraison et chargements
  - Sécurité des bureaux, salles & équipemets (7.3 ex 11.1.3)
  - + **Physical security Monitoring** (7.4)
  - Protection contre les menaces extérieurs et environnementales (7.5 ex 11.1.4)
  - Travail dans les zones sécurisés (7.6 ex 11.1.5)

Sécurité physique (7 ex §11)

- Sécurité du matériel
  - Politique du bureau et écran vide (7.7 ex 11.2.9)
  - Placer le matériel dans une zone non exposée (7.8 ex 11.2.1)
  - Sécurité des équipements en dehors de locaux (7.9 ex 11.2.6)
  - Sortie de matériel (7.10 regroupe 8.3.1, 8.3.2, 8.3.3 & 11.2.5)
  - Disponibilité de l'alimentation et des services essentiels (7.11 ex 11.2.2)
  - Sécurité du câblage (7.12 ex 11.2.3)
  - Maintenance du matériel (7.13 ex 11.2.4)
  - Mise au rebut et réutilisation des équipements (7.14 ex 11.2.7)

Listes de mesures de sécurité §8

Logging (8.15)

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence

- Regroupe les activités :
  - Journalisation des événements (ex 12.4.1 & 12.4.3)
  - Protection des informations journalisées (ex 12.4.2)
  - + Conservation
  - + Analyses pour aider à identifier une activité ou un comportement inhabituel (IOC)

- Mesures liées :
  - Synchronisation des horloges (8.17 ex 12.4.4)
  - Collecte des preuves (5.28 ex 16.1.7)
  - + Data Masking (8.11)
  - Gestion des évènements de sécurité (5.25 ex 16.1.4)
  - Protection des données à caractère personnel (5.34 ex 18.1.4)
  - Surveillance des activités (5.16 ex 9.2.1)

Pour préparer la migration vers la nouvelle Annexe A

- Utiliser l'annexe B pour faire le lien avec les mesures actuelles dans le plan de traitement des risques et la DdA
- Informer les responsables de mesures des évolutions :
  - Regroupement
  - Evolution du contenu en termes d'objectifs de sécurité et d'activités
  - Nouvelles mesures à étudier dans leur périmètre de responsabilités (en prévision de la révision de l'analyse des risques)
- Organiser le plan d'évolution des mesures de sécurité existantes (budget, documentation, processus, procédures opérationnelles, formation…)