

Club 27001

La norme ISO 27002



Elisabeth Manca
Hervé Schauer

- 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

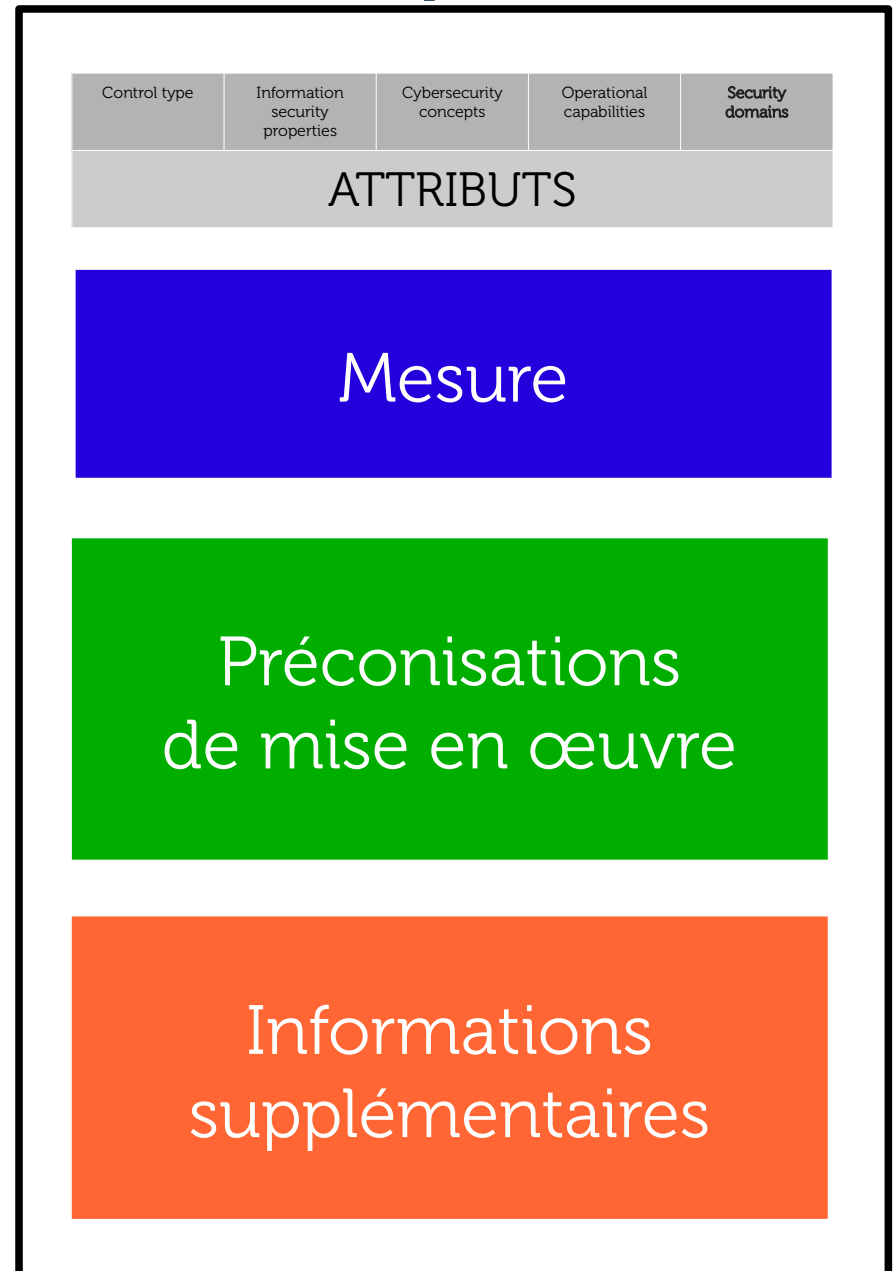
- ISO/IEC 27002:2022
 - *Information security, cybersecurity and privacy protection – Information security controls*
 - Rappels de la version 27002:2013 : *Code of practice for information security controls*
 - *Volumétrie*
 - *Nombre total de pages : 164*
 - *Notes préliminaires, vocabulaires et bibliographie*
 - → *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*

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*)



- 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



- 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

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

- 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

- 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.

- 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

- 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

- 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

5	Organizational controls	9
5.1	Policies for information security	9
5.2	Information security roles and responsibilities	11
5.3	Segregation of duties	12
5.4	Management responsibilities	13
5.5	Contact with authorities	14
5.6	Contact with special interest groups	15
5.7	Threat intelligence	15
5.8	Information security in project management	17
5.9	Inventory of information and other associated assets	18
5.10	Acceptable use of information and other associated assets	20
5.11	Return of assets	21
5.12	Classification of information	22
5.13	Labelling of information	23
5.14	Information transfer	24
5.15	Access control	27
5.16	Identity management	29
5.17	Authentication information	30
5.18	Access rights	32
5.19	Information security in supplier relationships	33
5.20	Addressing information security within supplier agreements	35
5.21	Managing information security in the ICT supply chain	37
5.22	Monitoring, review and change management of supplier services	39
5.23	Information security for use of cloud services	41
5.24	Information security incident management planning and preparation	43
5.25	Assessment and decision on information security events	44
5.26	Response to information security incidents	45
5.27	Learning from information security incidents	46
5.28	Collection of evidence	46
5.29	Information security during disruption	48
5.30	ICT readiness for business continuity	48
5.31	Legal, statutory, regulatory and contractual requirements	50
5.32	Intellectual property rights	51
5.33	Protection of records	53
5.34	Privacy and protection of PII	54
5.35	Independent review of information security	55
5.36	Compliance with policies, rules and standards for information security	56
5.37	Documented operating procedures	57

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



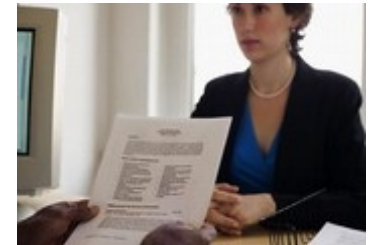
- *Fusion 5.1.1 et 5.1.2*
- Définir, Formaliser, approuver, publier, communiquer et réviser :
- Ensemble de politiques de sécurité :
 - Prennent en compte la stratégie, les exigences légales et contractuelles, les menaces
 - Contiennent la définition de la sécurité de l'information, les objectifs et 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 malveillants, 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



- 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 sécurité 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)

6	People controls	58
6.1	Screening.....	58
6.2	Terms and conditions of employment.....	59
6.3	Information security awareness, education and training.....	60
6.4	Disciplinary process.....	62
6.5	Responsibilities after termination or change of employment.....	63
6.6	Confidentiality or non-disclosure agreements.....	63
6.7	Remote working.....	65
6.8	Information security event reporting.....	66

- 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 événements de sécurité (intègre les failles) (6.8 ex 16.1.2 & 16.1.3)



7	Physical controls	67
7.1	Physical security perimeters.....	67
7.2	Physical entry.....	68
7.3	Securing offices, rooms and facilities.....	70
7.4	Physical security monitoring.....	70
7.5	Protecting against physical and environmental threats.....	71
7.6	Working in secure areas.....	72
7.7	Clear desk and clear screen.....	73
7.8	Equipment siting and protection.....	74
7.9	Security of assets off-premises.....	75
7.10	Storage media.....	76
7.11	Supporting utilities.....	77
7.12	Cabling security.....	78
7.13	Equipment maintenance.....	79
7.14	Secure disposal or re-use of equipment.....	80

- 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 & équipements (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 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)



8	Technological controls	81
8.1	User endpoint devices	81
8.2	Privileged access rights	83
8.3	Information access restriction	84
8.4	Access to source code	86
8.5	Secure authentication	87
8.6	Capacity management	89
8.7	Protection against malware	90
8.8	Management of technical vulnerabilities	92
8.9	Configuration management	95
8.10	Information deletion	97
8.11	Data masking	98
8.12	Data leakage prevention	100
8.13	Information backup	101
8.14	Redundancy of information processing facilities	102
8.15	Logging	103
8.16	Monitoring activities	106
8.17	Clock synchronization	108
8.18	Use of privileged utility programs	109
8.19	Installation of software on operational systems	110
8.20	Networks security	111
8.21	Security of network services	112
8.22	Segregation of networks	113
8.23	Web filtering	114
8.24	Use of cryptography	115
8.25	Secure development life cycle	117
8.26	Application security requirements	118
8.27	Secure system architecture and engineering principles	120
8.28	Secure coding	122
8.29	Security testing in development and acceptance	124
8.30	Outsourced development	126
8.31	Separation of development, test and production environments	127
8.32	Change management	128
8.33	Test information	129
8.34	Protection of information systems during audit testing	130

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)



- 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...)