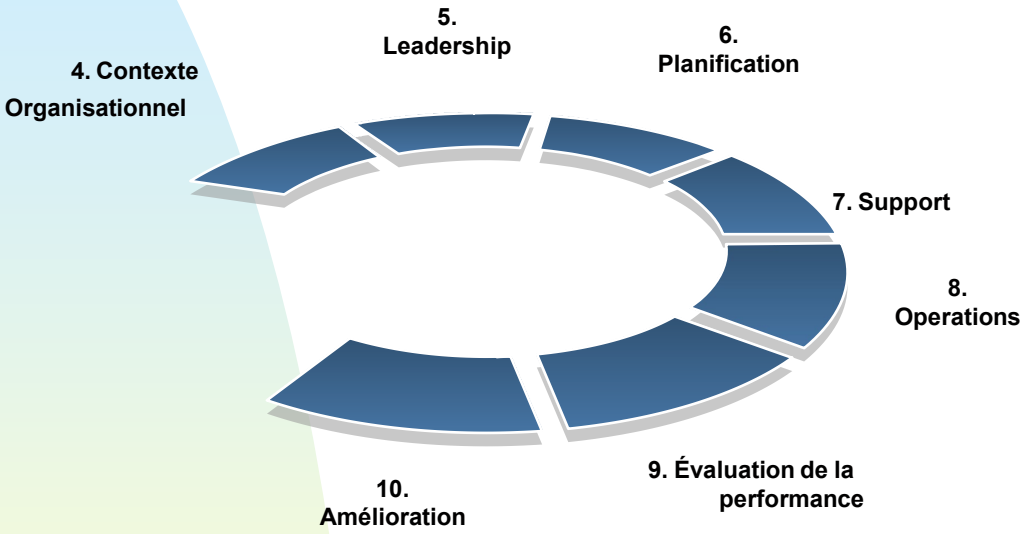
Le SMSi selon le standard ISO 27001

Par :
Nadir Kara Mostefa
Consultant Senior MEDCS

Structure de la Norme ISO 27001 : 2022

Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information - Exigences



Structure

Chapitre 4 – Contexte de l'organisation
- Comprehension de l'organisme, besoins des parties intéressées, domaine d'application

Chapitre 5 – Leadership
- Engagement de la Direction Générale
- Politique
- Responsabilités et autorités vis-à-vis du SMSI

Chapitre 6 – Planification -
- Planification des actions pour la maitrise des risques
- Objectifs et planning pour les atteindre

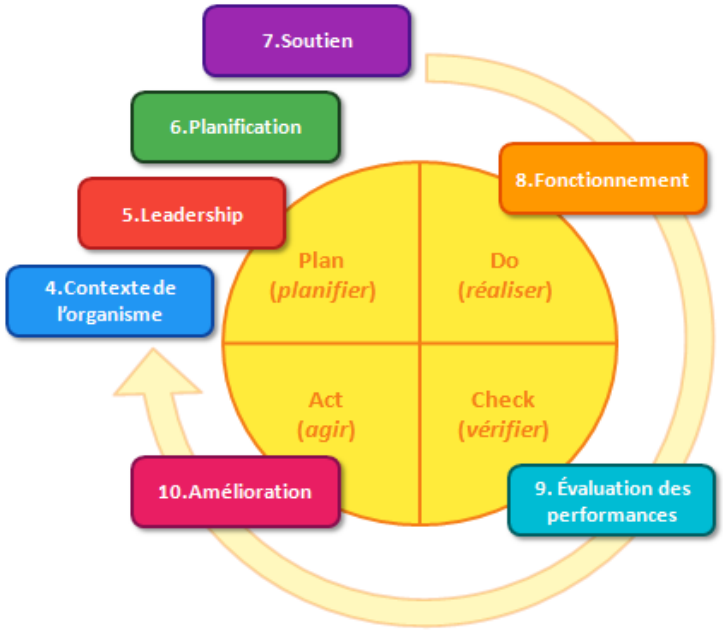
Chapitre 7 – Support
- Ressources humaines et compétence,
- Sensibilisation et Communication (interne & externe),
- Gestion de la documentation

Chapitre 8 – Operations
- Planning opérationnel
- Appréciation et traitement des risques

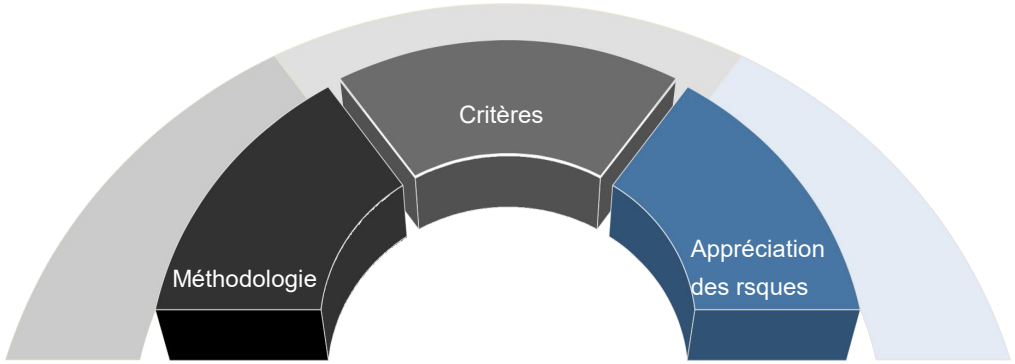
Chapitre 9 – Évaluation des performances
- Surveillance, Mesures, analyse et évaluation
- Audit interne,
- Revue de direction,

Chapitre 10 – Amélioration
- Amélioration continue
- Traitement des non-conformités et Actions correctives,

Structure de la Norme 27001 (PDCA)



La gestion des risques



Focus : ISO 27002 (Annexe A) : 2022 → Principaux changements

Nombre de contrôles

La version révisée de l'ISO 27002 publiée en 2022 fait passer le nombre de contrôles de sécurité de l'information de **114 contrôles à 93** contrôles, couverts en quatre sections :

- #37 Contrôles organisationnels (article 5) → (Politique, roles, gestion des actifs, classification, contrôle d'acces, vie privée, etc..)
- #8 Contrôles des personnes (article 6) → (Screening, sensibilisation, travail à distance, etc…)
- #14 Contrôles physiques (article 7) → (Bureau propre, périmètre de sécurité physique, accès physique, réutilisation des equipments, etc..
- #34 Contrôles technologiques (article 8) → (Droit d'acces, Suppression des données, gestion des configurations, prevention des fuites, etc…)

Nouveaux contrôles

L'ISO 27002:2022 a introduit 11 nouveaux contrôles, comme indiqué ci-dessous :

- 5.7 Renseignements sur les menaces
- 5.23 Sécurité des informations pour l'utilisation des services cloud
- 5.30 Préparation des TIC pour la continuité des activités
- 7.4 Surveillance de la sécurité physique
- 8.9 Gestion des configurations
- 8.10 Suppression des informations
- 8.11 Masquage des données
- 8.12 Prévention de fuite de données
- 8.16 Activités de surveillance
- 8.23 Filtrage Web
- 8.28 Codage sécurisé

Focus : ISO 27002 (Annexe A) : 2022

Chaque contrôle est caractérisé par 5 attributs regroupés au niveau de la table suivante

Type de contrôle	Propriété	Concept de cyber sécurité	Capacités opérationnelles	Domaine de sécurité

Type de contrôle	# Préventif | # Défectif | #Correctif
Propriété	#Confidentialité | #Intégrité | #Disponibilité
Concept de cybersécurité	(#Identifier, #Protéger, #Détecter, #Répondre, #Récupérer)
Capacités opérationnelles	#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 #Information_security_assurance
Domaine de sécurité	#Governance_and_Ecosystem #Protection #Defence #Resilience

Exemples

	Type de contrôle	Propriété	Concept de cyber sécurité	Capacités opérationnelles	Domaine de sécurité
Séparation des taches	#Préventif	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gouvernance	#Gouvernance_et_éco Système
Journalisation	#Détectif	#Confidentialité #Intégrité #Disponibilité	#Detection	#Gestion_des_événements_de_sécurité_de_l'information	#Protection #Défense
Sauvegarde	#Correctif	#Intégrité #Disponibilité	#Récupération	#Continuité	#Protection

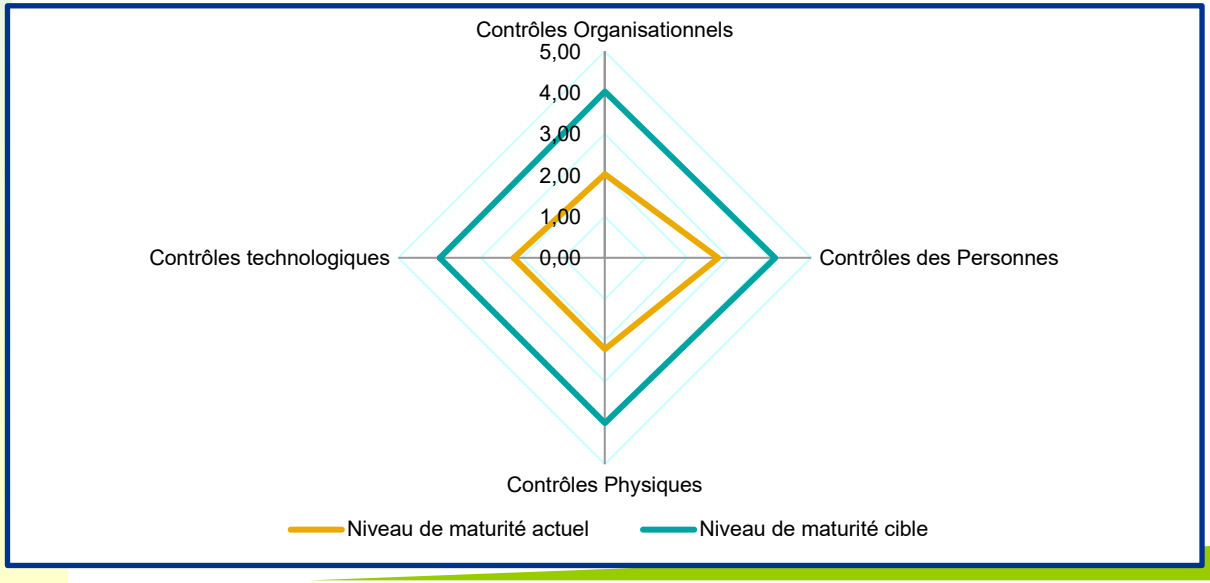
Focus : Définition du niveau de chaque mesure

Niveau	
0 Inexistant	Processus non identifié
1 Initial	Processus Identifié mais non appliqué
2 Géré	Processus Identifié, non standard en place
3 Défini	Processus Identifié, appliqué, documenté et communiqués
4 Géré quantitativement	Processus Identifié, appliqué, documenté, surveillés et mesurés
5 Optimisé	Processus Identifié, appliqué, documenté, surveillés, amélioré en continu

Exemple : Politique de sécurité de l'information

0 Inexistant	Absence de processus de sensibilisation du personnel
1 Initial	Conscience de la nécessité de mise en œuvre la sensibilisation du personnel
2 Géré	Un processus non standard est en place et non validé
3 Défini	Le processu est documenté, validée et communiqué
4 Géré quantitativement	La sensibilisation est mesurée et surveillée
5 Optimisé	La sensibilisation est continuellement ameliorée

Exemple de niveau de maturité global dans une entreprise



Quels avantages pour mon entreprise

Avantages

1. Amélioration de la sécurité
2. Bonne Gouvernance
3. Conformité
4. Réduction des coûts
5. Renforcement de la confiance des clients

Questions

Nous contacter

Nadir Kara
Consultant Senior

Mediterranean IT Consulting & Services (MEDCS)

info@medcs.net