



Agenda du 22 novembre 2022

ISO27x : se mettre à jour sur les bonnes versions

15'

Présentation des travaux du GT 27002:2022

30'





ISO27x : se mettre à jour sur les bonnes versions

Elisabeth Manca & William Bourgeois

ISO27x : se mettre à jour sur les bonnes versions



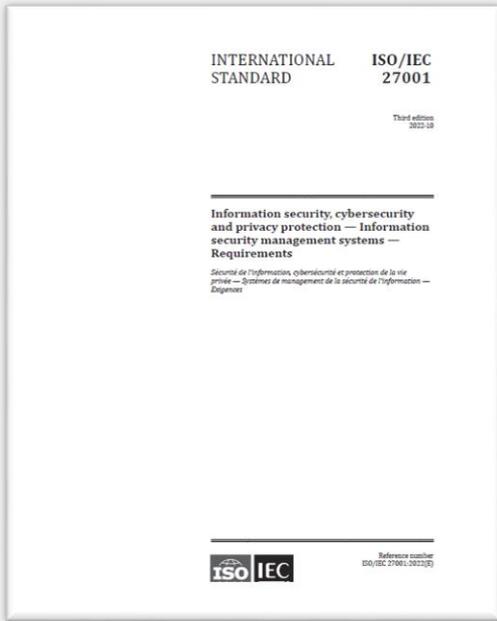
2022 : l'année de toutes les mises à jour

Février : ISO27002:2022 version anglaise
(Information security, cybersecurity and privacy protection — Information security controls)



Octobre

ISO27001:2022 version anglaise
(Information security, cybersecurity and privacy protection — Information security management systems — Requirements)



ISO27005:2022 version anglaise & française
(Information security, cybersecurity and privacy protection — Guidance on managing information security risks)



ISO27x : se mettre à jour sur les bonnes versions



Et les autres normes ?

- **ISO/IEC 27006:2015/Amd 1:2020** → remplacée par ISO/IEC 27006-1
 - Avis à commentaire a eu lieu en août 2022
- **ISO/IEC CD 27006-2.2** → audit pour la certification d'un PIMS, mise au vote du Comité le 18 Novembre 2022
- **ISO/IEC 27701:2019** → en phase d'enquête depuis le 27 octobre 2022
- **ISO/IEC 27017:2015** → mise à l'étude du projet de travail depuis le 26 octobre 2022
- **ISO/IEC PWI 27028** → futur guide sur l'utilisation des TAGS (draft)

ISO27x : se mettre à jour sur les bonnes versions



Et les versions françaises ?

- 27001:2022 Fr : avis à commentaire en octobre 2022

« Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27001:2013) qui a été amendée pour s'aligner sur l'ISO/IEC 27002:2022. Elle contient également les rectificatifs techniques ISO/IEC 27001:2013/COR 1:2014, ISO/IEC 27001:2013/COR 2:2015. »

- Pourquoi les normes en français sont si longues à être publiées ?

- La législation Européenne interdit la publication de norme NF tant que la norme Européenne CEN est en cours d'instruction

- La norme ISO 27002:2022 en français n'est donc pas encore publiée !

CLUB
27001



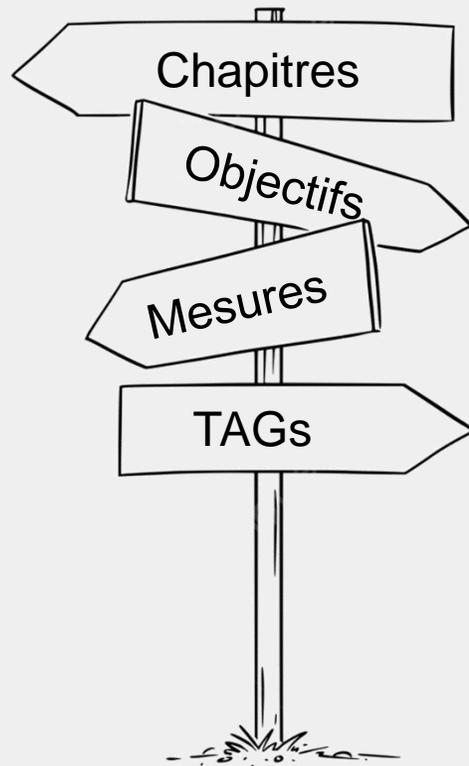
Présentation des travaux du GT 27002:2022

Emmanuel Petit & Jean-Christophe Touvet

Présentation des travaux du GT 27002:2022



Rappels des objectifs du groupe de travail



Source : pngtree.com



Quels sont les principaux changements apportés par la norme ?



Comment exploiter/utiliser les TAGS avec la nouvelle version ?



Comment utiliser cette nouvelle version ?
Quick Win, évolution, etc.

Présentation des travaux du GT 27002:2022



Axes d'analyse du groupe de travail

15 « Operational Capabilities »

Governance	Asset management	Information protection	Human resource security	Physical security	System and network security	Application security	Secure configuration
8 mesures identifiées	16 mesures identifiées	15 mesures identifiées	6 mesures identifiées	16 mesures identifiées	17 mesures identifiées	11 mesures identifiées	6 mesures identifiées
Identity and access management	Threat and vulnerability management	Continuity	Supplier relationships security	Legal and compliance	Information security event management	Information security assurance	
11 mesures identifiées	3 mesures identifiées	6 mesures identifiées	7 mesures identifiées	6 mesures identifiées	10 mesures identifiées	3 mesures identifiées	

Concept de TAGs

Redondances des mesures dans les TAGs

Rassemblement des mesures sous 4 chapitres – nouveaux libellés

Evolution/Fusion/Nouvelles mesures

5 « Cybersecurity concepts »

NIST

Identify	Protect	Detect	Respond	Recover
22 mesures identifiées	71 mesures identifiées	14 mesures identifiées	11 mesures identifiées	8 mesures identifiées

4 « Security domains »

enisa

Governance and Ecosystem	Protection	Defence	Resilience
27 mesures identifiées	69 mesures identifiées	22 mesures identifiées	8 mesures identifiées

Présentation des travaux du GT 27002:2022



Création d'un Tag par le Club 27001

TAG 'operational capabilities' (x15)

Governance	Asset management	Information protection	Human resource security	Physical security	System and network security	Application security	Secure configuration
8 mesures identifiées	16 mesures identifiées	15 mesures identifiées	6 mesures identifiées	16 mesures identifiées	17 mesures identifiées	11 mesures identifiées	6 mesures identifiées
Identity and access management	Threat and vulnerability management	Continuity	Supplier relationships security	Legal and compliance	Information security event management	Information security assurance	
11 mesures identifiées	3 mesures identifiées	6 mesures identifiées	7 mesures identifiées	6 mesures identifiées	10 mesures identifiées	3 mesures identifiées	

5 « Cybersecurity concepts »

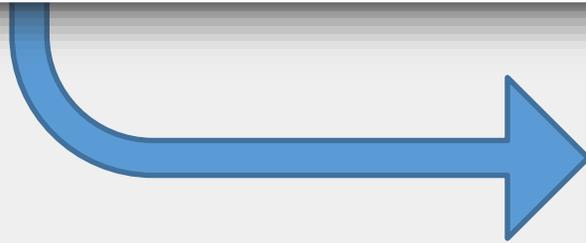
NIST

Identify	Protect	Detect	Respond	Recover
22 mesures identifiées	71 mesures identifiées	14 mesures identifiées	11 mesures identifiées	8 mesures identifiées

4 « Security domains »

enisa

Governance and Ecosystem	Protection	Defence	Resilience
27 mesures identifiées	69 mesures identifiées	22 mesures identifiées	8 mesures identifiées



'ACTIVITÉS' (x14) New tag proposé par le Club



Présentation des travaux du GT 27002:2022



Création d'un Tag par le Club 27001



14 « Activités »

Gouvernance	Gestion des actifs	Protection des informations	Ressources Humaines	Protection physique	Sécurité système et réseau	Protection des applications
7 MESURES	7 MESURES	11 MESURES	6 MESURES	9 MESURES	7 MESURES	9 MESURES
Durcissement des configurations	Gestion des identités et des accès	Gestion des menaces et des vulnérabilités	Continuité	Relations fournisseurs	Conformité	Gestion des événements et incidents
3 MESURES	7 MESURES	2 MESURES	6 MESURES	5 MESURES	5 MESURES	9 MESURES

Présentation des travaux du GT 27002:2022



Apport du groupe de travail

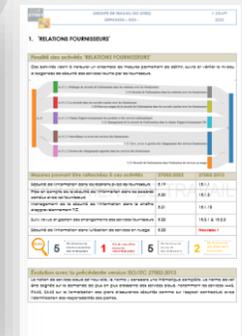
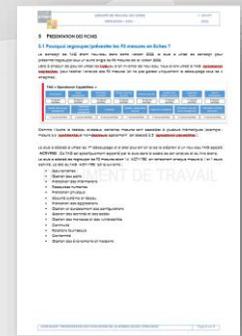


Source : pngtree.com



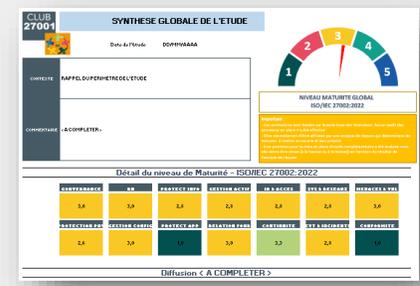
~20 contributeurs

1 livre blanc



6 fiches d'analyse

1 outillage





Focus sur le livre blanc

Partie 1 du livrable : Découverte de la norme

Présentation globale de l'ISO 27002

Partie 2 du livrable : Focus changements

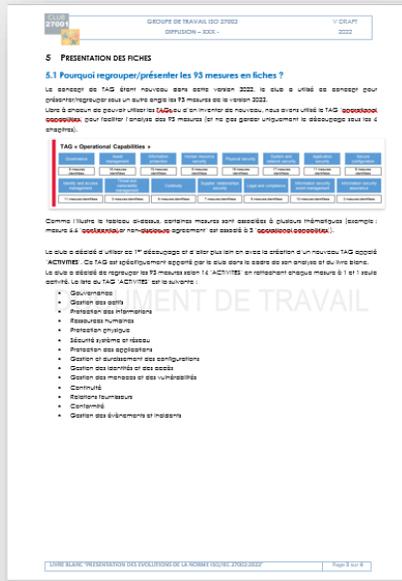
Focus sur ce qui a changé avec version 2022 et introduction des tags

Partie 3 du livrable : Quick wins & axes prioritaires

Sous un angle 'lead implementor', focus sur quelques mesures et quick win associé

Partie 4 du livrable : Impact / use cases

Retour de Use case ou d'exemples concrets (angle 'lead implementor')





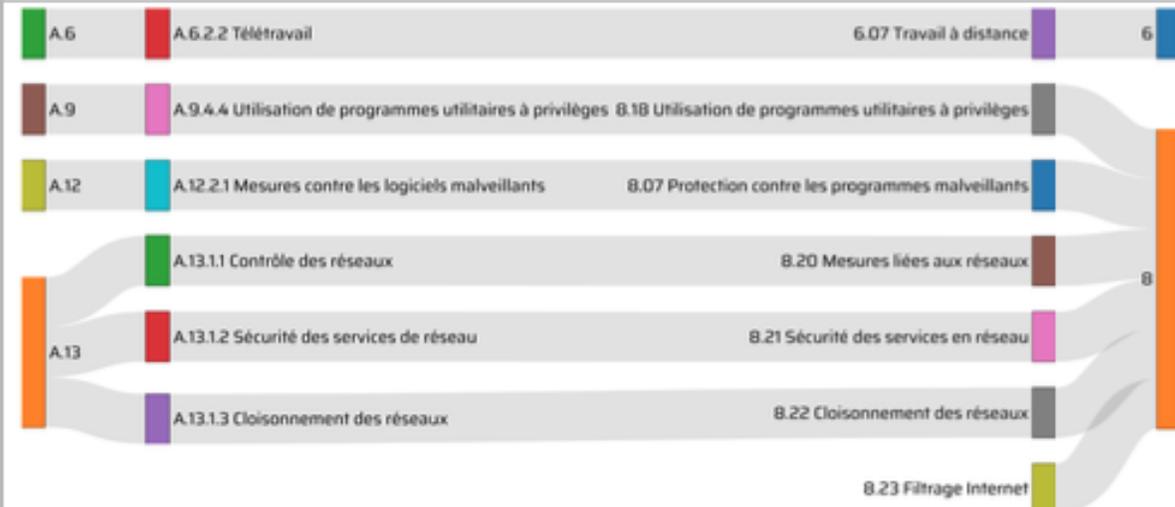
Focus sur les fiches d'analyse

1. 'SÉCURITÉ SYSTÈME ET RÉSEAU'

Finalité des activités 'SÉCURITÉ SYSTÈME ET RÉSEAU'

Ces activités visent à protéger l'information dans les réseaux et les infrastructures ("facilities") supportant l'information contre les compromissions à distance.

Le nouveau processus intègre la finalité expresse de réduire l'exposition aux contenus malveillants via le web en s'appuyant sur des mesures techniques et organisationnelles ou liées aux personnes.



Mesures pouvant être rattachées à ces activités	27002:2022	27002:2013
Cloisonnement des réseaux	8.22	13.1.3
Filtrage Internet	8.23	Nouveau !
Mesures liées aux réseaux	8.20	13.1.1
Protection contre les programmes malveillants	8.07	12.2.1
Sécurité des services en réseau	8.21	13.1.2
Travail à distance	6.07	06.2.2
Utilisation de programmes utilitaires à privilèges	8.18	09.4.4



7

Nb de mesures
totales associées
ISO 27002:2022

1

Nb de nouvelles
mesures
ISO 27002:2022

6

Nb de mesures
issues de
ISO 27002:2013

0

Nb de mesures
ISO 27001:2013
fusionnées

Référentiels

- ANSSI – GUIDE D'HYGIÈNE INFORMATIQUE
<https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>
- ANSSI – RECOMMANDATIONS SUR LE NOMADISME NUMÉRIQUE
<https://www.ssi.gouv.fr/administration/guide/recommandations-sur-le-nomadisme-numerique/>
- ANSSI – GUIDE D'ÉLABORATION D'UNE CHARTE D'UTILISATION DES MOYENS INFORMATIQUES ET DES OUTILS NUMÉRIQUES
<https://www.ssi.gouv.fr/administration/guide/guide-delaboration-dune-charte-dutilisation-des-moyens-informatiques-et-des-outils-numeriques/>



Focus sur les fiches d'analyse

Finalité de la mesure '8.23 – Filtrage Internet'

Il convient de gérer l'accès aux sites Web externes pour réduire l'exposition à tout contenu malveillant

Control Type	Information security	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
Responsable(s) (acteur/porteur)		RSSI, SEC OP		

Vision du club 27001 concernant la mesure 8.23

Nouveau !

Au-delà des aspects purement techniques (nécessité d'une politique et d'outils de filtrage de sites Internet malveillants, en lien avec la mesure 5.7 « intelligence des menaces »), cette mesure couvre des aspects d'organisation et de sensibilisation/formation du personnel à une utilisation sûre d'Internet.

Même si ce n'est pas exigé dans la norme, la signature d'une charte d'utilisation des ressources en ligne par le personnel nous semble constituer une bonne pratique dans le cadre de la mise en place de cette mesure.

La sensibilisation du personnel doit inclure une information sur la conduite à tenir en cas de survenance d'une alerte ou d'un incident de sécurité (coordonnées du point de contact notamment).

Indice de difficulté global de la mesure

★★★★

Gouvernance sécurité	Aspect contractuel et juridique	Management du risque
★★★★	★★★★	★★★★
Expertise technique	Exploitation	Surveillance et revue
★★★★	★★★★	★★★★

Exemples d'actions de mise en œuvre (Vision 'Lead implementer')

- Définition et tenue à jour d'une politique de filtrage des sites malveillants, tenant compte éventuellement des catégories de personnel
- Formalisation de cette politique dans une charte de bon usage des ressources en ligne et annexion de celle-ci au contrat de travail du personnel
- Mise en place d'outils de filtrage adéquats, se mettant automatiquement à jour en fonction de l'évolution des menaces et/ou de la réputation des sites (filtrage DNS)
- Organisation de campagnes régulières d'information/sensibilisation/formation du personnel

Exemple d'éléments de preuves (Vision 'Lead auditor')

- Charte d'utilisation du réseau Internet
- Règles de filtrage de contenu / sites malveillants
- Programme de sensibilisation et indicateurs de couverture de l'effectif, supports de campagnes de communication, résultats de tests de phishing et « sites web malveillants » etc.

Proposition par le Club 27001 qui n'engage que le Club (dépend évidemment de la maturité de l'organisation)

Échelle de 1 à 4 sous l'angle lead implementeur



Focus sur l'outillage

Évaluation de la maturité
En lien avec le nouveau TAG 'ACTIVITÉS' proposé par le Club

Également un outil pour les auditeurs
Exemples de questions à poser et de preuves à obtenir pour chaque mesure

CLUB 27001

SYNTHESE GLOBALE DE L'ETUDE

Date de l'étude DD/MM/AAAA

NIVEAU MATURETE GLOBAL ISO/IEC 27002:2022

Important :

- Ces estimations sont basées sur la seule base des interviews. Aucun audit des processus en place n'a été effectué
- Elles nécessiteront d'être affinées par une analyse de risques qui déterminera les mesures à mettre en oeuvre et leur priorité
- Une provision pour la mise en place d'outils complémentaire a été évaluée mais elle devra être revue (à la hausse ou à la baisse) en fonction du résultat de l'analyse de risques

CONTEXTE RAPPEL DU PERIMETRE DE L'ETUDE

COMMENTAIRE < A COMPLETER >

Détail du niveau de Maturité - ISO/IEC 27002:2022

GOUVERNANCE	RH	PROTECT INFO	GESTION ACTIF	ID & ACCES	SYS & RESEAUX	MENACES & VUL
3,0	3,0	2,8	2,8	2,8	2,8	3,0
PROTECTION PHY	GESTION CONFIG	PROTECT APP	RELATION FOUR	CONTINUITE	EVT & INCIDENTS	CONFORMITE
2,6	3,0	1,0	3,0	3,3	2,8	1,0

1- CONTEXTE

2- MESURES

3- GRAPH_v2022

4- TAG_v2022

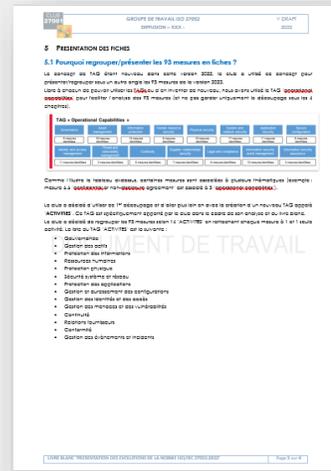
5- RESTITUTION

Diffusion < A COMPLETER >

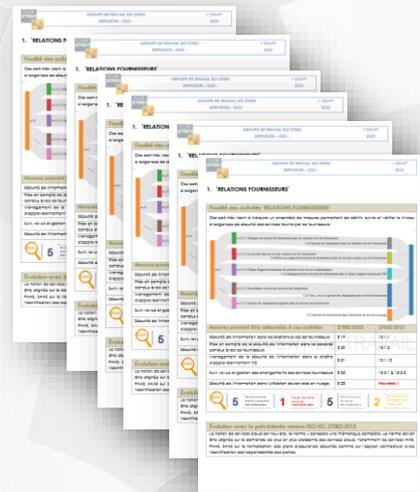
Présentation des travaux du GT 27002:2022



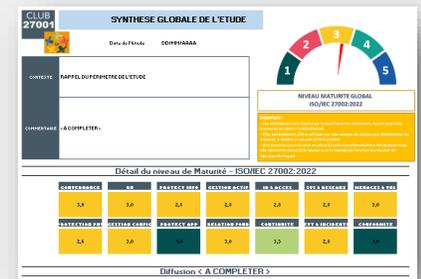
Disponible à partir de mi-décembre 2022



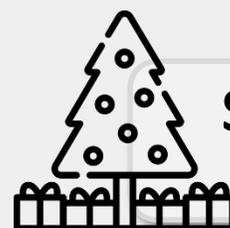
1 livre blanc



6 fiches d'analyse



1 tableur dédié



**Synthèse publiée sur
le site du club**



**Publication sur le site du club
réservée aux membres**

Présentation des travaux du GT 27002:2022



Pour 2023...

Fiches d'analyse supplémentaires

Déclaration D'Applicabilité au format 2022

Appel aux contributeurs



CLUB
27001



MERCI



GROUPE TRAVAIL ISO 27002



Modélisation des fiches descriptives

ISO 27002:2022

TAG 'operational capabilities' (x15)

- #Governance
- #Asset_management
- #Information_protection
- #Human_ressource_security
- #Physical security
- #System_&_network_security
- #Application_security
- #Secure_configuration
- #Identity_&_Access_mgt
- #Threat_&_vuln_mgt
- #Continuity
- #Supplier_relationship
- #Legal_&_compliance
- #Information_securit_event_mgt
- #Information_security_assurance

'ACTIVITÉS' (x14)

New tag proposé par le Club

Activités	Nb mesures	Nb NEW mesures
Gouvernance	7	/
Gestion des actifs	7	/
Protection des informations	11	3
Ressources humaines	6	/
Protection physique	9	1
Sécurité système et réseau	7	1
Protection des applications	9	1
Gestion et durcissement des configurations	3	1
Gestion des identités et des accès	7	/
Gestion des menaces et des vulnérabilités	2	1
Continuité	6	1
Relations fournisseurs	5	1
Conformité	5	/
Gestion des évènements et incidents	9	1