CLUSIR

#Nouvelle-Aquitaine

Afterwork mars 2022

Les nouveautés de l'ISO 27002 dans sa version 2022 & rappel sur les basiques du développement sécurisé

CLUSIR #Aquitaine

Club de la Sécurité Informatique Régionale d'Aquitaine

Afterwork du 24 mars 2022

 # Norme ISO/IEC 27002:2022-02

Son évolution de la norme et la suite pour l'ISO 27001

Par Michaël CATROUX – Consultant cybersécurité Thales

CLUSIR
#Aquitaine

L'approche du cadre cybersécurité « Cybersecurity framework »

CLUSIR #Aquitaine

Cybersecurity framework

- Le cadre de cybersécurité est une approche structurelle par concepts de sécurité. Il est propre à chaque organisation. Il prend en compte les besoins des parties prenantes, est flexible et interopérable.
- Pas obligatoire dans le cadre d'un SMSI mais recommandé pour la montée en maturité de l'entité.
- L'ISO propose l'ISO/IEC TS 27110:2021. Il existe également le NIST CSF (beaucoup plus complet).

NIST CSF

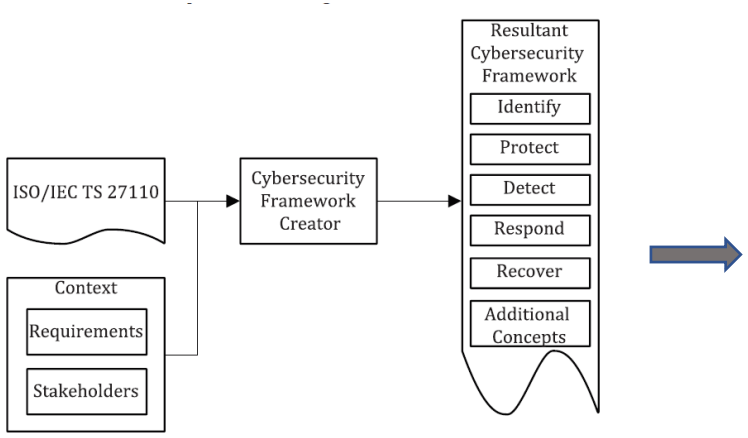


Figure 1 — Creating a cybersecurity framework using ISO/IEC TS 27110

Table A.2 — Example categories and references within Protect

Category	Description	References
Access control	Limiting access to facilities and assets to only authorized entities and associated activities. Included in access management is entity authentication	ISO/IEC 27002:2013, Clause 9 ISO/IEC 29146 ISO/IEC 29115
Awareness and training	Ensuring users and stakeholders are aware of policies, procedures, and responsibilities relating to cybersecurity responsibilities.	ISO/IEC 27002:2013, Clauses 6 and 7
Data security	Responsible for the confidentiality, integrity, and availability of data and information.	ISO/IEC 27002:2013, Clause 8
Information protection processes and procedures	Security policies, processes, and procedures are maintained and used to manage protection of information systems.	ISO/IEC 27002:2013
Maintenance	Processes and procedures for ongoing maintenance and modernization	ISO/IEC 27002:2013, Clause 11
Protective technology	Technical security solutions (such as logging, removable media, least access principles, and network protection)	ISO/IEC 27002:2013 ISO/IEC 27033 (all parts)

NIST CSF : National Institute of Standards and Technology Cybersecurity Framework

- Document élaboré initialement pour **améliorer la gestion des risques de cybersécurité** dans les infrastructures critiques (aux USA).
- Peut être utilisé par des organisations de n'importe quel secteur ou communauté.
- Permet **aux organisations, quels que soient leur taille**, leur degré de risque de cybersécurité ou de sophistication en matière de cybersécurité **d'appliquer les principes et les meilleures pratiques de gestion des risques** pour **améliorer la sécurité et la résilience**
- Le noyau (Core) : basé sur 5 « fonctions » : **Identify, Protect, Detect, Respond** and **Recover**

CLUSIR #Aquitaine

NIST CSF - Identificateurs uniques de fonction et de catégorie

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Identifiant unique de fonction	Fonction	Identifiant unique de catégorie	Catégorie
ID	Identifier	ID.AM	Gestion des actifs
		ID.BE	Environnement métier
		ID.GV	Gouvernance
		ID.RA	Appréciation des risques
		ID.RM	Stratégie de gestion des risques
		ID.SC	Gestion des risques de la chaîne d'approvisionnement
PR	Protéger	PR.AC	Gestion des identités et contrôle d'accès
		PR.AT	Sensibilisation et formation
		PR.DS	Sécurité des données
		PR.IP	Processus et procédures de protection des informations
		PR.MA	Maintenance
		PR.PT	Technologie de protection
DE	Détecter	DE.AE	Anomalies et événements
		DE.CM	Surveillance continue de la sécurité
		DE.DP	Processus de détection
RS	Répondre	RS.RP	Plan d'intervention
		RS.CO	Communications
		RS.AN	Analyse
		RS.MI	Atténuation
		RS.IM	Améliorations
RC	Rétablir	RC.RP	Planification de la récupération
		RC.IM	Améliorations
		RC.CO	Communications

Ci-contre : l'organisation du NIST CSF selon les 5 fonctions.

Désormais la nouvelle version de l'ISO 27002 *(historiquement très organisationnelle)* se rapproche beaucoup plus des mesures techniques et fonctions de résilience du NIST de part les concepts de cybersécurité…

CLUSIR #Aquitaine

Un extrait du NIST Framework Core

Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 fonctions — 23 catégories — 108 sous-catégories — 6 référentiels pour complements d'informations

CLUSIR #Aquitaine

Un extrait du NIST Control Catalog

Le document “Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53r5)” apporte des éléments de details sur les mesures de sécurité à mettre en oeuvre.

Extrait du “Control Catalog and Control Baselines in Spreadsheet Format”

PM-16	Threat Awareness Program	Implement a threat awareness program that includes a cross-organization information-sharing capability for	Because of the constantly changing and increasing sophistication of adversaries, especially the advanced	IR-4, PM-12.
PM-16(1)	Threat Awareness Program | Automated Means for Sharing Threat Intelligence	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.	To maximize the effectiveness of monitoring, it is important to know what threat observables and indicators the sensors need to be searching for. By using well-established frameworks, services, and automated tools, organizations improve their ability to rapidly share and feed the relevant threat detection signatures into monitoring tools.	None.

CLUSIR
#Aquitaine

La norme ISO/IEC 27002:2022-02

Publiée en février 2022

CLUSIR #Aquitaine

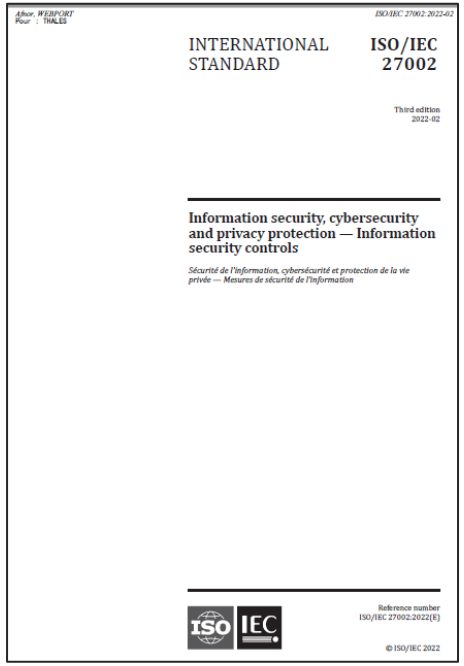
Troisième édition de la norme ISO 27002

On passe de 114 mesures* à 93 mesures *(controls en anglais)*

- *Un ensemble de mesures ont fusionnées*
- *11 nouvelles mesures apparaissent*

Regroupement des mesures dans 4 thèmes (catégories)

- Mesures organisationnelles
- Mesures liées aux personnes
- Contrôles Physiques
- Mesures technologique


INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition 2022-02

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Reference number ISO/IEC 27002:2022(E)

© ISO/IEC 2022

* Une mesure est une action destinée à modifier ou à gérer un risque

Attributs

A chaque mesure sont associés des attributs. Valeurs d'attributs correspondantes :

- **types** de mesures de sécurité
  - #Prévention, #Détection, #Correction ;
- **propriétés** de sécurité de l'information
  - #Confidentialité, #Intégrité, #Disponibilité
- **concepts** de cybersécurité
  - #Identification, #Protection, #Détection, #Traitement, #Récupération ;
  - concepts de cybersécurité tels que définis dans le cadre de cybersécurité décrit dans l'ISO/IEC 27110* mais très proches du NIST CSF

Framework Version 1.1

*ISO/IEC TS 27110:2021 : Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines
https://www.iso.org/obp/ui/#iso:std:iso-iec:ts:27110:ed-1:v1:en

Attributs (suite)

- **capacités** opérationnelles :
  - Les valeurs d'attributs correspondent à #Gouvernance, #Gestion_des_actifs, #Protection_des_informations, #Sécurité_des_ressources_humaines, #Sécurité_physique, #Sécurité_système_et_réseau, #Sécurité_des_applications, #Configuration_sécurisée, #Gestion_des_identités_et_des_accès, #Gestion_des_menaces_et_des_vulnérabilités, #Continuité, #Sécurité_des_relations_fournisseurs,v #Législation_et_conformité, #Gestion_des_événements_de_sécurité_de_l'information et #Assurance_de_sécurité_de_l'information
- **domaines** de sécurité :
  - #Gouvernance_et_écosystème,
  - #Protection,
  - #Défense,
  - #Résilience ;

Mesure de sécurité

Chaque mesure de sécurité comporte les informations suivantes:

- **titre de la mesure** : nom court de la mesure ;
- tableau d'**attributs** : tableau indiquant la ou les valeurs de chaque attribut pour la mesure concernée ;
- **mesure de sécurité** : description de la mesure ;
- **objet** : texte expliquant l'objet de la mesure ;
- **préconisations** : préconisations de mise en œuvre de la mesure ;
- **autres informations** : texte explicatif ou références aux autres documents connexes.

CLUSIR #Aquitaine

Exemple avec une mesure

5.15 Contrôle d'accès

Titre de la mesure

Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_identités_et_des_accès	#Protection

Tableau d'attributs

Mesure de sécurité

Mesure de sécurité

Il convient de définir et de mettre en œuvre des règles visant à gérer l'accès physique et logique à l'information et aux autres actifs associés en fonction des exigences métier et de sécurité de l'information.

Objectif

Objectif

Garantir l'accès par le biais d'autorisations et empêcher l'accès non autorisé à l'information et aux autres actifs associés.

Préconisations

Préconisations

Il convient que les propriétaires des informations et des autres actifs associés déterminent les exigences métier et de sécurité de l'information relatives au contrôle d'accès et qu'ils définissent une politique portant sur le thème du contrôle d'accès, puis qu'ils communiquent ces éléments à toutes les parties prenantes pertinentes, telles que les utilisateurs et les propriétaires de services.

Informations supplémentaires

Informations complémentaires

On a souvent recours à des principes globaux dans le contexte du contrôle d'accès. Les deux principes les plus couramment utilisés sont les suivants :

a) le besoin d'en connaître : une entité a uniquement accès à l'information dont elle a besoin pour réaliser les tâches qui lui incombent (différentes tâches ou fonctions impliquent des besoins d'en connaître différents, d'où des profils d'accès différents) ;

CLUSIR #Aquitaine

Matrice des mesures et valeurs d'attributs

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
5.1	Politiques de sécurité de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème #Résilience
5.2	Fonctions et responsabilités liées à la sécurité de l'information	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème #Protection #Résilience
5.3	Séparation des tâches	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gouvernance	#Gouvernance_et_écosystème
5.4	Responsabilités de la direction	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gouvernance	#Gouvernance_et_écosystème
5.5	Relations avec les autorités	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement #Récupération	#Gouvernance	#Défense #Résilience
5.6	Relations avec des groupes de travail spécialisés	#Prévention #Correction	#Confidentialité #Intégrité #Disponibilité	#Protection #Traitement #Récupération	#Gouvernance	#Défense
5.7	Intelligence des menaces	#Prévention #Détection	#Confidentialité #Intégrité #Disponibilité	#Identification #Détection	#Gestion_des_menaces_et_des_vulnérabilités	#Défense #Résilience
5.8	Sécurité de l'information dans la gestion de projet	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification #Protection	#Gouvernance	#Gouvernance_et_écosystème #Protection
5.9	Inventaire des informations et des autres actifs associés	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Identification	#Gestion_des_actifs	#Gouvernance_et_écosystème #Protection
5.10	Utilisation correcte de l'information et des actifs associés	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Gestion_des_actifs #Protection_des_informations	#Gouvernance_et_écosystème #Protection

Identifiant de mesure dans l'ISO/ IEC 27002	Nom de la mesure	Type de mesure de sécurité	Propriétés de sécurité de l'information	Concepts de cybersécurité	Capacités opérationnelles	Domaines de sécurité
8.20	Mesures liées aux réseaux	#Prévention #Détection	#Confidentialité #Intégrité #Disponibilité	#Protection #Détection	#Sécurité_système_et_réseau	#Protection
8.21	Sécurité des services en réseau	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection
8.22	Filtrage Internet	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection
8.23	Cloisonnement des réseaux	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_système_et_réseau	#Protection
8.24	Utilisation de la cryptographie	#Prévention	#Confidentialité #Intégrité	#Protection	#Configuration_sécurisée	#Protection
8.25	Cycle de vie de développement sécurisé	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection
8.26	Exigences de sécurité des applications	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection #Défense
8.27	Principes d'ingénierie et d'architecture système sécurisée	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection
8.28	Codage sécurisé	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Protection	#Sécurité_des_applications #Sécurité_système_et_réseau	#Protection
8.29	Tests de sécurité dans le développement et l'acceptation	#Prévention	#Confidentialité #Intégrité #Disponibilité	#Détection	#Sécurité_des_applications #Assurance_de_sécurité_de_l'information #Sécurité_système_et_réseau	#Protection

CLUSIR #Aquitaine

Tableau de correspondance - Exemple

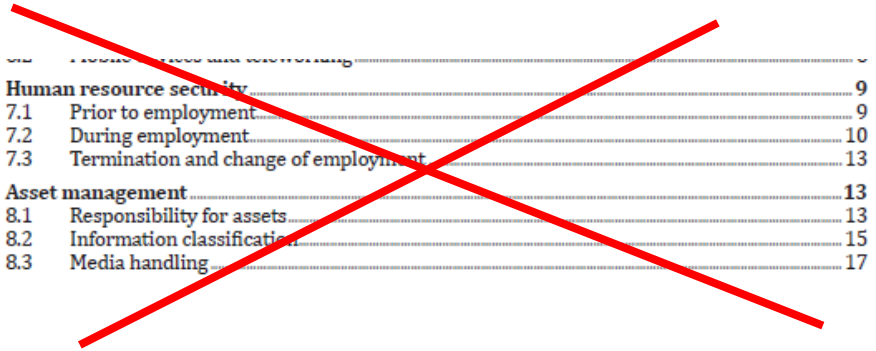
Identifiant de mesure dans l'ISO/IEC 27002	Identifiant de mesure dans l'ISO/IEC 27002:2013	Nom de la mesure
8.24	10.1.1, 10.1.2	Utilisation de la cryptographie
8.25	14.2.1	Cycle de vie de développement sécurisé
8.26	14.1.2, 14.1.3	Exigences de sécurité des applications
8.27	14.2.5	Principes d'ingénierie et d'architecture système sécurisée
8.28	Nouveau	Codage sécurisé
8.29	14.2.8, 14.2.9	Tests de sécurité dans le développement et l'acceptation
8.30	14.2.7	Développement externalisé
8.31	12.1.4, 14.2.6	Séparation des environnements de développement, de test et de production
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Gestion des changements
8.33	14.3.1	Informations relatives aux tests
8.34	12.7.1	Protection des systèmes d'information en cours d'audit et de test

CLUSIR #Aquitaine

Tableau de correspondance depuis l'ancienne version - Exemple

Identifiant de mesure dans l'ISO/ IEC 27002:2013	Identifiant de mesure dans l'ISO/IEC 27002	Nom de la mesure conformément à l'ISO/IEC 27002:2013
7		Sécurité des ressources humaines
7.1		Avant l'embauche
7.1.1	6.1	Présélection
7.1.2	6.2	Conditions générales d'embauche
7.2		Pendant la durée du contrat
7.2.1	5.4	Responsabilités de la direction
7.2.2	6.3	Sensibilisation, apprentissage et formation à la sécurité de l'information
7.2.3	6.4	Processus disciplinaire
7.3		Rupture, terme ou modification du contrat de travail
7.3.1	6.5	Achèvement ou modification des responsabilités associées au contrat de travail
8		Gestion des actifs
8.1		Responsabilités relatives aux actifs
8.1.1	5.9	Inventaire des actifs

On peut observer que les noms des chapitres, sous-chapitres de la précédente version de la norme disparaissent.



CLUSIR #Aquitaine

Les nouvelles mesures

- 5.7 Intelligence des menaces
- 5.23 Sécurité de l'information dans l'utilisation de services en nuage
- 5.30 Préparation des TIC pour la continuité d'activité
- 7.4 Surveillance de la sécurité physique
- 8.9 Gestion de la configuration
- 8.10 Suppression d'information
- 8.11 Masquage des données
- 8.12 Prévention de la fuite de données
- 8.16 Activités de surveillance
- 8.22 Filtrage Internet
- 8.28 Codage sécurisé

Suppression
- 11.2.5 Sortie des actifs

CLUSIR #Aquitaine

Les nouvelles mesures en détail

N° Section	Section	N° sous-section	Sous-section	Mesure en version 2022	Objectif en version 2022
5	Mesures organisationnelles	7	Intelligence des menaces	Il convient de recueillir les informations relatives aux menaces pour la sécurité de l'information et de les analyser pour produire une intelligence des menaces.	Apporter une connaissance de l'environnement de menaces susceptible d'affecter l'organisation pour que celle-ci puisse prendre les mesures d'atténuation appropriées.
5	Mesures organisationnelles	23	Sécurité de l'information dans l'utilisation de services en nuage	Il convient que les processus d'acquisition, d'utilisation, de management et de cessation des services en nuage soient définis conformément aux exigences de sécurité de l'information de l'organisation.	Spécifier et gérer la sécurité de l'information concernant l'utilisation des services en nuage.
5	Mesures organisationnelles	30	Préparation des TIC pour la continuité d'activité	Il convient de planifier, de mettre en oeuvre, de gérer et de tester la préparation des TIC en fonction des objectifs de continuité d'activité et des exigences de continuité des TIC.	Assurer la disponibilité de l'information et des autres actifs associés de l'organisation en cas de perturbation.
7	Mesures physiques	4	Surveillance de la sécurité physique	Il convient que les locaux fassent l'objet d'une surveillance continue concernant l'accès physique non autorisé.	Détecter et empêcher tout accès physique non autorisé.
8	Mesures technologiques	9	Gestion de la configuration	Il convient de définir, de documenter, de mettre en oeuvre, de surveiller et réviser les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux.	S'assurer du bon fonctionnement du matériel, des logiciels, des services et des réseaux avec les paramètres de sécurité requis, et du fait que la configuration ne soit pas altérée par des changements non autorisés ou incorrects.
8	Mesures technologiques	10	Suppression d'information	Il convient de supprimer l'information stockée dans les systèmes d'information et les dispositifs lorsqu'elle n'est plus utile.	Éviter l'exposition inutile d'information sensible et se conformer aux exigences légales, statutaires, réglementaires et contractuelles en matière de suppression de données.
8	Mesures technologiques	11	Masquage des données	Il convient d'utiliser le masquage des données conformément à la politique de l'organisation portant sur le thème du contrôle d'accès et aux exigences métier, tout en prenant en compte les exigences d'ordre légal.	Limiter l'exposition de données sensibles, notamment les données à caractère personnel, et se conformer aux exigences légales, statutaires, réglementaires et contractuelles.
8	Mesures technologiques	12	Prévention de la fuite de données	Il convient d'appliquer des mesures de prévention de la fuite de données aux systèmes, réseaux et terminaux qui traitent, stockent ou transmettent de l'information sensible.	Détecter et empêcher la divulgation et l'extraction non autorisées d'information par des personnes ou des systèmes.
8	Mesures technologiques	16	Activités de surveillance	Il convient de surveiller les réseaux, systèmes et applications pour détecter tout comportement anormal et de prendre les mesures appropriées pour évaluer les incidents liés à la sécurité de l'information potentiels.	Détecter les comportements anormaux et les incidents liés à la sécurité de l'information potentiels.
8	Mesures technologiques	22	Filtrage Internet	Il convient de gérer l'accès aux sites Web externes pour réduire l'exposition à tout contenu malveillant.	Protéger les systèmes de la compromission par des programmes malveillants et empêcher l'accès aux ressources Internet non autorisées.
8	Mesures technologiques	28	Codage sécurisé	Il convient d'appliquer des principes de codage sécurisé au développement de logiciels.	S'assurer que le logiciel est développé dans un souci de sécurité et réduire ainsi le nombre de vulnérabilités potentielles du logiciel en termes de sécurité de l'information.

CLUSIR
#Aquitaine

Évolution de l'ISO 27001

CLUSIR #Aquitaine

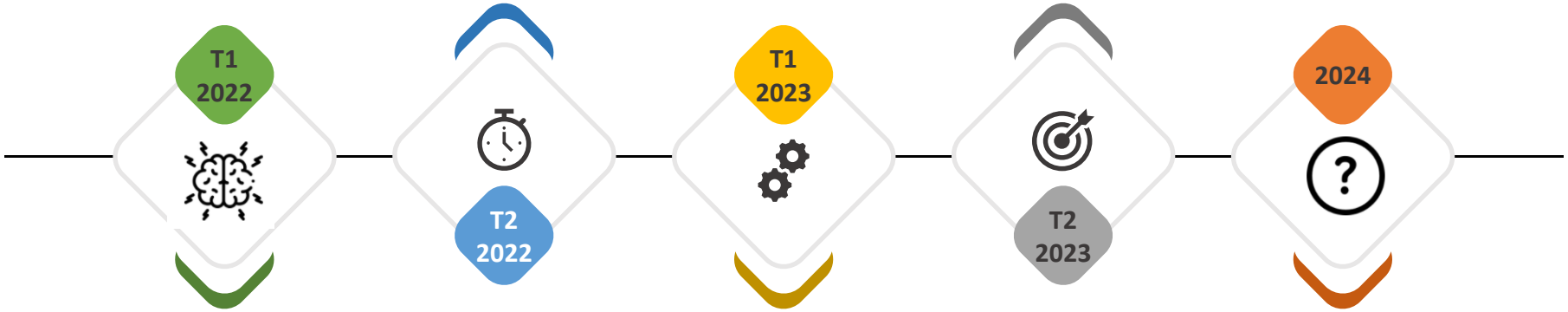
et la révision de l'ISO/IEC 27001:2013 dans l'histoire ?

amendement

Publication prévue au second semestre 2022 d'un amendement de l'ISO 27001 contenant seulement la nouvelle Annexe A afin de prendre en compte la révision de l'ISO 27002.

certificats

Les certificats émis selon l'ISO/IEC 27001:2013 devront être réémis sous la version 2017 avant le 31/12/2023.



évolution

Les travaux pour la révision complète vont démarrer en avril 2022 (groupe de travail SC 27/WG1).

sortie

On pourrait imaginer une sortie de la v3 à l'horizon 2024…

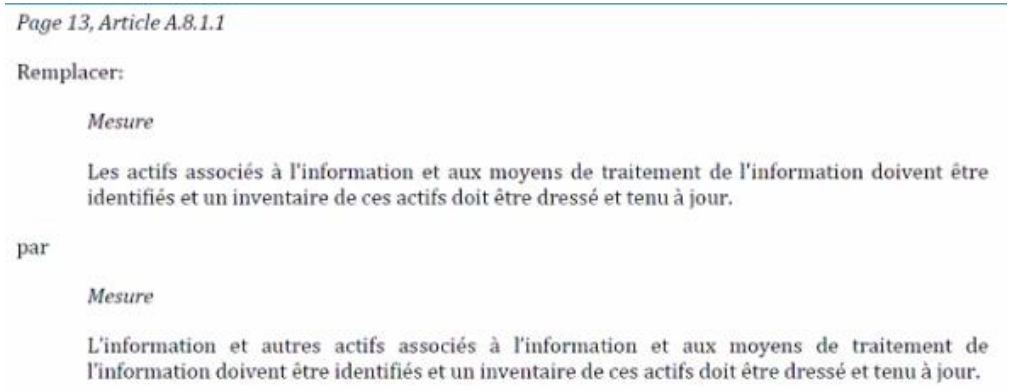
L'annexe A (NF EN ISO/IEC 27001:2017) reste obligatoire pour la certification.

CLUSIR #Aquitaine

Transition NF EN ISO/IEC 27001:2017

Rappel : l'évolution des deux rectificatifs sont très limités et peu impactant

- Rectificatif 1 : précision mineure de l'article A.8.1.1. Les informations doivent être inclues dans l'inventaire des actifs



Page 13, Article A.8.1.1

Remplacer:

Mesure

Les actifs associés à l'information et aux moyens de traitement de l'information doivent être identifiés et un inventaire de ces actifs doit être dressé et tenu à jour.

par

Mesure

L'information et autres actifs associés à l'information et aux moyens de traitement de l'information doivent être identifiés et un inventaire de ces actifs doit être dressé et tenu à jour.

- Rectificatif 2 : Mise en forme du texte (texte aéré, introduction de tirets)

CLUSIR
#Aquitaine

Ressources

CLUSIR #Aquitaine

Ressources et recommandations

- Norme ISO/IEC 27022:2022 : https://www.iso.org/standard/75652.html
- Site du NIST : https://www.nist.gov/cyberframework
- NIST en version française : https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018fr.pdf
- NIST Control Catalog : https://www.nist.gov/news-events/news/2021/01/nist-releases-supplemental-materials-sp-800-53-and-sp-800-53b-control
- Publication NIST par catégorie (fonction) : https://www.nist.gov/cyberframework/protect
- Secure Software Development Framework : https://www.nist.gov/publications/secure-software-development-framework-ssdf-version-11-recommendations-mitigating-risk
- OWASP Application Security Verification Standard : https://owasp.org/www-project-application-security-verification-standard/
- Outil de Niji : https://www.niji.fr/fr/actualite/decryptage/mise-%C3%A0-disposition-d%E2%80%99un-outil-pour-la-r%C3%A9vision-d%E2%80%99isoiec-27002-sign%C3%A9-imineti
- Accès aux standards disponibles publiquement : https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

CLUSIR #Aquitaine

Définitions

cybersécurité désigne les politiques, outils, méthodes de gestion des risques, bonnes pratiques de sécurité et technologies qui peuvent être utilisés pour protéger les personnes et les actifs des organisations contre toute atteinte à une perte de disponibilité, d'intégrité ou de confidentialité.

cyber-résilience souvent définie comme « la capacité attendue d'une entreprise (ou d'un individu) à identifier, prévenir, détecter et répondre aux défaillances technologiques ou de processus issues d'une attaque du cyberespace, et à se rétablir en réduisant au minimum les impacts négatifs pour ses activités, ses clients, ses préjudices en matière de réputation et ses pertes financières. »

Accès aux définitions de l'ISO 27000 : https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_F.zip

CLUSIR
#Aquitaine

MERCI DE VOTRE ATTENTION

CLUSIR #Aquitaine

Club de la Sécurité Informatique Régionale d'Aquitaine

Afterwork du 24 mars 2022

Rappel des basiques du développement sécurisé

Faire du développement Web sécurisé : protéger ses données et ses services

Par Stanislas GRANEL– Consultant cybersécurité Thales

CLUSIR #Aquitaine

SOMMAIRE

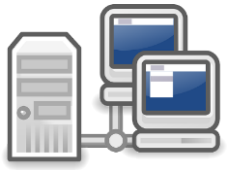
1. Les méthodes HTTP
2. Chiffrement ou hachage
3. Les librairies tierces

CLUSIR
#Aquitaine

Les méthodes HTTP

CLUSIR #Aquitaine

Les méthodes HTTP - rappel



Tout échange entre deux machines sur un réseau, reposant sur le protocole HTTP, est basé sur les méthodes.

Les différentes méthodes :

- GET
- POST
- PUT
- DELETE
- HEAD
- CONNECT
- OPTIONS
- TRACE
- PATCH

CLUSIR #Aquitaine

Les méthodes HTTP – rappel

GET et DELETE :

- Les valeurs sont dans l'url
- Interceptables même en HTTPS
- Loguées par défaut par les serveurs front (apache, nginx)

POST, PUT et PATCH:

- Les valeurs sont dans le content
- Non lisibles en HTTPS
- Contenu non logué par les serveurs front

Les méthodes HTTP – rappel

OPTIONS :

- Les valeurs sont dans l'url
- Interceptables même en HTTPS
- Requête de pré-vérification CORS
- Non logué par défaut

HEAD :

- Similaire au GET, mais ne renvoie que les en-têtes.
- Permet de vérifier si un élément en cache est encore valide

CLUSIR #Aquitaine

Les méthodes HTTP – rappel

TRACE :

- Utile au débuggage
- Envoie un message à un destinataire qui accuse réception de ce message.

CONNECT :

- Permet de créer une communication bidirectionnelle avec la machine demandée.
- Est utilisée pour le HTTPS

CLUSIR #Aquitaine

Les méthodes HTTP – rappel

Exemple de log apache

```
82.230.154.123 - - [10/Mar/2012:11:03:02 +0100] "GET /wiki/index.php/Sp%C3%A9cial:T%C3%A91%C3%A9verser HTTP/1.
82.230.154.123 - - [10/Mar/2012:11:03:08 +0100] "GET /wiki/index.php?action=ajax&rs=SpecialUpload%3A%3AajaxGet
82.230.154.123 - - [10/Mar/2012:11:03:24 +0100] "GET /wiki/index.php/Cat%C3%A9gorie:Awstats_Capture_Ecran HTTP
82.230.154.123 - - [10/Mar/2012:11:03:25 +0100] "GET /wiki/images/thumb/1/14/Awstats_hote_accueil.png/120px-Aw
82.230.154.123 - - [10/Mar/2012:11:03:30 +0100] "GET /wiki/index.php/Fichier:Awstats_hote_accueil.png HTTP/1.1
82.230.154.123 - - [10/Mar/2012:11:03:31 +0100] "GET /wiki/images/thumb/1/14/Awstats_hote_accueil.png/800px-Aw
82.230.154.123 - - [10/Mar/2012:11:03:33 +0100] "GET /wiki/index.php/Sp%C3%A9cial:Renommer_une_page/Fichier:Aw
82.230.154.123 - - [10/Mar/2012:11:03:40 +0100] "POST /wiki/index.php?title=Sp%C3%A9cial:Renommer_une_page&act
82.230.154.123 - - [10/Mar/2012:11:03:40 +0100] "GET /wiki/load.php?debug=false&lang=fr&modules=mediawiki.lega
82.230.154.123 - - [10/Mar/2012:11:03:40 +0100] "GET /wiki/load.php?debug=false&lang=fr&modules=site&only=styl
82.230.154.123 - - [10/Mar/2012:11:03:40 +0100] "GET /wiki/load.php?debug=false&lang=fr&modules=site&only=scri
82.230.154.123 - - [10/Mar/2012:11:03:40 +0100] "GET /wiki/load.php?debug=false&lang=fr&modules=startup&only=s
82.230.154.123 - - [10/Mar/2012:11:03:43 +0100] "GET /wiki/index.php?title=Fichier:Awstats_hote_accueil.png&re
82.230.154.123 - - [10/Mar/2012:11:03:46 +0100] "GET /wiki/index.php/Sp%C3%A9cial:Pages_li%C3%A9es/Fichier:Aws
82.230.154.123 - - [10/Mar/2012:11:03:52 +0100] "GET /wiki/index.php?title=Fichier:Awstats_hote_accueil.png&ac
82.230.154.123 - - [10/Mar/2012:11:03:54 +0100] "POST /wiki/index.php?title=Fichier:Awstats_hote_accueil.png&a
```

CLUSIR #Aquitaine

Les méthodes HTTP – quel usage?

GET :

- Pour récupérer de l'information

POST :

- Créer une nouvelle ressource ou la remplace de façon successive

PUT :

- Créer une nouvelle ressource ou la remplace de façon idempotente

Les méthodes HTTP – qui et quand ?

PATCH :

- Pour une modification partielle d'une ressource

DELETE :

- Pour supprimer une information

CLUSIR
#Aquitaine

Chiffrement ou hachage

CLUSIR #Aquitaine

Chiffrement ou hachage

Chiffrement :

- Permet de rendre illisible une information via une clef.
- Possibilité de revenir à la valeur initiale

Hachage :

- Pour une modification partielle d’une ressource
- Impossibilité de revenir à la valeur initiale
- Résultat de longueur fixe

CLUSIR #Aquitaine

Chiffrement

Un peu de vocabulaire :

- Chiffrement : action de rendre illisible un message via une clef de chiffrement
- Déchiffrement : action de rendre lisible un message via une clef de déchiffrement
- Décrypter : action de rendre lisible un message sans la clef
- Crypter : anglicisme. N'existe pas en cryptographie

CLUSIR #Aquitaine

Chiffrement

Symétrique :

- 1 seule clef pour chiffrer et déchiffrer
- Utile lorsque seul l'élément ayant chiffré a besoin d'accéder à la donnée
- Exemple : AES

image : Flaticon.com

CLUSIR #Aquitaine

Chiffrement

Asymétrique :

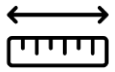
- 2 clefs : une pour le chiffrement, une pour le déchiffrement
- Utile lorsque la donnée doit être partagée avec une autre machine
- Exemple : RSA

image : Flaticon.com

CLUSIR #Aquitaine

Chiffrement

Problématiques : la clef



- Taille de la clef
  - 256 bits pour AES
  - 2048 bits pour RSA (jusqu'en 2030, 3072 bits à partir de 2031)

- Sa protection

image : Flaticon.com

CLUSIR #Aquitaine

Hachage

Les algorithmes :

- À partir de SHA-256
- Bcrypt

Taille minimale des empreintes : 256 bits

⚠ Résultat de taille fixe = risque de collision

image : Flaticon.com

Hachage

Utilisation d’un sel :

- Augmentation de l’entropie
- Empêche l’utilisation de rainbow tables
- Doit être unique par utilisateur.

CLUSIR
#Aquitaine

Les librairies tierces

CLUSIR #Aquitaine

Les librairies tierces

Indispensable mais ….

- Fiabilité ?

- Maintenabilité ?

- Licence appliquée ?

- Attention aux dates des derniers commits/push sur les repositories.

image : Flaticon.com

CLUSIR
#Aquitaine

AVEZ-VOUS DES QUESTIONS ?

CLUSIR
#Aquitaine

MERCI DE VOTRE ATTENTION