Nouvelle norme ISO/IEC 27002:2022

Comment s'y préparer ?

Livre blanc du Club 27001

1ère édition janvier 2023

CLUB 27001 – Association loi de 1901 (Numéro RNA : W913001368)
http://www.club-27001.fr | contact principal : club-27001@club-27001.fr

Avant-propos par Alia FOURATI

Experte en cybersécurité à EDF R&D et co-éditrice de la norme ISO/IEC 27002:2022

La nouvelle version de la norme ISO/IEC 27002:2022 apporte des changements significatifs par rapport à la version précédente de 2013, tant sur le fond que sur la forme. Sur la forme, la structure de la norme a été simplifiée : elle est désormais présentée comme une liste de mesures de sécurité groupées en 4 thèmes, et chaque mesure de sécurité est présentée par : 5 attributs et leurs valeurs, une description de la mesure de sécurité, un objectif unique, des recommandations de mise en œuvre et des informations supplémentaires. Sur le fond, chaque ligne de la norme a été révisée et discutée pour s'aligner au mieux à l'état de l'art et aux pratiques récentes de sécurité de l'information et de cybersécurité. Parmi les améliorations à noter : la fusion des mesures de sécurité redondantes a impliqué la réduction du nombre total de mesures de sécurité ; l'introduction de nouvelles mesures de sécurité reflète les nouvelles pratiques en cybersécurité ; l'introduction de 5 exemples d'attributs apporte de la flexibilité dans l'utilisation de la norme, et enfin 2 nouvelles annexes portent sur l'utilisation des attributs et la correspondance des mesures de sécurité entre les versions de 2013 et de 2022. Finalement, plusieurs "outils" sont proposés dans cette nouvelle version permettant aux praticiens une utilisation plus flexible et plus aisée de la longue liste de mesures de sécurité proposée dans cette norme.

À la suite de la publication de cette nouvelle version, le Club 27001 et son groupe de travail 27002 s'est emparé du nouveau texte, s'est approprié ses nouveaux "outils" et s'est proposé de développer ce Livre Blanc pour partager son analyse de cette nouvelle version, et surtout pour apporter un exemple d'utilisation de ce nouveau concept qu'est les "attributs", et c'est en effet l'objectif de ces "attributs" : que chaque organisation, utilisateur ou praticien crée son propre attribut, celui qui répond aux besoins spécifiques de son contexte et qui lui permette d'utiliser le plus efficacement possible cet ensemble de mesures de sécurité. Ainsi, ce Livre blanc propose un nouvel attribut "Activités " en ligne avec le concept d'attributs proposé dans l'édition 2022 de l'ISO/IEC 27002. Ce nouvel attribut a les mêmes "valeurs" que l'exemple d'attribut "Capacités opérationnelles" de la norme mais avec une association différente de ces valeurs à chaque mesure de sécurité ; de plus, des informations supplémentaires issues de l'expérience des contributeurs sont suggérées pour chaque mesure de sécurité.

Notons que la finalité de ces attributs, qui ne sont pas obligatoires dans l'utilisation des mesures de sécurité, est surtout de faciliter la navigation dans cette longue liste de mesures de sécurité pour identifier, sélectionner ou trier facilement et rapidement la ou les mesures qui répondent au mieux aux besoins de l'utilisateur.

Bien qu'il s'agisse ici d'une première version, cette contribution représente un apport pertinent de par son appropriation rapide des nouveaux concepts de l'ISO/IEC 27002:2022 et de par son pragmatisme. Les contributions des utilisateurs et les retours d'expérience seront par ailleurs essentiels pour l'évolution de cet attribut prometteur qui sera d'une utilité précieuse pour les utilisateurs.

Remerciements

L'association "Club 27001" rassemble de nombreux professionnels de la Sécurité des Systèmes d'Information impliqués dans les travaux et dans la mise en œuvre des normes de la série ISO 27000.

Le Club 27001 tient à remercier toutes les personnes ayant participé au groupe de travail **'ISO/IEC 27002:2022'** et permis la rédaction de ce livre blanc.

Les animateurs du groupe de travail :

Emmanuel	**PETIT**	*CGI France*
Jean-Christophe	**TOUVET**	*SIMPLOS*

Les contributeurs :

Jean-François	**BAILETTE**	*G-echo*
Didier	**BARZIN**	*Centre Hospitalier Emile Mayrisch*
Gaëtan	**BOURDILLON**	
William	**BOURGEOIS**	*KyNeo*
Alban	**CAOUREN**	*INOTYKO*
Laurent	**CORDIVAL**	*HeadMind Partners*
Célian	**COSTES**	*OWN*
Sylvain	**CROUET**	*Neocase Software*
Eric	**DELAYE**	
Gilles	**LINDER**	*MGEN*
Ilan	**MALLET**	
Elisabeth	**MANCA**	*Alekso – formatrice HS2*
Emmanuel	**PRAT**	*Airbus Protect*

C'est avec plaisir que le groupe de travail vous livre cette première édition. Celle-ci ne saurait être considérée comme exhaustive. Elle fera, nous l'espérons, l'objet de nouvelles versions avec l'aide de vous tous, désireux de rejoindre ce projet.

Cette initiative vous intéresse ? N'hésitez pas à nous rejoindre pour la prochaine version !

Sommaire

1 INTRODUCTION

À l'heure où la Sécurité des Systèmes d'Information est devenue de plus en plus prégnante et une exigence pour les entreprises et administrations, la mise en place d'un système de management de la sécurité de l'information (SMSI) est un élément déterminant qui permet de cadrer et d'améliorer les activités relatives à la cybersécurité et plus généralement à la Sécurité de l'Information.

L'année 2022 a vu la publication d'une nouvelle version de la norme ISO 27002, avec des changements conséquents. Il était important de pouvoir rappeler pourquoi et comment utiliser cette norme, présenter ces évolutions, vous aider dans l'appropriation de la notion d'attribut avec une proposition d'un attribut spécifique "Activités", et enfin mettre à disposition un référentiel d'audit de la maturité des pratiques en sécurité de l'information sur la base de cette norme.

Pour apporter une réponse à ces questions, le Club 27001 est très heureux de partager avec la communauté ce livre blanc.

Le conseil d'administration du Club 27001, se joint à moi pour remercier l'ensemble des contributeurs et auteurs de ce livre blanc, et plus particulièrement les animateurs Jean-Christophe et Emmanuel pour avoir capté l'énergie de chacun et finalisé la production de cette 1ère version de ce livre blanc.

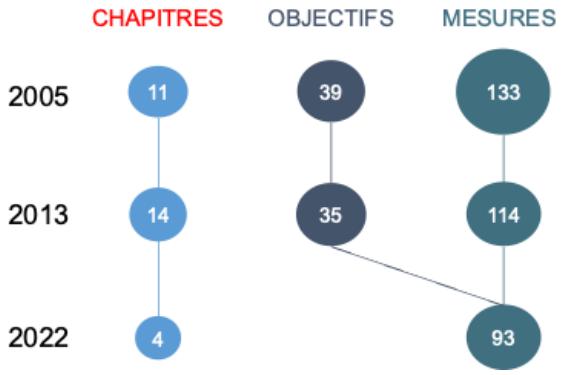
Emmanuel GARNIER, président du Club 27001

2 DECOUVERTE DE LA NORME ISO 27002

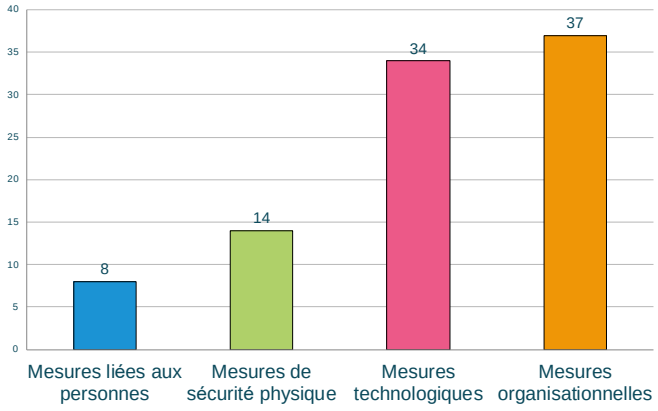
Jusqu'en 2021, la norme ISO 27002 était historiquement un « *Code de bonnes pratiques pour le management de la sécurité de l'information* » qui trouve notamment son origine dans les années 1990 avec le standard britannique BS 7799 (apparu en 1995 pour la 1ère édition).

Étroitement liée à la norme ISO 27001 initialement publiée en 2005, elle présentait depuis sa dernière révision datant de 2013 une série de mesures de sécurité (au nombre de 114) destinées à satisfaire des objectifs de sécurité (au nombre de 35) répartis en 14 chapitres couvrant différents domaines de la sécurité de l'information et pouvant être mises en œuvre dans le cadre d'une certification ISO 27001.

Depuis début 2022, la norme a évolué en profondeur dans sa structure en prenant le titre de « *Sécurité de l'information, cybersécurité et protection de la vie privée – Mesures de sécurité de l'information* ».



Évolution de la structure de la norme ISO 27002 depuis 2005



Répartition des mesures ISO 27002:2022 par domaine

On dénombre à présent 93 mesures de sécurité réparties dans 4 chapitres :

1. Mesures **organisationnelles**
2. Mesures liées aux **personnes**
3. Mesures[1] de **sécurité physique**
4. Mesures **technologiques**

Chaque mesure de sécurité a un objectif spécifique, plutôt qu'un objectif commun avec d'autres mesures (comme dans la version 2013).

Les mesures de sécurité de la norme ISO 27002 étant répertoriées dans l'annexe A de la norme ISO 27001, celle-ci a fait également l'objet d'une révision en 2022, en versions anglaise et française alors que la version française de la 27002 n'a été publiée qu'en janvier 2023.

Pourquoi et comment utiliser la norme ISO 27002 ?

La norme ISO 27002 fournit un référentiel de mesures de sécurité de l'information génériques incluant des recommandations de mise en œuvre. Selon le domaine d'application de la norme, ce document est destiné à être utilisé indifféremment :

- Dans le cadre d'un Système de Management de la Sécurité de l'Information (SMSI) basé sur la norme ISO 27001:2022.
- Pour l'implémentation de mesures de sécurité informatique basées sur des bonnes pratiques reconnues internationalement.
- Pour définir des lignes directrices de management de la sécurité de l'information propres à une organisation.

[1] Certains pourront s'étonner de l'utilisation du mot « contrôles » plutôt que « mesures » dans l'annexe A de la version française de la norme ISO/IEC 27001:2022 publiée fin décembre 2022. En effet, la traduction la plus correcte de l'anglais « *security control* » est « mesure de sécurité » en français, comme dans l'intégralité du texte de la norme à l'exception de ce titre ainsi que dans la version française de la norme ISO/IEC 27002:2022.

L'annexe A de la 27001 est normative, donc d'application obligatoire pour assurer la conformité avec la norme (dans le cadre d'une certification notamment) ; les utilisateurs peuvent mettre en œuvre des mesures de sécurité différentes, mais doivent les comparer à celles de la 27002 (cf. ISO 27001 § 6.1.3 c) et apporter une justification de leur exclusion (cf. ISO 27001 § 6.1.3 d).

D'un point de vue pratique, l'objectif d'une mesure de sécurité est de maintenir ou modifier un ou plusieurs risques. Le choix des mesures de sécurité à mettre en œuvre devrait donc s'inscrire dans une démarche de ***management du risque*** (telle que définie dans la norme ISO 27005:2022 par exemple) en tenant compte :

- De l'organisation.
- Des exigences légales ou réglementaires.
- Des actifs à protéger.
- Des aspects techniques.

Un référentiel de mesures de sécurité comme l'ISO/IEC 27002 pourrait également servir à évaluer le niveau de protection d'une organisation en matière de sécurité de l'information en dehors d''une démarche de sécurisation par les risques. Ceci pourrait s'appliquer si la liste des mesures de sécurité pertinentes pour améliorer le niveau de sécurité de l'organisation a été identifiée au préalable.

Le Club 27001 propose de s'appuyer sur ce référentiel pour créer un ***référentiel d'audit de la maturité des pratiques en sécurité de l'information*** (cf. outillage proposé et publié par le Club sur son portail).

3 NOUVEAUTES ET EVOLUTIONS AVEC LA VERSION 2022

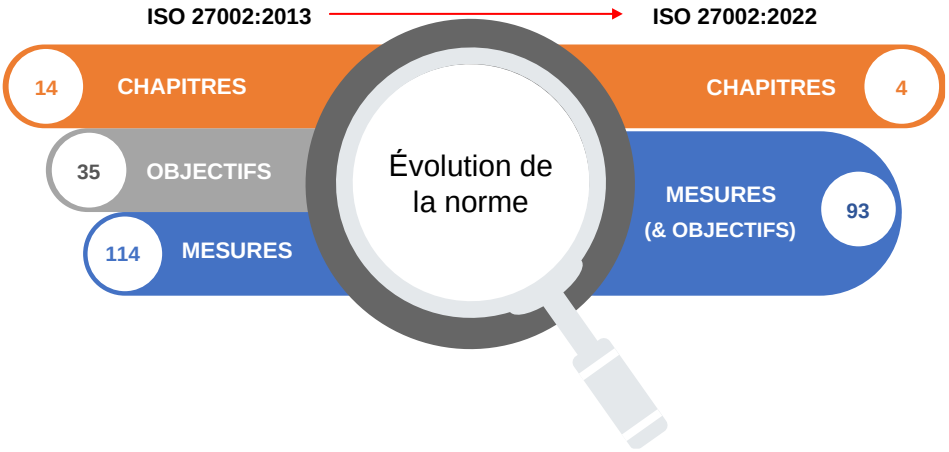
Il est rappelé que tous les 5 ans les normes peuvent faire l'objet d'une révision si l'étude d'opportunité (également appelé "*study period*") met en avant le caractère pertinent et nécessaire de la révision.

Face aux nouveaux enjeux technologiques et aux usages grandissants de l'IT et du numérique, la "*study period*" a suscité beaucoup d'intérêt et de contributions. Un réel besoin de simplification et de refonte a été identifié pour mettre à jour les mesures de sécurité et tenir compte de l'état de l'art et des pratiques actuelles de cybersécurité.

C'est chose faite, puisque la nouvelle norme ISO 27002 est parue en début d'année 2022 en anglais. Dans le prolongement de l'ISO 27005:2022 et de l'ISO 27001:2022, publiées toutes deux en français et en anglais entre octobre et décembre 2022, la version française définitive de la 27002 a été publiée en janvier 2023.

Il est intéressant que ces normes dédiées au management du risque informatique aient été revues dans la même période, afin de permettre une meilleure approche du management de profils de risques et un rapprochement avec d'autres grands référentiels : la 27002:2022 a repris les 5 fonctions du modèle du NIST (en complétant son modèle originel avec les nouvelles fonctions *detect* et *respond*) quand la 27005:2022, elle, reprend dans son annexe le concept de base du framework EBIOS RM.

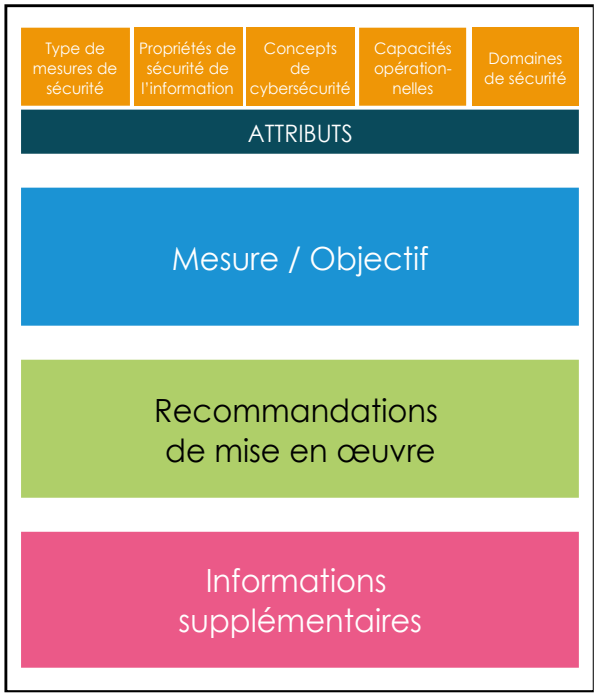
Il s'agissait aussi de mettre à jour le contenu technique et d'inclure de nouvelles pratiques en sécurité de l'information et cybersécurité, telles que le "5.7 – *Threat intelligence*" ("Renseignement sur les menaces" est le terme en français), et d'introduire les attributs permettant d'appréhender les mesures selon différents critères.



En effet, une grande nouveauté de cette version est la possibilité de trier, sélectionner, grouper les mesures de sécurité selon différents critères apportés par les attributs ; 5 exemples d'attributs sont proposés par la norme, mais les utilisateurs peuvent définir leurs propres attributs pour répondre à des besoins spécifiques (cf. exemple d'un nouvel attribut § 6). Ces normes sont le résultat des travaux d'experts du domaine et accompagnent l'évolution des usages des systèmes d'information et de leurs environnements technologiques.

Ainsi, il est possible de grouper les mesures de sécurité de la nouvelle version selon différentes visions (grâce aux attributs), celle du NIST framework avec les *concepts de cybersécurité*, celle de l'ENISA avec les *domaines de sécurité*, et d'autres visions plus largement partagées avec les *types de mesures de sécurité* ou *les propriétés de sécurité de l'information*.

3.1 En termes de structure



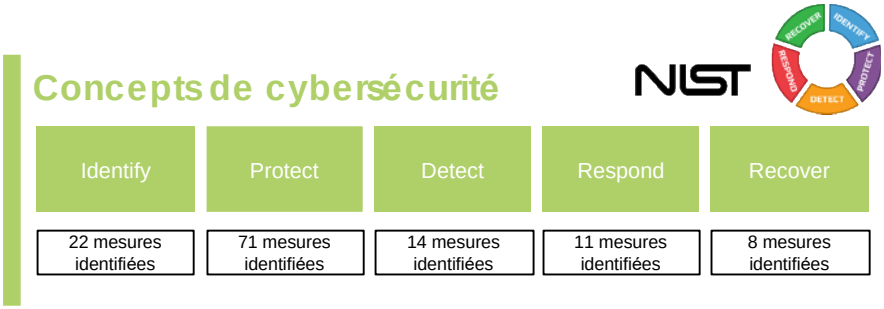
Au niveau macroscopique, la norme change radicalement avec une structure simplifiée. Ce ne sont plus 114 mesures réparties dans 14 chapitres déroulés de manière thématique, mais 93 mesures organisées selon 4 thèmes : l'organisation, les personnes, le physique et le technologique, encore un point très structurant !

Un peu moins de mesures allez-vous dire, mais ne pensez pas que vous allez faire des économies de papier, car au niveau microscopique, des mesures ont fait l'objet de fusions. De plus une mini révolution est apparue avec l'introduction d'attributs associés à chaque mesure (cf. ci-dessous).

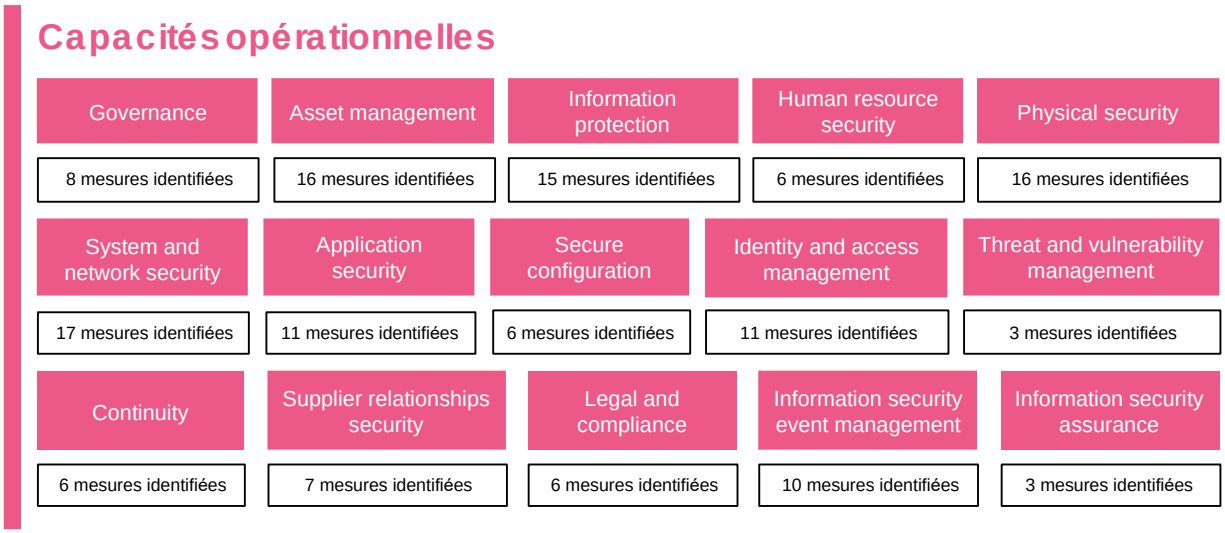
En outre, chaque mesure possède son propre objectif dans cette nouvelle version. Ceci impacte la norme ISO 27001, dont l'annexe A est alignée sur la 27002, et donc directement la déclaration d'applicabilité (DdA) du SMSI.

5 types d'attributs sont proposés pour chaque mesure :

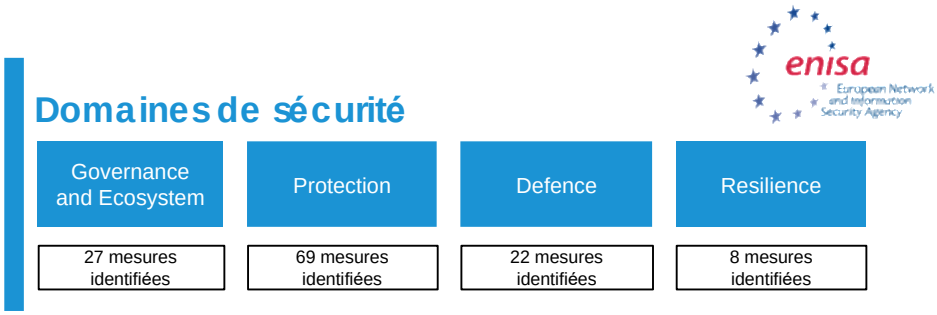
- ***Type de mesure de sécurité*** → à quel moment et comment la mesure agit sur un incident de sécurité :
  - *Preventive* (avant), *Detective* (pendant), *Corrective* (après)
- ***Propriétés de sécurité de l'information*** → sur quel critère de sécurité la mesure agit :
  - Disponibilité, Intégrité et/ou Confidentialité
- ***Concepts de cybersécurité*** → en lien avec la norme ISO/IEC TS 27110 et le framework du NIST :
  - Identify, Protect, Detect, Respond and Recover



- ***Capacités opérationnelles*** → du point de vue de l'implémenteur, lien avec des activités métiers cyber (cf. § 6.1) :



- ***Domaines de sécurité*** → en lien avec la vision de l'ENISA des domaines de sécurité de l'information :
  - Governance and Ecosystem, Protection, Defence and Resilience



Exemple : Mesure 5.7 "Threat intelligence" / "Renseignement sur les menaces"

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience
Control	Information relating to information security threats shall be collected and analysed to produce threat intelligence		**Purpose**	To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken
Guidance	Information about existing or emerging threats is collected and analysed in order to: a) Facilitate informed actions to prevent the threats from causing harm to the organization; b) Reduce the impacts of such threats. Threat intelligence can be divided into three layers, which should…			
Other information	…			

Remarques :

- Mesure de sécurité (*control* en anglais) : dans cet exemple, la norme conseille d'avoir une politique d'anticipation des menaces ; il n'est pas obligatoire de suivre le texte à la lettre et il est possible de formuler sa propre règle.
- Recommandations (*guidance* en anglais) : ce sont des recommandations de mise en œuvre de la mesure de sécurité proposant différentes pratiques, actions, mesures technologiques, processus, etc. (dans l'exemple : collecte et analyse, division en 3 couches stratégie/tactique/opérationnelle…).
- Informations supplémentaires : cette section n'est pas nouvelle, mais elle est plus systématique, avec une volonté de se rattacher le plus souvent possible et plus systématiquement aux grands référentiels ou normes ISO/IEC spécifiques (dans cet exemple, il y a un renvoi à l'ISO 27005 concernant la gestion des risques). Plus l'interdépendance avec d'autres mesures de la norme :

  5.25 Évaluation des événements de sécurité de l'information et prise de décision

  8.7 Protection contre les programmes malveillants (malware)

  8.16 Activités de surveillance

  8.23 Filtrage web

Avis du Club 27001 : ce qu'on peut retenir de cette nouvelle structure

- La flexibilité introduite par les attributs permet de catégoriser les mesures de sécurité selon les besoins de l'organisation (quelle que soit sa taille), tels que les capacités opérationnelles ou les propriétés de sécurité de l'information proposés par la norme, ou selon de nouveaux attributs créés par l'organisation pour répondre à des besoins spécifiques (e.g. indicateurs de risques).
- Une mesure peut relever de plusieurs domaines cyber, ou concepts défensifs, et croiser plusieurs capacités opérationnelles.
- La richesse des critères/attributs et leur diversité ouvrent la voie sur la production et l'interopérabilité des indicateurs et en font un outil redoutable de pilotage de risques, d'auditabilité ou pour gérer la conformité.
- Attention à ne pas « se mélanger » dans les attributs : on peut par exemple avoir du mal à distinguer les "Concepts de sécurité" des "*Domaines de sécurité*" où l'on retrouve le terme "*Protect*" dans le premier et "*protection*" dans le second. En réalité, ces 2 attributs ne sont pas censés être utilisés en même temps, donc il ne devrait pas y avoir de confusion.

3.2 En termes de contenu

11 nouvelles mesures apparaissent avec la nouvelle version 2022 : (cf. fiches présentées dans le document)

- 5.7 Renseignement sur les 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 des configurations
- 8.10 Suppression des informations
- 8.11 Masquage des données
- 8.12 Prévention de la fuite de données
- 8.16 Activités de surveillance
- 8.23 Filtrage web
- 8.28 Codage sécurisé

Toutes les mesures de la norme 27002 ont été révisées en profondeur et complétées selon l'état de l'art et les pratiques les plus récentes. Les redondances ont également été supprimées en fusionnant certaines mesures de sécurité, par exemple :

- La thématique « **sécurité du réseau** » regroupe désormais toutes les mesures liées au réseau et s'enrichit d'un chapitre filtrage Internet qui fait l'objet d'une fiche descriptive dans ce livre blanc (cf. § 9).

- La thématique « **relation avec les fournisseurs** » rassemble toutes les mesures liées à la gestion des fournisseurs, et s'enrichit enfin d'un processus de sécurisation des services Cloud, qui est également détaillé dans une fiche descriptive (cf. § 10).

D'autres mesures ont fait l'objet de **renforcements** notamment :

- **La thématique « protection de l'information » a été renforcée** avec des mesures remarquables telles que l'inventaire des informations et autres actifs associés (5.9), la prévention de la fuite de données, la suppression des informations, la définition « usage acceptable de l'information et classement » contrairement à la version 2013. Étant donné que la norme ISO 27701 s'appuie sur la 27002 et ajoute des exigences supplémentaires concernant la protection des données personnelles avec le PIMS, elle devra faire l'objet de révision pour s'aligner avec les nouvelles versions des normes 27001 et 27002

Il est également constaté des modifications non substantielles ou des transferts tels que :

- Pour l'ancien chapitre « **aspects de la sécurité de l'information dans la gestion de la continuité de l'activité** », le transfert des 3 mesures traitant de la **continuité de la sécurité de l'information** dans deux mesures organisationnelles « **sécurité de l'information pendant une perturbation** » et « **préparation des TIC pour la continuité d'activité** » (qui renvoie toujours, pour la *gestion de la continuité d'activité* à proprement parler, aux normes ISO 22301, 27301 et 22313) et le transfert de la mesure traitant de la **redondance** dans le chapitre « **mesures technologiques** ».
- « **Orientations de la direction en matière de sécurité de l'information** » n'est plus identifié comme un chapitre autonome, ce qui ne veut pas dire pour autant que le "processus activité" gouvernance s'est vidé de son contenu, comme le montre la fiche détaillée dans le § 7.

Avis du Club 27001 : ce qu'on peut retenir de ces évolutions

- Les évolutions se retrouvent à la fois dans le contenu technique mais aussi dans la structure, les inclusions, les renvois et les ajouts**.**
- Les chapitres n'indiquent aucune priorisation ou un niveau d'importance mais permettent simplement de structurer le contenu des 93 mesures. La norme 27002:2022 est à considérer comme une liste de mesures de sécurité sans aucune hiérarchie.
- On aimerait avoir plus de détail sur la partie 'architecture' notamment pour les nouvelles technologies IoT, Edge Computing, les couches multi Cloud complexes, mais l'essentiel y figure. Par exemple les principes du Zero Trust sont présentés dans la mesure 8.27 "secure system architecture and engineering principles".

  NOTE : Ce point est tout à fait intentionnel, car l'objectif de la 27002 est de rester une norme générique applicable à tous les types d'organisations et de contextes ; pour des contextes/cas spécifiques, il existe des normes dédiées dont les références sont indiquées dans le texte de la 27002.

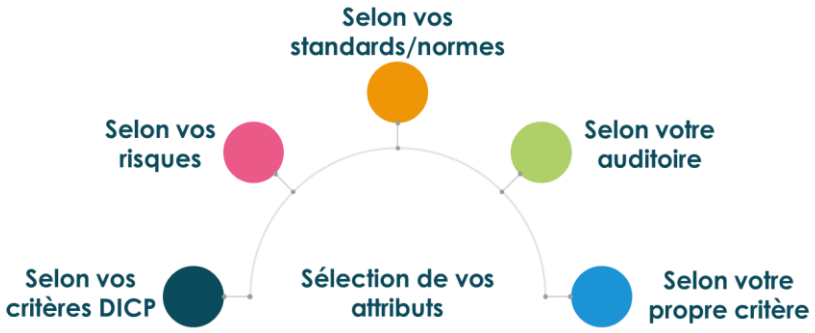
4 UTILISATION DES ATTRIBUTS AVEC LA VERSION 2022

L'ISO 27002:2022 est un support incontournable pour bénéficier de recommandations et sélectionner les bonnes mesures à mettre en œuvre, notamment dans la cadre de la certification ISO/IEC 27001.

La lecture de l'ISO/IEC 27002:2022 est moins hiérarchique que dans les précédentes versions, ce qui est notamment lié au regroupement sous 4 chapitres. Cependant, les attributs permettent de s'approprier et de naviguer plus facilement cette nouvelle liste de mesures de sécurité. Un des axes d'utilisation ou d'implémentation de la norme est de sélectionner un ou plusieurs attributs pour prendre en compte rapidement les mesures et grouper la mise en œuvre pour ne pas se disperser.

Cette sélection peut se faire selon différents points de vue :

NOTE : une nouvelle norme « ISO/IEC PWI 27028 Guidance on ISO/IEC 1 27002 attributes » (actuellement en mode draft) vise à présenter l'utilisation de ces attributs.



Une mesure de sécurité peut être vue de différentes manières selon le contexte et le besoin de l'utilisateur ; c'est l'objectif des attributs introduits dans la nouvelle version de l'ISO/IEC 27002 permettant de présenter, trier et grouper les mesures de sécurité selon différents critères. Par exemple, il est possible de catégoriser les mesures de sécurité en fonction de "quand" et "comment" une mesure de sécurité réduit un risque en cas d'incident de sécurité :

- En agissant sur la vulnérabilité ou la menace : mesures de **prévention**.
- En surveillant le risque ou en agissant lorsqu'il se produit : mesures de **détection**.
- En préparant la réaction après incident : mesures **correctives**.

Par exemple avec l'attribut "Capacités opérationnelles", une organisation qui a besoin de mettre en œuvre rapidement un pilotage de la gouvernance de la sécurité de l'information pourra rechercher les mesures de sécurité appropriées relatives à la gouvernance en filtrant la liste de mesures de sécurité selon la valeur #Gouvernance de cet attribut [voir ANNEX A_ISO/IEC 27002:2022].

Une bonne pratique suggérée par le Club 27001 est de sélectionner les mesures en les filtrant avec les attributs. Ceci permettra de mettre en œuvre des mesures 'quick win' afin que le projet produise des effets positifs et l'adhésion des collaborateurs. Par exemple une organisation pourrait mettre en œuvre les mesures dédiées aux ressources humaines en sélectionnant celles associées à l'attribut #Human_resource [ANNEX A_ISO/IEC 27002:2022] afin que chacun puisse prendre en compte son implication au sein du projet et plus largement contribuer à la lutte contre les menaces de cybersécurité.

Les organisations familiarisées avec le référentiel NIST, peuvent prendre en compte les attributs "Concepts de sécurité" (#Identify, #Protect, #Detect, #Respond, #Recover) pour rapprocher la nouvelle version de la norme ISO 27002 :2022 avec ce référentiel.

Pour les organisations qui engagent une démarche d'amélioration de leur niveau de maturité sécurité, l'utilisation des attributs filtrés sur les concepts de sécurité et/ou les typologies de mesures (préventive, détection, corrective) peut être un axe pour démarrer rapidement sur l'optimisation du plan de traitement et se concentrer sur les points forts et faibles de l'organisation.

5 IMPACT & USE CASES AVEC LA VERSION 2022

La nouvelle norme ISO/IEC 27002:2022 présente une évolution majeure, qui va nécessiter de repenser et tenir compte des mises à jour, notamment dans le cadre du plan de traitement et la déclaration d'applicabilité de la certification ISO/IEC 27001 ainsi que les revues d'analyse des risques qui vont devoir tenir compte de la nouvelle version.

Une nouvelle version de l'ISO/IEC 27001 a été publiée en 2022 (anglais et français) consistant essentiellement en la mise à jour de son Annexe A pour tenir compte de la nouvelle version de l'ISO/IEC 27002.

Il convient de prendre en compte la nouvelle norme ISO 27002:2022 pour plusieurs raisons :

- La première dans un contexte hors certification ISO 27001, pour tenir compte des nouvelles mesures de sécurité et renforcer la sécurité des systèmes d'information, la protection de l'information doit être considérée comme une composante essentielle du système d'information dès sa conception.
- La deuxième pour se préparer à la transition vers les nouvelles versions :
  - Se renseigner auprès de l'organisme de certification pour obtenir le processus de transition (le processus peut aller jusqu'à 3 ans selon les organismes)
  - Revoir sa gestion des risques pour redéfinir son plan de traitement
  - Publier une nouvelle déclaration d'applicabilité
  - Mettre à jour le corpus documentaire (politique, procédure, etc.) pour modifier l'ensemble des références à l'annexe A de la version ISO 27001:2017 pour la version 2022. Elles sont souvent nombreuses, de nombreuses organisations ayant conservé les références (N° et intitulé) de l'annexe A pour s'y retrouver.

Sous un angle 'Lead Implementor', le Club 27001 propose une liste (non exhaustive) de questions relevées lors des échanges avec le Club si vous souhaitez utiliser la norme ISO 27002:2022 ou l'annexe A de la norme ISO 27001:2022.

1- Je suis certifié(e) ISO 27001, dois-je changer tout de suite ma DdA avec la norme ISO 27002:2022 ou l'annexe A de l'ISO 27001:2022 ?

Réponse du Club : **NON** pas tout de suite, **MAIS** plus tôt vous réaliserez une analyse d'écart, plus rapidement vous identifierez le chemin à parcourir pour mettre en place les nouvelles mesures (ou améliorer les existantes).

2- Mon organisme est déjà certifié ISO 27001:2013 ou 2017, comment utiliser la version 2022 de l'ISO 27002 ?

Réponse du Club : Vos équipes peuvent s'approprier la norme ISO 27002:2022 dès maintenant, notamment au travers des actions suivantes :

- Utiliser l'annexe B de la norme IS 27002:2022 pour faire le lien avec les mesures actuelles dans le plan de traitement des risques et la DdA.
- Vous pouvez également vous approprier les 11 nouvelles mesures de la version 2022 et les inclure dans votre DdA.
- Informer les responsables de mesures des évolutions : (cf. chapitre 6 sur les fiches descriptives) :
  - Regroupement
  - Évolution du contenu en termes d'objectifs de sécurité et d'activités

3- Je ne suis pas certifié(e) ISO 27001, puis-je initier un audit sur la base de la norme ISO 27002:2022 ?

Réponse du Club : Il est tout à fait envisageable de procéder à un audit de maturité pour évaluer votre organisation selon les 93 mesures de cette norme. Le Club 27001 propose à ses membres un outil pour vous aider à réaliser cette évaluation.

4- Je suis certifié(e) 27001:2017 depuis 1 ans, la mise à jour en 2022 de la 27001 me fait-elle perdre ma certification ou bien l'organisme certificateur va-t-il juste modifier l'année de la 27001 sur mon certificat ?

Réponse du Club : **NON et NON**, la mise à jour ne fait pas perdre la certification et il n'y aura pas de changement automatique d'année. Pour rappel, la durée d'une certification 27001 est de 3 ans. Vous serez audité sur la version 2013 ou 2017.

Il est important de rappeler que nous sommes dans une phase de transition :

- La 27001:2022 annule la version 27001:2013
- Fin de validité : 31/10/2025 pour l'ISO 27001:2013
- La norme NF EN ISO/IEC 27001:2017 (norme française et européenne) n'est pas remplacée par la norme ISO/IEC 27001:2022 (norme internationale)

5- Je suis certifié(e) 27001:2017, j'ai tout mon système d'information collaboratif dans le cloud, puis-je ajouter la mesure A.5.23 Sécurité de l'information dans l'utilisation de services en nuage à ma DdA ?

Réponse du Club : **OUI**, mais la norme le prévoit déjà ! Pour rappel il s'agit de la clause '6.1.3 c) NOTE 2' : « Les objectifs et les mesures énumérés dans l'Annexe A ne sont pas exhaustifs […] et des mesures additionnelles peuvent s'avérer nécessaires ».

Attention cependant à bien justifier leur insertion ce qui peut demander une revue/mise à jour de votre analyse de risques.

6- Mon prochain audit de suivi est au printemps 2023, devrai-je présenter à mon organisme de certification mon projet de mise à jour de mon SMSI en 27001:2022 ?

Réponse du Club : **NON** ce n'est à priori pas obligatoire : vous serez audité sur la version ISO 27001:2013 ou 2017.

CEPENDANT, sans montrer un plan projet, l'auditeur va quand même s'attendre à ce que le changement de norme soit mentionné quelque part, dans le contexte par exemple d'une revue de Direction, ou dans le processus de conformité. Ne voir mentionner nulle part ce changement de norme serait un signe que quelque chose ne fonctionne pas dans le SMSI…

Le Club 27001 vous recommande dès à présent de :

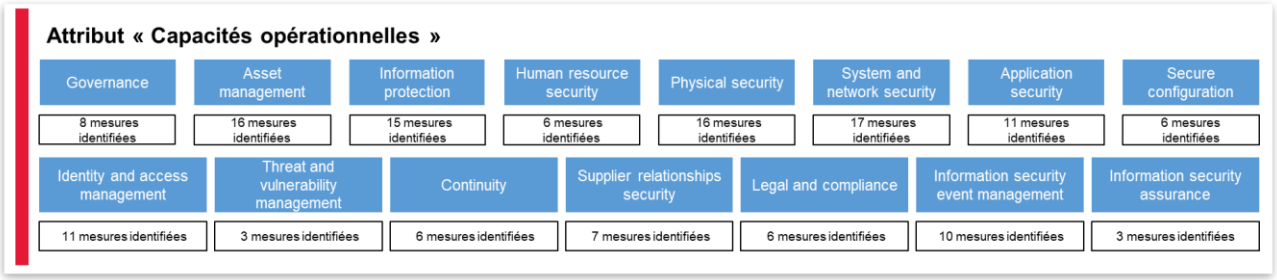
- Prendre connaissance des nouveautés (notamment au travers des fiches publiées par le Club) et/ou suivre des formations qui expliquent ces nouveautés.
- Acheter la nouvelle norme.
- Réaliser une analyse d'écart avec votre existant.
- Reprendre votre DdA, ce qui nécessite une revue de l'analyse de risques pour justifier l'insertion ou l'exclusion des nouvelles mesures.
- Documenter les critères sur les processus et le plan de contrôle associé.
- Revoir les objectifs et le processus de surveillance.
- Revoir le plan de communication.
- Ajouter une entrée dans la revue de Direction.
- Mettre à jour les politiques et procédures si nécessaire.
- Revoir les questionnaires de vos audits.
- Communiquer en interne sur les évolutions.
- Vérifier si vos outils de sécurité tiers fournissent les preuves suffisantes pour démontrer votre conformité avec les nouvelles exigences.

6 PRESENTATION DES FICHES

6.1 Pourquoi regrouper/présenter les 93 mesures en fiches ?

Le concept d'ATTRIBUT étant nouveau dans cette version 2022, le Club 27001 a utilisé ce concept pour présenter/regrouper sous un autre angle les 93 mesures de la version 2022 en définissant un nouvel attribut.

Libre à chacun de pouvoir utiliser les Attributs ou d'en inventer de nouveau. Nous avons utilisé l'attribut 'capacités opérationnelles' pour faciliter l'analyse des 93 mesures (et ne pas garder uniquement le découpage sous les 4 chapitres).



Comme l'illustre le tableau ci-dessus, certaines mesures sont associées à plusieurs valeurs de l'attribut " capacités opérationnelles " (exemple : mesure 6.6 'Accords de confidentialité ou de non-divulgation' est associé à 3 valeurs de l'attribut 'capacités opérationnelles').

Le Club 27001 a décidé d'utiliser ce 1er découpage et d'aller plus loin avec la création d'un nouvel Attribut appelé '**ACTIVITÉS**'. Celui-ci est spécifiquement créé par le Club dans le cadre de son analyse et du livre blanc.

Le Club a décidé de regrouper les 93 mesures selon 14 valeurs du nouvel attribut 'ACTIVITÉS' en rattachant chaque mesure à une et une seule valeur de cet attribut notamment pour faciliter l'identification et l'appropriation de ces 93 mesures par les porteurs de celle-ci. La liste détaillée de l'attribut 'ACTIVITÉS' est la suivante :

- Gouvernance
- Gestion des actifs
- Protection des informations
- Ressources humaines
- Protection physique
- Sécurité système et réseau
- Protection des applications
- Gestion et durcissement des configurations
- Gestion des identités et des accès
- Gestion des menaces et des vulnérabilités
- Continuité
- Relations fournisseurs
- Conformité
- Gestion des évènements et incidents

NOTE : le regroupement détaillé des 93 mesures sous l'attribut 'ACTIVITÉS' est présentée dans le tableur mis à disposition par le Club 27001

Regroupement des 93 mesures sous l'attribut 'ACTIVITES'

'Capacités opérationnelles' (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 ATTRIBUT proposé par le Club

ISO 27002:2022

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**

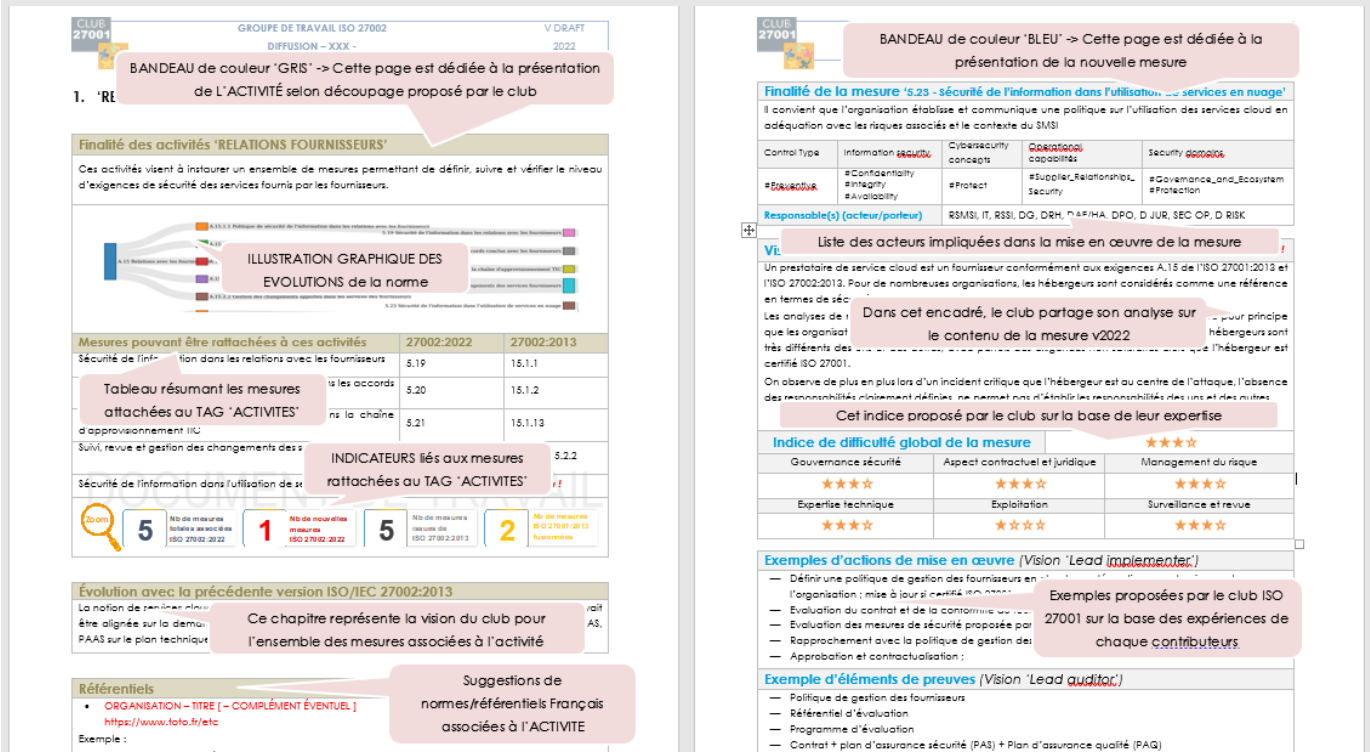
6.2 Comment lire les fiches proposées par le Club ?

6 fiches de lecture sont proposées dans ce livre blanc présentant une nouvelle vision apportée par le Club 27001 des nouvelles mesures de l'ISO/IEC 27002:2022.

Dans cette 1ère version du livre blanc, le Club a souhaité proposer une priorité sur les activités indispensables à regarder au démarrage en termes de gouvernance, gestion d'incidents, relations fournisseurs, etc. La liste des fiches fera l'objet d'évolution dans la prochaine version de ce livre blanc.

Chaque fiche est découpée en 2 parties :

- 1ère partie/page (avec un encadré gris) : présentation sommaire de l'attribut 'ACTIVITÉS' et des mesures rattachées.
- 2ème partie (avec un encadré bleu) : présentation et analyse de la nouvelle mesure.



Responsable(s) (acteur/porteur) : RSMSI, IT, RSSI, DG, DRH, DAF/HA, DPO, D JUR, SEC OP, D RISK (cf. acronymes).

Fiches uniquement disponibles dans la version du livre blanc réservée aux membres du Club 27001

7 FICHE #1 : GOUVERNANCE

8 FICHE #2 : GESTION DES ACTIFS

9 FICHE #3 : PROTECTION DE L'INFORMATION

10 FICHE #4 : SÉCURITÉ SYSTÈME ET RÉSEAU

11 FICHE #5 : RELATIONS FOURNISSEURS

12 FICHE #6 : GESTION DES ÉVÉNEMENTS ET DES INCIDENTS

Table des acronymes

Acronyme	Description
DAF/HA	Directeur Administratif et Financier / Directeur des Achats
DG	Directeur Général
D JUR	Directeur Juridique
DPO	Délégué à la Protection des données
DRH	Directeur des Ressources Humaines
D RISK	Directeur des Risques
ISO	Organisation Internationale de normalisation
IT	Responsable/Directeur IT
RSMSI	Responsable du pilotage/animation du SMSI
RSSI	Responsable de la Sécurité des Systèmes d'Information
SEC OP	Équipe Sécurité Opérationnelle
SMSI	Système de Management de la Sécurité de l'Information
SoA / DdA	*Statement of Applicability* / Déclaration d'Applicabilité

Publication des résultats

Les documents suivants sont disponibles en téléchargement sur le site Internet du Club 27001, rubrique « ISO 27002:2022 » :

- ***En accès public***
  - Ce livre blanc (sans les fiches descriptives)
  - Présentation du 22/11/2022 – conférence annuelle du Club 27001
- ***Accès réservé aux membres du Club***
  - Ce livre blanc (avec les fiches descriptives)
  - Outil d'audit de maturité et de transition (format XLSX)
  - Présentation du 28/09/2022 – groupe de Paris du Club 27001

http://www.club-27001.fr/