SÉCURITÉ DE L'INFORMATION

Guide de transition ISO/IEC 27001

→ L'ESSENTIEL DE LA VERSION 2022

afnor CERTIFICATION

SOMMAIRE

afnor CERTIFICATION

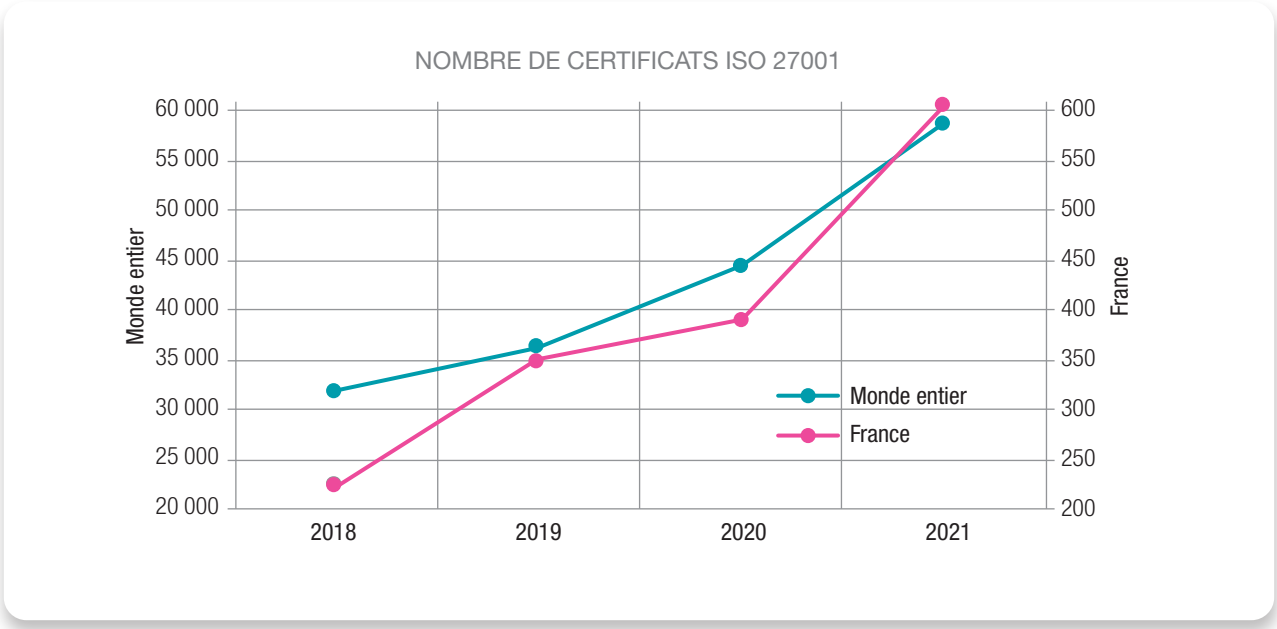
Remerciements : nous tenons à remercier toutes les personnes ayant contribué, de près ou de loin, à l'élaboration de ce guide.

Date de publication : janvier 2023.

→ INTRODUCTION

La norme ISO/IEC 27001 est la référence internationale pour organiser la sécurité de l'information au sein d'un organisme. Elle définit une méthodologie pour identifier les cybermenaces, maîtriser les risques associés et mettre en place les mesures de protection appropriées afin d'assurer la confidentialité, la disponibilité et l'intégrité des informations.

Le nombre de certificats ISO/IEC 27001 a progressé de +55% en France en 2021 par rapport à 2020, pour atteindre 606 selon l'ISO Survey publiée fin septembre 2022 qui rassemble les chiffres déclarés par tous les organismes d'accréditation (en France le COFRAC).



L'étude sur les organismes certifiés ISO/IEC 27001 lancée par AFNOR CERTIFICATION en 2019 avait montré que pour 62% d'entre eux, la certification ISO/IEC 27001 était une contrainte imposée dans un appel d'offres.

Depuis 2019 les incitations des donneurs d'ordres se sont intensifiées. Plusieurs lois et règlementations imposant la certification ISO/IEC 27001 ou de façon plus large la mise en œuvre de mesures de cybersécurité sont entrées en application (décret Hébergeurs de données de santé, règlement RGPD, règlement n°155 du WP29 de la Commission économique pour l'Europe des Nations unies (UNECE)). D'autres textes règlementaires sectoriels sont en cours d'élaboration et seront publiés prochainement.

Face à cette demande en forte croissance, la version 2022 de l'ISO/IEC 27001 s'actualise. Elle prend en considération les nouveaux contextes des organisations (développement du télétravail suite à la crise covid, développement des services cloud, etc.) et impose notamment la mise en œuvre de nouvelles mesures de sécurité.

Les organismes déjà certifiés selon la NF EN ISO/IEC 27001:2017 vont devoir transiter vers la version 2022 de la norme. Plus que jamais, AFNOR Certification et ses auditeurs sont à vos côtés pour vous aider à vous engager aussi sereinement que possible dans la transition.

LE CALENDRIER DE TRANSITION

La note de transition du COFRAC révisée le 20 mars 2023, en adéquation avec la 2e version du document IAF MD 26 publiée le 15 février 2023 par l'International Accreditation Forum (association internationale des organismes d'accréditation, dont fait partie le COFRAC), définit les grandes étapes de la transition vers la version 2022 de l'ISO/IEC 27001 :

- la période de transition est de trois ans. Elle débute le 31 octobre 2022 et se termine le 31 octobre 2025 ;
- à partir du 30 avril 2024, il ne sera plus possible pour les organismes de certification d'émettre de nouveaux certificats sur la base de la version 2017 de la norme NF EN ISO/IEC 27001 dans le cadre d'une certification initiale ou d'un renouvellement de certification ;
- les organismes avec un certificat en lien avec la version 2017 de la NF EN ISO/IEC 27001 auront jusqu'au 31 octobre 2025 pour passer à la version 2022 de l'ISO/IEC 27001. La transition peut être effectuée lors d'un audit de suivi ou de renouvellement, ou même lors d'un audit complémentaire réalisé en dehors du cycle classique d'audit.

Les audits de transition doivent inclure, sans s'y limiter, les éléments suivants :

- la mise à jour de la déclaration d'applicabilité (DDA) ;
- le cas échéant, la mise à jour du plan de gestion des risques ;
- la mise en œuvre et l'efficacité des mesures de sécurité de l'information nouvelles ou modifiées.

Cas particulier des hébergeurs de données de santé certifiés HDS :

Tant que les référentiels HDS n'ont pas été révisés, les hébergeurs de données de santé sont tenus par la loi d'être certifiés sur la version 2017 de la NF EN ISO/IEC 27001.

Pour ceux qui souhaitent migrer au plus tôt sans attendre la révision des référentiels HDS, il est possible de réaliser un audit combiné qui prend en compte toutes les exigences des deux versions de la norme : version 2017 et version 2022.

À la suite de cet audit, deux certificats distincts coexisteront :

- un certificat accrédité selon la version 2017 ;
- un certificat selon la version 2022 qui sera non-accrédité tant que la transition vers cette norme par l'organisme de certification n'aura pas été actée par le COFRAC.

→ SYNTHÈSE DE LA NOUVELLE ANNEXE A

Les changements majeurs de la nouvelle version de l'ISO/IEC 27001:2022 concernent les mesures de sécurité de l'Annexe A.

	DANS LA VERSION 2017	DANS LA VERSION 2022
Nombre de mesures de l'Annexe A	**114 mesures**	**93 mesures :** • **82 mesures** reprenant de façon synthétique le contenu des 114 mesures de l'ancienne version avec quelques légères variations • **11 nouvelles mesures** prenant en compte le contexte actuel des entreprises (utilisation du cloud, préparation des outils numériques pour la continuité d'activité, …)
Chapitrage de l'Annexe A	**14 chapitres liés à des thématiques opérationnelles :** • **A.9 :** Contrôle d'accès • **A.11 :** Sécurité physique et environnementale • **A.13 :** Sécurité des communications • **A.15 :** Relations avec les fournisseurs • **A.16 :** Gestion des incidents liés à la sécurité de l'information • **…**	**4 chapitres liés à la nature des mesures :** • **A.5 :** Mesures de sécurité organisationnelles • **A.6 :** Mesures de sécurité applicables aux personnes • **A.7 :** Mesures de sécurité physique • **A.8 :** Mesures de sécurité technologiques
Précision des mesures	**L'Annexe A fait environ 12 pages.** Certaines mesures intègrent des précisions pour aider à cerner leur signification.	**L'Annexe A a été réduite à 7 pages** en simplifiant de façon optimale certaines mesures.

La lecture de la norme ISO/IEC 27002:2022 (guide de bonnes pratiques pour mettre en œuvre l'ISO/IEC 27001) est fortement recommandée et essentielle pour organiser au mieux le suivi de l'application des mesures de sécurité de la version 2022 de l'ISO/IEC 27001.

En particulier l'ISO/IEC 27002 associe à chaque mesure de sécurité de l'ISO/IEC 27001 cinq types d'attributs pour les identifier :

- type de mesure (préventive, détective, corrective) ;
- propriété de sécurité de l'information (confidentialité, intégrité, disponibilité) ;
- concept de cybersécurité (identifier, protéger, détecter, répondre, rétablir) ;
- capacité opérationnelle (voir dans la suite du chapitre) ;
- domaine de sécurité (gouvernance et écosystème, protection, défense, résilience).

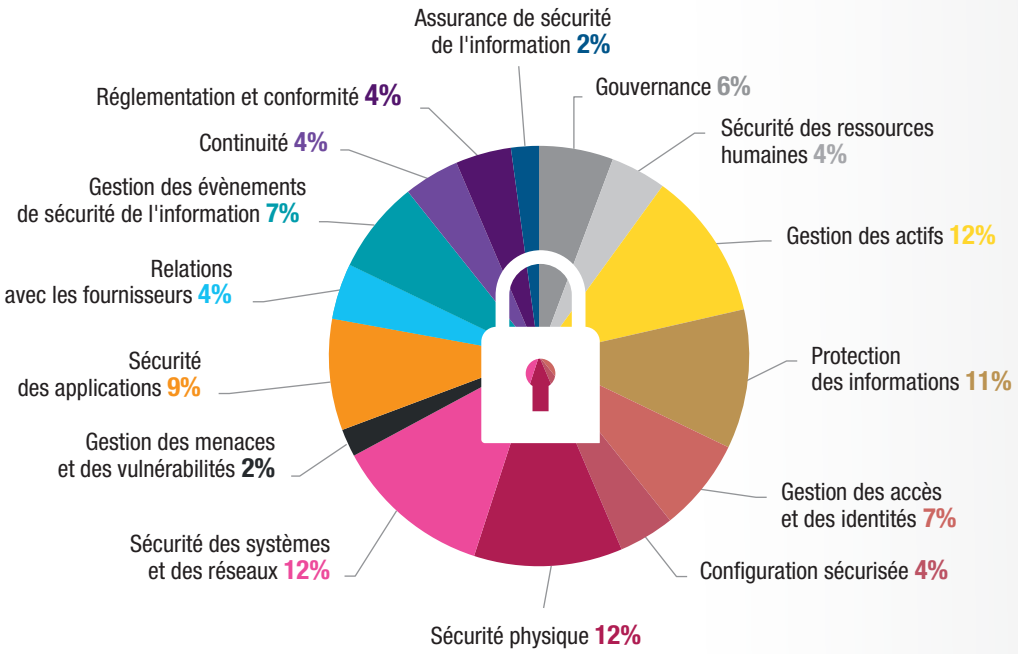
Il est ainsi possible en sélectionnant l'attribut adéquat, de distinguer toutes les mesures préventives de toutes les mesures correctives ou d'identifier toutes les mesures en lien avec une thématique (par exemple la gestion des accès).

Pour ceux qui seraient déroutés par le nouveau chapitrage de l'Annexe A, l'ancien chapitrage est disponible en consultant l'ISO/IEC 27002 au travers de l'attribut « capacités opérationnelles ». Cet attribut reprend les thématiques des chapitres de l'ancienne Annexe A en les améliorant (en particulier l'ancien chapitre A.12 « sécurité liée à l'exploitation » a été divisé car trop générique). Cet attribut permet d'assurer la continuité entre la nouvelle et l'ancienne version de l'ISO/IEC 27001.

Attention, certaines mesures sont dorénavant associées à plusieurs thématiques, permettant un suivi plus souple et efficace.

CHAPITRES DE L'ANNEXE A DE LA VERSION 2017 DE LA NF EN ISO/IEC 27001	ATTRIBUT « CAPACITÉS OPÉRATIONNELLES » DE LA VERSION 2022 DE L'ISO/IEC 27002
• **A.5** Politiques de sécurité de l'information	Gouvernance
• **A.6** Organisation de la sécurité de l'information	Sécurité des ressources humaines
• **A.7** Sécurité des ressources humaines	Gestion des actifs
• **A.8** Gestion des actifs	Protection des informations
• **A.9** Contrôle d'accès	Gestion des accès et des identités
• **A.10** Cryptographie	Configuration sécurisée
• **A.11** Sécurité physique et environnementale	Sécurité physique
• **A.12** Sécurité liée à l'exploitation	Sécurité des systèmes et des réseaux
• **A.13** Sécurité des communications	Gestion des menaces et des vulnérabilités
• **A.14** Acquisition, développement et maintenance des systèmes d'information	Sécurité des applications
• **A.15** Relations avec les fournisseurs	Relations avec les fournisseurs
• **A.16** Gestion des incidents liés à la sécurité de l'information	Gestion des évènements de sécurité de l'information
• **A.17** Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	Continuité
• **A.18** Conformité	Réglementation et conformité
	Assurance de sécurité de l'information

RÉPARTITION DES MESURES DE SÉCURITÉ PAR THÉMATIQUE



→ PRINCIPALES ÉVOLUTIONS : LES 11 NOUVELLES MESURES DE SÉCURITÉ

L'évolution principale de l'ISO/IEC 27001:2022 concerne l'intégration de 11 nouvelles mesures de sécurité dans l'Annexe A qui regroupe le socle minimal des mesures de sécurité à considérer dans le système de management de la sécurité de l'information. Ces 11 nouvelles mesures de sécurité sont à intégrer dans la Déclaration d'Applicabilité.

Elles viennent compléter l'ancien socle de mesures en prenant en compte le contexte actuel de la cybersécurité et des cybermenaces : application de nouvelles règlementations sur la protection des données personnelles, transformation numérique des organismes, intensification des cyberattaques, préparation aux crises sanitaires, etc.

La plupart de ces mesures sont déjà connues voire appliquées totalement ou partiellement par les organismes certifiés ISO/IEC 27001 et sont également mentionnées dans d'autres textes de références comme le guide d'hygiène informatique de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ou le Cybersecurity Framework du National Institute of Standard and Technology (NIST).

Les niveaux d'impacts indiqués sont approximatifs et peuvent varier dans chaque organisme en fonction de l'existant et du contexte.

N°	INTITULÉ	THÉMATIQUE(S) RATTACHÉE(S)	INTÉGRATION DANS LE SYSTÈME DE MANAGEMENT EXISTANT	IMPACT
5.7	Renseignement sur les menaces	Gestion des menaces et des vulnérabilités	Complète la mesure existante sur les contacts avec les groupes d'intérêts spécialisés en vue notamment de mieux se préparer contre les logiciels malveillants et les cyberattaques.	MAJEUR
5.23	Sécurité de l'information dans l'utilisation des services cloud	Relation avec les fournisseurs	Renforce les mesures existantes sur la maîtrise des fournisseurs pour les services *cloud*. Il n'est plus seulement question pour ces prestataires de définir une méthode d'évaluation du service, il faut maintenant également établir des procédures pour l'acquisition, le suivi et la fin du service.	MAJEUR
5.30	Préparation des technologies de l'information et de la communication (TIC) pour la continuité d'activité	Continuité	Complète la mesure existante sur la continuité de la sécurité de l'information et l'étend à la continuité d'activité. Étant donné la transformation numérique des entreprises, maintenir un niveau d'activité acceptable dépend fortement des TIC et de leur préparation.	MOYEN
7.4	Surveillance de la sécurité physique	Sécurité physique	Complète les mesures existantes liées à la sécurisation des bureaux et des salles en imposant une surveillance continue (alarme, vidéosurveillance, etc.).	MINEUR
8.9	Gestion des configurations	Configuration sécurisée	Complète les mesures en lien avec la gestion des actifs, des accès, des vulnérabilités et des changements en imposant une gestion des configurations (actifs, relations entre les actifs, adressages, configurations par défaut, accès à privilèges, etc.).	MAJEUR
8.10	Suppression des informations	Protection de l'information / Conformité et légalité	Complète principalement la mesure existante en lien avec le respect du RGPD pour ce qui concerne le respect des durées de conservation des données personnelles.	MINEUR
8.11	Masquage des données	Protection de l'information	Complète les mesures existantes en lien avec l'utilisation du chiffrement et le respect du RGPD et comprend l'utilisation de différentes techniques (anonymisation, pseudonymisation, masquage, etc.).	MINEUR
8.12	Prévention contre les fuites de données	Protection de l'information	Complète les mesures existantes en lien avec le contrôle d'accès et la classification des données. Les actions de préventions peuvent impliquer une surveillance de certains canaux de communication et un blocage de certaines actions des utilisateurs.	MAJEUR
8.16	Surveillance des activités	Gestion des évènements de sécurité de l'information	Complète les mesures existantes sur la journalisation et la protection contre les malwares en imposant une surveillance continue des comportements et des activités (accès, utilisation des ressources, comportement typique de *malware*,…).	MAJEUR
8.23	Filtrage web	Sécurité des systèmes et des réseaux	Complète notamment la mesure existante sur la protection contre les *malwares* en imposant un filtrage web pour se prémunir notamment contre les sites web avec un contenu malveillant.	MINEUR
8.28	Codage sécurisé	Sécurité des applications / Sécurité des systèmes et des réseaux	Complète la mesure liée aux principes d'ingénierie de la cybersécurité pendant les développements logiciels en renforçant la sécurité du codage.	MOYEN

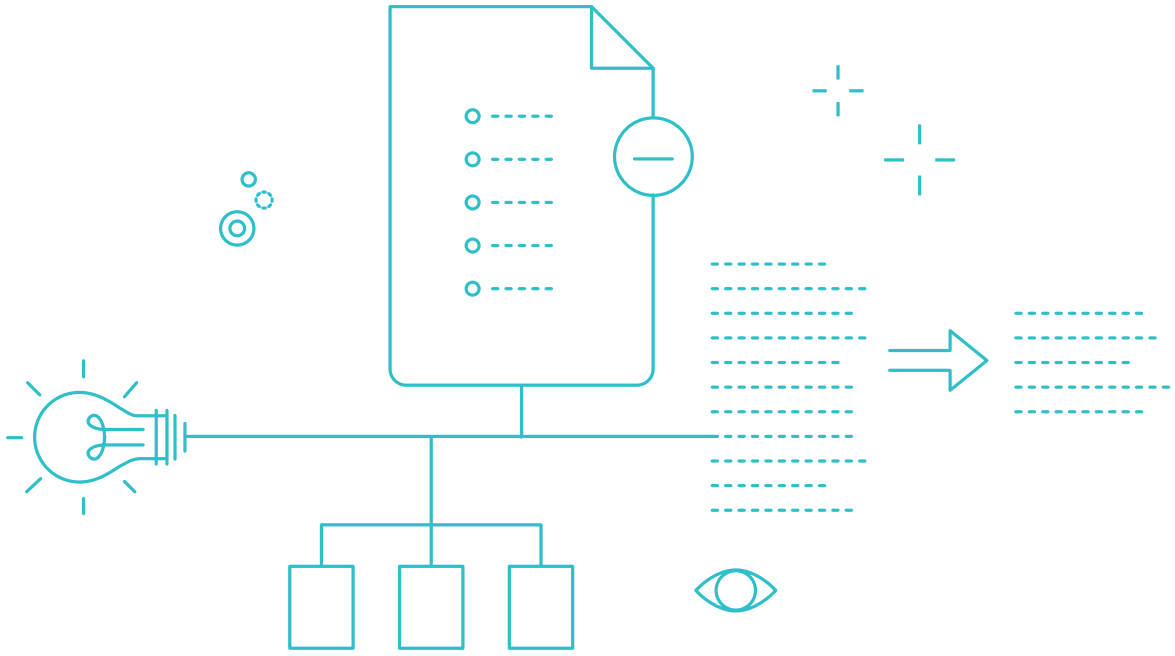
LES AUTRES ÉVOLUTIONS

→ SIMPLIFICATION DES MESURES EXISTANTES

Outre les 11 nouvelles mesures de sécurité, les 93 mesures de l'ISO/IEC 27001:2022 intègrent également 82 mesures qui résultent de réécritures et fusions des mesures existantes issues de la version 2017.

Bien que toutes les mesures existantes aient été considérées et réintégrées à la nouvelle version de la norme, de nombreuses simplifications ont été réalisées et certains détails qui permettaient aux néophytes de mieux cerner la signification des mesures ont été supprimés. Ces détails sur la signification des mesures et bien d'autres précisions relatives à la mise en œuvre des mesures sont mentionnés dans l'ISO/IEC 27002 (guide de bonnes pratiques sur la mise en œuvre de l'ISO/IEC 27001).

Une synthèse des quelques évolutions notables présentes dans les 82 mesures de l'ISO/IEC 27001:2022 issues de mesures existantes est disponible ci-contre. Ces évolutions ont un impact mineur.



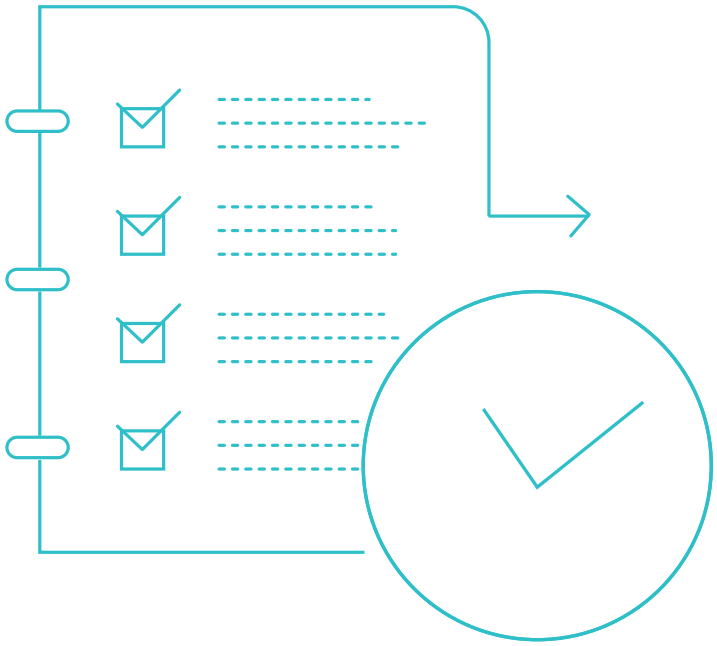
MESURE DE LA VERSION 2022	INTITULÉ	MESURE(S) CORRESPONDANTES DANS LA VERSION 2017	ANALYSE DE L'ÉVOLUTION
5.16	Gestion des identités	09.2.1	La mesure liée aux enregistrements et désinscriptions des utilisateurs est étoffée pour prendre en compte le cycle de vie des identités incluant notamment les entités non-humaines.
5.29	Sécurité de l'information durant les perturbations	17.1.1, 17.1.2, 17.1.3	Les mesures liées à la continuité de la sécurité de l'information ont été beaucoup simplifiées. Seule la planification de la continuité de la sécurité est clairement mentionnée. Néanmoins les actions de surveillance et d'amélioration en lien avec cette planification sont traitées dans l'ISO/IEC 27002.
6.4	Processus disciplinaire	07.2.3	La mesure liée au processus disciplinaire concerne dorénavant les parties intéressées pertinentes en plus du personnel.
7.1	Périmètres de sécurité physique	11.1.1	Des périmètres de sécurité doivent également être définis pour les zones contenant des informations non sensibles.
7.2	Entrée physique	11.1.2, 11.1.6	Simplification et suppression de la précision du contrôle à mettre en œuvre pour les zones de livraisons. Cette précision est toujours incluse dans l'ISO/IEC 27002.
8.1	Terminaux finaux des utilisateurs	06.2.1, 11.2.8	Les mesures liées à la protection des appareils mobiles et aux matériels laissés sans surveillance sont étoffées pour considérer la protection complète de tous les terminaux dont les postes de travail.
8.4	Accès au code source	09.4.5	Extension de la mesure existante aux outils de développement et aux librairies logiciels en supplément du code source.
8.29	Tests de sécurité et acceptation lors des développements	14.2.8, 14.2.9	Par mesure de simplification, les tests de sécurité et de conformité sont tous considérés comme des tests de sécurité.
8.32	Gestion des changements	12.1.2, 14.2.2, 14.2.3, 14.2.4	Les mesures en lien avec les changements du système d'information ont été synthétisées. Les précisions concernant les progiciels et les systèmes d'exploitation ont été supprimées. Cette mesure est à considérer en lien avec la mesure sur la gestion des configurations.

LES ÉVOLUTIONS DANS LE CORPS DE LA NORME

Le corps de la norme (chapitre 4 à 10) compte quelques modifications et reformulations qui auront un impact mineur voire nul pour les organismes déjà certifiés.

Les évolutions suivantes méritent d'être soulignées :

CHAPITRE DE L'ISO/ IEC 27001:2022	ANALYSE DE L'ÉVOLUTION
6.3 Planification des changements	Il est dorénavant mentionné que les changements dans le SMSI doivent être réalisés de manière planifiée.
8.1 Planification et contrôle opérationnels	L'approche processus dans est renforcée et mise en avant dans les chapitres 4.4 et 8.1, en adéquation avec les autres normes de système de management. Il est également mentionné que des critères doivent être établis pour maîtriser les processus.
9.3 Revue de direction	La revue de direction doit intégrer un nouveau sujet : les changements liés aux besoins et attentes de parties intéressées pertinents pour le SMSI.



→ PRÉPAREZ VOTRE TRANSITION

01 Se procurer la norme ISO/IEC 27001 et si possible la norme ISO/IEC 27002

La norme ISO/IEC 27001:2022 Système de management de la sécurité de l'information – Exigences et la norme ISO/IEC 27002:2022 Mesures de sécurité (guide de bonnes pratiques pour mettre en œuvre l'ISO/IEC 27001) sont disponibles sur www.boutique.afnor.org.
Il est préférable de se procurer les transcriptions en normes françaises des normes internationales: les normes NF EN ISO/IEC 27001 de janvier 2023 et NF EN ISO/IEC 27002 de novembre 2022.

02 S'informer sur les nouveautés introduites par l'ISO/IEC 27001

Vous souhaitez en savoir plus sur cette norme et appréhender ses impacts sur votre démarche actuelle ?

- Assistez à l'une de nos web-conférences (une heure – gratuit) ou visionner son replay : https://afnor.zoom.us/rec/share/XqTcrz7x-Y7_mmL-ZeHJu6XLpfwzeTO-7uC-YPLPGQ8w0jer0UUjvgwjJrfR2whis.nb57y0mljmY85EBY
- Faites le point en une heure avec nos experts sur les grands impacts de cette révision et posez-leur toutes vos questions : certification@afnor.org

03 Se former aux exigences de la norme ISO/IEC 27001

AFNOR Compétences propose des formations pour vous aider à mieux appréhender les points-clés de l'ISO/IEC 27001:2022 :

- ISO/IEC 27001 – Comprendre le référentiel : https://competences.afnor.org/formations/iso-27001
- Auditeur ICA ISO/IEC 27001 : https://competences.afnor.org/formations/auditeur-ica-iso-27001-devenir-auditeur-de-systeme-de-management-de-la-securite-de-linformation
- Lead Implementer ISO/IEC 27001 : https://competences.afnor.org/formations/lead-implementer-iso-27001

04 Se positionner par rapport à l'ISO/IEC 27001:2022

AFNOR Certification propose des prestations intermédiaires pour vous accompagner dans votre mise en conformité ISO/IEC 27001:2022 :

- Visite d'évaluation : https://certification.afnor.org/qualite/visite-d-evaluation

Demandez un exercice à blanc au moment qui vous convient le mieux avant votre audit de certification, pour une préparation optimale et sécurisante. Réalisée par un auditeur compétent, elle vous apporte une vision claire sur vos points forts et vos axes d'amélioration en vue de la certification.

Cette prestation convient aux certifiés qui sont en transition et également aux non-certifiés qui souhaitent s'engager dans une démarche de certification.

- Focus Cybersécurité (pour les non-certifiés ISO/IEC 27001) : https://certification.afnor.org/numerique/focus-cybersecurite

Pour les organismes qui initient leur mise en conformité ISO/IEC 27001, nous mettons à disposition une grille d'auto-évaluation focalisée sur les points clés de l'ISO/IEC 27001 en 44 questions, avec remise d'un rapport complet et personnalisé. Il est également possible pour les organismes de faire évaluer son auto-évaluation par un auditeur compétent.

05 Déterminer le bon moment pour passer à l'ISO/IEC 27001:2022

Au vu des évolutions de l'ISO/IEC 27001:2022, les organismes devront adapter leur SMSI en prenant notamment en compte les 11 nouvelles mesures de sécurité. Parmi la documentation charnière du SMSI, la déclaration d'applicabilité (DDA) et le plan de traitement des risques devront être revus.

Une fois que leur SMSI aura intégré les évolutions de l'ISO/IEC 27001:2022, plusieurs possibilités s'offrent aux organismes certifiés pour réaliser leur audit de transition :

- Réaliser la transition pendant leur prochain audit de renouvellement. Dans ce cas, l'audit des évolutions sera réalisé sans allongement de la durée d'audit classiquement prévue.
- Réaliser la transition pendant leur prochain audit de suivi. Dans ce cas, il sera nécessaire d'augmenter la durée d'audit prévue. L'organisme certifié devra prendre contact en ce sens avec le commercial en charge de son dossier pour gérer les modalités contractuelles.
- Réaliser un audit complémentaire hors cycle classique de certification pour transiter au plus tôt. L'organisme certifié devra prendre contact en ce sens avec le commercial en charge de son dossier pour gérer les modalités contractuelles.

afaq
ISO/IEC 27001
Sécurité de l'information
AFNOR CERTIFICATION

Retrouvez les solutions AFNOR Certification sur :

certification.afnor.org

Retrouvez les offres du Groupe AFNOR :

www.afnor.org

Contactez-nous :

01 41 62 80 11
certification@afnor.org

S2212006 Groupe AFNOR – Septembre 2024 _Graphisme : gayacom@orange.fr

afnor CERTIFICATION

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis cedex - France
Tél. : +33 (0)1 41 62 80 11 - Fax. : +33 (0)1 49 17 90 00