étude

ISO 27001 : VINGT ANS D'ENGAGEMENT AU SERVICE DE LA SÉCURITÉ DE L'INFORMATION

OCTOBRE 2025

CLUB 27001

afnor GROUPE

SOMMAIRE

ÉDITO
CONFIANCE ET INNOVATION

© Havas

Emmanuel Garnier,
président du Club 27001

© Arthur Enard

Julien Nizri,
directeur général d'AFNOR Certification, président du collège International de la Fédération française de cybersécurité

Déjà vingt ans que la norme volontaire ISO/IEC 27001 a été publiée ! Trois versions sont sorties : ce n'est pas une norme figée, mais un langage vivant. C'est aussi devenu un standard incontournable.

Je suis ravi, en tant que président du Club 27001, d'apporter mon éclairage. Le Club 27001, c'est avant tout une aventure humaine. Il deviendra une association en 2008 après avoir réalisé quelques conférences sur la base de la British Standard BS 7799 et rapidement l'ISO 27001 (après quelques modifications du chapitre 2 de la BS 7799).

Le Club 27001, c'est aussi une conférence annuelle et des groupes de travail, un livre blanc de benchmark des outils d'aide à la gestion des SMSI, les réglementations en vigueur et à venir comme le GT NIS 2, les bonnes pratiques de terrain comme le GT ISO 27002 et des pratiques issues des autres normes et standards comme le GT processus.

À l'occasion de cet anniversaire, l'étude du groupe AFNOR dresse un état des lieux éclairant. Elle met en lumière les thématiques ayant généré le plus de non-conformités et de points sensibles au niveau du système de management de la sécurité de l'information (SMSI), et aussi pour les mesures de sécurité.

Cette étude est diffusée en octobre 2025, en plein Cybermois : une opportunité de calendrier qui me permet de souligner, en termes d'appropriation de la norme dans le tissu économique, que les points forts sont le leadership, l'engagement et la sensibilisation.

Les vingt prochaines années s'écriront sans doute moins en termes de conformité, d'exigences. Et si au fond la véritable maturité consistait à faire de la cybersécurité un réflexe de confiance et un moteur d'innovation ?

Cela fait maintenant vingt ans que la norme ISO/IEC 27001 s'est imposée comme un référentiel mondial pour les responsables de la sécurité des systèmes d'information (RSSI), et que sa certification constitue un marqueur de confiance pour les clients finals. Dans un paysage de menaces en évolution continue, souvent sous-estimées, disposer d'un référentiel reconnu internationalement est devenu indispensable.

La certification ISO/IEC 27001 offre un socle de maîtrise des risques. Tous nos certifiés le disent : mieux préparés, ils préviennent, détectent, remédient et restaurent plus efficacement. Et ils progressent dans la durée : un système de management ISO/IEC 27001, c'est l'amélioration continue. Victime d'une cyberattaque en 2021, le groupe AFNOR est bien placé pour le savoir.

À la lumière des grands enseignements tirés des rapports de nos auditeurs et auditrices, et alors que la réglementation européenne se renforce avec NIS 2, je souhaite vingt nouvelles belles années à la norme ISO/IEC 27001 et à la certification qui l'accompagne, pour toujours tirer les pratiques vers le haut, favoriser la confiance et structurer le marché selon des repères exigeants.

Retrouver notre dossier complet sur :
www.afnor.org/numerique/cybersecurite

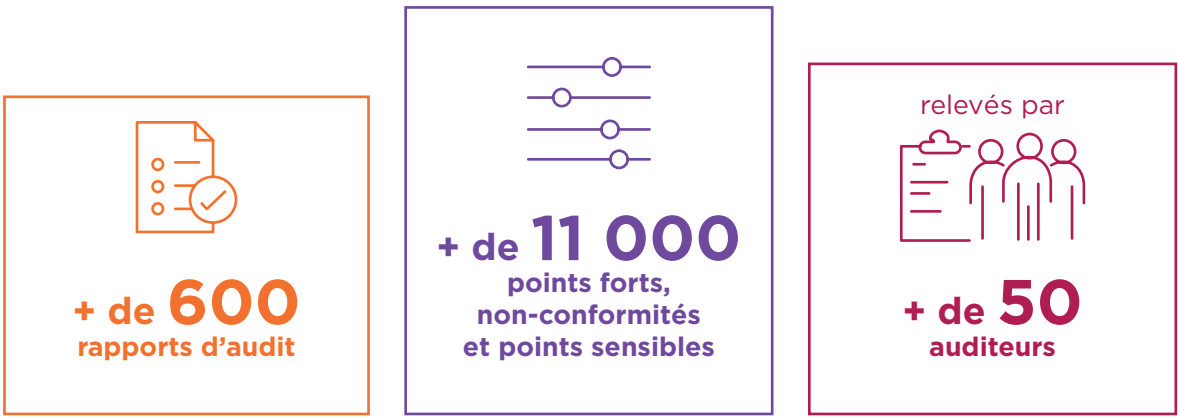
CONTEXTE DE L'ÉTUDE

Depuis sa première publication en 2005, la norme volontaire ISO/IEC 27001 a évolué pour prendre en compte l'évolution des pratiques et conserver une position de démarche de référence pour les organisations désireuses d'établir une démarche efficace de gestion de la sécurité de l'information.

Cette norme internationale propose un ensemble de mesures portant à la fois sur des dispositions organisationnelles et des éléments techniques. Cette vision à 360 degrés de la sécurité peut rendre son application au sein des organismes parfois complexe.

Cette étude vise à identifier les principales tendances concernant les défis rencontrés par les organismes, ainsi que les domaines dans lesquels ils excellent. Il s'agit d'un retour d'expérience fondé sur les constats réels constatés lors des audits de certification ISO 27001 : non-conformités (NC), points sensibles (PS) et points forts (PF).

Cette analyse repose sur les constats issus des audits réalisés selon la version 2022 de la norme ISO 27001 par AFNOR Certification, soit au total :



N.B. : par commodité, nous simplifierons le libellé de la norme « NF EN ISO/IEC 27001 » en France en « ISO 27001 ».

L'ISO 27001, UN OUTIL COMPLET AU SERVICE DES SMSI

Une histoire qui commence en 2005

L'ISO/IEC 27001 est une norme internationale qui définit les exigences relatives à un système de management de la sécurité de l'information (SMSI). Elle fournit un cadre structuré permettant aux organisations de gérer la sécurité de leurs informations de manière efficace et pérenne. Son objectif principal est de protéger la confidentialité, l'intégrité et la disponibilité des données, en identifiant, évaluant et traitant les risques associés à la sécurité de l'information.

2005

ISO/IEC 27001:2005
Première version publiée, elle établit les exigences pour un SMSI et a introduit le concept de gestion des risques. Elle s'appuie sur les travaux britanniques sur la norme **BS 7799**

2013

ISO/IEC 27001:2013
Révision majeure, cette version a apporté des modifications significatives, notamment :

- l'intégration de la **structure de haut niveau (HLS)** pour faciliter l'intégration avec d'autres normes de systèmes de management,
- une mise à jour des **mesures de sécurité**,
- un renforcement de la prise en compte du **contexte et des parties intéressées**.

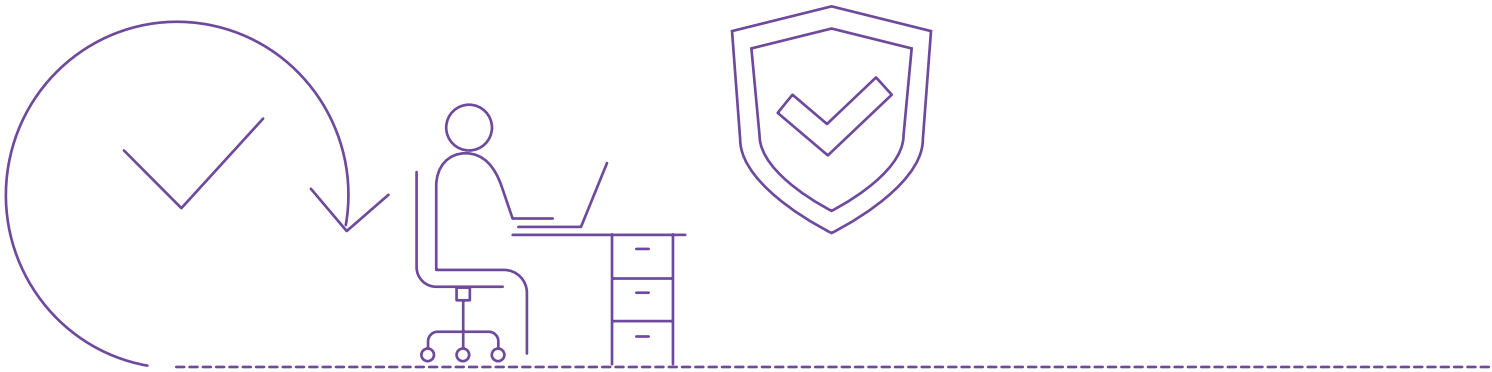
2022

ISO/IEC 27001:2022
Révision majeure, cette version a apporté des modifications significatives, notamment :

- mise à jour des **mesures de sécurité** pour refléter les nouvelles menaces et technologies,
- clarification des exigences relatives à la **gestion des risques et à l'évaluation des performances** du SMSI.

2024

ISO/IEC 27001: 2024/Amd 1
Ajout des exigences pour que les organisations prennent en compte les impacts des **changements climatiques** sur leurs SMSI.



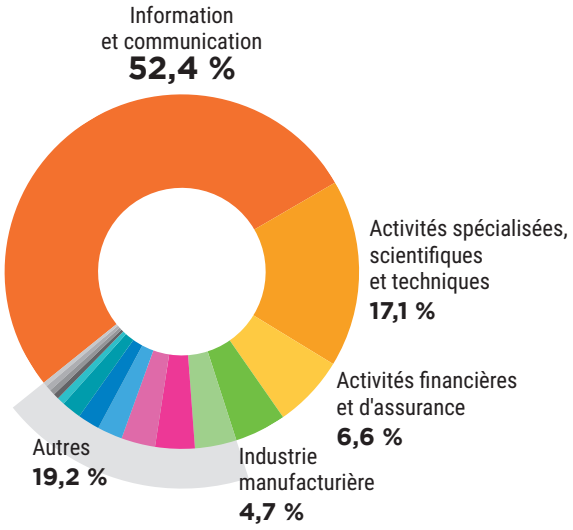
Une norme au sein d'une famille complète et cohérente

La famille des normes ISO 27x offre un cadre complet et cohérent pour la gestion de la sécurité de l'information, abordant divers aspects tels que la mise en œuvre de systèmes de management, la gestion des risques, et la protection des données personnelles. Ces normes volontaires permettent aux organisations de renforcer leur posture de sécurité, d'assurer la conformité réglementaire et de promouvoir des pratiques de sécurité efficaces. En intégrant des lignes directrices spécifiques pour des contextes variés, comme le *cloud computing* et les télécommunications, elles répondent aux besoins diversifiés des organisations. Voici une sélection des plus utilisées :

Une norme qui intéresse des secteurs d'activité divers

L'ISO 27001 est une norme applicable à toutes les organisations, indépendamment de leur secteur d'activité ou de leur taille, ce qui en fait un outil précieux pour renforcer la sécurité de l'information. Une étude menée par le groupe AFNOR en 2019 a révélé que 80 % des organisations certifiées appartenaient au secteur des **services et des technologies de l'information**. Bien que ce secteur demeure le principal concerné, sa part a diminué, pour représenter désormais moins de 70 % des certificats, témoignant d'une diversification croissante des secteurs impliqués. Nous constatons notamment une montée en puissance des **secteurs financiers** et de l'**industrie manufacturière** parmi les organismes certifiés.

De plus, l'ensemble des secteurs jugés hautement critiques, tels que définis par la directive européenne NIS 2, est représenté parmi les organisations certifiées. Ces dernières disposent ainsi d'une base solide pour mettre en œuvre les exigences de cette nouvelle réglementation et renforcer leurs mesures de sécurité existantes, en s'inscrivant dans une dynamique d'amélioration continue déjà établie.



RÉPARTITION DES ORGANISATIONS CERTIFIÉES PAR SECTEUR D'ACTIVITÉ

Secteurs d'activité	%	Concerné par NIS 2
Information et communication	52,4	oui
Activités spécialisées, scientifiques et techniques	17,1	oui
Activités financières et d'assurance	6,6	oui
Industrie manufacturière	4,7	oui
Commerce ; réparation d'automobiles et de motocycles	3,8	non
Activités de services administratifs et de soutien	3,6	non
Santé humaine et action sociale	3,1	oui
Construction	2,3	non
Administration publique	2,0	oui
Transports et entreposage	1,8	oui
Activités immobilières	0,7	non
Production et distribution d'eau ; assainissement, gestion des déchets et dépollution	0,5	oui
Enseignement	0,5	non
Autres activités de services	0,5	non
Production et distribution d'électricité, de gaz, de vapeur et d'air conditionné	0,4	oui

Ce que dit la directive européenne NIS 2

Prolongement de la directive NIS 1 du 6 juillet 2016, cette directive du 27 décembre 2022 définit des secteurs hautement critiques (annexe I) en reprenant le sigle NIS (*Network and Information Security*) :

- Administrations publiques
- Eaux potables et usées
- Énergies
- Espace
- Gestion des technologies de l'information et de la communication
- Infrastructures des marchés financiers
- Infrastructures numériques
- Santé
- Secteur bancaire
- Transports

Et d'autres secteurs critiques (annexe II) :

- Fabrication, production et distribution de produits chimiques
- Fournisseurs numériques
- Gestion des déchets
- Industries manufacturières
- Production, transformation et distribution de denrées alimentaires
- Recherche
- Services postaux et d'expéditions

Pour déterminer l'applicabilité de NIS 2, le secteur d'activité seul ne suffit pas, l'ensemble des critères est disponible sur le site : https://monespacenis2.cyber.gouv.fr

Bien que les secteurs d'activité se diversifient, les certifications ISO 27001 concernent encore principalement les **équipes en charge des systèmes d'information**, comme le montrent les activités formulées sur les certificats. Cela dit, un SMSI s'étend souvent au-delà de son périmètre de certification pour faire bénéficier à la structure certifiée des bonnes pratiques mises en œuvre.

La transition version 2022

L'année 2025 représente un tournant important, avec la fin de la période de transition vers la nouvelle version de la norme ISO 27001. Tous les organismes certifiés doivent obtenir le maintien ou le renouvellement de leur certification selon la version 2022 de la norme, et cela, au plus tard le 31 octobre 2025. Cette mise à jour introduit 11 nouvelles mesures qui ont parfois suscité des défis lors de leur mise en œuvre. Voici ces mesures, classées par ordre des difficultés rencontrées :

Chapitre	Mesure	Niveau de difficulté rencontré	Observation
A.8.12	Prévention des fuites de données	Dans le top 10 des difficultés	
A.8.10	Suppression des informations		
A.5.30	Préparation des TIC pour la continuité d'activité	1er tiers du classement des mesures ayant posé le plus de difficultés	Dans le top 10 des sujets sur lesquels les organismes se démarquent
A.8.9	Gestion des configurations		
A.8.11	Masquage des données		
A.5.23	Sécurité de l'information dans l'utilisation des services cloud		
A.7.4	Surveillance de la sécurité physique		
A.5.7	Renseignement sur les menaces		Dans le top 10 des sujets sur lesquels les organismes se démarquent
A.8.28	Codage sécurisé	2e tiers du classement des mesures ayant posé le plus de difficultés	
A.8.23	Filtrage web		
A.8.16	Surveillance des activités		

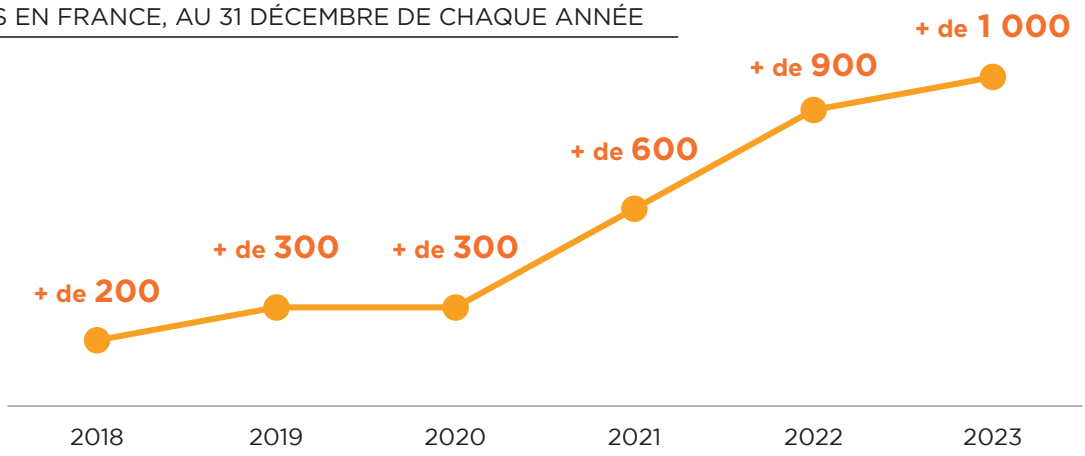
Une progression de la certification

La certification du système de management de la sécurité de l'information peut générer des **bénéfices internes et externes**. En interne, il s'agit d'une démarche d'amélioration continue des pratiques et l'entretien d'une culture de la sécurité qui permet de protéger les actifs informationnels de l'organisation. Les audits réguliers permettent d'identifier des pistes d'amélioration.

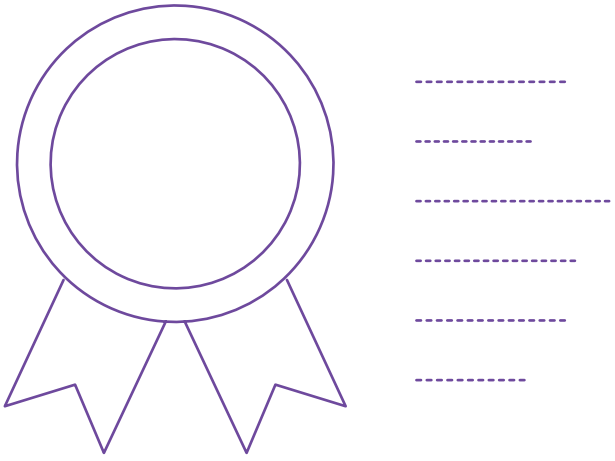
En adoptant l'ISO 27001, les organisations peuvent démontrer leur engagement envers la sécurité de l'information, renforcer la confiance au sein de leur écosystème, et se conformer aux exigences légales et réglementaires en matière de protection de l'information. Notamment, les assureurs peuvent prendre en compte cette démarche comme une **logique de prévention des risques** avant de décider de couvrir ou non certains risques. Plusieurs autorités de contrôle ont également des positions globalement bienveillantes par rapport à cette certification. Enfin, cette norme est utilisée dans le monde entier et **traverse donc les frontières** et les réglementations nationales. Enfin, elle sert de référence à plusieurs autres démarches spécifiques sectorielles.

De plus en plus d'organismes ont saisi l'opportunité. Les chiffres fournis par l'ISO Survey permettent d'observer une adhésion à la démarche de certification en France depuis 2018. Cette période est notamment marquée par le renforcement des exigences réglementaires pour l'hébergement des données de santé (HDS) et pour la protection des données personnelles (RGPD).

LA PROGRESSION DU NOMBRE DE CERTIFICATS ISO 27001 ACTIFS EN FRANCE, AU 31 DÉCEMBRE DE CHAQUE ANNÉE



Source : ISO Survey, arrondis



LE SMSI, POUR UNE GESTION GLOBALE ET PÉRENNE DE **LA SÉCURITÉ DE L'INFORMATION**

Le corps de la norme ISO 27001 décrit les exigences pour établir un système de management de la sécurité de l'information (SMSI). L'accent est mis sur la compréhension du contexte organisationnel, l'engagement de la direction, la planification des actions face aux risques, opportunités et objectifs. Ces chapitres, l'évaluation des performances et l'amélioration continue, garantissent ainsi une approche systématique pour protéger les informations sensibles.

Top 3 des thématiques ayant généré le plus de non-conformités (NC) et points sensibles (PS)

6.1. Actions à mettre en œuvre face aux risques et opportunités	669	15,3 %
7.5. Informations documentées	288	6,6 %
9.3. Revue de direction	224	5,1 %

Top 3 des thématiques ayant généré le plus de points forts (PF)

5.1. Leadership et engagement	157	13,6 %
8.1. Planification et contrôle opérationnels	61	5,3 %
7.2. Compétences	57	4,9 %

Les thématiques qui ont posé le plus de difficultés

On peut regrouper en trois catégories les points que les rapports d'audit identifient comme ayant posé le plus de difficultés.

Actions à mettre en œuvre face aux risques et opportunités

- **Analyses de risques incomplètes :** actifs manquants, scénarios absents, nouveaux risques liés à l'IA non identifiés conduisent à un risque pour l'organisme de baser ses mesures sur une vision qui n'est pas représentative de l'actualité.
- **Plans de traitement des risques :** l'absence de leur validation par les propriétaires concernés, de suivi de l'efficacité des actions engagées et d'évaluation des risques résiduels remettent en question la maîtrise des risques par l'organisme.

- **Saisie des opportunités :** les opportunités ne sont pas systématiquement identifiées ou exploitées, les organismes se concentrant sur les risques négatifs ; cela peut freiner la dynamique d'amélioration continue du SMSI.

Informations documentées

- **Gestion documentaire :** mise à jour irrégulière, absence de versioning, documents obsolètes ou non approuvés, autant de problématiques pouvant entraîner de la confusion au sein du SMSI.
- **Classification et sensibilité des documents :** les critères de classification mal définis ou non appliqués peuvent compromettre le niveau de protection appliqué à ces actifs.
- **Stockage et accessibilité :** multiplication des plateformes et des copies de document, l'accès à la version la plus récente et validée est complexe, générant des risques de confusion et d'utilisation de documents non valides.

Revue de direction

- **Contenu de la revue :** absence de retours des parties intéressées, des modifications d'enjeux internes ou externes, des résultats d'audits peut conduire à une évaluation incomplète de la performance et de l'efficacité du SMSI.
- **Suivi des objectifs :** le manque de mesures ou d'indicateurs pour évaluer l'atteinte des objectifs peut compromettre la capacité de l'organisation à piloter l'efficacité de son SMSI.
- **Décisions et actions issues des revues de direction :** le manque de formalisation d'actions suite aux discussions peut réduire l'engagement de la direction et l'efficacité des actions d'amélioration continue.

Les thématiques sur lesquelles les audités se démarquent

On peut également regrouper en trois catégories les points que les rapports d'audit identifient comme ayant permis de se démarquer.

Leadership et engagement

- **Leadership fort :** les dirigeants des organismes audités sont activement impliqués dans la définition des objectifs, la mise en place de politiques de sécurité, et le soutien des initiatives de sécurité.
- **Stratégie globale :** la sécurité de l'information est identifiée comme un axe stratégique majeur, alignée avec les objectifs de l'organisation.
- **Implication des collaborateurs :** les démarches de sécurité sont déployées dans un esprit collaboratif et participatif, responsabilisant ainsi les collaborateurs et les intégrant dans les processus.

Compétences

- **Gestion des compétences :** des matrices de compétences détaillées et des outils de gestion des compétences permettent de s'assurer que les compétences des collaborateurs sont alignées avec les besoins de l'organisme et les exigences de sécurité de l'information.
- **Implication des équipes :** forte implication des équipes qui se traduit par une responsabilisation accrue des collaborateurs et une culture organisationnelle qui valorise la sécurité de l'information.
- **La technologie au service de la gestion des compétences :** des plateformes de gestion des compétences, des outils de suivi des formations, et des systèmes de gestion des ressources humaines soutiennent ce processus.

Planification et contrôle opérationnels

- **Contrôles opérationnels :** bien planifiés et exécutés, avec des dispositifs en place pour suivre et évaluer les actions.
- **Évaluation des performances :** les organismes démontrent une capacité à exploiter les résultats de l'activité de contrôle au service de l'amélioration continue.
- **La technologie au service des contrôles :** des plateformes permettent d'automatiser et centraliser les contrôles, assurant une traçabilité et une efficacité accrues.

LE SMSI, L'ALLIANCE
DES MESURES TECHNIQUES ET ORGANISATIONNELLES

L'annexe A est le cœur sécurité de l'ISO 27001. Elle se compose de 93 mesures de sécurité regroupées en quatre catégories principales : mesures organisationnelles, mesures applicables aux personnes, sécurité physique et mesures technologiques.

Top 3 des thématiques ayant généré le plus de non-conformités (NC) et points sensibles (PS)

A.5.9. Inventaire des informations et autres actifs associés	264	4,9 %
A.5.34. Protection de la vie privée et des données à caractère personnel (DCP)	251	4,6 %
A.5.18. Droits d'accès	151	4,6 %

Top 3 des thématiques ayant généré le plus de points forts (PF)

A.5.31. Exigences légales, statutaires, réglementaires et contractuelles	49	4,0 %
A.8.32. Gestion des changements	38	3,1 %
A.6.3. Sensibilisation, enseignement et formation en sécurité de l'information	37	3,0 %

Les thématiques qui ont posé le plus de difficultés

On peut regrouper en trois catégories les points que les rapports d'audit identifient comme ayant posé le plus de difficultés.

Les inventaires d'actifs

- **Inventaires des actifs :** inventaires non exhaustifs, non mis à jour, incohérence des fichiers d'inventaire ou encore absence de revue ou de contrôle. Ces situations entraînent un manque de visibilité des organismes sur les valeurs à protéger.
- **Propriétaires d'actifs :** non identifiés ou avec des responsabilités non clairement attribuées.
- Besoins de sécurité : l'évaluation des besoins en confidentialité, intégrité, disponibilité n'étant pas correctement effectuée, les mesures de sécurité pourraient ne pas être suffisantes.

La protection des données à caractère personnel

- **Registre de traitement :** absence de certains traitements, non-distinction entre les rôles de responsable de traitement et de sous-traitant, manque de détails sur les durées de conservation des données. Ces trois points préviennent l'organisme d'avoir une vision sur ce qu'il est nécessaire de protéger.

- **Vidéoprotection :** information des personnes concernées non réalisée, durée de conservation excessive, droit d'accès aux images trop étendus rendent la mesure non conforme.
- **Gestion des visiteurs :** manque d'information des visiteurs sur le traitement et leurs droits, défaut de sécurisation des informations personnelles collectées mettent en défaut la conformité de ce traitement.

Les droits d'accès

- **Gestion des comptes :** comptes inactifs non désactivés ou non supprimés, comptes administrateurs et comptes à privilèges non maîtrisés, comptes génériques et comptes de service non contrôlés, sont autant de vecteurs facilitant une possible intrusion.
- **Revue des droits :** absence de planification, de documentation des résultats, et/ou de suivi des actions de remédiation, ce qui génère des risques d'accès non autorisés aux informations sensibles.
- **Séparation des tâches et des rôles :** les mêmes personnes sont parfois responsables de la vérification et de l'analyse des droits d'accès, ce qui peut conduire à des conflits d'intérêts et à des erreurs non détectées.

Les thématiques sur lesquelles les audités se démarquent

On peut également regrouper en trois catégories les points que les rapports d'audit identifient comme ayant permis de se démarquer.

Exigences légales et réglementaires

- **Veille :** utilisation de plateformes spécialisées, participation à des groupes de travail et des clubs, collaboration avec des experts permettent d'assurer une veille efficace et à jour.
- **Participation à des clubs :** la participation active à des clubs, associations, ou instances nationales et internationales permettent d'anticiper les changements et de préparer des plans d'action en conséquence.
- **Intégration de la conformité dans les processus :** La conformité légale et réglementaire en sécurité de l'information est directement intégrée dans divers processus (ex : commercial, gestion des fournisseurs, ressources humaines).

Gestion des changements

- **Processus de gestion des changements :** les processus sont formalisés, avec des documents de référence, des procédures si nécessaire. Des normes ou standards reconnus sont utilisés pour baser les processus.
- **Comités des changements :** ces comités incluent des représentants de la sécurité, de la production, et d'autres parties prenantes clés. Ils jouent un rôle crucial dans l'évaluation, la validation, et le suivi des changements.
- **Outillage de la gestion des changements :** les outils (notamment les outils « de *ticketing* ») facilitent la traçabilité, la communication, et l'amélioration continue.

Sensibilisation

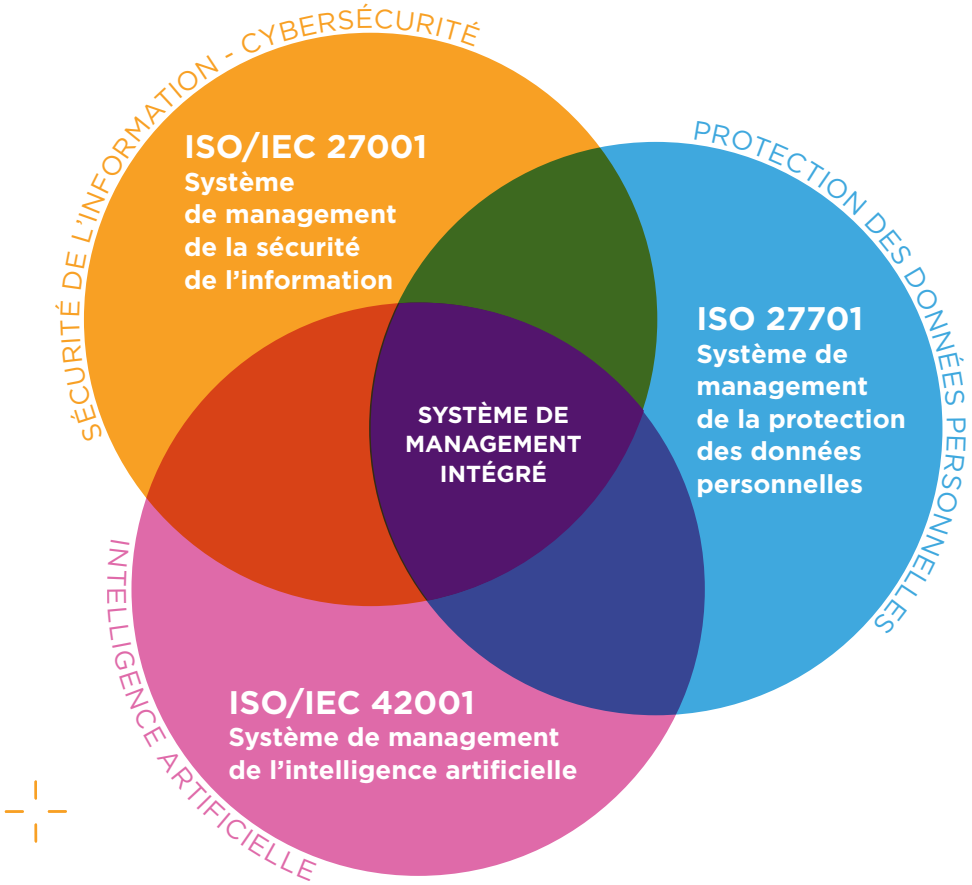
- **Processus d'intégration** *(onboarding)* **:** sont bien structurés et incluent des éléments de référence comme la présence de la sécurité de l'information dans les livrets d'accueil, des présentations de chartes, et des sessions de formation initiales.
- **Moyens de sensibilisation variés :** *e-learning*, quiz, campagnes de *phishing*, intégration dans des instances de l'organisation. Les moyens technologiques et interactifs sont privilégiés.
- **Approche contextualisée :** les contenus sont adaptés aux besoins spécifiques de l'organisme et des collaborateurs. Cela inclut l'implication active des équipes en charge de la sécurité et l'utilisation de retours d'expérience pour améliorer continuellement les programmes de sensibilisation.

VERS UN SYSTÈME DE **MANAGEMENT DE LA CONFIANCE NUMÉRIQUE ?**

Dans un contexte de transformation et de transition numérique, instaurer la confiance au sein du tissu économique est primordial. Cela nécessite non seulement une gestion et une protection efficaces des données, mais aussi une maîtrise de **l'impact environnemental des technologies** et un engagement pour un **impact social positif**. En agissant de la sorte, les structures peuvent promouvoir une adoption responsable et durable du numérique.

La sécurité de l'information représente l'un des piliers d'un système de management plus large axé sur la confiance numérique. Un système de management intégré permet d'harmoniser et de coordonner les divers processus et mesures au sein d'une organisation, améliorant ainsi son efficacité opérationnelle. Ce système de management de la confiance numérique facilite la gestion des risques en offrant une vue d'ensemble des enjeux liés à la sécurité de l'information, à la protection des données personnelles et à l'utilisation de nouvelles technologies telles que l'intelligence artificielle, permettant ainsi une prise de décision plus éclairée.

Cette approche favorise également la **conformité réglementaire** et renforce la **satisfaction des parties prenantes** en garantissant une gestion cohérente et durable des activités.



LE GROUPE AFNOR

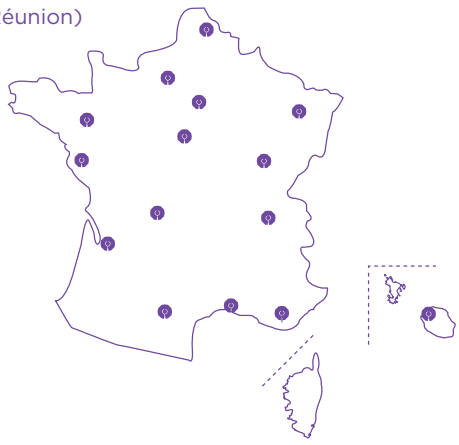
L'association AFNOR, chargée d'une mission d'intérêt général, constitue avec ses filiales un groupe international au service du développement durable. Le groupe de 1 318 collaborateurs, 37 implantations dans le monde et 70 000 clients, conçoit des solutions fondées sur les normes volontaires, sources de progrès et de confiance depuis 1926. Sa vocation est d'accompagner les organisations et les personnes pour diffuser cette confiance. Cet accompagnement s'effectue au travers de cinq métiers : la normalisation, l'édition, la formation, la certification et l'intermédiation avec des experts des normes.

LE CLUB 27001

Le Club 27001 est une association loi de 1901 qui rassemble les acteurs et passionnés des normes de la série ISO 27000, relatives à la gestion de la sécurité de l'information. Son objectif est de créer un espace d'échanges et de réflexion, favorisant la collaboration entre intervenants issus d'administrations, d'entreprises, d'universités et d'associations européennes. Des groupes de travail sont actifs dans plusieurs villes de France, permettant aux membres de se rencontrer pour discuter des normes ISO 27000. Ces rencontres, ouvertes à tous, incluent des présentations et des discussions, offrant un cadre dynamique pour le partage d'expériences.

Depuis 2007, le Club organise une conférence annuelle, point de rencontre essentiel pour les professionnels, permettant de partager des retours d'expérience et d'explorer l'évolution des normes. Membre du Campus Cyber, le Club 27001 renforce son réseau et son influence, contribuant à l'amélioration des pratiques de sécurité de l'information et jouant un rôle clé dans la promotion des normes ISO 27000.

Bordeaux
Dijon
Le Port (La Réunion)
Lille
Lyon
Marseille
Montpellier
Nancy
Nantes
Orléans
Paris
Rennes
Rouen
Toulouse



Contact :
Groupe AFNOR
11, rue Francis de Pressensé
93571 La Plaine Saint-Denis cedex
01 41 62 80 00

www.afnor.org