ISO/IEC 27001:2022 + Amd 1:2024 Systèmes de management de la sécurité de l'information (SMSI)

Sécurité de l'information, SMSI, certifiable dans le monde entier

181 exigences. Cette norme peut être certifiée par un organisme accrédité. Version de 07/2026.

L'ISO/IEC 27001 fixe les exigences relatives à un système de management de la sécurité de l'information : fondé sur le risque, documenté et à l'efficacité démontrable. Une évaluation par rapport à cette norme est un audit de certification accrédité en deux étapes (revue documentaire, puis revue d'efficacité sur site), suivi d'audits de surveillance annuels et d'une recertification au bout de trois ans.

Entreprise	Date	Établi par

4 Contexte de l'organisme 8

4.1-1 Les enjeux externes et internes qui influent sur la capacité de l'organisme à atteindre les résultats attendus du SMSI sont déterminés et tenus à jour.

Comment le prouver: Se démontre au moyen d'une analyse de contexte, sous forme de document autonome ou de section du manuel du SMSI : environnement de marché, situation des clients et des contrats, cadre juridique (RGPD, NIS2), pile technologique, effectif, dépendance vis-à-vis des fournisseurs cloud. Pour les petits organismes, un tableau d'une page avec une date et un cycle de revue suffit, à condition que la revue de direction montre qu'il est réellement mis à jour.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

4.1-2 L'organisme a déterminé si le changement climatique constitue pour lui un enjeu pertinent. La détermination est justifiée, que la réponse soit affirmative ou négative.

Comment le prouver: Cette exigence a été introduite par l'Amd 1:2024 et les auditeurs la demandent spécifiquement. Prévoyez une ligne dédiée dans l'analyse de contexte : périodes de forte chaleur affectant les salles serveurs et la disponibilité, phénomènes météorologiques extrêmes affectant les centres de données des fournisseurs cloud, stabilité du réseau électrique. Un résultat justifié de non pertinent est acceptable, une entrée manquante ne l'est pas.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

4.2-1 Les parties intéressées pertinentes pour le SMSI sont déterminées.

Comment le prouver: Liste des parties prenantes couvrant les clients, le personnel, les sous-traitants et sous-traitants ultérieurs, les autorités de contrôle, les assureurs, l'organisme de certification et les actionnaires. Dans les petits organismes, un tableau avec la partie prenante, son attente et la source de cette attente suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

4.2-2 Les exigences pertinentes de ces parties intéressées sont déterminées, y compris toute exigence liée au changement climatique.

Comment le prouver: Pour chaque partie prenante, indiquez la source concrète : clause contractuelle, accord de sous-traitance des données, questionnaire client, obligation légale. L'Amd 1:2024 ajoute une note selon laquelle les parties intéressées peuvent avoir des exigences liées au changement climatique. Ce n'est pas une exigence distincte en tant que telle, mais les auditeurs la soulèvent régulièrement, par exemple des questions de durabilité dans l'audit fournisseur d'un client important. Une ligne dans le tableau des parties prenantes avec le résultat, y compris aucune de ce type, suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

4.2-3 Il est décidé et traçable lesquelles de ces exigences sont traitées par le SMSI.

Comment le prouver: Ajoutez une colonne au tableau des parties prenantes renvoyant à la règle qui traite l'exigence (politique, mesure, annexe contractuelle). Cela montre que les exigences n'ont pas seulement été recensées, mais réellement traitées.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

4.3-1 **Le domaine d'application du SMSI est déterminé et tient compte des enjeux du point 4.1, des exigences du point 4.2 ainsi que des interfaces et dépendances avec les activités réalisées par des tiers.**

Comment le prouver: Le domaine d'application nomme les sites, unités organisationnelles, produits, systèmes et limites réseau. Les parties externalisées (hébergement, prestataires de paiement, support) sont décrites comme des interfaces avec une frontière de responsabilité claire. Un domaine d'application artificiellement restreint qui exclut des processus centraux est rejeté par les organismes de certification.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

4.3-2 **Le domaine d'application est disponible sous forme d'information documentée et indique sans ambiguïté les limites du SMSI.** Document

Comment le prouver: Un document de domaine d'application approuvé avec version, date et validation par la direction générale. Sa formulation exacte apparaîtra ensuite sur le certificat, il convient donc de la rédiger avec précision et de manière citable publiquement.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

4.4-1 **Le SMSI, y compris les processus nécessaires et leurs interactions, est établi, mis en œuvre, tenu à jour et amélioré en continu.**

Comment le prouver: Une cartographie ou une liste des processus reliant la gestion des risques, la gestion des incidents, la gestion des changements, l'audit et la revue de direction, avec propriétaires et fréquence. La preuve vivante compte plus que le schéma : tickets, comptes rendus, entrées d'agenda.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5 Leadership 8

5.1-1 **La direction générale assume la responsabilité de l'efficacité du SMSI et veille à ce que la politique et les objectifs soient établis et compatibles avec l'orientation stratégique.**

Comment le prouver: Les preuves comprennent les approbations signées de la politique, du domaine d'application et de la Déclaration d'applicabilité, les comptes rendus de revue de direction et les décisions budgétaires documentées. Dans les très petits organismes, la direction générale est souvent la même personne que le propriétaire du SMSI, ce qui est acceptable mais doit être indiqué ouvertement dans la définition du rôle.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.1-2 **Les exigences du SMSI sont intégrées aux processus métier et l'importance d'une sécurité de l'information efficace est communiquée.**

Comment le prouver: Se démontre le mieux lorsque la sécurité n'est pas un classeur à part : un critère de sécurité dans la définition de terminé, une vérification de sécurité dans le processus commercial ou d'achat, un point récurrent de sécurité dans les comptes rendus de réunion d'équipe.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.1-3 **La direction fournit les ressources nécessaires, soutient les personnes qui contribuent à l'efficacité du SMSI et promeut l'amélioration continue.**

Comment le prouver: Budget de sécurité approuvé, temps alloué à la formation, recours à des auditeurs externes ou à des testeurs d'intrusion. Un registre d'amélioration ou d'actions comportant des entrées sur plusieurs trimestres démontre une continuité plutôt qu'un effort ponctuel.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.2-1 **Une politique de sécurité de l'information est établie, appropriée à la finalité de l'organisme et fournissant un cadre pour les objectifs de sécurité de l'information.** Document

Comment le prouver: Un document de politique court et approuvé, deux à trois pages suffisent. Il nomme les objectifs de protection, le domaine d'application, les responsabilités et le principe d'une approche fondée sur le risque. Un texte de modèle générique sans lien avec l'activité réelle se remarque négativement lors de l'audit.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.2-2 **La politique inclut un engagement à satisfaire les exigences applicables et un engagement d'amélioration continue du SMSI.** Document

Comment le prouver: Les deux engagements doivent figurer comme des phrases explicites dans la politique, et ils sont lus mot pour mot lors de l'audit de phase 1. Renvoyez en outre aux processus sous-jacents (registre légal, registre d'amélioration).

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.2-3 **La politique est communiquée au sein de l'organisme et mise à disposition des parties intéressées selon les besoins.** Document

Comment le prouver: Preuve via une entrée d'intranet ou de wiki avec obligation de lecture, une liste de vérification d'intégration avec confirmation, ou un résumé publié sur le site web. Une liste de diffusion avec accusés de réception est la preuve solide la plus simple.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.3-1 **Les responsabilités et autorités pour les rôles pertinents en matière de sécurité sont attribuées et communiquées au sein de l'organisme.**

Comment le prouver: Une matrice de rôles (RACI) couvrant le propriétaire du SMSI, les propriétaires de risques, les propriétaires d'actifs, le coordinateur des incidents et le contact protection des données. Dans les équipes unipersonnelles ou très petites, attribuez chaque rôle à une personne nommée et documentez ouvertement le cumul de rôles qui en résulte plutôt que de le dissimuler.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

5.3-2 **L'autorité pour garantir que le SMSI est conforme à la norme et pour rendre compte de la performance du SMSI à la direction générale est attribuée à un rôle.**

Comment le prouver: Une lettre de nomination ou une description de rôle pour le propriétaire du SMSI avec une ligne de reporting explicite vers la direction. Cette ligne de reporting doit être réellement attestée par les comptes rendus de revue de direction.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6 Planification 21

6.1.1-1 **En partant des enjeux du point 4.1 et des exigences du point 4.2, les risques et opportunités qu'il est nécessaire de traiter sont déterminés, de sorte que le SMSI atteigne les résultats attendus et que les effets indésirables soient évités.**

Comment le prouver: Un registre reliant les enjeux du contexte aux risques et opportunités, tenu séparément ou intégré au registre des risques. Ce qui compte est la traçabilité : chaque enjeu de l'analyse de contexte doit conduire visiblement à une évaluation ou à une décision justifiée de ne pas le prendre en compte.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.1.1-2 **Les actions pour traiter ces risques et opportunités sont planifiées, intégrées aux processus du SMSI, et leur efficacité est évaluée.**

Comment le prouver: Plan d'action avec propriétaire, échéance et critère d'efficacité. Conservez l'évaluation d'efficacité dans une colonne propre, faute de quoi l'audit manquera de preuve que l'action n'a pas seulement été mise en œuvre mais également vérifiée.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

6.1.2-1 **Un processus d'appréciation du risque de sécurité de l'information est défini et appliqué ; il comprend des critères d'acceptation du risque et des critères de réalisation des appréciations du risque.** Document

Comment le prouver: Une politique de gestion des risques avec des échelles de vraisemblance et d'impact, une matrice des risques définie et un seuil d'acceptation clair. Le seuil doit être un chiffre ou une zone, pas une formule du type à notre appréciation.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

6.1.2-2 **Le processus garantit que des appréciations du risque répétées produisent des résultats cohérents, valides et comparables.**

Comment le prouver: Se démontre au moyen d'une méthodologie fixe avec des échelles définies et en comparant deux versions de l'appréciation : mêmes risques, même logique de cotation, écarts explicables. Une version datée du registre des risques de l'année précédente constitue la preuve la plus solide sur ce point.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

6.1.2-3 **Les risques de sécurité de l'information sont identifiés pour détecter la perte de confidentialité, d'intégrité et de disponibilité au sein du domaine d'application, et un propriétaire du risque est attribué à chaque risque.**

Comment le prouver: Registre des risques référençant des actifs ou des processus, les trois objectifs de protection et un propriétaire du risque nommé. Le propriétaire du risque doit avoir l'autorité pour accepter le risque ; dans les petits organismes, il s'agit normalement du gérant.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

6.1.2-4 **Les risques identifiés sont analysés : les conséquences potentielles, la vraisemblance réaliste et le niveau de risque qui en résulte sont déterminés.**

Comment le prouver: Colonnes pour l'impact, la vraisemblance et le niveau de risque résultant, chacune avec une brève justification. Une phrase de raisonnement par risque évite le constat d'audit le plus fréquent, à savoir des chiffres sans justification.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

6.1.2-5 **Les risques sont comparés aux critères d'acceptation et priorisés en vue de leur traitement.**

Comment le prouver: Le registre des risques doit montrer quels risques dépassent le seuil d'acceptation et dans quel ordre ils seront traités. Une vue triée ou une colonne de priorité suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

6.1.2-6 **Le processus d'appréciation du risque est disponible sous forme d'information documentée.** Document

Comment le prouver: La méthodologie elle-même est un document obligatoire, pas seulement son résultat. Une politique approuvée avec version et date d'approbation, reliée à l'index documentaire du SMSI.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

6.1.3-1 **Pour chaque risque dépassant le seuil d'acceptation, une option de traitement appropriée est sélectionnée (réduire, éviter, transférer ou accepter).**

Comment le prouver: Une colonne d'option de traitement dans le registre des risques. Lorsqu'un risque est accepté, consignez la justification et l'approbation formelle du propriétaire du risque ; lorsqu'il est transféré, nommez le contrat ou la police d'assurance.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.1.3-2 **Toutes les mesures nécessaires à la mise en œuvre des options de traitement du risque retenues sont déterminées.**

Comment le prouver: Formulez les mesures de manière concrète et vérifiable, avec un propriétaire et une échéance. Renvoyer à des travaux techniques déjà en cours (déploiement de la MFA, test de sauvegarde) est admis dès lors que cela pointe vers un ticket ou un artefact de configuration.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.1.3-3 **Les mesures déterminées sont comparées aux mesures de l'annexe A afin de vérifier qu'aucune mesure nécessaire n'a été omise.**

Comment le prouver: La comparaison est une étape distincte et traçable, pas un sous-produit. Elle est attestée par une colonne de correspondance dans le registre des risques référençant les numéros de l'annexe A, ainsi que par un compte rendu daté de la comparaison.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.1.3-4 **Une Déclaration d'applicabilité (DdA) existe. Elle évalue individuellement les 93 mesures de l'annexe A, indique l'applicabilité avec justification pour chaque mesure, le statut de mise en œuvre, et la justification de chaque exclusion.** Document

Comment le prouver: La Déclaration d'applicabilité est le document obligatoire central et la carte de l'ensemble de l'audit. Elle doit être complète : les mesures non applicables figurent aussi avec une justification, jamais comme une ligne vide. Colonnes recommandées : numéro de mesure, titre, applicable oui ou non, justification, statut de mise en œuvre, référence à la politique ou à la preuve, lien vers le risque. La version et l'approbation de la direction sont obligatoires, car la Déclaration d'applicabilité est confrontée à la réalité à chaque audit de surveillance.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.1.3-5 **Un plan de traitement du risque est produit, rassemblant les mesures, les responsabilités, les échéances et les ressources nécessaires.** Document

Comment le prouver: Cela peut être un onglet dans le tableur des risques ou un tableau de projet. Ce qui compte, c'est que les échéances soient réalistes et que les retards aient été visiblement replanifiés, car c'est précisément ce que l'auditeur vérifie.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.1.3-6 **Le plan de traitement du risque est approuvé par les propriétaires de risques et les risques résiduels restants sont formellement acceptés par eux.** Document

Comment le prouver: Signature, approbation électronique ou décision datée dans un compte rendu. Une ligne dans le compte rendu de revue de direction renvoyant à la version du registre suffit, à condition que la version soit sans ambiguïté.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.1.3-7 **Le processus de traitement du risque est disponible sous forme d'information documentée.** Document

Comment le prouver: Généralement couvert dans le même document de politique que l'appréciation du risque. Le flux depuis l'appréciation, en passant par le choix de l'option, jusqu'à l'acceptation du risque résiduel doit être décrit.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.2-1 **Des objectifs de sécurité de l'information sont établis pour les fonctions et niveaux pertinents, sont cohérents avec la politique et sont mesurables lorsque cela est possible.**

Comment le prouver: Une fiche d'objectifs avec trois à six objectifs, chacun avec un indicateur, une valeur de départ, une valeur cible et une échéance. Exemple : part des systèmes équipés de la MFA portée de 80 à 100 % avant la fin du trimestre. Les objectifs sans chiffre ne comptent pas comme mesurables.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.2-2 **Les objectifs tiennent compte des exigences de sécurité de l'information applicables ainsi que des résultats de l'appréciation et du traitement du risque.**

Comment le prouver: Ajoutez une colonne d'origine à la fiche d'objectifs : de quel risque, de quelle exigence client ou de quelle obligation légale provient l'objectif. Cela évite des objectifs qui paraissent arbitraires.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.2-3 **Les objectifs sont surveillés, communiqués et mis à jour si nécessaire.**

Comment le prouver: Suivi trimestriel de l'avancement dans la fiche d'objectifs, plus une communication à l'équipe, par exemple une brève note sur le wiki ou un point à l'ordre du jour de la réunion d'équipe. Les versions historiques démontrent que les mises à jour ont bien lieu.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.2-4 **Les objectifs de sécurité de l'information sont disponibles sous forme d'information documentée.** Document

Comment le prouver: Un document d'objectifs approuvé et daté suffit. Il peut faire partie de la revue de direction, mais il doit y exister comme une section propre et récupérable.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.2-5 **Pour chaque objectif, il est planifié ce qui sera fait, quelles ressources sont requises, qui en est responsable, quand ce sera achevé et comment les résultats seront évalués.**

Comment le prouver: Ces cinq points sont vérifiables individuellement et sont demandés individuellement lors de l'audit. Configurez-les comme cinq colonnes dans la fiche d'objectifs, la conformité devient alors visible d'un coup d'œil.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

6.3-1 **Lorsque l'organisme détermine que des changements du SMSI sont nécessaires, ces changements sont réalisés de façon planifiée.**

Comment le prouver: Se démontre par des demandes de changement, des comptes rendus ou des tickets montrant le déclencheur, l'évaluation d'impact, l'approbation et la mise en œuvre. Déclencheurs typiques dans les petits organismes : changement de fournisseur cloud, nouveaux sites, première embauche.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7 Support 15

7.1-1 **Les ressources nécessaires à l'établissement, la mise en œuvre, le maintien et l'amélioration continue du SMSI sont déterminées et fournies.**

Comment le prouver: Une ligne budgétaire de sécurité, des licences d'outils (gestionnaire de mots de passe, MDM, plateforme de journalisation), des jours-personne planifiés pour le maintien du SMSI et des prestations d'audit externe. Une facture ou une approbation budgétaire le démontre plus rapidement que n'importe quel texte.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7.2-1 **La compétence nécessaire des personnes dont le travail a une incidence sur la performance de sécurité de l'information est déterminée.**

Comment le prouver: Matrice de compétences ou profils de rôle énumérant les connaissances requises par rôle, par exemple développement sécurisé pour les développeurs, gestion des incidents pour le coordinateur. Dans les très petites équipes, une ligne par personne suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

7.2-2 **La compétence est assurée sur la base d'une formation initiale, d'une formation continue ou d'une expérience appropriées.**

Comment le prouver: Certificats, confirmations de cours, CV ou expérience pratique documentée. L'autoformation est acceptable si elle est attestée, par exemple par des attestations de suivi de cours en ligne ou par des tests de connaissances internes réussis.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

7.2-3 **Lorsque des écarts de compétence existent, des actions ont été menées pour les combler et l'efficacité de ces actions a été évaluée.**

Comment le prouver: Plan de formation avec une comparaison entre prévu et réalisé et une vérification d'efficacité, par exemple une note d'examen, un taux de clics lors d'une simulation d'hameçonnage ou une observation sur le poste de travail. La vérification d'efficacité est souvent oubliée et constitue un écart mineur classique.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

7.2-4 **Une information documentée appropriée est disponible en tant que preuve de la compétence.** Document

Comment le prouver: Un dossier de compétence ou de formation par personne avec preuves et dates. Dans les petits organismes, un répertoire de fichiers PDF conservés plus un tableau de synthèse suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

7.3-1 **Les personnes travaillant dans le domaine d'application ont connaissance de la politique de sécurité de l'information.**

Comment le prouver: Accusé de réception lors de l'intégration et après chaque modification de la politique, avec date et version. Une fonction d'accusé de lecture sur wiki ou une liste signée suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

7.3-2 **Les personnes connaissent leur propre contribution à l'efficacité du SMSI et les avantages de l'amélioration de la performance de sécurité de l'information.**

Comment le prouver: Supports de formation et listes de présence dans lesquels le lien avec le travail propre de la personne est visible. Les auditeurs interrogent directement le personnel, il convient donc de former avec des exemples concrets du quotidien plutôt qu'avec des citations abstraites de la norme.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

7.3-3 **Les personnes connaissent les conséquences du non-respect des exigences du SMSI.**

Comment le prouver: Indiquez les conséquences dans les supports de formation et les instructions de travail, et reliez-les au processus du point A.6.4. Même les organismes sans salariés doivent couvrir ce point pour les prestataires indépendants et les freelances via leurs contrats.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

7.4-1 **La communication interne et externe pertinente pour le SMSI est déterminée : ce qui est communiqué, quand, avec qui et par quels moyens.**

Comment le prouver: Une matrice de communication avec des lignes telles que incident de sécurité vers les clients, notification à l'autorité de contrôle sous 72 heures, rapport d'état mensuel à la direction. C'est la base de la communication de crise et elle est revue après chaque incident.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7.5.1-1 **Le SMSI comprend l'information documentée exigée par la norme ainsi que l'information documentée que l'organisme a déterminée comme nécessaire à l'efficacité du SMSI.** Document

Comment le prouver: Un index documentaire recensant chaque document du SMSI avec finalité, propriétaire, version et lieu de stockage. Il démontre que les documents obligatoires sont complets et constitue le point d'entrée le plus rapide pour l'auditeur.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7.5.2-1 **Lors de la création et de la mise à jour des documents, une identification, un format et un support appropriés sont assurés, et les documents sont revus et approuvés quant à leur pertinence.**

Comment le prouver: Un en-tête de document uniforme avec titre, version, date, auteur et approbateur. Dans les environnements basés sur Git, les revues de pull request avec approbation satisfont l'exigence de revue et d'approbation, à condition que l'historique soit immuable.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7.5.3-1 **L'information documentée est disponible et appropriée à l'utilisation, là où et quand elle est nécessaire.**

Comment le prouver: Un emplacement de stockage central accessible à toutes les personnes habilitées, avec une fonction de recherche. Testable par sondage : n'importe quelle instruction de travail donnée doit pouvoir être retrouvée en moins d'une minute.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7.5.3-2 **L'information documentée est protégée de manière adéquate, en particulier contre la perte de confidentialité, l'utilisation inappropriée et la perte d'intégrité.**

Comment le prouver: Droits d'accès fondés sur les rôles pour les documents du SMSI, versionnage avec historique, protection en écriture pour les versions approuvées et une sauvegarde du dépôt documentaire. La preuve de sauvegarde est la partie la plus souvent oubliée.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7.5.3-3 **La distribution, l'accès, la récupération, le stockage, la maîtrise des modifications ainsi que la conservation et le sort final de l'information documentée sont encadrés.**

Comment le prouver: Une brève règle de maîtrise documentaire avec des durées de conservation et des règles de suppression. Elle doit être conciliée avec les obligations légales (droit commercial, droit fiscal, RGPD) et sert de base aux points A.5.33 et A.8.10.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

7.5.3-4 **L'information documentée d'origine externe nécessaire à la planification et au fonctionnement du SMSI est identifiée et maîtrisée.**

Comment le prouver: Une liste de documents externes avec version et source : normes, textes juridiques, guides de durcissement des fournisseurs, documentation de sécurité cloud, accords de sous-traitance des données. Sans référence de version, la maîtrise ne peut pas être démontrée.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8 Fonctionnement 8

8.1-1 **Les processus nécessaires pour satisfaire les exigences de sécurité de l'information et pour mettre en œuvre les actions du point 6 sont planifiés, mis en œuvre et maîtrisés, et des critères pour ces processus sont établis.**

Comment le prouver: Un manuel d'exploitation ou des runbooks avec des critères clairs, par exemple le délai maximal de déploiement des correctifs critiques, les critères de mise en production des déploiements, les seuils d'alerte. Des critères sans chiffres n'ont aucune valeur lors de l'audit.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.1-2 **L'information documentée est disponible dans la mesure nécessaire pour avoir confiance dans le fait que les processus ont été réalisés comme prévu.** Document

Comment le prouver: Enregistrements opérationnels comme preuve : historique de tickets, exécutions du pipeline d'intégration continue, rapports de correctifs, journaux de sauvegarde, revues d'accès. Ces enregistrements constituent la preuve réelle d'efficacité lors de l'audit de phase 2.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.1-3 **Les changements planifiés sont maîtrisés et les conséquences des changements non intentionnels sont revues ; si nécessaire, les effets indésirables sont atténués.**

Comment le prouver: Un processus de changement avec approbation et une voie de retour arrière, relié au point A.8.32. Pour les changements non intentionnels (erreur de configuration, élévation de privilèges accidentelle), documentez l'incident et attestez la correction.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.1-4 **Les processus, produits et services fournis en externe et pertinents pour le SMSI sont déterminés et maîtrisés.**

Comment le prouver: Une liste de fournisseurs avec la criticité, la référence contractuelle et l'état des preuves (certificat ISO 27001 du fournisseur, rapport SOC 2, accord de sous-traitance des données). Pour les petits organismes, c'est le levier le plus important, car l'essentiel de l'informatique repose de toute façon sur l'externe.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.2-1 **Des appréciations du risque sont réalisées à intervalles planifiés et chaque fois que des changements ou des incidents significatifs surviennent, en tenant compte des critères établis.**

Comment le prouver: Un rythme (généralement annuel) plus des déclencheurs définis pour des appréciations non planifiées. Attesté par des versions datées du registre des risques et des entrées dans le calendrier ou le système de tickets.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.2-2 **Les résultats des appréciations du risque sont conservés sous forme d'information documentée.** Document

Comment le prouver: Versions historiques du registre des risques avec dates, pas seulement l'état actuel. Écraser le fichier rend l'évolution impossible à prouver ; le versionnage dans le système de fichiers ou dans Git résout ce problème.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.3-1 **Le plan de traitement du risque est mis en œuvre.**

Comment le prouver: Comparez le plan à la réalité : actions achevées avec une date de mise en œuvre et un artefact concret (configuration, politique, contrat). Les actions ouvertes nécessitent une justification documentée et une nouvelle échéance.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

8.3-2 **Les résultats du traitement du risque sont conservés sous forme d'information documentée.** Document

Comment le prouver: Rapports d'état ou actions clôturées avec une référence à la preuve. Le registre seul suffit si chaque ligne comporte une date d'achèvement et un lien vers la preuve.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

9 Évaluation des performances 21

9.1-1 **Il est déterminé ce qui doit être surveillé et mesuré, y compris les processus et mesures de sécurité de l'information.**

Comment le prouver: Une fiche d'indicateurs avec un nombre gérable de mesures solides : arriéré de correctifs, couverture de la MFA, délai de résolution des incidents, résultat du dernier test de restauration, constats ouverts. Quelques indicateurs réellement collectés valent mieux qu'une longue liste de souhaits.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

9.1-2 **Les méthodes de surveillance, de mesure, d'analyse et d'évaluation sont définies et produisent des résultats valides.**

Comment le prouver: Documentez la source de données et le calcul pour chaque indicateur, par exemple un export du scanner de vulnérabilités ou du rapport du fournisseur d'identité. La traçabilité de la source est le cœur de la validité.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

9.1-3 **Il est défini quand et par qui la surveillance et la mesure sont réalisées et quand les résultats sont analysés et évalués.**

Comment le prouver: Ajoutez des colonnes de fréquence et de propriétaire à la fiche d'indicateurs. Un rendez-vous récurrent au calendrier pour l'évaluation démontre la régularité mieux que toute description.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

9.1-4 **Les résultats de la surveillance et de la mesure sont conservés sous forme d'information documentée.** Document

Comment le prouver: Évaluations archivées, tableaux de bord exportés ou fiche d'indicateurs tenue comme série temporelle. Une vue en direct sans historique ne satisfait pas l'exigence.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

9.1-5 **La performance de sécurité de l'information et l'efficacité du SMSI sont évaluées sur la base des résultats de mesure.**

Comment le prouver: Une évaluation écrite, pas seulement des chiffres : tendance, causes, besoin d'action. Ce texte d'évaluation constitue en même temps une entrée pour la revue de direction.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

9.2.1-1 **Des audits internes sont menés à intervalles planifiés et fournissent des informations permettant de savoir si le SMSI est conforme aux exigences propres de l'organisme et aux exigences de la norme, et s'il est mis en œuvre efficacement.**

Comment le prouver: Avant l'audit de certification, au moins un cycle complet d'audit interne couvrant l'ensemble du domaine d'application doit être achevé. Sans cela, la certification est hors de portée ; c'est l'un des obstacles les plus fréquents lors des premières certifications.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

9.2.2-1 **Un programme d'audit est planifié, établi et tenu à jour ; il définit la fréquence, les méthodes, les responsabilités, les exigences de planification et de rapport, et il tient compte de l'importance des processus concernés et des résultats des audits précédents.**

Comment le prouver: Un programme d'audit pluriannuel couvrant tous les points et toutes les mesures applicables sur l'ensemble du cycle de certification, avec une fréquence plus élevée pour les domaines critiques. Un simple tableau sur trois ans suffit amplement.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.2.2-2 **Des critères d'audit et un périmètre d'audit sont définis pour chaque audit.**

Comment le prouver: Un plan d'audit par date avec les critères (la norme, les politiques internes, les contrats) et un périmètre clair. Un plan d'audit d'une page par audit suffit et sert en même temps de base au rapport.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.2.2-3 **Les auditeurs sont sélectionnés et les audits sont menés de manière à garantir l'objectivité et l'impartialité. Personne n'audite son propre travail.**

Comment le prouver: L'indépendance est ici l'obstacle le plus exigeant : quiconque a rédigé les politiques et configuré les systèmes ne doit pas les auditer. Dans les très petits organismes, cela implique presque toujours un auditeur interne externe, par exemple un consultant sous contrat ou un collègue d'une entreprise partenaire ; un contrat d'audit accompagné de la déclaration d'indépendance de l'auditeur constitue la preuve. Ce n'est que dans des équipes suffisamment grandes que le rôle peut être tourné en interne vers une personne sans responsabilité sur le domaine audité, ce qui doit alors apparaître dans la matrice de rôles.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.2.2-4 **Les résultats de l'audit sont rapportés à la direction concernée.**

Comment le prouver: Un rapport d'audit avec les constats, les non-conformités, les recommandations et une liste de diffusion, ainsi que la preuve de la transmission à la direction, par exemple un point en compte rendu ou un courriel daté de transmission.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.2.2-5 **L'information documentée relative au programme d'audit et aux résultats des audits est conservée.** Document

Comment le prouver: Conservez le programme d'audit, les plans d'audit, les rapports d'audit et les actions qui en résultent en un seul endroit. Le lien entre un constat et une action corrective (point 10.2) doit être visible de bout en bout.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.1-1 **La direction générale revoit le SMSI à intervalles planifiés pour s'assurer qu'il demeure pertinent, adapté et efficace.**

Comment le prouver: Au moins une fois par an et programmée avant l'audit externe. Même dans les très petits organismes, il doit exister un compte rendu daté et signé, même lorsque la direction et le propriétaire du SMSI sont la même personne.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.2-1 **La revue de direction tient compte de l'état des actions issues des revues de direction précédentes.**

Comment le prouver: Le compte rendu commence par un tableau de suivi des décisions de l'année précédente et de leur statut actuel. Sans ce renvoi en arrière, la revue est considérée comme incomplète.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.2-2 **La revue de direction tient compte des changements des enjeux externes et internes pertinents pour le SMSI, y compris les aspects pertinents du changement climatique.**

Comment le prouver: Un point d'ordre du jour propre renvoyant à l'analyse de contexte actualisée. Le changement climatique n'est pas nommé explicitement dans le texte de ce point (l'Amd 1:2024 ne modifie que les points 4.1 et 4.2), mais il y entre par le biais des changements des enjeux du point 4.1, et les auditeurs l'attendent. Même un résultat de non pertinent, inchangé doit figurer dans le compte rendu.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.2-3 **La revue de direction tient compte des changements des besoins et attentes des parties intéressées pertinentes pour le SMSI.**

Comment le prouver: Nouvelles exigences clients issues des contrats et des questionnaires de sécurité, nouvelles obligations légales, exigences de l'organisme de certification. Consignez-les comme une liste avec les sources dans le compte rendu.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.2-4 **La revue de direction tient compte des retours sur la performance de sécurité de l'information, y compris les non-conformités et actions correctives, les résultats de surveillance et de mesure, les résultats d'audit et le respect des objectifs de sécurité de l'information.**

Comment le prouver: Traitez ces quatre blocs comme des points d'ordre du jour distincts, faute de quoi l'un d'eux manquera plus tard dans le compte rendu. Joignez la fiche d'indicateurs, le rapport d'audit et la fiche d'objectifs en annexes.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.2-5 **La revue de direction tient compte des retours des parties intéressées.**

Comment le prouver: Réclamations clients à composante sécurité, résultats d'audits clients, signalements du canal de lancement d'alerte, retours des prestataires. Consignez-le dans le compte rendu même lorsque le constat est qu'aucun n'a été reçu.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.2-6 **La revue de direction tient compte des résultats de l'appréciation du risque et de l'état du plan de traitement du risque.**

Comment le prouver: Joignez le registre des risques actuel et l'état de mise en œuvre du plan de traitement, avec une confirmation explicite de l'acceptation du risque résiduel par les propriétaires de risques.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.2-7 **La revue de direction tient compte des opportunités d'amélioration continue.**

Comment le prouver: Un point d'ordre du jour avec des idées d'amélioration concrètes et une décision sur chacune. Les idées retenues passent dans le registre d'amélioration comme des entrées avec échéances.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.3-1 **Les résultats de la revue de direction comprennent des décisions relatives aux opportunités d'amélioration continue et à tout besoin de changement du SMSI.**

Comment le prouver: Le compte rendu se termine par une section décisions : décision, propriétaire, échéance. Un compte rendu sans décisions est un constat d'audit, car l'effet de leadership fait alors défaut.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

9.3.3-2 **L'information documentée est conservée comme preuve des résultats de la revue de direction.** Document

Comment le prouver: Compte rendu signé avec date, participants, entrées, évaluation et décisions. C'est l'un des premiers documents qu'un organisme de certification demande lors de la phase 1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

10 Amélioration 7

10.1-1 **La pertinence, l'adéquation et l'efficacité du SMSI sont améliorées en continu.**

Comment le prouver: Un registre d'amélioration alimenté par plusieurs sources (audits, incidents, idées, écarts d'indicateurs) avec une progression visible dans le temps. La continuité sur plusieurs mois constitue la preuve, pas le nombre d'entrées.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

10.2-1 **Lorsqu'une non-conformité survient, l'organisme y réagit : il la maîtrise et la corrige et traite les conséquences.**

Comment le prouver: Un rapport de non-conformité avec une action immédiate et une date. Les sources sont les audits internes, les audits externes, les incidents et les observations de l'exploitation quotidienne ; toutes alimentent le même registre.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

10.2-2 **Il est évalué si une action est nécessaire pour éliminer les causes afin que la non-conformité ne se reproduise pas ou ne se produise pas ailleurs ; cela comprend la vérification de l'existence ou de l'apparition possible de non-conformités similaires.**

Comment le prouver: Documentez l'analyse des causes profondes, par exemple avec les 5 pourquoi ou le diagramme d'Ishikawa, ainsi qu'une déclaration explicite sur la transposabilité à d'autres systèmes ou processus. L'étape de transposabilité est celle qui est le plus souvent omise.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

10.2-3 **Les actions correctives nécessaires sont mises en œuvre et leur efficacité est revue.**

Comment le prouver: Pour chaque action, consignez la date de mise en œuvre, l'artefact de preuve et une revue d'efficacité ultérieure avec sa propre date. Deux champs de date par ligne constituent le moyen le plus simple de ne pas perdre de vue la revue d'efficacité.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

10.2-4 **Si nécessaire, des changements sont apportés au SMSI en conséquence de la non-conformité.**

Comment le prouver: Si une non-conformité remonte à une lacune dans une politique, dans le registre des risques ou dans la Déclaration d'applicabilité, le changement doit y devenir visible. Une référence entre la non-conformité et la version actualisée du document referme la chaîne.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

10.2-5 **Les actions correctives sont appropriées aux effets des non-conformités rencontrées.**

Comment le prouver: Une cotation de gravité dans le registre d'où ressort la proportionnalité de l'action. Ni un détail traité comme un projet, ni un écart grave traité par un simple courriel de rappel.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

10.2-6 **L'information documentée est conservée sur la nature des non-conformités, les actions menées en réponse et les résultats des actions correctives.** Document

Comment le prouver: Un registre des non-conformités et actions correctives avec des colonnes pour la nature, la cause, l'action, le propriétaire, l'échéance et le résultat de la revue d'efficacité. C'est une preuve obligatoire demandée à chaque audit de surveillance.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5 Annexe A : mesures organisationnelles 37

A.5.1 **Politiques de sécurité de l'information : Une politique globale de sécurité de l'information et des politiques thématiques sont définies, approuvées par la direction, communiquées et revues à intervalles planifiés et en cas de changements significatifs.** Document

Comment le prouver: Un ensemble de politiques avec version, date d'approbation et prochaine date de revue, plus la preuve de l'accusé de réception. Pour les petits organismes, une politique cadre et une poignée de politiques thématiques (accès, cryptographie, travail à distance, incidents) suffisent.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.2 **Rôles et responsabilités liés à la sécurité de l'information : Les rôles et responsabilités liés à la sécurité de l'information sont définis et attribués selon les besoins de l'organisme.**

Comment le prouver: Une matrice de rôles avec noms, suppléants et tâches. Dans les très petits organismes, indiquez ouvertement où plusieurs rôles se cumulent sur une même personne et reliez cela aux mesures compensatoires du point A.5.3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.3 **Séparation des tâches : Les tâches et domaines de responsabilité destinés à se contrôler mutuellement ne sont pas détenus par une seule personne. L'objectif est que personne ne puisse initier, approuver et dissimuler un changement de sa propre initiative.**

Comment le prouver: Dans les petits organismes, une séparation complète est structurellement impossible ; une affirmation générique de conformité s'effondre immédiatement lors de l'entretien d'audit. Ce qui tient est une analyse honnête : quelles combinaisons de tâches sont critiques (développer et mettre en production, accorder des droits et les utiliser, initier et approuver des paiements), lesquelles reposent sur une seule personne, et quelles mesures compensatoires s'appliquent. Des approches éprouvées sont les journaux d'audit immuables accessibles à un tiers, la MFA sur les comptes à privilèges, des portes de contrôle automatisées en intégration continue et une protection des branches à la place de la revue à quatre yeux, une revue périodique des journaux par une personne externe, et une approbation séparée pour les paiements. Conservez l'analyse et les mesures compensatoires comme un document propre et daté, et reliez-le depuis la Déclaration d'applicabilité.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.4 **Responsabilités de la direction : La direction exige de l'ensemble du personnel qu'il applique la sécurité de l'information conformément aux politiques et procédures établies.**

Comment le prouver: Un engagement dans les contrats de travail et de prestataires, un accusé de réception des politiques lors de l'intégration, et des rappels réguliers de la direction. Preuve : déclarations d'engagement signées et comptes rendus de réunion.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.5 **Relations avec les autorités : Des contacts appropriés avec les autorités pertinentes sont entretenus et joignables en cas de besoin.**

Comment le prouver: Une liste de contacts avec l'autorité de protection des données compétente, la police ou l'unité de cybercriminalité, le point national de signalement en cybersécurité et, le cas échéant, les canaux de notification NIS2. Notez les délais (tels que les 72 heures du RGPD) directement dans la liste.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.6 **Relations avec des groupes de travail spécialisés : Des contacts avec des groupes de travail spécialisés, des forums de sécurité et des associations professionnelles sont entretenus.**

Comment le prouver: Adhésions, alertes souscrites (CERT national, bulletins des éditeurs), participation à des groupes de travail spécialisés. Une preuve simple : une liste d'abonnements plus un exemple montrant comment une alerte a conduit à une action.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.7 **Renseignement sur les menaces : Des informations sur les menaces de sécurité de l'information sont recueillies et analysées afin d'en tirer des actions appropriées.**

Comment le prouver: Nouveau dans l'édition 2022. Réalisable pour les petits organismes : s'abonner aux alertes du CERT national et des éditeurs, puis réaliser une brève revue mensuelle avec une décision de pertinence et des tickets qui en découlent. La preuve est l'analyse, pas l'abonnement.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.8 **Sécurité de l'information dans la gestion de projet : La sécurité de l'information est intégrée à la gestion de projet, quel que soit le type de projet.**

Comment le prouver: Points de sécurité dans la liste de vérification du projet : besoins de protection, revue des risques, vérification protection des données, validation sécurité avant mise en production. Dans les équipes agiles, ancrez-les comme des points fixes dans la définition de prêt et la définition de terminé.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.9 **Inventaire des informations et autres actifs associés : Un inventaire des informations et autres actifs associés avec des propriétaires nommés est créé et tenu à jour.**

Comment le prouver: Un inventaire des actifs couvrant le matériel, les logiciels, les services cloud, les dépôts de données, les domaines et les comptes, chacun avec un propriétaire et ses besoins de protection. Dans les petits organismes, il peut être assemblé automatiquement à partir d'un export MDM, d'une liste de licences et de la console cloud ; une date actuelle est obligatoire.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.10 **Utilisation acceptable des informations et autres actifs associés : Des règles pour l'utilisation acceptable et la manipulation des informations et autres actifs associés sont identifiées, documentées et mises en œuvre.** Document

Comment le prouver: Une politique d'utilisation acceptable pour les appareils, les réseaux, les comptes cloud et les outils d'IA, avec accusé de réception. Les appareils personnels et les services d'IA externes doivent être couverts explicitement, car c'est là que se produit la majorité des fuites.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.11 **Restitution des actifs : Lorsqu'une relation de travail prend fin ou change, il est encadré et confirmé par écrit que tous les appareils, clés, comptes et documents remis sont restitués.**

Comment le prouver: Une liste de vérification de départ avec un accusé de restitution pour l'ordinateur portable, les jetons, les clés, les certificats et les supports de stockage, plus la désactivation des comptes le jour même. Cela s'applique tout autant aux freelances et aux stagiaires.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.12 **Classification des informations : Les informations sont classifiées selon leurs besoins de protection en matière de confidentialité, d'intégrité, de disponibilité et d'exigences légales.**

Comment le prouver: Un schéma simple avec trois ou quatre niveaux (public, interne, confidentiel, strictement confidentiel) et des règles de manipulation concrètes par niveau. Consignez l'attribution dans l'inventaire des actifs ou dans le registre des activités de traitement.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.13 **Marquage des informations : Le niveau de classification est reconnaissable sur le document, le fichier ou le message lui-même, de sorte que les destinataires sachent comment le traiter sans avoir à demander.**

Comment le prouver: Marquage dans l'en-tête du document, le nom du fichier, l'objet du courriel ou via des étiquettes de sensibilité dans la suite bureautique cloud. Preuve par des échantillons de documents effectivement marqués, pas seulement par la règle.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.14 **Transfert des informations : Des règles, procédures et accords pour le transfert d'informations au sein de l'organisme et avec des parties externes sont en place.**

Comment le prouver: Une règle indiquant quel canal est autorisé pour quel niveau de classification : courriel chiffré ou salle de données pour le contenu confidentiel, aucun envoi via des messageries privées. Adossez les transferts confidentiels à des accords de confidentialité.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.15 **Contrôle d'accès : Des règles pour contrôler l'accès physique et logique aux informations et autres actifs associés sont établies et mises en œuvre sur la base des exigences métier et de sécurité.**

Comment le prouver: Une politique de contrôle d'accès suivant les principes de besoin d'en connaître et de moindre privilège, avec une correspondance rôle vers droits. Preuve par la configuration réelle des droits chez le fournisseur d'identité, pas seulement par la politique.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.16 **Gestion des identités : Le cycle de vie complet des identités est géré.**

Comment le prouver: Un processus depuis la création, en passant par la modification, jusqu'à la désactivation, idéalement centralisé dans un fournisseur d'identité avec authentification unique. Pas de comptes de groupe partagés ; lorsque cela est techniquement inévitable, nommez le compte, justifiez-le et journalisez son utilisation.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.17 **Informations d'authentification : L'attribution et la gestion des informations d'authentification sont contrôlées par un processus de gestion exigeant des personnes qu'elles les manipulent correctement.**

Comment le prouver: Un gestionnaire de mots de passe comme outil obligatoire, une politique sur la qualité des mots de passe et la MFA, un accès initial sécurisé et une procédure de réinitialisation avec vérification d'identité. Preuve par des captures d'écran de configuration et le rapport du gestionnaire de mots de passe.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.18 **Droits d'accès : Les droits d'accès sont attribués, revus, modifiés et supprimés conformément à la politique de contrôle d'accès.**

Comment le prouver: Une revue d'accès périodique, au moins annuelle, avec un résultat documenté par compte et la preuve des droits supprimés. La suppression le jour même du départ est un point que les auditeurs aiment retracer sur un cas concret.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.19 **Sécurité de l'information dans les relations avec les fournisseurs : Des processus et procédures sont définis et mis en œuvre pour gérer les risques de sécurité découlant de l'utilisation de produits et services tiers.**

Comment le prouver: Une liste de fournisseurs avec un niveau de criticité et la profondeur d'évaluation. Pour les fournisseurs critiques, obtenez des preuves (certificat ISO 27001, rapport SOC 2) plutôt que de mener vos propres audits, ce qui est la seule voie réaliste pour les petits organismes.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.20 **Prise en compte de la sécurité de l'information dans les accords avec les fournisseurs : Des exigences de sécurité pertinentes sont convenues avec chaque fournisseur et fixées dans les contrats.**

Comment le prouver: Une annexe contractuelle de sécurité de l'information avec des obligations de notification d'incident, des règles sur les sous-traitants ultérieurs, des obligations de suppression et des droits d'audit. Pour les services standards, les conditions du fournisseur plus un accord de sous-traitance des données suffisent, à condition que leur contenu ait été revu et documenté.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.21 **Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC : Des processus pour gérer les risques de sécurité dans la chaîne d'approvisionnement des technologies de l'information et de la communication sont définis et mis en œuvre.**

Comment le prouver: Cela couvre les dépendances logicielles et les propres sous-fournisseurs des fournisseurs. En pratique : une nomenclature logicielle (SBOM) ou une liste de dépendances, des vérifications automatisées des paquets vulnérables en intégration continue, et un approvisionnement en logiciels uniquement via des canaux signés ou officiels.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.22 **Surveillance, revue et gestion des changements des services fournisseurs : Les changements des services fournisseurs sont régulièrement surveillés, revus et gérés.**

Comment le prouver: Une revue annuelle des fournisseurs portant sur les incidents, les rapports de disponibilité et la validité des certificats, plus un canal pour les annonces de changement du fournisseur. Consignez le résultat comme une brève note par fournisseur.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.23 **Sécurité de l'information pour l'utilisation de services cloud : Des processus pour l'acquisition, l'utilisation, la gestion et la sortie des services cloud sont établis conformément aux exigences de sécurité.**

Comment le prouver: Nouveau dans l'édition 2022 et la mesure centrale pour les petits organismes fondés sur le cloud. Preuve par une politique cloud avec un processus d'approbation pour les nouveaux services, un modèle de responsabilité partagée documenté par service, des paramètres de durcissement, et une stratégie de sortie incluant la restitution des données et la confirmation de suppression.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.24 **Planification et préparation de la gestion des incidents de sécurité de l'information : Des processus, rôles et responsabilités pour la gestion des incidents sont planifiés et établis.** Document

Comment le prouver: Un plan de réponse aux incidents avec la voie de signalement, les rôles, les niveaux d'escalade, les contacts en dehors des heures de travail et des modèles de communication. Réaliste pour les petites équipes : une page, mais mise en pratique.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.25 **Évaluation et décision relatives aux événements de sécurité de l'information : Les événements de sécurité sont évalués et une décision est prise sur leur classification éventuelle en incidents de sécurité de l'information.**

Comment le prouver: Critères de tri avec une matrice de gravité et un registre d'événements dans lequel les événements écartés apparaissent également avec une justification. La séparation entre événement et incident doit être visible dans le registre.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.26 **Réponse aux incidents de sécurité de l'information : Les incidents sont traités conformément aux procédures documentées.**

Comment le prouver: Dossiers d'incidents avec une chronologie, les actions menées, les personnes impliquées et la décision de clôture. S'il n'y a pas encore eu d'incident réel, un exercice de simulation documenté constitue la meilleure preuve disponible.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.27 **Tirer des enseignements des incidents de sécurité de l'information : Les connaissances tirées des incidents sont utilisées pour renforcer les mesures de sécurité.**

Comment le prouver: Une revue post-incident sans recherche de coupable, avec une analyse des causes profondes et des actions qui en découlent, reliée au registre d'amélioration et, si nécessaire, au registre des risques.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.28 **Collecte de preuves : Il est encadré comment les traces relatives à un événement de sécurité sont identifiées, préservées et conservées afin de rester exploitables ultérieurement.**

Comment le prouver: Une brève procédure de préservation des preuves : ne pas reconstruire prématurément les systèmes, préserver les images et les journaux, documenter la chaîne de traçabilité. Pour les petits organismes, il suffit de définir le niveau de gravité à partir duquel un prestataire forensique externe est sollicité, avec les coordonnées de contact.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.29 **Sécurité de l'information pendant une perturbation : L'organisme planifie la manière dont la sécurité de l'information est maintenue à un niveau approprié pendant une perturbation.**

Comment le prouver: Les dispositifs d'urgence ne doivent pas désactiver la sécurité. Documentez que la MFA, la journalisation et les restrictions d'accès s'appliquent également en fonctionnement dégradé, et que les comptes d'urgence (comptes bris de glace) sont scellés, documentés et revus après coup.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.30 **Préparation des TIC pour la continuité d'activité : La préparation des TIC est planifiée, mise en œuvre, tenue à jour et testée sur la base des objectifs de continuité d'activité et des exigences de continuité des TIC.**

Comment le prouver: Nouveau dans l'édition 2022. Preuve par des objectifs de délai de reprise (RTO) et de point de reprise (RPO) définis par système critique, une procédure de reprise et au moins un test documenté par an. Un test de restauration réussi avec date et durée constitue la preuve individuelle la plus solide.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.31 **Exigences légales, statutaires, réglementaires et contractuelles : Les exigences pertinentes et l'approche pour les satisfaire sont identifiées, documentées et tenues à jour.** Document

Comment le prouver: Un registre juridique couvrant le RGPD, le droit des télécommunications, le droit commercial et fiscal et, le cas échéant, NIS2 ou des règles sectorielles, chacun avec la règle qui le met en œuvre et la date de revue. Une revue annuelle suffit, mais elle doit être datée.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.32 **Droits de propriété intellectuelle : Des procédures appropriées sont mises en œuvre pour protéger les droits de propriété intellectuelle.**

Comment le prouver: Un inventaire des licences du logiciel utilisé, une vérification des licences open source dans le produit (un scanner de licences en intégration continue) et une règle pour la gestion du code de tiers et du code généré. Preuve : le rapport de licences issu de la compilation.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.33 **Protection des enregistrements : Les enregistrements métier et probants sont stockés de sorte qu'ils ne puissent être perdus, ne puissent être altérés sans que cela soit remarqué et ne puissent tomber entre de mauvaises mains, et ce pendant toute la durée de conservation.**

Comment le prouver: Un calendrier de conservation avec les durées légales, un stockage résistant à l'altération, un accès restreint et une sauvegarde. Pour les enregistrements pertinents sur le plan fiscal, indiquez explicitement les durées légales de conservation, car les auditeurs aiment vérifier ce point spécifiquement.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.5.34 **Vie privée et protection des données à caractère personnel : Les exigences de protection de la vie privée et des données à caractère personnel sont identifiées et satisfaites conformément au droit applicable.**

Comment le prouver: Registre des activités de traitement, accords de sous-traitance des données, un dispositif de suppression, un processus pour les droits des personnes concernées et, lorsque requis, une analyse d'impact relative à la protection des données. Relier cela au SMSI via une liste d'actifs partagée évite de tout maintenir en double.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.35 **Revue indépendante de la sécurité de l'information : L'approche de l'organisme en matière de gestion de la sécurité de l'information est revue de manière indépendante à intervalles planifiés et en cas de changements significatifs.**

Comment le prouver: Attesté par l'audit interne réalisé par un auditeur indépendant, par des tests d'intrusion externes ou par l'audit de certification lui-même. Indépendant signifie non réalisé par la personne responsable du domaine revu.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.36 **Conformité aux politiques, règles et normes de sécurité de l'information : La conformité aux politiques de sécurité propres de l'organisme et aux règles applicables est revue régulièrement.**

Comment le prouver: Vérifications de conformité avec date et résultat, par exemple une vérification de configuration par rapport à sa propre base de durcissement, un sondage du marquage documentaire, des vérifications automatisées de politiques dans le cloud. Les écarts alimentent le registre des actions correctives.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.5.37 **Procédures d'exploitation documentées : Les procédures d'exploitation pour les moyens de traitement de l'information sont documentées et mises à disposition des personnes qui en ont besoin.** Document

Comment le prouver: Runbooks pour la sauvegarde et la restauration, le déploiement, l'administration des utilisateurs, l'application des correctifs et la gestion des incidents. Court et à jour vaut mieux qu'exhaustif et obsolète ; une date de dernière modification par runbook est obligatoire.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6 Annexe A : mesures liées aux personnes 8

A.6.1 **Vérification des antécédents : Les candidats appelés à travailler pour l'organisme sont vérifiés au préalable, dans les limites de la loi et proportionnellement aux besoins de protection ; pour les rôles sensibles, la vérification est répétée pendant l'emploi.**

Comment le prouver: En l'absence de salariés, cette mesure peut être justifiée comme actuellement non applicable, mais la procédure à suivre en cas d'embauche doit néanmoins être définie et consignée comme prévue dans la Déclaration d'applicabilité. Un périmètre réalisable : vérification de l'identité, du CV et des références, plus les diplômes ; une vérification du casier judiciaire uniquement lorsque les besoins de protection le justifient et que la loi l'autorise. Exigez le même standard des freelances et des prestataires via leurs contrats, faute de quoi la brèche s'ouvre exactement là.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6.2 **Termes et conditions du contrat de travail : Les accords contractuels énoncent les responsabilités de sécurité de l'information du personnel et de l'organisme.**

Comment le prouver: Une clause de sécurité dans le contrat de travail ou de prestation renvoyant aux politiques applicables. Pour les freelances, la même clause dans le contrat de prestation, plus un accord de confidentialité.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6.3 **Sensibilisation, formation initiale et continue à la sécurité de l'information : Le personnel et les parties externes pertinentes reçoivent une sensibilisation et une formation appropriées ainsi que des mises à jour régulières sur les politiques de l'organisme.**

Comment le prouver: Formation annuelle avec preuve de présence et date, complétée par des simulations d'hameçonnage avec un taux de clics évalué. Même les travailleurs indépendants sans personnel ont besoin d'une preuve de leur propre formation continue, par exemple des attestations de suivi de cours.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6.4 **Processus disciplinaire : Un processus formel et communiqué existe pour engager des mesures à l'encontre des personnes ayant enfreint les politiques de sécurité.**

Comment le prouver: En l'absence de salariés, cela peut être justifié comme actuellement non applicable, mais le processus doit néanmoins être défini pour le cas d'une embauche ; seule son application est alors caduque, pas la règle. Ce qui est requis est une échelle de réponses graduée et communiquée (entretien, avertissement, mise en demeure formelle, licenciement) conforme au droit du travail et aux règles de représentation du personnel. Pour les prestataires, reflétez le niveau de sanction dans le contrat, par exemple une pénalité contractuelle ou un droit de résiliation.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6.5 **Responsabilités après la fin ou le changement de l'emploi : Les responsabilités et obligations de sécurité qui restent valables après la fin de l'emploi ou un changement de rôle sont définies, appliquées et communiquées aux personnes concernées.**

Comment le prouver: Une liste de vérification de départ avec suppression des droits, restitution des actifs, transmission des dossiers, et un rappel explicite des obligations de confidentialité qui subsistent. Un compte rendu signé de l'entretien de départ constitue la preuve la plus simple.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6.6 **Accords de confidentialité ou de non-divulgation : Il est déterminé qui doit signer un accord de confidentialité. Le contenu correspond aux besoins de protection de l'information, les accords sont signés, archivés et revus régulièrement afin de rester à jour.**

Comment le prouver: Accords de confidentialité signés pour les salariés, freelances, prestataires et stagiaires, avec une durée de survie. Un tableau de synthèse avec la contrepartie, la date et la validité rend le portefeuille auditable.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6.7 **Travail à distance : Des mesures de sécurité sont mises en œuvre lorsque des personnes travaillent en dehors des locaux de l'organisme et accèdent à des informations de l'organisme ce faisant.**

Comment le prouver: Une politique de télétravail et de travail à distance avec des exigences sur le chiffrement du disque, le verrouillage d'écran, le Wi-Fi sécurisé, l'utilisation d'un VPN ou d'un accès à confiance zéro, des filtres de confidentialité et une interdiction d'utiliser des appareils personnels sans approbation. Preuve par le rapport de conformité MDM des terminaux.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.6.8 **Signalement des événements de sécurité de l'information : Un mécanisme existe permettant aux personnes de signaler en temps utile les événements de sécurité observés ou soupçonnés.**

Comment le prouver: Un canal de signalement clairement communiqué (boîte aux lettres, canal de discussion, numéro de téléphone) avec l'assurance d'une absence de sanction pour les signalements de bonne foi. Preuve : le volume de signalements dans le registre des événements ; un registre en permanence vide est un signal d'alerte lors de l'audit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7 Annexe A : mesures physiques 14

A.7.1 Périmètres de sécurité physique : Des périmètres de sécurité sont définis et utilisés pour protéger les zones contenant des informations et des moyens de traitement de l'information.

Comment le prouver: Une description des périmètres avec un croquis ou des photos : bâtiment, bureau, baie serveur. En télétravail, le périmètre est la pièce de travail verrouillable ou, à défaut, une armoire verrouillable ; décrivez-la plutôt que de l'omettre.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.2 Entrées physiques : Les zones sécurisées sont protégées par des contrôles d'entrée et des points d'accès appropriés.

Comment le prouver: Un registre de clés ou de badges avec remise et restitution, et une règle pour les visiteurs avec accompagnement et un journal. En cas d'utilisation d'un espace de coworking ou d'un centre de données, retenez comme preuve les contrôles d'entrée de l'exploitant et sécurisez-les contractuellement.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.3 Sécurisation des bureaux, des salles et des équipements : La sécurité physique des bureaux, des salles et des équipements est conçue et mise en œuvre.

Comment le prouver: Portes verrouillables, protection des fenêtres au rez-de-chaussée, aucun écran confidentiel visible de l'extérieur, aucune enseigne d'entreprise sur les zones sensibles. Une brève description plus une photo suffit comme preuve.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.4 Surveillance de la sécurité physique : Les locaux sont surveillés en continu contre les accès physiques non autorisés.

Comment le prouver: Nouveau dans l'édition 2022. Les options sont un système d'alarme, des détecteurs de mouvement, la vidéosurveillance ou des journaux d'entrée. La vidéosurveillance doit être vérifiée quant à sa conformité en matière de protection des données ; en télétravail, l'alternative justifiée est une combinaison d'un système d'alarme, d'une pièce verrouillée et du constat qu'aucun serveur sensible n'y est conservé.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.5 Protection contre les menaces physiques et environnementales : Une protection contre les menaces physiques et environnementales, telles que les catastrophes naturelles et les dommages intentionnels ou non intentionnels, est en place.

Comment le prouver: Une revue de l'incendie, de l'eau, de la chaleur, de la coupure d'alimentation et de l'effraction, ainsi que des mesures en place (détecteurs de fumée, extincteurs, aucun équipement sous des canalisations d'eau, sauvegarde stockée à un autre endroit). C'est ici que se rattache la détermination sur le changement climatique du point 4.1.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.6 Travail dans les zones sécurisées : Des mesures pour le travail dans les zones sécurisées sont conçues et mises en œuvre.

Comment le prouver: Règles pour la salle serveur ou les zones de haute confidentialité : aucun accès de tiers sans surveillance, aucun enregistrement avec des caméras ou des appareils mobiles, journalisation du travail réalisé. En l'absence de zones sécurisées, cela peut être justifié en renvoyant à un fonctionnement exclusivement cloud.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.7 **Bureau dégagé et écran verrouillé : Des règles pour un bureau dégagé concernant les papiers et supports amovibles et pour des écrans verrouillés sont définies et suivies.**

Comment le prouver: Cela s'applique intégralement aussi en télétravail et ne doit donc pas être déclaré non applicable. Attesté par une brève règle (ranger les documents sous clé, verrouillage d'écran après cinq minutes, aucune note autocollante avec des identifiants) plus le verrouillage techniquement imposé via la politique d'appareils, dont la configuration peut être exportée.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.8 **Emplacement et protection du matériel : Le matériel est installé et protégé de manière sécurisée.**

Comment le prouver: Emplacement éloigné des zones de passage et des espaces publics, aucune vue depuis l'extérieur, protection contre la chaleur et l'humidité, câbles antivol pour les appareils mobiles. Une brève description au sein de la politique de bureau ou de télétravail suffit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.9 **Sécurité des actifs hors des locaux : Les actifs situés hors des locaux sont protégés.**

Comment le prouver: Dans les petits organismes, il s'agit surtout de l'ordinateur portable, du smartphone et des supports externes, et cela ne peut être écarté d'un revers de main. Preuve : chiffrement de disque imposé, effacement à distance activé via MDM, une règle interdisant de laisser des appareils dans des véhicules et d'utiliser des réseaux publics sans VPN, plus une voie de signalement de perte. Le rapport de conformité MDM montrant l'état de chiffrement par appareil constitue la preuve individuelle la plus solide.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.10 **Supports de stockage : Les supports de stockage sont gérés sur l'ensemble de leur cycle de vie conformément au schéma de classification et aux exigences de manipulation, de l'acquisition à l'élimination en passant par l'utilisation et le transport.**

Comment le prouver: Cela s'applique même au travail purement mobile, car des clés USB, des disques externes et des supports de sauvegarde existent. Preuve : un registre des supports, des supports chiffrés, une interdiction techniquement imposée des supports amovibles non approuvés, un stockage sécurisé dans un endroit verrouillable, et une transmission au point A.7.14 en fin de vie.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.11 **Services généraux : Les moyens de traitement de l'information sont protégés contre les défaillances des services généraux, en particulier l'alimentation électrique.**

Comment le prouver: Lorsque des serveurs sont exploités en interne, un onduleur avec un test documenté. Dans une configuration exclusivement cloud, la preuve est le renvoi aux engagements du fournisseur plus une règle sur la manière de continuer à travailler en cas de coupure locale d'électricité ou d'internet (partage de connexion mobile, site de repli).

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.12 **Sécurité du câblage : Le câblage électrique, de données et de communication est protégé contre l'interception, les interférences et les dommages.**

Comment le prouver: Lorsque le câblage est propre à l'organisme, protection contre les dommages et contre l'accès non autorisé aux panneaux de brassage. Dans les petits bureaux et en télétravail, la justification est légère, mais elle doit être donnée : le routeur et les prises réseau ne sont pas accessibles publiquement, les ports inutilisés sont désactivés.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.13 **Maintenance du matériel : Le matériel est entretenu correctement afin de garantir la disponibilité, l'intégrité et la confidentialité de l'information.**

Comment le prouver: Un plan de maintenance ou l'état de support du fabricant par appareil, et une règle pour les réparations réalisées par des tiers (retirer d'abord le support de stockage ou effacer les données, et mettre en place un accord de confidentialité avec le prestataire). Suivez les dates de fin de support dans l'inventaire des actifs.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.7.14 **Élimination ou réutilisation sécurisée du matériel : Avant qu'un appareil contenant un support de stockage soit transmis, vendu ou mis au rebut, il est vérifié et consigné qu'aucune donnée protégée ni logiciel sous licence ne peut encore y être reconstitué.**

Comment le prouver: Cela s'applique également en télétravail et aux appareils personnels retirés qui ont été utilisés à des fins professionnelles. Preuve : un enregistrement d'effacement par appareil avec numéro de série, date et méthode (effacement cryptographique sur SSD chiffrés, écrasement, destruction physique), ou un certificat de destruction d'un prestataire. Pour les appareils chiffrés, la destruction documentée de la clé suffit, à condition que la procédure soit décrite.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8 Annexe A : mesures technologiques 34

A.8.1 **Terminaux utilisateur : Les informations stockées, traitées ou accessibles via les terminaux utilisateur sont protégées.**

Comment le prouver: Une base de durcissement par système d'exploitation, une gestion centralisée via MDM, le chiffrement de disque, les mises à jour automatiques et le verrouillage d'écran. Le rapport de conformité MDM avec un état par appareil atteste tout cela en une seule fois.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.2 **Droits d'accès privilégiés : L'attribution et l'utilisation des droits d'accès privilégiés sont restreintes et gérées.**

Comment le prouver: Une liste de tous les comptes administrateur avec une justification, des comptes admin distincts non utilisés pour le travail quotidien, une MFA imposée, une élévation limitée dans le temps lorsque cela est possible, et une revue périodique. Dans les petits organismes, c'est la mesure compensatoire la plus importante pour le point A.5.3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.3 **Restriction d'accès à l'information : L'accès aux informations et autres actifs associés est restreint conformément à la politique de contrôle d'accès établie.**

Comment le prouver: Un concept d'habilitation fondé sur les rôles et les groupes plutôt que sur des attributions individuelles, attesté par un export des appartenances aux groupes. Revoyez régulièrement les liens de partage public dans le stockage cloud et laissez-les expirer.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.4 **Accès au code source : L'accès en lecture et en écriture au code source, aux outils de développement et aux bibliothèques logicielles est géré de manière appropriée.**

Comment le prouver: Permissions de dépôt par rôle, branches principales protégées, revues obligatoires ou vérifications d'état obligatoires, aucun push direct vers la branche principale. Preuve par la configuration de protection des branches et la liste des membres de l'organisation.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.5 **Authentification sécurisée : Des technologies et procédures d'authentification sécurisées sont mises en œuvre sur la base des restrictions d'accès et de la politique thématique.**

Comment le prouver: MFA pour tout accès externe et tous les comptes administrateur, méthodes résistantes à l'hameçonnage (clés d'accès, FIDO2) lorsque cela est possible, et blocage après échecs répétés. Preuve par le rapport de couverture MFA du fournisseur d'identité.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.6 **Gestion de la capacité : Le stockage, le calcul, la bande passante et les licences sont surveillés, et la demande est ajustée suffisamment tôt pour que les goulots d'étranglement ne menacent jamais la disponibilité.**

Comment le prouver: Surveillance du stockage, de la charge de calcul, des quotas de licences et des budgets cloud avec des alertes de seuil. Dans les petits organismes, une alerte sur l'utilisation du disque et sur les limites de coût plus un examen annuel de la capacité suffit.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.7 **Protection contre les logiciels malveillants : Des défenses techniques contre les logiciels malveillants sont actives et à jour, et les personnes qui utilisent les appareils sont suffisamment formées pour ne pas affaiblir ces défenses.**

Comment le prouver: Protection active des terminaux avec une vue d'état centralisée, un filtre de messagerie qui inspecte les pièces jointes et les liens, et une règle interdisant l'exécution de logiciels non approuvés. Le rapport d'état daté de la solution de protection constitue la preuve directe.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.8 **Gestion des vulnérabilités techniques : L'organisme s'informe activement des vulnérabilités de la technologie qu'il utilise, décide pour chaque constat de son degré d'exposition et referme la faille dans des délais définis ou justifie une réponse différente.**

Comment le prouver: Gestion des vulnérabilités avec une source (scanner, vérification des dépendances en intégration continue, alertes des éditeurs), une cotation de gravité et des délais définis par niveau, par exemple critique sous 7 jours. Preuve : rapports de scan à plusieurs moments dans le temps montrant la baisse des constats ouverts.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.9 **Gestion de la configuration : Les configurations du matériel, des logiciels, des services et des réseaux, y compris les configurations de sécurité, sont établies, documentées, mises en œuvre, surveillées et revues.**

Comment le prouver: Nouveau dans l'édition 2022. Preuve par des configurations de référence documentées (bases de durcissement) et leur application forcée, idéalement en tant qu'infrastructure comme code sous contrôle de version ou via des profils MDM. La détection des dérives et une comparaison de configuration périodique complètent le dispositif.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.10 **Suppression des informations : Les informations stockées dans les systèmes d'information, sur les appareils et sur les supports de stockage sont supprimées dès qu'elles ne sont plus nécessaires.**

Comment le prouver: Nouveau dans l'édition 2022 et étroitement lié au RGPD. Preuve par un dispositif de suppression avec des durées de conservation par catégorie de données, des règles de rétention techniquement mises en œuvre dans les services cloud et les bases de données, et des journaux de suppression. Les sauvegardes et les archives de journaux ont elles aussi besoin d'une durée de conservation.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.11 **Masquage des données : Le masquage des données est appliqué conformément à la politique thématique sur le contrôle d'accès et aux exigences métier et légales.**

Comment le prouver: Nouveau dans l'édition 2022. En pratique : aucune donnée de production dans les environnements de test et de développement, mais des données anonymisées ou synthétiques à la place ; pseudonymisation dans l'analytique ; masquage des numéros de compte et des identifiants dans les journaux et les interfaces de support. Preuve par le script ou la procédure qui génère les données de test.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.12 **Prévention de la fuite de données : Des mesures de prévention de la fuite de données sont appliquées aux systèmes, réseaux et appareils qui traitent, stockent ou transmettent des informations sensibles.**

Comment le prouver: Nouveau dans l'édition 2022. Réaliste dans les petits organismes : contrôle des liens de partage dans le stockage cloud, blocage des supports amovibles non approuvés, règles interdisant le transfert vers des boîtes aux lettres personnelles, vérifications sur la saisie de données confidentielles dans des services d'IA externes, et détection de secrets dans le code source. Preuve par la configuration et par des revues des occurrences détectées.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.13 **Sauvegarde des informations : Des sauvegardes des données, des logiciels et des systèmes existent selon une règle définie (périmètre, fréquence, conservation, emplacement), et la restauration à partir de celles-ci est réellement testée à intervalles réguliers.**

Comment le prouver: Une politique de sauvegarde avec fréquence, conservation et une copie externalisée suivant le principe 3-2-1, le chiffrement des sauvegardes, et une protection contre l'écrasement par rançongiciel (sauvegardes immuables). Ce qui est déterminant est le test de restauration documenté avec date et résultat, car une sauvegarde non testée est considérée comme inexistante lors de l'audit.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.14 **Redondance des moyens de traitement de l'information : Les moyens de traitement de l'information sont mis en œuvre avec une redondance suffisante pour satisfaire les exigences de disponibilité.**

Comment le prouver: La redondance doit correspondre aux objectifs de disponibilité, pas au maximum possible. Preuve par une description d'architecture avec des instances ou des zones redondantes, du matériel de rechange, et une décision justifiée sur les points où l'on renonce délibérément à la redondance.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.15 **Journalisation : Les activités pertinentes pour la sécurité laissent une trace. Les journaux sont produits, conservés, protégés contre l'altération et réellement analysés, pas seulement collectés.**

Comment le prouver: Journalisez au minimum les connexions et les tentatives échouées, les changements de droits, les actions administratives et l'accès aux données confidentielles. Les journaux sont protégés contre l'altération et disposent d'une durée de conservation définie ; dans les petits organismes, des journaux immuables constituent en même temps la compensation de l'absence de séparation des tâches du point A.5.3.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.16 **Activités de surveillance : Les réseaux, systèmes et applications sont surveillés à la recherche de comportements anormaux et des actions appropriées sont menées pour évaluer d'éventuels incidents de sécurité.**

Comment le prouver: Nouveau dans l'édition 2022. Réalisable sans équipe de sécurité dédiée : alertes du fournisseur d'identité sur les déplacements impossibles et les séries d'échecs, alertes de la plateforme cloud sur les dépenses inhabituelles ou les changements de droits, transmises vers une boîte aux lettres surveillée avec un délai de réponse défini. Preuve par les règles d'alerte plus des exemples d'alertes traitées.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.17 **Synchronisation des horloges : Tous les systèmes qui produisent des journaux tirent leur heure d'une source définie et fiable, de sorte que les événements puissent être ordonnés correctement entre les systèmes.**

Comment le prouver: Configuration NTP sur les serveurs et les terminaux, et un fuseau horaire uniforme dans les journaux (idéalement UTC). Sans synchronisation de l'heure, la reconstitution d'un incident au titre du point A.5.28 ne tient pas ; un extrait de configuration suffit comme preuve.

◯ Ouvert ◯ En cours ◯ Satisfait ◯ Non applicable

Preuve / justification

A.8.18 **Utilisation de programmes utilitaires à privilèges : L'utilisation de programmes utilitaires susceptibles de contourner les protections du système est restreinte et étroitement contrôlée.**

Comment le prouver: Une liste des outils d'administration approuvés, une restriction des droits d'administrateur local, un contrôle des applications (liste blanche) lorsque possible, et une journalisation de l'utilisation. Preuve : la politique plus la configuration de la gestion des droits.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.19 **Installation de logiciels sur des systèmes opérationnels : Des procédures et mesures pour gérer de manière sécurisée l'installation de logiciels sur les systèmes opérationnels sont mises en œuvre.**

Comment le prouver: Uniquement des logiciels approuvés provenant de sources fiables, installation via une distribution centralisée ou un gestionnaire de paquets, une voie de retour arrière et la conservation de la version précédente. Preuve par la liste d'approbation et les journaux de déploiement.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.20 **Sécurité des réseaux : Les réseaux et les équipements réseau actifs ont un propriétaire nommé, une configuration durcie et un jeu de règles traçable définissant quel trafic est autorisé.**

Comment le prouver: Un jeu de règles de pare-feu suivant le principe de refus par défaut, des ports ouverts documentés avec justification, une configuration Wi-Fi sécurisée, et des identifiants par défaut modifiés sur les équipements réseau. Preuve par un export du jeu de règles et un scan de ports externe.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.21 **Sécurité des services réseau : Les mécanismes de sécurité, les niveaux de service et les exigences de gestion des services réseau sont identifiés, mis en œuvre et surveillés.**

Comment le prouver: Pour chaque service réseau utilisé (VPN, DNS, messagerie, CDN), documentez les engagements de sécurité et votre propre configuration, y compris le chiffrement en transit et les engagements de niveau de service du fournisseur. Preuve : une vue d'ensemble de la configuration plus le contrat ou la description du service.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.22 **Séparation des réseaux : Le réseau est divisé en zones de sorte que les services, groupes d'utilisateurs et systèmes ayant des besoins de protection différents ne puissent pas s'atteindre mutuellement sans filtrage.**

Comment le prouver: Segments réseau ou VLAN distincts pour les invités, l'administration et la production ; dans le cloud, des comptes ou réseaux virtuels distincts avec des groupes de sécurité. En télétravail, la mise en œuvre réalisable est un réseau ou un VLAN distinct pour les appareils professionnels, séparé des appareils personnels et de la domotique.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.23 **Filtrage web : L'accès aux sites web externes est géré afin de réduire l'exposition aux contenus malveillants.**

Comment le prouver: Nouveau dans l'édition 2022. Réalisable avec peu d'effort via un service DNS avec filtrage ou le filtrage web inclus dans la protection des terminaux, avec des catégories bloquées et une journalisation des requêtes bloquées. Preuve par la configuration du filtre et un extrait de rapport.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.24 **Utilisation de la cryptographie : Il est défini de manière contraignante où le chiffrement est appliqué, avec quels algorithmes, et comment les clés sont générées, stockées, renouvelées et détruites sur l'ensemble de leur cycle de vie.** Document

Comment le prouver: Une politique de cryptographie avec des algorithmes approuvés et des longueurs de clé minimales, un chiffrement en transit (TLS) et au repos, plus une procédure de gestion des clés couvrant la génération, le stockage, le renouvellement et la destruction. Preuve par la politique plus la configuration du service de gestion des clés ou du coffre-fort.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.25 **Cycle de vie de développement sécurisé : Des règles pour le développement sécurisé des logiciels et des systèmes sont établies et appliquées.**

Comment le prouver: Une description du processus de développement avec des points de contrôle de sécurité par phase : exigences, conception, mise en œuvre, tests, mise en production, exploitation. Pour les petites équipes, une seule page renvoyant aux portes de contrôle concrètes de l'intégration continue et à l'obligation de revue suffit.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.26 **Exigences de sécurité des applications : Les exigences de sécurité pour les applications sont identifiées, spécifiées et approuvées pendant le développement et l'acquisition.**

Comment le prouver: Exigences de sécurité comme points explicites dans la liste des exigences ou comme liste de vérification réutilisable, orientée par exemple sur des référentiels courants de vérification de sécurité des applications. Preuve par des tickets ou des documents d'exigences avec une composante sécurité.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.27 **Principes d'architecture et d'ingénierie système sécurisées : Des principes d'ingénierie système sécurisée sont établis, documentés et appliqués aux activités de développement.**

Comment le prouver: Des principes documentés tels que le moindre privilège, la défense en profondeur, les configurations sécurisées par défaut, la minimisation des données et une approche de confiance zéro, avec leur application visible dans des croquis d'architecture ou des registres de décisions.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.28 **Codage sécurisé : Des principes de codage sécurisé sont appliqués dans le développement logiciel.**

Comment le prouver: Nouveau dans l'édition 2022. Preuve par des règles de codage contraignantes, une analyse statique de code et une détection de secrets comme portes de contrôle obligatoires en intégration continue, l'utilisation de bibliothèques vérifiées, et des revues de code documentées. Lorsque la séparation des tâches est impossible, des portes automatisées obligatoires remplacent la revue à quatre yeux ; justifiez-le et attestez-le avec la configuration du pipeline.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.29 **Tests de sécurité en développement et en recette : Des processus de tests de sécurité sont définis et mis en œuvre au sein du cycle de vie de développement.**

Comment le prouver: Tests de sécurité automatisés dans le pipeline (vérifications de dépendances, analyses statiques et dynamiques) plus un test d'intrusion périodique lorsque les besoins de protection sont élevés. Preuve par des rapports de test datés et le suivi des constats.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.30 **Développement externalisé : Les activités de développement externalisées sont dirigées, surveillées et revues.**

Comment le prouver: Lorsque le développement est externalisé, fixez les exigences de sécurité dans le contrat, sécurisez la propriété du code et le droit de revue, et réalisez des revues de code et des tests de sécurité avant la recette. En l'absence de développement externalisé, la non-applicabilité doit être justifiée de manière cohérente dans la Déclaration d'applicabilité.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.31 **Séparation des environnements de développement, de test et de production : Les environnements de développement, de test et de production sont séparés et protégés.**

Comment le prouver: Comptes, projets ou espaces de noms distincts, identifiants distincts et jeux de données distincts. En combinaison avec le point A.8.11, assurez-vous qu'aucune donnée de production ne se retrouve dans des environnements hors production. Preuve par la vue d'ensemble des environnements et l'attribution des droits.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.32 **Gestion des changements : Les changements apportés aux moyens et aux systèmes de traitement de l'information sont soumis à des procédures de gestion des changements.**

Comment le prouver: Un processus de changement avec demande, évaluation d'impact, tests, approbation, mise en œuvre et une voie de retour arrière. Dans les équipes de développement, un pipeline de pull requests avec des vérifications obligatoires et des déploiements journalisés satisfait ce point, à condition que l'historique soit immuable.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.33 **Informations de test : Les informations de test sont sélectionnées, protégées et gérées de manière appropriée.**

Comment le prouver: Le principe : aucune donnée personnelle réelle dans les systèmes de test. Lorsque cela est inévitable, documentez l'approbation, le masquage, la restriction d'accès et la suppression après le test. Preuve par le dispositif de données de test et les journaux de suppression.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

A.8.34 **Protection des systèmes d'information lors des tests d'audit : Les tests d'audit impliquant un accès aux systèmes opérationnels sont planifiés et convenus avec la direction afin d'éviter toute perturbation de l'exploitation.**

Comment le prouver: Un accord d'audit avec une fenêtre temporelle, un périmètre, un accès en lecture seule lorsque possible, une journalisation de l'accès d'audit et une approbation de la direction. Cela s'applique également aux tests d'intrusion : une autorisation de test écrite avec une fenêtre temporelle et un contact d'urgence constitue la preuve.

○ Ouvert ○ En cours ○ Satisfait ○ Non applicable

Preuve / justification

Les exigences sont formulées de manière autonome et ne remplacent pas le texte de la norme. Seule la norme originale de son éditeur fait foi. Cette liste est un outil de travail, elle ne constitue ni une preuve de conformité ni une certification. Leanshift n'est certifiée selon aucune de ces normes, n'est pas un organisme de certification et n'a aucun lien avec ISO, IEC, DIN, IATF, IAQG ou SAE. En cas de doute, la version allemande de cette liste prévaut.