Modèle de déclaration d'applicabilité ISO 27001

Les 93 mesures de l'Annexe A d'ISO/IEC 27001:2022, préchargées et prêtes à compléter — colonnes applicabilité, justification, état de mise en œuvre et preuves, exactement comme l'exige l'article 6.1.3(d).

Ce PDF est le compagnon d'impression et de revue. Le fichier de travail est le XLSX (validations par listes déroulantes, synthèse calculée automatiquement et feuille de correspondance avec l'article 21 de NIS2) ; une variante Markdown lisible par machine est fournie pour les agents IA. Les trois fichiers sont gratuits sur orbiqhq.com/templates/iso-27001-statement-of-applicability-template — sans e-mail requis.

Base normative : ISO/IEC 27001:2022 (y compris Amd 1:2024), article 6.1.3(d) et Annexe A. Les intitulés des mesures reprennent ceux de l'Annexe A ; le texte des mesures et les recommandations restent dans la norme et dans ISO/IEC 27002:2022 et ne sont pas reproduits.

Ce qu'exige l'article 6.1.3(d)

La déclaration d'applicabilité doit contenir : (1) les mesures nécessaires déterminées par le processus de traitement des risques ; (2) la justification de l'inclusion de chaque mesure ; (3) l'indication du caractère mis en œuvre ou non de chaque mesure nécessaire ; (4) la justification de l'exclusion de toute mesure de l'Annexe A. C'est l'un des documents obligatoires du SMSI, et votre auditeur de certification s'en sert comme feuille de route pour l'ensemble de l'audit.

Comment compléter le registre

1. Partez de votre évaluation des risques, pas de la liste des mesures. Les mesures sont retenues parce qu'elles traitent des risques identifiés ; la SoA consigne le résultat de cette décision.

2. Tranchez chaque ligne. Chacune des 93 mesures doit être marquée applicable ou exclue — une ligne vide se lit comme une SoA incomplète.

3. Justifiez les inclusions. Nommez le risque ou l'exigence légale, contractuelle ou métier que la mesure traite, indiquez son état de mise en œuvre et référencez les preuves.

4. Justifiez les exclusions sur le fond. « Aucun bureau physique » convient pour les mesures de périmètre physique ; « trop coûteux » non.

5. Maintenez-la à jour. Actualisez-la à chaque évolution substantielle des risques, des mesures ou du contexte, et revoyez-la au moins une fois par cycle du SMSI. Depuis l'Amd 1:2024, l'article 4.1 impose explicitement de déterminer si le changement climatique constitue un enjeu pertinent.

Les quatre thèmes de l'Annexe A

Thème	Mesures	Plage
Organisationnel	37	A.5.1 – A.5.37
Personnel	8	A.6.1 – A.6.8
Physique	14	A.7.1 – A.7.14
Technologique	34	A.8.1 – A.8.34
Total	93	

Onze mesures sont nouvelles dans la révision 2022 (signalées par un N dans le registre) : A.5.7, A.5.23, A.5.30, A.7.4, A.8.9, A.8.10, A.8.11, A.8.12, A.8.16, A.8.23 et A.8.28. Si votre dernière SoA a été rédigée au regard de l'édition 2013, c'est là que se trouvent généralement les écarts — et depuis le 31 octobre 2025, tous les certificats valides portent sur l'édition 2022.

Registre de la déclaration d'applicabilité

Complétez une ligne par mesure. Applicable : Oui/Non · Statut : Mise en œuvre / Partiellement mise en œuvre / Planifiée / Non mise en œuvre · Justification et preuves dans le XLSX de travail.

Mesures organisationnelles

ID	Intitulé de la mesure	Nouvelle 2022	Applicable	Statut
A.5.1	Politiques de sécurité de l'information		[ ] Oui [ ] Non	
A.5.2	Fonctions et responsabilités liées à la sécurité de l'information		[ ] Oui [ ] Non	
A.5.3	Séparation des tâches		[ ] Oui [ ] Non	
A.5.4	Responsabilités de la direction		[ ] Oui [ ] Non	
A.5.5	Relations avec les autorités		[ ] Oui [ ] Non	
A.5.6	Relations avec des groupes d'intérêt spécifiques		[ ] Oui [ ] Non	
A.5.7	Renseignement sur les menaces	N	[ ] Oui [ ] Non	
A.5.8	Sécurité de l'information dans la gestion de projet		[ ] Oui [ ] Non	
A.5.9	Inventaire des informations et autres actifs associés		[ ] Oui [ ] Non	
A.5.10	Utilisation acceptable des informations et autres actifs associés		[ ] Oui [ ] Non	
A.5.11	Restitution des actifs		[ ] Oui [ ] Non	
A.5.12	Classification des informations		[ ] Oui [ ] Non	
A.5.13	Marquage des informations		[ ] Oui [ ] Non	
A.5.14	Transfert d'informations		[ ] Oui [ ] Non	
A.5.15	Contrôle d'accès		[ ] Oui [ ] Non	
A.5.16	Gestion des identités		[ ] Oui [ ] Non	
A.5.17	Informations d'authentification		[ ] Oui [ ] Non	
A.5.18	Droits d'accès		[ ] Oui [ ] Non	
A.5.19	Sécurité de l'information dans les relations avec les fournisseurs		[ ] Oui [ ] Non	
A.5.20	Prise en compte de la sécurité de l'information dans les accords avec les fournisseurs		[ ] Oui [ ] Non	
A.5.21	Gestion de la sécurité de l'information dans la chaîne d'approvisionnement TIC		[ ] Oui [ ] Non	
A.5.22	Surveillance, revue et gestion des changements des services fournisseurs		[ ] Oui [ ] Non	
A.5.23	Sécurité de l'information liée à l'utilisation de services cloud	N	[ ] Oui [ ] Non	
A.5.24	Planification et préparation de la gestion des incidents de sécurité de l'information		[ ] Oui [ ] Non	
A.5.25	Évaluation des événements de sécurité de l'information et prise de décision		[ ] Oui [ ] Non	
A.5.26	Réponse aux incidents de sécurité de l'information		[ ] Oui [ ] Non	
A.5.27	Tirer des enseignements des incidents de sécurité de l'information		[ ] Oui [ ] Non	
A.5.28	Collecte de preuves		[ ] Oui [ ] Non	
A.5.29	Sécurité de l'information pendant une perturbation		[ ] Oui [ ] Non	
A.5.30	Préparation des TIC pour la continuité d'activité	N	[ ] Oui [ ] Non	
A.5.31	Exigences légales, statutaires, réglementaires et contractuelles		[ ] Oui [ ] Non	

ID	Intitulé de la mesure	Nouvelle 2022	Applicable	Statut
A.5.32	Droits de propriété intellectuelle		[ ] Oui [ ] Non	
A.5.33	Protection des enregistrements		[ ] Oui [ ] Non	
A.5.34	Protection de la vie privée et des données à caractère personnel (DCP)		[ ] Oui [ ] Non	
A.5.35	Revue indépendante de la sécurité de l'information		[ ] Oui [ ] Non	
A.5.36	Conformité aux politiques, règles et normes de sécurité de l'information		[ ] Oui [ ] Non	
A.5.37	Procédures d'exploitation documentées		[ ] Oui [ ] Non	

Mesures relatives au personnel

ID	Intitulé de la mesure	Nouvelle 2022	Applicable	Statut
A.6.1	Sélection des candidats		[ ] Oui [ ] Non	
A.6.2	Termes et conditions d'embauche		[ ] Oui [ ] Non	
A.6.3	Sensibilisation, apprentissage et formation à la sécurité de l'information		[ ] Oui [ ] Non	
A.6.4	Processus disciplinaire		[ ] Oui [ ] Non	
A.6.5	Responsabilités après la fin ou le changement d'un emploi		[ ] Oui [ ] Non	
A.6.6	Engagements de confidentialité ou de non-divulgation		[ ] Oui [ ] Non	
A.6.7	Travail à distance		[ ] Oui [ ] Non	
A.6.8	Signalement des événements de sécurité de l'information		[ ] Oui [ ] Non	

Mesures physiques

ID	Intitulé de la mesure	Nouvelle 2022	Applicable	Statut
A.7.1	Périmètres de sécurité physique		[ ] Oui [ ] Non	
A.7.2	Entrées physiques		[ ] Oui [ ] Non	
A.7.3	Sécurisation des bureaux, des salles et des installations		[ ] Oui [ ] Non	
A.7.4	Surveillance de la sécurité physique	N	[ ] Oui [ ] Non	
A.7.5	Protection contre les menaces physiques et environnementales		[ ] Oui [ ] Non	
A.7.6	Travail dans les zones sécurisées		[ ] Oui [ ] Non	
A.7.7	Bureau propre et écran vide		[ ] Oui [ ] Non	
A.7.8	Emplacement et protection du matériel		[ ] Oui [ ] Non	
A.7.9	Sécurité des actifs hors des locaux		[ ] Oui [ ] Non	
A.7.10	Supports de stockage		[ ] Oui [ ] Non	
A.7.11	Services généraux		[ ] Oui [ ] Non	
A.7.12	Sécurité du câblage		[ ] Oui [ ] Non	
A.7.13	Maintenance du matériel		[ ] Oui [ ] Non	
A.7.14	Mise au rebut ou réutilisation sécurisée du matériel		[ ] Oui [ ] Non	

Mesures technologiques

ID	Intitulé de la mesure	Nouvelle 2022	Applicable	Statut
A.8.1	Terminaux utilisateurs		[ ] Oui [ ] Non	
A.8.2	Droits d'accès privilégiés		[ ] Oui [ ] Non	
A.8.3	Restriction d'accès à l'information		[ ] Oui [ ] Non	
A.8.4	Accès au code source		[ ] Oui [ ] Non	
A.8.5	Authentification sécurisée		[ ] Oui [ ] Non	
A.8.6	Dimensionnement		[ ] Oui [ ] Non	
A.8.7	Protection contre les logiciels malveillants		[ ] Oui [ ] Non	
A.8.8	Gestion des vulnérabilités techniques		[ ] Oui [ ] Non	
A.8.9	Gestion des configurations	N	[ ] Oui [ ] Non	
A.8.10	Suppression des informations	N	[ ] Oui [ ] Non	
A.8.11	Masquage des données	N	[ ] Oui [ ] Non	
A.8.12	Prévention de la fuite de données	N	[ ] Oui [ ] Non	
A.8.13	Sauvegarde des informations		[ ] Oui [ ] Non	
A.8.14	Redondance des moyens de traitement de l'information		[ ] Oui [ ] Non	
A.8.15	Journalisation		[ ] Oui [ ] Non	
A.8.16	Activités de surveillance	N	[ ] Oui [ ] Non	
A.8.17	Synchronisation des horloges		[ ] Oui [ ] Non	
A.8.18	Utilisation de programmes utilitaires à privilèges		[ ] Oui [ ] Non	
A.8.19	Installation de logiciels sur des systèmes en exploitation		[ ] Oui [ ] Non	
A.8.20	Sécurité des réseaux		[ ] Oui [ ] Non	
A.8.21	Sécurité des services réseau		[ ] Oui [ ] Non	
A.8.22	Cloisonnement des réseaux		[ ] Oui [ ] Non	
A.8.23	Filtrage web	N	[ ] Oui [ ] Non	
A.8.24	Utilisation de la cryptographie		[ ] Oui [ ] Non	
A.8.25	Cycle de vie de développement sécurisé		[ ] Oui [ ] Non	
A.8.26	Exigences de sécurité applicatives		[ ] Oui [ ] Non	
A.8.27	Principes d'ingénierie et d'architecture des systèmes sécurisés		[ ] Oui [ ] Non	
A.8.28	Codage sécurisé	N	[ ] Oui [ ] Non	
A.8.29	Tests de sécurité dans le développement et la recette		[ ] Oui [ ] Non	
A.8.30	Développement externalisé		[ ] Oui [ ] Non	
A.8.31	Séparation des environnements de développement, de test et de production		[ ] Oui [ ] Non	
A.8.32	Gestion des changements		[ ] Oui [ ] Non	
A.8.33	Informations de test		[ ] Oui [ ] Non	
A.8.34	Protection des systèmes d'information pendant les tests d'audit		[ ] Oui [ ] Non	

Réutiliser la SoA comme preuve NIS2

Pour les entités de l'UE relevant de NIS2 (directive (UE) 2022/2555), l'ensemble des mesures applicables et leurs preuves se rattachent aux mesures de gestion des risques de l'article 21(2) — le XLSX contient la feuille de correspondance complète. L'alignement sur ISO 27001 soutient la conformité à NIS2 mais ne la démontre pas à lui seul : NIS2 comporte ses propres exigences de gouvernance, de signalement et de sanction au titre des lois nationales de transposition.

Du tableur à la preuve vivante

Une SoA sur tableur est périmée dès le lendemain de l'audit. Orbiq maintient le même registre de mesures connecté à des preuves vivantes et publie la face client vers un Trust Center européen — voir orbiqhq.com/platform/isms-software.

Version 1.0 · publié le 2026-07-13 · Utilisation libre ; attribution appréciée. Source : orbiqhq.com/templates/iso-27001-statement-of-applicability-template