M-KIS MERLIN KEEP IT SIMPLE

Annexe A ISO 27001:2022 : les 93 contrôles

Liste par thème, nouveautés 2022 repérées, colonnes pour votre déclaration d'applicabilité (SoA).

93	37	8	14	34
CONTRÔLES	A.5	A.6	A.7	A.8

Comment s'en servir. Pour chaque contrôle, cochez s'il est applicable et écrivez pourquoi : un risque de votre analyse, une exigence légale (RGPD, NIS2), une exigence d'un client ou une décision de la direction. Un contrôle exclu se justifie toujours : c'est la première question de l'auditeur.

Intitulés en anglais, tels que la norme les publie, avec une explication en français. Ce document ne remplace pas la norme ISO/IEC 27001:2022.

2022 **Les 11 contrôles nouveaux** de la version 2022, absents de la version 2013 : 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, A.8.28.

Explications détaillées, critères d'applicabilité et erreurs fréquentes en SoA : m-kis.fr/blog/iso-27001-annexe-a-2022-93-controles/

A.5 Contrôles organisationnels 37 contrôles

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.5.1	**Policies for information security** Politique SI globale + politiques thématiques (mot de passe, classification, télétravail). Validée direction, revue annuellement.	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.2	**Information security roles and responsibilities** Rôles SI documentés (RSSI, propriétaires d'actifs, RACI).	Organisationnel		Faible	☐ Oui ☐ Non	
A.5.3	**Segregation of duties** Séparation des tâches sensibles (qui demande, qui approuve, qui exécute).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.4	**Management responsibilities** Engagement direction sur conformité aux politiques.	Organisationnel		Faible	☐ Oui ☐ Non	
A.5.5	**Contact with authorities** Annuaire CNIL, ANSSI, gendarmerie/police, CERT. À jour.	Organisationnel		Faible	☐ Oui ☐ Non	
A.5.6	**Contact with special interest groups** Adhésion CLUSIF, CERT-FR, ISACA, OWASP…	Organisationnel		Faible	☐ Oui ☐ Non	

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.5.7	**Threat intelligence** Veille menaces (sources OSINT, CTI, IoC) intégrée à la gestion de risque.	Organisationnel	2022	Élevée	☐ Oui ☐ Non	
A.5.8	**Information security in project management** Sécurité dans cycle projet (analyse de risque dès cadrage).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.9	**Inventory of information and other associated assets** Inventaire des actifs (info, hardware, software, services). À jour.	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.10	**Acceptable use of information and other associated assets** Charte informatique signée.	Organisationnel		Faible	☐ Oui ☐ Non	
A.5.11	**Return of assets** Procédure de restitution départ collaborateur (laptop, badge, mobile).	Organisationnel		Faible	☐ Oui ☐ Non	
A.5.12	**Classification of information** Schéma de classification (public/interne/confidentiel/secret).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.13	**Labelling of information** Marquage documents selon classification.	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.14	**Information transfer** Règles de transfert (chiffrement, NDA, canaux autorisés).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.15	**Access control** Politique de contrôle d'accès (RBAC, moindre privilège).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.16	**Identity management** Cycle de vie des identités (création, modification, suppression).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.17	**Authentication information** Gestion mots de passe, secrets, clés.	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.18	**Access rights** Revue périodique des droits d'accès.	Organisationnel		Élevée	☐ Oui ☐ Non	
A.5.19	**Information security in supplier relationships** Politique fournisseurs (risk assessment, NDA, clauses SI).	Organisationnel		Moyenne	☐ Oui ☐ Non	

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.5.20	**Addressing information security within supplier agreements** Clauses SI dans contrats fournisseurs.	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.21	**Managing information security in the ICT supply chain** Sécurité supply chain logicielle (SBOM, signatures).	Organisationnel		Élevée	☐ Oui ☐ Non	
A.5.22	**Monitoring, review and change management of supplier services** Suivi performance/sécurité fournisseurs (SLA, audits).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.23	**Information security for use of cloud services** Politique cloud (IaaS/PaaS/SaaS), responsabilités partagées, sortie réversibilité.	Organisationnel	2022	Élevée	☐ Oui ☐ Non	
A.5.24	**Information security incident management planning and preparation** Plan de gestion d'incident SI (équipe, process, escalade).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.25	**Assessment and decision on information security events** Triage : incident vs événement, criticité, traitement.	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.26	**Response to information security incidents** Procédure de réponse (containment, eradication, recovery).	Organisationnel		Élevée	☐ Oui ☐ Non	
A.5.27	**Learning from information security incidents** Post-mortem, REX, plan d'amélioration.	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.28	**Collection of evidence** Préservation preuves (chain of custody, forensics).	Organisationnel		Élevée	☐ Oui ☐ Non	
A.5.29	**Information security during disruption** Maintien SI en cas de crise (BC).	Organisationnel		Élevée	☐ Oui ☐ Non	
A.5.30	**ICT readiness for business continuity** Préparation TIC à la continuité (RTO/RPO, tests PRA, redondance).	Organisationnel	2022	Élevée	☐ Oui ☐ Non	
A.5.31	**Legal, statutory, regulatory and contractual requirements** Registre des exigences légales applicables (RGPD, NIS2...).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.32	**Intellectual property rights** Gestion DPI (licences logicielles, contrefaçon).	Organisationnel		Faible	☐ Oui ☐ Non	

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.5.33	**Protection of records** Conservation registres (logs, contrats, traçabilité).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.34	**Privacy and protection of PII** Conformité RGPD (registres, DPIA, droits personnes).	Organisationnel		Élevée	☐ Oui ☐ Non	
A.5.35	**Independent review of information security** Audit indépendant SI (interne ou externe).	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.36	**Compliance with policies, rules and standards for information security** Vérification application des politiques.	Organisationnel		Moyenne	☐ Oui ☐ Non	
A.5.37	**Documented operating procedures** Procédures opérationnelles documentées.	Organisationnel		Faible	☐ Oui ☐ Non	

A.6 Contrôles humains 8 contrôles

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.6.1	**Screening** Vérifications d'antécédents avant embauche (selon poste).	Humain		Moyenne	☐ Oui ☐ Non	
A.6.2	**Terms and conditions of employment** Clauses SI dans contrat de travail (confidentialité, charte).	Humain		Faible	☐ Oui ☐ Non	
A.6.3	**Information security awareness, education and training** Programme de sensibilisation (e-learning, phishing, mise en route).	Humain		Moyenne	☐ Oui ☐ Non	
A.6.4	**Disciplinary process** Procédure disciplinaire en cas de violation SI.	Humain		Faible	☐ Oui ☐ Non	
A.6.5	**Responsibilities after termination or change of employment** Obligations post-emploi (NDA, restitution, désactivation comptes).	Humain		Faible	☐ Oui ☐ Non	
A.6.6	**Confidentiality or non-disclosure agreements** NDA collaborateurs, prestataires, partenaires.	Humain		Faible	☐ Oui ☐ Non	

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.6.7	**Remote working** Politique télétravail (VPN, MFA, EDR, domicile sécurisé).	Humain		Moyenne	☐ Oui ☐ Non	
A.6.8	**Information security event reporting** Procédure de signalement par les collaborateurs.	Humain		Faible	☐ Oui ☐ Non	

A.7 Contrôles physiques 14 contrôles

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.7.1	**Physical security perimeters** Périmètres physiques sécurisés (zones, contrôle d'accès).	Physique		Moyenne	☐ Oui ☐ Non	
A.7.2	**Physical entry** Contrôle d'accès aux locaux (badges, biométrie, sas).	Physique		Moyenne	☐ Oui ☐ Non	
A.7.3	**Securing offices, rooms and facilities** Sécurisation bureaux, salles serveurs, archives.	Physique		Moyenne	☐ Oui ☐ Non	
A.7.4	**Physical security monitoring** Vidéosurveillance, alarmes, détection intrusion physique.	Physique	2022	Moyenne	☐ Oui ☐ Non	
A.7.5	**Protecting against physical and environmental threats** Protection incendie, dégât des eaux, séismes selon contexte.	Physique		Moyenne	☐ Oui ☐ Non	
A.7.6	**Working in secure areas** Règles dans zones sécurisées (pas de mobile, pas de photo).	Physique		Faible	☐ Oui ☐ Non	
A.7.7	**Clear desk and clear screen** Bureau dégagé, écran verrouillé en absence.	Physique		Faible	☐ Oui ☐ Non	
A.7.8	**Equipment siting and protection** Implantation et protection des équipements.	Physique		Faible	☐ Oui ☐ Non	
A.7.9	**Security of assets off-premises** Sécurité des actifs hors site (laptops voyageurs).	Physique		Moyenne	☐ Oui ☐ Non	

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.7.10	**Storage media** Gestion supports amovibles (USB, disques).	Physique		Moyenne	☐ Oui ☐ Non	
A.7.11	**Supporting utilities** Services support (électricité, climatisation, eau).	Physique		Moyenne	☐ Oui ☐ Non	
A.7.12	**Cabling security** Sécurité des câblages (alimentation, données).	Physique		Faible	☐ Oui ☐ Non	
A.7.13	**Equipment maintenance** Maintenance équipements (sous-traitance, accès).	Physique		Faible	☐ Oui ☐ Non	
A.7.14	**Secure disposal or re-use of equipment** Mise au rebut sécurisée (effacement, destruction).	Physique		Moyenne	☐ Oui ☐ Non	

A.8 Contrôles technologiques 34 contrôles

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.8.1	**User end point devices** Sécurisation postes utilisateurs (EDR, MDM, durcissement).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.2	**Privileged access rights** Gestion comptes à privilèges (PAM, MFA, audit).	Technologique		Élevée	☐ Oui ☐ Non	
A.8.3	**Information access restriction** Restriction d'accès aux informations selon le besoin.	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.4	**Access to source code** Contrôle d'accès au code source (Git, branches protégées).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.5	**Secure authentication** Authentification forte (MFA, SSO, FIDO2).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.6	**Capacity management** Gestion capacité (CPU, stockage, bande passante).	Technologique		Moyenne	☐ Oui ☐ Non	

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.8.7	**Protection against malware** Antimalware, EDR, sandbox, scan.	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.8	**Management of technical vulnerabilities** Gestion vulnérabilités (scan, patch, CVE).	Technologique		Élevée	☐ Oui ☐ Non	
A.8.9	**Configuration management** Gestion des configurations (baselines, IaC, drift detection).	Technologique	2022	Élevée	☐ Oui ☐ Non	
A.8.10	**Information deletion** Effacement sécurisé des données (RGPD, fin de contrat).	Technologique	2022	Moyenne	☐ Oui ☐ Non	
A.8.11	**Data masking** Masquage / anonymisation données sensibles (test, dev, BI).	Technologique	2022	Élevée	☐ Oui ☐ Non	
A.8.12	**Data leakage prevention** DLP (e-mail, endpoint, cloud) pour prévenir l'exfiltration.	Technologique	2022	Élevée	☐ Oui ☐ Non	
A.8.13	**Information backup** Sauvegardes régulières, testées, hors-ligne (3-2-1).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.14	**Redundancy of information processing facilities** Redondance des installations de traitement.	Technologique		Élevée	☐ Oui ☐ Non	
A.8.15	**Logging** Journalisation des événements (système, applicatif, sécurité).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.16	**Monitoring activities** Supervision SI active (SIEM, SOC, alertes, corrélation).	Technologique	2022	Élevée	☐ Oui ☐ Non	
A.8.17	**Clock synchronization** Synchronisation NTP des systèmes.	Technologique		Faible	☐ Oui ☐ Non	
A.8.18	**Use of privileged utility programs** Maîtrise utilitaires à privilèges (sysinternals, scripts admin).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.19	**Installation of software on operational systems** Contrôle de l'installation logicielle en production.	Technologique		Moyenne	☐ Oui ☐ Non	

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.8.20	**Networks security** Sécurité réseau (segmentation, VLAN, firewall).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.21	**Security of network services** Sécurité services réseau (DNS, mail, proxy).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.22	**Segregation of networks** Cloisonnement réseau (DMZ, zones de confiance).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.23	**Web filtering** Filtrage URL / DNS / catégories de sites web.	Technologique	2022	Moyenne	☐ Oui ☐ Non	
A.8.24	**Use of cryptography** Politique de cryptographie (algos, clés, KMS).	Technologique		Élevée	☐ Oui ☐ Non	
A.8.25	**Secure development life cycle** Cycle de développement sécurisé (SDLC, SSDLC).	Technologique		Élevée	☐ Oui ☐ Non	
A.8.26	**Application security requirements** Exigences de sécurité applicative (OWASP, threat modeling).	Technologique		Élevée	☐ Oui ☐ Non	
A.8.27	**Secure system architecture and engineering principles** Architecture sécurisée par conception (zero trust, least privilege).	Technologique		Élevée	☐ Oui ☐ Non	
A.8.28	**Secure coding** Pratiques de codage sécurisé (lint, SAST, revue, OWASP Top 10).	Technologique	2022	Élevée	☐ Oui ☐ Non	
A.8.29	**Security testing in development and acceptance** Tests sécurité (DAST, SAST, pentest).	Technologique		Élevée	☐ Oui ☐ Non	
A.8.30	**Outsourced development** Développement externalisé encadré.	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.31	**Separation of development, test and production environments** Séparation dev/test/prod.	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.32	**Change management** Gestion du changement (CAB, ITIL, traçabilité).	Technologique		Moyenne	☐ Oui ☐ Non	

N°	Contrôle	Thème	Nouveau	Difficulté	Applicable	Justification (SoA)
A.8.33	**Test information** Données de test (anonymisation, dérivation).	Technologique		Moyenne	☐ Oui ☐ Non	
A.8.34	**Protection of information systems during audit testing** Précautions durant audits (read-only, fenêtre, sauvegarde).	Technologique		Moyenne	☐ Oui ☐ Non	

Passer de la liste à une SoA réelle ?

M-KIS confronte chaque contrôle à votre existant et livre une SoA et un plan d'action chiffré, à prix forfaitaire publié. Réponse par écrit.

contact@m-kis.fr
m-kis.fr