ayinedjimi-consultants.fr
ISO/IEC 27001:2022 — Template Gratuit

Checklist d'audit de certification ISO/IEC 27001:2022

Stage 1 (revue documentaire) + Stage 2 (audit opérationnel)

Référence	CHK-AUDIT-ISO27001-v1.0
Version	1.0
Date	—
Auditeur	—
Organisation auditée	—
Périmètre	—
Nombre de questions	103

Cette checklist est destinée à préparer et à conduire un audit de certification ISO/IEC 27001:2022, ou à servir de support d'auto-évaluation à l'auditée. Elle s'inspire des bonnes pratiques de la norme ISO/IEC 19011:2018 « Lignes directrices pour l'audit des systèmes de management » et couvre les deux phases d'audit telles que définies par ISO/IEC 17021-1.

> **Légende :** OK = preuve d'efficacité présentée — NOK = écart ou absence de preuve — N/A = non applicable. Une non-conformité majeure (NCM) doit être levée avant la certification ; une non-conformité mineure (NCm) fait l'objet d'un plan d'action ; une observation (OBS) signale un risque ou une opportunité d'amélioration.

STAGE 1 — Revue documentaire et préparation

> Le Stage 1 vise à vérifier que le SMSI est documenté, mis en œuvre depuis suffisamment longtemps (au minimum un cycle PDCA complet), et que l'organisation est prête pour le Stage 2. L'auditeur examine la documentation, conduit des entretiens préliminaires et identifie les zones d'attention pour le Stage 2.

Documentation SMSI

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
1.1.1	La politique de sécurité de l'information est-elle approuvée par la direction, datée, signée et diffusée ?	☐	☐	☐	
1.1.2	Le périmètre du SMSI est-il documenté (clause 4.3) et cohérent avec le contexte de l'organisation ?	☐	☐	☐	
1.1.3	Les parties intéressées et leurs exigences sont-elles formellement identifiées (clause 4.2) ?	☐	☐	☐	
1.1.4	La déclaration d'applicabilité (SoA) est-elle complète, à jour et justifie-t-elle les inclusions/exclusions ?	☐	☐	☐	
1.1.5	La méthode d'appréciation des risques est-elle documentée et reproductible (clause 6.1.2) ?	☐	☐	☐	
1.1.6	Les critères d'acceptation des risques sont-ils définis et approuvés (clause 6.1.2.a) ?	☐	☐	☐	
1.1.7	Le plan de traitement des risques est-il formalisé et approuvé par les propriétaires (clause 6.1.3) ?	☐	☐	☐	
1.1.8	Les objectifs de sécurité sont-ils définis, mesurables, planifiés (clause 6.2) ?	☐	☐	☐	
1.1.9	Les rôles et responsabilités SMSI sont-ils définis et communiqués (clause 5.3) ?	☐	☐	☐	
1.1.10	Les informations documentées requises sont-elles maîtrisées (clause 7.5) ?	☐	☐	☐	

Leadership et engagement

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
1.2.1	Comment la direction démontre-t-elle son engagement (clause 5.1) ? Preuves disponibles ?	☐	☐	☐	
1.2.2	Les ressources nécessaires au SMSI sont-elles attribuées (clause 7.1) ?	☐	☐	☐	
1.2.3	Le RSSI (ou équivalent) est-il rattaché à un niveau hiérarchique pertinent ?	☐	☐	☐	
1.2.4	La revue de direction est-elle planifiée et tenue (clause 9.3) ? Périodicité ?	☐	☐	☐	
1.2.5	Les comptes-rendus de revue de direction sont-ils archivés et signés ?	☐	☐	☐	

Compétences et sensibilisation

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
1.3.1	Le plan de formation SMSI est-il établi et exécuté (clause 7.2) ?	☐	☐	☐	
1.3.2	Les compétences des acteurs SMSI sont-elles évaluées (référentiel de compétences) ?	☐	☐	☐	

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
1.3.3	La sensibilisation est-elle déployée et tracée pour tout collaborateur (clause 7.3) ?	☐	☐	☐	
1.3.4	Quel est le taux de complétion des modules de sensibilisation obligatoires ?	☐	☐	☐	

Audit interne et amélioration

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
1.4.1	Le programme d'audit interne couvre-t-il l'ensemble du SMSI sur 3 ans (clause 9.2) ?	☐	☐	☐	
1.4.2	Les auditeurs internes sont-ils qualifiés et indépendants de l'audité ?	☐	☐	☐	
1.4.3	Le registre des non-conformités est-il maintenu (clause 10.2) ?	☐	☐	☐	
1.4.4	Les actions correctives sont-elles efficaces (mesure d'efficacité documentée) ?	☐	☐	☐	
1.4.5	Le processus d'amélioration continue est-il opérationnel (clause 10.1) ?	☐	☐	☐	

Préparation à l'audit Stage 2

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
1.5.1	Le SMSI a-t-il complété au moins un cycle PDCA complet (12 mois minimum) ?	☐	☐	☐	
1.5.2	Au moins un audit interne complet a-t-il été réalisé et clôturé ?	☐	☐	☐	
1.5.3	Au moins une revue de direction a-t-elle eu lieu avec PV ?	☐	☐	☐	
1.5.4	Les non-conformités identifiées en interne sont-elles soldées ou en plan d'action ?	☐	☐	☐	
1.5.5	Les indicateurs ISO 27004 sont-ils alimentés sur au moins 2 trimestres ?	☐	☐	☐	
1.5.6	La direction est-elle disponible pour l'audit Stage 2 ?	☐	☐	☐	

STAGE 2 — Audit opérationnel

> Le Stage 2 vérifie la mise en œuvre effective et l'efficacité du SMSI. L'auditeur conduit des entretiens, observe les opérations, examine les enregistrements et teste des contrôles. Les 93 contrôles de l'Annexe A sont audités par échantillonnage en fonction de la déclaration d'applicabilité (SoA).

A.5 — Contrôles organisationnels (37 contrôles)

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
2.1.1	A.5.1 — Les politiques de sécurité sont-elles approuvées, communiquées et révisées annuellement ?	☐	☐	☐	
2.1.2	A.5.2 — Les rôles et responsabilités sécurité sont-ils définis dans les fiches de poste ?	☐	☐	☐	
2.1.3	A.5.3 — La séparation des tâches est-elle effective pour les activités sensibles (financières, IT) ?	☐	☐	☐	
2.1.4	A.5.4 — La direction définit-elle et communique-t-elle ses attentes en matière de sécurité ?	☐	☐	☐	
2.1.5	A.5.5 — Les contacts avec les autorités (ANSSI, CNIL, police) sont-ils identifiés et tenus à jour ?	☐	☐	☐	
2.1.6	A.5.6 — Des contacts avec des groupes spécialisés (CERT-FR, CLUSIF) sont-ils maintenus ?	☐	☐	☐	
2.1.7	A.5.7 — La threat intelligence est-elle collectée, analysée et opérationnalisée ?	☐	☐	☐	
2.1.8	A.5.8 — La sécurité est-elle intégrée dès la phase d'avant-projet (security by design) ?	☐	☐	☐	
2.1.9	A.5.9 — L'inventaire des actifs informationnels est-il complet, à jour et propriétaire identifié ?	☐	☐	☐	
2.1.10	A.5.10 — Les règles d'utilisation acceptable sont-elles publiées et acceptées (charte SI signée) ?	☐	☐	☐	
2.1.11	A.5.15 — Le contrôle d'accès est-il basé sur des rôles documentés (RBAC) ?	☐	☐	☐	
2.1.12	A.5.16 — La gestion des identités est-elle centralisée (IAM/IGA) ?	☐	☐	☐	
2.1.13	A.5.17 — La politique de mots de passe est-elle conforme aux exigences (longueur, MFA, etc.) ?	☐	☐	☐	
2.1.14	A.5.18 — Les revues périodiques des droits d'accès sont-elles tracées ?	☐	☐	☐	
2.1.15	A.5.19 à A.5.23 — Les fournisseurs sont-ils évalués, contractualisés (clauses sécurité), suivis ?	☐	☐	☐	
2.1.16	A.5.24 — Existe-t-il une procédure de gestion des incidents avec rôles et responsabilités ?	☐	☐	☐	
2.1.17	A.5.25 à A.5.27 — Les incidents sont-ils qualifiés, traités, et donnent-ils lieu à un RETEX ?	☐	☐	☐	
2.1.18	A.5.29 — La sécurité est-elle maintenue durant les perturbations (PCA, PRA) ?	☐	☐	☐	
2.1.19	A.5.30 — Les TIC sont-elles préparées à la continuité (RTO, RPO, tests) ?	☐	☐	☐	
2.1.20	A.5.31 — Le registre des exigences légales/contractuelles est-il maintenu ?	☐	☐	☐	

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
2.1.21	A.5.34 — La protection des données personnelles est-elle conforme RGPD (registre, AIPD, DPO) ?	☐	☐	☐	
2.1.22	A.5.35 — Une revue indépendante de la sécurité est-elle réalisée (audit externe) ?	☐	☐	☐	

A.6 — Contrôles relatifs aux personnes (8 contrôles)

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
2.2.1	A.6.1 — Les candidats font-ils l'objet d'un filtrage pré-embauche proportionné ?	☐	☐	☐	
2.2.2	A.6.2 — Les contrats incluent-ils les obligations sécurité et confidentialité ?	☐	☐	☐	
2.2.3	A.6.3 — La sensibilisation est-elle obligatoire à l'embauche et annuellement ?	☐	☐	☐	
2.2.4	A.6.4 — Le processus disciplinaire pour les violations sécurité est-il défini ?	☐	☐	☐	
2.2.5	A.6.5 — Les responsabilités post-emploi sont-elles précisées dans les contrats ?	☐	☐	☐	
2.2.6	A.6.6 — Des engagements de confidentialité (NDA) sont-ils signés avec tiers ?	☐	☐	☐	
2.2.7	A.6.7 — La politique de télétravail est-elle déployée et respectée ?	☐	☐	☐	
2.2.8	A.6.8 — Un canal de signalement des événements sécurité est-il opérationnel et connu ?	☐	☐	☐	

A.7 — Contrôles physiques (14 contrôles)

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
2.3.1	A.7.1 — Les périmètres de sécurité physique sont-ils définis et matérialisés ?	☐	☐	☐	
2.3.2	A.7.2 — Les contrôles d'accès physique sont-ils opérationnels (badges, biométrie, journalisation) ?	☐	☐	☐	
2.3.3	A.7.3 — Les bureaux et locaux sont-ils sécurisés (caméras, alarmes, gardiennage) ?	☐	☐	☐	
2.3.4	A.7.4 — La surveillance physique est-elle continue (vidéo, ronde, télésurveillance) ?	☐	☐	☐	
2.3.5	A.7.5 — La protection contre les menaces environnementales (incendie, eau, électrique) est-elle en place ?	☐	☐	☐	
2.3.6	A.7.7 — Les politiques de bureau propre et écran vide sont-elles appliquées ?	☐	☐	☐	
2.3.7	A.7.8 — L'implantation du matériel est-elle sécurisée (salle blanche, climatisation, onduleurs) ?	☐	☐	☐	
2.3.8	A.7.10 — Les supports amovibles sont-ils maîtrisés (interdiction USB non chiffrée, etc.) ?	☐	☐	☐	
2.3.9	A.7.14 — La mise au rebut du matériel est-elle sécurisée (effacement sécurisé, certificat destruction) ?	☐	☐	☐	

A.8 — Contrôles technologiques (34 contrôles)

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
2.4.1	A.8.1 — Les terminaux utilisateurs sont-ils protégés (EDR, chiffrement, durcissement) ?	☐	☐	☐	

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
2.4.2	A.8.2 — Les comptes à privilèges sont-ils gérés via PAM, avec MFA et journalisation ?	☐	☐	☐	
2.4.3	A.8.3 — L'accès aux informations est-il restreint selon le besoin d'en connaître ?	☐	☐	☐	
2.4.4	A.8.4 — L'accès au code source est-il restreint et tracé ?	☐	☐	☐	
2.4.5	A.8.5 — L'authentification sécurisée (MFA, FIDO2) est-elle déployée ?	☐	☐	☐	
2.4.6	A.8.6 — Le dimensionnement (capacité) des ressources est-il surveillé et planifié ?	☐	☐	☐	
2.4.7	A.8.7 — Une protection anti-malware est-elle déployée sur 100% des endpoints ?	☐	☐	☐	
2.4.8	A.8.8 — La gestion des vulnérabilités est-elle continue (scans, patch management) ?	☐	☐	☐	
2.4.9	A.8.9 — La gestion des configurations (baseline, drift detection) est-elle en place ?	☐	☐	☐	
2.4.10	A.8.10 — La suppression des informations est-elle sécurisée (effacement cryptographique) ?	☐	☐	☐	
2.4.11	A.8.11 — Le masquage / pseudonymisation est-il appliqué (pré-prod, tests) ?	☐	☐	☐	
2.4.12	A.8.12 — La prévention de fuite de données (DLP) est-elle déployée ?	☐	☐	☐	
2.4.13	A.8.13 — Les sauvegardes sont-elles testées (restauration trimestrielle) et immuables ?	☐	☐	☐	
2.4.14	A.8.14 — La redondance des moyens de traitement est-elle effective (HA, DR) ?	☐	☐	☐	
2.4.15	A.8.15 — La journalisation centralisée (SIEM) couvre-t-elle ≥ 95% des sources critiques ?	☐	☐	☐	
2.4.16	A.8.16 — Une surveillance active (SOC) est-elle opérationnelle 24/7 ?	☐	☐	☐	
2.4.17	A.8.17 — Les horloges sont-elles synchronisées (NTP) ?	☐	☐	☐	
2.4.18	A.8.18 — Les programmes utilitaires privilégiés sont-ils restreints ?	☐	☐	☐	
2.4.19	A.8.19 — L'installation de logiciels est-elle contrôlée (whitelist, app catalog) ?	☐	☐	☐	
2.4.20	A.8.20 — La sécurité des réseaux est-elle assurée (segmentation, IDS/IPS) ?	☐	☐	☐	
2.4.21	A.8.22 — Les réseaux sont-ils cloisonnés (DMZ, zones de confiance, micro-segmentation) ?	☐	☐	☐	
2.4.22	A.8.23 — Un filtrage web est-il en place (proxy, secure web gateway) ?	☐	☐	☐	
2.4.23	A.8.24 — La cryptographie est-elle conforme à la politique (algorithmes ANSSI, KMS) ?	☐	☐	☐	
2.4.24	A.8.25 à A.8.30 — Le cycle de vie de développement sécurisé (SDLC) est-il opérationnel ?	☐	☐	☐	
2.4.25	A.8.31 — Les environnements (dev/test/prod) sont-ils strictement séparés ?	☐	☐	☐	
2.4.26	A.8.32 — La gestion des changements (CAB, RFC, rollback) est-elle effective ?	☐	☐	☐	

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
2.4.27	A.8.33 — Les données de test sont-elles maîtrisées (pas de prod en clair en test) ?	☐	☐	☐	
2.4.28	A.8.34 — Les tests d'audit sont-ils planifiés sans perturber la production ?	☐	☐	☐	

Conduite d'audit Stage 2 — questions transverses

#	Question d'audit	OK	NOK	N/A	Évidence / Commentaire
2.5.1	Les preuves d'efficacité (et non seulement de mise en œuvre) sont-elles disponibles ?	☐	☐	☐	
2.5.2	Un échantillon représentatif d'enregistrements est-il fourni à l'auditeur sur demande ?	☐	☐	☐	
2.5.3	Les acteurs interviewés démontrent-ils une connaissance opérationnelle de leur rôle ?	☐	☐	☐	
2.5.4	Le SMSI fonctionne-t-il en routine, indépendamment de l'audit (artificialité limitée) ?	☐	☐	☐	
2.5.5	Les indicateurs ISO 27004 sont-ils utilisés en revue de direction pour pilotage ?	☐	☐	☐	
2.5.6	Le SMSI s'améliore-t-il (tendances positives sur 12-24 mois) ?	☐	☐	☐	

Synthèse de l'audit

Catégorie	Nombre	Référence(s)
Non-conformités majeures (NCM)		
Non-conformités mineures (NCm)		
Observations (OBS)		
Opportunités d'amélioration (OA)		
Conclusion auditeur lead		

Signature auditeur lead :

Nom	Date	Signature