Kit Audit Interne ISO 27001:2022

50 questions essentielles | Questionnaire d'évaluation | Ayi NEDJIMI Consultants

Auditeur	
Date d'audit	
Périmètre audité	
Personnes interviewées	

Notation : C = Conforme | OC = Observation (conformité partielle) | NC min = Non-conformité mineure | NC maj = Non-conformité majeure | NA = Non applicable
Chaque question doit être documentée avec la preuve collectée (document, capture, témoignage).

1. Contexte et leadership (Clauses 4-5)

#	Question d'audit	Statut	Preuve
1	Le périmètre du SMSI est-il clairement défini et documenté ?		
2	Les parties intéressées et leurs exigences sont-elles identifiées ?		
3	La direction a-t-elle formellement approuvé la PSSI ?		
4	Les rôles et responsabilités SSI sont-ils clairement attribués ?		
5	Un budget dédié à la sécurité est-il alloué annuellement ?		

2. Planification et gestion des risques (Clause 6)

#	Question d'audit	Statut	Preuve
6	Une analyse de risques formelle a-t-elle été réalisée (EBIOS RM, ISO 27005) ?		
7	Les critères d'acceptation des risques sont-ils définis par la direction ?		
8	Le plan de traitement des risques est-il à jour et suivi ?		
9	Les objectifs de sécurité sont-ils mesurables et suivis ?		
10	La Déclaration d'Applicabilité (SoA) est-elle à jour (version 2022) ?		

3. Ressources et compétences (Clause 7)

#	Question d'audit	Statut	Preuve
11	Les compétences SSI nécessaires sont-elles identifiées ?		
12	Un plan de formation cybersécurité est-il en place ?		
13	Des campagnes de sensibilisation sont-elles menées régulièrement ?		
14	La documentation du SMSI est-elle contrôlée (versions, approbations) ?		
15	Les enregistrements de sécurité sont-ils conservés et accessibles ?		

4. Contrôle d'accès et identités

#	Question d'audit	Statut	Preuve
16	Le principe du moindre privilège est-il appliqué systématiquement ?		
17	L'authentification multi-facteurs (MFA) est-elle déployée sur les accès critiques ?		

18	Les comptes privilégiés sont-ils gérés par une solution PAM ?		
19	Les revues de droits d'accès sont-elles réalisées périodiquement ?		
20	Les comptes sont-ils désactivés immédiatement lors des départs ?		

5. Sécurité opérationnelle

#	Question d'audit	Statut	Preuve
21	Les procédures d'exploitation sont-elles documentées et à jour ?		
22	La gestion des changements est-elle formalisée (CAB, validation) ?		
23	Les environnements (dev/test/prod) sont-ils séparés ?		
24	Un antimalware est-il déployé et à jour sur tous les postes ?		
25	Les vulnérabilités sont-elles scannées et patchées régulièrement ?		

6. Journalisation et surveillance

#	Question d'audit	Statut	Preuve
26	Les logs sont-ils centralisés (SIEM) et conservés suffisamment ?		
27	Les événements de sécurité sont-ils surveillés en temps réel ?		
28	Les horloges sont-elles synchronisées (NTP) ?		
29	Des alertes sont-elles configurées pour les événements critiques ?		
30	Les logs sont-ils protégés contre la modification/suppression ?		

7. Sécurité réseau et chiffrement

#	Question d'audit	Statut	Preuve
31	Le réseau est-il segmenté (VLAN, zones, DMZ) ?		
32	Les flux réseau sont-ils filtrés par des pare-feu configurés ?		
33	Le chiffrement est-il appliqué aux données sensibles au repos ?		
34	Les communications sensibles sont-elles chiffrées en transit (TLS) ?		
35	Les clés de chiffrement sont-elles gérées de manière sécurisée ?		

8. Gestion des incidents

#	Question d'audit	Statut	Preuve
36	Une procédure de gestion des incidents est-elle définie ?		
37	Les incidents sont-ils classifiés par niveau de gravité ?		
38	Les délais de notification (NIS2 : 24h/72h) sont-ils respectables ?		
39	Un retour d'expérience est-il systématique après chaque incident ?		
40	Les preuves numériques sont-elles collectées conformément aux règles ?		

9. Continuité et sauvegarde

#	Question d'audit	Statut	Preuve
41	Un PCA/PRA est-il formalisé et approuvé ?		

42	Les sauvegardes suivent-elles la règle 3-2-1 ?
43	Les restaurations sont-elles testées régulièrement ?
44	Les RTO/RPO sont-ils définis par processus métier ?
45	Un exercice de crise a-t-il été réalisé dans les 12 derniers mois ?

10. Fournisseurs et amélioration continue

#	Question d'audit	Statut	Preuve
46	Les fournisseurs critiques sont-ils évalués sur leur sécurité ?		
47	Les clauses de sécurité sont-elles intégrées aux contrats ?		
48	Les non-conformités sont-elles suivies jusqu'à résolution ?		
49	Des indicateurs de performance SSI (KPIs) sont-ils mesurés ?		
50	La revue de direction du SMSI est-elle réalisée au moins annuellement ?		