# Rapport d'Audit ISO 27001 - dna

Date : 07/08/2025

## 4. Contexte de l'organisation

Question : Le contexte interne et externe de l'organisation est-il documenté ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '4. Contexte de l'organisation'.

## 4. Contexte de l'organisation

Question : Les besoins et attentes des parties prenantes sont-ils identifiés ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '4. Contexte de l'organisation'.

## 4. Contexte de l'organisation

Question : Le périmètre du SMSI est-il défini et documenté ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '4. Contexte de l'organisation'.

## 5. Leadership

Question : La direction démontre-t-elle son engagement envers le SMSI ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '5. Leadership'.

## 5. Leadership

Question : Une politique de sécurité est-elle définie et approuvée par la direction ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '5. Leadership'.

## 6. Planification

Question : Les risques liés à la sécurité de l'information sont-ils identifiés et évalués ?

Statut : nan

Réponse : no

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '6. Planification'.

## 6. Planification

Question : Des objectifs mesurables de sécurité sont-ils définis et suivis ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '6. Planification'.

## 7. Support

Question : Les ressources nécessaires au SMSI sont-elles allouées ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '7. Support'.

## 7. Support

Question : Le personnel est-il compétent et formé à la sécurité de l'information ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '7. Support'.

## 8. Fonctionnement

Question : Les opérations sont-elles planifiées et maîtrisées ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '8. Fonctionnement'.

## 8. Fonctionnement

Question : Les résultats des évaluations des risques sont-ils intégrés aux activités ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '8. Fonctionnement'.

## 9. Évaluation des performances

Question : La performance du SMSI est-elle mesurée et évaluée ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '9. Évaluation des performances'.

## 9. Évaluation des performances

Question : Des audits internes sont-ils réalisés conformément au programme d'audit ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '9. Évaluation des performances'.

## 10. Amélioration

Question : Les non-conformités sont-elles traitées par des actions correctives ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '10. Amélioration'.

## 10. Amélioration

Question : L'amélioration continue du SMSI est-elle démontrée ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine '10. Amélioration'.

## A.5 Politiques de sécurité de l'information

Question : Existe-t-il une politique de sécurité formellement approuvée par la direction ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.5 Politiques de sécurité de l'information'.

## A.5 Politiques de sécurité de l'information

Question : La politique est-elle communiquée à tous les employés et parties prenantes pertinentes ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.5 Politiques de sécurité de l'information'.

## A.5 Politiques de sécurité de l'information

Question : Un processus de révision régulière de la politique est-il en place et documenté ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.5 Politiques de sécurité de l'information'.

## A.6 Organisation de la sécurité de l'information

Question : Les rôles et responsabilités en matière de sécurité de l'information sont-ils clairement définis et communiqués ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.6 Organisation de la sécurité de l'information'.

## A.6 Organisation de la sécurité de l'information

Question : Existe-t-il un responsable de la sécurité de l'information désigné (RSSI) ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.6 Organisation de la sécurité de l'information'.

## A.6 Organisation de la sécurité de l'information

Question : La sécurité est-elle coordonnée entre les différents départements ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.6 Organisation de la sécurité de l'information'.

## A.7 Sécurité des ressources humaines

Question : Les candidats font-ils l’objet d’une vérification d’antécédents avant embauche ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.7 Sécurité des ressources humaines'.

## A.7 Sécurité des ressources humaines

Question : Une formation à la sécurité est-elle dispensée à l’intégration ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.7 Sécurité des ressources humaines'.

## A.7 Sécurité des ressources humaines

Question : Les obligations contractuelles incluent-elles des exigences de sécurité ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.7 Sécurité des ressources humaines'.

## A.8 Gestion des actifs

Question : Un inventaire des actifs est-il tenu à jour et approuvé ?

Statut : nan

Réponse : oui

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.8 Gestion des actifs'.

## A.8 Gestion des actifs

Question : Les actifs sont-ils classifiés selon leur sensibilité ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.8 Gestion des actifs'.

## A.8 Gestion des actifs

Question : Des règles d'utilisation acceptable des actifs sont-elles définies ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.8 Gestion des actifs'.

## A.9 Contrôle d'accès

Question : Existe-t-il une politique de contrôle d’accès ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.9 Contrôle d'accès'.

## A.9 Contrôle d'accès

Question : Les droits sont-ils accordés selon le principe du moindre privilège ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.9 Contrôle d'accès'.

## A.9 Contrôle d'accès

Question : Les droits sont-ils révoqués immédiatement en cas de départ ou changement de poste ?

Statut : nan

Réponse : non

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.9 Contrôle d'accès'.

## A.10 Cryptographie

Question : Une politique d’utilisation de la cryptographie est-elle définie ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.10 Cryptographie'.

## A.10 Cryptographie

Question : Les clés cryptographiques sont-elles gérées de manière sécurisée ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.10 Cryptographie'.

## A.11 Sécurité physique et environnementale

Question : Les accès physiques aux zones sensibles sont-ils contrôlés ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.11 Sécurité physique et environnementale'.

## A.11 Sécurité physique et environnementale

Question : Les équipements sont-ils protégés contre les menaces environnementales ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.11 Sécurité physique et environnementale'.

## A.11 Sécurité physique et environnementale

Question : Une procédure de gestion des visiteurs est-elle appliquée ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.11 Sécurité physique et environnementale'.

## A.12 Sécurité opérationnelle

Question : Les procédures opérationnelles sont-elles documentées et accessibles ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.12 Sécurité opérationnelle'.

## A.12 Sécurité opérationnelle

Question : Les changements sont-ils contrôlés par un processus de gestion des changements ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.12 Sécurité opérationnelle'.

## A.12 Sécurité opérationnelle

Question : Les journaux d'activité sont-ils collectés et analysés régulièrement ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.12 Sécurité opérationnelle'.

## A.13 Sécurité des communications

Question : Les réseaux sont-ils segmentés et protégés ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.13 Sécurité des communications'.

## A.13 Sécurité des communications

Question : Les communications sensibles sont-elles chiffrées ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.13 Sécurité des communications'.

## A.13 Sécurité des communications

Question : Une politique d'utilisation des services de messagerie est-elle définie ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.13 Sécurité des communications'.

## A.14 Acquisition, développement et maintenance des systèmes

Question : Les exigences de sécurité sont-elles intégrées dans les projets ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.14 Acquisition, développement et maintenance des systèmes'.

## A.14 Acquisition, développement et maintenance des systèmes

Question : Des tests de sécurité sont-ils effectués avant mise en production ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.14 Acquisition, développement et maintenance des systèmes'.

## A.14 Acquisition, développement et maintenance des systèmes

Question : Les vulnérabilités applicatives sont-elles corrigées rapidement ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.14 Acquisition, développement et maintenance des systèmes'.

## A.15 Relations avec les fournisseurs

Question : Les contrats fournisseurs incluent-ils des clauses de sécurité ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.15 Relations avec les fournisseurs'.

## A.15 Relations avec les fournisseurs

Question : Les performances sécurité des fournisseurs sont-elles évaluées ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.15 Relations avec les fournisseurs'.

## A.16 Gestion des incidents de sécurité

Question : Un processus de gestion des incidents est-il défini ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.16 Gestion des incidents de sécurité'.

## A.16 Gestion des incidents de sécurité

Question : Les incidents sont-ils documentés et analysés ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.16 Gestion des incidents de sécurité'.

## A.16 Gestion des incidents de sécurité

Question : Les leçons apprises sont-elles intégrées aux procédures ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.16 Gestion des incidents de sécurité'.

## A.17 Continuité d'activité

Question : La sécurité de l'information est-elle intégrée au PCA ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.17 Continuité d'activité'.

## A.17 Continuité d'activité

Question : Le PCA est-il testé régulièrement ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.17 Continuité d'activité'.

## A.18 Conformité

Question : Les exigences légales et réglementaires sont-elles respectées ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.18 Conformité'.

## A.18 Conformité

Question : Des audits internes sont-ils réalisés périodiquement ?

Statut : nan

Réponse : nan

Recommandation : Compléter et formaliser les mesures existantes pour le domaine 'A.18 Conformité'.