# Rapport d'Audit ISO 27001 - d&a

Date : 06/08/2025

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

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

Statut : ✅ Conforme

Réponse : Oui

Recommandation : Continuer à maintenir et à promouvoir la PGSSI au sein de l'organisation.

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

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

Statut : ✅ Conforme

Réponse : Oui

Recommandation : Assurer une communication régulière et des sessions de sensibilisation sur la PGSSI.

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

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus de révision régulière de la PGSSI et le documenter.

## 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 : ✅ Conforme

Réponse : Oui

Recommandation : S'assurer que tous les employés comprennent leurs rôles et responsabilités en matière de sécurité.

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

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

Statut : ✅ Conforme

Réponse : Oui

Recommandation : Renforcer le rôle du RSSI en lui fournissant des ressources adéquates.

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

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un mécanisme de coordination de la sécurité entre les départements.

## A.7 Sécurité des ressources humaines

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus de vérification d'antécédents pour tous les candidats.

## A.7 Sécurité des ressources humaines

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un programme de formation à la sécurité pour les nouveaux employés lors de leur intégration.

## A.7 Sécurité des ressources humaines

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Inclure des exigences de sécurité dans les contrats avec les employés et les partenaires.

## A.8 Gestion des actifs

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir et maintenir un inventaire des actifs à jour et approuvé.

## A.8 Gestion des actifs

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

Statut : ✅ Conforme

Réponse : Oui

Recommandation : Continuer à appliquer la classification des actifs et à sensibiliser le personnel.

## A.8 Gestion des actifs

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir des règles d'utilisation acceptable des actifs et les communiquer à tous les employés.

## A.9 Contrôle d'accès

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Élaborer une politique de contrôle d'accès et la communiquer à tous les employés.

## A.9 Contrôle d'accès

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place des contrôles pour garantir que les droits d'accès respectent le principe du moindre privilège.

## A.9 Contrôle d'accès

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un processus pour révoquer immédiatement les droits d'accès en cas de départ ou changement de poste.

## A.10 Cryptographie

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Élaborer une politique d'utilisation de la cryptographie et la communiquer à tous les employés.

## A.10 Cryptographie

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place des procédures pour la gestion sécurisée des clés cryptographiques.

## A.11 Sécurité physique et environnementale

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir des contrôles d'accès physiques pour les zones sensibles.

## A.11 Sécurité physique et environnementale

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place des mesures de protection pour les équipements contre les menaces environnementales.

## A.11 Sécurité physique et environnementale

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir une procédure de gestion des visiteurs pour contrôler l'accès aux locaux.

## A.12 Sécurité opérationnelle

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Documenter et rendre accessibles toutes les procédures opérationnelles.

## A.12 Sécurité opérationnelle

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un processus de gestion des changements pour contrôler les modifications.

## A.12 Sécurité opérationnelle

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus pour collecter et analyser régulièrement les journaux d'activité.

## A.13 Sécurité des communications

Question : Les réseaux sont-ils segmentés et protégés ?

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place des mesures de segmentation et de protection des réseaux.

## A.13 Sécurité des communications

Question : Les communications sensibles sont-elles chiffrées ?

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir des procédures pour chiffrer les communications sensibles.

## A.13 Sécurité des communications

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Élaborer une politique d'utilisation des services de messagerie.

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

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : S'assurer que les exigences de sécurité sont intégrées dans tous les projets.

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

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place des tests de sécurité avant toute mise en production.

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

Question : Les vulnérabilités applicatives sont-elles corrigées rapidement ?

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un processus pour corriger rapidement les vulnérabilités applicatives.

## A.15 Relations avec les fournisseurs

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Inclure des clauses de sécurité dans tous les contrats avec les fournisseurs.

## A.15 Relations avec les fournisseurs

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus d'évaluation des performances sécurité des fournisseurs.

## A.16 Gestion des incidents de sécurité

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un processus de gestion des incidents de sécurité.

## A.16 Gestion des incidents de sécurité

Question : Les incidents sont-ils documentés et analysés ?

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus pour documenter et analyser les incidents de sécurité.

## A.16 Gestion des incidents de sécurité

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un processus pour intégrer les leçons apprises aux procédures de sécurité.

## A.17 Continuité d'activité

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Intégrer la sécurité de l'information dans le PCA.

## A.17 Continuité d'activité

Question : Le PCA est-il testé régulièrement ?

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus pour tester régulièrement le PCA.

## A.18 Conformité

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un processus pour garantir le respect des exigences légales et réglementaires.

## A.18 Conformité

Question : Des audits internes sont-ils réalisés périodiquement ?

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus pour réaliser des audits internes périodiques.