# Rapport d'Audit ISO 27001 - cfg

Date : 18/08/2025

## 4. Contexte de l'organisation

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Documenter le contexte interne et externe de l'organisation.

## 4. Contexte de l'organisation

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Identifier et documenter les besoins et attentes des parties prenantes.

## 4. Contexte de l'organisation

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Définir et documenter le périmètre du SMSI.

## 5. Leadership

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir des preuves de l'engagement de la direction envers le SMSI.

## 5. Leadership

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Définir et faire approuver une politique de sécurité par la direction.

## 6. Planification

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus d'identification et d'évaluation des risques liés à la sécurité de l'information.

## 6. Planification

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Définir des objectifs mesurables de sécurité et mettre en place un suivi.

## 7. Support

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Allouer les ressources nécessaires au SMSI.

## 7. Support

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un programme de formation à la sécurité de l'information pour le personnel.

## 8. Fonctionnement

Question : Les opérations sont-elles planifiées et maîtrisées ?

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir des procédures pour la planification et la maîtrise des opérations.

## 8. Fonctionnement

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Intégrer les résultats des évaluations des risques dans les activités opérationnelles.

## 9. Évaluation des performances

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place des indicateurs de performance pour mesurer et évaluer le SMSI.

## 9. Évaluation des performances

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir un programme d'audit interne et réaliser des audits conformément à ce programme.

## 10. Amélioration

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus pour traiter les non-conformités par des actions correctives.

## 10. Amélioration

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir des mécanismes pour démontrer l'amélioration continue du SMSI.

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

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir et faire approuver une politique de sécurité formelle par la direction.

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

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un plan de communication pour diffuser la politique de sécurité.

## 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 : Établir un processus de révision régulière de la politique de sécurité.

## 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 : Continuer à communiquer ces rôles et responsabilités aux nouvelles recrues.

## 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 : Assurer que le RSSI dispose des ressources nécessaires pour remplir ses fonctions.

## 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 : Mettre en place des mécanismes 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 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 obligations contractuelles des employés.

## 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 : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place un processus de classification des actifs selon leur sensibilité.

## 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.

## A.9 Contrôle d'accès

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Établir une politique de contrôle d'accès.

## 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 sont accordés selon 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 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 : Établir une politique d'utilisation de la cryptographie.

## 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 : Mettre en place des contrôles d'accès physiques aux 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 : Établir des mesures de protection des 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.

## A.12 Sécurité opérationnelle

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

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Documenter et rendre accessibles 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.

## A.12 Sécurité opérationnelle

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

Statut : ✅ Conforme

Réponse : Oui

Recommandation : Continuer à assurer la collecte et l'analyse régulières des 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 le chiffrement des 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 : Établir 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 : Intégrer les exigences de sécurité 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 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.

## 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.

## 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 plan de continuité d'activité (PCA).

## A.17 Continuité d'activité

Question : Le PCA est-il testé régulièrement ?

Statut : ❌ Non conforme

Réponse : Non trouvé

Recommandation : Mettre en place des tests réguliers du 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 programme d'audits internes périodiques.