**Rapport de Pré-Audit ISO 27001  
Nom de l'organisation**

Date du rapport : à compléter

Consultant : à compléter

# 1. Contexte et objectifs

Ce rapport présente les résultats du pré-audit ISO 27001 réalisé sur le système de management de la sécurité de l'information (SMSI) de l'organisation. L'objectif est d'identifier les écarts par rapport aux exigences de la norme et de proposer des recommandations d'amélioration.

# 2. Méthodologie

L'évaluation a été réalisée à partir d'un questionnaire basé sur les exigences de la norme ISO 27001:2022 et l'Annexe A. Les réponses ont été analysées afin de déterminer le niveau de conformité et de proposer des recommandations adaptées.

# 3. Résultats de la Gap Analysis

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Domaine ISO 27001 | Question | Réponse | Statut | Recommandation | Priorité | Échéance |
| 4. Contexte de l'organisation | Le contexte interne et externe de l'organisation est-il documenté ? | Non trouvé | ❌ Non conforme | Documenter le contexte interne et externe de l'organisation. | Haute | 31/12/2023 |
| 4. Contexte de l'organisation | Les besoins et attentes des parties prenantes sont-ils identifiés ? | Non trouvé | ❌ Non conforme | Identifier et documenter les besoins et attentes des parties prenantes. | Haute | 31/12/2023 |
| 4. Contexte de l'organisation | Le périmètre du SMSI est-il défini et documenté ? | Oui | ✅ Conforme | Maintenir la documentation à jour et accessible. | Basse | 31/12/2023 |
| 5. Leadership | La direction démontre-t-elle son engagement envers le SMSI ? | Oui | ✅ Conforme | Continuer à promouvoir l'engagement de la direction. | Basse | 31/12/2023 |
| 5. Leadership | Une politique de sécurité est-elle définie et approuvée par la direction ? | Oui | ✅ Conforme | Assurer la diffusion de la politique à tous les niveaux. | Basse | 31/12/2023 |
| 6. Planification | Les risques liés à la sécurité de l'information sont-ils identifiés et évalués ? | Non trouvé | ❌ Non conforme | Mettre en place un processus d'identification et d'évaluation des risques. | Haute | 31/12/2023 |
| 6. Planification | Des objectifs mesurables de sécurité sont-ils définis et suivis ? | Non trouvé | ❌ Non conforme | Définir des objectifs mesurables et établir un suivi. | Moyenne | 31/12/2023 |
| 7. Support | Les ressources nécessaires au SMSI sont-elles allouées ? | Non trouvé | ❌ Non conforme | Évaluer et allouer les ressources nécessaires au SMSI. | Haute | 31/12/2023 |
| 7. Support | Le personnel est-il compétent et formé à la sécurité de l'information ? | Non trouvé | ❌ Non conforme | Mettre en place un programme de formation à la sécurité de l'information. | Haute | 31/12/2023 |
| 8. Fonctionnement | Les opérations sont-elles planifiées et maîtrisées ? | Non trouvé | ❌ Non conforme | Établir des procédures pour la planification et le contrôle des opérations. | Moyenne | 31/12/2023 |
| 8. Fonctionnement | Les résultats des évaluations des risques sont-ils intégrés aux activités ? | Non trouvé | ❌ Non conforme | Intégrer les résultats des évaluations des risques dans les processus opérationnels. | Moyenne | 31/12/2023 |
| 9. Évaluation des performances | La performance du SMSI est-elle mesurée et évaluée ? | Non trouvé | ❌ Non conforme | Mettre en place des indicateurs de performance pour le SMSI. | Moyenne | 31/12/2023 |
| 9. Évaluation des performances | Des audits internes sont-ils réalisés conformément au programme d'audit ? | Non trouvé | ❌ Non conforme | Établir un programme d'audit interne pour le SMSI. | Moyenne | 31/12/2023 |
| 10. Amélioration | Les non-conformités sont-elles traitées par des actions correctives ? | Non trouvé | ❌ Non conforme | Mettre en place un processus pour traiter les non-conformités. | Moyenne | 31/12/2023 |
| 10. Amélioration | L'amélioration continue du SMSI est-elle démontrée ? | Non trouvé | ❌ Non conforme | Établir un processus pour démontrer l'amélioration continue du SMSI. | Moyenne | 31/12/2023 |
| A.5 Politiques de sécurité de l'information | Existe-t-il une politique de sécurité formellement approuvée par la direction ? | Oui | ✅ Conforme | Assurer la mise à jour régulière de la politique. | Basse | 31/12/2023 |
| A.5 Politiques de sécurité de l'information | La politique est-elle communiquée à tous les employés et parties prenantes pertinentes ? | Non trouvé | ❌ Non conforme | Mettre en place un plan de communication pour diffuser la politique. | Moyenne | 31/12/2023 |
| A.5 Politiques de sécurité de l'information | Un processus de révision régulière de la politique est-il en place et documenté ? | Non trouvé | ❌ Non conforme | Établir un processus documenté de révision régulière de la politique. | Moyenne | 31/12/2023 |
| A.6 Organisation de la sécurité de l'information | Les rôles et responsabilités en matière de sécurité de l'information sont-ils clairement définis et communiqués ? | Oui | ✅ Conforme | Assurer la communication continue des rôles et responsabilités. | Basse | 31/12/2023 |
| A.6 Organisation de la sécurité de l'information | Existe-t-il un responsable de la sécurité de l'information désigné (RSSI) ? | Oui | ✅ Conforme | Assurer le soutien et les ressources pour le RSSI. | Basse | 31/12/2023 |
| A.6 Organisation de la sécurité de l'information | La sécurité est-elle coordonnée entre les différents départements ? | Non trouvé | ❌ Non conforme | Établir des mécanismes de coordination de la sécurité entre les départements. | Moyenne | 31/12/2023 |
| A.7 Sécurité des ressources humaines | Les candidats font-ils l’objet d’une vérification d’antécédents avant embauche ? | Non trouvé | ❌ Non conforme | Mettre en place un processus de vérification d'antécédents pour les candidats. | Moyenne | 31/12/2023 |
| A.7 Sécurité des ressources humaines | Une formation à la sécurité est-elle dispensée à l’intégration ? | Non trouvé | ❌ Non conforme | Établir un programme de formation à la sécurité pour les nouveaux employés. | Haute | 31/12/2023 |
| A.7 Sécurité des ressources humaines | Les obligations contractuelles incluent-elles des exigences de sécurité ? | Non trouvé | ❌ Non conforme | Inclure des exigences de sécurité dans les contrats avec les employés. | Moyenne | 31/12/2023 |
| A.8 Gestion des actifs | Un inventaire des actifs est-il tenu à jour et approuvé ? | Non trouvé | ❌ Non conforme | Établir et maintenir un inventaire des actifs. | Moyenne | 31/12/2023 |
| A.8 Gestion des actifs | Les actifs sont-ils classifiés selon leur sensibilité ? | Non trouvé | ❌ Non conforme | Mettre en place un processus de classification des actifs. | Moyenne | 31/12/2023 |
| A.8 Gestion des actifs | Des règles d'utilisation acceptable des actifs sont-elles définies ? | Non trouvé | ❌ Non conforme | Établir des règles d'utilisation acceptable des actifs. | Moyenne | 31/12/2023 |
| A.9 Contrôle d'accès | Existe-t-il une politique de contrôle d’accès ? | Non trouvé | ❌ Non conforme | Établir une politique de contrôle d'accès. | Haute | 31/12/2023 |
| A.9 Contrôle d'accès | Les droits sont-ils accordés selon le principe du moindre privilège ? | Non trouvé | ❌ Non conforme | Mettre en œuvre le principe du moindre privilège pour l'attribution des droits. | Haute | 31/12/2023 |
| A.9 Contrôle d'accès | Les droits sont-ils révoqués immédiatement en cas de départ ou changement de poste ? | Non trouvé | ❌ Non conforme | Établir un processus pour révoquer les droits immédiatement. | Haute | 31/12/2023 |
| A.10 Cryptographie | Une politique d’utilisation de la cryptographie est-elle définie ? | Non trouvé | ❌ Non conforme | Établir une politique d'utilisation de la cryptographie. | Moyenne | 31/12/2023 |
| A.10 Cryptographie | Les clés cryptographiques sont-elles gérées de manière sécurisée ? | Non trouvé | ❌ Non conforme | Mettre en place des procédures pour la gestion sécurisée des clés cryptographiques. | Moyenne | 31/12/2023 |
| A.11 Sécurité physique et environnementale | Les accès physiques aux zones sensibles sont-ils contrôlés ? | Non trouvé | ❌ Non conforme | Établir des contrôles d'accès physiques pour les zones sensibles. | Haute | 31/12/2023 |
| A.11 Sécurité physique et environnementale | Les équipements sont-ils protégés contre les menaces environnementales ? | Non trouvé | ❌ Non conforme | Mettre en place des mesures de protection contre les menaces environnementales. | Moyenne | 31/12/2023 |
| A.11 Sécurité physique et environnementale | Une procédure de gestion des visiteurs est-elle appliquée ? | Non trouvé | ❌ Non conforme | Établir une procédure de gestion des visiteurs. | Moyenne | 31/12/2023 |
| A.12 Sécurité opérationnelle | Les procédures opérationnelles sont-elles documentées et accessibles ? | Non trouvé | ❌ Non conforme | Documenter et rendre accessibles les procédures opérationnelles. | Moyenne | 31/12/2023 |
| A.12 Sécurité opérationnelle | Les changements sont-ils contrôlés par un processus de gestion des changements ? | Non trouvé | ❌ Non conforme | Établir un processus de gestion des changements. | Moyenne | 31/12/2023 |
| A.12 Sécurité opérationnelle | Les journaux d'activité sont-ils collectés et analysés régulièrement ? | Non trouvé | ❌ Non conforme | Mettre en place un processus de collecte et d'analyse des journaux d'activité. | Moyenne | 31/12/2023 |
| A.13 Sécurité des communications | Les réseaux sont-ils segmentés et protégés ? | Non trouvé | ❌ Non conforme | Établir des mesures de segmentation et de protection des réseaux. | Moyenne | 31/12/2023 |
| A.13 Sécurité des communications | Les communications sensibles sont-elles chiffrées ? | Non trouvé | ❌ Non conforme | Mettre en place des mesures de chiffrement pour les communications sensibles. | Moyenne | 31/12/2023 |
| A.13 Sécurité des communications | Une politique d'utilisation des services de messagerie est-elle définie ? | Non trouvé | ❌ Non conforme | Établir une politique d'utilisation des services de messagerie. | Moyenne | 31/12/2023 |
| A.14 Acquisition, développement et maintenance des systèmes | Les exigences de sécurité sont-elles intégrées dans les projets ? | Non trouvé | ❌ Non conforme | Intégrer les exigences de sécurité dans tous les projets. | Moyenne | 31/12/2023 |
| A.14 Acquisition, développement et maintenance des systèmes | Des tests de sécurité sont-ils effectués avant mise en production ? | Non trouvé | ❌ Non conforme | Mettre en place des tests de sécurité avant la mise en production. | Moyenne | 31/12/2023 |
| A.14 Acquisition, développement et maintenance des systèmes | Les vulnérabilités applicatives sont-elles corrigées rapidement ? | Non trouvé | ❌ Non conforme | Établir un processus pour corriger rapidement les vulnérabilités applicatives. | Moyenne | 31/12/2023 |
| A.15 Relations avec les fournisseurs | Les contrats fournisseurs incluent-ils des clauses de sécurité ? | Non trouvé | ❌ Non conforme | Inclure des clauses de sécurité dans tous les contrats fournisseurs. | Moyenne | 31/12/2023 |
| A.15 Relations avec les fournisseurs | Les performances sécurité des fournisseurs sont-elles évaluées ? | Non trouvé | ❌ Non conforme | Mettre en place un processus d'évaluation des performances sécurité des fournisseurs. | Moyenne | 31/12/2023 |
| A.16 Gestion des incidents de sécurité | Un processus de gestion des incidents est-il défini ? | Non trouvé | ❌ Non conforme | Établir un processus de gestion des incidents. | Haute | 31/12/2023 |
| A.16 Gestion des incidents de sécurité | Les incidents sont-ils documentés et analysés ? | Non trouvé | ❌ Non conforme | Mettre en place un processus pour documenter et analyser les incidents. | Haute | 31/12/2023 |
| A.16 Gestion des incidents de sécurité | Les leçons apprises sont-elles intégrées aux procédures ? | Non trouvé | ❌ Non conforme | Établir un processus pour intégrer les leçons apprises aux procédures. | Moyenne | 31/12/2023 |
| A.17 Continuité d'activité | La sécurité de l'information est-elle intégrée au PCA ? | Non trouvé | ❌ Non conforme | Intégrer la sécurité de l'information dans le Plan de Continuité d'Activité (PCA). | Moyenne | 31/12/2023 |
| A.17 Continuité d'activité | Le PCA est-il testé régulièrement ? | Non trouvé | ❌ Non conforme | Mettre en place des tests réguliers du PCA. | Moyenne | 31/12/2023 |
| A.18 Conformité | Les exigences légales et réglementaires sont-elles respectées ? | Non trouvé | ❌ Non conforme | Établir un processus pour garantir le respect des exigences légales et réglementaires. | Haute | 31/12/2023 |
| A.18 Conformité | Des audits internes sont-ils réalisés périodiquement ? | Non trouvé | ❌ Non conforme | Mettre en place un programme d'audits internes périodiques. | Moyenne | 31/12/2023 |

# 4. Plan d'actions recommandé

- Documenter le contexte interne et externe de l'organisation. (4. Contexte de l'organisation)

- Identifier et documenter les besoins et attentes des parties prenantes. (4. Contexte de l'organisation)

- Mettre en place un processus d'identification et d'évaluation des risques. (6. Planification)

- Définir des objectifs mesurables et établir un suivi. (6. Planification)

- Évaluer et allouer les ressources nécessaires au SMSI. (7. Support)

- Mettre en place un programme de formation à la sécurité de l'information. (7. Support)

- Établir des procédures pour la planification et le contrôle des opérations. (8. Fonctionnement)

- Intégrer les résultats des évaluations des risques dans les processus opérationnels. (8. Fonctionnement)

- Mettre en place des indicateurs de performance pour le SMSI. (9. Évaluation des performances)

- Établir un programme d'audit interne pour le SMSI. (9. Évaluation des performances)

- Mettre en place un processus pour traiter les non-conformités. (10. Amélioration)

- Établir un processus pour démontrer l'amélioration continue du SMSI. (10. Amélioration)

- Mettre en place un plan de communication pour diffuser la politique. (A.5 Politiques de sécurité de l'information)

- Établir un processus documenté de révision régulière de la politique. (A.5 Politiques de sécurité de l'information)

- Établir des mécanismes de coordination de la sécurité entre les départements. (A.6 Organisation de la sécurité de l'information)

- Mettre en place un processus de vérification d'antécédents pour les candidats. (A.7 Sécurité des ressources humaines)

- Établir un programme de formation à la sécurité pour les nouveaux employés. (A.7 Sécurité des ressources humaines)

- Inclure des exigences de sécurité dans les contrats avec les employés. (A.7 Sécurité des ressources humaines)

- Établir et maintenir un inventaire des actifs. (A.8 Gestion des actifs)

- Mettre en place un processus de classification des actifs. (A.8 Gestion des actifs)

- Établir des règles d'utilisation acceptable des actifs. (A.8 Gestion des actifs)

- Établir une politique de contrôle d'accès. (A.9 Contrôle d'accès)

- Mettre en œuvre le principe du moindre privilège pour l'attribution des droits. (A.9 Contrôle d'accès)

- Établir un processus pour révoquer les droits immédiatement. (A.9 Contrôle d'accès)

- Établir une politique d'utilisation de la cryptographie. (A.10 Cryptographie)

- Mettre en place des procédures pour la gestion sécurisée des clés cryptographiques. (A.10 Cryptographie)

- Établir des contrôles d'accès physiques pour les zones sensibles. (A.11 Sécurité physique et environnementale)

- Mettre en place des mesures de protection contre les menaces environnementales. (A.11 Sécurité physique et environnementale)

- Établir une procédure de gestion des visiteurs. (A.11 Sécurité physique et environnementale)

- Documenter et rendre accessibles les procédures opérationnelles. (A.12 Sécurité opérationnelle)

- Établir un processus de gestion des changements. (A.12 Sécurité opérationnelle)

- Mettre en place un processus de collecte et d'analyse des journaux d'activité. (A.12 Sécurité opérationnelle)

- Établir des mesures de segmentation et de protection des réseaux. (A.13 Sécurité des communications)

- Mettre en place des mesures de chiffrement pour les communications sensibles. (A.13 Sécurité des communications)

- Établir une politique d'utilisation des services de messagerie. (A.13 Sécurité des communications)

- Intégrer les exigences de sécurité dans tous les projets. (A.14 Acquisition, développement et maintenance des systèmes)

- Mettre en place des tests de sécurité avant la mise en production. (A.14 Acquisition, développement et maintenance des systèmes)

- Établir un processus pour corriger rapidement les vulnérabilités applicatives. (A.14 Acquisition, développement et maintenance des systèmes)

- Inclure des clauses de sécurité dans tous les contrats fournisseurs. (A.15 Relations avec les fournisseurs)

- Mettre en place un processus d'évaluation des performances sécurité des fournisseurs. (A.15 Relations avec les fournisseurs)

- Établir un processus de gestion des incidents. (A.16 Gestion des incidents de sécurité)

- Mettre en place un processus pour documenter et analyser les incidents. (A.16 Gestion des incidents de sécurité)

- Établir un processus pour intégrer les leçons apprises aux procédures. (A.16 Gestion des incidents de sécurité)

- Intégrer la sécurité de l'information dans le Plan de Continuité d'Activité (PCA). (A.17 Continuité d'activité)

- Mettre en place des tests réguliers du PCA. (A.17 Continuité d'activité)

- Établir un processus pour garantir le respect des exigences légales et réglementaires. (A.18 Conformité)

- Mettre en place un programme d'audits internes périodiques. (A.18 Conformité)

# 5. Conclusion

Le présent rapport constitue une première étape dans la préparation à la certification ISO 27001. Il est recommandé de mettre en œuvre les actions proposées et de réaliser un audit interne complet avant l'audit de certification.