ANSSI Hygiene – Assessment Report

Date: 2025-08-28

Secteur: Banque | Employés: 93 | Pays: Maroc

# Executive Summary

**Maturité globale:** 38.1%

Répartition statuts: ✅ 2 | 🟡 28 | ❌ 12 | ⚪ 0 | 🚫 0

# Synthèse par thème

|  |  |
| --- | --- |
| Thème | Maturité moyenne (%) |
| IX – Superviser, auditer, réagir | 66.7 |
| I – Sensibiliser et former | 50.0 |
| VIII – Maintenir le SI à jour | 50.0 |
| IV – Sécuriser les postes | 50.0 |
| V – Sécuriser le réseau | 43.8 |
| II – Connaître le SI | 37.5 |
| X – Pour aller plus loin | 37.5 |
| VII – Gérer le nomadisme | 25.0 |
| III – Authentifier & contrôler les accès | 16.7 |
| VI – Sécuriser l’administration | 16.7 |

# Résultats détaillés

## I – Sensibiliser et former

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| I-1 | Former les équipes opérationnelles | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des sessions de sensibilisation annuelles et un programme de formation continue pour les utilisateurs, ce qui montre un effort pour former les équipes opérationnelles. Cependant, il manque des détails sur les processus formels de validation et de suivi des formations, ainsi que sur les indicateurs de performance spécifiques pour évaluer l'efficacité de ces formations. |
| I-2 | Sensibiliser les utilisateurs | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Conforme  \*\*Justification\*\* : L'organisation a mis en place un programme de sensibilisation continue, incluant des sessions annuelles et des modules de formation actualisés pour informer les utilisateurs sur les menaces et les bonnes pratiques. De plus, les utilisateurs sont tenus informés des incidents et des mesures préventives, ce qui démontre une approche proactive en matière de sensibilisation. |
| I-3 | Maîtriser les risques de l’infogérance | 🟡 Partiellement conforme | 50 | {  "status": "Partiellement conforme",  "justification": "L'organisation a mis en place des processus de gouvernance et de gestion des logs, ainsi que des mesures de réponse aux incidents. Cependant, il manque des détails sur les contrôles techniques spécifiques liés à l'infogérance et sur la supervision des indicateurs de performance pour évaluer l'efficacité de ces mesures. Par exemple, bien que le comité de gouvernance supervise les KPI, il n'est pas précisé comment ces indicateurs sont appliqués spécifiquement à l'infogérance.",  "citations": [  {"doc": "CFG - Procédure de gestion et revue des logs V0.1.docx", "page": 4},  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 12},  {"doc": "CFG Politique de lutte contre les fuites de données.do |

## II – Connaître le SI

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| II-4 | Identifier données/serveurs sensibles & schéma réseau | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus pour identifier les données et serveurs sensibles, ainsi qu'un schéma réseau, mais il manque des éléments de gouvernance et de supervision clairs. Bien que des audits réguliers et une équipe dédiée à la gestion des incidents soient mentionnés, l'absence d'indicateurs spécifiques et de documentation exhaustive sur les contrôles techniques limite la conformité totale. |
| II-5 | Inventaire des comptes privilégiés | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas d'inventaire spécifique des comptes privilégiés, ni de processus formalisé pour leur gestion. Bien que des procédures de gestion des logs et des audits soient mentionnées, elles ne couvrent pas explicitement les comptes privilégiés, ce qui est essentiel pour répondre à cette exigence. |
| II-6 | Procédures arrivée/départ/changement | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des procédures pour la gestion des logs et des changements, mais il manque des détails explicites sur les procédures d'arrivée et de départ des employés. Les processus de gestion des demandes d'ajout de sources de logs sont bien définis, mais les procédures spécifiques pour les changements de personnel ne sont pas clairement documentées. |
| II-7 | Autoriser la connexion aux seuls équipements maîtrisés | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des procédures de gestion des logs et des contrôles techniques via des équipements comme des firewalls et des systèmes de détection d'intrusion. Cependant, il n'est pas clairement établi comment les connexions aux équipements non maîtrisés sont explicitement interdites ou contrôlées, ce qui laisse une part d'incertitude sur la conformité totale à l'exigence. |

## III – Authentifier & contrôler les accès

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| III-10 | Règles de mots de passe | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas de règles spécifiques concernant la gestion des mots de passe dans les documents fournis. Bien que des processus de gouvernance et de gestion des logs soient décrits, il n'y a aucune mention des exigences relatives aux mots de passe, telles que la complexité, la durée de vie ou la gestion des exceptions. Cela indique un manque de conformité à l'exigence sur les règles de mots de passe. |
| III-11 | Protéger les mots de passe stockés | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas de mesures spécifiques pour protéger les mots de passe stockés. Bien que des procédures de gestion des logs et des fuites de données soient en place, il n'y a aucune mention de contrôles techniques ou de processus dédiés à la protection des mots de passe, ce qui est essentiel pour répondre à cette exigence. |
| III-12 | Changer les identifiants par défaut | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne mentionne pas explicitement de processus ou de contrôles techniques pour changer les identifiants par défaut. Bien que des procédures de gestion des logs et des audits soient en place, il n'y a pas d'indication sur la gestion des identifiants par défaut, ce qui est essentiel pour la sécurité des systèmes. |
| III-13 | Authentification forte | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne semble pas avoir mis en place des mesures spécifiques pour garantir l'authentification forte, comme l'exige la réglementation. Bien que des processus de gestion des logs et des mesures de sécurité soient mentionnés, il n'y a pas d'indication claire sur l'implémentation d'une authentification forte, qui est essentielle pour protéger les accès aux systèmes critiques. |
| III-8 | Comptes nominatifs & séparation des rôles | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de sensibilisation pour gérer les comptes nominatifs et la séparation des rôles, mais il manque des détails sur les contrôles techniques spécifiques et les indicateurs de supervision. Par exemple, la politique de lutte contre les fuites de données mentionne la nécessité d'audits réguliers et de sensibilisation des employés, mais ne précise pas comment la séparation des rôles est techniquement mise en œuvre (doc, p.3). |
| III-9 | Droits sur les ressources sensibles | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de sensibilisation concernant les ressources sensibles, mais il manque des détails sur les contrôles techniques spécifiques et les preuves de suivi des droits d'accès. Par exemple, le comité de gouvernance supervise la gestion des logs et valide les évolutions (doc, p.4), mais il n'est pas précisé comment les droits d'accès sont attribués et contrôlés techniquement. |

## IV – Sécuriser les postes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| IV-14 | Niveau de sécurité minimal du parc | 🟡 Partiellement conforme | 50 | {  "status": "Partiellement conforme",  "justification": "L'organisation a mis en place des processus de gouvernance et de supervision, ainsi que des contrôles techniques pour la gestion des logs et la sécurité des actifs. Cependant, il manque des détails sur les indicateurs spécifiques de performance et de sécurité du parc, ainsi que sur les preuves tangibles de conformité, comme des logs ou des tickets de suivi. Cela limite l'évaluation complète de la conformité à l'exigence de niveau de sécurité minimal du parc.",  "citations": [  {"doc": "CFG - Procédure de gestion et revue des logs V0.1.docx", "page": 4},  {"doc": "CFG - Procédure de gestion et revue des logs V0.1.docx", "page": 5},  {"doc": "CFG - Politique de lutte contre les fuites de données.docx", "page": 12} |
| IV-15 | Se protéger des supports amovibles | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des politiques de lutte contre les fuites de données et des processus de gestion des alertes, mais il n'est pas clairement indiqué comment les supports amovibles sont spécifiquement protégés. Bien que des mesures de sensibilisation et de formation soient prévues, l'absence de détails sur les contrôles techniques spécifiques pour les supports amovibles limite la conformité. |
| IV-16 | Gestion centralisée des politiques de sécurité | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place un comité de gouvernance qui supervise la gestion des logs et valide les évolutions des politiques de sécurité. Cependant, il manque des détails sur la centralisation des processus et des contrôles techniques spécifiques pour assurer une gestion uniforme des politiques de sécurité à travers l'ensemble de l'organisation. |
| IV-17 | Activer/configurer le pare-feu local | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation utilise des firewalls tels que Fortigate et Palo Alto pour la protection périmétrique, mais il n'est pas précisé si le pare-feu local est activé ou configuré spécifiquement pour chaque système. Les procédures de gestion des logs et de gouvernance sont en place, mais des détails sur la configuration spécifique des pare-feu locaux manquent. |
| IV-18 | Chiffrer les données sensibles transmises | 🟡 Partiellement conforme | 50 | {  "status": "Partiellement conforme",  "justification": "L'organisation a mis en place des processus de classification des données et des outils de prévention des pertes de données (DLP), mais il n'est pas clairement indiqué que toutes les données sensibles transmises sont systématiquement chiffrées. Les mesures de réponse aux incidents et la gestion des exceptions sont documentées, mais le chiffrement des données sensibles lors de leur transmission n'est pas explicitement mentionné comme une exigence systématique.",  "citations": [  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 4},  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 9},  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 1 |

## IX – Superviser, auditer, réagir

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| IX-36 | Activer/configurer les journaux | ✅ Conforme | 100 | \*\*Statut\*\* : Conforme  \*\*Justification\*\* : L'organisation a mis en place une procédure de gestion des logs qui définit clairement les responsabilités, les processus d'intégration et de supervision des journaux. Le comité de gouvernance supervise la conformité et l'évolution des dispositifs de journalisation, garantissant ainsi une gestion conforme aux exigences réglementaires et aux bonnes pratiques. |
| IX-37 | Politique de sauvegarde | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne fournit pas d'informations claires sur la politique de sauvegarde, notamment sur le périmètre, la fréquence, le chiffrement, les tests de restauration et la supervision. Les documents mentionnent des aspects de sécurité et de gestion des logs, mais aucun détail sur les sauvegardes et la restauration n'est présent. |
| IX-38 | Audits réguliers & actions correctives | ✅ Conforme | 100 | \*\*Statut\*\* : Conforme  \*\*Justification\*\* : L'organisation a mis en place un comité de gouvernance qui supervise les audits réguliers et les actions correctives, en examinant les KPI et en validant les évolutions nécessaires. De plus, des mesures de réponse et de remédiation sont clairement définies, avec un contrôle rigoureux par le RSSI et une fréquence d'audit trimestrielle pour assurer la conformité et l'efficacité des processus. |

## V – Sécuriser le réseau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| V-19 | Segmenter & cloisonner le réseau | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des dispositifs de sécurité tels que des firewalls et un WAF pour segmenter et cloisonner le réseau, mais il manque des détails sur les processus de gouvernance et les indicateurs de supervision spécifiques à cette exigence. Les logs sont collectés et analysés, mais la documentation sur la gestion des exceptions et les audits de sécurité pourrait être renforcée. |
| V-20 | Sécurité du Wi-Fi & séparation des usages | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas de mesures spécifiques concernant la sécurité du Wi-Fi et la séparation des usages. Bien que des processus de gestion des logs et des mesures de sécurité soient mentionnés, il n'y a pas d'indications sur la gouvernance ou les contrôles techniques relatifs à la sécurité des réseaux sans fil. Les documents fournis se concentrent principalement sur la gestion des logs et la lutte contre les fuites de données, sans aborder directement la sécurité Wi-Fi. |
| V-21 | Protocoles réseau sécurisés | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des dispositifs de sécurité tels que des firewalls et un WAF pour protéger le réseau, et un comité de gouvernance supervise la gestion des logs. Cependant, il manque des détails sur les processus spécifiques relatifs aux protocoles réseau sécurisés et sur la supervision des indicateurs liés à ces protocoles. |
| V-22 | Passerelle d’accès sécurisé à Internet | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des dispositifs de sécurité tels que des firewalls et un WAF pour protéger l'accès à Internet, mais il manque des détails sur les processus formels de gouvernance et de supervision des incidents. Bien que des indicateurs clés soient suivis, la documentation ne précise pas suffisamment les processus d'approbation et de remédiation associés à la passerelle d'accès sécurisé. |
| V-23 | Cloisonner les services exposés Internet | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des dispositifs de sécurité tels que des firewalls et un WAF pour protéger les services exposés à Internet, ce qui indique une volonté de cloisonner ces services. Cependant, il manque des détails sur les processus de gouvernance et de supervision spécifiques à cette cloisonnement, ainsi que sur les indicateurs de performance associés. |
| V-24 | Protéger la messagerie professionnelle | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des outils de détection des fuites de données (DLP) et des processus de traitement des alertes, mais il manque des détails sur la gouvernance spécifique à la messagerie professionnelle et sur les indicateurs de performance associés. Les mesures de réponse et remédiation sont définies, mais une documentation plus précise sur la supervision des systèmes de messagerie serait nécessaire. |
| V-25 | Sécuriser les interconnexions partenaires | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et des contrôles techniques pour sécuriser les interconnexions partenaires, notamment à travers la gestion des logs et la surveillance des équipements critiques. Cependant, il manque des détails sur les processus d'approbation spécifiques aux interconnexions partenaires et sur les indicateurs de performance dédiés à cette exigence. |
| V-26 | Contrôler l’accès aux salles serveurs/locaux techniques | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de gestion des logs, mais il n'est pas clairement indiqué comment l'accès aux salles serveurs est spécifiquement contrôlé. Bien que des mesures de sécurité soient mentionnées, comme la surveillance des équipements critiques, il manque des détails sur les contrôles d'accès physiques et les procédures d'approbation spécifiques pour ces locaux. |

## VI – Sécuriser l’administration

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| VI-27 | Interdire Internet sur postes/serveurs d’admin | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne mentionne pas explicitement l'interdiction d'accès à Internet sur les postes ou serveurs d'administration. Bien que des mesures de sécurité soient en place, comme l'utilisation de firewalls et de systèmes de détection, il n'y a pas de processus documenté ou de contrôle technique spécifiant cette interdiction. Cela laisse place à des interprétations et à des risques potentiels. |
| VI-28 | Réseau d’administration dédié/cloisonné | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne semble pas avoir mis en place un réseau d'administration dédié ou cloisonné, ce qui est essentiel pour sécuriser les opérations critiques. Bien que des mesures de sécurité soient mentionnées, comme l'utilisation de firewalls et de systèmes de détection, il n'y a pas d'indication claire d'une séparation physique ou logique des réseaux d'administration des autres réseaux. Cela compromet la sécurité des opérations sensibles. |
| VI-29 | Limiter les droits d’admin sur postes | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de gestion des logs, mais il n'est pas clairement indiqué comment les droits d'administration sont spécifiquement limités sur les postes. Bien que des mesures de sécurité soient mentionnées, telles que la surveillance des alertes et la gestion des incidents, l'absence de détails sur la gestion des droits d'accès administratifs laisse des zones d'incertitude. |

## VII – Gérer le nomadisme

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| VII-30 | Sécurisation physique des terminaux nomades | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas de mesures spécifiques pour la sécurisation physique des terminaux nomades. Bien que des processus de gestion des logs et des incidents soient en place, il n'y a pas d'indications sur des contrôles techniques ou des processus dédiés à la protection physique des terminaux nomades, ce qui est essentiel pour répondre à cette exigence. |
| VII-31 | Chiffrer les données sensibles (matériel perdable) | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de détection et de traitement des fuites de données, ainsi qu'une politique de classification des données qui inclut des niveaux de sensibilité. Cependant, il n'est pas explicitement mentionné que toutes les données sensibles sur matériel perdable sont systématiquement chiffrées, ce qui laisse une incertitude sur l'application uniforme de cette exigence. |
| VII-32 | Sécuriser la connexion réseau en mobilité | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des mesures de sécurité pour protéger les connexions réseau, notamment à travers des dispositifs de protection périmétrique comme des firewalls et des systèmes de détection des fuites de données. Cependant, il manque des détails spécifiques sur les processus de sécurisation des connexions en mobilité, tels que des politiques explicites ou des contrôles techniques dédiés à cette exigence. |
| VII-33 | Politiques dédiées aux terminaux mobiles | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne semble pas avoir de politiques spécifiques dédiées aux terminaux mobiles, ce qui est essentiel pour répondre à l'exigence. Bien que des procédures de gestion des logs et des mesures de lutte contre les fuites de données soient en place, aucune mention explicite des processus, contrôles techniques ou gouvernance relatifs aux terminaux mobiles n'est fournie dans la documentation examinée. |

## VIII – Maintenir le SI à jour

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| VIII-34 | Politique de mise à jour | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place une gouvernance et des processus pour la gestion des logs, mais il manque des détails spécifiques sur la politique de mise à jour des systèmes et des contrôles techniques associés. Bien que le comité de gouvernance supervise les indicateurs clés et valide les évolutions, les processus de mise à jour ne sont pas explicitement décrits dans les documents fournis. |
| VIII-35 | Anticiper fin de support & limiter adhérences | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place une gouvernance solide avec un comité dédié à la gestion des logs, mais il manque des processus explicites pour anticiper la fin de support des systèmes et limiter les adhérences. Bien que des indicateurs soient suivis, il n'est pas mentionné comment les évolutions technologiques sont intégrées dans la gestion des actifs pour éviter des dépendances excessives. |

## X – Pour aller plus loin

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Mesure | Statut | Score (%) | Justification |
| X-39 | Gestion des vulnérabilités avancée (option) | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gestion des alertes et des incidents, ainsi qu'une gouvernance par un comité qui supervise les indicateurs clés. Cependant, il manque des éléments spécifiques sur la gestion des vulnérabilités avancées, notamment des contrôles techniques dédiés et des indicateurs de performance clairement définis pour cette exigence. |
| X-40 | Durcissement renforcé (option) | 🟡 Partiellement conforme | 50 | {  "status": "Partiellement conforme",  "justification": "L'organisation a mis en place des processus de gestion des alertes et des incidents, ainsi qu'une gouvernance pour superviser les logs et les mesures de sécurité. Cependant, il manque des détails sur les contrôles techniques spécifiques au durcissement renforcé et sur les indicateurs de performance associés à cette exigence. Les documents mentionnent des mesures de réponse et de remédiation, mais ne précisent pas les aspects techniques de durcissement renforcé.",  "citations": [  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 11},  {"doc": "CFG - Procédure de gestion et revue des logs V0.1.docx", "page": 4},  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": |
| X-41 | Tests d’intrusion réguliers (option) | ❌ Non conforme | 0 | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne mentionne pas de processus formel pour la réalisation de tests d'intrusion réguliers, ni de gouvernance ou d'indicateurs associés à cette exigence. Bien que des mesures de sécurité soient en place, telles que la gestion des logs et la réponse aux incidents, il n'y a pas de preuve de tests d'intrusion documentés ou planifiés, ce qui est essentiel pour évaluer la sécurité des systèmes. |
| X-42 | Plans d’amélioration continue (option) | 🟡 Partiellement conforme | 50 | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de suivi des indicateurs clés (KPI) pour l'amélioration continue, mais il manque des éléments sur la formalisation des plans d'amélioration et leur mise en œuvre systématique. Le comité de gouvernance supervise les KPI et valide les évolutions, mais il n'est pas précisé comment les résultats sont intégrés dans un plan d'amélioration structuré. |

# Plan d’actions recommandé

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID | Thème | Action | Priorité | Responsable | Justification | Échéance | Statut |
| I-1 | I – Sensibiliser et former | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des sessions de sensibilisation annuelles et un programme de formation continue pour les utilisateurs, ce qui montre un effort pour former les équipes opérationnelles. Cependant, il manque des détails sur les processus formels de validation et de suivi des formations, ainsi que sur les indicateurs de performance spécifiques pour évaluer l'efficacité de ces formations. |  | Ouvert |
| I-2 | I – Sensibiliser et former | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Conforme  \*\*Justification\*\* : L'organisation a mis en place un programme de sensibilisation continue, incluant des sessions annuelles et des modules de formation actualisés pour informer les utilisateurs sur les menaces et les bonnes pratiques. De plus, les utilisateurs sont tenus informés des incidents et des mesures préventives, ce qui démontre une approche proactive en matière de sensibilisation. |  | Ouvert |
| I-3 | I – Sensibiliser et former | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | {  "status": "Partiellement conforme",  "justification": "L'organisation a mis en place des processus de gouvernance et de gestion des logs, ainsi que des mesures de réponse aux incidents. Cependant, il manque des détails sur les contrôles techniques spécifiques liés à l'infogérance et sur la supervision des indicateurs de performance pour évaluer l'efficacité de ces mesures. Par exemple, bien que le comité de gouvernance supervise les KPI, il n'est pas précisé comment ces indicateurs sont appliqués spécifiquement à l'infogérance.",  "citations": [  {"doc": "CFG - Procédure de gestion et revue des logs V0.1.docx", "page": 4},  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 12},  {"doc": "CFG Politique de lutte contre les fuites de données.do |  | Ouvert |
| II-4 | II – Connaître le SI | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus pour identifier les données et serveurs sensibles, ainsi qu'un schéma réseau, mais il manque des éléments de gouvernance et de supervision clairs. Bien que des audits réguliers et une équipe dédiée à la gestion des incidents soient mentionnés, l'absence d'indicateurs spécifiques et de documentation exhaustive sur les contrôles techniques limite la conformité totale. |  | Ouvert |
| II-5 | II – Connaître le SI | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas d'inventaire spécifique des comptes privilégiés, ni de processus formalisé pour leur gestion. Bien que des procédures de gestion des logs et des audits soient mentionnées, elles ne couvrent pas explicitement les comptes privilégiés, ce qui est essentiel pour répondre à cette exigence. |  | Ouvert |
| II-6 | II – Connaître le SI | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des procédures pour la gestion des logs et des changements, mais il manque des détails explicites sur les procédures d'arrivée et de départ des employés. Les processus de gestion des demandes d'ajout de sources de logs sont bien définis, mais les procédures spécifiques pour les changements de personnel ne sont pas clairement documentées. |  | Ouvert |
| II-7 | II – Connaître le SI | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des procédures de gestion des logs et des contrôles techniques via des équipements comme des firewalls et des systèmes de détection d'intrusion. Cependant, il n'est pas clairement établi comment les connexions aux équipements non maîtrisés sont explicitement interdites ou contrôlées, ce qui laisse une part d'incertitude sur la conformité totale à l'exigence. |  | Ouvert |
| III-10 | III – Authentifier & contrôler les accès | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas de règles spécifiques concernant la gestion des mots de passe dans les documents fournis. Bien que des processus de gouvernance et de gestion des logs soient décrits, il n'y a aucune mention des exigences relatives aux mots de passe, telles que la complexité, la durée de vie ou la gestion des exceptions. Cela indique un manque de conformité à l'exigence sur les règles de mots de passe. |  | Ouvert |
| III-11 | III – Authentifier & contrôler les accès | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas de mesures spécifiques pour protéger les mots de passe stockés. Bien que des procédures de gestion des logs et des fuites de données soient en place, il n'y a aucune mention de contrôles techniques ou de processus dédiés à la protection des mots de passe, ce qui est essentiel pour répondre à cette exigence. |  | Ouvert |
| III-12 | III – Authentifier & contrôler les accès | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne mentionne pas explicitement de processus ou de contrôles techniques pour changer les identifiants par défaut. Bien que des procédures de gestion des logs et des audits soient en place, il n'y a pas d'indication sur la gestion des identifiants par défaut, ce qui est essentiel pour la sécurité des systèmes. |  | Ouvert |
| III-13 | III – Authentifier & contrôler les accès | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne semble pas avoir mis en place des mesures spécifiques pour garantir l'authentification forte, comme l'exige la réglementation. Bien que des processus de gestion des logs et des mesures de sécurité soient mentionnés, il n'y a pas d'indication claire sur l'implémentation d'une authentification forte, qui est essentielle pour protéger les accès aux systèmes critiques. |  | Ouvert |
| III-8 | III – Authentifier & contrôler les accès | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de sensibilisation pour gérer les comptes nominatifs et la séparation des rôles, mais il manque des détails sur les contrôles techniques spécifiques et les indicateurs de supervision. Par exemple, la politique de lutte contre les fuites de données mentionne la nécessité d'audits réguliers et de sensibilisation des employés, mais ne précise pas comment la séparation des rôles est techniquement mise en œuvre (doc, p.3). |  | Ouvert |
| III-9 | III – Authentifier & contrôler les accès | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de sensibilisation concernant les ressources sensibles, mais il manque des détails sur les contrôles techniques spécifiques et les preuves de suivi des droits d'accès. Par exemple, le comité de gouvernance supervise la gestion des logs et valide les évolutions (doc, p.4), mais il n'est pas précisé comment les droits d'accès sont attribués et contrôlés techniquement. |  | Ouvert |
| IV-14 | IV – Sécuriser les postes | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | {  "status": "Partiellement conforme",  "justification": "L'organisation a mis en place des processus de gouvernance et de supervision, ainsi que des contrôles techniques pour la gestion des logs et la sécurité des actifs. Cependant, il manque des détails sur les indicateurs spécifiques de performance et de sécurité du parc, ainsi que sur les preuves tangibles de conformité, comme des logs ou des tickets de suivi. Cela limite l'évaluation complète de la conformité à l'exigence de niveau de sécurité minimal du parc.",  "citations": [  {"doc": "CFG - Procédure de gestion et revue des logs V0.1.docx", "page": 4},  {"doc": "CFG - Procédure de gestion et revue des logs V0.1.docx", "page": 5},  {"doc": "CFG - Politique de lutte contre les fuites de données.docx", "page": 12} |  | Ouvert |
| IV-15 | IV – Sécuriser les postes | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des politiques de lutte contre les fuites de données et des processus de gestion des alertes, mais il n'est pas clairement indiqué comment les supports amovibles sont spécifiquement protégés. Bien que des mesures de sensibilisation et de formation soient prévues, l'absence de détails sur les contrôles techniques spécifiques pour les supports amovibles limite la conformité. |  | Ouvert |
| IV-16 | IV – Sécuriser les postes | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place un comité de gouvernance qui supervise la gestion des logs et valide les évolutions des politiques de sécurité. Cependant, il manque des détails sur la centralisation des processus et des contrôles techniques spécifiques pour assurer une gestion uniforme des politiques de sécurité à travers l'ensemble de l'organisation. |  | Ouvert |
| IV-17 | IV – Sécuriser les postes | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation utilise des firewalls tels que Fortigate et Palo Alto pour la protection périmétrique, mais il n'est pas précisé si le pare-feu local est activé ou configuré spécifiquement pour chaque système. Les procédures de gestion des logs et de gouvernance sont en place, mais des détails sur la configuration spécifique des pare-feu locaux manquent. |  | Ouvert |
| IV-18 | IV – Sécuriser les postes | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | {  "status": "Partiellement conforme",  "justification": "L'organisation a mis en place des processus de classification des données et des outils de prévention des pertes de données (DLP), mais il n'est pas clairement indiqué que toutes les données sensibles transmises sont systématiquement chiffrées. Les mesures de réponse aux incidents et la gestion des exceptions sont documentées, mais le chiffrement des données sensibles lors de leur transmission n'est pas explicitement mentionné comme une exigence systématique.",  "citations": [  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 4},  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 9},  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 1 |  | Ouvert |
| IX-37 | IX – Superviser, auditer, réagir | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne fournit pas d'informations claires sur la politique de sauvegarde, notamment sur le périmètre, la fréquence, le chiffrement, les tests de restauration et la supervision. Les documents mentionnent des aspects de sécurité et de gestion des logs, mais aucun détail sur les sauvegardes et la restauration n'est présent. |  | Ouvert |
| V-19 | V – Sécuriser le réseau | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des dispositifs de sécurité tels que des firewalls et un WAF pour segmenter et cloisonner le réseau, mais il manque des détails sur les processus de gouvernance et les indicateurs de supervision spécifiques à cette exigence. Les logs sont collectés et analysés, mais la documentation sur la gestion des exceptions et les audits de sécurité pourrait être renforcée. |  | Ouvert |
| V-20 | V – Sécuriser le réseau | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas de mesures spécifiques concernant la sécurité du Wi-Fi et la séparation des usages. Bien que des processus de gestion des logs et des mesures de sécurité soient mentionnés, il n'y a pas d'indications sur la gouvernance ou les contrôles techniques relatifs à la sécurité des réseaux sans fil. Les documents fournis se concentrent principalement sur la gestion des logs et la lutte contre les fuites de données, sans aborder directement la sécurité Wi-Fi. |  | Ouvert |
| V-21 | V – Sécuriser le réseau | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des dispositifs de sécurité tels que des firewalls et un WAF pour protéger le réseau, et un comité de gouvernance supervise la gestion des logs. Cependant, il manque des détails sur les processus spécifiques relatifs aux protocoles réseau sécurisés et sur la supervision des indicateurs liés à ces protocoles. |  | Ouvert |
| V-22 | V – Sécuriser le réseau | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des dispositifs de sécurité tels que des firewalls et un WAF pour protéger l'accès à Internet, mais il manque des détails sur les processus formels de gouvernance et de supervision des incidents. Bien que des indicateurs clés soient suivis, la documentation ne précise pas suffisamment les processus d'approbation et de remédiation associés à la passerelle d'accès sécurisé. |  | Ouvert |
| V-23 | V – Sécuriser le réseau | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des dispositifs de sécurité tels que des firewalls et un WAF pour protéger les services exposés à Internet, ce qui indique une volonté de cloisonner ces services. Cependant, il manque des détails sur les processus de gouvernance et de supervision spécifiques à cette cloisonnement, ainsi que sur les indicateurs de performance associés. |  | Ouvert |
| V-24 | V – Sécuriser le réseau | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des outils de détection des fuites de données (DLP) et des processus de traitement des alertes, mais il manque des détails sur la gouvernance spécifique à la messagerie professionnelle et sur les indicateurs de performance associés. Les mesures de réponse et remédiation sont définies, mais une documentation plus précise sur la supervision des systèmes de messagerie serait nécessaire. |  | Ouvert |
| V-25 | V – Sécuriser le réseau | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et des contrôles techniques pour sécuriser les interconnexions partenaires, notamment à travers la gestion des logs et la surveillance des équipements critiques. Cependant, il manque des détails sur les processus d'approbation spécifiques aux interconnexions partenaires et sur les indicateurs de performance dédiés à cette exigence. |  | Ouvert |
| V-26 | V – Sécuriser le réseau | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de gestion des logs, mais il n'est pas clairement indiqué comment l'accès aux salles serveurs est spécifiquement contrôlé. Bien que des mesures de sécurité soient mentionnées, comme la surveillance des équipements critiques, il manque des détails sur les contrôles d'accès physiques et les procédures d'approbation spécifiques pour ces locaux. |  | Ouvert |
| VI-27 | VI – Sécuriser l’administration | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne mentionne pas explicitement l'interdiction d'accès à Internet sur les postes ou serveurs d'administration. Bien que des mesures de sécurité soient en place, comme l'utilisation de firewalls et de systèmes de détection, il n'y a pas de processus documenté ou de contrôle technique spécifiant cette interdiction. Cela laisse place à des interprétations et à des risques potentiels. |  | Ouvert |
| VI-28 | VI – Sécuriser l’administration | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne semble pas avoir mis en place un réseau d'administration dédié ou cloisonné, ce qui est essentiel pour sécuriser les opérations critiques. Bien que des mesures de sécurité soient mentionnées, comme l'utilisation de firewalls et de systèmes de détection, il n'y a pas d'indication claire d'une séparation physique ou logique des réseaux d'administration des autres réseaux. Cela compromet la sécurité des opérations sensibles. |  | Ouvert |
| VI-29 | VI – Sécuriser l’administration | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de gestion des logs, mais il n'est pas clairement indiqué comment les droits d'administration sont spécifiquement limités sur les postes. Bien que des mesures de sécurité soient mentionnées, telles que la surveillance des alertes et la gestion des incidents, l'absence de détails sur la gestion des droits d'accès administratifs laisse des zones d'incertitude. |  | Ouvert |
| VII-30 | VII – Gérer le nomadisme | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne présente pas de mesures spécifiques pour la sécurisation physique des terminaux nomades. Bien que des processus de gestion des logs et des incidents soient en place, il n'y a pas d'indications sur des contrôles techniques ou des processus dédiés à la protection physique des terminaux nomades, ce qui est essentiel pour répondre à cette exigence. |  | Ouvert |
| VII-31 | VII – Gérer le nomadisme | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de détection et de traitement des fuites de données, ainsi qu'une politique de classification des données qui inclut des niveaux de sensibilité. Cependant, il n'est pas explicitement mentionné que toutes les données sensibles sur matériel perdable sont systématiquement chiffrées, ce qui laisse une incertitude sur l'application uniforme de cette exigence. |  | Ouvert |
| VII-32 | VII – Gérer le nomadisme | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des mesures de sécurité pour protéger les connexions réseau, notamment à travers des dispositifs de protection périmétrique comme des firewalls et des systèmes de détection des fuites de données. Cependant, il manque des détails spécifiques sur les processus de sécurisation des connexions en mobilité, tels que des politiques explicites ou des contrôles techniques dédiés à cette exigence. |  | Ouvert |
| VII-33 | VII – Gérer le nomadisme | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne semble pas avoir de politiques spécifiques dédiées aux terminaux mobiles, ce qui est essentiel pour répondre à l'exigence. Bien que des procédures de gestion des logs et des mesures de lutte contre les fuites de données soient en place, aucune mention explicite des processus, contrôles techniques ou gouvernance relatifs aux terminaux mobiles n'est fournie dans la documentation examinée. |  | Ouvert |
| VIII-34 | VIII – Maintenir le SI à jour | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place une gouvernance et des processus pour la gestion des logs, mais il manque des détails spécifiques sur la politique de mise à jour des systèmes et des contrôles techniques associés. Bien que le comité de gouvernance supervise les indicateurs clés et valide les évolutions, les processus de mise à jour ne sont pas explicitement décrits dans les documents fournis. |  | Ouvert |
| VIII-35 | VIII – Maintenir le SI à jour | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place une gouvernance solide avec un comité dédié à la gestion des logs, mais il manque des processus explicites pour anticiper la fin de support des systèmes et limiter les adhérences. Bien que des indicateurs soient suivis, il n'est pas mentionné comment les évolutions technologiques sont intégrées dans la gestion des actifs pour éviter des dépendances excessives. |  | Ouvert |
| X-39 | X – Pour aller plus loin | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gestion des alertes et des incidents, ainsi qu'une gouvernance par un comité qui supervise les indicateurs clés. Cependant, il manque des éléments spécifiques sur la gestion des vulnérabilités avancées, notamment des contrôles techniques dédiés et des indicateurs de performance clairement définis pour cette exigence. |  | Ouvert |
| X-40 | X – Pour aller plus loin | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | {  "status": "Partiellement conforme",  "justification": "L'organisation a mis en place des processus de gestion des alertes et des incidents, ainsi qu'une gouvernance pour superviser les logs et les mesures de sécurité. Cependant, il manque des détails sur les contrôles techniques spécifiques au durcissement renforcé et sur les indicateurs de performance associés à cette exigence. Les documents mentionnent des mesures de réponse et de remédiation, mais ne précisent pas les aspects techniques de durcissement renforcé.",  "citations": [  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": 11},  {"doc": "CFG - Procédure de gestion et revue des logs V0.1.docx", "page": 4},  {"doc": "CFG Politique de lutte contre les fuites de données.docx", "page": |  | Ouvert |
| X-41 | X – Pour aller plus loin | Établir un plan de remédiation documenté, définir un owner et une échéance; mettre en place le contrôle requis. | High |  | \*\*Statut\*\* : Non conforme  \*\*Justification\*\* : L'organisation ne mentionne pas de processus formel pour la réalisation de tests d'intrusion réguliers, ni de gouvernance ou d'indicateurs associés à cette exigence. Bien que des mesures de sécurité soient en place, telles que la gestion des logs et la réponse aux incidents, il n'y a pas de preuve de tests d'intrusion documentés ou planifiés, ce qui est essentiel pour évaluer la sécurité des systèmes. |  | Ouvert |
| X-42 | X – Pour aller plus loin | Compléter la documentation et étendre la couverture du contrôle; formaliser les preuves et indicateurs. | Medium |  | \*\*Statut\*\* : Partiellement conforme  \*\*Justification\*\* : L'organisation a mis en place des processus de gouvernance et de suivi des indicateurs clés (KPI) pour l'amélioration continue, mais il manque des éléments sur la formalisation des plans d'amélioration et leur mise en œuvre systématique. Le comité de gouvernance supervise les KPI et valide les évolutions, mais il n'est pas précisé comment les résultats sont intégrés dans un plan d'amélioration structuré. |  | Ouvert |