|  |  |
| --- | --- |
| **Rapport d'audit — ISACA** AUDIT-001 Client : Client X Date : 2025-09-24 Auditeur : |  |

# 1. Résumé exécutif

31 contrôles évalués. Répartition : N/A 0 • Conforme 31 • Partiel 0 • Non conforme 0.

Priorités : traiter d’abord les risques « Très élevé/Élevé » et les non-conformités associées ; planifier la mise en conformité des points partiels avec jalons réalistes ; sécuriser les tiers et les accès à privilèges.

# 2. Méthodologie

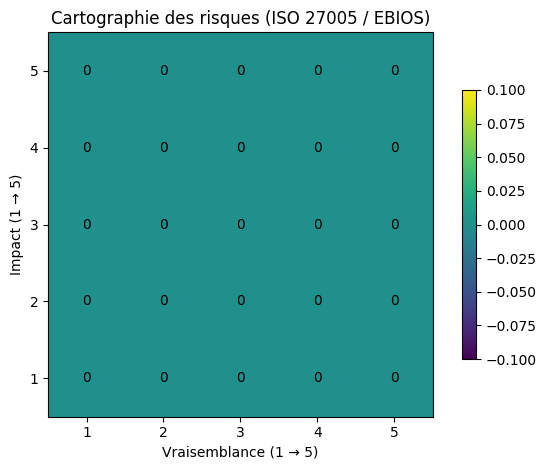
Référentiel : grille de contrôle basée sur la norme sélectionnée et adaptée au périmètre.

Échelle d’évaluation (contrôles) : Non applicable | Conforme | Partiellement conforme | Non conforme.

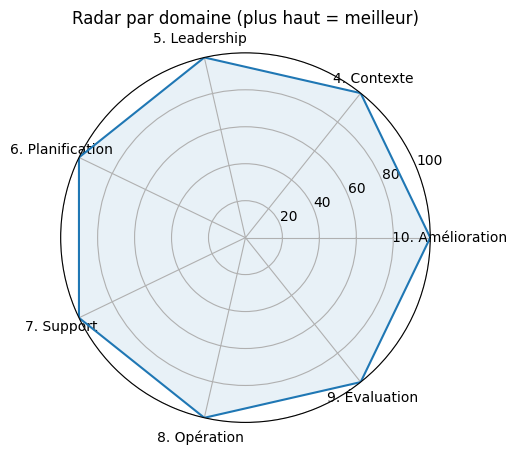
Gestion des risques (ISO 27005/EBIOS) : chaque risque est qualifié par Impact (1–5) et Vraisemblance (1–5). Le score I×V détermine la classe : Très faible (<4), Faible (4–7), Moyen (8–11), Élevé (12–19), Très élevé (≥20).

# 3. Cartographie des risques et vision par domaine

Cartographie 5×5 (ISO 27005/EBIOS) — uniquement basée sur le registre des risques.



Radar par domaine (maturité issue des contrôles).



# 4. Résultats détaillés des contrôles

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Domaine | ID | Intitulé | Contrôle/objectif | Niveau | Constats | Risques liés |
| 4. Contexte | 42001-4.1 | Contexte | Définir le contexte interne/externe pour l'AIMS (IA Management System). | Conforme | nan |  |
| 4. Contexte | 42001-4.2 | Parties intéressées | Identifier les besoins/attentes des parties intéressées liées à l’IA. | Conforme | nan |  |
| 4. Contexte | 42001-4.3 | Périmètre | Définir le périmètre de l’AIMS et ses interfaces. | Conforme | nan |  |
| 4. Contexte | 42001-4.4 | AIMS & Processus | Établir, mettre en œuvre et améliorer les processus de l’AIMS. | Conforme | nan |  |
| 5. Leadership | 42001-5.1 | Leadership & engagement | Démontrer l’engagement de la direction vis‑à‑vis de l’AIMS. | Conforme | nan |  |
| 5. Leadership | 42001-5.2 | Politique IA | Établir et communiquer la politique IA alignée aux objectifs et obligations. | Conforme | nan |  |
| 5. Leadership | 42001-5.3 | Rôles & responsabilités | Attribuer responsabilités et autorités pour l’AIMS (incl. gouvernance IA). | Conforme | nan |  |
| 6. Planification | 42001-6.1 | Risques & opportunités | Identifier et traiter risques/opportunités liés à l’IA et à l’AIMS. | Conforme | nan |  |
| 6. Planification | 42001-6.2 | Objectifs AIMS | Définir objectifs mesurables pour l’AIMS et plans pour les atteindre. | Conforme | nan |  |
| 6. Planification | 42001-6.3 | Changements | Planifier les changements de l’AIMS de manière contrôlée. | Conforme | nan |  |
| 7. Support | 42001-7.1 | Ressources | Fournir ressources suffisantes (humaines, techniques, financières). | Conforme | nan |  |
| 7. Support | 42001-7.2 | Compétences | Assurer compétences/formation pour les rôles IA et AIMS. | Conforme | nan |  |
| 7. Support | 42001-7.3 | Sensibilisation | Garantir la sensibilisation aux politiques, risques et obligations IA. | Conforme | nan |  |
| 7. Support | 42001-7.4 | Communication | Définir et appliquer la communication interne/externe relative à l’IA. | Conforme | nan |  |
| 7. Support | 42001-7.5 | Informations documentées | Créer, mettre à jour et maîtriser la documentation AIMS (procédures, enregistrements). | Conforme | nan |  |
| 8. Opération | 42001-8.1 | Planif. & contrôle opérationnels | Planifier, mettre en œuvre et maîtriser les processus opérationnels IA. | Conforme | nan |  |
| 8. Opération | 42001-8.2 | Gouvernance données | Gérer la qualité, l’origine, la sécurité et la conformité des données IA. | Conforme | nan |  |
| 8. Opération | 42001-8.3 | Conception & dév. modèles | Encadrer le design, l’entraînement et la validation des modèles IA. | Conforme | nan |  |
| 8. Opération | 42001-8.4 | Vérification & validation | Vérifier/valider les systèmes IA selon critères définis (performances, biais, sûreté). | Conforme | nan |  |
| 8. Opération | 42001-8.5 | Mise en production | Gérer le déploiement, l’activation et le rollback des systèmes IA. | Conforme | nan |  |
| 8. Opération | 42001-8.6 | Surveillance & logs | Surveiller les IA en production (drift, incidents, journalisation, alertes). | Conforme | nan |  |
| 8. Opération | 42001-8.7 | Gestion des incidents | Traiter incidents IA (sécurité, éthique, performance) et retours utilisateurs. | Conforme | nan |  |
| 8. Opération | 42001-8.8 | Changements IA | Encadrer les changements (données, modèles, prompts, features) avec approbations. | Conforme | nan |  |
| 8. Opération | 42001-8.9 | Fournisseurs & tiers | Maîtriser les fournisseurs/tiers IA (contrats, évaluations, SOC2/ISO, SLA). | Conforme | nan |  |
| 8. Opération | 42001-8.10 | Sécurité & sûreté | Assurer sécurité/sûreté des systèmes IA (cyber, résilience, abus). | Conforme | nan |  |
| 8. Opération | 42001-8.11 | Conformité réglementaire | Satisfaire aux exigences légales et normatives (ex. AI Act, RGPD). | Conforme | nan |  |
| 9. Évaluation | 42001-9.1 | Suivi & mesures | Définir indicateurs, mesurer et analyser l’efficacité de l’AIMS. | Conforme | nan |  |
| 9. Évaluation | 42001-9.2 | Audit interne | Planifier et réaliser des audits internes de l’AIMS et des systèmes IA. | Conforme | nan |  |
| 9. Évaluation | 42001-9.3 | Revue de direction | Conduire des revues de direction régulières, décisions & actions. | Conforme | nan |  |
| 10. Amélioration | 42001-10.1 | Non-conformités & actions correctives | Traiter les NC, analyser causes, mettre en œuvre actions correctives. | Conforme | nan |  |
| 10. Amélioration | 42001-10.2 | Amélioration continue | Améliorer en continu l’adéquation, l’efficacité et l’efficience de l’AIMS. | Conforme | nan |  |

# 5. Plan d’actions priorisé

Aucune action requise.