Kernel Conseil

Rapport de préaudit cyber

Rapport de préaudit et plan de remédiation

Évaluation de maturité et plan d'action par Kernel Conseil

Synthèse dirigeante — le rapport détaillé et le plan d'action sont joints.

Organisation	Ateliers Morvan SAS
Secteur	Services TIC gérés (infogérance, MSP, MSSP)
Date de l'audit	22/09/2026
Périmètre	Système d’information, sites de Dijon et de Beaune
Référentiels évalués	ISO/IEC 27001:2022
Auditeur	Inès Kaci
Version	v1
Classification	Confidentiel

1. Résumé exécutif

Niveau de maturité global

Les chiffres clés de cette évaluation :

Score global	Exigences conformes	Non-conformités	NC critiques
47 %	**29**	**74**	**27**

Appréciation générale

L'organisation présente une maturité initiale qui expose ses activités critiques à des risques opérationnels et de continuité majeurs. L'absence de cadres formels pour la gestion des accès et la continuité d'activité fragilise la résilience des services TIC face à des menaces d'usurpation ou de sinistre. Le maintien de cette situation expose l'entreprise à des interruptions de service prolongées et à une perte de contrôle sur ses actifs informationnels. Une structuration immédiate de la gouvernance est indispensable pour sécuriser les fondations du système de management.

Points forts identifiés

• La communication interne et externe est structurée et documentée, ce qui assure une diffusion cohérente des directives de sécurité auprès des parties prenantes.
• La gestion des actifs documentés est opérationnelle, permettant une identification et une mise à jour régulière des informations essentielles au fonctionnement du système.
• Les procédures d'exploitation sont documentées et font l'objet d'une revue annuelle, garantissant une application stable des mesures techniques par les équipes IT.
• Le processus d'élimination sécurisée des supports est maîtrisé, assurant la traçabilité et la destruction effective des données sensibles en fin de vie.

Points de vigilance

• L'absence totale de politique de contrôle d'accès et de gestion des identités expose l'organisation à des risques élevés d'usurpation d'identité et d'accès non autorisés.
• Le manque de plan de reprise d'activité formalisé empêche toute garantie de continuité des services TIC en cas de perturbation majeure.
• L'absence de déploiement de l'authentification multi-facteurs sur les accès sensibles fragilise la sécurité logique face aux menaces externes.
• La gestion des vulnérabilités techniques repose sur des pratiques informelles, ce qui retarde la correction des failles de sécurité critiques sur les systèmes opérationnels.

Recommandation principale

La priorité absolue est de sécuriser les accès et de garantir la continuité des services. Il est impératif de déployer l'authentification multi-facteurs et de formaliser une politique de contrôle d'accès pour limiter immédiatement la surface d'exposition. Parallèlement, la réalisation d'une analyse d'impact sur l'activité permettra de définir les objectifs de reprise et de structurer le plan de continuité nécessaire à la survie des activités critiques.

Point budgétaire

La temporalité initiale de 2 ans apparaît trop courte. Une projection sur 3 ans est recommandée, soit un allongement estimé de 12 mois. Estimation établie à partir de la charge projetée (349,4 jours-homme), valorisée au tarif d'un RSSI externe (850 € HT par jour) appliqué à 50 % de la charge : le reste est supposé réalisable en interne.

2. Top 5 des chantiers prioritaires

Les chantiers sont classés par le poids de risque qu'ils retirent : chaque exigence en écart couverte par le chantier pèse 3 si elle est en non-conformité critique, 2 en non-conformité, 1 si le dispositif est partiel. À poids égal, le domaine le plus faible passe devant, puis le chantier le moins coûteux. Un domaine sans action rattachée au catalogue n'apparaît pas ici. Le coût est la somme des charges projetées des actions du chantier, valorisée sur 3 ans selon les hypothèses rappelées dans la section « Plan de remédiation ». La cible d'amélioration est le score que le domaine atteindrait si les exigences visées passaient le seuil de conformité de 80 % : c'est un objectif de chantier, pas une note acquise.

Chantier	Risque couvert	Actions	Coût	Amélioration ciblée
1. Mesures organisationnelles	31 exigences en écart (12 critiques, 12 majeurs, 7 partiels) : ISO27001-A5.1, ISO27001-A5.11, ISO27001-A5.12, ISO27001-A5.14…	• Mettre en place la gestion de la propriété intellectuelle et des licences • Adhérer a des groupes d'intérêt sécurité et mettre en place la veille • Mettre en place un processus de Cyber Threat Intelligence (CTI) • + 29 autres actions du plan joint	96 jours-homme — 40 821 € HT	41 % → cible 80 %
2. Mesures de sécurité technologiques	24 exigences en écart (7 critiques, 12 majeurs, 5 partiels) : ISO27001-A8.1, ISO27001-A8.10, ISO27001-A8.11, ISO27001-A8.12…	• Déployer la supervision et la planification de capacité • Déployer la synchronisation NTP sur l'ensemble du parc • Déployer la prévention de la fuite de données (DLP) • + 22 autres actions du plan joint	113,4 jours-homme — 48 182 € HT	49 % → cible 80 %
3. Mesures de sécurité physique	9 exigences en écart (3 critiques, 4 majeurs, 2 partiels) : ISO27001-A7.1, ISO27001-A7.10, ISO27001-A7.11, ISO27001-A7.13…	• Définir les règles de travail dans les zones sécurisées • Mettre en place le programme de maintenance du matériel • Définir et documenter les périmètres de sécurité physique • + 6 autres actions du plan joint	24,3 jours-homme — 10 340 € HT	49 % → cible 80 %
4. Mesures applicables aux personnes	7 exigences en écart (1 critique, 4 majeurs, 2 partiels) : ISO27001-A6.1, ISO27001-A6.2, ISO27001-A6.3, ISO27001-A6.4…	• Déployer la politique de télétravail sécurisé • Déployer le programme de formation sécurité par rôle • Intégrer les clauses de sécurité dans les contrats de travail • + 5 autres actions du plan joint	12,7 jours-homme — 5 385 € HT	48 % → cible 80 %

Chantier	Risque couvert	Actions	Coût	Amélioration ciblée
5. Planification	5 exigences en écart (1 critique, 4 majeurs) : ISO27001-6.1.1, ISO27001-6.1.2, ISO27001-6.1.3, ISO27001-6.2…	• Intégrer les actions dans les processus du SMSI • Mettre en place le processus de gestion des changements du SMSI • Évaluer l'efficacité des actions mises en œuvre • + 13 autres actions du plan joint	33 jours-homme — 14 025 € HT	36 % → cible 80 %

3. Synthèse globale des résultats

3.1 Score par référentiel

Le score global reflète une maturité encore embryonnaire, marquée par une forte dépendance aux pratiques informelles. L'écart entre les exigences de la norme et la réalité opérationnelle souligne un besoin urgent de formalisation documentaire pour transformer les acquis techniques en processus pérennes. Score global calculé sur les 123 exigence(s) renseignées et évaluées.

Référentiel	Note d'audit	Conformes	Partiels	Non-conformités	Non évaluées
ISO/IEC 27001:2022	47 %	29	20	74	0

3.2 Répartition des statuts de conformité

La répartition des écarts révèle une concentration préoccupante de non-conformités critiques, particulièrement dans les domaines de la sécurité logique et de la continuité. Cette distribution indique que les mesures de protection les plus fondamentales ne sont pas encore intégrées dans un cadre de gestion structuré.

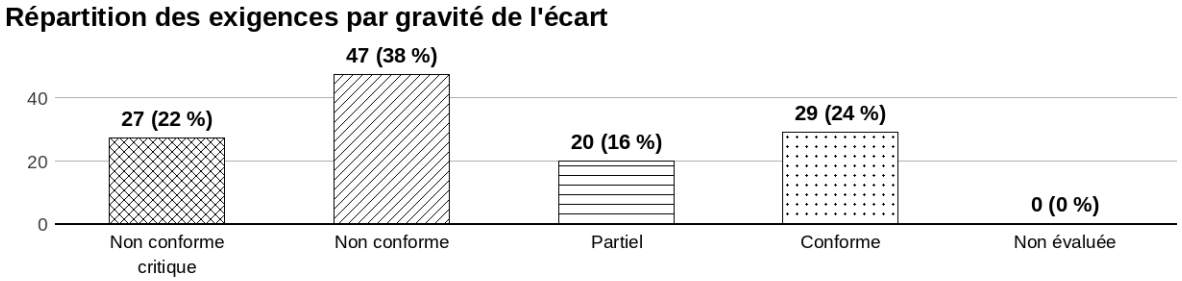

Figure 1 — Répartition de 123 exigences du périmètre : 27 « Non conforme critique » (22 %), 47 « Non conforme » (38 %), 20 « Partiel » (16 %), 29 « Conforme » (24 %), 0 « Non évaluée » (0 %). Une exigence non évaluée (sans réponse ou sans note) n'est comptée ni parmi les conformes ni parmi les non-conformités ; le détail exigence par exigence figure au chapitre « Détail des constats par exigence ».

3.3 Maturité par domaine de sécurité

Maturité par domaine de sécurité

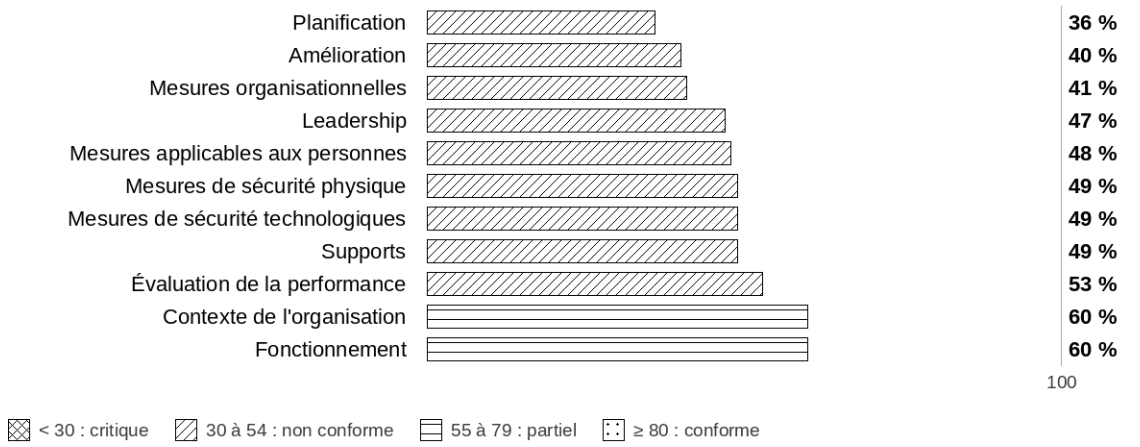

Figure 2 — Maturité par domaine de sécurité, du plus faible au plus fort. 11 domaines évalués, moyenne 48 % ; le plus faible est « Planification » à 36 %, le plus élevé « Fonctionnement » à 60 %. Le seuil de conformité est fixé à 80 %. Les scores exacts figurent dans le tableau ci-dessous.

Domaine	Score	Écarts relevés
Planification	36 %	5 évaluées · 5 non conformes dont 1 critique
Amélioration	40 %	2 évaluées · 2 non conformes
Mesures organisationnelles	41 %	37 évaluées · 7 partielles · 24 non conformes dont 12 critiques
Leadership	47 %	3 évaluées · 1 partielle · 2 non conformes
Mesures applicables aux personnes	48 %	8 évaluées · 2 partielles · 5 non conformes dont 1 critique
Supports	49 %	7 évaluées · 1 partielle · 4 non conformes dont 2 critiques
Mesures de sécurité physique	49 %	14 évaluées · 2 partielles · 7 non conformes dont 3 critiques
Mesures de sécurité technologiques	49 %	34 évaluées · 5 partielles · 19 non conformes dont 7 critiques
Évaluation de la performance	53 %	6 évaluées · 1 partielle · 3 non conformes dont 1 critique
Contexte de l'organisation	60 %	4 évaluées · 2 non conformes
Fonctionnement	60 %	3 évaluées · 1 partielle · 1 non conforme

4. Plan de remédiation priorisé

Cette section présente le plan d'action consolidé établi par Kernel Conseil, issu du rapprochement entre les non-conformités identifiées et le catalogue d'actions de remédiation des référentiels évalués.

4.1 Synthèse du plan

Le plan de remédiation est conçu pour traiter en priorité les failles critiques identifiées, en allouant les ressources nécessaires sur une période de trois ans. Cette approche permet de sécuriser les fondations avant d'engager des projets de maturité plus avancés.

Actions totales	Priorité critique	Priorité haute	Charge estimée
132	**53**	**39**	**350 jours-homme**

4.2 Actions prioritaires

Liste des actions de remédiation classées par priorité et par ordre d'exécution recommandé. Le détail complet de chaque action est disponible dans le plan d'action opérationnel joint à ce rapport.

ID	Libellé de l'action	Exigence liée	Priorité	Responsable	Échéance
ACT-A8.6-01	Déployer la supervision et la planification de capacité	ISO27001-A8.6	P0	Fixé en revue du plan	Année 1 · Mois 1
ACT-A5.32-01	Mettre en place la gestion de la propriété intellectuelle et des licences	ISO27001-A5.32	P0	Fixé en revue du plan	Année 1 · Mois 1
ACT-A5.6-01	Adhérer a des groupes d'intérêt sécurité et mettre en place la veille	ISO27001-A5.6	P0	Fixé en revue du plan	Année 1 · Mois 1
ACT-LDR-18	Communiquer les rôles et responsabilités sécurité	ISO27001-5.3	P0	Fixé en revue du plan	Année 1 · Mois 1
ACT-SUP-05	Constituer le dossier de preuves de compétences	ISO27001-7.2	P0	Fixé en revue du plan	Année 1 · Mois 1
ACT-A7.6-01	Définir les règles de travail dans les zones sécurisées	ISO27001-A7.6	P0	Fixé en revue du plan	Année 1 · Mois 1
ACT-A8.17-01	Déployer la synchronisation NTP sur l'ensemble du parc	ISO27001-A8.17	P0	Fixé en revue du plan	Année 1 · Mois 1
ACT-A7.13-01	Mettre en place le programme de maintenance du matériel	ISO27001-A7.13	P0	Fixé en revue du plan	Année 1 · Mois 1
ACT-LDR-13	Mettre la PSSI a disposition des parties intéressées externes	ISO27001-5.2	P0	Fixé en revue du plan	Année 1 · Mois 1

ID	Libellé de l'action	Exigence liée	Priorité	Responsable	Échéance
ACT-LDR-07	Promouvoir l'amélioration continue du SMSI	ISO27001-5.1	P0	Fixé en revue du plan	Année 1 · Mois 1

4.3 Feuille de route proposée

La feuille de route privilégie une montée en charge progressive, débutant par la sécurisation des accès et la mise en place de la veille sécurité. Les étapes suivantes se concentreront sur le déploiement de solutions de protection avancées et la formalisation des processus de continuité.