26/01/2026

Audit de conformité – NIS2

Société VESTA Corporate

MORA Florian – Consultant GRC

Table des matières

I. Contexte

Entreprise auditée : VESTA Corporate – filiale de production de climatiseurs (60 M€ de CA, 260 personnes)

Date de l'audit : 26/01/2026

Objet de l'audit :
Évaluer l'état de conformité de la société vis-à-vis du **texte provisoire français de la directive NIS 2**, afin de :

1. Identifier les écarts et risques existants dans la gestion de la sécurité des systèmes d'information.
2. Déterminer les chantiers prioritaires de mise en conformité.
3. Fournir à la direction et au RSSI une vision claire du niveau de maturité SSI de la société.

Contexte réglementaire :

- La directive NIS 2 transpose les exigences européennes en matière de cybersécurité pour les **opérateurs de services essentiels et les entités importantes**.
- Les obligations couvrent plusieurs domaines : gouvernance et gestion des risques, gestion des incidents, sécurité des accès, sécurité réseau et systèmes, continuité des services, sensibilisation et formation, supervision et journalisation.
- Le respect de ces exigences est obligatoire pour garantir la **résilience opérationnelle et la conformité légale**.

Sources utilisées :

- Audit interne de maturité selon le **Guide Hygiène ANSSI** (tableau fourni par VESTA Corporate)
- Entretiens avec le RSSI et responsables IT
- Documentation interne sur les procédures et politiques de sécurité

Périmètre de l'audit :

- Cette évaluation porte exclusivement sur la filiale ciblée pour l'acquisition, incluant :
    - Les infrastructures informatiques et systèmes
    - Les procédures opérationnelles et de gouvernance en cybersécurité
    - Les services tiers et prestataires impactant la sécurité du SI

Limites :

- L'audit se base sur les informations fournies par l'entreprise et sur les observations disponibles au moment de l'évaluation.
- Certaines pratiques opérationnelles peuvent ne pas être documentées ou vérifiables de manière complète.

II. Méthodologie d'audit

Sources et données utilisées

- Tableau d'audit de maturité selon le **Guide Hygiène ANSSI** fourni par l'entreprise.
- Entretiens avec le RSSI, responsables IT et responsables opérationnels.
- Documentation interne : politiques, procédures, contrats avec prestataires.
- Observations directes et contrôle des mesures techniques (pare-feu, sauvegardes, journalisation, MFA…).

4. Approche et critères d'évaluation

- **Comparaison avec le texte provisoire français NIS 2**, article par article.
- Évaluation par **niveau de conformité** :
    - Conforme
    - Partiellement conforme
    - Non conforme
- Prise en compte :
    - Impact sur la continuité des services essentiels.
    - Risque opérationnel et cybersécurité.
    - Degré de formalisation et documentation des processus.

III. Applicabilité de NIS 2

Références utilisées

- *Directive (UE) 2022/2555 (NIS 2)*
- *Annexe I : secteurs hautement critiques*
- *Annexe II : autres secteurs critiques*
- *Critères de taille :*
  - *≥ 50 salariés ou ≥ 10 M€ de CA → entité concernée par défaut*
- *Principe : analyse entité par entité, pas au niveau groupe*

1 – Tableau d'évaluation EE/EI (Annexe 1-1) :

Secteur / Annexe	Taille entreprise	Employés	Chiffre d'affaires (€)	Bilan (€)	Classification NIS 2	Applicabilité	Remarques
Annexe I – Secteurs critiques	Grande	> 250	> 50 M€	> 43 M€	Entité Essentielle (EE)	☑ Applicable automatiquement	Ex. énergie, transports, santé, agroalimentaire critique
Annexe I	Moyenne	50–250	10–50 M€	10–43 M€	Entité Importante (EI)	☑ Applicable automatiquement	Taille suffisante, secteur critique
Annexe I	Petite	< 50	< 10 M€	< 10 M€	Entité Importante (EI)	⚠ Applicable par désignation	Si service critique ou impact systémique
Annexe II – Secteurs importants	Grande	> 250	> 50 M€	> 43 M€	Entité Importante (EI)	☑ Applicable automatiquement	Ex. services numériques, industrie stratégique
Annexe II	Moyenne	50–250	10–50 M€	10–43 M€	Entité Importante (EI)	☑ Applicable automatiquement	Taille et secteur conformes
Annexe II	Petite	< 50	< 10 M€	< 10 M€	Non concernée	✗ Non applicable	Hors scope, sauf désignation exceptionnelle par l'autorité
Hors annexe	Toute taille	–	–	–	Non applicable	✗ Non applicable	Activité non critique, hors scope NIS 2

2 – Tableau d'évaluation de l'application de NIS2 (Annexe 1-2)

Entité	Activité principale	Secteur NIS 2	Secteur listé Annexe I/II	Activité critique	Effectif ≥ 50	CA ≥ 10 M€	Taille NIS 2 atteinte	Type d'entité	Applicabilité NIS 2	Justification réglementaire détaillée
VESTA Holding	Siège / fonctions support	Hors périmètre	✗ Non	✗ Non	✗ 40	☑ 15 M€	✗ Non (critère incomplet)	Aucune	✗ Non applicable	Activité non listée en annexe I ou II. Holding sans service critique propre. Effectif < 50. Hors périmètre NIS 2.
VESTA Power	Production & distribution d'électricité	Énergie	☑ Annexe I (Énergie)	☑ Oui	☑ 1 200	☑ 800 M€	☑ Oui	Entité Essentielle	☑ Applicable	Secteur énergie explicitement visé (Annexe I). Activité critique nationale. Taille largement supérieure aux seuils réglementaires.
VESTA Invest	Plateforme SaaS crypto	Services numériques	☑ Annexe II	☑ Oui	☑ 55	☑ 100 M€	☑ Oui	Entité Importante	☑ Applicable	Fournisseur de service numérique. Dépassement des seuils de taille. Exposition élevée aux risques cyber systémiques.
VESTA Foods	Industrie agroalimentaire	Agroalimentaire	☑ Annexe II	☑ Oui	☑ 200	☑ 45 M€	☑ Oui	Entité Importante	☑ Applicable	Industrie agroalimentaire listée Annexe II. Maillon critique de la chaîne d'approvisionnement alimentaire.
VESTA Digital	Hébergement / vote électronique	Services numériques	⚠ Annexe II	⚠ Oui	✗ 35	✗ 4 M€	✗ Non	Aucune (par défaut)	⚠ Désignation possible	Taille < seuils. Peut être désignée par l'autorité en raison de la criticité du service rendu à un opérateur essentiel (SNCF).
Cible M&A (Climatisation)	Industrie manufacturière	Industrie manufacturière	☑ Annexe II	☑ Oui	☑ 260	☑ 60 M€	☑ Oui	Entité Importante	☑ Applicable	Industrie manufacturière listée Annexe II. Seuils atteints. Applicabilité NIS 2 confirmée dès l'acquisition.

L'analyse montre que le groupe VESTA est directement impacté par la directive NIS 2, mais avec des niveaux de responsabilité différents selon les entités.

1. **Entités directement assujetties**

Quatre entités entrent immédiatement dans le champ d'application en raison de leur secteur et du franchissement des seuils (effectifs/CA) :

- **VESTA Power (Entité essentielle)** : Secteur Énergie. Soumise au niveau d'exigence le plus élevé (criticité majeure).
- **VESTA Invest & VESTA Foods (Entités importantes)** : Respectivement dans les services numériques et l'agroalimentaire. Obligations de sécurité et de notification immédiates.
- **Cible M&A (Entité *importante)* :** Le secteur manufacturier de la cible déclenche une mise en conformité dès l'intégration au groupe.

2. **Les points de vigilance**

- **VESTA Digital :** Bien qu'en dessous des seuils de taille, ses prestations pour des clients stratégiques (SNCF) font peser un risque de désignation forcée par l'autorité nationale.
- **VESTA Holding :** Reste en dehors du périmètre de la directive à ce jour.

IV. Analyse de Conformité NIS2

La société analysée est la société cible du M&A (fabrication de climatiseurs – 60 M€ / 260 personnes).

Rappel des exigences NIS 2 (France – provisoire)

Pour une Entité Importante, NIS 2 impose notamment :

- *Gestion formalisée des risques cyber,*
- *Mesures techniques et organisationnelles documentées,*
- *Gestion des incidents + notification,*
- *Contrôle des accès et des privilèges,*
- *Continuité d'activité,*
- *Supervision et journalisation,*
- *Responsabilité de la direction.*

1 – Tableau d'analyse de conformité NIS2 par rapport à l'audit (Annexe 2-1)

Exigence NIS 2 – Texte FR provisoire	Articles	Explication de l'article	Éléments observés (audit)	État	Justification
Politique de gestion des risques cyber	Art. 21.1.a	L'entité doit établir et maintenir une analyse formelle des risques cyber, incluant les actifs critiques, les menaces et les impacts potentiels	Analyse de risques jamais réalisée (41R)	Non conforme	Absence totale d'analyse de risques formelle
Gouvernance SSI	Art. 21.1	L'entité doit définir une gouvernance SSI claire : responsabilités, politique de sécurité, indicateurs, pilotage des mesures	RSSI identifié mais peu de politiques formalisées (39, 34)	Partiel	Gouvernance existante mais non alignée avec les exigences de pilotage et de responsabilité NIS 2(pas de politique SSI, pas d'indicateurs, pas de pilotage NIS 2).
Gestion des incidents	Art. 21.1.b / 23	L'entité doit mettre en place des procédures de détection, réponse et notification des incidents de cybersécurité	Aucune procédure, aucun retour d'expérience (40)	Non conforme	Incapacité à détecter et gérer un incident
Continuité & sauvegardes	Art. 21.1.c	L'entité doit assurer la continuité de ses services essentiels via sauvegardes et plans de reprise	Sauvegardes 3-2-1 en place (37)	Conforme	Sauvegardes opérationnelles
Sécurité de la supply chain	Art. 21.1.d	L'entité doit gérer la sécurité des tiers et prestataires, en encadrant leurs accès et obligations de sécurité	Prestataire N1 avec droits élevés sans exigences SSI (3)	Non conforme	Aucun encadrement sécurité des tiers
Gestion des accès	Art. 21.1.f	L'entité doit contrôler l'accès aux systèmes, limiter les droits au strict nécessaire et revoir périodiquement les permissions	Pas de revue des droits, droits admins mal maîtrisés (5,6,9,29)	Non conforme	Accès excessifs non contrôlés
Authentification forte	Art. 21.2	L'entité doit mettre en place une authentification forte sur les accès critiques (MFA)	MFA partiel avec dérogations (13)	Partiel	MFA non généralisé
Sécurité réseau	Art. 21.1.e	L'entité doit segmenter les réseaux, cloisonner les services et protéger les systèmes exposés	Segmentation faible, services exposés sans protection (19,23)	Partiel	Cloisonnement insuffisant
Journalisation & supervision	Art. 21.1.g	L'entité doit activer, configurer et centraliser les journaux, corréler et superviser les événements de sécurité	Logs limités aux AD, pas de corrélation (36)	Partiel	Capacité de détection insuffisante pour répondre aux exigences de détection précoce et de notification NIS 2 (Pas de SIEM, Pas de NTP, Pas de corrélation).Logs uniquement AD.
Sensibilisation & formation	Art. 21.2	L'entité doit former et sensibiliser régulièrement l'ensemble du personnel aux risques cyber et bonnes pratiques	Actions ponctuelles non structurées (2,2R)	Partiel	Absence de programme formalisé

Niveau global estimé de conformité NIS 2 : faible

La majorité des exigences structurantes (gestion des risques, incidents, gouvernance, IAM, supply chain) ne sont pas satisfaites. Les mesures en place relèvent principalement de l'hygiène technique et non d'une démarche de gestion des risques conforme à NIS 2.

V. Chantiers majeurs de mise en conformité

1 - Critères pour définir un chantier majeur

Un chantier est majeur si :

Non-conformité totale ou partielle critique	*Ex : gestion des incidents, gestion des accès, gouvernance/risk management.*
Impact opérationnel élevé	*Ex : droits administrateurs non contrôlés → risque de compromission du SI.*
Exigence réglementaire obligatoire	*Ex : analyse de risques formelle, reporting à l'ANSSI.*
Chantier transversal	*Ex : sécurité des réseaux et SI, journalisation → impact sur toutes les entités et systèmes.*

2 – Échelle de niveau de priorité (Annexe 3-1)

Niveau	Description	Critères d'attribution
Très haute (1 / Critique)	Chantiers indispensables pour atteindre la conformité NIS 2 et réduire le risque cyber majeur. Non traités, ils exposent l'entreprise à des sanctions ou à un incident majeur.	- Absence totale d'un processus requis par NIS 2- Impact direct sur les services critiques ou la notification d'incidents- Failles dans la gouvernance ou la gestion des risques
Haute (2 / Importante)	Chantiers nécessaires pour renforcer le contrôle et la sécurité, impact modéré sur la conformité si non traités mais risque significatif sur les accès ou les tiers.	- Contrôles partiels ou insuffisants- Gestion des accès, authentification, sécurité des prestataires- Risques importants mais non immédiats sur la continuité
Moyenne (3 / Recommandée)	Chantiers qui améliorent la robustesse et la résilience, mais dont l'absence n'empêche pas la conformité immédiate.	- Processus partiellement mis en place- Amélioration de supervision, formation ou réseau- Risque limité ou indirect
Faible (4 / Optionnelle)	Chantiers non critiques pour la conformité NIS 2 mais pouvant optimiser la sécurité ou la maturité globale.	- Amélioration marginale- Processus déjà existants mais perfectibles- Aucun impact légal direct

3 – Tableau des Chantiers majeurs de mise en conformité (Annexe 3-2)

Chantier majeur	Éléments du tableau / Audit	Commentaire	Priorité NIS 2	Articles liés
Gouvernance et gestion des risques cyber	41R, 34, 39	Analyse de risques absente, politique SSI partielle, RSSI présent mais gouvernance faible	Très haute	Art. 21.1.a / 21.1
Gestion des incidents de sécurité	40	Pas de procédure, incapacité à détecter et réagir à un incident	Très haute	Art. 21.1.b / 23
Gestion des accès et authentification	5,6,8,9,12,13,29	Pas de revue des droits, comptes admins mal maîtrisés, MFA partiel, absence de journalisation	Haute	Art. 21.1.f & 21.2
Sécurité réseau et cloisonnement	19,21,23	Segmentation limitée, services exposés sans protection frontale (firewall/WAF), absence de revue des flux	Haute	Art. 21.1.e
Supervision et journalisation	36,36R	Logs limités à l'AD, pas de corrélation, pas d'alerting centralisé, pas de SIEM ni NTP	Moyenne	Art. 21.1.g
Sensibilisation & formation	1,2,2R	Programme de sensibilisation partiel, non structuré, absence de suivi ou validation des connaissances	Moyenne	Art. 21.2
Nomadisme et postes de travail	30,30R,32,33,33R	Pas de protection réseau pour les nomades, pas de politique de sécurité dédiée aux terminaux mobiles	Moyenne	Art. 21.1.f / 21.2
Continuité & sauvegardes	37,37R	Sauvegardes 3-2-1 présentes mais sans tests réguliers ni classification des actifs critiques	Moyenne	Art. 21.1.c
Sécurité de la supply chain / infogérance	3	Prestataires non encadrés par des exigences de sécurité, accès privilégiés non contrôlés	Haute	Art. 21.1.d

Les chantiers de mise en conformité présentés ci-dessus regroupent les principaux axes d'amélioration nécessaires pour répondre aux obligations NIS 2. Ils couvrent aussi bien des aspects organisationnels (gouvernance, gestion des risques, gestion des incidents) que techniques (gestion des accès, sécurité réseau, supervision, nomadisme, relation avec les prestataires).

Une échelle de priorité est associée à chaque chantier afin de distinguer les actions critiques à mettre en œuvre en premier, notamment celles ayant un impact direct sur la capacité de l'organisation à prévenir, détecter et réagir à un incident de cybersécurité.

VI. Plan de mise en conformité NIS2

1 – tableau de mise en conformité NIS2 (Annexe 4-1)

Chantier / Action	Observation / Éléments d'audit	Priorité	Durée estimée	Chiffrage approximatif	Articles NIS 2	Explication de l'article	Description précise	Remédiation
Gouvernance et politique SSI	RSSI identifié, politiques partielles (34,39)	Très haute	2-3 mois	15-25k	Art. 21.1	Obligation de mettre en place une gouvernance, responsabilité, pilotage et reporting	Formaliser la gouvernance SSI : politique, responsabilités, comité pilotage, KPI, reporting NIS 2	- Nommer RSSI avec délégation COMEX- Comité pilotage NIS 2 avec PV- Politique SSI validée par la direction- Tableau de suivi des actions NIS 2
Analyse formelle des risques cyber	Analyse de risques jamais réalisée (41R)	Très haute	3-4 mois	30-50k	Art. 21.1.a	Obligation d'évaluer et traiter les risques cyber de manière formelle	Cartographier actifs critiques, identifier menaces et vulnérabilités, définir plan de traitement	- Inventaire des actifs critiques- Cartographie des risques avec probabilité × impact- Plan de traitement et priorisation- Intégrer risques supply chain
Gestion des incidents	Aucune procédure, aucun retour d'expérience (40)	Très haute	2-3 mois	10-20k	Art. 21.1.b / 23	Définir processus de gestion des incidents et notification aux autorités compétentes	Créer procédures d'incidents, workflow interne/externe, tests annuels	- Rédiger procédures écrites- Définir rôles et responsabilités- Workflow notification Incidents majeurs- Registre central des incidents et exercices annuels
Gestion des accès et authentification	Pas de revue des droits, comptes admins mal maîtrisés, MFA partiel, absence journalisation (5,6,8,9,17,13,29)	Haute	2-3 mois	15-30k	Art. 21.1.f & 21.2	Obligation de contrôle des accès, séparation des rôles, authentification forte	Revue périodique des droits, séparation des rôles, MFA généralisé, coffre-fort mots de passe, journalisation	- Revue des droits trimestrielle- Séparation comptes utilisateurs/admin- MFA obligatoire pour tous- Coffre-fort administrateurs- Journalisation immuable actions critiques
Supply chain / prestataires	Prestataires N1 avec droits élevés non encadrés (3)	Haute	1-2 mois	5-15k	Art. 21.1.d	Obligation de gérer les risques liés aux prestataires	Définir exigences SSI dans contrats, limiter droits selon principe du moindre privilège, suivi et audit prestataires	- Ajouter clauses SSI dans contrats- Limiter droits et privilèges- Audit périodique des prestataires- Intégrer prestataires au plan de reprise et gestion incident
Sécurité réseau et cloisonnement	Segmentation limitée, services exposés sans protection frontale (19,21,23)	Haute	3-4 mois	20-40k	Art. 21.1.e	Obligation de sécuriser les réseaux, segmenter, protéger zones critiques	Segmenter réseau, firewall/WAF, limitation services exposés, revue régulière des flux	- Segmenter réseau par zones critiques- Déployer firewall et WAF- Scanner services exposés et corriger vulnérabilités- Mettre en place IDS/IPS et supervision
Supervision et journalisation	Logs limités à AD, pas de corrélation (36,36R)	Moyenne	3-4 mois	25-50k	Art. 21.1.g	Obligation de journaliser, auditer et superviser les systèmes	Centraliser logs, corrélation SIEM, alerting, synchronisation NTP	- Déployer SIEM pour tous les composants critiques- Synchroniser horodatage NTP- Définir plan de conservation logs- Alerting et corrélation événements
Sensibilisation & formation	Programme partiel et non structuré (1,2,2R)	Moyenne	1-2 mois initial puis continu	5-10k/an	Art. 21.2	Obligation de sensibiliser/former utilisateurs et équipes	Définir programme structuré, ciblage par rôle, suivi et validation	- Élaborer programme annuel par rôle- Formation obligatoire- Suivi des validations- Campagnes périodiques et tests phishing
Nomadisme et postes de travail	Pas de protection réseau nomades, pas de politique mobiles (30,30R,32,33,33R)	Moyenne	2-3 mois	10-25k	Art. 21.1.f / 21.2	Obligation de sécuriser terminaux mobiles et nomades	VPN obligatoire, endpoint protection, chiffrement disque, politique terminaux mobiles, règles d'accès	- Installer VPN et endpoint protection- Chiffrement obligatoire- MDM / EMM pour mobiles- Contrôle d'accès réseau pour nomades
Continuité & sauvegardes	Sauvegardes présentes mais sans tests ni classification (37,37R)	Moyenne	1-2 mois + continu	5-15k	Art. 21.1.c	Obligation de maintenir continuité des services et restauration des données	Maintenir sauvegardes 3-2-1, tests réguliers, classifier actifs critiques, plans de restauration	- Tester restaurations régulièrement- Classifier actifs critiques- Documenter procédures, RPO/RTO par service- Intégrer continuité dans plan sécurité NIS 2
			Total =	(140 K - 280K) euros				

Au regard des écarts identifiés lors de l'analyse de conformité, un plan de mise en conformité NIS 2 a été élaboré afin de répondre aux exigences du texte français provisoire. Ce plan s'appuie sur les chantiers majeurs identifiés précédemment et propose des actions concrètes, priorisées en fonction de leur criticité réglementaire et de leur impact sur la sécurité des services.

VII. Evaluation de conformité Post remédiation

1 – Evaluation Post-Remédiation de conformité NIS2 (Annexe 5-2)

Exigence NIS 2 – Texte FR provisoire	Articles	Éléments observés (audit)	État actuel	Nouvel état post-remédiation	Justification post-remédiation	Explication article
Politique de gestion des risques cyber	Art. 21.1.a	Analyse de risques jamais réalisée (41R)	Non conforme	Conforme	Analyse formelle réalisée, cartographie des risques, plan de traitement documenté et validé par la direction	Obligation d'évaluer et traiter les risques cyber formellement
Gouvernance SSI	Art. 21.1	RSSI identifié mais peu de politiques formalisées (39,34)	Partiel	Conforme	Politique SSI complète, comité pilotage NIS2, reporting au COMEX et indicateurs KPI en place	Obligation de mettre en place une gouvernance avec responsabilités et pilotage
Gestion des incidents	Art. 21.1.b / 23	Aucune procédure, aucun retour d'expérience (40)	Non conforme	Conforme	Procédures documentées, workflow d'incidents, notification aux autorités, exercices annuels réalisés	Obligation de définir un processus de gestion des incidents et notification
Continuité & sauvegardes	Art. 21.1.c	Sauvegardes 3-2-1 en place (37)	Conforme	Conforme	Plan de sauvegarde testé, classification des actifs critiques, RPO/RTO définis	Obligation de maintenir continuité et restauration des données
Sécurité de la supply chain	Art. 21.1.d	Prestataire N1 avec droits élevés sans exigences SSI (3)	Non conforme	Conforme	Clauses SSI ajoutées dans les contrats, droits limités, audits périodiques prestataires, intégration dans plan reprise	Obligation de gérer les risques liés aux prestataires et tiers
Gestion des accès	Art. 21.1.f	Pas de revue des droits, droits admins mal maîtrisés (5,6,9,29)	Non conforme	Conforme	Revue trimestrielle des droits, séparation comptes utilisateurs/admin, MFA généralisé, journalisation immuable	Obligation de contrôler les accès et séparer les rôles critiques
Authentification forte	Art. 21.2	MFA partiel avec dérogations (13)	Partiel	Conforme	MFA généralisé pour tous les utilisateurs et administrateurs, politique de mots de passe renforcée	Obligation d'utiliser une authentification forte pour tous les accès critiques
Sécurité réseau	Art. 21.1.e	Segmentation faible, services exposés sans protection (19,23)	Partiel	Conforme	Segmentation complète, firewall/WAF, IDS/IPS, revue régulière des flux, protection des services exposés	Obligation de sécuriser les réseaux et protéger les zones critiques
Journalisation & supervision	Art. 21.1.g	Logs limités aux AD, pas de corrélation (36)	Partiel	Conforme	SIEM centralisé, logs de tous composants critiques, corrélation, alerting, horodatage NTP synchronisé	Obligation de journaliser et auditer pour détecter incidents et anomalies
Sensibilisation & formation	Art. 21.2	Actions ponctuelles non structurées (2,2R,1)	Partiel	Conforme	Programme annuel structuré par rôle, suivi des validations, tests phishing périodiques	Obligation de sensibiliser et former les utilisateurs régulièrement
Nomadisme & postes de travail	Art. 21.1.f / 21.2	Pas de protection réseau pour nomades, pas de politique mobiles	Partiel	Conforme	VPN et endpoint protection obligatoires, chiffrement disque et communications, MDM pour mobiles, contrôle d'accès réseau	Obligation de sécuriser les terminaux nomades et mobiles
Sécurité des postes de travail	Art. 21.1.f	Niveau minimal non appliqué (14R,15R,16,17R)	Partiel	Conforme	Sécurité minimale appliquée sur tous les postes : antivirus, firewall, GPO documentées, chiffrement, restriction droits admin	Obligation de sécuriser l'ensemble du parc informatique
Gestion des interconnexions et messagerie	Art. 21.1.e	Interconnexions limitées, messagerie partiellement protégée (22,24,25)	Partiel	Conforme	Passerelles sécurisées, authentification utilisateurs, contrôle interconnexions, messagerie filtrée	Obligation de sécuriser les échanges réseau et messageries critiques
Administration SI	Art. 21.1.f / 21.2	Accès aux postes admin non séparés, réseau admin non cloisonné (27,28,29)	Non conforme	Conforme	Réseau d'administration séparé, accès restreint, MFA, journalisation immuable, séparation postes admin et postes utilisateurs	Obligation de sécuriser administration SI et limiter droits admin

Sur la base du plan de mise en conformité proposé, un état de conformité post-remédiation a été établi afin d'évaluer le niveau de conformité NIS 2 atteignable une fois l'ensemble des actions mises en œuvre. Cette projection permet de mesurer l'impact des remédiations sur les exigences réglementaires et d'illustrer l'amélioration du niveau de maturité cybersécurité de l'entité auditée.

Le tableau post-remédiation présenté ci-après montre que la mise en œuvre complète des actions permettrait d'atteindre un niveau de conformité globalement conforme aux exigences NIS 2, avec des mesures formalisées, pilotées et auditées.

VIII. Estimation des délais, des coûts

Estimation des délais

- La mise en conformité avec la directive NIS 2 représente un effort significatif en termes de temps, de ressources humaines et d'investissement financier. Les actions identifiées dans le plan de mise en conformité s'inscrivent dans une démarche progressive, qui peut raisonnablement s'étaler sur une période de **12 à 24 mois**, en fonction des priorités retenues et de la capacité de l'organisation à mobiliser les équipes internes et les prestataires externes.

1 - Tableau des délais (Annexe 6-1) :

Axe de conformité	Actions principales associées	Priorité	Durée estimée
Gouvernance SSI & pilotage NIS 2	Politique SSI, comité NIS 2, KPI, reporting direction	Haute	2 à 3 mois
Analyse de risques cyber	Cartographie des actifs, analyse des risques, plan de traitement	Haute	2 mois
Gestion des incidents	Procédures, notification, exercices de crise	Haute	1 à 2 mois
Gestion des accès & identités	Revue des droits, MFA généralisé, comptes admins	Haute	3 à 4 mois
Sécurité réseau & services exposés	Segmentation, WAF, revue des flux, scans	Moyenne	3 à 4 mois
Supervision & journalisation	Centralisation des logs, SIEM, alerting	Moyenne	3 mois
Supply chain & prestataires	Clauses SSI, audits, limitation des accès	Moyenne	2 à 3 mois
Nomadisme & postes de travail	VPN, MDM, politiques terminaux	Moyenne	2 mois
Sensibilisation & formation	Programme annuel, campagnes, tests	Basse	1 mois (puis récurrent)
Continuité & sauvegardes	Tests PRA/PCA, RPO/RTO	Basse	1 à 2 mois
		Total =	12 à 18 mois

Estimation des coûts

- La mise en œuvre du plan de mise en conformité NIS 2 entraîne également des coûts financiers, principalement liés à l'accompagnement en gouvernance et gestion des risques, à la mise en place ou au renforcement de mesures techniques de sécurité, ainsi qu'à la formation et à la sensibilisation des utilisateurs.
- Ces coûts sont à la fois organisationnels et techniques, et varient selon le niveau de maturité initial de l'entité et les solutions déjà en place.
- Les estimations présentées ne prennent en compte les investissements initiaux (outils, intégration, accompagnement) ainsi que certains coûts récurrents, notamment pour la supervision, la maintenance des solutions de sécurité et la montée en compétence des équipes.

2 – Tableaux d'estimation des coûts (Annexe 6-2) :

Poste de coût	Description	Coût estimatif
Accompagnement GRC / RSSI	Analyse de risques, gouvernance, procédures, pilotage NIS 2	30 k€ – 50 k€
Solutions IAM / MFA / PAM	MFA généralisé, gestion des comptes à privilèges	20 k€ – 40 k€
Supervision & SIEM	Outil SIEM + intégration + exploitation initiale	40 k€ – 70 k€
Sécurité réseau	WAF, segmentation, audits et scans	20 k€ – 35 k€
Sécurité postes & nomadisme	VPN, MDM, protection endpoints	15 k€ – 25 k€
Supply chain & audits tiers	Audits prestataires, contractualisation SSI	10 k€ – 20 k€
Sensibilisation & formation	Campagnes, supports, simulations phishing	5 k€ – 10 k€
Continuité & PRA	Tests, exercices, accompagnement	5 k€ – 10 k€
	Total =	145 k€ à 260 k€

IX. Conclusion

Cette étude a permis de mettre en évidence les écarts existants entre la situation actuelle de l'entité auditée et les exigences de la directive NIS 2, ainsi que les actions nécessaires pour atteindre un niveau de conformité satisfaisant. La mise en conformité implique un effort réel en termes de temps, d'organisation et d'investissement financier, qui doit être envisagé dans une logique progressive et pilotée.

Bien que ces investissements puissent apparaître importants à court terme, la conformité NIS 2 apporte plusieurs **bénéfices structurants**. Elle permet avant tout de **réduire significativement les risques cyber**, d'améliorer la capacité de détection et de réaction face aux incidents, et de renforcer la résilience globale des services critiques. Elle contribue également à une meilleure maîtrise des responsabilités, à une clarification des rôles au sein de l'organisation et à une meilleure visibilité de la cybersécurité au niveau de la direction.

Enfin, au-delà de la seule obligation réglementaire, la conformité NIS 2 constitue un véritable levier de maturité et de confiance, tant vis-à-vis des partenaires et des clients que des autorités.

X. Annexes

Sources utilisées :

- NIS2 - Conformité (PWC France)
- Directive NIS 2 (Cyber Gouv)

Annexes :

- **Fichier Excel d'audit de conformité NIS2 (Mora Florian)**

Tableau annexes :

Annexe 1-1 : Tableau d'évaluation EE/EI :

Secteur / Annexe	Taille entreprise	Employés	Chiffre d'affaires (€)	Bilan (€)	Classification NIS 2	Applicabilité	Remarques
Annexe I – Secteurs critiques	Grande	> 250	> 50 M€	> 43 M€	Entité Essentielle (EE)	☑ Applicable automatiquement	Ex. énergie, transports, santé, agroalimentaire critique
Annexe I	Moyenne	50–250	10–50 M€	10–43 M€	Entité Importante (EI)	☑ Applicable automatiquement	Taille suffisante, secteur critique
Annexe I	Petite	< 50	< 10 M€	< 10 M€	Entité Importante (EI)	⚠ Applicable par désignation	Si service critique ou impact systémique
Annexe II – Secteurs importants	Grande	> 250	> 50 M€	> 43 M€	Entité Importante (EI)	☑ Applicable automatiquement	Ex. services numériques, industrie stratégique
Annexe II	Moyenne	50–250	10–50 M€	10–43 M€	Entité Importante (EI)	☑ Applicable automatiquement	Taille et secteur conformes
Annexe II	Petite	< 50	< 10 M€	< 10 M€	Non concernée	✗ Non applicable	Hors scope, sauf désignation exceptionnelle par l'autorité
Hors annexe	Toute taille	–	–	–	Non applicable	✗ Non applicable	Activité non critique, hors scope NIS 2

Annexe 1-2 : Tableau d'évaluation de l'application de NIS2

Entité	Activité principale	Secteur NIS 2	Secteur listé Annexe I/II	Activité critique	Effectif ≥ 50	CA ≥ 10 M€	Taille NIS 2 atteinte	Type d'entité	Applicabilité NIS 2	Justification réglementaire détaillée
VESTA Holding	Siège / fonctions support	Hors périmètre	✗ Non	✗ Non	✗ 40	☑ 15 M€	✗ Non (critère incomplet)	Aucune	✗ Non applicable	Activité non listée en annexe I ou II. Holding sans service critique propre. Effectif < 50. Hors périmètre NIS 2.
VESTA Power	Production & distribution d'électricité	Énergie	☑ Annexe I (Énergie)	☑ Oui	☑ 1 200	☑ 800 M€	☑ Oui	Entité Essentielle	☑ Applicable	Secteur énergie explicitement visé (Annexe I). Activité critique nationale. Taille largement supérieure aux seuils réglementaires.
VESTA Invest	Plateforme SaaS crypto	Services numériques	☑ Annexe II	☑ Oui	☑ 55	☑ 100 M€	☑ Oui	Entité Importante	☑ Applicable	Fournisseur de service numérique. Dépassement des seuils de taille. Exposition élevée aux risques cyber systémiques.
VESTA Foods	Industrie agroalimentaire	Agroalimentaire	☑ Annexe II	☑ Oui	☑ 200	☑ 45 M€	☑ Oui	Entité Importante	☑ Applicable	Industrie agroalimentaire listée Annexe II. Maillon critique de la chaîne d'approvisionnement alimentaire.
VESTA Digital	Hébergement / vote électronique	Services numériques	⚠ Annexe II	⚠ Oui	✗ 35	✗ 4 M€	✗ Non	Aucune (par défaut)	⚠ Désignation possible	Taille < seuils. Peut être désignée par l'autorité en raison de la criticité du service rendu à un opérateur essentiel (SNCF).
Cible M&A (Climatisation)	Industrie manufacturière	Industrie manufacturière	☑ Annexe II	☑ Oui	☑ 260	☑ 60 M€	☑ Oui	Entité Importante	☑ Applicable	Industrie manufacturière listée Annexe II. Seuils atteints. Applicabilité NIS 2 confirmée dès l'acquisition.

Annexe 2-1 : – Tableau d'analyse de conformité NIS2 par rapport à l'audit

Exigence NIS 2 – Texte FR provisoire	Articles	Explication de l'article	Éléments observés (audit)	État	Justification
Politique de gestion des risques cyber	Art. 21.1.a	L'entité doit établir et maintenir une analyse formelle des risques cyber, incluant les actifs critiques, les menaces et les impacts potentiels	Analyse de risques jamais réalisée (41R)	Non conforme	Absence totale d'analyse de risques formelle
Gouvernance SSI	Art. 21.1	L'entité doit définir une gouvernance SSI claire : responsabilités, politique de sécurité, indicateurs, pilotage des mesures	RSSI identifié mais peu de politiques formalisées (39,34)	Partiel	Gouvernance existante mais non alignée avec les exigences de pilotage et de responsabilité NIS 2(pas de politique SSI, pas d'indicateurs, pas de pilotage NIS 2).
Gestion des incidents	Art. 21.1.b / 23	L'entité doit mettre en place des procédures de détection, réponse et notification des incidents de cybersécurité	Aucune procédure, aucun retour d'expérience (40)	Non conforme	Incapacité à détecter et gérer un incident
Continuité & sauvegardes	Art. 21.1.c	L'entité doit assurer la continuité de ses services essentiels via sauvegardes et plans de reprise	Sauvegardes 3-2-1 en place (37)	Conforme	Sauvegardes opérationnelles
Sécurité de la supply chain	Art. 21.1.d	L'entité doit gérer la sécurité des tiers et prestataires, en encadrant leurs accès et obligations de sécurité	Prestataire N1 avec droits élevés sans exigences SSI (3)	Non conforme	Aucun encadrement sécurité des tiers
Gestion des accès	Art. 21.1.f	L'entité doit contrôler l'accès aux systèmes, limiter les droits au strict nécessaire et revoir périodiquement les permissions	Pas de revue des droits, droits admins mal maîtrisés (5,6,9,29)	Non conforme	Accès excessifs non contrôlés
Authentification forte	Art. 21.2	L'entité doit mettre en place une authentification forte sur les accès critiques (MFA)	MFA partiel avec dérogations (13)	Partiel	MFA non généralisé
Sécurité réseau	Art. 21.1.e	L'entité doit segmenter les réseaux, cloisonner les services et protéger les systèmes exposés	Segmentation faible, services exposés sans protection (19,23)	Partiel	Cloisonnement insuffisant
Journalisation & supervision	Art. 21.1.g	L'entité doit activer, configurer et centraliser les journaux, corréler et superviser les événements de sécurité	Logs limités aux AD, pas de corrélation (36)	Partiel	Capacité de détection insuffisante pour répondre aux exigences de détection précoce et de notification NIS 2 (Pas de SIEM, Pas de NTP, Pas de corrélation).Logs uniquement AD.
Sensibilisation & formation	Art. 21.2	L'entité doit former et sensibiliser régulièrement l'ensemble du personnel aux risques cyber et bonnes pratiques	Actions ponctuelles non structurées (2,2R)	Partiel	Absence de programme formalisé

Annexe 3-1 : Échelle de niveau de priorité

Niveau	Description	Critères d'attribution
Très haute (1 / Critique)	Chantiers indispensables pour atteindre la conformité NIS 2 et réduire le risque cyber majeur. Non traités, ils exposent l'entreprise à des sanctions ou à un incident majeur.	- Absence totale d'un processus requis par NIS 2- Impact direct sur les services critiques ou la notification d'incidents- Failles dans la gouvernance ou la gestion des risques
Haute (2 / Importante)	Chantiers nécessaires pour renforcer le contrôle et la sécurité, impact modéré sur la conformité si non traités mais risque significatif sur les accès ou les tiers.	- Contrôles partiels ou insuffisants- Gestion des accès, authentification, sécurité des prestataires- Risques importants mais non immédiats sur la continuité
Moyenne (3 / Recommandée)	Chantiers qui améliorent la robustesse et la résilience, mais dont l'absence n'empêche pas la conformité immédiate.	- Processus partiellement mis en place- Amélioration de supervision, formation ou réseau- Risque limité ou indirect
Faible (4 / Optionnelle)	Chantiers non critiques pour la conformité NIS 2 mais pouvant optimiser la sécurité ou la maturité globale.	- Amélioration marginale- Processus déjà existants mais perfectibles- Aucun impact légal direct

Annexe 3-2 : Tableau des Chantiers majeurs de mise en conformité

Chantier majeur	Éléments du tableau / Audit	Commentaire	Priorité NIS 2	Articles liés
Gouvernance et gestion des risques cyber	41R, 34, 39	Analyse de risques absente, politique SSI partielle, RSSI présent mais gouvernance faible	Très haute	Art. 21.1.a / 21.1
Gestion des incidents de sécurité	40	Pas de procédure, incapacité à détecter et réagir à un incident	Très haute	Art. 21.1.b / 23
Gestion des accès et authentification	5,6,8,9,12,13,29	Pas de revue des droits, comptes admins mal maîtrisés, MFA partiel, absence de journalisation	Haute	Art. 21.1.f & 21.2
Sécurité réseau et cloisonnement	19,21,23	Segmentation limitée, services exposés sans protection frontale (firewall/WAF), absence de revue des flux	Haute	Art. 21.1.e
Supervision et journalisation	36,36R	Logs limités à l'AD, pas de corrélation, pas d'alerting centralisé, pas de SIEM ni NTP	Moyenne	Art. 21.1.g
Sensibilisation & formation	1,2,2R	Programme de sensibilisation partiel, non structuré, absence de suivi ou validation des connaissances	Moyenne	Art. 21.2
Nomadisme et postes de travail	30,30R,32,33,33R	Pas de protection réseau pour les nomades, pas de politique de sécurité dédiée aux terminaux mobiles	Moyenne	Art. 21.1.f / 21.2
Continuité & sauvegardes	37,37R	Sauvegardes 3-2-1 présentes mais sans tests réguliers ni classification des actifs critiques	Moyenne	Art. 21.1.c
Sécurité de la supply chain / infogérance	3	Prestataires non encadrés par des exigences de sécurité, accès privilégiés non contrôlés	Haute	Art. 21.1.d

Annexe 4-1 : tableau de mise en conformité NIS2

Chantier / Action	Observation / Éléments d'audit	Priorité	Durée estimée	Chiffrage approximatif	Articles NIS 2	Explication de l'article	Description précise	Remédiation
Gouvernance et politique SSI	RSSI identifié, politiques partielles (34,39)	Très haute	2-3 mois	15-25k	Art. 21.1	Obligation de mettre en place une gouvernance, responsabilité, pilotage et reporting	Formaliser la gouvernance SSI : politique, responsabilités, comité pilotage, KPI, reporting NIS 2	- Nommer RSSI avec délégation COMEX- Comité pilotage NIS 2 avec PV- Politique SSI validée par la direction- Tableau de suivi des actions NIS 2
Analyse formelle des risques cyber	Analyse de risques jamais réalisée (4 FI)	Très haute	3-4 mois	30-50k	Art. 21.1.a	Obligation d'évaluer et traiter les risques cyber de manière formelle	Cartographier actifs critiques, identifier menaces et vulnérabilités, définir plan de traitement	- Inventaire des actifs critiques- Cartographie des risques avec probabilité x impact- Plan de traitement et priorisation- Intégrer risques supply chain
Gestion des incidents	Aucune procédure, aucun retour d'expérience (40)	Très haute	2-3 mois	10-20k	Art. 21.1.b/ 23	Définir processus de gestion des incidents et notification aux autorités compétentes	Créer procédures d'incidents, workflow interne/externe, tests annuels	- Rédiger procédures écrites- Définir rôles et responsabilités- Workflow notification incidents majeurs- Registre central des incidents et exercices annuels
Gestion des accès et authentification	Pas de revue des droits, comptes admins mal maîtrisés, MFA partiel, absence journalisation (5 FI, 6, 8, 9, 17, 17, 29)	Haute	2-3 mois	15-30k	Art. 21.1.f & 21.2	Obligation de contrôle des accès, séparation des rôles, authentification forte	Revue périodique des droits, séparation des rôles, MFA généralisé, coffre-fort mots de passe, journalisation	- Revue des droits trimestrielle- Séparation comptes utilisateurs/admin- MFA obligatoire pour tous- Coffre-fort administrateurs- Journalisation immuable actions critiques
Supply chain / prestataires	Prestataires NI avec droits élevés non encadrés (3)	Haute	1-2 mois	5-15k	Art. 21.1.d	Obligation de gérer les risques liés aux prestataires	Définir exigences SSI dans contrats, limiter droits selon principe du moindre privilège, suivi et audit prestataires	- Ajouter clauses SSI dans contrats- Limiter droits et privilèges- Audit périodique des prestataires- Intégrer prestataires au plan de reprise et gestion incident
Sécurité réseau et cloisonnement	Segmentation limitée, services exposés sans protection frontale (19,21,23)	Haute	3-4 mois	20-40k	Art. 21.1.e	Obligation de sécuriser les réseaux, segmenter, protéger zones critiques	Segmenter réseau, firewall/WAF, limitation services exposés, revue régulière des flux	- Segmenter réseau par zones critiques- Déployer firewall et WAF- Scanner services exposés et corriger vulnérabilités- Mettre en place IDS/IPS et supervision
Supervision et journalisation	Logs limités à AD, pas de corrélation (36,39FI)	Moyenne	3-4 mois	25-50k	Art. 21.1.g	Obligation de journaliser, auditer et superviser les systèmes	Centraliser logs, corrélation SIEM, alerting, synchronisation NTP	- Déployer SIEM pour tous les composants critiques- Synchroniser horodatage NTP- Définir plan de conservation logs- Alerting et corrélation événements
Sensibilisation & formation	Programme partiel et non structuré (1,2,2FI)	Moyenne	1-2 mois initial puis continu	5-10k/an	Art. 21.2	Obligation de sensibiliser/former utilisateurs et équipes	Définir programme structuré, ciblage par rôle, suivi et validation	- Élaborer programme annuel par rôle- Formation obligatoire- Suivi des validations- Campagnes périodiques et tests phishing
Nomadisme et postes de travail	Pas de protection réseau nomades, pas de politique mobiles (30,30FI,32,33,33FI)	Moyenne	2-3 mois	10-25k	Art. 21.1.f/ 21.2	Obligation de sécuriser terminaux mobiles et nomades	VPN obligatoire, endpoint protection, chiffrement disque, politique terminaux mobiles, règles d'accès	- Installer VPN et endpoint protection- Chiffrement obligatoire- MDM / EMM pour mobiles- Contrôle d'accès réseau pour nomades
Continuité & sauvegardes	Sauvegardes présentes mais sans tests ni classification (37,37FI)	1-2 mois + continu	5-15k	Art. 21.1.c	Obligation de maintenir continuité des services et restauration des données	Maintenir sauvegardes 3-2-1, tests réguliers, classifier actifs critiques, plans de restauration	- Tester restaurations régulièrement- Classifier actifs critiques- Documenter procédures, RPO/RTO par service- Intégrer continuité dans plan sécurité NIS 2
		Total =	(140 K - 288K) euros					

Annexe 5-1 : Evaluation Post Remédiation de conformité NIS2

Exigence NIS 2 – Texte FR provisoire	Articles	Éléments observés (audit)	État actuel	Nouvel état post-remédiation	Justification post-remédiation	Explication article
Politique de gestion des risques cyber	Art. 21.1.a	Analyse de risques jamais réalisée (41R)	Non conforme	Conforme	Analyse formelle réalisée, cartographie des risques, plan de traitement documenté et validé par la direction	Obligation d'évaluer et traiter les risques cyber formellement
Gouvernance SSI	Art. 21.1	RSSI identifié mais peu de politiques formalisées (39,34)	Partiel	Conforme	Politique SSI complète, comité pilotage NIS2, reporting au COMEX et indicateurs KPI en place	Obligation de mettre en place une gouvernance avec responsabilités et pilotage
Gestion des incidents	Art. 21.1.b / 23	Aucune procédure, aucun retour d'expérience (40)	Non conforme	Conforme	Procédures documentées, workflow d'incidents, notification aux autorités, exercices annuels réalisés	Obligation de définir un processus de gestion des incidents et notification
Continuité & sauvegardes	Art. 21.1.c	Sauvegardes 3-2-1 en place (37)	Conforme	Conforme	Plan de sauvegarde testé, classification des actifs critiques, RPO/RTO définis	Obligation de maintenir continuité et restauration des données
Sécurité de la supply chain	Art. 21.1.d	Prestataire N1 avec droits élevés sans exigences SSI (3)	Non conforme	Conforme	Clauses SSI ajoutées dans les contrats, droits limités, audits périodiques prestataires, intégration dans plan reprise	Obligation de gérer les risques liés aux prestataires et tiers
Gestion des accès	Art. 21.1.f	Pas de revue des droits, droits admins mal maîtrisés (5,6,9,29)	Non conforme	Conforme	Revue trimestrielle des droits, séparation comptes utilisateurs/admin, MFA généralisé, journalisation immuable	Obligation de contrôler les accès et séparer les rôles critiques
Authentification forte	Art. 21.2	MFA partiel avec dérogations (13)	Partiel	Conforme	MFA généralisé pour tous les utilisateurs et administrateurs, politique de mots de passe renforcée	Obligation d'utiliser une authentification forte pour tous les accès critiques
Sécurité réseau	Art. 21.1.e	Segmentation faible, services exposés sans protection (19,23)	Partiel	Conforme	Segmentation complète, firewall/WAF, IDS/IPS, revue régulière des flux, protection des services exposés	Obligation de sécuriser les réseaux et protéger les zones critiques
Journalisation & supervision	Art. 21.1.g	Logs limités aux AD, pas de corrélation (36)	Partiel	Conforme	SIEM centralisé, logs de tous composants critiques, corrélation, alerting, horodatage NTP synchronisé	Obligation de journaliser et auditer pour détecter incidents et anomalies
Sensibilisation & formation	Art. 21.2	Actions ponctuelles non structurées (2,29,1)	Partiel	Conforme	Programme annuel structuré par rôle, suivi des validations, tests phishing périodiques	Obligation de sensibiliser et former les utilisateurs régulièrement
Nomadisme & postes de travail	Art. 21.1.f / 21.2	Pas de protection réseau pour nomades, pas de politique mobiles	Partiel	Conforme	VPN et endpoint protection obligatoires, chiffrement disque et communications, MDM pour mobiles, contrôle d'accès réseau	Obligation de sécuriser les terminaux nomades et mobiles
Sécurité des postes de travail	Art. 21.1.f	Niveau minimal non appliqué (14R,15R,16,17R)	Partiel	Conforme	Sécurité minimale appliquée sur tous les postes : antivirus, firewall, GPO documentées, chiffrement, restriction droits admin	Obligation de sécuriser l'ensemble du parc informatique
Gestion des interconnexions et messagerie	Art. 21.1.e	Interconnexions limitées, messagerie partiellement protégée (22,24,25)	Partiel	Conforme	Passerelles sécurisées, authentification utilisateurs, contrôle interconnexions, messagerie filtrée	Obligation de sécuriser les échanges réseau et messageries critiques
Administration SI	Art. 21.1.f / 21.2	Accès aux postes admin non séparés, réseau admin non cloisonné (27,28,29)	Non conforme	Conforme	Réseau d'administration séparé, accès restreint, MFA, journalisation immuable, séparation postes admin et postes utilisateurs	Obligation de sécuriser administration SI et limiter droits admin

Annexe 6-1 : Tableau des délais :

Axe de conformité	Actions principales associées	Priorité	Durée estimée
Gouvernance SSI & pilotage NIS 2	Politique SSI, comité NIS 2, KPI, reporting direction	Haute	2 à 3 mois
Analyse de risques cyber	Cartographie des actifs, analyse des risques, plan de traitement	Haute	2 mois
Gestion des incidents	Procédures, notification, exercices de crise	Haute	1 à 2 mois
Gestion des accès & identités	Revue des droits, MFA généralisé, comptes admins	Haute	3 à 4 mois
Sécurité réseau & services exposés	Segmentation, WAF, revue des flux, scans	Moyenne	3 à 4 mois
Supervision & journalisation	Centralisation des logs, SIEM, alerting	Moyenne	3 mois
Supply chain & prestataires	Clauses SSI, audits, limitation des accès	Moyenne	2 à 3 mois
Nomadisme & postes de travail	VPN, MDM, politiques terminaux	Moyenne	2 mois
Sensibilisation & formation	Programme annuel, campagnes, tests	Basse	1 mois (puis récurrent)
Continuité & sauvegardes	Tests PRA/PCA, RPO/RTO	Basse	1 à 2 mois
		Total =	12 à 18 mois

Annexe 6-2 : Tableaux d'estimation des coûts :

Poste de coût	Description	Coût estimatif
Accompagnement GRC / RSSI	Analyse de risques, gouvernance, procédures, pilotage NIS 2	30 k€ – 50 k€
Solutions IAM / MFA / PAM	MFA généralisé, gestion des comptes à privilèges	20 k€ – 40 k€
Supervision & SIEM	Outil SIEM + intégration + exploitation initiale	40 k€ – 70 k€
Sécurité réseau	WAF, segmentation, audits et scans	20 k€ – 35 k€
Sécurité postes & nomadisme	VPN, MDM, protection endpoints	15 k€ – 25 k€
Supply chain & audits tiers	Audits prestataires, contractualisation SSI	10 k€ – 20 k€
Sensibilisation & formation	Campagnes, supports, simulations phishing	5 k€ – 10 k€
Continuité & PRA	Tests, exercices, accompagnement	5 k€ – 10 k€
	Total =	145 k€ à 260 k€