Annexe 2 — Matrice de criticité NIS2 des actifs IMEV

1. Méthode d'évaluation

Chaque actif est évalué selon quatre critères :

Critère	Description
Disponibilité	Impact d'une indisponibilité
Intégrité	Risque de modification ou corruption
Confidentialité	Sensibilité des informations
Traçabilité	Besoin d'audit et investigation

Notation :

Niveau	Signification
1	Faible
2	Modéré
3	Important
4	Critique

---

2. Matrice de criticité

Actif	Disponibilité	Intégrité	Confidentialité	Criticité globale
Active Directory	4	4	3	Critique
LDAP	4	4	3	Critique

Actif	Disponibilité	Intégrité	Confidentialité	Criticité globale
DNS	4	4	2	Critique
Firewall	4	4	3	Critique
VxRail	4	4	3	Critique
Unity XT	4	4	4	Critique
Veeam	4	4	4	Critique
VPN	3	4	4	Haute
Messagerie	3	3	3	Haute
Nextcloud	3	3	4	Haute
Serveurs scientifiques	3	4	4	Haute
GitLab	2	3	3	Moyenne
Postes utilisateurs	2	3	3	Moyenne

---

3. Priorisation des mesures de sécurité

Niveau critique

Mesures obligatoires :

- sauvegarde régulière ;
- supervision ;
- journalisation ;
- contrôle d’accès renforcé ;
- MFA si applicable ;
- maintien en condition de sécurité ;
- documentation.

Actifs concernés :

- AD ;
- LDAP ;

- DNS ;
- Unity XT ;
- VxRail ;
- Veeam ;
- Firewall.

Niveau haute

Mesures :

- suivi des mises à jour ;
- contrôle des accès ;
- supervision ;
- sauvegarde adaptée.

Actifs concernés :

- VPN ;
- messagerie ;
- Nextcloud ;
- serveurs scientifiques.

Niveau moyenne

Mesures :

- gestion standard ;
- mise à jour régulière ;
- protection poste.

Actifs concernés :

- postes utilisateurs ;
- services secondaires.

---

4. Correspondance avec les exigences NIS2

Exigence NIS2	Réponse IMEV
Gestion des risques	Analyse de criticité des actifs
Sécurité des infrastructures	Architecture réseau segmentée
Gestion des accès	AD / LDAP / MFA
Continuité activité	Sauvegarde Veeam et Acronis + PRA
Gestion incidents	Procédure SSI
Sécurité fournisseurs	Évaluation services externes
Protection données	Classification données
Amélioration continue	Revue annuelle SSI

---

5. Évolution attendue

Cette cartographie doit être maintenue :

- au minimum annuellement ;
- lors de l’arrivée d’un nouveau service critique ;
- lors d’une évolution majeure d’infrastructure ;
- après un incident significatif.

Responsables :

- SIR : mise à jour technique ;
- CSSI : suivi SSI ;
- Direction : validation des risques.

Revision #1
Created 7 August 2026 10:04:53 by Nicolas Champeil
Updated 7 August 2026 10:06:40 by Nicolas Champeil