Annexe 3 — Analyse des risques SSI IMEV

Méthode EBIOS simplifiée

Version : 1.0
Pilote : CSSI IMEV
Contributeurs : SIR, responsables de plateformes, responsables métiers

---

1. Objectifs

L’analyse des risques SSI vise à :

- identifier les risques pesant sur le système d’information de l’IMEV ;
- évaluer leurs impacts potentiels sur les activités scientifiques et administratives ;
- définir les mesures de sécurité adaptées ;
- prioriser les actions en fonction du niveau de risque.

Cette analyse s’inscrit dans une démarche d’amélioration continue et répond aux principes de gestion des risques attendus dans le cadre de NIS2.

---

2. Méthodologie retenue

La méthode retenue est une adaptation simplifiée de la méthode **EBIOS Risk Manager**.

Elle repose sur :

1. Identification des valeurs métiers ;
2. Identification des actifs supports ;
3. Identification des menaces ;

4. Évaluation des impacts ;
5. Définition des mesures de réduction du risque.

---

3. Valeurs métiers critiques IMEV

Valeur métier	Description	Criticité
Activités scientifiques	Recherche marine, observation, expérimentation	Critique
Données scientifiques	Mesures, acquisitions, résultats non publiés	Critique
Plateformes technologiques	Moyens numériques et scientifiques mutualisés	Critique
Services numériques	Messagerie, stockage, authentification	Haute
Données administratives	Gestion établissement	Haute
Communication scientifique	Diffusion des résultats	Moyenne

---

4. Actifs supports critiques

Actif support	Fonction	Criticité
Active Directory	Authentification utilisateurs	Critique
OpenLDAP	Authentification Linux/applications	Critique
DNS	Résolution services	Critique
Pare-feu Palo Alto	Sécurité réseau	Critique
VxRail	Virtualisation	Critique
Dell Unity XT	Stockage centralisé	Critique
Veeam	Sauvegarde/restauration	Critique
VPN GlobalProtect	Accès distant	Haute

Actif support	Fonction	Criticité
Serveurs scientifiques	Applications recherche	Haute
Nextcloud	Collaboration	Haute
Messagerie RENATER	Communication	Haute

---

5. Événements redoutés

ER01 — Indisponibilité du stockage central

Description

Perte d’accès aux données hébergées sur le stockage central.

Impacts

- arrêt de services scientifiques ;
- interruption des utilisateurs ;
- perte de productivité ;
- retard des projets.

Gravité

Critique

ER02 — Compromission d’un compte utilisateur

Description

Utilisation frauduleuse d’un compte légitime.

Impacts

- accès non autorisé aux données ;
- propagation malware ;
- fuite d’informations.

Gravité

Haute

ER03 — Ransomware

Description

Chiffrement des systèmes et données.

Impacts

- arrêt activité ;
- perte disponibilité ;
- restauration longue.

Gravité

Critique

ER04 — Perte d’un service d’identité

Description

Indisponibilité AD/LDAP.

Impacts :

- impossibilité de connexion ;
- arrêt applications ;
- blocage administration.

Gravité :

Critique

ER05 — Fuite de données scientifiques

Description

Divulgation de données avant publication.

Impacts :

- perte d’avantage scientifique ;
- impact réputation ;
- non-respect engagements.

Gravité :

Critique

ER06 — Défaillance matérielle majeure

Description

Panne stockage, serveur ou réseau.

Impacts :

- interruption service ;
- intervention urgente ;
- perte disponibilité.

Gravité :

Haute

---

6. Sources de menace

Menace	Origine possible
Cyberattaque externe	Internet
Phishing	Utilisateurs
Malware/Ransomware	Poste compromis
Erreur humaine	Manipulation utilisateur
Mauvaise configuration	Administration

Menace	Origine possible
Défaillance matériel	Infrastructure
Prestataire compromis	Chaîne fournisseur
Compte privilégié compromis	Administration

---

7. Analyse des risques

Notation :

- Probabilité : 1 à 4
- Impact : 1 à 4

Niveau risque :

Score	Niveau
1-4	Faible
5-8	Modéré
9-12	Important
13-16	Critique

Matrice des risques IMEV

Risque	Probabilité	Impact	Niveau
Ransomware	3	4	Critique
Compromission compte utilisateur	3	3	Important
Panne stockage Unity	2	4	Important
Perte AD/LDAP	2	4	Important
Fuite données scientifiques	2	4	Important
Défaillance serveur critique	2	3	Modéré

Risque	Probabilité	Impact	Niveau
Mauvaise configuration réseau	2	3	Modéré
Compromission fournisseur	2	3	Modéré

---

8. Mesures existantes IMEV

Protection identité

Déjà en place :

- AD
- OpenLDAP
- synchronisation annuaire
- gestion centralisée comptes

À renforcer :

- MFA généralisé ;
- revue droits régulière.

Protection infrastructure

Déjà en place :

- segmentation réseau
- firewall Palo Alto
- virtualisation VxRail
- stockage Unity XT
- sauvegarde Veeam

À renforcer :

- supervision sécurité ;
- analyse logs ;
- durcissement.

Protection données

Déjà en place :

- sauvegarde centralisée
- réplication secondaire
- stockage mutualisé

À renforcer :

- classification données ;
- règles conservation ;
- tests restauration.

9. Plan de traitement des risques

Risque	Action	Priorité
Ransomware	MFA + sensibilisation + sauvegardes immuables	Haute
Compte compromis	MFA + revue droits	Haute
Perte stockage	PRA + tests restauration	Haute
Fuite données	Classification + contrôle accès	Haute
Vulnérabilités	Gestion patchs	Haute
Logs insuffisants	SIEM / centralisation logs	Moyenne
Shadow IT	Processus validation outils	Moyenne

10. Risques résiduels et arbitrages

La réduction totale du risque n’étant pas possible, l’IMEV définit un niveau de risque résiduel acceptable.

Les risques résiduels nécessitant des moyens supplémentaires font l’objet d’un arbitrage de la Direction.

Le SIR assure la mise en œuvre opérationnelle des mesures validées dans la limite des ressources disponibles.

---

11. Gouvernance de suivi

Cette analyse est revue :

- annuellement ;
- lors d’une évolution majeure du SI ;
- après un incident significatif ;
- lors d’un changement réglementaire.

Participants :

- Direction IMEV ;
- CSSI ;
- SIR ;
- responsables métiers concernés.

Conclusion

Cette analyse permet à l’IMEV de disposer d’une vision structurée de ses risques numériques et de prioriser ses actions de sécurité conformément aux principes de NIS2.

Elle constitue également un support d’aide à la décision pour définir les moyens humains, techniques et financiers nécessaires au maintien d’un niveau de sécurité adapté aux missions scientifiques de l’établissement.

Revision #1
Created 2026-08-07 12:10:06 UTC by Nicolas Champeil
Updated 2026-08-07 12:11:43 UTC by Nicolas Champeil