RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

COLLECTION GESTION DES RISQUES CYBER

GUIDE EBIOS RISK MANAGER

FICHE METHODE 9 – Atelier 5

STRUCTURER LES MESURES DE TRAITEMENT DU RISQUE

Les fiches méthodes permettent aux responsables de la démarche d'analyse de risque d'identifier les points essentiels d'attention en fonction de la typologie du système d'information ou des concepts utilisés.

Elles n'ont pas vocation à remplacer les guides techniques de l'ANSSI ou les politiques de sécurité et les réglementations en vigueur qui doivent être appliquées.

Les mesures de traitement du risque peuvent être structurées selon les principes de sécurité en profondeur ci-contre :

GOUVERNANCE ET ANTICIPATION	**Gouvernance** ♦organisation de management du risque et d'amélioration continue ; ♦processus d'homologation ; ♦maîtrise de l'écosystème ; ♦gestion du facteur humain (sensibilisation, entrainement) ; ♦indicateurs de pilotage de la performance numérique. **Connaissance des vulnérabilités** ♦audits de sécurité, veille. **Connaissance de la menace** ♦veille (renseignement, intelligence économique).
PROTECTION	♦Cloisonnement des biens supports par domaines de confiance ; ♦Gestion de l'authentification et du contrôle d'accès ; ♦Gestion de l'administration/supervision ; ♦Gestion des entrées/sorties de données et des supports amovibles. ♦Protection des données (intégrité, confidentialité, gestion des clés cryptographiques) ; ♦Sécurité des passerelles d'interconnexion et des biens supports périmétriques (biens supports « de frontière ») ; ♦Sécurité physique et organisationnelle ; ♦Maintien en condition de sécurité et gestion d'obsolescence ; ♦Sécurité des processus de développement, d'acquisition (chaîne d'approvisionnement) et de maintien en condition opérationnelle ; ♦Sécurité vis-à-vis des signaux parasites compromettants.
DÉFENSE	♦Surveillance d'événements ; ♦Détection et classification d'incidents ; ♦Réponse à un incident cyber.
RÉSILIENCE	♦Continuité d'activité (sauvegarde et restauration, gestion des modes dégradés) ; ♦Reprise d'activité ; ♦Gestion de crise cyber.

L'amélioration de la sécurité d'un système d'information doit être une action menée dès sa conception et jusqu'à son décommissionnement. Toutes ces actions permettent de réduire les risques et doivent être compilées dans un document unique, le plan d'action.[1]

NOTE : Le plan d'action doit être le regroupement des actions permettant de traiter les non-conformités réglementaires, de réduire les risques identifiés (le plan de traitement des risques - PTR), de mitiger les vulnérabilités identifiées lors des audits et de traiter des évènements et incidents de sécurité

Pour être exploitable, il doit recenser des actions réalistes et utiles. La méthode SMART peut être utilisée :

- L'action doit être Spécifique au risque à diminuer ou à la mesure à appliquer ;
- Le résultat de l'action doit être Mesurable ;
- L'objectif de l'action doit être Atteignable et Réaliste ;
- Enfin l'action doit être Temporellement définie. Il est à noter qu'une action peut adresser plusieurs risques.

NOTE : Le plan d'action est la pierre angulaire de l'amélioration continue et doit permettre le renforcement de la sécurité du système d'information

Un propriétaire nommé, une complexité, un délai et une date d'exécution doivent au minima être renseignés. Les coûts associés à la réalisation de l'action peuvent être intégrés au plan.

Nom de l'action	Commentaires	Justification	Propriétaire	Complexité De + à +++	Date fin prévue
Suppression des services réseau non utilisés	Suppression des services telnet et http sur tous les serveurs, postes de travail et équipements réseau – environ 120 équipements	Respect du guide d'hygiène informatique	Responsable DSI : M ou Mme X	+	Février 2026

- Toutes les informations utiles pour le suivi des actions doivent être ajoutées.
- Les actions doivent être priorisées.
- Les actions permettant de traiter les risques ayant le plus grand impact et étant les plus vraisemblables doivent être effectuées en priorité.
- Les actions ayant une marge d'amélioration élevée sur la sécurité du système d'information sont aussi à privilégier

[1] Tous les éléments qui suivent sont issus du Guide sur l'homologation des systèmes d'information, 2025, 55-56.