LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

Politique de gestion des risques liés à la sécurité de l'information

Mai 2025

Table des Matières

1 Introduction

L'objectif de cette politique de gestion des risques de la sécurité de l'information est de définir un cadre global pour identifier, évaluer, et gérer les risques liés à la sécurité de l'information au sein de l'entité. Elle vise à permettre aux entités d'anticiper, de prioriser, et de répondre aux risques de manière proactive et efficace, permettant de protéger les actifs de l'entité et de réduire les impacts sur les opérations.

Cette politique a pour but d'apporter un support à destination des entités en matière de gestion des risques de la sécurité de l'information, en assurant une approche structurée et optimale pour la gestion des risques.

2 Périmètre, limites et exclusions

Cette politique s'applique à l'ensemble des risques de sécurité de l'information identifiés par l''entité, auxquels elle pourrait faire face. Elle couvre les risques liés aux opérations internes de l'entité, mais également les risques externes ou indirects susceptibles d'avoir un impact sur la sécurité des informations de l'entité, notamment les dépendances de l'entité envers les services fournis par un prestataire ou fournisseur externe.

Les exclusions spécifiques à cette politique, si elles existent, sont détaillées dans les sections correspondantes, afin de garantir une compréhension claire des domaines couverts et non couverts par cette politique de gestion des risques.

3 Définitions et terminologie

Actif (ou asset) : Tout élément ayant de la valeur pour l'entité, tel que des données, des informations, des systèmes, des processus, du personnel, des logiciels ou des équipements.

Vulnérabilité : Une faiblesse, susceptibilité ou faille de produits TIC ou de services TIC qui peut être exploitée par une cybermenace.

Menace : Toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes.

Impact : Conséquence d'un risque sur l'entité, en termes, de confidentialité, d'intégrité, et de disponibilité.

Probabilité : Estimation de la fréquence à laquelle une menace ou un incident est susceptible de survenir.

Risques : Le potentiel de perte ou de perturbation causé par un incident, à exprimer comme la combinaison de l'ampleur de cette perte ou de cette perturbation et de la probabilité qu'un tel incident se produise.

Mesure de sécurité : Ensemble des dispositifs techniques, organisationnels et opérationnels, tels que des procédures, ou pratiques permettant de réduire le niveau d'un ou plusieurs risques.

Appétit pour le risque : Seuil à partir duquel l'entité décide d'accepter un risque comme moyen de traitement, considérant qu'il est tolérable par rapport à ses objectifs stratégiques, opérationnels ou financiers, et qu'il ne nécessite pas d'autres actions pour être atténué.

Traitement des risques : Processus de gestion des risques identifiés. Incluant l'acceptation, la réduction, le transfert, le partage, ou la suppression du risque.

KPI : Indicateur de performance clé est une mesure qui permet d'évaluer l'efficacité d'une équipe, d'un projet, d'un processus, etc... dans l'atteinte d'un objectif spécifique.

4 Gestion des risques

4.1 Gouvernance de la gestion des risques

4.1.1 Mesures fondamentales

MF-001 L'entité devrait adopter une méthodologie d'évaluation des risques basée sur des critères de probabilité, d'impact et de niveau de vulnérabilité pour évaluer les risques.

- ISO/IEC 27001 :2022 6.1.2 (e)
- Règlement d'exécution UE 2024/2690 : 1.1.1 (j), 2.1.2 (a, c, e)
- ENISA guideline on security measures under the EECC 4th edition- SO2

MF-002 L'entité devrait définir des rôles et des responsabilités afin de gérer les risques liés à la sécurité des systèmes d'information.

- ISO/IEC 27001 :2022 A.5.2
- Règlement d'exécution UE 2024/2690 : 1.2
- ENISA guideline on security measures under the EECC 4th edition - SO3

MF-003 L'entité devrait s'assurer que les personnes impliquées dans la gestion des risques soient adéquatement formées.

- ISO/IEC 27001 :2022 A 6.3
- Règlement d'exécution UE 2024/2690 : 8.2.2
- ENISA guideline on security measures under the EECC 4th edition– SO6, SO29

MF-004 L'entité devrait mettre en place une structure de gouvernance pour superviser la sécurité de l'information et coordonner les initiatives de gestion des risques.

- ISO/IEC 27001 :2022 A.5.4
- Règlement d'exécution UE 2024/2690 : 2.1
- ENISA guideline on security measures under the EECC 4th edition - SO2

MF-005 Un seuil de tolérance aux risques formalisé devrait être défini pour orienter les décisions sur la gestion des risques acceptables.

- ISO/IEC 27001 :2022 6.1
- Règlement d'exécution UE 2024/2690 : 2.1.2 (b)
- ENISA guideline on security measures under the EECC 4th edition - SO2

4.1.2 Mesures complémentaires

MC-001 L'entité devrait identifier et documenter les menaces internes et externes susceptibles d'affecter son système d'information et ses processus critiques.

- ISO/IEC 27001 :2022 A.5.7
- Règlement d'exécution UE 2024/2690 : 2.1.2, 2.2.2
- ENISA guideline on security measures under the EECC 4th edition – SO2, SO28

MC-002 L'entité devrait définir des indicateurs clés des risques (KRI) pour le degré de risques d'une activité ou d'un process.

- ISO/IEC 27001 :2022 6.1
- Règlement d'exécution UE 2024/2690 : 7.1
- ENISA guideline on security measures under the EECC 4th edition - SO2

4.2 Identification, Évaluation et Classification des Risques

4.2.1 Mesures fondamentales

MF-006 L'entité devrait créer et maintenir un inventaire à jour des actifs (systèmes, données, applications) qu'elle possède lui permettant d'identifier ses actifs essentiels et de supports.

- ISO/IEC 27001 :2022 A.5.9
- Règlement d'exécution UE 2024/2690 12.4.1
- ENISA guideline on security measures under the EECC 4th edition – SO17

MF-007 Les risques devraient être évalués en fonction des échelles et des méthodes validées par l'entité.

- ISO/IEC 27001 :2022 6.1.2
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2 (a,f)
- ENISA guideline on security measures under the EECC 4th edition – SO17

MF-008 L'entité devrait effectuer régulièrement des analyses de risques pour identifier, évaluer et traiter les risques.

- ISO/IEC 27001 :2022 6.1
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2 (d,e), 2.1.4
- ENISA guideline on security measures under the EECC 4th edition – SO2

MF-009 L'entité devrait classer les risques selon leur gravité et leur impact afin de prioriser les actions du plan de traitement.

- ISO/IEC 27001 :2022 6.1.3
- Règlement d'exécution UE 2024/2690 : 2.1.2 (g), 2.1.3
- ENISA guideline on security measures under the EECC 4th edition – SO2

MF-010 Les risques résiduels devraient être approuvés, documentés et justifiés si nécessaire.

- ISO/IEC 27001 :2022 6.1.3 (f), 6.2
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2 (j)
- ENISA guideline on security measures under the EECC 4th edition – SO2

4.2.2 Mesures complémentaires

MC-003 L'entité devrait adapter régulièrement les échelles et critères utilisées pour refléter ses obligations légales, les évolutions technologiques et les nouvelles menaces.

- ISO/IEC 27001 :2022 6.1.2
- Règlement d'exécution UE 2024/2690 : 2.1.1,2.1.2
- ENISA guideline on security measures under the EECC 4th edition – SO2

MC-004 L'entité devrait mettre en place un processus de veille technologique afin d'anticiper toute évolution de la menace et de surveiller les éventuelles vulnérabilités émergeantes.

- ISO/IEC 27001 :2022 6.1.1, 6.2
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2, 6.10.1, 6.10.2
- ENISA guideline on security measures under the EECC 4th edition – SO28

4.3 Traitement des Risques

4.3.1 Mesures fondamentales

MF-011 L'entité devrait définir des options de traitement claires pour gérer les risques identifiés.

- ISO/IEC 27001 :2022 6.1.3
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2 (g)
- ENISA guideline on security measures under the EECC 4th edition - SO2

MF-012 L'entité devrait mettre en place des contrôles de sécurité pour réduire les risques de sécurité identifiés.

- ISO/IEC 27001 :2022 6.1.3
- Règlement d'exécution UE 2024/2690 : 1.1.1 (j), 2.1.2 (g)
- ENISA guideline on security measures under the EECC 4th edition - SO2

MF-013 Les plans de traitement des risques devraient inclure les mesures de traitement des risques choisies, les échéanciers, les priorités et les responsables d'implémentation correspondants.

- ISO/IEC 27001 :2022 6.1.3
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2 (g, i, j)
- ENISA guideline on security measures under the EECC 4th edition - SO2

4.4 Contrôles, revue et communication

4.4.1 Mesures fondamentales

MF-014 Les plans de traitement des risques devraient être régulièrement suivis en fonction des échéances définies pour chaque action de traitement.

- ISO/IEC 27001 :2022 6.1.3
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2 (h)

- ENISA guideline on security measures under the EECC 4th edition - SO2

MF-015 L'entité devrait revoir ses risques de sécurité de l'information régulièrement, ou dès l'apparition d'un évènement ou changement et qui nécessiterait la revue avant la date prévue.

- ISO/IEC 27001 :2022 6.1
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2 (h), 2.1.4, 2.2.3
- ENISA guideline on security measures under the EECC 4th edition - SO2

4.4.2 Mesures complémentaires

MC-004 L'entité devrait mettre en place des moyens de communication afin d'informer le personnel et les membres des organes de la direction vis-à-vis des risques de sécurité et des mesures de mitigation afin de faciliter la compréhension commune des risques, d'assurer la transparence, et de renforcer l'adhésion aux mesures de sécurité.

- ISO/IEC 27001 :2022 7.4
- Règlement d'exécution UE 2024/2690 : 2.1.1, 2.1.2
- ENISA guideline on security measures under the EECC 4th edition - SO2

MC-005 L'entité devrait revoir et améliorer régulièrement le processus d'évaluation des risques, permettant de mettre à jour les facteurs de risque (impact, menaces, vulnérabilités).

- ISO/IEC 27001 :2022 6.1
- Règlement d'exécution UE 2024/2690 : 2.1.2, 2.1.3
- ENISA guideline on security measures under the EECC 4th edition - SO2