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

Agence nationale de la sécurité
des systèmes d'information

Ligne directrice de gestion des risques liés à la sécurité de l'information

Mai 2025

1 Table des Matières

2 Introduction

L'objectif de ce document est de proposer des recommandations d'implémentation concernant la gestion des risques liés à la sécurité de l'information, permettant de mettre en place les mesures de sécurité indiquées dans la politique de sécurité correspondante.

3 Rôles et responsabilités

3.1 Organe de Direction

Les membres de l'organe de Direction sont en charge de l'approbation et de la supervision de la mise en œuvre des mesures de gestion de risques.

3.2 Délégué à la sécurité des systèmes d'informations (DSI)

Chaque entité devrait définir un délégué à la sécurité des systèmes d'informations (DSI) dont les responsabilités incluent, la supervision globale de la sécurité de l'information et de la conformité aux exigences de gestion des risques mais également :

- **Définition et mise à jour de la politique de gestion des risques** : S'assurer que la politique de gestion des risques est pertinente, à jour, et alignée avec les objectifs et les exigences de l'entité, en procédant à un examen périodique ;
- **Surveillance de l'implémentation des mesures de sécurité** : Veiller à ce que les procédures, méthodologies et plans de gestion des risques soient en place et appliqués pour atteindre les objectifs de sécurité ;
- **Supervision des évaluations de risques** : Valider les résultats des évaluations de risques majeures, en particulier pour les actifs critiques de l'entité, et approuver les actions de mitigation nécessaires.

Ces responsabilités viennent compléter celles définies dans la *politique d'organisation de la sécurité de l'information*, en apportant un cadre spécifique pour la gestion des risques de la sécurité de l'information.

3.3 Service informatique

Chaque entité devrait avoir un service informatique (interne ou externe) dont les responsabilités sont :

- **Implémentation des contrôles techniques** : Mettre en œuvre les mesures techniques requises par les plans de traitement des risques validés, en assurant la protection des systèmes, réseaux et applications critiques.
- **Documentation et maintenance des procédures de sécurité** : Développer, documenter et maintenir des procédures opérationnelles de sécurité, en s'assurant qu'elles sont alignées avec le cadre de gestion des risques.

- **Surveillance continue et reporting** : Assurer la surveillance continue des systèmes pour détecter toute vulnérabilité ou activité suspecte et remonter immédiatement les alertes critiques au DSI et au gestionnaire de risques.
- **Collaboration avec le DSI et/ou le gestionnaire de risques** : Fournir les informations techniques nécessaires pour l'évaluation des risques, notamment les configurations des systèmes, les vulnérabilités connues, et les mesures correctives en place.

Ces responsabilités viennent compléter celles définies dans la *politique d'organisation de la sécurité de l'information*, en apportant un cadre spécifique pour la gestion des risques de la sécurité de l'information.

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 maturité pour évaluer les risques.

- ISO/IEC 27001 :2022 6.1.2 (d)
- Règlement d'exécution : 1.1.1 (j), 2.1.2 (a, c, e)
- ENISA guideline on security measures under the EECC 4th edition - s02

	Recommandations
Niveau 1	L'entité devrait définir une méthodologie d'évaluation des risques simple et efficace, incluant les éléments essentiels pour identifier, documenter, et analyser chaque risque. **Création d'une méthodologie** Mettre en place des échelles qualitatives pour évaluer la probabilité (fréquence attendue), l'impact (dommages potentiels) des risques et le niveau de vulnérabilité des contrôles en place. Par exemple : **Probabilité** : Ce critère évalue la fréquence ou la probabilité d'occurrence d'un risque. Une échelle qualitative de 0 à 4 est utilisée, avec les niveaux suivants : ○ **Très faible** – Il est hautement improbable que l'évènement se réalise. ○ **Faible** – Il est improbable que l'évènement se réalise. ○ **Modérée** – Le risque peut survenir dans des circonstances particulières. ○ **Élevée** – Le risque est susceptible de se produire. ○ **Très élevée** – Le risque est quasi certain de se produire. **Impact** : Ce critère estime les conséquences potentielles si le risque se réalise. Une échelle qualitative de 0 à 4 est également utilisée : ○ **Très faible** – La réalisation du risque n'entraîne aucune conséquence. ○ **Faible**– Le risque a peu de conséquences pour l'entité. ○ **Modéré** – Le risque entraîne des conséquences gérables mais notables. ○ **Élevé** – Les conséquences du risque sont significatives pour l'entité. ○ **Très élevé** – Les conséquences sont extrêmement graves et affectent gravement l'entité. **Vulnérabilité** : Ce critère évalue le niveau de faiblesse ou de vulnérabilité des contrôles de sécurité en place face au risque. Une échelle de 0 à 3 est utilisée pour ce critère : ○ **Aucune vulnérabilité** – Les contrôles en place sont parfaitement efficaces. ○ **Vulnérabilité faible** – Les contrôles réduisent efficacement le risque mais avec quelques faiblesses mineures. ○ **Vulnérabilité modérée** – Les contrôles sont présents mais présentent plusieurs lacunes.

	○ **Vulnérabilité élevée** – Les contrôles sont insuffisants ou inexistants, laissant le risque exposé. **Processus d'évaluation** Chaque risque devrait être évalué selon la probabilité, l'impact, et la vulnérabilité. Cela consiste à calculer un score de risque pour quantifier le niveau de menace. Ce score de risque aide à prioriser les actions de gestion en fonction de la gravité des risques. ▪ **Score de Risque :** Le score de risque est obtenu en appliquant la formule suivante : **Risque=Menace × Impact × Vulnérabilité** ▪ Cette formule associe trois éléments fondamentaux pour fournir une estimation objective du risque : ○ **Menace (Probabilité)** : Elle représente la probabilité que le risque se matérialise. ○ **Impact** : Ce critère exprime la gravité des conséquences potentielles. ○ **Vulnérabilité** : Il mesure le niveau de faiblesse ou d'exposition aux menaces en prenant en considération les contrôles existants. Par exemple, un risque ayant une probabilité de 3 (Probable), un impact de 2 (Impact modéré), et une vulnérabilité de 3 (Vulnérabilité élevée) aurait un score de risque calculé comme suit : **Risque=3×2×3=18** Un score de risque élevé indique une menace importante nécessitant des mesures de traitement urgentes, tandis qu'un score bas peut indiquer un risque tolérable ou de moindre priorité. **Remarque** : *Dans le cas d'une analyse de risque NIS2, l'entité devrait s'aider du guide utilisateur MONARC mis à disposition par le HCPN.*
Niveau 2	**Développement de critères détaillés** : Pour évaluer l'impact de manière plus granulaire, l'entité devrait utiliser des sous-critères qui reflètent les conséquences spécifiques qu'un risque peut engendrer. Ces sous-critères sont définis selon l'échelle ROLFP (Réputation, Opérationnel, Légal, Financier, Personnel), ce qui permet une prise en compte complète des impacts potentiels. Chaque risque devrait être évalué en fonction de son impact potentiel sur, a minima, une de ces cinq catégories, avec une évaluation distincte pour chaque sous-critère. **Sous-critères et échelles d'impact** **Réputation (R) :** • **Aucun impact** – Aucun dommage à la réputation de l'entité. • **Faible impact** – Impact mineur sur la réputation, sans influence notable sur l'image publique. • **Impact modéré** – Dommages légers à la réputation, affectant de manière limitée l'image de l'entité auprès de certaines parties prenantes.

- **Impact élevé** – Dégradation significative de l'image de l'entité, pouvant entraîner des réactions négatives dans le secteur.
- **Impact critique** – Dommages graves et durables à la réputation, avec des conséquences sur la confiance des clients et partenaires.

Opérationnel (O) :

- **Aucun impact** – Aucun effet sur les opérations.
- **Faible impact** – Légère perturbation des opérations sans impact notable sur les activités.
- **Impact modéré** – Dysfonctionnement temporaire affectant certaines activités, mais maîtrisable.
- **Impact élevé** – Perturbation importante des opérations, nécessitant des ajustements pour revenir à la normale.
- **Impact critique** – Blocage sévère des opérations, interrompant une partie importante des activités et nécessitant un plan de crise.

Légal (L) :

- **Aucun impact** – Aucun risque légal ou réglementaire.
- **Faible impact** – Infraction mineure aux obligations légales, sans conséquences significatives.
- **Impact modéré** – Violation légale nécessitant une correction mais sans pénalités lourdes.
- **Impact élevé** – Non-conformité importante, avec risque d'amendes ou de sanctions.
- **Impact critique** – Violation grave des lois et réglementations, menant à des poursuites, sanctions majeures ou suspension des activités.

Financier (F) :

- **Aucun impact** – Aucune perte financière.
- **Faible impact** – Coût financier léger et absorbable par le budget courant.
- **Impact modéré** – Perte financière notable, impactant légèrement les budgets prévus.
- **Impact élevé** – Perte financière significative, nécessitant des ajustements budgétaires.
- **Impact critique** – Perte financière grave, compromettant la stabilité économique de l'entité.

Personnel (P) :

- **Aucun impact** – Aucun effet sur la santé, la sécurité, ou le bien-être du personnel.
- **Faible impact** – Impact mineur sur le bien-être ou la motivation des employés.
- **Impact modéré** – Quelques conséquences pour le personnel (ex. : stress accru, perte d'efficacité).
- **Impact élevé** – Conséquences significatives pour le personnel (ex. : perte de confiance, risque pour la santé).
- **Impact critique** – Risques graves pour la sécurité ou la santé, nécessitant une prise en charge immédiate.

Niveau 3	Il n'y a pas de recommandation supplémentaire.

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 - s03

	Recommandations
Niveau 1	L'entité devrait envisager de mettre en place une structure de gouvernance de la sécurité, en attribuant des rôles et responsabilités pour la gestion des risques. En particulier, l'entité devrait envisager de désigner un **Délégué à la Sécurité de l'Information (DSI)** ou un gestionnaire de risques pour superviser la mise en œuvre des mesures de sécurité, coordonner les efforts de gestion des risques, et s'assurer de l'application des contrôles.
Niveau 2	L'entité devrait renforcer la structure de gouvernance en mettant en place le rôle de **Gestionnaire de Risque**, pour coordonner l'identification, l'évaluation et le suivi des risques, en lien avec le DSI et les responsables d'actifs. L'entité devrait également attribuer la responsabilité des actifs critiques (données, systèmes, réseaux, applications) à des membres clés, les **Responsables d'Actifs**. Ces derniers devront gérer, en plus des responsabilités propres à leurs rôles, décrit dans la ***politique de gestion des actifs***, les risques associés à leurs actifs et veiller à ce que des mesures de sécurité adéquates soient appliquées.
Niveau 3	L'entité devrait renforcer davantage sa gouvernance de la sécurité de l'information en veillant à ce que le Délégué à la Sécurité de l'Information (DSI) et/ou le Gestionnaire de Risque ne soient pas rattachés à la même direction que le service informatique, afin de garantir leur indépendance fonctionnelle et éviter les conflits d'intérêts dans la gestion des risques. L'entité devrait également désigner un auditeur interne pour revoir la gestion des risques liés à la sécurité de l'information. L'objectif est d'évaluer l'efficacité des dispositifs en place, de vérifier l'application des mesures de sécurité, et de recommander des actions correctives le cas échéant.

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 - s06– s029

	Recommandations
Niveau 1	L'entité devrait s'assurer que les personnes impliquées dans la gestion des risques soient adéquatement formées afin de disposer des connaissances et des compétences suffisantes pour déterminer les risques et évaluer les pratiques de gestion des risques en matière de cybersécurité et leur impact sur les services fournis par l'entité. Elle devrait également encourager l'utilisation des ressources de formation aux outils de la gestion des risques. **Formation** • Les agents concernés (par exemple, le DSI et/ou gestionnaire des risques ou le gestionnaire projet) devraient suivre les sessions de formation organisées par l'INAP, l'Institut Luxembourgeois de Régulation (ILR) et le Luxembourg House of Cybersecurity (LHC), pour se familiariser avec les fonctionnalités de la plateforme de gestion des risques de l'ILR (SERIMA/MONARC). Ces sessions sont adaptées aux utilisateurs débutants et fournissent une introduction aux fonctionnalités clés ; • L'entité devrait également promouvoir l'accès aux **ressources mises à disposition par le LHC** sur les sessions de formation passées et le lien vers les formations à venir. Ces ressources offrent une base de connaissances importantes pour les utilisateurs de la plateforme de gestion des risques de l'ILR. **Matériel de référence et guide d'utilisation** • L'entité devrait encourager le personnel concerné (par exemple, le DSI et/ou gestionnaire des risques ou le gestionnaire projet) à consulter le **guide d'utilisation de la plateforme de gestion des risques de l'ILR**, qui est mis à disposition en ligne. Ce guide fournit des explications détaillées sur l'utilisation de la plateforme et permet une meilleure appropriation des fonctionnalités ; • Il pourrait être utile de partager le lien du guide : User Guide (SERIMA.lu) ; • Dans le cas d'une analyse de risque NIS2, l'entité devrait également s'aider du guide utilisateur MONARC mis à disposition par le HCPN.
Niveau 2	L'entité devrait mettre en place des formations spécifiques pour former le personnel impliqué dans la gestion des risques. **Programme de formation** : L'entité devrait organiser des sessions de formation qui couvrent les concepts fondamentaux de la gestion des risques (définitions de probabilité, impact, vulnérabilité, etc.), les objectifs de la gestion des risques, les rôles de chaque

	acteur impliqué et les processus de base (ex. : identification des risques, documentation des risques, utilisation des échelles de probabilité, d'impact, etc...). **Formation sur les rôles et responsabilités** : Former spécifiquement les Responsables des Actifs, les DSI ou les Gestionnaires de risques (si applicable) à leurs rôles dans le processus de gestion des risques, incluant la documentation des risques.
Niveau 3	**Évaluation de la Compréhension des Notions** : La compréhension des notions clés devraient être évaluée (p.ex. questionnaire), en identifiant les besoins éventuels de formation supplémentaire.

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 - s02

	Recommandations
Niveau 1	L'entité devrait mettre en place une structure de gouvernance pour assurer une supervision et une coordination des initiatives de sécurité de l'information et de gestion des risques, incluant des réunions périodiques (trimestriellement par exemple) pour faire le point sur les risques identifiés, les initiatives de sécurité en cours, et les besoins d'ajustements. Il est recommandé de documenter toutes les décisions prises dans le cadre de ces réunions, cela inclut par exemple les initiatives validées, et les ajustements nécessaires. Ces décisions pourraient être partagées avec les parties prenantes clés pour garantir une compréhension commune des priorités de sécurité.
Niveau 2	L'entité devrait former un **comité de sécurité de l'information**, qui est décrit dans la politique de gestion de l'organisation de la sécurité de l'information. L'entité devrait également envisager de mettre en place un **registre de suivi des actions** décidées lors des réunions de gouvernance, pour assurer une traçabilité et un suivi dans les temps.
Niveau 3	Il n'y a pas de recommandation supplémentaire.

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 6.1.1
- Règlement d'exécution UE 2024/2690 : 2.1.2 (b)
- ENISA guideline on security measures under the EECC 4th edition - s02

	Recommandations
Niveau 1	L'entité devrait mettre en place un seuil de tolérance aux risques, en se concentrant sur une définition claire et simple du niveau de risque acceptable, ainsi que sur la formalisation de ce seuil. Identification des risques acceptables : définir ce qui constitue un risque acceptable pour l'entité en fonction de sa mission, ses objectifs, et ses obligations réglementaires. Par exemple, un risque avec un impact faible et une probabilité réduite pourrait être jugé comme acceptable.
Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	L'entité devrait mettre en place des critères spécifiques de tolérance aux risques dans les domaines clés (opérationnel, financier, légal), en utilisant des échelles qualitatives simples (faible, moyen, élevé) pour évaluer l'acceptabilité des risques. **Détermination de la tolérance aux risques par domaine clé** 1. **Domaine Opérationnel** : • **Objectif** : Minimiser les interruptions des opérations et assurer la continuité des activités. • **Définition de la Tolérance au Risque** : Évaluer la tolérance de l'entité face aux interruptions potentielles dans les processus opérationnels critiques. • **Seuils de Tolérance** : • **Faible** : Risques entraînant des interruptions minimes, avec des impacts gérables, par exemple, une perturbation de quelques minutes à une heure pour un système non critique. • **Moyen** : Risques avec des interruptions plus significatives, telles que des arrêts temporaires d'opérations critiques, par exemple, un arrêt d'une demi-journée de production pour maintenance. • **Élevé** : Risques susceptibles de provoquer des interruptions graves ou prolongées des opérations (plusieurs jours) ou de toucher directement les services aux clients, ce qui est au-delà du seuil de tolérance de l'entité. • **Exemples de Tolérance** : Un risque opérationnel est jugé acceptable s'il ne perturbe pas les services de base au-delà de X heures/jours ou ne

nécessite pas de ressources supplémentaires importantes pour être résolu.

2. **Domaine Financier** :
    - **Objectif** : Limiter les pertes financières liées aux risques et respecter les budgets prévus.
    - **Définition de la Tolérance au Risque** : Fixer une limite pour les pertes financières acceptables sans compromettre les finances de l'entité.
    - **Seuils de Tolérance** :
        - **Faible** : Pertes financières minimes absorbables dans le budget courant, par exemple, moins de 1 % du budget annuel.
        - **Moyen** : Pertes significatives mais gérables, pouvant affecter le budget d'un département, par exemple, entre 1 % et 5 % du budget annuel.
        - **Élevé** : Pertes majeures nécessitant une intervention de la direction pour éviter un impact financier à long terme, dépassant 5 % du budget annuel.
    - **Exemples de Tolérance** : Un risque financier est considéré acceptable s'il ne génère pas de pertes dépassant un seuil de X % du budget ou ne compromet pas la capacité de l'entité à atteindre ses objectifs financiers.
3. **Domaine Légal** :
    - **Objectif** : Assurer la conformité avec les réglementations et éviter les sanctions légales.
    - **Définition de la Tolérance au Risque** : Identifier les risques légaux pouvant être tolérés sans entraîner de violation réglementaire grave.
    - **Seuils de Tolérance** :
        - **Faible** : Risques de non-conformité mineure, n'entraînant pas de sanctions ni de signalement obligatoire, par exemple, une documentation incomplète.
        - **Moyen** : Risques de non-conformité modérée, pouvant nécessiter des actions correctives mais sans amende significative.
        - **Élevé** : Risques de non-conformité grave pouvant entraîner des amendes importantes.
    - **Exemples de Tolérance** : Un risque légal est jugé acceptable s'il est conforme aux obligations réglementaires de l'entité ou s'il peut être corrigé sans entraîner de sanction.

	Documentation des critères de tolérance : l'entité devrait formaliser et communiquer les critères de tolérance aux risques. 1. **Formalisation de la Tolérance au Risque** : • Ce document devrait inclure des seuils définis pour chaque domaine (opérationnel, financier, légal), et préciser les actions attendues pour chaque niveau de risque. Ce document devrait être utilisé comme référence pour toutes les équipes impliquées dans la gestion des risques. 2. **Suivi et Ajustements** : • L'entité devrait mettre en place un suivi régulier pour évaluer si les critères de tolérance sont toujours en adéquation avec ses objectifs et selon l'évolution du contexte réglementaire.

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 - s02, s028

	Recommandations
Niveau 1	L'entité devrait utiliser les menaces fournis par la plateforme de gestion de risques de l'ILR, qui propose un cadre préétabli et adapté au contexte luxembourgeois. Ces ressources peuvent faciliter l'identification des menaces internes et externes susceptibles d'affecter les systèmes d'information.
Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	L'entité devrait affiner l'identification des menaces en incluant des menaces spécifiques à son secteur d'activité, telles que les cyberattaques ciblées ou les menaces liées à la chaîne d'approvisionnement. L'entité pourrait procéder, après chaque incident majeur, à un examen postincident pour enrichir la compréhension des menaces réelles. L'entité devrait alors documenter chaque menace identifiée dans une fiche de suivi ou un registre simple, en incluant : • Une description de la menace. • La source de la menace (interne/externe). • Les actifs ou processus critiques susceptibles d'être impactés. Ce registre des menaces devrait être revu et mis à jour une fois par an pour prendre en compte les nouvelles informations et évolutions dans l'environnement de risque.

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 - s02

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	**Identification et définition des KRI :** L'entité devrait identifier des KRI adaptés aux activités et processus critiques en tenant compte des menaces et vulnérabilités les plus pertinentes pour ses opérations. Ces KRI pourraient inclure, par exemple : • **Fréquence des incidents de sécurité** pour un processus donné. • **Taux d'erreurs humaines** dans les opérations sensibles. • **Vitesse de détection des incidents** de sécurité. • **Taux de traitement des vulnérabilités et taux de systèmes non patchés.** Chaque KRI devrait être défini de manière précise pour qu'il reflète un aspect mesurable du risque lié aux activités de l'entité. **Documentation des indicateurs et seuils de tolérance :** L'entité devrait documenter chaque KRI dans un registre ou tableau, incluant : • Une description de l'indicateur. • Les seuils de tolérance définis (ex. : acceptable, modéré, critique). • La fréquence de mesure et les unités utilisées (ex. : incidents par mois). • Le propriétaire du KRI. • Le lien avec un risque identifié dans la cartographie. Ces seuils de tolérance permettent de déterminer les niveaux d'alerte et de savoir à quel moment il est nécessaire d'intervenir. **Mise en place de seuils d'alertes et processus d'escalade :** Des seuils d'alertes devraient être définis pour chaque KRI. Lorsque ces seuils sont dépassés, une procédure d'escalade pourrait être déclenchée, pour alerter les responsables concernés et décider des actions à entreprendre. L'entité pourrait documenter ces seuils et procédures d'escalade dans un manuel de gestion des risques afin de standardiser les réponses et actions selon chaque niveau d'alerte. **Suivi régulier et reporting des KRI :** Il est recommandé que l'entité mette en place un suivi régulier de ses KRI, en produisant des rapports trimestriels. Ces rapports pourraient inclure : • Une analyse des tendances pour chaque indicateur.

	• Les dépassements de seuil et les mesures correctives appliquées. Ces rapports de suivi devraient être transmis à la direction et aux parties prenantes clés pour une visibilité constante sur le niveau de risque actuel.

4.2 Identification, Évaluation et Classification des Risques

4.2.1 Mesures fondamentales

MF-006 L'entité devrait 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 - s017

	Recommandations

Niveau 1	L'entité devrait établir un inventaire simplifié, en se concentrant sur l'identification des actifs essentiels et de support pour ses activités.
	
	Recensement des actifs essentiels et de support
	
	• L'entité devrait identifier les actifs essentiels (ceux qui sont critiques pour les opérations de l'entité) ainsi que les actifs de support (ceux qui soutiennent les actifs essentiels).
	
	• Les actifs essentiels à inclure peuvent couvrir :
	  ○ Un **service métier.**
	  ○ Un **processus critique** pour l'entité.
	
	• Les actifs de support à inclure peuvent couvrir :
	  ○ Les **systèmes** critiques (serveurs, équipements réseau).
	  ○ Les **applications** essentielles pour les opérations.
	
	• Un tableau ou registre simple pourrait être utilisé pour consigner ces actifs, en spécifiant le nom, la catégorie (hardware, software, organisation, personnal, site, outsourced service, network) et une description de l'actif.
	
	Remarques : *Dans le cas d'une analyse de risque NIS2, l'entité devrait effectuer une correspondance entre son tableau ou registre d'actifs et la bibliothèque d'actifs proposée par l'ILR à travers le modèle fourni sur la plateforme de gestion des risques. L'entité devrait, pour ce faire, s'aider du guide utilisateur MONARC.*

Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	Il n'y a pas de recommandation supplémentaire.

MF-007 Les risques devraient être évalués en fonction des échelles et des méthodes validés 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 - s02

	Recommandations
Niveau 1	L'entité devrait s'assurer que les échelles et méthodes validées sont appliquées de manière systématique dans tous les processus d'évaluation des risques, incluant les évaluations de risque projet, systèmes d'information et réglementaire. L'entité devrait veiller à ce que les échelles validées (par exemple, pour la probabilité, l'impact, et la vulnérabilité) soient utilisées de manière systématique dans toutes les évaluations de risques.
Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	Il n'y a pas de recommandation supplémentaire.

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 - s02

	Recommandations
Niveau 1	L'entité devrait établir une pratique régulière d'analyses de risques, en s'assurant de respecter l'obligation minimale d'une analyse annuelle dans le cadre de ses activités ou des services qu'elle fournit. **Planification des analyses de risques :** l'entité devrait réaliser, au minimum, une **analyse annuelle des risques** dans le cadre de ses activités ou des services qu'elle fournit. Cette analyse couvre les systèmes, processus et actifs critiques pour l'entité, en garantissant que les risques majeurs sont identifiés et documentés.
Niveau 2	L'entité devrait renforcer ses pratiques d'analyse de risques en intégrant des évaluations de risques projet pour tout nouveau projet. **Évaluation des risques pour chaque nouveau projet** • L'entité devrait systématiquement déterminer si une **analyse de risques spécifique pour un nouveau projet devrait être réalisé**. Cette évaluation couvrirait les risques propres au projet, en tenant compte des impacts potentiels sur la sécurité, la conformité et la continuité des activités. • Il est conseillé de procéder à cette analyse dès le lancement du projet et de la mettre à jour aux différentes étapes du projet. Cela permettrait d'anticiper les risques et de mettre en place des mesures de prévention dès le début du projet. **Fréquence accrue des analyses** • En plus de l'analyse annuelle obligatoire, il est recommandé que l'entité effectue des analyses additionnelles en cas de changements majeurs dans l'infrastructure ou les processus (ex. : ajout d'un nouveau système critique).
Niveau 3	L'entité devrait adopter une approche dynamique et réactive en matière de gestion des risques, en intégrant des réévaluations ponctuelles à la suite d'événements significatifs. Il est conseillé à l'entité de procéder à une réévaluation des risques lorsqu'un événement significatif survient, tel qu'un incident de sécurité majeur, la découverte d'une vulnérabilité critique ou les résultats d'un audit révélant des faiblesses importantes non connues.

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 A.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 - s02

Recommandations

Niveau 1

L'entité devrait s'assurer que chaque risque est classé selon une matrice de classification des risques, en utilisant des critères simples pour établir les priorités.

Application de la matrice de classification des risques

- L'entité devrait appliquer la matrice de classification fournie, qui repose sur le calcul de l'**Indice de vraisemblance** (Probabilité x Vulnérabilité) en abscisse et de l'**Impact** en ordonnée, pour chaque risque identifié.
- La matrice classe les risques en quatre niveaux (Faible, Modéré, Élevé, Critique), facilitant la priorisation des actions selon le niveau de gravité :
  - **Faible** : Risque avec un suivi minimal. (De 0 à 4)
  - **Modéré** : Risque nécessitant une surveillance régulière. (De 5 à 15)
  - **Élevé** : Risque nécessitant des actions de traitement prioritaires. (De 16 à 25)
  - **Critique** : Risque nécessitant une attention immédiate. (De 25 à 48)

Exemple en se basant sur les échelles proposées en **MF-001** :

Impact \ Indice de vraisemblance	0 à 1	2 à 4	5 à 8	9 à 12
0 - Aucun impact	0	0	0	0
1 - Faible impact	0 à 1	2 à 4	5 à 8	9 à 12
2 - Impact modéré	0 à 2	4 à 8	10 à 16	18 à 24
3 - Impact élevé	0 à 3	6 à 12	15 à 24	27 à 36
4 - Impact critique	0 à 4	8 à 16	20 à 32	36 à 48

Remarque : *Dans le cas d'une analyse de risque NIS2, l'entité devrait se conformer aux échelles proposées par l'ILR à travers le modèle fourni sur la plateforme de gestion des risques. Ce modèle se basant sur une échelle à 3 niveaux (Low, Medium, High), l'entité devrait faire correspondre les échelles tel que :*

- **Faible** équivaudrait à **Low**
- **Modéré** équivaudrait à **Medium**
- **Elevé** et **Critique** équivaudraient à **High**

Niveau 2

Il n'y a pas de recommandation supplémentaire.

Niveau 3

Il n'y a pas de recommandation supplémentaire.

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 - s02

	Recommandations

Niveau 1	L'entité devrait s'assurer que tous les risques résiduels identifiés sont approuvés par les parties prenantes et documentés de manière appropriée.
	
	Rappel : *Un **risque résiduel** est le risque qui subsiste après la mise en œuvre des mesures de traitement ou de contrôle pour réduire, transférer, supprimer ou accepter le risque initial. En d'autres termes, il s'agit du niveau de risque restant que l'entité est prête à tolérer, après avoir appliqué les actions de traitement.*
	
	Approbation formelle des risques résiduels
	
	• L'entité devrait s'assurer que chaque risque résiduel identifié après la mise en place des mesures de traitement est approuvé de manière formelle par le DSI, le responsable métier ou la direction.
	
	• Cette approbation devrait être formalisée et archivée.
	
	Documentation des risques résiduels
	
	• Les risques résiduels devraient être documentés dans un registre des risques résiduels, en précisant :
	  ○ La nature du risque résiduel.
	  ○ Les mesures de traitement appliquées ou existante.
	  ○ Le niveau de risque résiduel (Faible, Modéré, Élevé, Critique).
	• Cette documentation devrait être centralisée pour faciliter la traçabilité et permettre une consultation future par les parties prenantes.

Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	Il n'y a pas de recommandation supplémentaire.

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 - so02

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	Il n'y a pas de recommandation applicable.
Niveau 3	**Évolution des vulnérabilités** L'entité devrait planifier des revues périodiques, au minimum annuelles, des échelles de probabilité, d'impact, et de vulnérabilité pour s'assurer qu'elles demeurent pertinentes. Cette revue pourrait inclure : • Une évaluation des nouvelles menaces émergentes (ex. : cybermenaces, avancées en intelligence artificielle). • Une analyse des changements technologiques et de leurs impacts potentiels sur les actifs. **Exemple** : Un nouvel actif technologique introduit au sein de l'entité, comme une infrastructure cloud, pourrait nécessiter l'ajustement des critères d'impact pour prendre en compte des risques spécifiques au cloud (ex. : risques de violation de données, accès non autorisé). **Évolution des menaces** L'entité devrait également tenir compte de la fréquence d'apparition des nouvelles menaces dans le secteur. • **Impact** : Réévaluer les conséquences potentielles de chaque risque pour l'entité, notamment en intégrant des impacts financiers, opérationnels et réglementaires nouveaux. • **Vulnérabilité** : Modifier les critères de vulnérabilité en fonction des nouveaux contrôles technologiques ou des faiblesses identifiées. **Exemple** : Si une menace spécifique (ex. : ransomware) devient plus courante, augmenter le niveau de probabilité associé aux risques de ransomware dans l'échelle. De même, si des mesures de protection avancées (ex. : chiffrement des données) sont introduites, le niveau de vulnérabilité pourrait être ajusté à la baisse pour certains actifs.

MC-004 L'entité devrait mettre en place un processus de veille technologique afin d'anticiper toute évolution de la menace et 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

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	L'entité devrait identifier des sources de veille fiables et pertinentes pour recueillir des informations sur les menaces, les vulnérabilités et les technologies émergentes. • **Sources gouvernementales** : HCPN/GOVCERT, CERT.lu (Centre de réponse aux incidents de sécurité informatique), ENISA (Agence de l'Union européenne pour la cybersécurité), ANSSI (Agence nationale de la sécurité des systèmes d'information). • **Sources sectorielles** : Groupes d'échange entre RSSI et DSI du secteur, publications de sécurité spécifiques (ex. : ISACA, SANS). • **Outils de veille automatisée** : Utiliser des plateformes de renseignement sur les menaces (Threat Intelligence) telles que MISP (Malware Information Sharing Platform) ou des flux d'information sur les vulnérabilités comme CVE (Common Vulnerabilities and Exposures).
Niveau 3	**Mise en place d'un processus de surveillance régulier :** L'entité devrait établir un calendrier de surveillance pour effectuer une veille régulière, idéalement de manière hebdomadaire, afin de rester à jour sur les nouvelles menaces et vulnérabilités en lien avec les actifs de son système d'information. • **Exemple** : Une équipe de sécurité pourrait consulter les alertes CERT et les flux de CVE chaque semaine pour identifier les vulnérabilités affectant les systèmes de l'entité. Si une vulnérabilité critique est identifiée dans un logiciel utilisé par l'entité, une alerte peut être émise pour analyser son impact. **Analyse et priorisation des informations recueillies :** Une fois les informations collectées, l'entité devrait analyser leur pertinence et prioriser les menaces et vulnérabilités en fonction de leur impact potentiel. **Exemple** : Pour une nouvelle vulnérabilité critique, évaluer le niveau de vulnérabilité de l'entité face à cette menace. **Mise en place d'alerte et communication interne :** L'entité devrait mettre en place un système d'alerte interne pour informer les équipes concernées en cas de découverte de vulnérabilités critiques ou de menaces importantes. • **Exemple** : Créer un canal de communication dédié (par exemple, via Teams, Slack ou un outil de ticketing) où les nouvelles vulnérabilités et menaces sont

	communiquées aux responsables et aux administrateurs pour qu'ils puissent réagir rapidement.

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 - s02

	Recommandations
Niveau 1	**Définition des options de traitement des risques** L'entité devrait définir quatre options principales de traitement pour chaque risque identifié : • **Supprimer** : Éliminer le risque en modifiant ou en cessant l'activité qui crée le risque. • **Réduire** : Réduire la probabilité ou l'impact du risque en appliquant des mesures de contrôle ou des contrôles de sécurité. • **Transférer** : Déléguer la responsabilité du risque à une autre partie (ex. : contrat d'assurance, sous-traitance). Il est important de noter que la délégation du risque ne supprime pas la responsabilité globale de l'entité ni ses obligations légales concernant le risque. • **Accepter** : Accepter le risque en prenant notamment en considération sa probabilité, son impact, le coût de traitement par rapport aux bénéfices potentiels. **Exemple** : Pour un risque lié à une attaque par phishing, l'entité pourrait décider de l'atténuer en renforçant la sensibilisation des employés et en appliquant des règles de filtrage au niveau de la messagerie, ou de le transférer en souscrivant une assurance cyber. **Élaboration de critères pour choisir l'option de traitement :** L'entité devrait établir des critères clairs pour sélectionner l'option de traitement la plus appropriée en fonction du niveau de risque, de la criticité des actifs affectés, des coûts de traitement et de la tolérance au risque de l'entité. **Supprimer le Risque** • **Critères** : L'activité ou le processus générant le risque est **non essentiel** ou **peut être modifié** ou **arrêté** sans affecter significativement les opérations.

Exemple : Une entité décide d'éviter l'utilisation de certaines technologies non sécurisées (ex. : une application de messagerie non conforme aux normes de sécurité) en les remplaçant par des alternatives sécurisées pour éliminer le risque d'interception des communications.

Réduire le Risque

- **Critères** :
    - Le risque présente un niveau de **probabilité et d'impact modéré à élevé,** et reste sous les seuils de tolérance de l'entité après réduction.
    - Le coût et les efforts pour réduire le risque sont **raisonnables** par rapport à l'importance du risque et aux gains potentiels.
    - L'entité dispose de **contrôles de sécurité** ou de **mesures d'atténuation viables** (ex. : mise en place de contrôles techniques ou organisationnels pour réduire le risque).
    - La réduction du risque est jugée **suffisante** pour ramener le risque résiduel dans les niveaux acceptables de l'entité.

Exemple : Pour atténuer le risque de perte de données sensibles, l'entité met en place des solutions de chiffrement et des contrôles d'accès stricts, réduisant la probabilité de fuites de données.

Transférer le Risque

- **Critères** :
    - Le risque présente un niveau d'impact potentiellement **élevé** ou **critique,** mais l'entité n'a pas de contrôle direct ou complet sur le risque (ex. : risque de responsabilité juridique ou financière, actif géré par un fournisseur).
    - Des solutions de transfert existent, telles que des **assurances** (assurance cyber, responsabilité civile professionnelle) ou des contrats **de sous-traitance** (en cas de risque lié aux prestataires).

Exemple : L'entité identifie un risque de compromission des données sur les laptops utilisés par ses employés. Cependant, ces laptops sont gérés par le CTIE, qui est responsable de la maintenance, des mises à jour de sécurité et des contrôles de sécurité (comme le chiffrement des données et l'installation d'antivirus). Pour gérer ce risque, l'entité décide de transférer le risque au CTIE.

Accepter le Risque

- **Critères** :
    - Le risque présente un **niveau faible,** et le coût ou les efforts nécessaires pour le réduire seraient disproportionnés par rapport aux impacts potentiels.

	○ Le risque résiduel est jugé acceptable et dans les niveaux **de tolérance** définis par l'entité. ○ Les impacts possibles peuvent être absorbés par l'entité sans compromettre ses opérations ou sa sécurité. **Exemple** : L'entité décide d'accepter un risque faible de dégradation des performances d'un système non critique, estimant que l'impact sur les opérations est négligeable et que les coûts pour améliorer les performances ne sont pas justifiés.
Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	Il n'y a pas de recommandation supplémentaire.

MF-012 L'entité devrait mettre en place des contrôles de sécurité adaptés 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 - s02

	Recommandations
Niveau 1	L'entité devrait réduire efficacement les risques de sécurité identifiés en déployant des contrôles adaptés, couvrant les aspects techniques, gouvernance, physiques, organisationnels et juridiques. Exemple : **Contrôles Techniques :** Appliquer des contrôles techniques pour sécuriser les systèmes et les données. Tels que : • **Chiffrement des données** pour assurer la confidentialité. • **Authentification multifactorielle (MFA)** pour renforcer les accès aux systèmes. • **Pare-feu et IDS/IPS** pour détecter et bloquer les menaces en temps réel. **Contrôles Gouvernance :** Développer des politiques et procédures pour formaliser les pratiques de sécurité et sensibiliser le personnel. Tels que : • **Politique Générale de Sécurité de l'Information (PGSI)** pour définir les grandes orientations stratégiques en matière de sécurité des systèmes d'information et fournir un cadre de référence pour la mise en œuvre des mesures de sécurité. • **Charte de bonne conduite en matière de sécurité de l'information numérique** pour encadrer les comportements des utilisateurs dans l'utilisation des ressources numériques. • **Processus de gestion des changements** pour assurer la continuité des mesures de sécurité en cas de modification technologique.

	Contrôles Physiques : Sécuriser physiquement les installations et les équipements. Tels que : • **Contrôle d'accès physique** par badges et biométrie pour les zones sensibles. • **Surveillance vidéo (CCTV)** pour surveiller les installations. • **Systèmes de détection d'incendie et d'inondation** pour protéger les équipements. **Contrôles Organisationnels :** Mettre en place des structures de gouvernance et des processus pour coordonner la gestion des risques et garantir la conformité. Tels que : • **Désignation de rôles organisationnels** tels que gestionnaire des risques ; • **Comité de sécurité de l'information** pour assurer la conformité ainsi que l'efficacité des mesures de protection ; • **Réunions périodiques de revue des risques** pour suivre l'évolution des risques et l'efficacité des contrôles en place. **Contrôles Juridiques :** Mettre en place des contrôles juridiques pour assurer la conformité légale et réglementaire, gérer les risques liés aux responsabilités juridiques et protéger les droits de l'entité. Tels que : • **Clauses de sécurité dans les contrats de sous-traitance** : Insérer, si nécessaire, des clauses de responsabilité spécifiques pour garantir que les prestataires appliquent des mesures de sécurité conformes aux normes de l'entité. Exiger, par exemple, que le prestataire informe l'entité en cas de faille de sécurité. • **Accords de non-divulgation (NDA)** : Imposer des NDA pour protéger les informations confidentielles échangées avec les employés, les prestataires et les partenaires commerciaux.
Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	Il n'y a pas de recommandation supplémentaire.

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

- 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 - s02

	Recommandations
Niveau 1	L'entité devrait garantir une exécution efficace et un suivi des actions de réduction des risques à travers un ou des plans de traitement des risques, incluant des échéanciers précis, des priorités pour chaque action et des responsables d'implémentation. Cela

	assure que chaque mesure de traitement est planifiée, attribuée, et réalisée dans les délais prévus, tout en facilitant la coordination et la responsabilisation des parties impliquées. **Définition des échéanciers pour les actions essentielles :** L'entité devrait définir un échéancier pour chaque action de traitement, en précisant une date de début et de fin. • **Exemple** : Pour une action visant à mettre en œuvre des contrôles d'accès, définir une date de début pour la configuration initiale et une date de fin pour la validation complète du contrôle. **Priorisation des risques résiduels critiques :** L'entité devrait classer les risques en fonction de leur niveau de criticité (par exemple, Faible, Modéré, Élevé, Critique) pour s'assurer que les actions les plus critiques sont traitées en priorité. • **Exemple** : Accorder une priorité élevée aux risques critiques, comme la sécurisation des systèmes exposés à Internet, avant les risques modérés ou faibles. **Désignation de responsables pour les actions prioritaires :** L'entité devrait assigner un responsable pour chaque action de traitement prioritaire, afin d'assurer une supervision et un suivi rigoureux de sa mise en œuvre. • **Exemple** : Nommer le responsable de la sécurité informatique pour superviser les mesures de sécurité informatiques critiques, telles que la mise en place de pare-feu et le suivi des accès.
Niveau 2	L'entité devrait renforcer son plan de traitement des risques en intégrant un suivi des priorités, et un rapport d'avancement périodique pour chaque action. **Établissement de jalons pour les actions complexes :** Pour les actions de traitement plus complexes, l'entité devrait définir des jalons intermédiaires qui permettent d'évaluer les progrès régulièrement. • **Exemple** : Pour une mesure de traitement visant à instaurer une authentification multifactorielle, inclure des jalons pour chaque phase (ex. : test, déploiement progressif, déploiement complet) pour suivre la progression de l'implémentation. **Réévaluation et ajustement des priorités :** L'entité devrait revoir les priorités à intervalles réguliers pour adapter les ressources aux risques émergents ou aux changements de contexte. • **Exemple** : Si une nouvelle vulnérabilité critique est identifiée, ajuster les priorités pour traiter ce risque en priorité, même si cela implique de reporter d'autres actions de traitement de risques moins critiques.
Niveau 3	Il n'y a pas de recommandation supplémentaire.

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 - s02

	Recommandations
Niveau 1	L'entité devrait établir un suivi périodique pour les actions de traitement des risques pour s'assurer que chaque action est exécutée conformément aux échéances définies. La revue périodique couvre l'état d'avancement, les éventuels retards et les ajustements nécessaires, permettant ainsi à l'entité de rester proactive face aux risques. **Suivi mensuel des actions critiques** : Effectuer un suivi mensuel des actions de traitement, en documentant le statut de chaque action et les délais, afin de détecter tout retard potentiel. L'entité pourrait documenter le statut de chaque mesure d'atténuation (ex. : En cours, Terminé, Retard) et mettre à jour les informations dans un registre centralisé. • **Exemple** : Utiliser un tableur Excel partagé pour noter l'état de chaque action et indiquer si celle-ci est dans les délais ou nécessite un ajustement.
Niveau 2	**Suivi documenté avec des indicateurs de performance (KPI)** : L'entité pourrait utiliser des indicateurs clés de performance (KPI) pour mesurer l'efficacité des actions de traitement et suivre les progrès par rapport aux échéances. • **Exemple** : L'entité pourrait définir des KPI vis-à-vis du pourcentage d'actions terminées dans les délais, et analyser ces indicateurs lors de chaque revue.
Niveau 3	**Suivi continu et automatisé des actions de traitement** : L'entité devrait mettre en place un suivi automatisé avec des outils ou plateformes de gestion de projet permettant un suivi en temps réel de chaque action et l'identification rapide des retards. • **Exemple** : Utiliser un outil de gestion de projet pour suivre chaque action de traitement en temps réel et générer des alertes automatiques en cas de dépassement des échéances prévues.

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 - s02

	Recommandations
Niveau 1	L'entité devrait s'assurer que les risques de sécurité de l'information sont réévalués régulièrement et ajustés en fonction des nouveaux événements ou changements significatifs, permettant de maintenir une posture de sécurité à jour et réactive. **Établissement d'un calendrier de revue des risques :** Mettre en place un calendrier de revue des risques annuelle, pour analyser les risques de sécurité existants, évaluer leur pertinence et ajuster les évaluations de probabilité et d'impact. L'entité devrait également déclencher une revue des risques dès qu'un événement ou un changement majeur survient, comme une cyberattaque, une mise à jour importante de l'infrastructure, ou une modification réglementaire.
Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	L'entité devrait définir une **liste d'événements spécifiques** nécessitant une revue des risques anticipée, par exemple l'apparition de nouvelles vulnérabilités, le remplacement de systèmes critiques, ou l'introduction de nouvelles technologies. **Documentation des revues et suivi des changements :** Documenter chaque revue des risques, qu'elle soit programmée ou déclenchée par un événement, et consigner les modifications apportées aux évaluations de risque, en assurant une traçabilité des changements dans le registre de gestion des risques.

4.4.2 Mesures complémentaires

MC-004 L'entité devrait mettre en place des moyens de communication afin d'échanger avec le personnel responsable de l'implémentation des mesures de gestion des risques, ainsi que tous ceux ayant un intérêt, de comprendre les risques et les mesures de mitigation.

- 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 - s02

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	L'entité devrait garantir que les informations sur les risques de sécurité et les mesures de mitigation sont communiquées de manière efficace entre le personnel impliqué dans la gestion des risques et toutes les parties prenantes concernées. Cela permet de faciliter la compréhension commune des risques, d'assurer la transparence, et de renforcer l'adhésion aux mesures de sécurité.

	Identification des canaux de communication adaptés : L'entité devrait sélectionner des canaux de communication sécurisés et adaptés aux différents groupes de parties prenantes (ex. : réunions, courriels, plateformes collaboratives) pour échanger efficacement les informations sur les risques et les mesures de mitigation. **Création de documents de référence sur les risques et les mesures de mitigation :** L'entité devrait développer et diffuser des documents de référence (ex. : fiches sur les risques majeurs, guides de mitigation) pour aider le personnel à comprendre les risques identifiés et les mesures de traitement associées. **Formation et sensibilisation des parties prenantes :** L'entité pourrait organiser des sessions de formation et de sensibilisation pour expliquer les risques principaux et les stratégies de mitigation, en adaptant le contenu selon le niveau de responsabilité et d'implication des participants.
Niveau 3	Il n'y a pas de recommandation supplémentaire.

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 - s02

	Recommandations
Niveau 1	Il n'y a pas de recommandation applicable.
Niveau 2	Il n'y a pas de recommandation supplémentaire.
Niveau 3	L'entité devrait garantir que le processus de gestion et d'évaluation des risques demeure pertinent, efficace, et aligné avec les meilleures pratiques et l'évolution des nouvelles technologies. Cette amélioration continue du processus permet d'affiner les méthodes d'évaluation, de rendre les décisions plus fiables et de s'assurer que les pratiques de gestion des risques s'adaptent aux nouveaux contextes. **Revue périodique du processus d'évaluation des risques** : L'entité devrait organiser une revue annuelle du processus d'évaluation des risques pour vérifier son efficacité et identifier les améliorations possibles. Tous les ans, l'entité pourrait réunir les parties prenantes (ex. : DSI, Gestionnaire de risques, responsables métiers) pour examiner le processus d'évaluation des risques et identifier les points d'amélioration, comme l'efficacité des méthodes d'identification des menaces, actifs et la pertinence des critères d'évaluation. **Collecte des retours d'expérience :** Après chaque revue majeure ou incident important, l'entité pourrait collecter les retours d'expérience des équipes impliquées pour identifier les faiblesses du processus d'évaluation des risques et les opportunités d'amélioration.

	Mise à jour des méthodologies d'évaluation : Revoir et, si nécessaire, ajuster les méthodologies d'évaluation des risques (ex. : méthodes quantitatives/qualitatives, matrices de risque) pour s'assurer qu'elles restent alignées avec les meilleures pratiques et les besoins spécifiques de l'entité. Par exemple, si les méthodes actuelles d'évaluation sont jugées trop subjectives, l'entité pourrait envisager l'ajout de critères quantitatifs pour améliorer la précision du classement des risques, ou adopter une matrice de risque plus détaillée pour mieux distinguer les niveaux de priorité. **Intégration de nouvelles technologies dans le processus :** L'entité pourrait évaluer régulièrement l'utilisation de nouvelles technologies (ex. : outils de Threat Intelligence, systèmes d'automatisation) pour renforcer le processus d'évaluation des risques, et intégrer ces solutions si elles contribuent à une meilleure précision et réactivité. **Alignement avec les standards et réglementations actuels :** L'entité devrait vérifier périodiquement que le processus de gestion des risques est conforme aux obligations légales, aux exigences réglementaires et aux standards en vigueur (ex. : ISO 27001, NIS2), et effectuer les mises à jour nécessaires pour s'aligner sur ces normes.