EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

NIS2 ET CER AU LUXEMBOURG

Responsabilités de la direction

Obligations, décisions et risques personnels

Direction générale, conseil d’administration et cadres dirigeants
État du droit et vérification des sources : 22 novembre 2026



Illustration IA · établissement fictif

Ce qui relève de la direction

L’approbation et la surveillance font expressément partie des missions de direction.

Comprendre les risques	Faire présenter l’analyse des risques et les besoins d’action, les examiner et les évaluer.
Permettre la mise en œuvre	Décider de mesures appropriées et prévoir les moyens, le personnel et les responsabilités nécessaires.
Suivre l’efficacité	Contrôler la mise en œuvre, faire corriger les lacunes et suivre régulièrement des formations.

> **Déléguer les tâches techniques ne supprime pas ces obligations propres à la direction.**

NIS2 art. 20–21 · LU-NIS2 art. 12–13 · Guide ILR pour les dirigeants

Cadre juridique et entrée en vigueur

Les directives européennes et leur transposition luxembourgeoise sont citées séparément.

NIS2	Directive (UE) 2022/2555. Loi luxembourgeoise du 5 mai 2026, Mémorial A225, en vigueur depuis le 10 mai 2026.
CER	Directive (UE) 2022/2557. Loi luxembourgeoise du 5 mai 2026, Mémorial A226, en vigueur depuis le 10 mai 2026.
Vérifier le champ d'application	La forme juridique, l'activité, la qualification et les règles sectorielles déterminent les obligations concrètement applicables.

> **Cette présentation concerne le Luxembourg. La transposition peut différer dans les autres États.**

NIS2 : loi LU A225 · CER : loi LU A226 · UE 2022/2555 et 2022/2557

LU NIS2 LU CER EU NIS2 EU CER

Quelles entités et quelles personnes ?

L’emploi courant du terme « critique » ne suffit pas à déterminer la qualification juridique.

Sujet	Obligation et conséquence
Entité relevant de NIS2	Entité essentielle ou importante selon l’activité, la taille et les cas particuliers prévus par la loi. Des organismes publics peuvent aussi être concernés.
Entité relevant de CER	Le HCPN ou la CSSF identifie l’entité. La désignation formelle intervient par arrêté grand-ducal et est notifiée à l’entité.
Personne dirigeante	La qualité de membre d’un organe et les pouvoirs de représentation, de décision et de contrôle sont déterminants. Un titre informatique ne suffit pas.

Clarifier par écrit la qualification, l’autorité compétente et l’organe de direction effectivement responsable.

NIS2 art. 2–4, 20, 32(6) · LU-NIS2 art. 1, 3, 11, 13, 22(6), 23(5) · CER art. 6–8 · LU-CER art. 3, 7–8

EU NIS2 LU NIS2 EU CER LU CER EU – DORA

Approuver et superviser restent des devoirs de direction

La loi énonce expressément la responsabilité de l’organe de direction.

Approbation	La direction approuve les mesures de gestion des risques en matière de cybersécurité.
Surveillance	Elle suit leur mise en œuvre, leur efficacité et la correction des lacunes constatées.
Responsabilité propre	Sa responsabilité peut être engagée en cas de violation de ces obligations légales.

> **Un contrat de prestation ou la désignation d’un RSSI ne remplace pas une décision de la direction.**

NIS2 art. 20(1) · LU-NIS2 art. 13(1), 22(6), 23(5)

EU NIS2 LU NIS2

Répartir efficacement les missions

Toute responsabilité suppose des pouvoirs, des ressources et un circuit de décision accessible.

Sujet	Obligation et conséquence
Organe de direction	Approuve les objectifs de sécurité, le traitement des risques et les moyens. Arbitre les alertes et contrôle l'avancement.
Responsables spécialisés	Évaluent les risques, élaborent les mesures, les mettent en œuvre dans leur mandat et signalent clairement les obstacles.
Contrôle et suppléance	Délais, suppléances, obligations de compte rendu et contrôles indépendants évitent les lacunes de responsabilité.

Les missions, les pouvoirs de décision et les voies d'escalade doivent être cohérents.

NIS2 art. 20–21 · LU-NIS2 art. 12–13 · Recommandation pratique de mise en œuvre

Fonder les décisions sur l’analyse des risques

La direction doit connaître les interruptions tolérables des services et les menaces qui les exposent.

01 Inventaire

Recenser les services essentiels, l’informatique et les systèmes industriels, les sites, données, personnels, prestataires et leurs dépendances.

→ 02 Scénarios de risque

Évaluer la probabilité et les conséquences d’une cyberattaque, d’une panne électrique, d’un incendie, d’une inondation, d’un sabotage ou d’une erreur humaine.

→ 03 Traitement des risques

Documenter les besoins de protection, les contrôles existants, les risques résiduels, les mesures, les responsables et les échéances.

> **Une liste de mesures sans analyse des risques traçable ne suffit pas à étayer une décision budgétaire.**

NIS2 art. 21(1)–(2)(a) · LU-NIS2 art. 12(1)–(2) · Guide ILR pour les dirigeants

CER : analyser les risques de toute l’activité

La résilience des services critiques couvre aussi les menaces extérieures à l’informatique.

9
mois

4
ans

Délais et actualisation

Après notification : analyse sous 9 mois ; chapitre 4 applicable en principe après 10 mois. Actualiser au besoin et au moins tous les 4 ans.

Tous les risques pertinents

Risques naturels ou d’origine humaine, accidents, urgences sanitaires, menaces hybrides, terroristes et autres actes intentionnels.

Dépendances

Prendre en compte les défaillances d’autres secteurs et de services transfrontières, ainsi que les effets de ses propres activités sur d’autres entités.

> **Relier l’évaluation nationale aux risques concrets des sites et de l’exploitation.**

CER art. 6(3), 12 · LU-CER art. 7(4), 8, 11

EU CER LU CER

NIS2 : organisation et approvisionnement

Le socle légal comprend dix domaines. Voici les cinq premiers.

Sujet	Obligation et conséquence
1. Politique de risque	Politiques d’analyse des risques et de sécurité des systèmes d’information.
2. Incidents	Détection, traitement et limitation des incidents de sécurité.
3. Continuité	Sauvegardes, reprise après sinistre, continuité des activités et gestion des crises.
4. Chaîne d’approvisionnement	Exigences de sécurité applicables aux fournisseurs et prestataires directs.
5. Cycle de vie	Sécurité de l’acquisition, du développement et de la maintenance, ainsi que traitement et divulgation des vulnérabilités.

> **Pour chaque domaine, définir les responsabilités, les moyens nécessaires et des résultats vérifiables.**

NIS2 art. 21(2)(a)–(e) · LU-NIS2 art. 12(2), points 1–5

EU NIS2 LU NIS2

NIS2 : personnel et accès

Les cinq autres domaines associent sécurité technique et procédures fiables.

Sujet	Obligation et conséquence
6. Efficacité	Procédures permettant d’évaluer si les mesures de sécurité fonctionnent réellement.
7. Compétences	Pratiques de base en matière de cyberhygiène et formations à la cybersécurité.
8. Cryptographie	Politiques de cryptographie et, s’il y a lieu, de chiffrement.
9. Habilitations	Sécurité des ressources humaines, contrôle d’accès et gestion des actifs à protéger.
10. Authentification sûre	Authentification multifacteur ou continue, communications sécurisées et communications d’urgence, selon les besoins.

> **Mettre en œuvre et tester les contrôles ; corriger les lacunes sans retard injustifié.**

NIS2 art. 21(2)(f)–(j), 21(4) · LU-NIS2 art. 12(2), points 6–10, 12(5)

Coordonner accès physiques et cybersécurité

Même protégé numériquement, un système reste exposé par son environnement physique.

Zones protégées	Protéger salles serveurs, postes de conduite, locaux techniques et installations critiques par des droits d’accès gradués.
Sécurité des personnes	Coordonner évacuation, secours et protection incendie avec la prévention des accès non autorisés.
Scénarios de défaillance	Prévoir les pannes électriques, réseau et système, l’ouverture d’urgence, le fonctionnement manuel et la remise en service sûre.

> **Le fonctionnement d’une porte exige une décision coordonnée pour l’exploitation et les situations d’urgence.**

NIS2 art. 21(2) · LU-NIS2 art. 12(2) · CER art. 13(1)(b)–(d) · LU-CER art. 12

EU NIS2 LU NIS2 EU CER LU CER

CER : protection et réaction

Les entités critiques doivent déduire de leur évaluation des risques des mesures appropriées et proportionnées.

Prévention	Prévenir les incidents autant que possible, notamment par la préparation aux catastrophes et l'adaptation aux risques climatiques pertinents.
Protection physique	Sécuriser les installations et infrastructures critiques par des mesures adaptées de contrôle d'accès, de surveillance et de protection des sites.
Réaction	Limiter les conséquences, activer l'organisation de crise et appliquer les procédures définies de gestion des incidents.

> **Prévention, protection et réaction aux crises doivent former un dispositif de résilience cohérent.**

CER art. 13(1)(a)–(c) · LU-CER art. 12(1), points 1–3

EU CER LU CER

CER : continuité et personnel

La résilience va jusqu’au rétablissement sûr du service essentiel.

Rétablissement	Prévoir la continuité des activités et des chaînes d’approvisionnement alternatives pour reprendre la fourniture du service.
Sécurité du personnel	Identifier les catégories de personnes et fonctions sensibles. Organiser légalement droits d’accès, qualifications et vérifications d’aptitude.
Formation et exercices	Informer et former le personnel, développer la sensibilisation et organiser des exercices de préparation pratique.

> **Le plan de résilience relie les mesures de protection au personnel, aux procédures et à la reprise.**

CER art. 13–14 · LU-CER art. 12(1), points 4–6, 12(2)–(3), 13–15

EU CER LU CER

Budget et effectifs : des décisions de direction

Toute mesure approuvée doit disposer des conditions nécessaires à sa mise en œuvre effective.

Dossier de décision	Présenter clairement le risque, le fondement légal, les options, les coûts, les effectifs nécessaires et les conséquences de l'inaction.
Approbation	Accorder les moyens et capacités appropriés, ou décider d'une solution alternative techniquement solide avec une échéance.
Escalade	Saisir l'organe de direction compétent des risques majeurs non couverts et des mesures obligatoires bloquées.

> **L'absence de budget ne dispense pas, de manière générale, des obligations légales de protection.**

NIS2 art. 20–21 · LU-NIS2 art. 12–13 · CER art. 13 · Guide ILR pour les dirigeants

EU NIS2 LU NIS2 EU CER ILR – Direction EU 2024/2690

Former la direction et le personnel

Le Luxembourg impose expressément des formations régulières aux deux niveaux.

Direction

+

Personnel

Participation de la direction

Identifier les risques, évaluer les mesures et comprendre les effets sur les services fournis.

Organisation par l’entité

Proposer régulièrement au personnel des formations similaires, adaptées aux fonctions et aux risques.

Pratique et justificatifs

Documenter participations, contenus et objectifs pédagogiques. Compléter les formations par des exercices de crise et des tests de reprise.

> **La formation d’un RSSI ne remplace pas celle de la direction générale.**

NIS2 art. 20(2), 21(2)(g) · LU-NIS2 art. 13(2), 12(2), point 7 · CER art. 13(1)(f)

EU NIS2 LU NIS2 EU CER LU CER ILR – Direction

Prestataires et cycle de vie des produits

L’externalisation modifie l’exécution, mais pas les besoins de protection de l’entité.

Avant le contrat	Convenir des exigences de sécurité, responsabilités, circuits de notification, justificatifs et modalités de traitement des vulnérabilités.
Pendant l’exploitation	Surveiller habilitations, accès à distance, mises à jour, fin du support et qualité réelle des prestations.
En cas de changement ou de défaillance	Maintenir disponibles données, documentation et accès. Préparer le transfert, le fonctionnement dégradé et les solutions d’approvisionnement alternatives.

> **Contrats et certificats constituent des justificatifs. La prestation effective reste à contrôler.**

NIS2 art. 21(2)(d)–(e), 21(3) · LU-NIS2 art. 12(2), 12(4) · CER art. 13(1)(d)

EU NIS2 LU NIS2 EU CER

Contrôle et amélioration continue

La direction a besoin de résultats vérifiables, au-delà d'un simple indicateur de couleur.

01 Vérifier l'efficacité

Réaliser audits, tests de reprise, revues des habilitations et exercices selon des critères de contrôle clairs.

→ 02 Suivre les écarts

Prioriser les lacunes, désigner les responsables, fixer les échéances et faire remonter les mesures en retard.

→ 03 Décider sur les résultats

Réévaluer les risques résiduels et les conflits d'objectifs. Adapter, au besoin, le personnel, les procédures et les mesures.

> **Une lacune majeure identifiée ne doit pas rester dans un rapport sans décision.**

NIS2 art. 20(1), 21(2)(f), 21(4) · LU-NIS2 art. 12(2), point 6, 12(5), 13(1)

EU NIS2 LU NIS2

Plan d’urgence et organisation de crise

En cas d’incident, décision, communication et réaction opérationnelle doivent fonctionner immédiatement.

01 Déclenchement

Définir les seuils, l’alerte, les contacts joignables et les suppléances pour les différents scénarios.

→ 02 Direction de crise

Préparer les pouvoirs de décision, le budget d’urgence, les priorités et la coopération avec les spécialistes et les autorités.

→ 03 Communication

Organiser les points de situation internes, les moyens de communication de secours et l’information à temps des destinataires concernés et des autorités.

> **Le plan doit rester utilisable si les systèmes habituels ou des personnes clés sont indisponibles.**

NIS2 art. 21(2)(b)–(c), (j), art. 23 · LU-NIS2 art. 12, 14 · CER art. 13, 15

EU NIS2 LU NIS2 EU CER LU CER

Reprendre jusqu’au retour sûr à la normale

Disposer d’une sauvegarde ne démontre pas encore la capacité de rétablissement.

01 Priorités et objectifs

Définir les services critiques, l’interruption tolérable et la perte de données acceptable. Tenir compte des dépendances lors du redémarrage.

→ 02 Tester le rétablissement

Vérifier l’intégrité, la disponibilité et l’utilisabilité réelle des sauvegardes. Exercer la reprise dans des conditions réalistes.

→ 03 Validation et retour d’expérience

Confirmer un état sûr, assumer la décision de retour à la normale et suivre les causes ainsi que les améliorations.

> **La direction doit connaître la capacité de rétablissement du service, au-delà du plan de sauvegarde.**

NIS2 art. 21(2)(c), (f) · LU-NIS2 art. 12(2), points 3, 6 · CER art. 13(1)(d)

EU NIS2 LU NIS2 EU CER LU CER

Préparer les circuits de notification

Les deux cadres juridiques prévoient des séquences de notification différentes.

NIS2	Dès connaissance de l'incident important : alerte précoce sous 24 heures, notification sous 72 heures. Rapport final au plus tard un mois après la notification.
CER	Perturbation importante, effective ou potentielle : sans retard injustifié, en principe sous 24 heures après en avoir connaissance. Rapport détaillé, le cas échéant, dans le mois suivant.
Rôle de la direction	Clarifier à l'avance l'évaluation, la préservation des preuves, la suppléance et les pouvoirs de notification. Informer les destinataires concernés selon les règles applicables.

> **Des informations incomplètes ne justifient pas d'attendre systématiquement la fin de toutes les investigations.**

NIS2 art. 23 · LU-NIS2 art. 14 · CER art. 15 · LU-CER art. 16

EU NIS2 LU NIS2 EU CER LU CER

Des preuves pour la direction et l’autorité

Une documentation traçable montre ce qui a été décidé et effectivement mis en œuvre.

Décisions	Qualification, analyse des risques, approbation des mesures, budget, responsables et priorisation motivée.
Mise en œuvre	Configurations, maintenance, habilitations, formations, exercices et résultats des tests de rétablissement.
Corrections	Rapports de lacunes, escalades, échéances, justificatifs de clôture et nouveaux contrôles d’efficacité.

> **La documentation contribue à la preuve. Elle ne remplace pas la protection effective.**

NIS2 art. 32–33 · LU-NIS2 art. 22–23 · CER art. 13, 21 · LU-CER art. 12, 18

EU NIS2 LU NIS2 EU CER LU CER

Entités essentielles : nouvelles règles ILR

Le règlement ILR/N26/10 s’applique depuis le 3 novembre 2026 aux notifications à l’ILR.

Trois documents	Mesures de protection existantes, principaux scénarios de cyberrisque et plan pluriannuel de mesures avec délais, responsables et priorités.
Échéance et changements	Chaque année au plus tard le 15 mars, même sans changement. Aussi en cas de modification significative des risques, de nouveau risque majeur ou de mesures de sécurité particulièrement importantes.
Entités critiques	Les entités essentielles identifiées comme critiques au titre de CER déclarent aussi leurs dépendances envers les fournisseurs et prestataires directs.
Transmission sécurisée	Par SERIMA ou un canal sécurisé reconnu équivalent par l’ILR. Informations complémentaires à la demande de l’autorité.

> **Prochaine échéance annuelle : 15 mars 2027. Un événement ou une demande de l’autorité peut imposer un délai plus proche.**

LU-NIS2 art. 12(3), 22 · ILR/N26/10 art. 1–8 · Mémorial A532 du 30.10.2026

LU NIS2 ILR/N26/10

Ce que l’autorité peut exiger

Les sanctions financières ne sont qu’une partie des conséquences possibles.

Sujet	Obligation et conséquence
NIS2 : entités essentielles	Inspections sur place, contrôles à distance, audits, contrôles de sécurité, preuves et mesures correctrices obligatoires. Une surveillance continue est aussi possible.
NIS2 : entités importantes	Surveillance en principe a posteriori, en présence d’indices de manquement. Les pouvoirs d’information, de contrôle et d’exécution restent importants.
CER	Informations, inspections et audits de résilience. Les manquements constatés doivent être corrigés dans les délais fixés.

> **Les corrections imposées et les justificatifs mobilisent aussi du temps, du personnel et des auditeurs externes.**

NIS2 art. 32–33 · LU-NIS2 art. 22–23 · CER art. 21 · LU-CER art. 18

EU NIS2 LU NIS2 EU CER LU CER

NIS2 : amendes élevées contre l’entité

Pour les manquements à la gestion des risques ou aux principales obligations de notification, le plafond le plus élevé s’applique.

Entité essentielle

10 M€

ou 2 %

chiffre d’affaires mondial de l’exercice précédent

Entité importante

7 M€

ou 1,4 %

chiffre d’affaires mondial de l’exercice précédent

Le montant le plus élevé est retenu

Pour un chiffre d’affaires pertinent de 800 millions d’euros : au maximum 16 millions d’euros ou 11,2 millions d’euros, respectivement.

> **Ce sont des plafonds, sans peine minimale ni amende personnelle automatique pour la direction générale.**

NIS2 art. 34(4)–(5) · LU-NIS2 art. 26(4)–(5), pour les art. 12 et 14(1)–(4)

EU NIS2 LU NIS2

NIS2 : autres sanctions et astreinte

Les obligations de gouvernance et de formation disposent aussi d’un régime de sanctions spécifique.

Jusqu’à 250 000 euros	Contre l’entité pour les obligations visées à l’article 25 LU, notamment l’approbation, la surveillance et la formation régulière prévues à l’article 13.
Autres conséquences	Avertissement ou blâme. Selon le fondement juridique : corrections obligatoires, publications et autres mesures de surveillance.
Astreinte	Jusqu’à 1 250 euros par jour, dans la limite de 25 000 euros par manquement constaté, pour en obtenir la cessation.

> **Les montants et fondements juridiques ne doivent pas être additionnés comme un total automatique.**

LU-NIS2 art. 25(1), art. 26(7), art. 22–24

CER : le régime national de sanctions

CER ne reprend pas la formule NIS2 fondée sur le chiffre d’affaires.

Jusqu’à 250 000 euros	Avertissement, blâme et/ou amende administrative pouvant atteindre 250 000 euros contre l’entité critique pour les manquements visés par la loi.
Correction et contrôle	Instructions de l’autorité, inspections, audits et obligation de corriger dans les délais les lacunes constatées.
Conséquences distinctes	Des conséquences contractuelles, civiles ou pénales peuvent s’ajouter si leurs conditions propres sont remplies.

> **Présenter une sanction CER générale de 10 millions d’euros ou 2 % serait erroné pour ce cadre luxembourgeois.**

CER art. 21–22 · LU-CER art. 18(1)–(4), 19(1)–(5)

EU CER LU CER

Interdiction temporaire de fonctions dirigeantes

Une mesure judiciaire pour les entités essentielles NIS2 ; l'administration publique visée en est exclue.

01 Conditions préalables

Certaines mesures correctrices de l'autorité restent sans effet. Un délai supplémentaire fixé expire sans la mise en œuvre requise.

→ 02 Décision judiciaire

À la demande de l'autorité, le président du tribunal d'arrondissement de Luxembourg peut interdire temporairement des fonctions dirigeantes dans cette entité.

→ 03 Portée et fin

Sont visées les personnes au niveau du directeur général ou du représentant légal. La correction et la levée judiciaire mettent fin à la mesure.

> **Il ne s'agit ni d'une exclusion automatique de l'entreprise ni d'une interdiction professionnelle générale à vie.**

NIS2 art. 32(5) · LU-NIS2 art. 22(5)

EU NIS2 LU NIS2

Plusieurs fondements de responsabilité personnelle

L’amende contre l’entreprise et la responsabilité personnelle relèvent de niveaux juridiques différents.

Sujet	Obligation et conséquence
Obligation de direction NIS2	Les organes de direction peuvent répondre de leurs manquements. Les personnes disposant de pouvoirs de représentation, de décision ou de contrôle doivent assurer la conformité.
Droit civil	La société ou, sous des conditions particulières, des tiers peuvent demander réparation d’un dommage causé de manière imputable.
Droit pénal	Les peines personnelles supposent une infraction applicable et la réunion de ses conditions concrètes.

D’autres cadres peuvent aussi être concernés. Leurs obligations et pouvoirs effectifs sont déterminants.

NIS2 art. 20(1), 32(6), 33(5) · LU-NIS2 art. 13(1), 22(6), 23(5) · Guichet.lu

EU NIS2 LU NIS2 Guichet – Civil Guichet – Pénal

Quand une réparation personnelle est possible

En droit civil, le manquement, le dommage et le lien de causalité sont des questions centrales.

Sujet	Obligation et conséquence
Envers la société	SA : exécution du mandat et fautes de gestion selon l'article 441-9. SARL : responsabilité des gérants par renvoi de l'article 710-16 de la même loi.
Envers les tiers	Violations de la loi sur les sociétés ou des statuts : responsabilité particulière de l'article 441-9. Les autres fautes de gestion exigent un fondement distinct.
Examen individuel	Apprécier la forme juridique, la qualité de membre d'un organe, les compétences, le comportement, les connaissances et la contribution au dommage.

Un incident de sécurité ne prouve pas une faute. Des avertissements précis ignorés peuvent toutefois être déterminants.

LSC art. 441-8, 441-9, 710-16 · SA dualiste : art. 442-10, 442-16 · Guichet.lu

Guichet – Civil LSC

Négligence, défaillance grave et refus conscient

Il n’existe pas de barème général NIS2 reliant chaque degré de faute à un montant fixe.

Omission par négligence	Un examen ou contrôle nécessaire n’est pas réalisé. Il faut déterminer ce qu’une direction diligente aurait dû identifier et faire dans cette situation.
Défaillance particulièrement grave	Des risques majeurs manifestes ou des avertissements répétés restent sans suite. La qualification juridique dépend du cas concret.
Refus conscient	Des mesures nécessaires ou des injonctions contraignantes ne sont pas mises en œuvre, malgré leur connaissance et la possibilité d’agir.

> **Connaissance, durée, répétition, conséquences, coopération et possibilités concrètes d’action influencent l’appréciation.**

NIS2 art. 32(7), 34(3) · LU-NIS2 art. 22(7), 26(3) · Droit général de la responsabilité

Autres conséquences personnelles et opérationnelles

Un incident peut affecter simultanément plusieurs relations juridiques et commerciales.

Conséquences personnelles	Dommages et intérêts, révocation au titre du droit des sociétés ou conséquences en droit du travail, selon les règles applicables.
Conséquences pénales	Si une infraction distincte est constituée, une amende ou une peine d'emprisonnement peut être encourue. NIS2/CER ne rendent pas, à elles seules, chaque incident pénalement punissable.
Conséquences opérationnelles	Coûts d'interruption et de reprise, réclamations de clients, conséquences contractuelles et atteinte à la réputation peuvent dépasser l'amende elle-même.

> **L'assurance, y compris celle des dirigeants, n'efface pas les obligations et ne couvre pas automatiquement tout dommage ou sanction.**

Guichet.lu : responsabilités civile et pénale · Contrats et droit sectoriel applicables · Code pénal art. 418–420

Guichet – Civil Guichet – Pénal Code pénal

Droit pénal distinct en cas d’atteinte aux personnes

Ces infractions du Code pénal s’appliquent de manière autonome. Les fourchettes légales de base sont présentées ici.

Sujet	Obligation et conséquence
Art. 418 : conditions	Un défaut de prévoyance ou de précaution cause la mort ou des blessures sans intention d’attenter à la personne. Faute, dommage corporel et causalité doivent être prouvés.
Art. 419 : homicide involontaire	Emprisonnement de 3 mois à 2 ans et amende de 500 à 10 000 euros.
Art. 420 : blessures involontaires	Emprisonnement de 8 jours à 2 mois et amende de 500 à 5 000 euros, ou l’une de ces peines seulement.

> **L’imputabilité personnelle doit être examinée séparément. Une faute même légère peut constituer l’infraction.**

Code pénal art. 418–420 · Consolidation officielle en vigueur du 19.12.2025, p. 100–101

Code pénal Guichet – Pénal

Exemple : faille connue et moyens refusés

Cas fictif d’une entité essentielle permettant un accès à distance à des systèmes critiques.

Situation initiale

L’informatique signale un risque d’accès majeur. Une protection appropriée et une solution transitoire moins coûteuse sont présentées.

Décision de la direction

Les deux solutions sont refusées sans alternative viable. Les avertissements et les délais de mise en œuvre restent sans suite.

Conséquences possibles

Surveillance et corrections, amende NIS2 contre l’entité. Des recours personnels peuvent s’ajouter si un manquement et un dommage causal sont établis.



Illustration IA · établissement fictif

> **La décision démontrable concernant le risque connu et la protection nécessaire est déterminante.**

Exemple fictif · NIS2 art. 20–21, 32–34 · LU-NIS2 art. 12–13, 22, 26

Exemple : panne sans reprise testée

Cas fictif d’un opérateur critique disposant de systèmes informatiques et industriels et d’un site sécurisé.

Situation initiale

Une panne électrique et un dysfonctionnement des accès surviennent simultanément. La reprise n’a jamais été exercée avec l’exploitation.

Défaut d’organisation

Suppléance, ouverture d’urgence, approvisionnement de secours et ordre de rétablissement restent indéfinis. Les exercices nécessaires ont été reportés à plusieurs reprises.

Conséquences possibles

Corrections CER et amende nationale, avec éventuellement une procédure NIS2. Autres questions de responsabilité en cas de dommages corporels ou matériels imputables.



Illustration IA · établissement fictif

> **La responsabilité concerne la coordination de l’ensemble du service jusqu’à sa reprise sûre.**

Exemple fictif · CER art. 12–13, 21–22 · LU-CER art. 11–12, 18–19 · LU-NIS2 art. 12

EU CER LU CER LU NIS2 Guichet – Civil Guichet – Pénal

Exemple : refus des corrections imposées

Cas fictif d’une entité essentielle NIS2 après un contrôle de l’autorité.

Constat	L’autorité exige des corrections concrètes. La direction reçoit des exigences et des délais clairs.
Escalade	Les mesures restent sans effet. Un délai supplémentaire expire lui aussi sans la mise en œuvre requise.
Conséquences possibles	Suspension temporaire, ordonnée par le juge, d’une autorisation ou certification pertinente et interdiction de fonctions dirigeantes dans cette entité.

> **L’escalade légale peut toucher directement l’exercice personnel de la direction et l’activité de l’entreprise.**

Exemple fictif · NIS2 art. 32(5) · LU-NIS2 art. 22(5)

EU NIS2 LU NIS2

Exemple : formation et notification absentes

Cas fictif d’une entité importante NIS2 présentant des lacunes d’organisation répétées.

Formation omise	La direction refuse de se former et ne garantit pas une offre régulière de formation au personnel.
Défaillance de la notification	Un incident important est identifié. Personne ne dispose de la suppléance et des pouvoirs nécessaires pour le notifier dans les délais.
Conséquences possibles	Les obligations de direction et de formation relèvent de l’article 25 LU. Les violations des principales obligations de notification peuvent relever de l’article 26(5) LU.

> **Les différents manquements relèvent de fondements juridiques et de régimes de sanctions distincts.**

Exemple fictif · LU-NIS2 art. 13–14, 25–26 · NIS2 art. 20, 23, 34

LU NIS2 EU NIS2

Décider de façon proportionnée et combler les lacunes

La direction peut fixer des priorités. Elle doit assurer un niveau de protection conforme au droit.

Choix motivé	Mettre en balance les mesures équivalentes, les coûts de mise en œuvre, l'efficacité et les risques concrets.
Transition maîtrisée	Définir, jusqu'à la solution définitive, des mesures provisoires adaptées, des responsables, des délais et un contrôle.
Limite de l'acceptation du risque	Une approbation interne ne suspend ni les obligations légales ni les injonctions contraignantes de l'autorité.

> **Des alternatives solides sont possibles. Bloquer durablement des mesures nécessaires sans justification n'est pas une solution.**

NIS2 art. 21(1), 21(4) · LU-NIS2 art. 12(1), 12(5), 13 · CER art. 13

EU NIS2 LU NIS2 EU CER

Un dossier de décision pour la direction

Une décision utilisable relie le risque, l’arbitrage et la preuve de mise en œuvre.

Sujet	Obligation et conséquence
Base de décision	Service concerné, évaluation du risque, fondement légal, options et conséquences de l’inaction.
Décision engageante	Mesures retenues, budget, personnel, responsable, échéances et mesures provisoires nécessaires.
Contrôle	Date du compte rendu, critères d’efficacité, seuil d’escalade et preuve de mise en œuvre complète.

> **Recommandation : toute lacune majeure de protection encore ouverte reçoit une décision de direction traçable.**

Recommandation de mise en œuvre fondée sur LU-NIS2 art. 12–13 et LU-CER art. 11–12

Un plan possible pour les 90 prochains jours

Proposition d’organisation. Les obligations déjà exigibles et les délais de l’autorité priment.

01 Jours 1–30

Clarifier le champ d’application, les responsabilités de direction, les services essentiels, les risques ouverts et les mesures immédiates.

→ 02 Jours 31–60

Décider et mettre en œuvre le traitement des risques, les moyens nécessaires, les formations, l’organisation d’urgence et les exigences envers les fournisseurs.

→ 03 Jours 61–90

Tester la reprise et les procédures de crise, vérifier l’efficacité et assurer le suivi des lacunes restantes avec des engagements précis.

> **Ces 90 jours ne sont ni un délai de grâce légal ni un report des besoins urgents de protection.**

Recommandation pratique · Fondements légaux : LU-NIS2 art. 12–14, LU-CER art. 11–12, 16

LU NIS2 LU CER

Huit questions pour la prochaine réunion

Les réponses devraient s’appuyer sur des décisions et des justificatifs à jour.

Champ d’application et risques	La qualification et les compétences sont-elles clarifiées ? Dispose-t-on d’une analyse des risques actuelle et solide ?
Mesures et ressources	Les mesures nécessaires sont-elles approuvées ? Budget, personnel et pouvoirs permettent-ils leur mise en œuvre ?
Formation et contrôle	La direction suit-elle régulièrement des formations ? L’efficacité et la correction des lacunes sont-elles vérifiées ?
Crise et reprise	Les circuits de notification et l’organisation d’urgence fonctionnent-ils ? Le rétablissement sûr a-t-il réellement été testé ?

> **Les réponses encore ouvertes doivent déboucher sur des décisions avec responsables et échéances.**

Vérification de direction fondée sur NIS2 art. 20–23 et CER art. 12–15

EU NIS2 EU CER LU NIS2 LU CER

Sources juridiques et correspondance des articles

Les références courtes de chaque diapositive renvoient à ces textes officiels.

Sujet	Obligation et conséquence
NIS2 : gouvernance	Art. 20 UE → art. 13 LU. Art. 21 UE → art. 12 LU. Art. 23 UE → art. 14 LU.
NIS2 : exécution	Art. 32–34 UE → art. 22–23, 26 LU. Sanctions complémentaires : art. 25 LU. Protection des données : art. 35 UE → art. 24 LU.
CER	Art. 12–13 UE → art. 11–12 LU. Art. 15 UE → art. 16 LU. Art. 21–22 UE → art. 18–19 LU.

> **Les règles luxembourgeoises applicables sont déterminantes. Les articles de l'UE expliquent le cadre commun.**

Textes officiels intégraux : EUR-Lex et Legilux, lois A225 et A226 du 5 mai 2026

EU NIS2 LU NIS2 EU CER LU CER ILR/N26/10

Mise en perspective et ressources complémentaires

Une décision de direction solide associe examen juridique, évaluation spécialisée et mise en œuvre démontrable.

Explications officielles	ILR : NIS2 et guide pour les dirigeants. HCPN : résilience des entités critiques. Les dispositions juridiques applicables restent déterminantes.
Responsabilité personnelle	Guichet.lu explique les responsabilités civile et pénale. La forme juridique et les faits concrets déterminent les règles applicables.
Prochaine étape	Transformer les obligations et risques ouverts en un plan d'action engageant, avec les fonctions juridique, informatique, exploitation, sécurité et l'organe de direction compétent.

EIWTC Security Advisory · Conseil en sécurité et conception du contrôle d'accès · eiwtc.lu

Sources vérifiées le 22.11.2026 · Exemples fictifs · Information générale, sans conseil juridique individuel

ILR ILR – Direction HCPN Guichet – Civil Guichet – Pénal