BRIEFING STRATÉGIQUE DE CONFORMITÉ POUR DÉCIDEURS

L’alliance cyber-physique : NIS-2 et CER au Luxembourg

Comprendre la stratégie nationale de résilience, identifier les entités concernées et exercer la responsabilité de la direction grâce à une gouvernance des accès adaptée aux risques et à des preuves solides.

Fondé sur les lois luxembourgeoises du 5 mai 2026 et la stratégie nationale de résilience (SNR)

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

Trois axes relient résilience numérique et physique

01. DEUX CADRES LÉGAUX

Deux réglementations complémentaires

Les lois du 5 mai 2026 relient résilience physique (CER) et cybersécurité (NIS-2). Risques et dépendances doivent être examinés ensemble. Les obligations légales restent à évaluer séparément ; aucune structure organisationnelle unique n'est imposée de manière générale.

02. SUPERVISION ET NOTIFICATION

HCPN, ILR et CSSF coordonnés

ILR et HCPN supervisent leurs domaines respectifs ; la CSSF intervient dans les domaines financiers attribués par la loi. CER et NIS-2 ont des seuils et délais de suivi distincts. Un incident peut déclencher les deux circuits de notification.

03. INTÉGRATION SELON LE RISQUE

Le contrôle d'accès comme composante

L'état de l'art exige des mesures adaptées et proportionnées. Les serrures mécaniques ne sont pas interdites en général. L'électronique peut faciliter retrait des droits et traçabilité ; son efficacité doit être testée. Elle n'exonère pas de responsabilité.

Huit piliers interdépendants structurent la résilience luxembourgeoise

PILIER 1

Démocratie et gouvernement

Protéger les institutions contre les influences hybrides.

PILIER 2

Société résiliente

Préparation collective, kits d'urgence, LU-Alert.

PILIER 3 (CENTRAL)

Infrastructures et biens essentiels

Protection physique des infrastructures : ancrage CER.

PILIER 4

Économie résiliente

Diversification, approvisionnement et marché intérieur.

PILIER 5

Ressources logistiques

Stocks stratégiques, logistique et soutien civilo-militaire.

PILIER 6 (CENTRAL)

Cyberrésilience

Protection des réseaux et crise informatique (NIS-2).

PILIER 7

Défense civile

Coopération CGDIS, Police, douanes et armée.

PILIER 8

Défense militaire

Protection du territoire et des alliés.

CHRONOLOGIE RÉGLEMENTAIRE

Deux lois complètent le cadre de résilience luxembourgeois

Les lois du 5 mai 2026, publiées le 6 mai au Mémorial A 225 et 226, sont entrées en vigueur le 10 mai. Les obligations dépendent du type d'entité, de son classement et, pour certaines, de sa désignation individuelle sous CER.

5 MAI 2026

Signature par le Grand-Duc

Lois du 5 mai ; publication le 6 mai 2026.

10 MAI 2026 (EN VIGUEUR)

Loi sur la résilience (CER)

Résilience physique des entités critiques. Mesures de protection contre intrusion, sabotage et risques naturels.

10 MAI 2026 (EN VIGUEUR)

Loi cybersécurité (NIS-2)

Transposition nationale pour les entités essentielles et importantes. Gestion globale de risques obligatoire.

CER : analyse des risques sous 9 mois après notification ; chapitre 4 applicable en principe après 10 mois. Vérifier les exceptions. Évaluer séparément les obligations NIS-2.

EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

L’approche tous risques couvre les dangers physiques et numériques

UNE PROTECTION GLOBALE

Définition : tous risques

L’approche tous risques évalue les risques naturels et humains pertinents susceptibles de perturber les services essentiels. Les dépendances physiques, numériques, intersectorielles et transfrontières doivent être examinées ensemble.

Elle comprend notamment :
– Cybermenaces, sabotage et désinformation
– Incidents techniques et panne d’alimentation
– Catastrophes naturelles, canicules et inondations
– Risques internes et menaces d’initiés

EXIGENCES STRATÉGIQUES

Obligation légale de préparation

Les entités critiques mettent en œuvre des mesures adaptées et proportionnées à leur analyse des risques. Redondances, fournisseurs alternatifs et réserves peuvent y contribuer ; leur forme et leur ampleur suivent le besoin de protection.

Le contrôle d’accès comme lien :

Un accès non autorisé peut menacer l’IT et l’exploitation, par exemple par une intervention sur une baie serveur. Protection physique et sécurité numérique doivent être cohérentes. Le choix entre mécanique, organisation et électronique découle des risques, sans obligation technologique générale.

Onze secteurs NIS-2 en annexe I – vérifier CER séparément

01. Énergie
Électricité, gaz, pétrole, chaleur/froid, hydrogène

02. Transports
Air, rail, eau, route et transports publics

03. Secteur bancaire
Établissements de crédit dans le champ légal

04. Marchés financiers
Plateformes de négociation et contreparties centrales

05. Santé
Soins, recherche et fabrication concernés

06. Eau potable
Fourniture et distribution contrôlée

07. Eaux usées
Collecte, traitement et évacuation

08. Infrastructure numérique
Cloud, centres de données, DNS, services de confiance

09. Services gérés
Sécurité et support informatique B2B

10. Administration publique
Entités publiques concernées ; vérifier les exceptions

11. Espace
Infrastructures terrestres de communication satellitaire

NIS-2 : ILR ou CSSF selon compétence. CER possède sa propre annexe de 12 secteurs, dont l'alimentation et la gestion des déchets.

Sept autres secteurs élargissent le champ réglementaire

01. Poste et courrier
Services universels et acheminement de colis.

02. Gestion des déchets
Collecte, traitement et élimination concernés.

03. Industrie chimique
Fabrication, transport et distribution de substances.

04. Secteur alimentaire
Commerce de gros et transformation industrielle.

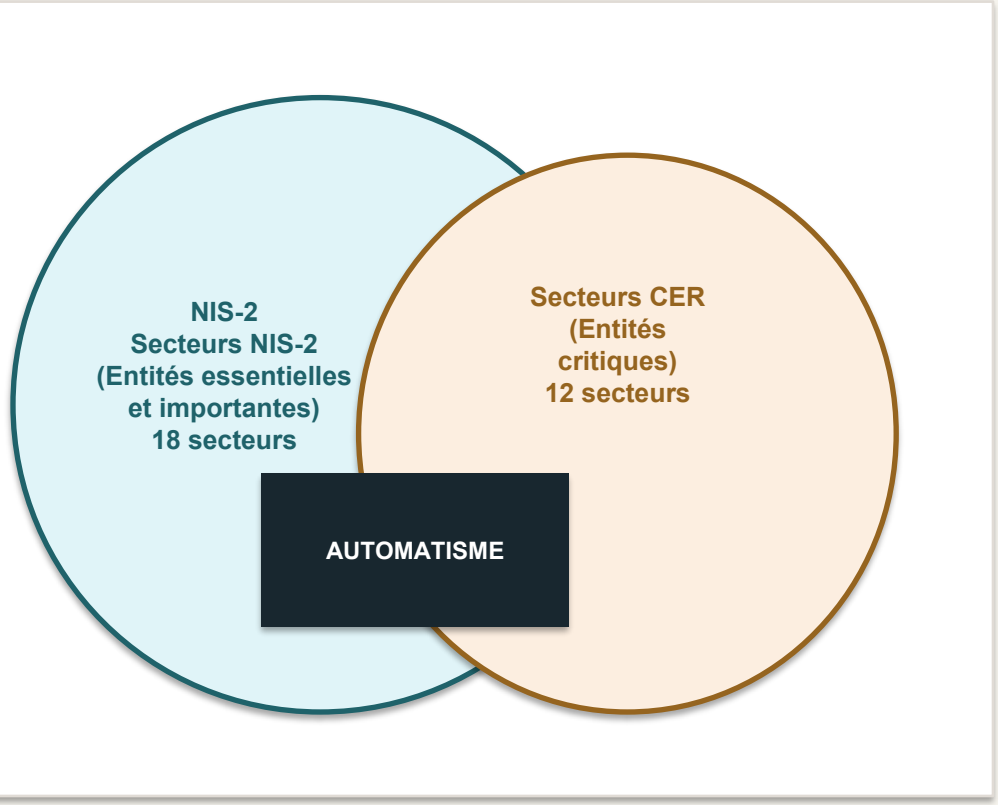
05. Industrie et fabrication
Dispositifs médicaux, IT, électronique et véhicules.

06. Services numériques
Moteurs de recherche, places de marché, réseaux sociaux.

07. Recherche et laboratoires
Organismes de recherche appliquée.

Précision sur le classement :
L'annexe II couvre en principe les entreprises moyennes et grandes des types mentionnés. Elles sont généralement importantes, sauf statut essentiel particulier. La supervision des entités importantes est ex post ; les obligations de sécurité et de notification s'appliquent néanmoins.

La désignation CER conduit au statut essentiel NIS-2



EFFET DE CLASSEMENT AUTOMATIQUE

Un mécanisme légal

Selon l'article 1, § 3, et l'article 11, § 1, point 6, de la loi luxembourgeoise NIS-2, pour les entités concernées :

Les entités désignées critiques sous CER sont essentielles au sens de NIS-2, quelle que soit leur taille.

Chaque cadre conserve ses obligations et compétences. Les entités essentielles relèvent d'une supervision NIS-2 active. Les règles particulières, notamment financières, doivent être examinées au cas par cas.

Trois autorités coordonnent la supervision au Luxembourg

ILR – RÉSEAUX ET INFORMATION

Supervision de la cybersécurité

Autorité de cybersécurité NIS-2 pour la plupart des secteurs réglementés.

Instruments :

– Contrôles sur site et à distance
– Audits réguliers et ciblés
– Scans de sécurité fondés sur les risques

HCPN – RÉSILIENCE NATIONALE

Supervision de la résilience physique

Le Haut-Commissariat à la Protection nationale est compétent pour la résilience physique (CER).

Instruments :

– Inspections et audits
– Demandes de preuves
– Accompagnement et exercices

CSSF – SECTEUR FINANCIER

Domaines attribués par la loi

La CSSF supervise les domaines financiers qui lui sont légalement attribués. CER et NIS-2 prévoient des règles particulières et des exceptions à examiner pour chaque entité.

À examiner :

– DORA : résilience opérationnelle numérique
– Équivalence pour chaque obligation
– Aucune exemption globale de principe

Direction : responsabilités, supervision et sanctions possibles

Amendes : art. 26 NIS-2 / art. 19 CER nationaux

Jusqu’à 10 M€

Ou 2 % du chiffre d’affaires mondial annuel, le montant le plus élevé étant retenu, pour les entités essentielles.

• Importantes : jusqu’à 7 M€ ou 1,4 % du CA mondial annuel, le montant le plus élevé étant retenu.
• CER : l’autorité compétente peut infliger une amende proportionnée jusqu’à 250 000 € pour les manquements visés.

Responsabilité de la direction

Responsabilité personnelle

Les organes de direction approuvent et supervisent les mesures NIS-2 et peuvent être tenus responsables des violations. Une formation régulière est obligatoire.

• Art. 13 NIS-2 : approbation, supervision et formation.
• Art. 22, § 5 : restrictions judiciaires des fonctions dirigeantes possibles sous conditions légales lorsque les mesures correctives échouent.
• Art. 22, § 4, point 8 : publication de certains aspects des violations pouvant être ordonnée.

CER et NIS-2 : distinguer déclencheurs et délais de suivi

PREMIÈRE NOTIFICATION

SOUS 24 HEURES

Dès connaissance : alerte précoce NIS-2 pour un incident important à l'autorité compétente ; notification CER pour une perturbation importante des services essentiels. Agir sans retard injustifié et vérifier séparément les deux circuits.

NIS-2 : NOTIFICATION D'INCIDENT

SOUS 72 HEURES

NIS-2 : actualiser gravité, impact et indicateurs de compromission disponibles. CER ne prévoit pas d'étape générale à 72 heures. Vérifier le délai particulier des services de confiance.

RAPPORTS DE SUIVI

DÉLAI DE 1 MOIS

NIS-2 : rapport final au plus tard un mois après la notification d'incident ; règles particulières si l'incident persiste. CER : rapport détaillé, le cas échéant, sous un mois après la première notification. Coordonner faits et communication.

Un accès physique peut contourner les protections numériques

EXEMPLE DE RISQUE : ACCÈS DIRECT AUX SYSTÈMES

Un accès non autorisé aux serveurs, automatismes ou câbles réseau peut compromettre la sécurité numérique.

Pare-feu, chiffrement et surveillance restent nécessaires. Des accès physiques contrôlés complètent leur protection. Le risque concret dépend du site, des systèmes et des mesures existantes.

Les limites des clés mécaniques

Les clés mécaniques exigent une gestion adaptée de la remise, du retrait et des preuves

Traçabilité :

Une serrure mécanique ne crée pas de journal numérique. Remise, retour et utilisation peuvent être documentés par l'organisation.

Perte d'une clé :

Une clé ne se bloque pas numériquement. Selon le risque, remplacement et mesures transitoires sont nécessaires ; évaluer protection contre la copie et gestion des clés.

Gestion des droits :

La mécanique n'applique pas automatiquement de plages horaires. Le besoin de protection détermine si des mesures organisationnelles suffisent ou si l'électronique est nécessaire.

Deux cadres exigent des mesures adaptées aux risques

LOI NIS-2 (CYBERRÉSILIENCE)

Luxembourg : art. 12, § 2, points 9–10

UE : art. 21, § 2, points i et j. Les entités essentielles et importantes doivent adopter des mesures adaptées et proportionnées, notamment :

Sécurité du personnel, contrôle d’accès, gestion des actifs et, le cas échéant, authentification multifacteur ou continue. La mise en œuvre technique suit les risques.

LOI CER (RÉSILIENCE PHYSIQUE)

Luxembourg : art. 12, § 1, points 2 et 5

UE : art. 13, § 1, points b et e. Les entités critiques prennent des mesures adaptées et proportionnées, notamment :

Protection physique des sites et infrastructures, contrôle des accès, sécurité du personnel et autorisations d’accès fondés sur l’analyse des risques.

Quatre étapes – la pertinence suit le besoin de protection

01

RÉACTIF(Mécanique)

Clé physique.

– Documenter remise et retour

– Organiser les limites horaires

– Évaluer perte et possibilité de copie

02

IDENTIFICATION(Électronique simple)

Carte ou support RFID.

– Tracer les événements selon le système

– Vérifier diffusion et effet du blocage

– Évaluer séparément l'intégration

03

DYNAMIQUE(Gouvernance des accès)

Droits par rôle et par horaire.

– Droits temporaires de maintenance

– Coordonner les départs avec les RH

– Prouver le retrait effectif

04

PROACTIF(Surveillance)

Surveillance adaptée au risque.

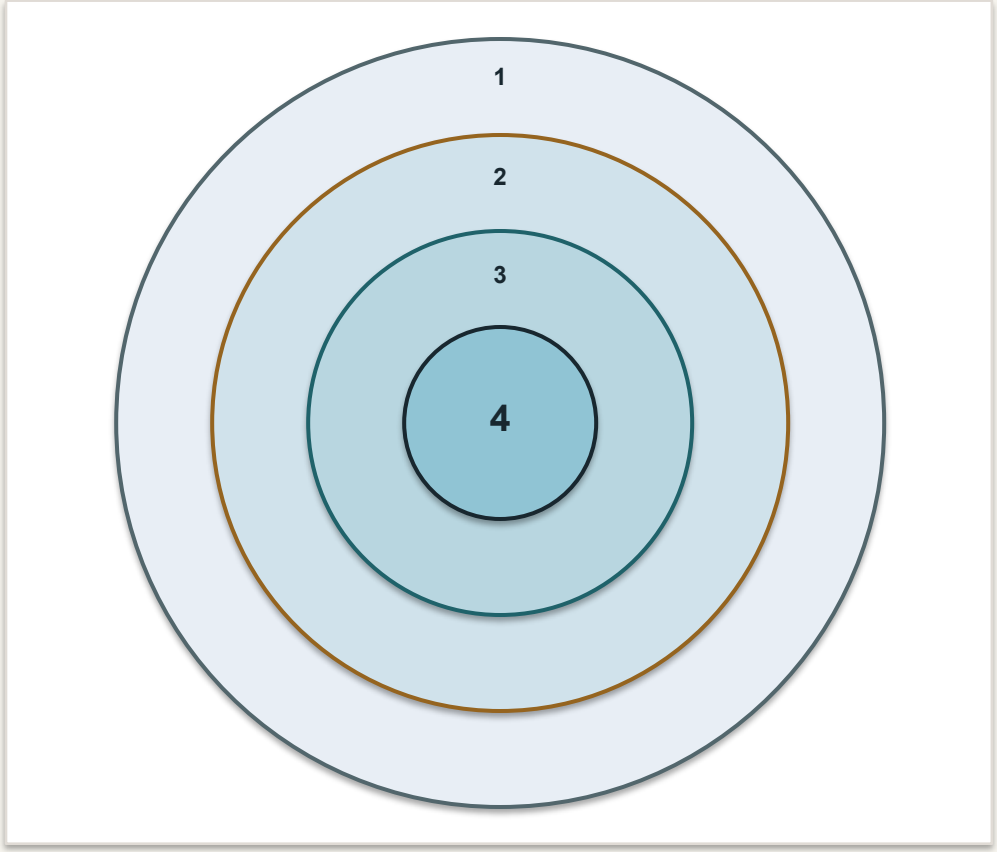
– MFA, par exemple carte et code

– Détecter les manipulations et réagir

– Tester le mode dégradé ; biométrie facultative

Aucune hiérarchie légale : état de l'art, pertinence et proportionnalité se démontrent en exploitation. La mécanique n'est pas exclue par principe.

Quatre couches de protection : exemple pour un site critique



EXEMPLE DE CONCEPTION · EN 50600-2-5 CONCERNE LES CENTRES DE DONNÉES

Zone 1 : périmètre extérieur

Clôtures, barrières et surveillance protègent le terrain. Premier filtre contre les accès non autorisés.

Zone 2 : enveloppe du bâtiment

Les portes extérieures contrôlées limitent l'accès. Autorisations du personnel, des visiteurs et prestataires selon mission, horaire et besoin de protection.

Zone 3 : locaux sensibles

Accès strictement encadré aux salles de contrôle, répartiteurs télécoms et locaux serveurs, pour éviter les déplacements intérieurs non contrôlés.

Zone 4 : baie informatique

Protéger les composants critiques de manière ciblée. Une authentification multifacteur peut être adaptée, par exemple carte et code. La biométrie n'est pas une obligation générale.

La décision sur les antécédents est valable cinq ans

1. Demande et critères

Base légale (art. 13)

Les entités critiques demandent une vérification pour les fonctions sensibles visées par la loi. L'autorité compétente approuve au préalable les catégories de personnes concernées.

Consentement écrit ou électronique et pièces de l'art. 13, § 2, sont requis, notamment identité, casier judiciaire, emplois et études.

2. Autorité exécutante

Missions et recherches

La Police grand-ducale réalise la vérification selon l'article 13.

Elle examine les informations prévues par la loi sur les cinq années précédant la demande et transmet au ministre un avis sur le risque potentiel pour la sécurité.

3. Décision et validité

Décision du ministre (art. 14)

Le ministre statue sur le risque. La personne reçoit la décision motivée ; l'entité reçoit la décision sans les informations personnelles de l'avis policier.

Validité : cinq ans. Demander le renouvellement six à quatre mois avant l'échéance (art. 14, § 5).

Comparer mécanique et électronique par des fonctions démontrées

Exigence (NIS-2 / CER)	Systèmes de fermeture mécaniques	Contrôle d’accès électronique	À vérifier
Traçabilité	Pas de journal numérique dans la serrure ; preuves organisationnelles possibles	Journaux selon le système ; vérifier exhaustivité, données personnelles et horodatage	VÉRIFIER VÉRIFIER
Retrait effectif après perte	Pas de blocage numérique individuel ; remplacement et mesures selon le risque	Délai selon architecture et transmission ; tester l’effet sur la serrure	VÉRIFIER VÉRIFIER
Attribution par rôle et horaire	Attribution par rôle possible ; limites horaires à organiser	Droits dynamiques pour les personnes et créneaux de maintenance	VÉRIFIER VÉRIFIER
Preuve de diligence	Démontrer pertinence et mesures complémentaires dans le concept concret	Prouver configuration et exploitation efficaces ; aucune exonération automatique	VÉRIFIER VÉRIFIER

Quatre étapes pratiques vers la conformité cyber-physique

ÉTAPE 01

Enregistrement auprès de l’ILR

Vérifier secteur, type, taille et cas particuliers. Les entités concernées s’enregistrent auprès de l’ILR ; maintenir les informations et la compétence à jour.

ÉTAPE 02

Analyse globale des risques

Mener ensemble les analyses cyber et les évaluations des périmètres physiques selon l’approche tous risques.

ÉTAPE 03

Modernisation des accès

Déduire le concept d’accès des risques et du zonage. Choisir et tester des mesures mécaniques, organisationnelles et électroniques adaptées.

ÉTAPE 04

Intégration dans le SMSI

Intégrer les journaux d’accès physique au système de management de la sécurité de l’information, par exemple ISO 27001.

La SNR prévoit des délégués à la résilience dans les organismes publics

LE RÉSEAU NATIONAL DE RÉSILIENCE

Le délégué à la résilience

Pour professionnaliser la préparation administrative au Luxembourg, la stratégie nationale de résilience prévoit une mesure structurelle centrale :

✓ Des délégués à la résilience dans les institutions publiques.

✓ Un soutien à la continuité d'activité et à la préparation.

✓ Des réseaux et exercices pour coopérer en temps normal et en crise.

SYNERGIES CIVILO-MILITAIRES (PILIERS 7 ET 8)

Soutien du pays hôte (HNS)

Le Luxembourg joue un rôle de transit pour le matériel et les troupes de l'OTAN. La préparation civile facilite notamment les mouvements par rail, route et aéroport.

Soutien civil aux forces armées :

La stratégie nationale relie préparation civile et capacité d'action des alliés. Les contributions concrètes des exploitants critiques sont à coordonner avec les autorités et à planifier selon les règles applicables.

De la gestion des bâtiments à la stratégie de direction

L’alliance cyber-physique comme protection stratégique

• **Responsabilité commune : IT, exploitation et sécurité physique coordonnent risques et dépendances. CER et NIS-2 conservent leurs exigences et compétences propres.**

• **Mission de la direction : approuver les mesures, superviser leur mise en œuvre et assurer la formation. Documenter les décisions adaptées aux risques et les contrôles efficaces.**

• **Des accès efficaces : combiner mécanique, organisation et électronique. Tester retrait des droits, mode dégradé et preuves en exploitation, puis améliorer en continu.**

La maturité démontrée peut influencer la supervision

STRATÉGIE NATIONALE DE RÉSILIENCE DES ENTITÉS CRITIQUES

Démontrer la maturité – sans exemption automatique d’audit

La stratégie nationale prévoit une supervision modulaire tenant compte de la maturité et de la criticité. Une participation active à la culture de résilience peut être reconnue :

Les preuves peuvent inclure communication proactive, transparence, certification ISO 22301 ou approches comparables, formations et exercices. L’autorité les apprécie dans leur contexte.

➔ Des allègements ciblés de supervision sont possibles. Aucun droit général à des audits plus espacés ni aucune exemption automatique des obligations légales.