LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

LËTZ PREPARE !
STRATÉGIE NATIONALE DE RÉSILIENCE

Stratégie nationale pour renforcer

LA RÉSILIENCE DES ENTITÉS CRITIQUES

LETZPREPARE.LU

Sommaire

Stratégie nationale pour renforcer la résilience des entités critiques — Version française
Approuvée et rendue exécutoire par le Conseil de gouvernement du 16 décembre 2025

Introduction

Nous évoluons dans une époque marquée par des polycrises, où les menaces sont multiples, interconnectées et en constante mutation. Qu'elles soient d'origine technologique, économique, naturelle, physique ou cyber, qu'elles soient accidentelles ou malveillantes, ces crises imposent une réévaluation permanente de notre niveau de préparation, tant au niveau sociétal qu'étatique.

Dans ce contexte, la sauvegarde des intérêts vitaux et des besoins essentiels de la population et du pays repose en grande partie sur la capacité des infrastructures et entités critiques à faire face à l'ensemble des risques - qu'ils soient contemporains ou émergents, connus ou imprévus. Chargées de soutenir les fonctions sociétales vitales, ces entités doivent faire preuve d'une résilience renforcée, afin de prévenir, atténuer et neutraliser tout risque de discontinuité des services essentiels, y compris en situation de crise.

Le Luxembourg a adopté en octobre 2025 sa Stratégie nationale de résilience, structurée autour de huit piliers interdépendants. Alors que la résilience des entités critiques est abordée de manière transversale dans plusieurs de ces piliers, elle trouve son ancrage principal dans le pilier 3, consacré aux biens et services essentiels ainsi qu'aux infrastructures et entités critiques.

La présente Stratégie nationale pour renforcer la résilience des entités critiques s'inscrit dans la continuité des objectifs de la Stratégie nationale de résilience. À l'instar de cette dernière, la présente stratégie poursuit une approche pangouvernementale ainsi qu'une approche tous secteurs et tous risques.

Pour être pleinement opérationnelle, la présente stratégie intègre le contexte européen et international dans lequel évolue le Luxembourg. Au niveau de l'UE, la protection des infrastructures critiques et la résilience des entités critiques assurent une fonction cruciale dans le bon fonctionnement du marché intérieur. Au niveau de l'OTAN, la préparation du secteur civil est considérée comme un pilier de la résilience nationale et un élément facilitateur critique de la défense collective de l'Alliance.

Conformément à l'article 4 de la Directive (UE) 2022/2557 sur la résilience des entités critiques, chaque État membre de l'Union européenne doit adopter une stratégie visant à renforcer la résilience des entités critiques. Le présent document répond à cette obligation. Sa structure suit la liste des éléments qu'une telle stratégie doit contenir selon la Directive.

Objectifs stratégiques, priorités et principes fondamentaux

Le présent chapitre décrit les objectifs stratégiques, les priorités et les principes fondamentaux de la stratégie nationale pour renforcer la résilience des entités critiques[1].

Objectifs stratégiques

La notion de « résilience des entités critiques » remplace celle de « protection des infrastructures critiques », en élargissant le champ d'action à une approche systémique. Comme la précédente, elle est ancrée dans le Concept de protection nationale et constitue un pilier de la résilience globale de la société[2].

La résilience des infrastructures et entités critiques est fondamentale pour le maintien des fonctions sociétales vitales. Par leur désignation, les entités critiques sont reconnues comme étant indispensables à la sauvegarde des intérêts vitaux et des besoins essentiels du pays et de la population. Le pilier 3 de la Stratégie nationale de résilience reconnaît explicitement que les entités critiques sont au cœur de la résilience nationale. Dès lors, les objectifs stratégiques visant à renforcer leur résilience se confondent naturellement avec ceux de la Stratégie nationale de résilience, dans une logique de cohérence et d'interdépendance.

Objectifs stratégiques :

- Assurer les fonctions sociétales vitales
- Garantir le fonctionnement de l'État et la protection de la démocratie et de l'état de droit
- Consolider le cycle de la gestion de crise
- Décloisonner l'approche des différents acteurs civils, publics et privés
- Renforcer la coopération civilo-militaire
- Favoriser une culture de la préparation et de la résilience individuelle et collective
- Consolider le partenariat public-privé
- Accroître la résilience et la compétitivité de l'économie luxembourgeoise
- Renforcer les capacités de cyberrésilience du Luxembourg
- Assurer une coordination plus étroite avec les alliés et les organisations européennes et internationales.

Priorités

La Stratégie nationale pour renforcer la résilience des entités critiques s'articule autour des trois priorités suivantes :

Priorité 1 : Renforcer la conscience de la situation

Afin de pouvoir mitiger les effets en cascade d'une perturbation de services essentiels, les interdépendances transfrontalières et transsectorielles entre les infrastructures critiques et les secteurs de l'énergie, des transports, des banques, des infrastructures du marché financier, de l'eau potable, des eaux usées, des déchets, des denrées alimentaires, de la santé, de l'espace, et des infrastructures numériques, et de l'administration publique seront cartographiées.

La veille stratégique des risques sera renforcée et dotée d'un outil dédié et façonnable aux besoins spécifiques des entités critiques et des autorités sectorielles et fonctionnelles.

1 Article 4, §2, point a) de la Directive (UE) 2022/2557.

2 Au niveau du cadre légal, le domaine de la « Protection des infrastructures critiques » prend l'appellation de la « Résilience des entités critiques », suite à la modification de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale par la loi sur la résilience des entités critiques.

Les échanges entre les autorités sectorielles, fonctionnelles et compétentes portant sur les menaces, les vulnérabilités, les évaluations des risques actuels et émergents ainsi que sur les retours d'expérience, notamment des crises, des incidents et des exercices, seront organisés d'une manière plus structurée.

Un système de collecte de données qui permettra de mesurer la performance de la protection et de la continuité d'activité des infrastructures critiques sera mis en place. Le partage de ces données avec les autorités compétentes leur offrira une meilleure compréhension des risques de perturbation des services essentiels et leur permettra de déterminer des options pour renforcer la résilience globale des entités critiques.

Priorité 2 : Renforcer la résilience systémique

Une approche systémique de la résilience des entités critiques sera poursuivie. Cette approche de résilience systémique privilégie :

- la modularité (capacité à segmenter un système en unités autonomes et interconnectées, afin que la défaillance d'un module n'entraîne pas l'effondrement du système entier),
- la distribution (décentralisation des fonctions pour éviter les points de défaillance uniques),
- la redondance (duplication des éléments critiques pour assurer la continuité),
- la diversité (hétérogénéité des éléments pour mieux faire face à une variété de menaces, notamment dans la chaîne d'approvisionnement) et
- l'adaptabilité (capacité d'adaptation dynamique à des conditions changeantes).

Dans ce prolongement, le principe de résilience intégrée dès la conception (*resilience by design*) devra orienter les politiques sectorielles relatives aux services essentiels. Lors de la conception d'un système, d'un réseau ou d'une autre infrastructure fournissant un service essentiel, il conviendra de prévenir toute concentration fonctionnelle susceptible de créer un point de défaillance unique et d'identifier puis réduire ceux qui existent.

La planification nationale des solutions de continuité des services essentiels, en complément des dispositifs déjà mis en place par les entités critiques, sera optimisée. Les besoins en stocks stratégiques seront réévalués en prenant en considération les interdépendances transfrontalières et transsectorielles, les capacités de continuité et d'adaptation dont disposent les entités critiques, ainsi que la priorisation des infrastructures critiques. Ceci contribuera à la résilience systémique des services essentiels et des entités critiques.

Une meilleure interconnexion entre les autorités compétentes, sectorielles et fonctionnelles contribue au renforcement progressif de la résilience systémique. Ce réseautage institutionnel vise à fluidifier les échanges d'informations et les réponses aux perturbations. En favorisant une gouvernance collaborative, cette approche permet de mieux anticiper les vulnérabilités systémiques et d'optimiser les capacités d'adaptation à l'échelle nationale.

La résilience systémique des entités critiques s'inscrit dans un maillage régional et international. Le Luxembourg renforcera la coopération transfrontalière avec ses voisins (Belgique, France, Allemagne) à travers les mécanismes de coordination existants, notamment BENELUX (Senn-Crise), en particulier dans les secteurs de l'énergie, des transports et des télécommunications.

Une articulation étroite avec les dispositifs européens, en particulier le Schéma directeur de l'UE pour les perturbations transfrontalières, les travaux du Groupe sur la résilience des entités critiques, les échanges d'informations sur les menaces ciblant les infrastructures critiques et les exercices européens de simulation de crise, sera maintenue.

Enfin, la stratégie s'aligne sur les sept exigences de base en matière de résilience nationale de l'OTAN visant la préparation du secteur civil par, notamment, la continuité des services essentiels et le soutien du secteur civil aux opérations militaires. Une intégration des entités critiques et de la continuité des services essentiels aux futurs plans de défense sera analysée. Après identification des besoins de support civil pour l'Armée luxembourgeoise dans l'éventualité d'une crise de défense ou d'un conflit armé, les capacités des entités critiques à soutenir les opérations militaires seront cartographiées et, si nécessaire, renforcées.[3]

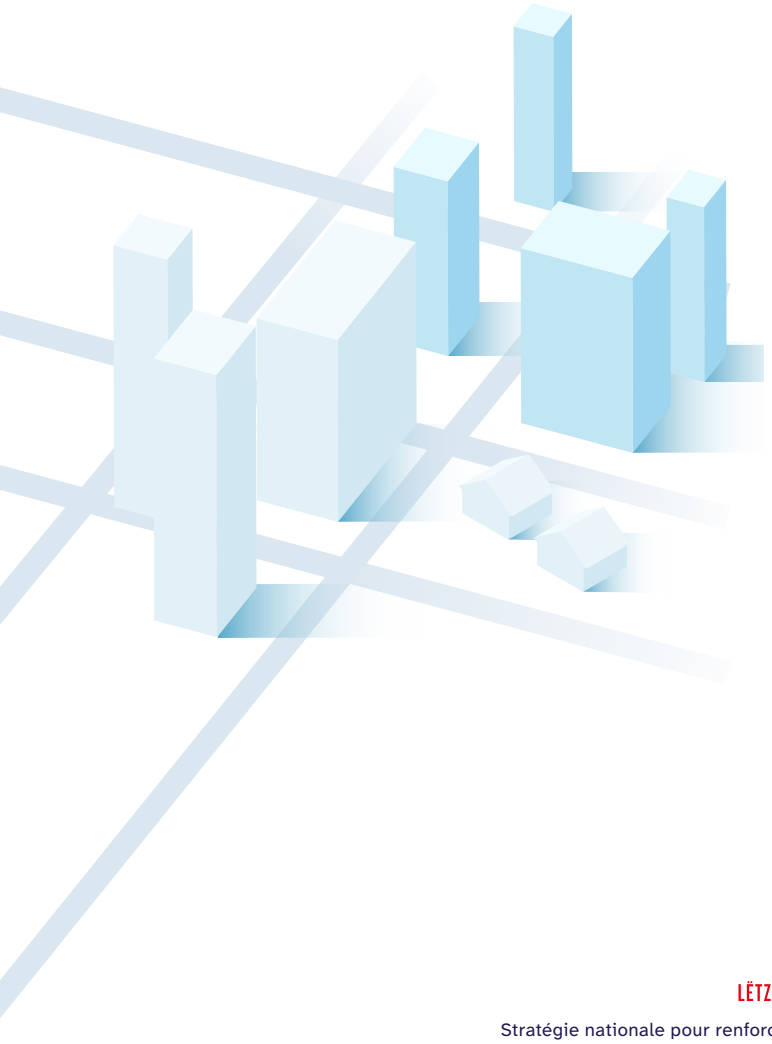
3 La préparation du secteur civil comprend trois fonctions essentielles : la continuité des pouvoirs publics, la continuité des services essentiels à la population et le soutien du secteur civil aux opérations militaires. Ces fonctions critiques ont été traduites en sept exigences de base pour la résilience nationale, à l'aune desquelles les Alliés peuvent mesurer leur niveau de préparation. Source : https://www.nato.int/cps/fr/natohq/topics_132722.htm

Priorité 3 : Renforcer la culture de résilience

Le développement d'une culture de résilience constitue un levier stratégique pour renforcer la capacité des entités critiques à faire face aux perturbations. Les autorités compétentes CER encouragent son intégration progressive dans les politiques, processus et pratiques internes des entités critiques. Ce renforcement est soutenu par des formations et des activités d'apprentissage en matière de continuité d'activité et de gestion de crise, organisées par les autorités compétentes CER.

Les activités de réseautage entre entités critiques seront poursuivies afin d'établir les relations directes entre acteurs clés en amont d'une crise et de faciliter le partage d'expériences, la mutualisation des bonnes pratiques et la réduction des vulnérabilités liées aux interdépendances.

La participation volontaire aux activités de soutien constitue un principe fondamental. Toutefois, une implication active et démontrée dans le renforcement de la culture de résilience pourra être valorisée dans l'évaluation du niveau de maturité d'une entité critique. Cette reconnaissance pourra se traduire par un allègement ciblé des mesures de supervision, notamment en matière d'audit.



Principes fondamentaux

La résilience des entités critiques : un pilier du Concept de protection nationale

La loi sur la résilience des entités critiques, transposant la Directive (UE) 2022/2557 sur la résilience des entités critiques, a modifié la loi du 23 juillet 2016 portant création du Haut-Commissariat à la protection nationale : l'attribution du Haut-Commissariat à la protection nationale en matière de « protection des infrastructures critiques » est substituée par sa nouvelle attribution en matière de « résilience des entités critiques », tandis que les obligations et modalités liées à la « protection des infrastructures critiques » du Chapitre 4 de la loi organique du Haut-Commissariat à la protection nationale ont été transférées dans la loi sur la résilience des entités critiques. Ainsi, « la résilience des entités critiques » remplace « la protection des infrastructures critiques » comme élément fondamental au cœur du Concept de protection nationale.

Le but ultime de la Protection des infrastructures critiques, voire de la Résilience des entités critiques, demeure inchangé : sauvegarder « les intérêts vitaux et les besoins essentiels du pays et de sa population », notion-racine à la fois de la définition d'une « crise » et de l'ancienne définition d'une « infrastructure critique ». Comme ce dernier terme est dorénavant défini en relation avec la notion du « service essentiel » et le « service essentiel » renvoie au « maintien de fonctions sociétales vitales », la loi sur la résilience des entités critiques établit le lien entre le « maintien des fonctions sociétales vitales » et « les intérêts vitaux et les besoins essentiels du pays et de sa population » afin de préserver la logique conceptuelle. Dans cette continuité, une infrastructure est recensée et désignée comme critique seulement si son dysfonctionnement entraîne une « crise » au sens du Concept de la protection nationale. Sinon, elle n'est pas reconnue comme critique - même si son service facilite la gestion d'une crise. Seule une entité qui exploite une infrastructure critique peut être désignée comme critique. Ainsi les termes « opérateur d'infrastructure critique » et « entité critique » sont interchangeables. Les critères de criticité des effets perturbateurs, pris en compte lors du recensement des entités critiques, sont assortis de seuils reflétant le potentiel de crise.

La résilience : un concept holistique

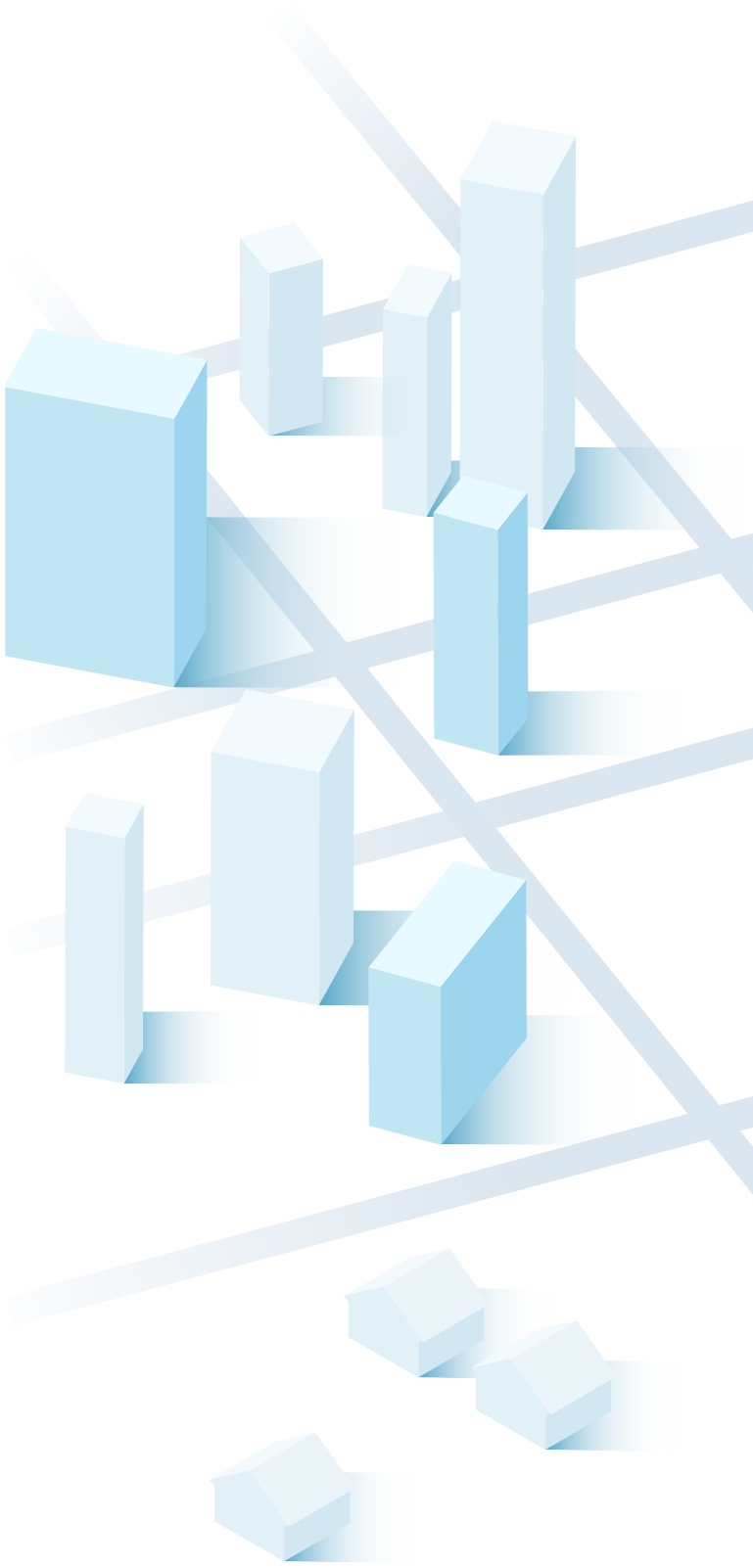
La résilience est appréhendée de manière holistique, comme un concept global et transversal dépassant les seules considérations techniques ou sectorielles. Elle désigne la capacité des entités critiques à anticiper, absorber et s'adapter à toute perturbation, indépendamment de son origine, qu'elle soit accidentelle ou intentionnelle, physique ou cyber. Pour développer cette capacité, les entités critiques mettront en œuvre des mesures de résilience prévues par la loi sur la résilience des entités critiques (CER), ainsi que des mesures de cybersécurité prévues par la loi sur la cybersécurité (NIS2). Complémentaires et interdépendantes, ces deux lois constituent un socle cohérent pour renforcer la sécurité et la continuité des services essentiels.

Le principe de la résilience intégrée dès la conception

La résilience des entités critiques repose sur le principe de la sécurité et de la résilience *by design*, c'est-à-dire intégrées dès les premières phases de conception et incarnées dans l'architecture même des systèmes, des infrastructures et des processus.

Plutôt que d'ajouter des mesures a posteriori, cette approche vise à anticiper les risques et à intégrer des mécanismes de protection dès l'origine. Elle se traduit par des choix de conception favorisant la modularité, la distribution, la redondance, la diversité et l'adaptabilité, afin de garantir la sécurité en cas de défaillance et la continuité des services essentiels.

Ces principes s'appliquent tant aux dimensions physiques que cyber des infrastructures critiques. En adoptant cette logique, les entités renforcent leur capacité de prévention, d'anticipation et de gestion de crise, consolidant ainsi leur résilience systémique.



Cadre de gouvernance

Le présent chapitre décrit le cadre de gouvernance de la résilience des entités critiques[4].

Autorités compétentes CER et NIS2

Par « autorité compétente CER », on entend une autorité nationale compétente chargée de la résilience et de la supervision en vertu de la loi sur la résilience des entités critiques (« loi CER »), qui transpose la Directive (UE) 2022/2557 sur la résilience des entités critiques (« Directive CER »). Cette loi désigne le Haut-Commissariat à la protection nationale et la Commission de Surveillance du Secteur Financier comme autorités compétentes CER et détermine leurs rôles et responsabilités dans ce contexte. Elle désigne aussi le Haut-Commissariat à la protection nationale comme point de contact unique chargé d'exercer une fonction de liaison afin d'assurer la coopération transfrontière dans le cadre de la loi CER.

Par « autorité compétente NIS2 », on entend une autorité nationale compétente chargée de de la cybersécurité et de la supervision en vertu de la loi concernant des mesures destinées à assurer un niveau élevé de cybersécurité (« loi NIS2 »), qui transpose la Directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (« Directive NIS2 »). La loi NIS2 désigne l'Institut luxembourgeois de régulation et la Commission de Surveillance du Secteur Financier comme autorités compétentes NIS2 et détermine leurs rôles et responsabilités dans ce contexte. Elle désigne aussi le Haut-Commissariat à la protection nationale comme point de contact unique chargé d'exercer une fonction de liaison afin d'assurer la coopération transfrontière dans le cadre de la loi NIS2.

Dans une approche holistique de la résilience, il incombe au Haut-Commissariat à la protection nationale d'assurer la coordination globale en matière de résilience des entités critiques. Il s'agit d'une attribution légale liée au Concept de protection nationale[5].

La présente Stratégie nationale pour renforcer la résilience des entités critiques, élaborée par le Haut-Commissariat à la protection nationale en coordination étroite avec la Commission de Surveillance du Secteur Financier, est proposée pour approbation au Gouvernement, suivant une approche pangouvernementale. Ceci favorise une coordination horizontale entre les ministères et les administrations publiques et s'inscrit dans une dynamique de concertation préalable à toute décision gouvernementale.

Le Haut-Commissariat à la protection nationale a la responsabilité de procéder à l'évaluation des risques d'État membre, visée par l'Article 5 de la Directive CER.

Dans l'exercice de ses missions en matière de résilience des entités critiques ou de protection des infrastructures critiques, le Haut-Commissariat à la protection nationale veille à maintenir une collaboration étroite tant avec la Commission de Surveillance du Secteur Financier et l'Institut luxembourgeois de régulation qu'avec les autorités sectorielles et fonctionnelles concernées. Le cadre de gouvernance de la résilience des entités critiques inclut en particulier un cadre d'action pour la coordination entre les autorités compétentes CER et NIS2, décrit plus loin dans un chapitre y dédié.

Enfin, en tant que point de contact unique chargé d'exercer une fonction de liaison afin d'assurer la coopération transfrontière en matière de résilience des entités critiques, le Haut-Commissariat à la protection nationale remplit la fonction d'interlocuteur unique auprès de la Commission européenne, notamment au Groupe sur la résilience des entités critiques, et des autres États membres de l'Union européenne, y compris pour les mécanismes de notification des incidents avec effet transfrontalier dans le contexte de la Directive CER et dans le contexte de la Recommandation du Conseil C/2024/4371 du 25 juin 2024 relative à un schéma directeur visant à coordonner au niveau de l'Union la réponse en cas de perturbations des infrastructures critiques ayant une dimension transfrontière notable, « Schéma directeur ».

4 Article 4, §2, point b) de la Directive CER 2022/2557.

5 Cette responsabilité s'exerce en complémentarité avec les autorités de tutelle, qui conservent pleinement leurs compétences et seront désignées dans le cadre de la présente stratégie comme autorités sectorielles, auxquelles il sera fait référence plus loin.

La répartition des secteurs entre le Haut-Commissariat à la protection nationale et la Commission de Surveillance du Secteur Financier est comme suit :

- Haut-Commissariat à la protection nationale : secteurs de l'énergie, du transport, de la santé, de l'eau potable, des eaux résiduaires, de l'administration publique, de l'espace, des denrées alimentaires, des déchets et des infrastructures numériques (pour les activités qui ne tombent pas sous la surveillance de la Commission de Surveillance du Secteur Financier) ;
- Commission de Surveillance du Secteur Financier : secteur bancaire, secteur des infrastructures des marchés financiers et secteur des infrastructures numériques (pour les activités qui tombent sous sa surveillance).

Pour les secteurs respectifs, chaque autorité compétente CER est responsable du recensement des entités critiques, de leur soutien et de leur supervision.

Les attributions en matière de résilience des entités critiques du Haut-Commissariat à la protection nationale sont définies par la loi sur la résilience des entités critiques, tandis que celles de la Commission de Surveillance du Secteur Financier sont précisées notamment par le règlement DORA (*Digital Operational Resilience Act*), ainsi que dans d'autres textes applicables au secteur financier.

Dans le cadre des échanges sur les plans de résilience des entités critiques, le Haut-Commissariat à la protection nationale sollicite les avis et expertises de la part des autorités sectorielles et fonctionnelles en raison de leurs compétences spécifiques dans les domaines concernés.

Autorités sectorielles

Le terme « autorité sectorielle » réfère à une autorité nationale compétente pour la régulation, la supervision ou la coordination d'un secteur économique spécifique, conformément aux législations sectorielles en vigueur. Il s'agit du ministre – ou de son délégué – compétent pour le secteur, sous-secteur ou service essentiel en question, conformément à l'organisation du Gouvernement et à la législation sectorielle.

Les autorités sectorielles contribuent à la mise en œuvre de la présente stratégie en partageant leur expertise sectorielle avec le Haut-Commissariat à la protection nationale.

Leur contribution inclut :

- des éléments d'évaluation des risques sectoriels ;
- des éléments d'informations pour identifier des infrastructures et entités en relation avec les critères de recensement ;
- des éléments d'informations concernant les éventuelles exigences sectorielles en matière de résilience ;
- des éléments d'analyse des incidents ayant eu un impact sur le secteur, sous-secteur ou service essentiel en question ;
- des éléments pour évaluer la satisfaction des exigences sectorielles par les mesures de résilience mises en place par les entités critiques.

La liste des autorités sectorielles se trouve en annexe.

Autorités fonctionnelles

Le terme « autorité fonctionnelle » réfère à un membre du Gouvernement ou à son délégué / une autorité nationale/ compétent[e] pour la sécurité nationale, la défense, la sécurité intérieure, la sécurité civile ou la gestion de crises. Les autorités fonctionnelles contribuent à la mise en œuvre de la présente stratégie en partageant leur expertise fonctionnelle avec le Haut-Commissariat à la protection nationale.

Leur contribution inclut :

- une évaluation des menaces à la sécurité nationale, la défense, la sécurité intérieure ou la sécurité civile respectivement ;
- des éléments d'informations concernant les éventuelles exigences fonctionnelles en matière de résilience ;
- des éléments d'analyse des incidents ayant eu un impact sur la sécurité nationale, la défense, la sécurité intérieure ou la sécurité civile respectivement ;
- des éléments pour évaluer la satisfaction des exigences fonctionnelles par les mesures de résilience mises en place par les entités critiques.

La liste des autorités fonctionnelles se trouve en annexe.

Entités critiques

Conformément au principe fondamental de la protection des infrastructures critiques, une entité est désignée comme étant critique seulement si le dysfonctionnement de son infrastructure a des effets perturbateurs assimilés à une crise. Le rôle des entités critiques réside dans le fait que, par la fourniture d'un ou de plusieurs services essentiels, elles contribuent directement à la sauvegarde des intérêts vitaux et des besoins essentiels du pays et de la population. À ce titre, elles constituent des acteurs clés dans le maintien des fonctions sociétales vitales et donc de la protection nationale et de la résilience nationale.

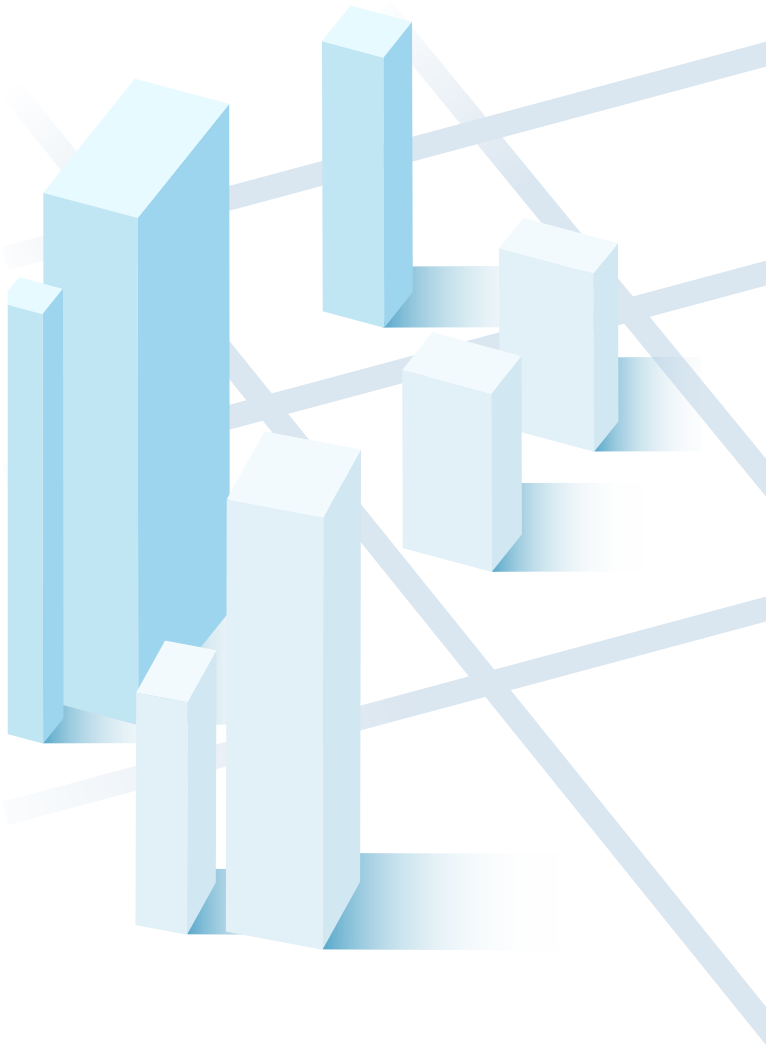
Formellement, pour être considérée comme critique, une entité doit remplir simultanément trois conditions :

1. elle fournit un ou plusieurs services essentiels ;
2. elle exerce ses activités sur le territoire luxembourgeois et son infrastructure critique y est également située et
3. un incident [événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel] aurait des effets perturbateurs importants sur la fourniture par l'entité d'un ou de plusieurs services essentiels ou sur la fourniture d'autres services essentiels.

Au niveau des responsabilités, les entités critiques assument, aux côtés des autorités compétentes CER, sectorielles et fonctionnelles, une responsabilité partagée en matière de continuité des services essentiels. Leur responsabilité s'étend de la protection de leur infrastructure critique à la garantie de la continuité des services essentiels qu'elles assurent.

Les obligations légales des entités critiques sont stipulées d'une part par la loi sur la résilience des entités critiques et d'autre part par la loi concernant des mesures destinées à assurer un niveau élevé de cybersécurité. Ces obligations s'ajoutent à celles stipulées par les législations sectorielles[6]. Ne sont pas soumises aux obligations prévues par la loi sur la résilience des entités critiques, les entités critiques recensées :

- dans le secteur bancaire ;
- dans le secteur des instruments des marchés financiers ;
- dans le secteur des infrastructures numériques pour les activités qui tombent sous la surveillance de la Commission de Surveillance du Secteur Financier ;
- dans le secteur de l'administration publique qui exercent des activités dans les domaines de la défense et de la sécurité nationale.



6 Lorsque des actes juridiques sectoriels de l'Union européenne imposent aux entités critiques des exigences de résilience ayant un effet au moins équivalent à celles prévues par la loi sur la résilience des entités critiques, les dispositions correspondantes, y compris celles relatives à la supervision et à l'exécution, ne s'appliquent pas. Les actes reconnus comme équivalents sont fixés par règlement grand-ducal.

Mesures nécessaires pour renforcer la résilience globale des entités critiques

Ce chapitre élabore les mesures nécessaires afin de renforcer la résilience globale des entités critiques[7].

Créer un cycle stratégique de résilience des entités critiques

Afin d'optimiser les flux d'informations entre autorités compétentes CER, sectorielles et fonctionnelles, un cycle pluriannuel de planification et de supervision pour la résilience des entités critiques sera instauré. Il structurera dans le temps les contributions des autorités sectorielles et fonctionnelles au niveau de l'évaluation des risques CER, du recensement des infrastructures et entités critiques, de la formulation des exigences de sécurité et de résilience et de la supervision des entités critiques.

Optimiser l'évaluation des risques CER

Conformément à l'article 5 de la Directive CER, l'évaluation des risques CER est utilisée pour recenser les entités critiques et pour les aider à adopter des mesures de résilience. Lors de l'évaluation des risques CER une approche « tous secteurs » est suivie : à partir de l'ensemble des activités économiques[8], les services qui soutiennent le maintien des fonctions sociétales vitales sont recensés comme services essentiels. Cette liste nationale des services essentiels comprend les services essentiels identifiés par la Commission européenne[9].

Lors de cette évaluation, les menaces susceptibles d'affecter la continuité des services essentiels sont identifiées et hiérarchisées. Une approche semi quantitative et alignée sur l'ISO 31000 est suivie afin de produire des résultats comparables et vérifiables.

Cette évaluation s'appuie sur plusieurs sources complémentaires : l'évaluation nationale des risques, l'évaluation des risques générale effectuée en vertu du mécanisme de protection civile de l'UE, les évaluations de risques effectuées par les autorités sectorielles et fonctionnelles, les évaluations de risques réalisées par les entités critiques, l'évaluation des incidents notifiés aux autorités compétentes CER, ainsi que les informations provenant des autres États membres concernant les risques transfrontaliers.

L'analyse repose sur deux critères fondamentaux : la vraisemblance d'occurrence et l'impact sur des sous-critères déterminés. La vraisemblance et l'impact permettent de positionner chaque risque dans une matrice de risques, outil central pour déterminer les niveaux de risque et pour hiérarchiser les menaces. Les résultats sont ensuite croisés avec le degré de dépendance des services essentiels, ce qui met en évidence les secteurs les plus critiques, notamment ceux caractérisés par de fortes interdépendances ou par des opérateurs uniques.

L'évaluation des risques CER complète le registre national des risques et contribue à la planification de la résilience nationale dans le contexte de la Stratégie nationale de résilience. Pour optimiser ce processus, les référentiels d'évaluation de l'évaluation des risques CER et de l'évaluation des risques nationale seront harmonisés. Les flux d'informations qui alimentent l'évaluation des risques CER seront synchronisés dans le cycle stratégique de résilience des entités critiques.

7 Article 4, §2, point c) de la Directive CER 2022/2557.

8 Voir la nomenclature NACELUX Rév. 2.

9 Règlement délégué (UE) 2023/2450 de la Commission du 25 juillet 2023 complétant la directive (UE) 2022/2557 du Parlement européen et du Conseil en établissant une liste de services essentiels.

Cartographier les dépendances et interdépendances

Afin d'approfondir l'analyse des risques systémiques et des effets en cascade, et de mieux les anticiper, une cartographie nationale détaillée des dépendances et interdépendances transsectorielles et transfrontières sera élaborée.

Cette cartographie visera à identifier les relations fonctionnelles critiques entre secteurs, ainsi qu'entre acteurs situés au-delà des frontières nationales. Elle permettra de visualiser les points de défaillance uniques, de repérer les chaînes d'approvisionnement critiques et de mieux comprendre les dynamiques de propagation en cas de perturbation.

Pour ce faire, une méthodologie commune, alignée sur des normes ISO[10], sera développée pour collecter, structurer et analyser ces interdépendances, en étroite collaboration entre le Haut-Commissariat à la protection nationale et les autorités sectorielles.

À l'échelle nationale, cette démarche constituera un levier stratégique pour la planification de crise, l'élaboration de scénarios et la conduite d'exercices de simulation.

Les entités critiques seront également encouragées à réaliser leur propre cartographie des dépendances et interdépendances, qu'elles soient transfrontalières ou transsectorielles, afin de mieux comprendre leurs vulnérabilités systémiques et d'adapter leurs dispositifs de continuité en conséquence. La détermination des dépendances et interdépendances des activités prioritaires constitue d'ailleurs une étape clé du bilan d'impact sur l'activité (BIA), utilisé par les entités critiques dans le cadre de leur système de management de la continuité d'activité, aligné sur la norme ISO 22301.

Prioriser les infrastructures critiques

La priorisation des infrastructures critiques représente un levier stratégique pour renforcer la résilience globale des entités critiques et, par conséquent, la résilience nationale. Elle permettra de rendre plus performantes la planification de crise (constitution de stocks / capacités de gestion de crise) et la gestion de crise (ordre des interventions).

Cette priorisation résultera d'une analyse approfondie de la criticité des services essentiels et des infrastructures critiques, c'est-à-dire d'une analyse des impacts potentiels liés à leur interruption ou défaillance. Une méthode spécifique sera développée pour structurer cette analyse, en identifiant les infrastructures dont l'indisponibilité aurait des conséquences majeures sur les intérêts vitaux et les besoins essentiels du pays et de la population.

Le recensement des infrastructures et entités critiques, détaillé ci-dessous, s'appuiera sur cette analyse d'impacts pour évaluer leur criticité, c'est-à-dire leur importance stratégique en fonction des effets induits par leur indisponibilité. La criticité ainsi déterminée permettra d'établir un degré de priorité, indispensable pour orienter les mesures dans un contexte de crise : savoir quelles infrastructures sécuriser ou rétablir en premier, ou quels stocks stratégiques (re)constituer en priorité.

Recenser les besoins en stocks stratégiques

Au niveau des infrastructures critiques, les entités critiques identifieront les ressources nécessaires au soutien des activités prioritaires, y compris les stocks liés à l'activité courante. Elles détermineront également les exigences spécifiques pour mettre en œuvre et maintenir leurs solutions de continuité d'activité. Cela inclut les stocks de réserve détenus directement par les entités critiques, qui constituent une composante essentielle de leur résilience opérationnelle.

Les informations relatives à ces ressources seront transmises à l'autorité sectorielle et au Haut-Commissariat à la protection nationale, afin de permettre aux autorités d'évaluer le niveau de résilience effectivement assuré par les entités critiques.

À l'échelle nationale, les autorités sectorielles définiront les objectifs de continuité des services essentiels ou de leurs sous-secteurs. Sur cette base, les besoins en stocks stratégiques seront recensés. Ces stocks stratégiques, distincts des stocks de réserve détenus par les entités, constitueront des solutions de continuité pour les services essentiels et des capacités de gestion de crise. Ces stocks stratégiques permettront d'évaluer la résilience des services essentiels ou des sous-secteurs concernés et de détecter tout point de défaillance unique, lequel est systématiquement considéré comme un risque inacceptable au regard des objectifs de continuité.

10 Voir notamment ISO 22301, ISO/TS 22317 et ISO/TS 22318.

Renforcer la résilience cyber-physique des infrastructures critiques

La résilience des infrastructures critiques repose sur une double dimension, à la fois physique et cyber, qui doit être abordée de manière intégrée et holistique. Cette approche dite « cyber-physique » vise à anticiper les risques, à renforcer les capacités de réponse et à garantir la continuité des services essentiels. La présente stratégie s'appuie sur une coordination étroite entre les volets physiques et cyber, assurée notamment par :

- Le Haut-Commissariat à la protection nationale dans son rôle de coordinateur national en matière de crise ;
- Le Haut-Commissariat à la protection nationale comme point de contact national unique en matière d'incidents transfrontaliers, qu'ils soient d'origine physique ou cyber ;
- Le Haut-Commissariat à la protection nationale comme représentant national au sein du *NIS Cooperation Group* et du *Critical Entities Resilience Group* (CERG) ;
- Le Comité de coordination et de supervision, réunissant le Haut-Commissariat à la protection nationale, la Commission de Surveillance du Secteur Financier et l'Institut luxembourgeois de régulation.

Les mesures de résilience physique sont encadrées par la loi sur la résilience des entités critiques, tandis que les mesures de cybersécurité relèvent de la loi sur la cybersécurité et de la Stratégie nationale de cybersécurité.

Afin d'optimiser les mesures pour renforcer la résilience globale des entités critiques, les autorités sectorielles et fonctionnelles partageront leurs avis et recommandations sur des éventuelles mesures techniques, organisationnelles et de sécurité à mettre en œuvre avec le Haut-Commissariat à la protection nationale.

Dans le cadre de l'élaboration de leurs plans de résilience, les entités critiques sont encouragées de mettre en œuvre de manière coordonnée trois dispositifs complémentaires :

1. La gestion des risques, qui vise à identifier, analyser, évaluer et traiter les menaces connues. Elle doit couvrir un large éventail de scénarios, incluant notamment :

- La rupture d'approvisionnement énergétique ;
- La pénurie d'eau potable ;
- L'indisponibilité du personnel ;
- Les intempéries et inondations ;
- Les effets du changement climatique ;
- Le sabotage et l'espionnage, par des moyens physiques ou cyber ;
- La menace interne.

Cette gestion intégrera les éléments pertinents issus de l'évaluation des risques CER établie par le Haut-Commissariat à la protection nationale, ainsi que les mesures de traitement des risques (prévention, protection et atténuation). Dans ce cadre, les entités critiques définiront, en concertation avec le Haut-Commissariat à la protection nationale, les catégories de personnes à soumettre à la vérification des antécédents.

2. La gestion de la continuité d'activité, qui repose sur une analyse d'impact indépendante des menaces. Elle vise à assurer la poursuite des activités prioritaires, indépendamment de la nature des événements déclencheurs. Cette approche agnostique des menaces est indispensable dans un environnement marqué par l'incertitude de l'avenir et l'imprévisibilité des crises.

3. La gestion de crise, également agnostique des menaces et alignée à la norme ISO 22361, permet d'organiser la réponse opérationnelle et la communication en situation de rupture, quelle que soit la cause de la crise. Elle repose sur le développement de capacités de gestion de crise robustes et adaptables.

Pour structurer ces trois dispositifs, les entités critiques sont invitées à s'appuyer sur un Système de Management de la Continuité d'Activité conforme à la norme ISO 22301. Ce socle structurant intègre de manière cohérente :

- la politique et les objectifs de continuité ;
- l'analyse d'impact sur l'activité (BIA), incluant l'identification des ressources critiques ;
- l'évaluation des risques ;
- les stratégies de continuité, fondées sur la modularité, la distribution, la redondance, la diversité et l'adaptabilité ;
- les plans de sécurité et de sûreté ;
- les procédures de gestion des incidents[11] ;
- les plans et procédures de continuité de l'activité ;
- les plans de gestion et de communication de crise ;
- des tests et exercices réguliers pour garantir l'efficacité du dispositif.

Harmoniser les régimes de vérification des antécédents

Dans le cadre du renforcement de la résilience globale des entités critiques, une évaluation des régimes existants de vérification des antécédents sera menée. Cette analyse visera à identifier les différences, notamment en matière de types d'infractions considérées, de niveau d'accès aux fichiers (affaires courantes, casiers judiciaires), de catégories de personnes concernées et de finalités poursuivies. Elle permettra également de recenser les bonnes pratiques et les axes d'amélioration.

Sur la base des résultats obtenus, des recommandations pourront être formulées en vue d'une harmonisation des procédures et des dispositions légales. L'objectif est d'assurer, dans la mesure du possible et compte tenu des obligations internationales et des considérations de protection des données personnelles, un niveau cohérent de vérification des antécédents, quel que soit le secteur d'appartenance de l'infrastructure critique.

Développer une culture de la résilience

Le développement d'une culture de la résilience au sein des entités critiques et des autorités constitue un levier essentiel pour renforcer la résilience globale du pays. Ce développement poursuit un objectif stratégique de la Stratégie nationale de résilience.

Cette mesure vise à ancrer la compréhension, l'appropriation et l'intégration des enjeux de résilience dans les pratiques quotidiennes des acteurs concernés. Pour ce faire, des programmes de soutien, de supervision et d'exercices réguliers seront mis en œuvre pour sensibiliser, former et accompagner les entités critiques dans l'identification des menaces, de leurs vulnérabilités, de leurs activités et ressources prioritaires et la mise en place de mesures adaptées.

Les activités de soutien déjà en place offrent des espaces de rencontre et de collaboration entre les entités critiques et les autorités sectorielles, favorisant le réseautage, le renforcement de la cohésion et une meilleure capacité collective à faire face aux crises. Le Haut-Commissariat à la protection nationale poursuivra l'organisation de ces mécanismes de soutien.

Développer la coopération public-privé

Le renforcement de la coopération entre les acteurs publics et privés constitue un levier stratégique pour stimuler l'innovation, anticiper les risques émergents et consolider la résilience globale des entités critiques.

Dans ce cadre, les autorités compétentes CER, en coordination avec les autorités sectorielles, initieront des partenariats de coopération avec des institutions de recherche, nationales voire européennes, afin de mener des études prospectives et des projets de recherche ciblés. Ces collaborations permettront de croiser les expertises académiques et opérationnelles pour mieux comprendre les évolutions technologiques, les vulnérabilités liées aux interdépendances et les opportunités d'innovation. Elles contribueront à la création d'un écosystème de confiance et de partage.

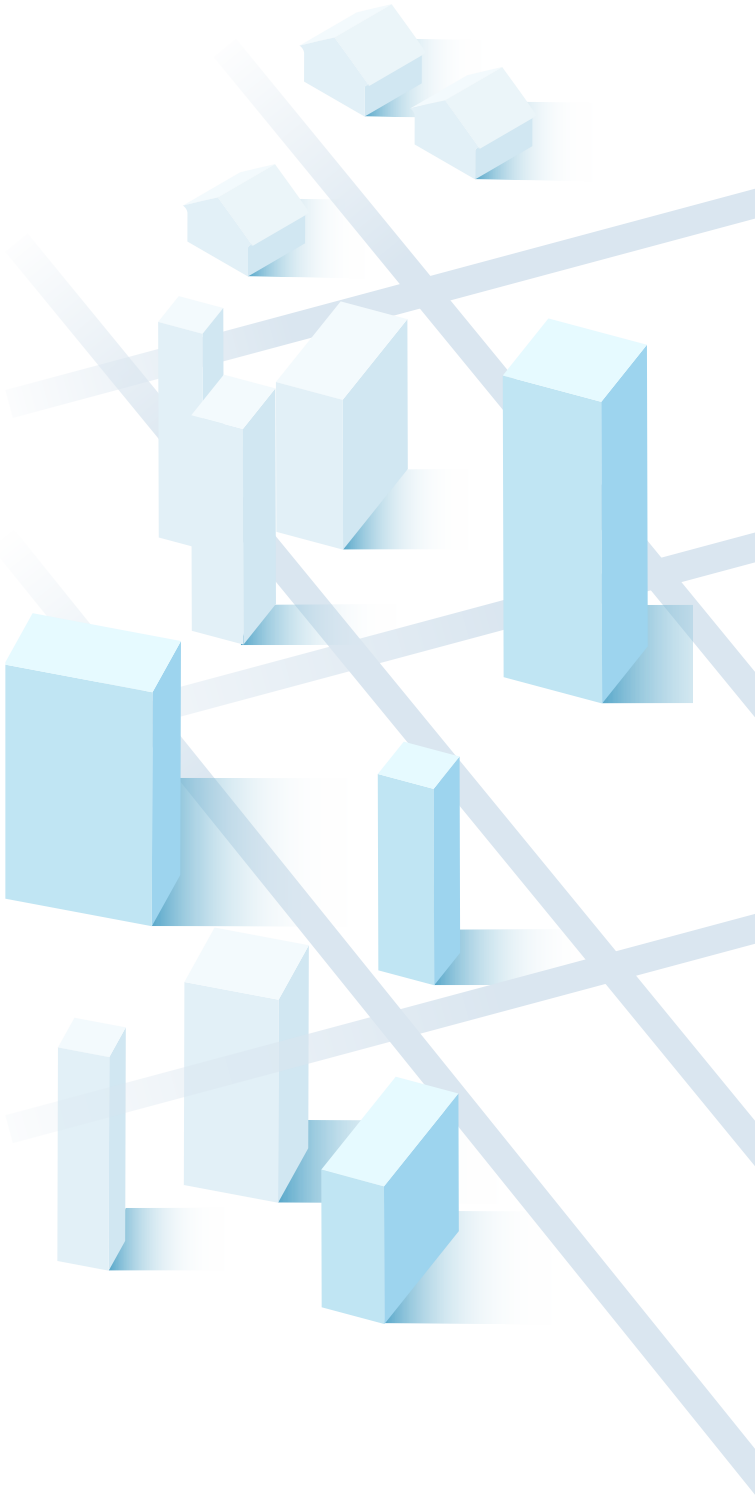
11 Au-delà du SMCA, la stratégie intègre les normes ISO 31000 (gestion des risques), ISO 22361 (gestion de crise), ISO 22316 (résilience organisationnelle), ainsi que des pratiques de gestion du changement et de sécurisation de la chaîne d'approvisionnement.

Recensement des infrastructures et entités critiques

Le présent chapitre décrit le processus de recensement des infrastructures et entités critiques[12].

En se basant sur la présente stratégie et l'évaluation des risques CER, le Haut-Commissariat à la protection nationale et la Commission de Surveillance du Secteur Financier initient et pilotent le recensement des infrastructures et entités critiques selon les secteurs attribués. Ces deux autorités compétentes CER élaborent ensemble des critères intersectoriels pour déterminer la criticité des infrastructures critiques et des entités critiques. Les autorités sectorielles, visées en annexe, proposent au Haut-Commissariat à la protection nationale une liste d'infrastructures et d'entités qui répondent à ces critères. Cette proposition peut également tenir compte de critères sectoriels complémentaires. Après concertation entre les autorités compétentes CER et l'autorité sectorielle, les premières arrêtent les critères qui s'appliquent et proposent au Gouvernement une liste d'infrastructures et d'entités pour désignation comme critiques.

Le recensement des infrastructures et entités critiques constituera l'un des volets structurants du cycle stratégique de résilience des entités critiques.



12 Article 4, §2, point d) de la Directive CER 2022/2557.

Soutien aux entités critiques

Le Haut-Commissariat à la protection nationale poursuivra son soutien aux entités critiques en mobilisant une diversité d'outils et d'espaces de rencontre dédiés. Les dispositifs de soutien visent à augmenter la conscience de la situation, à développer les compétences, à favoriser une culture durable de la résilience, à renforcer le réseautage entre entités critiques et à encourager l'échange entre entités critiques et entre entités et autorités. Le présent chapitre traite des mesures de soutien aux entités critiques[13].

Conscience partagée de la situation

À côté du partage des éléments pertinents de l'évaluation des risques CER, le Haut-Commissariat à la protection nationale continuera à mettre à la disposition des entités critiques différents outils destinés à renforcer la conscience de la situation.

Une nouvelle lettre de veille des risques courants et émergents sera partagée avec les entités critiques, qui auront un accès direct à un outil dédié.

Les briefings de sensibilisation aux menaces pesant sur les infrastructures critiques, organisés par le Haut-Commissariat à la protection nationale en concertation avec les autorités fonctionnelles, seront maintenus et renforcés. Pour pouvoir y participer, les entités critiques devront désigner un officier de sécurité et veiller à ce que des membres de leur personnel soient dûment habilités.

Ces dispositifs visent à renforcer la capacité d'anticipation des entités critiques, à soutenir leurs démarches internes de préparation, et à favoriser la prise en compte des informations de veille dans l'actualisation de leurs plans de résilience.

Le Colloque Résilience OIC

Le Colloque annuel sur la résilience des opérateurs d'infrastructures critiques restera un moment privilégié d'échange et de partage de bonnes pratiques entre les entités critiques. Organisé une fois par an par le Haut-Commissariat à la protection nationale, cet événement unique rassemble exclusivement l'ensemble des opérateurs d'infrastructures critiques, dans un cadre propice à la mise en commun des savoir-faire et au partage des retours d'expérience. Les thématiques portent principalement sur la sécurité et la résilience, à travers des axes tels que la protection, la continuité d'activité et la gestion de crise.

Les « Plats de résilience »

Les « Plats de résilience » sont des rencontres thématiques en format restreint, conçues pour favoriser le dialogue intersectoriel autour de sujets spécifiques, sensibles et d'actualité liés à la sécurité et la résilience des infrastructures critiques. Organisés par le Haut-Commissariat à la protection nationale, ces rendez-vous auront lieu au moins quatre fois par an.

Les OIC *Learning Expeditions*

Les *Learning Expeditions* pour OIC sont des visites d'apprentissage immersives, ouvertes aux opérateurs d'infrastructures critiques. Elles leur permettent de découvrir, sur le terrain, des solutions innovantes en matière de sécurité, de continuité d'activité ou de gestion de crise, ou encore de s'inspirer des pratiques d'autres entités critiques. Organisées une ou deux fois par an par le Haut-Commissariat à la protection nationale, ces expériences stimulantes visent à favoriser le partage d'expériences, l'amélioration continue des pratiques et le renforcement des liens entre acteurs clés. Véritables leviers d'ouverture, elles offrent aux participants une plongée dans des environnements agiles, résilients et à la pointe de l'innovation.

13 Article 4, §2, point e) de la Directive CER 2022/2557.

Le développement des compétences

Les formations actuellement proposées par le Haut-Commissariat à la protection nationale aux entités critiques, notamment en matière de management de la continuité d'activité et de gestion de crise, seront maintenues. Le programme pourra être enrichi progressivement, en fonction des besoins identifiés et du niveau de maturité des entités critiques.

Les PME et les entreprises de taille intermédiaire[14]

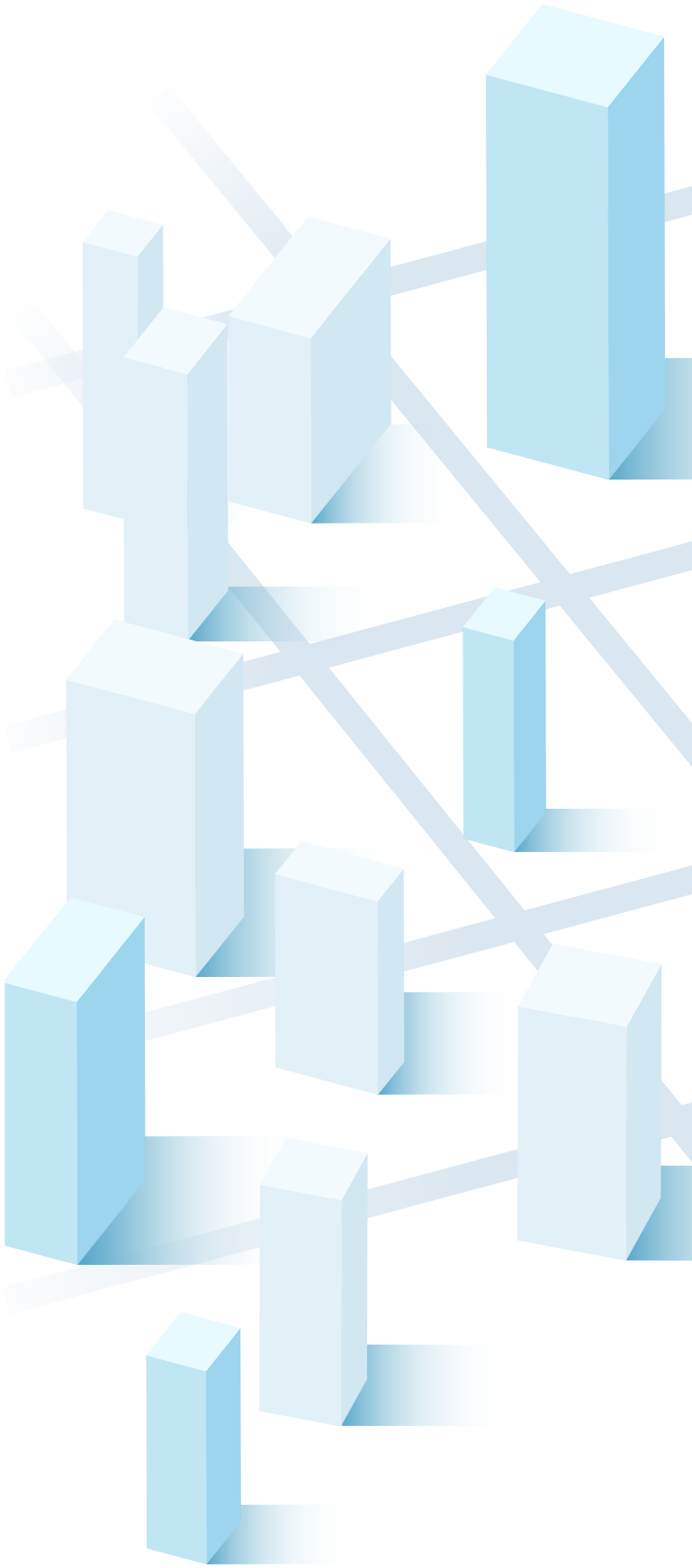
Les entités critiques ayant le statut d'une PME bénéficieront de l'ensemble des mesures de soutien aux entités critiques visées par le sous-chapitre 5.1. Les PME seront prioritaires dans l'accès aux formations en matière du management de la continuité d'activité organisées par le Haut-Commissariat à la protection nationale.

Dans le cadre du cycle de suivi et de mise à jour de la présente stratégie, des efforts d'amélioration continueront à être déployés afin d'adapter les dispositifs de soutien aux besoins spécifiques des PME et d'assurer une mise en œuvre efficace.

Les exercices et les tests de résistance

Conformément à la Stratégie nationale de résilience, le Haut-Commissariat à la protection nationale, en concertation avec les autorités sectorielles et fonctionnelles ainsi qu'avec les entités critiques, établira et mettra en œuvre un programme pluriannuel d'exercices intersectoriels et de tests de résistance. La périodicité de ces exercices sera déterminée en fonction du niveau de criticité des services essentiels et de la priorisation des infrastructures critiques. Les entités critiques seront également encouragées à participer à des exercices internationaux et à organiser leurs propres exercices annuels, afin de renforcer leur préparation opérationnelle.

À l'issue de chaque exercice ou test de résistance, le Haut-Commissariat à la protection nationale procédera à une évaluation, en concertation avec les autres autorités impliquées, et émettra des observations à l'attention de l'entité critique concernée.



14 Article 4, §2, point h) de la Directive CER 2022/2557.

Cadre d'action pour la coordination entre autorités compétentes CER et NIS2

Le présent cadre d'action vise à garantir une coordination renforcée entre les autorités compétentes et oriente le partage d'informations concernant les risques, les menaces et les incidents visant la fourniture d'un service essentiel entre ces autorités. Ce cadre d'action soutient la cohérence de l'exercice de la supervision des entités critiques par chaque autorité compétente selon leur mandat[15].

Les autorités compétentes CER et NIS2, à savoir le Haut-Commissariat à la protection nationale, la Commission de Surveillance du Secteur Financier et l'Institut luxembourgeois de régulation, se réunissent au moins une fois tous les quatre mois en « Comité de coordination et de supervision ». Au sein de ce comité, les autorités compétentes s'échangent les informations sur les risques, menaces et incidents visant les services essentiels, les entités critiques ou les infrastructures critiques. Si besoin, le comité peut se réunir de façon ad hoc, notamment en cas d'incident notifié par une entité critique.

Les modalités de fonctionnement de ce comité font l'objet d'un accord de collaboration entre ces autorités. Le comité établit un programme de supervision des entités critiques articulé autour de trois axes principaux d'interventions : les audits, les inspections et la surveillance à distance. Ce programme aura pour vocation de permettre aux autorités compétentes de s'assurer que les entités et infrastructures critiques respectent leurs obligations légales. Le programme précisera la fréquence des audits et des inspections inopinées.

Pour établir le programme le comité suit une approche de supervision modulaire : selon le niveau de maturité en résilience de l'entité critique, indiqué notamment par une attitude proactive de résilience (communication prompte, transparence), par une certification ISO 22301 ou similaire, par un programme de formations et d'exercices ; et selon le niveau de criticité/en fonction de la priorisation des infrastructures critiques.

Suivi et mise à jour

La présente stratégie fera l'objet d'une révision quadriennale, avec la possibilité de mises à jour ad hoc en cas de besoin particulier. Un plan d'action sera établi pour opérationnaliser les mesures décrites, et une revue intermédiaire simplifiée sera réalisée à mi-parcours.

Les actions contenues dans la Stratégie nationale pour renforcer la résilience des entités critiques seront évaluées et budgétisées conformément à la trajectoire retenue et les propositions budgétaires, et une estimation et priorisation pourront être établies le cas échéant. Les mesures contenues dans la présente stratégie qui ont déjà été adoptées et incorporées dans une loi ou un règlement grand-ducal seront prises en compte dans la planification budgétaire pluriannuelle. Les mesures nouvelles ou renforcées devront faire l'objet de la procédure budgétaire habituelle.

Le suivi s'inscrira dans un cycle structuré, fondé sur l'approche PDCA (*Plan – Do – Check – Act*), réparti sur quatre années. Ce cycle reposera sur un séquençage cohérent entre la stratégie, l'évaluation des risques et le recensement des entités et infrastructures critiques.

Les activités de soutien et de supervision seront poursuivies de manière continue tout au long du cycle.

15 Article 4, §2, point g) de la Directive CER 2022/2557.

Annexes

Liste des secteurs, sous-secteurs et services essentiels

Secteur	Sous-secteur	Service essentiel
Énergie	**Électricité**	• Fourniture d'électricité (entreprises d'électricité) • Exploitation, maintenance et développement d'un réseau de distribution d'électricité (gestionnaires de réseau de distribution) • Exploitation, maintenance et développement d'un réseau de transport d'électricité (gestionnaires de réseau de transport) • Production d'électricité (producteurs) • Service d'opérateur désigné du marché de l'électricité (opérateurs désignés du marché de l'électricité) • Participation active de la demande (acteurs du marché de l'électricité) • Agrégation d'électricité (acteurs du marché de l'électricité) • Stockage d'énergie (acteurs du marché de l'électricité)
	Réseaux de chaleur et de froid	• Fourniture de réseaux de chaleur ou de réseaux de froid (opérateurs de réseaux de chaleur ou de réseaux de froid)
	Pétrole	• Transport de pétrole (exploitants d'oléoducs) • Production de pétrole (exploitants de production de pétrole) • Raffinage et traitement de pétrole (exploitants d'installations de raffinage et de traitement de pétrole) • Stockage de pétrole (exploitants de stockage de pétrole) • Gestion de stocks de pétrole, notamment de stocks de sécurité et de stocks spécifiques de pétrole (entités centrales de stockage)
	Gaz	• Fourniture de gaz (entreprises de fourniture) • Distribution de gaz (gestionnaires de réseau de distribution) • Transport de gaz (gestionnaires de réseau de transport) • Stockage de gaz (gestionnaires d'installation de stockage) • Exploitation d'une installation de gaz naturel liquéfié (GNL) (gestionnaires d'installation de GNL) • Production de gaz naturel (entreprises de gaz naturel) • Achat de gaz naturel (entreprises de gaz naturel) • Raffinage et traitement de gaz naturel (exploitants d'installations de raffinage et de traitement de gaz naturel)
	Hydrogène	• Production d'hydrogène (exploitants de production d'hydrogène) • Stockage d'hydrogène (exploitants de stockage d'hydrogène) • Transport d'hydrogène (exploitants de transport d'hydrogène)

Secteur	Sous-secteur	Service essentiel
Transports	Transports aériens	• Services de transport aérien utilisés à des fins commerciales (passagers et fret) (transporteurs aériens) • Exploitation, gestion et entretien des aéroports et des infrastructures du réseau aéroportuaire (entités gestionnaires d'aéroports) • Services du contrôle de la circulation aérienne (services du contrôle de la circulation aérienne)
	Transports ferroviaires	• Services de transport ferroviaire (voyageurs et fret) (entreprises ferroviaires) • Exploitation, gestion et entretien de l'infrastructure ferroviaire, y compris les gares de voyageurs, les terminaux de marchandises, les gares de triage et les centres de contrôle du trafic (gestionnaires de l'infrastructure) • Exploitation, gestion et entretien d'installations de service ferroviaire (exploitants d'installations de service) • Exploitation, gestion et entretien de systèmes pour la gestion du trafic ferroviaire, le contrôle-commande et la signalisation, ainsi que d'installations et de systèmes de télécommunications utilisés pour le contrôle-commande et la signalisation (gestionnaires de l'infrastructure)
	Transports par eau	• Services de transport par voie d'eau intérieure, maritime et côtier (passagers et fret) (sociétés de transport par voie d'eau intérieure, maritime et côtier de passagers et de fret) • Exploitation, gestion et entretien des ports et installations portuaires, et exploitation d'ateliers et d'équipements à l'intérieur des ports, y compris le soutage, la manutention des cargaisons, l'amarrage, les services aux passagers, la collecte des déchets d'exploitation des navires et des résidus de cargaison, le pilotage et le remorquage (entités gestionnaires des ports et entités exploitant des ateliers et des équipements à l'intérieur des ports) • Services de trafic maritime (exploitants de services de trafic maritime)
	Transports routiers	• Contrôle de la gestion de la circulation, y compris les aspects liés aux services de planification, de contrôle et de gestion du réseau routier, à l'exclusion de la gestion de la circulation ou de l'exploitation de systèmes de transport intelligents lorsqu'elles ne constituent pas une partie essentielle de l'activité générale des entités publiques (autorités routières) • Services de systèmes de transport intelligents (exploitants de systèmes de transport intelligents)
Bancaire		• Réception de dépôts (établissements de crédit) • Prêt (établissements de crédit)
Infrastructures des marchés financiers		• Exploitation d'une plate-forme de négociation (exploitants de plates-formes de négociation) • Exploitation de systèmes de compensation (contreparties centrales)

Secteur	Sous-secteur	Service essentiel
Santé		• Fourniture de services de soins de santé (prestataires de soins de santé) • Analyse effectuée par un laboratoire de référence de l'Union européenne (laboratoires de référence de l'Union européenne) • Recherche et développement de médicaments (entités exerçant des activités de recherche et de développement dans le domaine des médicaments) • Fabrication de produits pharmaceutiques de base et de préparations pharmaceutiques de base (entités fabriquant des produits pharmaceutiques de base et des préparations pharmaceutiques) • Fabrication de dispositifs médicaux considérés comme critiques en cas d'urgence de santé publique (entités fabriquant des dispositifs médicaux) • Distribution de médicaments (entités titulaires d'une autorisation de distribution)
Eau potable		• Approvisionnement en eau potable et distribution d'eau potable, à l'exclusion de la distribution d'eaux destinées à la consommation humaine lorsque ce service constitue une partie non essentielle de l'activité générale de distributeurs distribuant d'autres produits et biens (fournisseurs et distributeurs d'eaux destinées à la consommation humaine)
Eaux résiduaires		• Collecte, traitement et évacuation des eaux usées, à l'exclusion de la collecte, de l'évacuation ou du traitement des eaux urbaines résiduaires, des eaux ménagères usées ou des eaux industrielles usées lorsqu'ils ne constituent pas une partie essentielle de l'activité générale des entreprises (entreprises collectant, évacuant ou traitant les eaux urbaines résiduaires, des eaux ménagères usées et des eaux industrielles usées)
Infrastructures numériques		• Fourniture et exploitation de services de points d'échange internet (fournisseurs de points d'échange internet) • Fourniture de services de système de noms de domaine (DNS), à l'exclusion des services liés aux serveurs racines de noms de domaine (fournisseurs de services DNS) • Exploitation et administration de registres de noms de domaines de premier niveau (registres de noms de domaines de premier niveau) • Fourniture de services d'informatique en nuage (fournisseurs de services d'informatique en nuage) • Fourniture de services de centre de données (fournisseurs de services de centre de données) • Fourniture de réseaux de diffusion de contenu (fournisseurs de réseaux de diffusion de contenu) • Fourniture de services de confiance (prestataires de services de confiance) • Fourniture de services de communications électroniques accessibles au public (fournisseurs de services de communications électroniques) • Fourniture de réseaux de communications électroniques publics (fournisseurs de réseaux de communications électroniques publics)

Secteur	Sous-secteur	Service essentiel
Administration publique	Sécurité nationale	• L'administration et la supervision des activités de sécurité nationale au sens de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.
	Défense	• L'administration et la supervision des activités de défense nationale et des forces armées terrestres, navales, aériennes et spatiales.
	Justice	• L'administration des établissements pénitentiaires, y compris les services d'assistance aux détenus en vue de faciliter leur réinsertion, que cette gestion et exploitation soient assurées par des organismes publics ou par des organisations privées pour le compte de cette dernière.
	Sécurité intérieure	• L'administration et la supervision des activités de sécurité intérieure au sens de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, notamment les missions de police administrative et les missions de police judiciaire.
	Sécurité civile	• L'administration et la supervision des activités de sécurité civile au sens de la loi modifiée du 27 mars 2018 portant organisation de la sécurité civile.
Espace		• Exploitation d'infrastructures au sol, détenues, gérées et exploitées par des États membres ou par des parties privées, qui soutiennent la fourniture de services spatiaux, à l'exclusion des fournisseurs de réseaux de communications électroniques publics (exploitants d'infrastructures au sol)
Denrées alimentaires		• Production et transformation industrielles à grande échelle de denrées alimentaires
		• Services de la chaîne d'approvisionnement alimentaire, y compris l'entreposage et la logistique
		• Distribution en gros de denrées alimentaires
Déchets		• Gestion des déchets au sens de l'article 4, point 22, de la loi modifiée du 21 mars 2012 relative aux déchets

Remarques :
1. Les transports intelligents et les transports publics sont à considérer dans les sous-secteurs respectifs (transport aérien, transport ferroviaire, transport par eau, transport routier).
2. Pour le secteur de l'administration publique seuls les services dont la fourniture requiert une infrastructure indispensable à la sauvegarde des intérêts vitaux ou des besoins essentiels du pays ou de la population ont été retenus.

Liste des autorités sectorielles et fonctionnelles[16]

Les autorités sectorielles

Secteur	Sous-secteur	Autorité sectorielle (*)
Energie	Électricité	• Ministre ayant l'Energie dans ses attributions
	Réseaux de chaleur et de froid	
	Pétrole	
	Gaz	
	Hydrogène	
Transports	Transports aériens	• Ministre ayant les Transports dans ses attributions
	Transports ferroviaires	
	Transports routiers	
	Transports par eau	
Bancaire		• Ministre des Finances
Infrastructures des marchés financiers		
Santé		• Ministre ayant la Santé dans ses attributions
Eau potable		• Ministre ayant l'Environnement dans ses attributions
Eaux résiduaires		
Infrastructures numériques		• Ministre ayant l'Économie dans ses attributions • Ministre ayant les Médias dans ses attributions • Ministre ayant la Digitalisation dans ses attributions • (selon les attributions respectives)
Administration publique	Sécurité nationale	• Ministre ayant le renseignement de l'État dans ses attributions
	Défense	• Ministre ayant la Défense dans ses attributions
	Justice	• Ministre ayant la Justice dans ses attributions
	Sécurité intérieure	• Ministre ayant la Sécurité intérieure dans ses attributions
	Sécurité civile	• Ministre ayant les Services de secours dans ses attributions
Espace		• Ministre ayant les Médias dans ses attributions
Denrées alimentaires		• Ministre ayant l'Alimentation dans ses attributions
Déchets		• Ministre ayant l'Environnement dans ses attributions

(*) le ministre ou son délégué

Les autorités fonctionnelles

Fonction	Autorité fonctionnelle (*)
Sécurité nationale	• Ministre ayant le renseignement de l'État dans ses attributions
Défense	• Ministre ayant la Défense dans ses attributions
Sécurité intérieure	• Ministre ayant la Sécurité intérieure dans ses attributions
Sécurité civile	• Ministre ayant les Services de secours dans ses attributions
Gestion de crise	• Ministre ayant la Protection nationale dans ses attributions

(*) le ministre ou son délégué

16 Article 4, §2, point f) de la Directive CER 2022/2557.

Glossaire des termes clés

Notion	Définition
Entité critique	Entité publique ou privée qui fournit un ou plusieurs services essentiels par l'intermédiaire de son ou ses infrastructures critiques et dont le dysfonctionnement aurait des effets perturbateurs assimilés à une crise. Synonyme : Opérateur d'infrastructure critique.
Incident	« [U]n événement qui perturbe ou est susceptible de perturber de manière importante la fourniture d'un service essentiel, y compris lorsqu'il affecte les systèmes nationaux qui préservent l'état de droit. » Article 2, point 3 de la Loi sur la résilience des entités critiques
Infrastructure critique	« [U]n bien, une installation, un équipement, un réseau ou un système, ou une partie d'un bien, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel. » Article 2, point 4 de la Loi sur la résilience des entités critiques
Résilience des entités critiques	« Capacité d'une entité critique à prévenir tout incident, à s'en protéger, à y réagir, à y résister, à l'atténuer, à l'absorber, à s'y adapter et à s'en rétablir. » Article 2, point 2) de la Directive CER 2022/2557
Résilience nationale	« Capacité d'un système, d'une communauté ou d'une société exposée à des perturbations d'y résister et de les absorber, de s'adapter à leurs effets et de s'en relever rapidement et efficacement, notamment en préservant et en rétablissant ses fonctions sociétales essentielles. » Stratégie nationale de résilience (2025)
Résilience de l'OTAN	« Aptitude individuelle et collective à se préparer, à résister et à répondre aux perturbations et aux chocs, ainsi qu'à s'en remettre rapidement, et à veiller à la continuité des activités de l'Alliance. La préparation du secteur civil est un pilier de la résilience des pays de l'OTAN et l'un des éléments facilitateurs critiques de la défense collective de l'Alliance. » Source : https://www.nato.int/cps/fr/natohq/topics_132722.htm consultée le 10 novembre 2025
Concept de protection nationale	« Concept qui consiste à prévenir les crises, respectivement à protéger le pays et la population contre les effets d'une crise. En cas de survenance d'une crise, il comprend la gestion des mesures et activités destinées à faire face à la crise et à ses effets et à favoriser le retour à l'état normal. » Article 2, point 1 de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale
Maintien de fonctions sociétales vitales	« La disponibilité de services indispensables à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population » Article 2, point 6 de la Loi sur la résilience des entités critiques
Service essentiel	« Service qui est crucial pour le maintien de fonctions sociétales ou d'activités économiques vitales, de la santé publique et de la sûreté publique, ou de l'environnement » Article 2, point 5 de la Loi sur la résilience des entités critiques

Haut-Commissariat à la Protection nationale
46, rue du Château — L-6961 Senningen — T. (+352) 247-88900 — info@letzprepare.lu