EIWTC SECURITY ADVISORY
Security · Resilience · Technical Consulting

CER & NIS-2

Résilience au Luxembourg

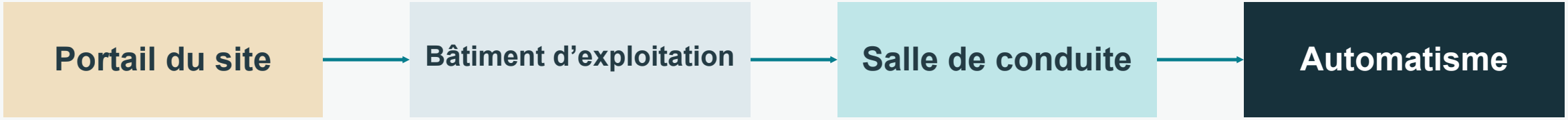
Contrôle d’accès aux infrastructures critiques

Le CRA complète la sécurité des produits numériques



Notre exemple : une usine d’eau potable critique

L’eau potable doit rester disponible.



Les visiteurs sont accueillis et accompagnés.

Les techniciens reçoivent des droits liés à leur mission.

Le personnel maintient l’approvisionnement.

La maintenance nécessite une autorisation.

Autre cas : une station de pompage isolée dont la connexion réseau est intermittente.

Exemple fictif : la désignation officielle comme entité critique est supposée.

Une porte ouverte peut affecter l’approvisionnement

Accès non autorisé → **Intervention sur l’automatisme** → **Interruption du service**

Un badge perdu reste valable

Une armoire ou le réseau est accessible

Le service d’eau potable est affecté

Autres causes

Crue · Coupure électrique · Absence de personnel
Pénurie · Cyberattaque · Sabotage

Évaluer ensemble : voies d’accès, dépendances, conséquences et reprise.

Les huit piliers de la résilience du Luxembourg

PRÉPARATION CIVILE

PRÉPARATION MILITAIRE

1 Démocratie, État de droit et gouvernement

2 Société résiliente

3 **Services essentiels et infrastructures critiques** — CER

4 Économie résiliente

8 Protection et défense du territoire national et des alliés

5 Ressources stratégiques et logistiques

6 **Cyberrésilience** — NIS-2

7 Défense civile

CER : continuité du service · NIS-2 : protection des systèmes · CRA : sécurité des produits.

Intitulés abrégés. Mise en évidence et rattachement réglementaire : interprétation professionnelle.

Quels secteurs sont concernés ?

12 secteurs CER

Également couverts par NIS-2

- Énergie
- Transports
- Secteur bancaire
- Infrastructures des marchés financiers
- Santé
- **Eau potable**
- Eaux usées
- Infrastructure numérique
- Administration publique
- Espace
- Denrées alimentaires
- Gestion des déchets

6 autres secteurs NIS-2

- Services TIC (B2B)
- Services postaux et de courrier
- Produits chimiques
- Certaines activités de fabrication
- Fournisseurs numériques
- Recherche

Exemples : gestionnaire de réseau électrique, hôpital, fournisseur d'eau, centre de données.

Le secteur est un premier repère. Le type d'entité et sa classification sont déterminants.

Critique, essentielle ou importante ?

CER

Critique

Désignation officielle selon l’importance du service et les effets possibles d’une perturbation.

Exemple : usine d’eau potable désignée.

NIS-2

Essentielle

En principe, grandes entités de l’annexe I. Des cas particuliers prévus par la loi s’y ajoutent.

Exemple : grand hôpital ou fournisseur DNS.

NIS-2

Importante

En principe, entités moyennes de l’annexe I et moyennes ou grandes de l’annexe II, sans statut spécial.

Exemple : fabricant de machines de taille moyenne.

Notre usine désignée au titre de CER est essentielle selon NIS-2, quelle que soit sa taille.

Les entités essentielles et importantes ont toutes des obligations de sécurité et de notification.

NIS-2 : classification à partir d’exemples

Entité fictive	Classification habituelle	Motif
Fournisseur d’eau désigné CER	Essentielle, même de petite taille	Entité critique CER
Grand hôpital	Essentielle	Type d’entité visé à l’annexe I
Hôpital moyen, sans statut spécial	Importante	Annexe I, taille moyenne
Fabricant de machines moyen ou grand	Importante, si la fabrication est visée	Annexe II, sans statut essentiel spécial
Fournisseur DNS à petite équipe	Essentielle	Cas particulier indépendant de la taille

« Moyenne » et « grande » renvoient à la définition européenne des PME, entreprises partenaires et liées incluses.

Vérifier secteur et type d’entité, calculer la taille, examiner les cas particuliers.

Le contrôle d’accès relie CER et NIS-2

CER

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

UE : art. 13, par. 1, points b et e

Protection physique, personnel et autorisations d’accès.

NIS-2

Luxembourg : art. 12, par. 2, points 8 à 10

UE : art. 21, par. 2, points h, i et j

Cryptographie, contrôle d’accès et authentification appropriée.

Dans notre usine **Les personnes autorisées accèdent à la salle de conduite. Serveur d’accès, révocation et mode dégradé sont sécurisés.**

Preuves : plan de zonage, validation des droits, tests de révocation et de reprise.

Les deux lois nationales citent l’art. 12. Les numéros d’articles européens diffèrent.

La responsabilité de la direction en pratique

1	**Approuver**	Valider les besoins de protection, le concept d’accès et les risques résiduels
2	**Permettre**	Désigner les responsables, le budget et les moyens de secours
3	**Surveiller**	Vérifier délais de révocation, droits de maintenance et tests de panne
4	**Apprendre**	Former la direction et suivre les écarts

NIS-2 · essentielle
10 M€ / 2 %*

NIS-2 · importante
7 M€ / 1,4 %*

CER · amende jusqu’à
250 000 €

* Le montant le plus élevé entre le plafond fixe et la part du chiffre d’affaires annuel mondial.

La surveillance et les sanctions diffèrent

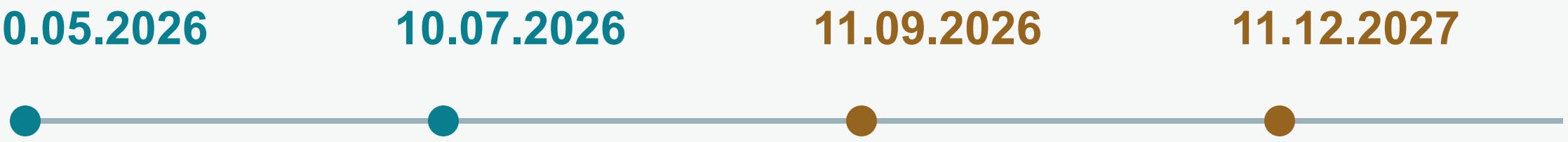
Sujet	NIS-2	CER
Autorité compétente	ILR ; CSSF pour les domaines financiers attribués par la loi	HCPN dans le cadre CER ; tenir compte des secteurs particuliers
Amendes	Essentielle : jusqu'à 10 M€ / 2 %* Importante : jusqu'à 7 M€ / 1,4 %*	Jusqu'à 250 000 € selon l'art. 19 national
Direction	Approbation, surveillance et formation selon l'art. 13 national	Mise en œuvre responsable des mesures de résilience

* Le montant le plus élevé entre le plafond fixe et la part du chiffre d'affaires annuel mondial.

DORA : résilience opérationnelle numérique du secteur financier. Vérifier les recoupements par obligation.

La mise en œuvre est déjà engagée

État au 19 novembre 2026



CER & NIS-2

Entrée en vigueur des lois luxembourgeoises

NIS-2

Échéance du premier auto-enregistrement

CRA

Les fabricants doivent notifier les incidents et vulnérabilités concernés

CRA

Application des principales obligations pour les produits numériques

Pour chaque entité, les délais CER sont liés à sa désignation.

NIS-2 : dix groupes de mesures pour les accès

01 Analyse des risques et politiques de sécurité
Évaluer zones, rôles et conséquences des pannes

02 Gestion des incidents
Bloquer, contenir, documenter et notifier

03 Continuité d'activité et gestion de crise
Tester accès de secours, sauvegarde et reprise

04 Sécurité de la chaîne d'approvisionnement
Évaluer mainteneur, fabricant et assistance

05 Acquisition, développement et maintenance
Gérer durcissement, mises à jour et vulnérabilités

06 Évaluation de l'efficacité des mesures
Tests de révocation, de panne et de restauration

07 Cyberhygiène et formation
Former administration, exploitation et intervenants

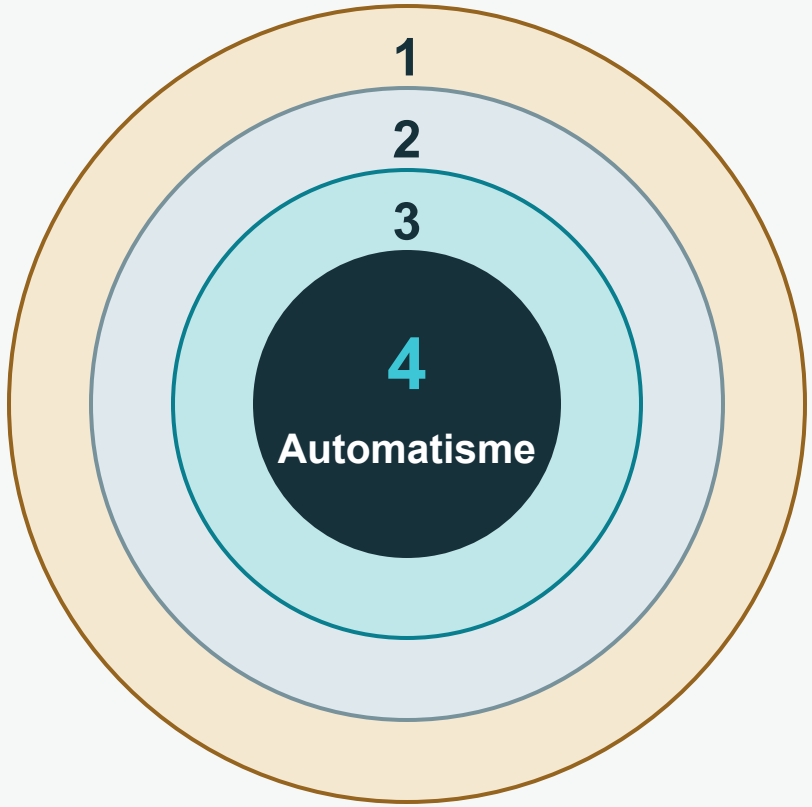
08 Cryptographie et chiffrement
Protéger communications, clés et micrologiciels

09 Personnel, accès et gestion des actifs
Relier arrivée, mobilité, départ et inventaire

10 MFA et communications sécurisées
Sécuriser accès administratifs et communications de crise

Art. 12 national / art. 21 UE : mettre en œuvre des mesures appropriées et proportionnées.

Le principe des couches de protection



1 Site / périmètre extérieur

Clôture, portail et parcours visiteurs limitent l’accès au site.

2 Bâtiment / périmètre intérieur

Les portes extérieures contrôlées n’admettent que les personnes autorisées.

3 Locaux sensibles

Salle de conduite et salle serveurs ont des droits propres, liés aux rôles.

4 Composants critiques

Ouvrir armoire de commande ou baie uniquement pour la tâche autorisée.

Chaque couche protège la suivante. Les cercles montrent des limites de protection, pas un plan de bâtiment.

Quatre zones à titre d’exemple. EN 50600-2-5 traite des systèmes de sécurité des centres de données.

Une maintenance passe par quatre autorisations

Un technicien externe intervient sur l’automatisme. Sa mission définit son parcours autorisé.

1 · Portail du site	2 · Bâtiment	3 · Salle de conduite	4 · Automatisme
Vérifier identité et rendez-vous	Accès limité au créneau prévu	L’exploitation autorise l’accès	Autoriser séparément l’intervention précise
Se présenter à l’accueil	Limiter la durée des droits	Accompagnement selon le besoin de protection	Tracer mission et ouverture

Après la maintenance **Les droits expirent, les composants sont verrouillés et la mission est documentée.**

Les couches doivent fonctionner ensemble

Une barrière extérieure est défaillante.

Les limites intérieures doivent encore restreindre l’accès et permettre une réaction.

Éviter les contournements	Livraisons, portes latérales et prestataires suivent les mêmes règles d’autorisation.
Traiter les événements	Une porte de salle de conduite ouverte trop longtemps est détectée. Un responsable désigné réagit.
Maîtriser les pannes	Fonctionnement local, accès de secours et évacuation sûre sont définis et testés ensemble.

Test : même portail ouvert, la salle de conduite reste inaccessible aux personnes non autorisées.

Les droits suivent la mission

Arrivée	→ Changement	→ Départ
Vérifier l’identité Valider le rôle	Retirer les anciens droits Examiner la nouvelle mission	Bloquer le badge Confirmer l’efficacité

Mission de maintenance

Un technicien externe accède à la station de pompage : uniquement au créneau autorisé et dans la zone nécessaire. Sans mission, salle de conduite et automatisme restent interdits.

Fonctions sensibles : examiner la vérification CER du personnel avant autorisation. Voir diapositive 17.

Les fonctions sensibles exigent un examen particulier

Qui peut intervenir en salle de conduite ?

La fonction et l’accès au service critique déterminent le besoin de vérification.

1. Définir la fonction sensible
2. Suivre la procédure légale
3. Autoriser séparément les accès

5 ans

Validité de la décision

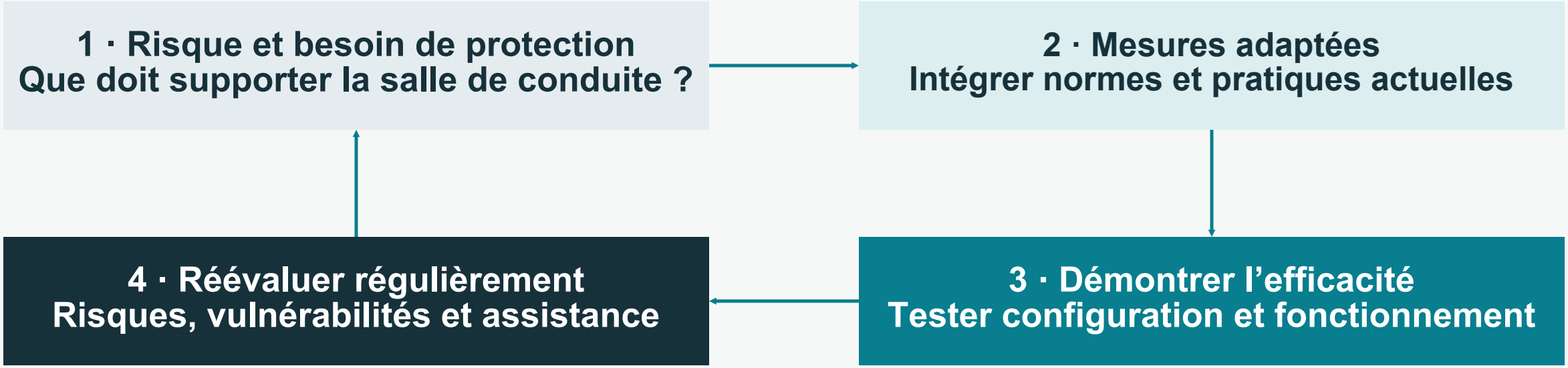
Demander le renouvellement :

6 à 4 mois avant l’expiration

Pas de vérification générale de tous les salariés ; respecter les conditions légales.

Que signifie « état de l’art » ?

Des mesures au niveau actuel du développement technique, adaptées au risque concret et efficaces en pratique.



Efforts et coûts entrent dans la proportionnalité. Le niveau de protection requis reste déterminant.

Les limites des clés purement mécaniques

Qui peut ouvrir la salle de conduite après la perte d’une clé ?

La réponse exige une procédure de retrait efficace.

Traçabilité

La serrure ne produit pas de journal d’événements.
Remise et restitution doivent être traçables.

Perte et copies

Une clé ne se bloque pas numériquement.
Examiner cylindres concernés et mesures compensatoires.

Horaires et rôles

Les clés purement mécaniques n’appliquent pas automatiquement des droits horaires.

La mécanique peut convenir. Des exigences élevées peuvent nécessiter des mesures complémentaires.

Quatre stades d’évolution du contrôle d’accès

01

Réactif

Mécanique

Attribuer les clés et demander leur restitution.

Tracer l’attribution. En cas de perte, remplacer la serrure si nécessaire.

02

Identifié

Électronique

Support individuel et événements d’accès.

Bloquer un badge précis. Le délai dépend de l’architecture du système.

03

Dynamique

Gestion des droits

Rôles et créneaux liés à chaque maintenance.

Bloquer au départ. Coordonner les changements avec les RH.

04

Proactif

Surveillance

Détecter les attaques. Réagir de façon ciblée.

MFA adaptée au risque : carte et PIN possibles. Tester le mode dégradé.

L’état de l’art découle du besoin de protection et du fonctionnement démontré.

Modèle d’évolution, sans hiérarchie légale. La biométrie n’est pas une condition générale.

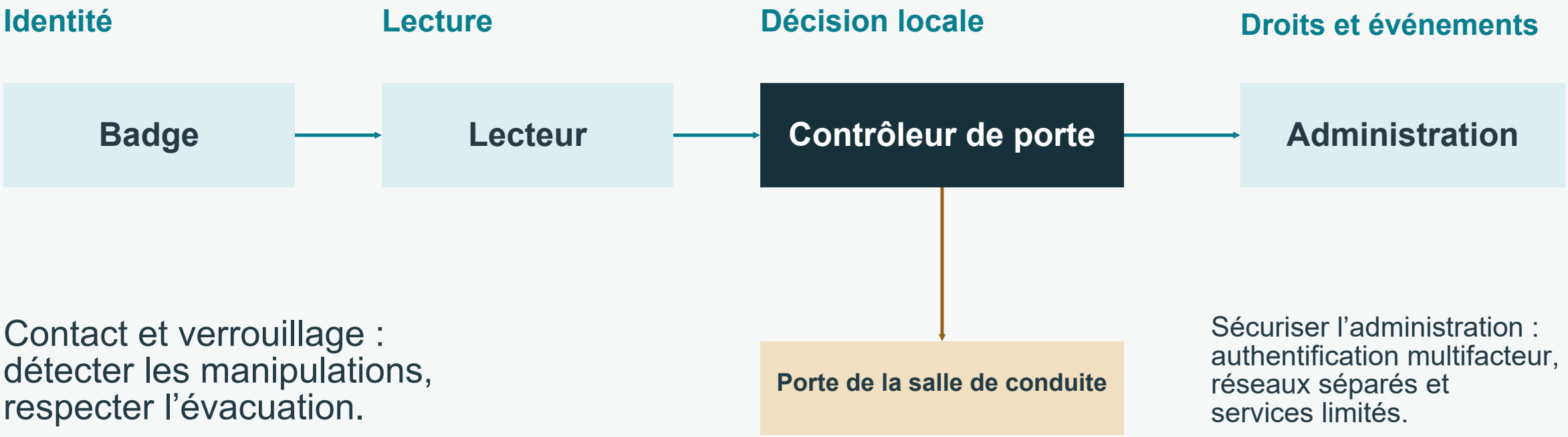
Comparer les systèmes d’accès par leurs fonctions

Critère	Mécanique	Électronique hors ligne	Électronique en ligne
Modifier les droits	Attribution des clés / remplacement éventuel des cylindres	Localement, par support de données ou canal de retour défini	Diffusion centralisée avec contrôle d’efficacité
Perte et révocation	Restitution ou remplacement ; évaluer la possibilité de copie	Diffusion des révocations et durée de validité déterminantes	Confirmation au contrôleur ; prévoir les coupures réseau
Tracer les événements	Preuves organisationnelles de remise et d’utilisation	Vérifier mémoire, lecture et horodatage	Sécuriser collecte, transmission et analyse
Maîtriser les pannes	Accès mécanique de secours et disponibilité des clés	Source d’énergie, droits locaux et procédures de remplacement	Réserve électrique, autonomie locale et reprise

« Électromécanique » ou « sans pile » ne précise pas comment les droits sont actualisés.

La combinaison adaptée dépend de la protection requise, de l’usage et du fonctionnement démontré.

Le système d’accès doit aussi être protégé



Contact et verrouillage : détecter les manipulations, respecter l’évacuation.

Sécuriser l’administration : authentification multifacteur, réseaux séparés et services limités.

Des interfaces définies et limitées relient le réseau d’accès et l’automatisme de procédé.

Protection physique des portes et durcissement numérique sont conçus ensemble.

La cryptographie protège toute la liaison

Badge ↔ Lecteur	**Lecteur ↔ Contrôleur**	Contrôleur ↔ Serveur
Vérifier l’authenticité ; compliquer la copie et le rejeu des signaux.	Authentifier les messages ; protéger l’intégrité et la confidentialité requise.	Vérifier les correspondants ; sécuriser transmission et administration.

Clés Générer → protéger → distribuer → renouveler → révoquer / supprimer

Mises à jour Vérifier provenance et intégrité ; n’accepter que les micrologiciels autorisés.

Adapter méthodes et paramètres au risque ; aucune obligation générale d’AES-256 ou de TLS 1.3.

Le CRA complète la sécurité des produits

CER et NIS-2 guident le concept de protection.

Lecteurs et contrôleurs

Paramètres sûrs par défaut, protection des accès et intégrité

Logiciel de gestion

Traiter les vulnérabilités, fournir des mises à jour sûres

Cycle de vie du produit

Documenter la conformité, annoncer la fin de l’assistance

Évaluer concrètement support, périmètre du produit et modifications.

CRA : art. 13–14 et 71. Obligations principales dès le 11.12.2027, notifications des fabricants depuis le 11.09.2026.

Lignes directrices CRA au Journal officiel de l’UE

17.11.2026

C/2026/6013

67 exemples pratiques · 24 langues officielles de l’UE

Interprétation de la Commission

Sans force juridique obligatoire. L’évaluation au cas par cas reste déterminante.

11.09.2026 Obligations de notification
11.12.2027 Obligations principales

Les dates d’application restent inchangées.

Communication C/2026/6013, points 6–8. Actualité de la Commission mise à jour le 18.11.2026.

Les produits hors ligne peuvent aussi être concernés

L’échange d’informations numériques est déterminant.

Exemple de produit	Connexion numérique	Évaluation
Lecteurs, contrôleurs, Logiciel de gestion	Communication avec des appareils ou des réseaux	Examiner produit et interfaces au regard du CRA
Serrure électronique hors ligne	Données via badge, clé ou programmateur	Le fonctionnement hors ligne ne suffit pas à justifier une exclusion
Mécanique pure ou simple contact de commutation	Aucune transmission de données codées numériquement	La connexion de données peut manquer. Examiner séparément les produits raccordés

Application EIWTC : documenter le périmètre du produit pour chaque composant.

CRA art. 2, § 1. Lignes directrices, points 26–28. Exemples transposés au contrôle d’accès.

Examiner les fonctions cloud avec le produit

Trois critères pour un traitement de données à distance associé

1. Le traitement s’effectue à distance.
2. Sans lui, au moins une fonction du produit ne fonctionne plus.
3. Le logiciel est développé sous la responsabilité du fabricant.

Exemple de l’usine d’eau potable

Les portes peuvent rester opérationnelles localement. Une fonction cloud nécessaire à la gestion centrale des droits peut néanmoins appartenir au produit.

Clarifier périmètre, responsabilité des mises à jour et dépendances tierces.

CRA art. 3, points 1–2. Lignes directrices, section 8, notamment points 184, 189 et 202.

Le support suit l’utilisation prévisible

Exigence CRA

En principe, au moins 5 ans.

Une utilisation prévisible plus longue exige un support prolongé en conséquence. Si elle est plus courte, sa durée s’applique.

Conception et exploitation

Planifier la durée d’utilisation. Connaître la fin précise du support. Vérifier le support restant. Définir les mises à jour et la migration.

Exemple de conception : 15 ans d’utilisation. Aucune durée légale générale imposée.

L’engagement doit correspondre au cycle de vie prévu du produit.

CRA art. 13, § 8, 9 et 19. Lignes directrices, points 125–135. Distinguer disponibilité des mises à jour et support.

Des modifications peuvent entraîner un rôle de fabricant

Maintenance prévue

Réparation, configuration et mises à jour dans le cadre déjà évalué. Pas automatiquement substantielles.

Nouvelle fonction ou nouveau risque

Ouverture à distance, connexion cloud ou gestion externe des clés. Évaluer les effets au cas par cas.

Rôle éventuel de fabricant

Modifier substantiellement le produit puis le mettre à disposition : examiner l’art. 22.

Définir l’évaluation et les responsabilités avant la transformation.

CRA art. 3, point 30, art. 21–22 et 71. Lignes directrices, section 4. Application générale dès le 11.12.2027.

Les notifications CRA couvrent aussi le parc existant

Déclencheur de notification pour le fabricant

Connaissance d’une vulnérabilité activement exploitée dans le produit ou d’un incident grave affectant sa sécurité.

Également les anciens produits

Mis sur le marché avant le 11.12.2027 : la notification s’applique déjà.

Également après la fin du support

Notifier dès connaissance de l’événement. Pas de nouvelle obligation automatique de mise à jour.

Les exploitants examinent aussi NIS-2 et CER. Pas de remplacement général en 2027.

CRA art. 14 et 69. Lignes directrices, points 209–218, notamment 210. Comparaison des délais : diapositive 44.

Informations du fabricant pour une exploitation sûre

Sujet	Information pour l’équipe d’exploitation
Produit et catégorie	Périmètre, version, fonction principale et informations de conformité
Cycle de vie	Utilisation prévue, période de support et date précise de fin
Mises à jour de sécurité	Distribution, intégrité et responsabilité de l’installation
Cloud et dépendances	Services associés, responsables et comportement en cas de panne
Vulnérabilités et notification	Contact de sécurité joignable et circuits d’escalade convenus
Modifications et remise	Évaluation et validation des modifications, tests fonctionnels et de panne

Associer informations du fabricant et processus d’exploitation clairs.

Conception et exploitation : CRA art. 7, 13–14, 21–22 et lignes directrices, sections 4–9.

Badge perdu : quand le blocage devient-il effectif ?

Perte signalée

Vérifier l’identité.
Bloquer le badge.
Limiter activement le risque avant le blocage.

Porte en ligne · Salle de conduite

Blocage diffusé ? Contrôleur confirmé ?
Tentative d’accès effectivement refusée ?

Porte hors ligne · Station de pompage

Mise à jour locale ou expiration du droit.
D’ici là : mesure compensatoire prédéfinie.

Mesurer le délai à la serrure réelle, y compris lorsque la connexion est interrompue.

Panne électrique ou réseau : l’exploitation doit agir

1 **Connexion interrompue**

Les droits locaux et les règles de blocage définies restent actifs.

2 **Alimentation perturbée**

Dimensionner porte, contrôleur et alimentation selon le besoin de protection.

3 **Accès de secours nécessaire**

Le personnel autorisé atteint l’installation critique.

4 **Système de nouveau disponible**

Synchroniser de façon contrôlée droits, heure et événements.



Définir pour chaque porte : évacuation, protection contre l’accès et rétablissement sûr.

Exercice commun : maîtriser le déroulement

08:10

Le réseau tombe en panne

Un technicien doit atteindre la salle de conduite.

CER : accès de secours réussi, évacuation garantie.

08:20

Badge perdu

Le droit est encore enregistré à la station de pompage.

NIS-2 : limiter le risque résiduel, prouver le blocage.

08:35

Le système redémarre

Droits, heure et événements sont synchronisés.

Ensemble : tester les fonctions, évaluer les incidents.

Défaut produit : le CRA complète le dispositif. Associer le fabricant et vérifier une correction sûre.

Un incident peut déclencher deux notifications

Exemple : une manipulation du contrôle d’accès perturbe l’exploitation de l’usine.

NIS-2	**24 h** Alerte précoce	**72 h** Notification d’incident	**1 mois*** Rapport final
CER	**24 h** Première notification	**1 mois** Rapport détaillé, si pertinent	**HCPN** Canal compétent

* NIS-2 : un mois après la notification d’incident. Premiers délais à compter de la prise de connaissance.

Évaluer chaque seuil de gravité ; notification du fabricant au titre du CRA distincte.

Démontrer l’état de l’art lors de l’audit

Salle de conduite

Un badge perdu doit devenir inutilisable de manière fiable.

Le délai admissible découle de l’analyse des risques.

Exigence

Objectif, délai admissible et responsables sont définis par écrit.

Solution

Architecture, paramètres sûrs et assistance fabricant répondent à l’objectif.

Test d’exploitation

Le badge est refusé à la porte réelle. Coupure réseau et reprise sont également testées.

Documentation

Procès-verbal, écarts et mesures montrent le résultat et les responsabilités restantes.

La preuve relie analyse des risques, choix du produit et efficacité en exploitation.

La réception technique exige des preuves vérifiables

Objectif de protection	Question de contrôle	Preuve adaptée
Identité et droits	Les appareils sont-ils identifiables sans ambiguïté et les droits effectivement révocables ?	Concept d'identité, tests de blocage et de rôles
Communications protégées	Authenticité, intégrité et confidentialité requise sont-elles protégées de bout en bout ?	Concept protocolaire/cryptographique, contrôle de configuration
Micrologiciels et mises à jour	Le produit n'accepte-t-il que des mises à jour autorisées et non altérées ?	Tests de mise à jour et de rejet, contrôle de signature
Clés et certificats	Renouvellement, révocation et remplacement après compromission fonctionnent-ils ?	Procédures de cycle de vie, tests d'expiration et de révocation
Disponibilité et assistance	Le mode dégradé défini fonctionne-t-il jusqu'à la fin de vie prévue ?	Test de panne, engagement d'assistance, plan de remplacement et de migration

Aucune prescription universelle pour AES-256, TLS 1.3, HSM ou les méthodes post-quantiques.

Inscrire durablement les preuves dans le SMSI

SMSI = système de management de la sécurité de l’information



Risque	Mesure	Preuve	Amélioration
Badge perdu à la station de pompage	Validité limitée et procédure de blocage	Test de blocage et journal d’événements	Corriger l’écart et tester à nouveau

Un ensemble commun de preuves

Zonage · Revue des droits · Configuration · Maintenance · Incidents · Comptes rendus d’exercice

Une maturité documentée facilite la surveillance ; elle n’exonère pas automatiquement des audits.

Plan de mise en œuvre pour l’usine

01–30

Classer et recenser

Champ d’application et enregistrement
Zones, actifs et prestataires
Clés et droits d’accès

31–60

Combler les lacunes

Analyse des risques et priorités
Choix technique et révocation
Accès de secours et engagements produit

61–90

Tester et pérenniser

Tests de panne et de reprise
Formation et preuves
SMSI et revue continue des droits

Exemple de plan de travail. Les délais légaux et liés à la désignation sont prioritaires.

Quatre décisions pour une protection efficace

1 **Confirmer le besoin de protection**

Définir service d’eau potable, zones et interruptions maximales admissibles.

2 **Relier les responsabilités**

Engager ensemble direction, exploitation, informatique, RH et fournisseurs.

3 **Valider le concept d’accès**

Financer révocation, mode dégradé, cryptographie et assistance.

4 **Démontrer l’efficacité**

Planifier un test commun de panne et évaluer les preuves.

CER et NIS-2 guident le programme. Le CRA renforce les produits utilisés.

CER : secteurs et exploitants types

01 **Énergie**
Réseau électrique, fourniture de gaz, stockage d’énergie

02 **Transports**
Aéroport, infrastructure ferroviaire, transports publics

03 **Secteur bancaire**
Établissements de crédit

04 **Infrastructures des marchés financiers**
Plateformes de négociation et contreparties centrales

05 **Santé**
Hôpitaux et autres prestataires concernés

06 **Eau potable**
Fourniture et distribution d’eau potable

07 **Eaux usées**
Collecte, traitement et évacuation

08 **Infrastructure numérique**
Centres de données, cloud, DNS et télécommunications

09 **Administration publique**
Entités publiques centrales concernées

10 **Espace**
Exploitants d’infrastructures terrestres concernées

11 **Denrées alimentaires**
Production industrielle, transformation et commerce de gros concernés

12 **Gestion des déchets**
Collecte, traitement et élimination des déchets concernés

L’entité devient critique par désignation officielle selon l’art. 7 de la loi CER.

CER : délais et fonctions sensibles

Désignation

Notification à l’entité

9 mois

Réaliser l’analyse des risques

10 mois

Chapitre 4 applicable en principe

Actualiser l’analyse des risques

Selon les besoins, au moins tous les quatre ans.

Vérifications des antécédents

Fonctions sensibles définies par la loi. Respecter consentement et procédure prévue.

Décision valable cinq ans. Demander le renouvellement six à quatre mois avant l’expiration.

La catégorie CRA suit la fonction principale

01

Catégorie de base

Les exigences CRA s’appliquent. La procédure dépend des conditions légales.

02

Produits importants

Annexe III, classes I et II. La classe I, point 1, couvre aussi la gestion des accès et les lecteurs d’authentification.

03

Produits critiques

Catégories spécifiques à l’annexe IV. Examiner la procédure et la certification séparément.

L’usage en infrastructure critique ne suffit pas à rendre un produit critique au sens du CRA.

CRA art. 7–8 et annexes III–IV. Règlement d’exécution (UE) 2025/2392, annexe I. Lignes directrices, section 6.

Notifications : déclencheurs et rapports de suivi

Régime / déclencheur	Première notification	Notification de suivi	Rapport final
NIS-2 Incident important	24 h après connaissance	72 h après connaissance*	1 mois après la notification de l'incident*
CER Perturbation importante	24 h après connaissance	Pas d'étape générale à 72 h	Rapport détaillé sous 1 mois, si pertinent
Fabricant CRA : vulnérabilité activement exploitée	24 h après connaissance	72 h après connaissance	14 jours après disponibilité d'une correction ou atténuation
Fabricant CRA : incident de sécurité grave	24 h après connaissance	72 h après connaissance	1 mois après la notification de l'incident à 72 heures

Délais maximaux : notifier sans retard. * NIS-2 : règles particulières pour les services de confiance et incidents persistants.

CRA art. 14, § 1–6. Lignes directrices, points 209–218. Appliquer séparément les règles nationales NIS-2 et CER.

La résilience nationale exige des responsabilités liées

Organismes publics

La SNR prévoit des responsables de résilience et des plans de continuité dans toutes les institutions publiques.

Préparation civile et militaire

Services essentiels, transports et logistique soutiennent aussi la capacité d’action de l’Alliance.

Lien avec notre usine

Coordonner contacts de crise, ressources de remplacement et reprise avec les autorités compétentes.

La SNR fixe le cadre stratégique ; les obligations concrètes des entreprises découlent du droit.

Bases juridiques au Luxembourg

NIS-2 au Luxembourg	Loi du 5 mai 2026, Mémorial A 225 legilux.public.lu · A 225
CER au Luxembourg	Loi du 5 mai 2026, Mémorial A 226 legilux.public.lu · A 226
Mesures de sécurité	ILR/N26/10 du 26 octobre 2026 ILR · Notification des mesures de sécurité
Résilience et surveillance	Stratégie nationale et indications des autorités letzprepare.public.lu hcpn.gouvernement.lu ilr.lu

CER/NIS-2 : base du 13.10.2026 avec compléments ponctuels. Sources CRA : 19.11.2026.

CRA : bases juridiques et interprétation

Règlement (UE) 2024/2847	Base juridique contraignante du CRA EUR-Lex · Règlement sur la cyberrésilience
Règlement d’exécution (UE) 2025/2392	Catégories techniques de produits contraignantes EUR-Lex · Annexe I, classe I, point 1
Communication C/2026/6013	Orientations non contraignantes du 17.11.2026 EUR-Lex · Lignes directrices en allemand
Actualité de la Commission	27.07.2026, dernière mise à jour le 18.11.2026 Commission européenne · 67 exemples, 24 langues officielles

Articles, points et liens complets figurent également dans les notes de l’intervenant.