LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Luxembourg, le 2 avril 2026

Lettre circulaire à l'attention des ministères, administrations et services de l'État et aux établissements publics

Objet : Transposition de la directive « NIS 2 ».

Je vous prie de trouver ci-joint une circulaire relative à la transposition de la directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 Décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive dite « SRI 2 » ou « NIS 2 »), que je vous prie de bien vouloir diffuser à l'ensemble des administrations et services de l'État ainsi qu'aux établissements publics relevant de votre tutelle.

Le Premier ministre,

Luc FRIEDEN

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Luxembourg, le 2 avril 2026

Circulaire aux ministères, administrations et services de l'État et aux établissements publics

Objet : Transposition de la directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive dite « SRI 2 » ou « NIS 2 »).

Résumé synthétique

La présente circulaire a pour objet :

- d'informer les entités de l'État des implications de la transposition de la directive (UE) 2022/2555 dite NIS 2, qui renforce le cadre européen de cybersécurité et s'applique à l'administration publique ;
- de présenter l'accompagnement mis à disposition par les acteurs nationaux compétents pour soutenir les entités de l'État dans leur mise en conformité ;
- d'annoncer l'organisation de séances d'information dédiées à la directive NIS 2, destinées à faciliter la compréhension des exigences et la préparation des entités concernées.

1. Contexte et objectifs de la directive NIS 2

La directive NIS 2 vise à renforcer la cybersécurité dans toute l'Union européenne. Elle remplace la directive NIS 1 de 2016 et harmonise les exigences à travers les États membres en fixant des règles communes pour assurer un niveau approprié de sécurité des réseaux et systèmes d'information. Les entités de l'État sont désormais concernées.

2. Implications pour les entités de l'État

2.1 Pourquoi les entités de l'État sont-elles directement concernées ?

La directive NIS 2 et le projet de loi n° 8364 définissent ce qu'il y a lieu d'entendre par « entité de l'administration publique » et selon les critères cumulatifs de cette définition les entités de l'État tombent sous cette définition. Ainsi, ces entités sont directement visées en tant qu'entités essentielles (indépendamment de leur taille) par les dispositions applicables.

2.2 Obligations pour les entités de l'État

Les entités de l'État seront notamment tenues de prendre les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques pesant sur la sécurité de leurs réseaux et systèmes d'information.

Ces mesures doivent garantir un niveau de sécurité adapté aux risques, en tenant compte de l'état des connaissances et, le cas échéant, des normes européennes et internationales applicables, ainsi que du coût de mise en œuvre.

Lors de l'évaluation de la proportionnalité de ces mesures, il convient de tenir compte du degré d'exposition aux risques et de la probabilité de survenance d'incidents et de leur gravité, y compris leurs conséquences sociétales et économiques.

Ces mesures devront être fondées sur une approche « tous risques » qui vise à protéger les réseaux et les systèmes d'information ainsi que leur environnement physique contre les incidents, et elles comprennent notamment :

- La mise en place d'une gouvernance de la cybersécurité, comprenant notamment l'implication et la formation continue des membres des organes de direction, l'attribution formelle des responsabilités en matière de cybersécurité et l'intégration de la cybersécurité dans la gestion des projets, etc. ;

- L'analyse et l'évaluation des risques liés à la cybersécurité pesant sur les réseaux et systèmes d'information ;

- La gestion des incidents de cybersécurité, y compris la notification à l'autorité compétente (ILR) des incidents ayant un impact important susceptibles de nuire à la fourniture des services de l'entité, selon les modalités et les délais définis ;

- L'assurance de la continuité des activités et la gestion de crises ;

- La définition et la mise en œuvre des politiques en matière de gestion de la cybersécurité telles que la sécurité des ressources humaines, la gestion des identités et des accès ; le recours systématique à l'authentification forte, la gestion des actifs, la cryptographie, la sécurisation des communications, etc. ;

- La sécurité de la chaîne d'approvisionnement y compris les aspects liés à la sécurité concernant les relations entre les entités et leurs fournisseurs ou prestataires de services directs ;

- La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information, y compris la gestion et la divulgation des vulnérabilités ;

- La sensibilisation des agents de l'État aux bonnes pratiques de cybersécurité et intégration de la cybersécurité dans les programmes de formation continue.

Dans ce contexte, les organes de direction des entités sont tenus d'approuver les mesures de gestion des risques en matière de cybersécurité, de superviser leur mise en œuvre, et de suivre des formations adaptées afin de disposer des connaissances et compétences nécessaires pour évaluer et encadrer les risques cyber.

Les entités de l'État procèdent également à la notification, auprès de l'autorité compétente (ILR), des mesures de sécurité mises en œuvre afin de démontrer leur conformité aux obligations de gestion des risques prévues par le cadre NIS2.

3. Se préparer dès maintenant

La transposition de la directive NIS 2 en droit national est actuellement en cours par le biais du projet de loi n° 8364.

Nous recommandons vivement aux entités de l'État d'entamer dès à présent les démarches de préparation :

- Répertorier les activités essentielles et les systèmes qui les supportent ;

- Initier une autoévaluation de maturité en cybersécurité ;

- Sensibiliser les membres des organes de direction et les agents aux risques cyber ;

- Mettre en place un processus de gestion des incidents ;

- Suivre les recommandations de l'ILR et d'autres acteurs appropriés.

4. Ressources et support

Plusieurs institutions sont à disposition pour accompagner les entités de l'État dans la mise en œuvre des exigences NIS 2 :

- L'ILR organise régulièrement des séances d'informations NIS 2, en collaboration notamment avec le HCPN/ANSSI et le CTIE ;

- Le Haut-Commissariat à la Protection Nationale (HCPN), dans sa fonction d'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), accompagne les entités de l'État dans l'amélioration de leur sécurité de l'information et leur mise en conformité avec les exigences de la directive NIS 2. Cet accompagnement se décline notamment à travers les actions suivantes:

    - Mettre à disposition un cadre de référence complet, comprenant un guide structuré présentant les étapes clés pour initier une démarche de sécurité de l'information, un modèle de Politique Générale de Sécurité de l'Information (PGSI), des politiques thématiques et lignes directrices associées ainsi que des modèles (« templates ») opérationnels.

    - Conseiller et soutenir les entités de l'État dans la mise en œuvre concrète et opérationnelle de ce cadre de référence.

    - Accompagner, à leur demande, les entités de l'État dans la réalisation d'analyses de risques, notamment au moyen d'une macro-cartographie offrant une vision globale ou d'une approche orientée services, plus opérationnelle.

- Le Haut-Commissariat à la Protection Nationale (HCPN), dans sa fonction de CERT Gouvernemental (GOVCERT.LU), est compétent pour assister les entités publiques dans la gestion des incidents de cybersécurité affectant leurs systèmes d'information.

- L'institut national d'administration publique (INAP) organise également des formations relatives à la sécurité de l'information. Ces formations, élaborées en concertation avec le HCPN/ANSSI, comprennent notamment une *sensibilisation à la sécurité de l'information* et une *Cybersecurity Escape Room*. Des formations à destination des organes de direction et des agents impliqués dans la cybersécurité seront également intégrées au catalogue de l'INAP.

- Le Centre des technologies de l'information de l'État (CTIE), en tant que fournisseur de services IT privilégié de l'État est également soumis à la directive NIS 2. La sécurité de l'information des services proposés est gérée et assurée par des mesures techniques et organisationnelles adéquates afin de garantir un niveau approprié de confidentialité, d'intégrité, de disponibilité et de résilience. Dans ce cadre, les modalités et garanties de sécurité, ainsi que les informations utiles et nécessaires sont mises à disposition sur le portail LogON (https://logon.etat.lu), permettant à l'entité d'implémenter les exigences NIS 2 en toute autonomie.

L'ILR, le HCPN/ANSSI et le CTIE ont par ailleurs le plaisir de vous convier à leurs prochaines séances d'information sur la directive NIS 2, à destination des organes de direction. Ces séances se dérouleront en présentiel et en ligne. Les informations pratiques, dont notamment les dates et les modalités d'inscription, sont disponibles via le lien suivant : https://pretix.eu/ILR-NIS2-information-session/rybml/.

Enfin, je vous prie de bien vouloir vous adresser aux institutions suivantes pour toute question relative à la présente circulaire :

Entité	Domaine de responsabilité	Adresse mail
ANSSI	Accompagnement en matière de sécurité de l'information	support@anssi.etat.lu
CTIE	Fournisseur de services IT	Division Organisation et support, service Délivrance des services : servicemanagement@ctie.etat.lu Division sécurité de l'information, service Gouvernance, risques et conformité : dsi.grc-int@ctie.etat.lu
GOVCERT.LU	Gestion des incidents de cybersécurité	info@govcert.etat.lu
ILR	Autorité compétente NIS 2	nis2@ilr.lu
INAP	Formations	info@inap.etat.lu