

La directive NIS2 vous concerne-t-elle ?

Trois vérifications fondées sur l'ordonnance d'urgence roumaine (OUG) 155/2024, dans sa version consolidée applicable. L'applicabilité dépend du type d'entité et de l'activité visés à l'annexe, pas seulement du nom général du secteur.

1 Exercez-vous dans l'un des 18 secteurs ?

ANNEXE 1 · SECTEURS HAUTEMENT CRITIQUES

- ☐ Énergie (électricité, réseaux de chaleur et de froid, pétrole, gaz, hydrogène)
- ☐ Transports (air, rail, eau ; la route vise les autorités routières et les exploitants de systèmes de transport intelligents)
- ☐ Banque (voir la note DORA)
- ☐ Infrastructures des marchés financiers (voir DORA)
- ☐ Santé (soins, production et distribution pharmaceutiques, pharmacies)
- ☐ Eau potable
- ☐ Eaux usées
- ☐ Infrastructures numériques (DNS, TLD, cloud, centres de données, communications électroniques, services de confiance)
- ☐ Services TIC gérés (y compris les services de sécurité gérés)
- ☐ Administration publique centrale
- ☐ Espace

ANNEXE 2 · AUTRES SECTEURS CRITIQUES

- ☐ Services postaux et de courrier
- ☐ Gestion des déchets (si c'est l'activité principale)
- ☐ Produits chimiques (fabrication, production, distribution)
- ☐ Alimentation (production et transformation industrielles, distribution en gros)
- ☐ Industrie manufacturière (dispositifs médicaux, électronique et optique, équipements électriques, machines, véhicules et autres matériels de transport)
- ☐ Fournisseurs numériques (places de marché en ligne, moteurs de recherche, réseaux sociaux)
- ☐ Recherche

Base : annexes 1 et 2 de l'OUG 155/2024

Transport routier : d'autres activités ou situations peuvent entraîner l'inclusion. **DORA** : les risques TIC des entités financières concernées relèvent du régime sectoriel spécial. Une mention dans une annexe NIS2 n'implique pas le cumul intégral des mêmes obligations. L'identification et l'enregistrement sont vérifiés séparément.

2 Remplissez-vous les critères légaux de taille ?

L'effectif n'est pas le seul critère. Moins de 50 salariés n'entraîne pas une exclusion automatique. Vérifiez les seuils légaux, les règles des entreprises partenaires ou liées et les catégories visées quelle que soit leur taille.

- ☐ **Moyenne entreprise** : 50–249 salariés et chiffre d'affaires ≤ 50 millions EUR ou actifs ≤ 43 millions EUR.
- ☐ **Visées quelle que soit la taille** : par exemple, administration publique centrale, services DNS, registres TLD et services de confiance. Liste non exhaustive.
- ☐ **Grande entreprise** : au-delà des seuils de la moyenne entreprise.

Base : art. 5–9, OUG 155/2024 ; art. 4, loi 346/2004

3 Avez-vous des clients dans ces secteurs ?

- ☐ Nous fournissons des produits ou des services à des entités dans les secteurs à l'étape 1 (IT, logiciels, maintenance, logistique, conseil ou tout service ayant accès à leurs systèmes ou données)

Les entités concernées doivent gérer les risques de sécurité liés aux fournisseurs directs et prestataires. Elles peuvent imposer des exigences contractuelles proportionnées aux risques (art. 11 et 13, OUG 155/2024).

COMMENT LIRE LE RESULTAT

Secteur de l'annexe 1 et grande entreprise ; administration publique centrale, services DNS, registres TLD, services de confiance qualifiés

Très probablement une entité essentielle
Art. 5

Secteur de l'annexe 1 et moyenne entreprise ; secteur de l'annexe 2 et moyenne ou grande entreprise

Très probablement une entité importante

Des exceptions existent : certaines catégories sont essentielles même de taille moyenne ou quelle que soit leur taille, dont les prestataires de sécurité gérée (MSSP). La classification finale est vérifiée selon les art. 5–9 de l'OUG 155/2024.

Seule l'étape 3 s'applique

Si vous ne remplissez pas vous-même les critères d'applicabilité directe, vos clients concernés peuvent imposer des exigences contractuelles de sécurité. Le seul statut de fournisseur ne suffit pas à établir l'applicabilité de NIS2.

Calendrier des obligations

Les délais courent à partir d'événements différents pour chaque entité. Identifiez d'abord votre situation dans ce parcours.

DÉLAI	OBLIGATION	POINT DE DÉPART ET EXIGENCES	BASE
30 jours	Notification d'enregistrement	Soumettre dans les 30 jours suivant la date à laquelle l'entité devient assujettie aux dispositions applicables.	Art. 18(2)
30 jours	Désignation du responsable de la sécurité	De la notification de la décision d'enregistrement, sous réserve des conditions pour la catégorie de rôle et d'entité. Un contrat de soutien informatique ne constitue pas, en soi, la nomination statutaire.	Art. 14(3)–(4)
60 jours	Transmission de l'évaluation du niveau de risque	Pour les entités soumises à cette procédure: de la notification de la décision d'enregistrement. Le niveau d'assurance résultant diffère du statut juridique de l'entité importante ou essentielle.	Art. 18(6)
60 jours	Autoévaluation initiale de maturité	Préparer et soumettre dans les 60 jours suivant la présentation de l'évaluation du niveau de risque.	Art. 18(7)
30 jours	Transmission du plan de remédiation	Les entités essentielles soumettent le plan dans les 30 jours suivant l'autoévaluation, ce qui correspond à la date limite de soumission du plan, et non à celle de la totalité de l'assainissement.	Art. 12(5)
Tous les ans	Autoévaluation périodique	Résultats annuels, approuvés par la direction et présentés selon la procédure applicable.	Art. 12(4)
24 h · 72 h	Signalement d'un incident important	Alerte précoce sous 24 heures et notification de l'incident sous 72 heures, à compter de sa découverte. Rapport final sous un mois après la notification, avec des règles spécifiques pour les incidents en cours. Rapport intermédiaire à la demande de l'autorité ; délai particulier pour les prestataires de services de confiance.	Art. 15(7)–(8)

AU-DELÀ DES FORMALITÉS

Agir au-delà de l'enregistrement

L'enregistrement et l'autoévaluation ne remplacent pas la mise en œuvre : gestion des risques, sécurité des accès et systèmes, gestion des incidents, continuité, sauvegardes, sécurité des fournisseurs, formation et contrôle de l'efficacité des mesures.

Base : art. 11 et 13, OUG 155/2024

POUR LA RÉUNION DE DIRECTION

Cinq questions à poser

- ☐ Savons-nous, par écrit, si nous sommes une entité essentielle, une entité importante ou seulement un fournisseur?
- ☐ Avons-nous soumis la notification d'enregistrement et reçu la décision d'enregistrement?
- ☐ Qui est responsable de la sécurité, et à qui se rapportent-ils?
- ☐ Prouvons-nous l'application de nos politiques ?
- ☐ Est-ce que quelqu'un sait quoi faire au cours des 24 premières heures suivant un incident?

ART. 60 DU OUG 155/2024

Ce que prévoit la loi

- **Violations administratives:** certaines infractions, y compris le non-respect des obligations d'enregistrement, entraînent des sanctions pour les actes énumérés à l'article 60. Le plafond dépend de la violation et de la catégorie d'entités.
- **Plafond maximal :** pour les infractions visées, le plus élevé du montant fixe et du pourcentage légal du chiffre d'affaires annuel mondial total de l'exercice précédent : 7 millions EUR ou 1,4 % pour les entités importantes ; 10 millions EUR ou 2 % pour les entités essentielles. L'amende est fixée conformément à la loi.
- **La direction** approuve et supervise les mesures et doit se former. Elle répond, dans les conditions légales, des manquements à ses obligations (art. 14).

A RETENIR

L'autoévaluation couvre les documents et la mise en œuvre effective. Pour certains fournisseurs numériques et services gérés, vérifiez aussi le règlement d'exécution (UE) 2024/2690.

Besoin d'une évaluation raisonnée de l'applicabilité?

Clarified IT prépare votre fiche d'applicabilité : conclusion motivée, obligations et calendrier préliminaire.

it.clarified.ro/nis2

office@clarified.ro · +40 774 456 127

Sources: OUG 155/2024, approuvé avec modifications et ajouts par la loi 124/2025, sous sa forme consolidée applicable; directive (UE) 2022/2555; règlement (UE) 2022/2554 (DORA); loi 346/2004. Cette liste de contrôle est informative: elle offre des orientations basées sur les informations disponibles et ne remplace pas l'évaluation de la situation spécifique ou de la décision ou des pouvoirs de l'autorité.