Qu’est-ce que la directive NIS2 ?

À l’ère du numérique, la cybersécurité est une préoccupation majeure pour les individus et les organisations en raison de la fréquence croissante des cyberattaques. Consciente de cette situation, la Commission européenne a introduit en 2016 la directive sur la sécurité des réseaux et de l’information (NIS) afin de renforcer la cybersécurité dans l’ensemble de l’Union européenne. Cependant, la directive n’a pas été suffisamment responsabilisée, ce qui a incité la Commission à prévoir son remplacement par la directive NIS2, plus robuste.

La NIS2 oblige les entreprises à mettre en œuvre des mesures de cybersécurité essentielles, notamment la sécurité de la chaîne d’approvisionnement, la cryptographie et le cryptage (article 18). L’article 89 met l’accent sur l’adoption de pratiques d’hygiène cybernétique de base, telles que les principes de confiance zéro, les mises à jour logicielles, la configuration des appareils, la segmentation du réseau et la gestion des identités et des accès pour les entités essentielles et importantes.

NIS vs NIS2 - Qu’est-ce qui a changé ?

Il existe des différences importantes entre l’ancienne et la nouvelle directive :

- La nouvelle proposition supprime la distinction entre les opérateurs de services essentiels (OES) et les fournisseurs de services numériques (DSP), et classe les entités comme étant soit essentielles, soit importantes.
- Le champ d’application de la directive est élargi à de nouveaux secteurs en fonction de leur criticité pour l’économie et la société, y compris toutes les moyennes et grandes entreprises de ces secteurs. Les États membres peuvent également identifier des entités plus petites présentant un profil de risque élevé.
- Il est proposé de créer un réseau européen d’organisations de liaison en cas de cybercrise (EU-CyCLONe) afin de travailler collectivement à la préparation et à la mise en œuvre de plans d’intervention d’urgence rapides, par exemple en cas d’incident ou de crise cybernétique de grande ampleur.
- Une coordination accrue de la divulgation des nouvelles vulnérabilités découvertes dans l’ensemble de l’Union. Une liste de sanctions administratives (similaires à celles du GDPR) est établie, y compris des amendes pour violation des obligations de déclaration et de gestion des risques de cybersécurité.
- Le NIS2 impose des obligations directes aux organes de direction pour mettre en œuvre et superviser la conformité de leur organisation avec la législation - ce qui peut entraîner des amendes et l’interdiction temporaire d’exercer des fonctions de direction, y compris au niveau de la direction générale.

En outre, elle introduit des dispositions plus précises sur le processus de notification des incidents, le contenu des rapports et le délai (dans les 24 heures suivant la découverte de l’incident). Au niveau européen, la proposition renforce la cybersécurité des technologies clés de l’information et de la communication. Les États membres, en coopération avec la Commission et l’ENISA, l’agence de l’Union européenne pour la cybersécurité, devront procéder à des évaluations coordonnées des risques liés aux chaînes d’approvisionnement critiques.

À qui s’applique-t-elle ?

Alors que l’ancienne directive NIS laissait aux États membres le soin de déterminer quelles entités répondaient aux critères de qualification des opérateurs de services essentiels, la nouvelle directive NIS2 introduit une règle de plafonnement par la taille. Cela signifie que toutes les moyennes et grandes entités opérant dans les secteurs ou fournissant des services couverts par la directive entreront dans son champ d’application.

Vous trouverez ci-dessous un classement par règle de capitalisation :

Entités essentielles (EE) Seuil de taille : variable selon le secteur, mais généralement 250 employés, chiffre d’affaires annuel de 50 millions d’euros ou bilan de 43 millions d’euros.	**Entités importantes (IE)** Seuil de taille : variable selon le secteur, mais généralement 50 employés, chiffre d’affaires annuel de 10 millions d’euros ou bilan de 10 millions d’euros.
Energie	Services postaux
Transport	Gestion des déchets
Finance	Produits chimiques
Administration publique	Recherche
Santé	Alimentation
Aérospatiale	Industrie manufacturière
Approvisionnement en eau (potable et usée)	Fournisseurs numériques (par exemple, réseaux sociaux, moteurs de recherche, marchés en ligne)
Infrastructure numérique (par exemple, fournisseurs de services d’informatique Cloud et gestion des TIC)	

Le NIS2 couvre également les organismes de l’administration publique au niveau central et régional, mais exclut les parlements et les banques centrales.

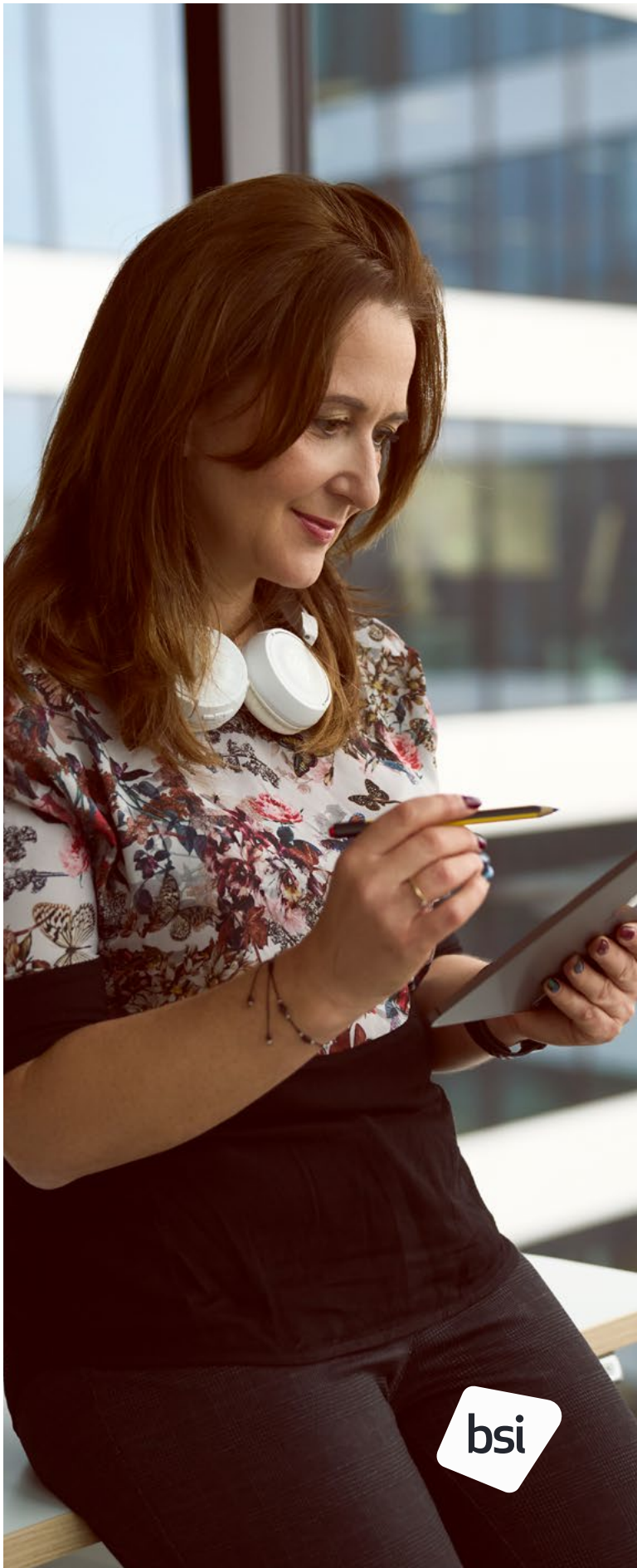
Quand sera-t-elle appliquée ?

Tous les États membres de l'UE doivent intégrer les nouvelles obligations dans leur législation nationale avant le 17 octobre 2024. Suite à l'approbation finale le 16 janvier 2023, les entités couvertes ont reçu une fenêtre de conformité de 21 mois après l'entrée en vigueur de la directive. La liste suivante présente le calendrier de développement du NIS :

- **6 juillet 2016 :** Adoption du NIS
- **9 mai 2018 :** Date limite pour la transposition du NIS en droit national par les États membres
- **7 juillet 2020 :** La Commission européenne lance une consultation sur la réforme du NIS
- **16 décembre 2020 :** La Commission européenne publie une proposition pour le NIS2
- **22 novembre 2021 :** Le Parlement européen adopte sa position de négociation
- **3 décembre 2021 :** Le Conseil européen adopte sa position de négociation
- **13 janvier 2022 :** Premier cycle de négociations du trilogue
- **16 février 2022 :** Deuxième cycle de négociations du trilogue
- **13 mai 2022 :** Accord politique conclu
- **10 novembre 2022 :** Le Parlement européen vote l'adoption du NIS2
- **28 novembre 2022 :** NIS2 approuvé par le Conseil de l'UE
- **27 décembre 2022 :** NIS2 publié au Journal officiel et entrant en vigueur 20 jours plus tard, le 16 janvier 2023
- **17 octobre 2024 :** Date limite pour la transposition du NIS2 en droit national par les États membres

Comment pouvons-nous aider votre entreprise à rester conforme à la norme NIS2 ?

Chez BSI, nous disposons d'une vaste équipe d'experts hautement expérimentés, leaders dans leur secteur, qui vous aideront à vous assurer que vous et votre entreprise disposez de toutes les exigences de sécurité dont vous avez besoin pour anticiper la directive NIS2. Avec notre aide, les organisations peuvent éviter des pénalités financières potentielles et inspirer davantage de confiance à leurs clients. De l'identification initiale de l'OES à l'auto-évaluation, en passant par l'évaluation et le traitement des risques, notre expérience de travail avec des organisations de tous les secteurs peut vous aider à vous mettre en conformité avec la directive NIS2.



BSI offre actuellement les services suivants en relation avec les exigences du NIS2 :

- Stratégie et gouvernance cybernétiques
- Évaluations de la posture/maturité en matière de cybersécurité par rapport à des cadres normalisés de l'industrie
- Sécurité de l'information/développement d'une stratégie cybernétique/présentations au conseil d'administration
- Analyse des écarts et soutien à la mise en œuvre (ISO 27001, SOC 2, NIST CSF/800-53)
- Sensibilisation et formation à la sécurité de l'information Continuité des activités (ISO 22301)

Gestion de crise et réponse aux incidents

- Continuité des Activités (ISO 22301)
  - Analyse de l'impact sur les entreprises/ (BIA)/Élaboration de politiques/Planification de la continuité des activités
- Soutien à la reprise après sinistre, mise en œuvre et tests périodiques
- Test de pénétration à la menace (TLPT)
- Renseignement de source ouverte (OSINT)
- Évaluations de la sécurité physique Simulation d'attaque (équipe rouge/bleue/violette)
- Planification et mise en œuvre de la réponse aux incidents (ISO27035)
- Modélisation des menaces/évaluation des menaces
- Évaluation de la capacité actuelle de planification et de communication des réponses aux incidents
- Test de réponse aux incidents/formation du personnel

Gestion des risques et rapports

- Développement et mise en œuvre du cadre de gestion des risques informatiques (ISO 27005)
  - Gestion des risques liés aux tiers (ISO 27036-2)
  - Évaluation de l'état actuel de la gestion du cycle de vie des tiers
  - Développer un cadre de gestion des fournisseurs de bout en bout
  - Mise en œuvre d'un cadre de gestion des risques par des tiers et soutien permanent à la gestion des risques
- BSI travaille avec des partenaires technologiques qui disposent d'outils facilitant la gestion de l'ensemble du cycle de vie des fournisseurs.
  - Certification Threat Intelligence/Computer Emergency Response Team (CERT)
  - Évaluer la situation actuelle et déterminer l'état futur
  - Élaborer un cadre pour l'établissement de rapports

Pourquoi les normes ISO 27001 et ISO 22301 sont-elles essentielles à la conformité au NIS2 ?

Les règlements du NIS recommandent aux entreprises, dans leurs efforts de mise en conformité, de donner la priorité au «respect des normes internationales». En outre, les lignes directrices techniques de l'Agence européenne pour la cybersécurité (ENISA) alignent chaque objectif de sécurité sur les normes de meilleures pratiques, telles que la norme ISO 27001.

Parmi tous les services que BSI peut fournir à votre entreprise en relation avec NIS2, deux normes semblent être essentielles

- La mise en œuvre d'un système de gestion de l'information (SGI) conforme à la norme ISO 27001 permet aux organisations de minimiser les risques et l'exposition aux menaces de sécurité. Il s'agit d'identifier les politiques nécessaires, d'employer les technologies adéquates et de former le personnel pour éviter les erreurs. En imposant des évaluations annuelles des risques, la norme ISO 27001 permet aux organisations de faire face de manière proactive à l'évolution du paysage des risques.
- La norme ISO 27001 facilite non seulement le respect des exigences du NIS2, mais permet également aux organisations d'obtenir une certification faisant l'objet d'un audit indépendant. Cette certification sert de preuve tangible pour les fournisseurs, les parties prenantes et les régulateurs, en démontrant l'adoption de mesures techniques et organisationnelles «appropriées et proportionnées» et en établissant un avantage concurrentiel sur le marché.
- Pour les organisations qui souhaitent une approche plus poussée, il est recommandé d'ajouter la norme ISO 22301 pour la gestion de la continuité des activités. La norme ISO 22301 facilite la mise en œuvre, le maintien et l'amélioration continue des pratiques de continuité des activités. Alors que la norme ISO 27001 intègre des aspects de la gestion de la continuité des activités (BCM), la norme ISO 22301 fournit un processus défini pour la mise en œuvre de la BCM. La certification ISO 22301 renforce la conformité à la norme NIS2.

La synergie entre les normes ISO 27001 et ISO 22301 permet aux organisations de développer un système de management intégré englobant à la fois un SMSI et un SMCA. Cette approche holistique facilite non seulement la mise en conformité, mais favorise également le développement d'une cyber-résilience solide.

Pourquoi choisir BSI ?

Chez BSI, nos capacités au niveau mondial inspirent confiance aux clients en matière de cybersécurité et d'hygiène. Nous offrons une expertise approfondie en matière de cybersécurité, de gestion des risques et de résilience de l'information, avec une perspective intersectorielle globale. Notre compréhension couvre les questions affectant le secteur public, les menaces émergentes et l'expérience pratique de l'industrie dans la gestion des cyber-risques et de la résilience.

Que faire ensuite ?

- Vérifiez si votre organisation entre dans le champ d'application
- Informez votre direction/conseil d'administration de l'imminence de la réglementation
- Contactez-nous pour obtenir une aide à la mise en conformité avec la norme NIS2 : **sales.fr@bsigroup.com**