2023

Ce qui change avec l'adoption de la nouvelle directive NIS2

Les atouts d'un framework global de sécurité des identités

# L'importance de l'identité pour préparer la conformité à la directive NIS2

okta

# Sommaire

# Introduction

La directive NIS (Network and Information Systems) de l'Union européenne a été adoptée en 2016 et est entrée en vigueur en 2018. Elle avait pour objectif d'assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information au sein de l'UE, exigeait la mise en œuvre de mesures de sécurité et imposait des obligations de signalement aux opérateurs de services essentiels et aux fournisseurs de services numériques. La directive NIS2 est une version mise à jour de la directive NIS de 2016. Elle renforce les mesures de sécurité et les obligations de signalement déjà établies, et s'étend à de nouveaux secteurs d'activité.

Ce livre blanc passe en revue la directive NIS2, explique comment elle peut être mise en correspondance avec des frameworks de sécurité bien connus tels que la norme ISO 27001, souligne l'importance de l'identité et décrit les mesures que les entreprises peuvent prendre pour se préparer à l'implémentation de la directive NIS2.

# Présentation de la directive NIS2

À mesure que les grandes organisations intègreront des contrôles NIS2 à leurs programmes de gestion des risques tiers, la plupart des entreprises devront se mettre en conformité à la directive NIS2 pour rester compétitives.

La directive NIS2 est une version mise à jour de la directive NIS de 2016, visant à améliorer la cybersécurité des entreprises au sein de l'Union européenne qui fournissent des infrastructures essentielles et critiques pour l'économie européenne. La directive NIS initiale a été adoptée en 2016 et est entrée en vigueur en mai 2018. La directive NIS2 a été officiellement adoptée par le Parlement, puis par le Conseil en novembre 2022. Elle est entrée en vigueur le 16 janvier 2023. Les États membres ont désormais jusqu'au 17 octobre 2024 pour intégrer ses mesures à leur législation nationale.

La directive NIS2 s'applique à toutes les entités employant au moins 50 personnes et réalisant un chiffre d'affaires annuel minimum de 10 millions d'euros qui fournissent des services essentiels ou importants pour l'économie et la société européennes, y compris les entreprises et les fournisseurs, ce qui inclut également les entreprises établies en dehors de l'UE qui fournissent des services au sein de l'UE. Bien que la directive prévoie des exclusions pour les entreprises de petite taille, les grandes entreprises intègreront sans doute des contrôles NIS2 à leurs programmes de gestion des risques tiers. La plupart des entreprises devront donc se conformer à la directive NIS2 pour rester compétitives.

La directive exige des entités concernées qu'elles mettent en œuvre des mesures techniques et organisationnelles appropriées et proportionnées afin de réduire les risques pesant sur les réseaux et les systèmes d'information ainsi que sur l'environnement physique, y compris les datacenters. Elle oblige également les entreprises à signaler les incidents de sécurité aux autorités compétentes et introduit des exigences de signalement plus strictes pour celles fournissant des services d'infrastructure numérique.

# Préparation à la directive NIS2

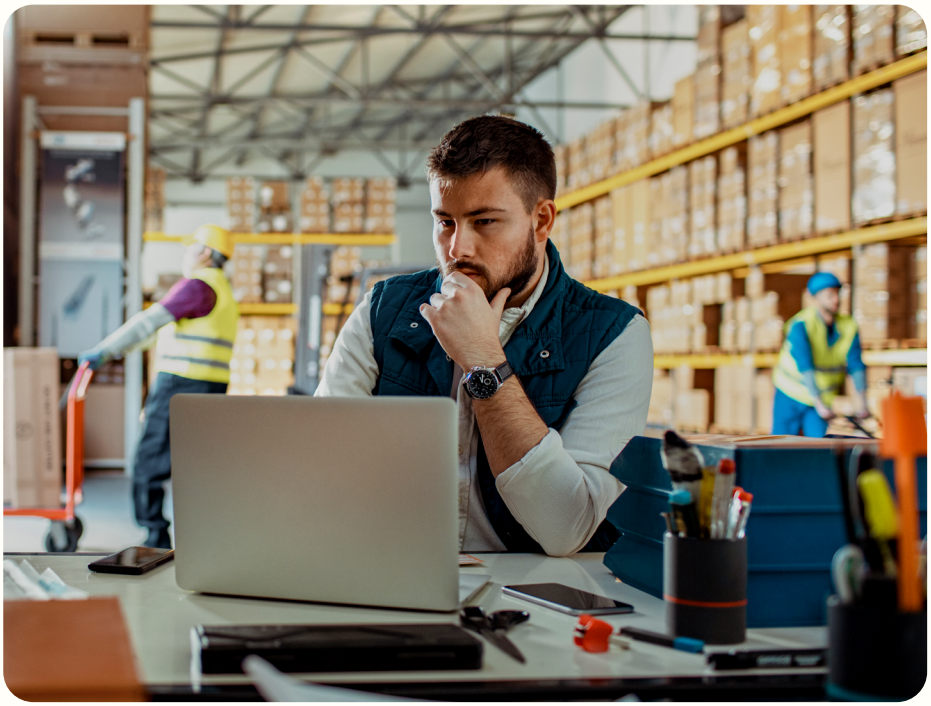
Les États membres de l'UE ont jusqu'à octobre 2024 pour intégrer la directive NIS2 à leur législation nationale. Les entreprises doivent mettre cette période à profit pour commencer à se préparer à la directive en prenant les mesures suivantes :

- **Identifier, évaluer et atténuer vos risques :** la directive NIS2 exige des organes de gestion des entités essentielles et importantes qu'ils prennent des mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques pesant sur les réseaux et les systèmes d'information ainsi que sur l'environnement physique. Les entreprises doivent identifier les risques auxquels elles sont exposées, évaluer leur impact et prendre des mesures pour les atténuer.
- **Évaluer votre niveau de sécurité :** une évaluation des risques et de la sécurité peut faciliter l'identification des vulnérabilités, comme les mots de passe non gérés ou les comptes mal configurés ou inactifs susceptibles d'entraîner des vols d'identifiants. Les entreprises doivent procéder à une évaluation complète de la sécurité afin d'évaluer leur niveau de sécurité et d'identifier les points à améliorer, par exemple en mettant en place des facteurs d'authentification résistants au phishing.
- **Prendre des mesures pour protéger les accès à privilèges :** les cybercriminels peuvent exploiter des comptes à privilèges pour orchestrer des attaques, paralyser des infrastructures critiques et perturber des services essentiels. La directive NIS2 conseille aux entités critiques de limiter l'accès aux comptes administrateur et d'imposer la modification régulière des mots de passe administrateur. Les entreprises doivent prendre les mesures nécessaires pour protéger les accès à privilèges en implémentant de bonnes pratiques telles que l'accès sur le principe du moindre privilège, l'authentification continue et l'analyse des menaces.

# Octobre 2024

Date limite à laquelle la directive NIS2 doit être intégrée aux législations nationales

- **Renforcer vos défenses contre les ransomwares :** coûteuses et paralysantes, les attaques de ransomware sont une préoccupation majeure pour les autorités réglementaires de l'UE et l'un des principaux moteurs de la directive NIS2. Les entreprises doivent adopter des solutions et de bonnes pratiques de sécurité pour se défendre de façon proactive contre les ransomwares. Cela passe par l'utilisation de solutions de protection des endpoints à privilèges pour appliquer le principe du moindre privilège, contrôler les applications, ainsi que renforcer les antivirus de nouvelle génération (NGAV) et les solutions EDR (Endpoint Detection and Response).
- **Adopter une stratégie Zero Trust :** les architectures de sécurité traditionnelles basées sur le périmètre, conçues pour défendre les frontières du réseau des entreprises, ne sont pas adaptées aux services cloud et aux effectifs hybrides. Adoptez une approche Zero Trust en implémentant plusieurs couches de défense, comme l'accès sur le principe du moindre privilège, l'authentification continue et l'analyse des menaces, pour valider toutes les tentatives d'accès.
- **Inspecter votre chaîne logistique logicielle :** les attaques de la chaîne logistique constituent une préoccupation importante pour les autorités réglementaires de l'UE et l'un des éléments fondateurs de la directive NIS2. Les entreprises doivent poser un regard neuf sur leur chaîne logistique logicielle et envisager d'implémenter une solution de gestion des secrets afin de réduire les risques.



# L'importance de l'identité pour la conformité à la directive NIS2

La sécurité constitue un défi de taille, car elle implique de gérer l'interaction complexe entre les personnes, les processus et les technologies. Dans le paysage actuel, l'identité joue un rôle déterminant dans l'élaboration des stratégies de cybersécurité et le maintien de bonnes pratiques en ce domaine, tout en assurant la conformité aux frameworks réglementaires tels que la directive NIS2.

L'identité est le fondement des politiques de sécurité, des procédures opérationnelles et des systèmes IT gouvernant l'accès aux informations critiques d'une entreprise. Elle englobe la vérification des identités utilisateurs, l'authentification de leur accès, l'autorisation de leurs actions et permissions, ainsi que la gestion des contrôles d'accès. Une gouvernance efficace des identités garantit que seules les personnes autorisées peuvent accéder à des ressources spécifiques, leur permettant d'utiliser ces ressources de manière appropriée avec les privilèges les moins élevés possible pour s'acquitter de leurs tâches. Les couches de sécurité supplémentaires, comme l'authentification multifacteur (MFA), renforcent encore davantage la protection des identités.

Dans le contexte de la conformité réglementaire, et notamment de la directive NIS2, l'identité est un outil puissant permettant d'atténuer les risques associés aux accès non autorisés. Elle établit la responsabilité au sein de l'entreprise en permettant l'identification des individus responsables d'actions, ce qui améliore la traçabilité. Par ailleurs, la gestion des identités permet une gestion efficace des utilisateurs en rationalisant les processus d'administration et en assurant la sécurité du paysage organisationnel. Une solution de gestion des identités bien développée fournit une piste d'audit facilement accessible pour toutes les applications critiques d'une entreprise, qui démontre le contrôle approprié des accès et la gestion adéquate des autorisations.

L'identité est le fondement des politiques de sécurité, des procédures opérationnelles et des systèmes IT gouvernant l'accès aux informations critiques d'une entreprise.

Voici certains des domaines dans lesquels la gestion des identités facilite la mise en conformité à la directive NIS2 :

1. **Contrôle des accès :** une gestion adéquate des identités utilisateurs permet aux entreprises d'appliquer des mesures robustes de contrôle des accès. En attribuant des identités uniques aux individus ou aux entités, elles peuvent faire en sorte que seul le personnel autorisé peut accéder à des ressources spécifiques ou réaliser certaines actions au sein de leur réseau et de leurs systèmes d'information.
2. **Authentification et autorisation :** la gestion des identités facilite l'implémentation de mécanismes d'authentification robustes, tels que l'authentification multifacteur (MFA), pour vérifier l'identité des utilisateurs avant de leur accorder un accès. Elle permet également aux entreprises de définir des politiques d'autorisation granulaires afin que les utilisateurs disposent de privilèges et d'autorisations appropriés en fonction de leur rôle et de leurs responsabilités.
3. **Résolution des incidents :** en cas d'incident de sécurité, la gestion des identités joue un rôle essentiel dans l'identification des individus ou des entités impliqués. Une gestion adéquate des identités permet aux entreprises de suivre et de retracer les actions effectuées au sein de leurs systèmes, ce qui facilite les investigations sur les incidents, ainsi que leur attribution et leur correction.
4. **Surveillance de la conformité :** la directive NIS2 exige des entreprises qu'elles appliquent des mesures pour gérer les risques pesant sur les réseaux et les systèmes d'information. La gestion des identités permet aux entreprises de surveiller et d'auditer les activités utilisateurs afin de respecter la conformité aux exigences réglementaires, ainsi que de démontrer la responsabilité en documentant qui a accédé à des ressources spécifiques et quand.

En reconnaissant l'importance de l'identité dans les stratégies de cybersécurité et les efforts de conformité, les entreprises peuvent établir une base solide pour protéger leurs actifs informationnels, préserver la conformité réglementaire et favoriser un environnement résilient et sécurisé.

# Framework global de sécurité des identités avec Okta

L'approche complète de la gestion des identités adoptée par Okta est conçue pour protéger les identités numériques et défendre les personnes, les applications et les terminaux d'une entreprise. En reconnaissant que n'importe quel utilisateur, qu'il soit humain ou non, peut acquérir des privilèges et présenter un risque de sécurité, Okta souligne l'importance des identités dans la mise en œuvre de bonnes pratiques de cybersécurité, en particulier selon un modèle Zero Trust.

En se concentrant sur des mécanismes efficaces et adaptables pour réglementer l'accès aux données et sécuriser les informations, les solutions d'Okta intègrent des pratiques d'authentification et d'autorisation continues qui s'alignent sur les principes du Zero Trust. Grâce à un contrôle rigoureux des accès aux ressources cloud et à une surveillance et un audit continus des activités utilisateurs, Okta préserve la conformité tout en réduisant les risques. L'implémentation d'une stratégie d'identité complète est essentielle pour protéger les infrastructures critiques contre diverses menaces, dont les cyberattaques, les ransomwares et les vulnérabilités de la chaîne logistique logicielle.

Qui plus est, elle peut aider les entreprises à se conformer aux exigences de l'article 21 de la directive NIS2, qui couvre les mesures de gestion des risques de cybersécurité et les obligations de signalement, et formule de nombreuses recommandations. Okta propose une large gamme de solutions de sécurité pour défendre les entreprises contre les cybermenaces et protéger les identités et les données sensibles, notamment une solution MFA de pointe résistante au phishing — une exigence explicite de la directive NIS2.

Évolutive et flexible, la plateforme d'Okta permet aux entreprises d'implémenter des approches d'authentification basées sur des politiques au sein de leurs systèmes et de leurs environnements. Les clients peuvent ainsi fournir des services, améliorer l'expérience utilisateur et garantir la confidentialité et la protection des données.

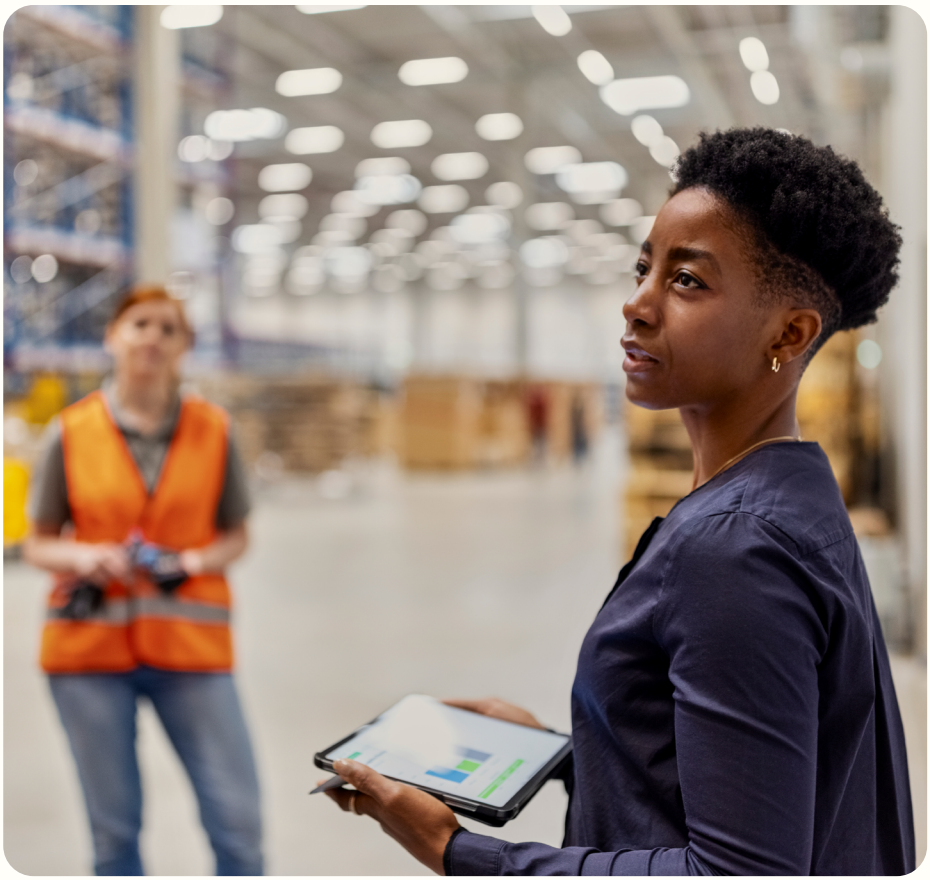
Okta Workforce Identity Cloud (WIC) est une solution qui protège l'accès de tous les utilisateurs (collaborateurs, prestataires et partenaires commerciaux), où qu'ils soient et quel que soit le terminal qu'ils utilisent. Elle est conçue pour aider les responsables à améliorer la productivité et l'efficacité, à moderniser l'IT et l'infrastructure, ainsi qu'à renforcer la sécurité. Par le biais de politiques facilement configurables, Okta Workforce Identity Cloud (WIC) vous permet d'optimiser les mesures de sécurité nécessaires pour chaque catégorie de risques d'accès, offrant le juste équilibre entre frictions de sécurité et facilité d'accès.

L'implémentation d'une stratégie d'identité complète est primordiale pour lutter contre les menaces telles que les cyberattaques, les ransomwares et les vulnérabilités de la chaîne logistique logicielle.

Des solutions telles que Single Sign-On (SSO), Adaptive Multi-Factor Authentication (MFA) et Passwordless Authentication permettent aux entreprises d'améliorer leur niveau de cybersécurité et d'offrir une expérience fluide à leurs collaborateurs.

API Access Management, Advanced Server Access et Access Gateway permettent aux entreprises de centraliser l'administration, de gérer les accès à privilèges et d'automatiser la configuration, ce qui accroît l'efficacité à l'échelle de l'entreprise. La solution Okta Identity Governance (OIG) combine Okta Workflows, Okta Lifecycle Management et Okta Access Governance pour atténuer les risques et améliorer l'efficacité.

Par conséquent, un framework d'identité moderne comme Workforce Identity Cloud aide les entreprises à simplifier leur mise en conformité à la directive NIS2 en améliorant la cybersécurité, en implémentant des processus de gestion des accès plus robustes et en garantissant la distribution fiable de services d'identité avec une disponibilité inégalée.



## Conséquences en cas de non-conformité à la directive NIS2

# Amende de 10 millions €

ou équivalant à 2 % du chiffre d'affaires annuel en cas de non-conformité à la directive NIS2, le montant le plus élevé étant retenu

En cas de non-conformité à la directive NIS2, les entreprises s'exposent à des amendes administratives. La directive NIS2 fait la distinction entre les entités essentielles et les entités importantes. Sont qualifiées « entités essentielles » les entreprises publiques et privées évoluant dans des secteurs comme le transport, l'énergie et les services publics, la santé, l'administration publique et l'infrastructure numérique (y compris les fournisseurs de services cloud), avec une amende de 10 millions d'euros ou équivalant à 2 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu. Le terme « entités importantes » inclut les entreprises publiques et privées évoluant dans des secteurs comme l'alimentation, les produits chimiques, les services postaux, la gestion des déchets, la fabrication, etc., avec une amende de 7 millions d'euros ou équivalant à 1,4 % du chiffre d'affaires annuel, le montant le plus élevé étant retenu. Par ailleurs, l'article 32(5) stipule que les entités essentielles qui ne se conforment pas aux mesures d'application pourraient voir leurs certifications suspendues et leur directeur général interdit d'exercer ses fonctions.

## La directive NIS2 et la sécurisation de votre chaîne logistique

L'intégrité et la sécurité de la chaîne logistique constituent un aspect fondamental de la directive NIS2, compte tenu des conséquences potentiellement dévastatrices observées pendant des événements tels que la pandémie.

Pour réduire le risque de cyberattaques externes, les entreprises ne doivent pas se contenter de procéder à des évaluations régulières des risques pesant sur leur chaîne logistique. Elles doivent impérativement s'assurer que tous les partenaires de la chaîne logistique se conforment quotidiennement aux exigences de la directive NIS2. Cela passe par l'implémentation de mesures de sécurité au sein de la chaîne logistique, comme la réalisation d'évaluations et d'audits des risques liés aux fournisseurs, l'établissement d'ententes contractuelles qui définissent des exigences de sécurité spécifiques et le maintien d'une surveillance et d'une communication continues avec les fournisseurs. En s'assurant que les fournisseurs respectent les exigences de la directive NIS2, les entreprises peuvent réduire efficacement leur risque global et renforcer la sécurité de leur infrastructure numérique. Les entreprises doivent attendre de leurs fournisseurs qu'ils transmettent des rapports de conformité aux normes du secteur (comme la norme ISO 27001) et des rapports de tests d'intrusion externes, et qu'ils autorisent leurs clients à effectuer leurs propres tests d'intrusion.

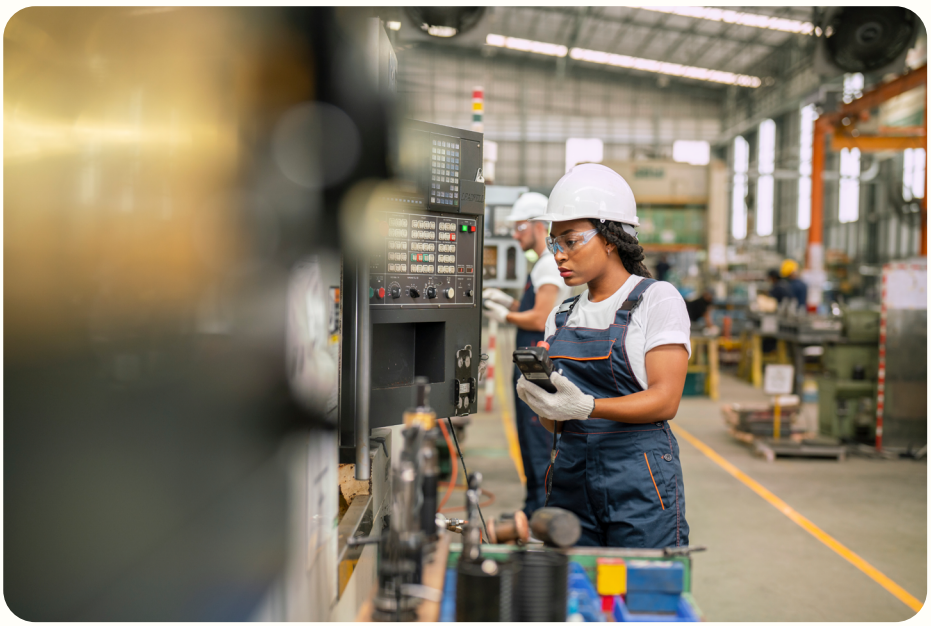
Les solutions Okta Workforce Identity Cloud (WIC) et Okta Customer Identity Cloud (CIC) protègent les identités dans les relations B2B et B2C, et servent de fondement à la mise en conformité à la directive NIS2.

## Formalisation de votre plan de résolution des incidents

La réglementation NIS2 impose un délai de signalement des incidents rapide. En effet, elle exige que le rapport initial soit déposé sous 24 heures, suivi d'un rapport technique dans les 72 heures. Pour respecter cette exigence, il est crucial d'établir un plan de résolution des incidents bien structuré. Okta joue un rôle déterminant dans cette préparation en offrant une visibilité complète sur les tentatives d'autorisation et d'accès pour un large éventail d'infrastructures et de technologies. Cette fonctionnalité aide les entreprises à réduire les délais de reconnaissance des réseaux ou des ressources, un élément essentiel du signalement des incidents. Pour maintenir la conformité aux exigences de la directive NIS2, il est recommandé de passer en revue minutieusement vos procédures de notification d'événements, de collecte d'informations et de signalement. Des exercices doivent être régulièrement organisés pour évaluer et améliorer l'efficacité de votre plan de résolution des incidents.

## Formation de vos collaborateurs

La directive NIS2 insiste sur l'importance des formations aux bonnes pratiques de cybersécurité pour les collaborateurs, les prestataires et les fournisseurs tiers. Redoublez d'efforts pour améliorer la sensibilisation à la cybersécurité et instaurer une culture de la sécurité au sein de votre entreprise. Assurez-vous que les collaborateurs comprennent le rôle qu'ils jouent dans le maintien de la sécurité des réseaux et des systèmes d'information, et qu'ils ont conscience des risques potentiels et des menaces auxquelles ils peuvent être confrontés.



# Mise en correspondance de la directive NIS2 avec la norme ISO 27001

L'ISO 27001 est une norme internationale qui fournit un cadre pour l'établissement, le maintien et l'amélioration continue d'un système de gestion de la sécurité de l'information. Elle est conçue pour aider les entreprises à gérer les risques en la matière et à protéger leurs actifs informationnels.

La directive NIS2 et la norme ISO 27001 partagent un objectif commun : améliorer la sécurité des réseaux et des systèmes d'information. De ce fait, la directive NIS2 peut être mise en correspondance avec la norme ISO 27001, ce qui permet aux entreprises d'utiliser leur certification ISO 27001 existante pour satisfaire aux exigences de la directive NIS2.

Le tableau suivant présente une corrélation indicative, mais non exhaustive, entre les exigences de la directive NIS2 de l'UE et les contrôles ISO 27001 de l'annexe A de la norme ISO/IEC 27001:2023. Compte tenu de la complexité et des objectifs et champs d'application uniques de cet exercice, il est essentiel de noter que cette mise en correspondance générale n'est pas exhaustive. Des spécialistes doivent effectuer une mise en correspondance détaillée adaptée à votre contexte spécifique. Considérez donc ce tableau comme un point de référence initial. Pour mettre pleinement en correspondance la directive NIS2 avec la norme ISO 27001, les entreprises doivent réaliser une analyse des écarts afin d'identifier tout domaine dans lequel l'implémentation de l'ISO 27001 ne respecte pas les exigences de la directive NIS2. Elles doivent ensuite mettre à jour leur système de gestion de la sécurité de l'information pour combler les éventuelles lacunes et contrôler leur conformité à la norme ISO 27001 et à la directive NIS2.

| Domaine | Exigences de la directive NIS2 | Contrôle ISO 27001 pertinent |
|---|---|---|
| **Gestion des risques** | Les entités doivent mettre en place des pratiques de gestion des risques. | A.6.1 (Organisation interne)<br>A.8 (Gestion des actifs)<br>A.12.1 (Procédures et responsabilités opérationnelles) |
| **Sécurité des systèmes et des installations** | Les entités doivent assurer la sécurité de leurs réseaux et de leurs systèmes d'information. | A.11 (Sécurité physique et environnementale) A.12.1 (Procédures et responsabilités liés à l'exploitation) A.13 (Sécurité des communications) A.14 (Acquisition, développement et maintenance des systèmes d'information) |
| **Traitement des incidents** | Les entités doivent être préparées à résoudre les incidents rapidement et de manière appropriée. | A.16 (Gestion des incidents liés à la sécurité de l'information)<br>A.12.6 (Gestion des vulnérabilités techniques) |
| **Gestion de la continuité des activités** | Les entités doivent mettre en place des mesures pour assurer la continuité de leurs services. | A.17 (Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité) |
| **Surveillance, audits et tests** | Les entités doivent procéder à des audits et à des tests réguliers pour valider leurs mesures de sécurité. | A.18.2 (Audit interne)<br>A.12.7 (Considérations sur l'audit du système d'information) |
| **Conformité aux exigences légales et contractuelles** | Les entités doivent se conformer à toutes les exigences de sécurité légales et contractuelles pertinentes. | A.18 (Conformité)<br>A.15.2 (Sécurité de l'information dans la gestion de projet) |
| **Signalement des incidents** | Les entités doivent signaler les incidents ayant un impact significatif. | A.16.1 (Gestion des incidents liés à la sécurité de l'information et améliorations) |
| **Sécurité de la chaîne logistique** | Les entités doivent assurer la sécurité au sein de leur chaîne logistique. | A.15 (Relations avec les fournisseurs) |

# Conclusion

La directive NIS2 est une réglementation de cybersécurité complète conçue pour améliorer la sécurité des réseaux et des systèmes d'information au sein de l'UE pour les entreprises proposant des infrastructures importantes et critiques. Les entreprises concernées par la directive doivent prendre des mesures pour assurer leur conformité aux exigences, notamment l'identification et la gestion des risques, l'évaluation de leur niveau de sécurité, la protection des accès à privilèges, le renforcement de leurs défenses contre les ransomwares, l'adoption d'une stratégie Zero Trust, l'inspection de leur chaîne logistique logicielle, la formalisation de leur plan de résolution des incidents et la formation de leurs collaborateurs.

Plusieurs frameworks de cybersécurité et de sécurité de l'information assurent un certain alignement sur ces exigences. C'est le cas de la norme ISO 27001. En mettant en correspondance la directive NIS2 avec la norme ISO 27001, les entreprises peuvent utiliser leur certification ISO 27001 existante pour satisfaire aux exigences de la directive NIS2, ce qui leur permet de gagner du temps et d'économiser des ressources. En fin de compte, la conformité à la directive NIS2 et à la norme ISO 27001 peut aider les entreprises à réduire les risques de cybersécurité, à protéger leurs actifs informationnels et à conserver la confiance de leurs clients et parties prenantes.

Pour découvrir comment Okta Workforce Identity Cloud, Okta Customer Identity Cloud et d'autres solutions peuvent aider votre entreprise à se mettre en conformité à la directive NIS2, **contactez notre équipe**.

**À propos d'Okta**

Pour en savoir plus, consultez notre site www.okta.com/fr. Okta est le leader indépendant des solutions de gestion des identités pour les développeurs et les entreprises. Okta Identity Cloud connecte les entreprises à leurs clients, partenaires et collaborateurs en toute sécurité. Avec des intégrations avancées à plus de 7 000 applications, Okta Identity Cloud permet une connexion simple et sécurisée pour tous à partir de n'importe quel terminal.

Des milliers de clients, dont 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn et News Corp, font confiance à Okta pour travailler plus rapidement, augmenter les revenus et préserver la sécurité. Okta aide les clients à remplir leurs missions plus rapidement en favorisant une utilisation simple et sûre des technologies dont ils ont besoin pour réaliser des tâches critiques.

okta

Okta France
Tour Europlaza
20 avenue André Prothin
92400 Courbevoie
France

+33 (0)1 85 64 08 80