2024

NIS 2 : êtes-vous prêt ?

Un livre blanc SOFTEAM

UNE MARQUE DE DOCAPOSTE

Avant propos

La directive européenne NIS 2 est une réglementation dont les attendus, ambitieux, nécessitent une approche « projet » pour assurer une mise en conformité utile, allant au-delà de l'empilement de mesures pour « cocher des cases » ;
Cette réglementation a été pensée pour apporter une réelle plus-value en termes de sécurité des systèmes d'information si elle est mise en œuvre en prenant en compte la réalité des besoins métier et l'environnement cyber déjà existant ;
Ce livre blanc présente simplement NIS 2, son périmètre et ses objectifs ainsi qu'une approche méthodologique de mise en œuvre qui fera de son implémentation un facteur de renforcement significatif de votre cybersécurité, quel que soit votre secteur d'activité, dans le public comme dans le privé.

Guillaume Poupard,
Directeur Général Adjoint Docaposte

Sommaire

Introduction

Les interrogations autour de NIS 2 sont nombreuses.
NIS 2, une directive de trop ? Est-ce vraiment nécessaire ? Vous redoutez l'arrivée de NIS 2 ? Vous imaginez déjà un chantier interminable, des audits à répétition et une course contre-la-montre pour éviter des sanctions ?

La directive NIS 2 (Network and Information Security) est une initiative de l'Union Européenne visant à améliorer la sécurité des réseaux et des systèmes d'information des États membres. Le monde numérique est en constante évolution, les menaces se multiplient et les cyberattaques sont de plus en plus sophistiquées. La sécurité et la résilience des réseaux et des systèmes d'information sont donc plus que jamais une priorité pour les organisations. La directive NIS 2 est la réponse de l'Union Européenne à ce défi majeur.
NIS 2 est loin d'être une directive de trop dans l'univers réglementaire européen, elle s'inscrit en complémentarité avec d'autres réglementations et normes existantes. Cette directive couvre plusieurs secteurs, notamment l'énergie, les transports, la santé, les services financiers, la défense, le numérique, l'industrie, l'alimentation...

La directive NIS 2 étant une réponse proactive aux défis croissants de la cybersécurité, l'ignorer serait sans doute une erreur.

Alors, que faire ? Comment s'y prendre ? Tout d'abord, il est important de ne pas céder à la panique. Être en non-conformité n'est pas un drame en soi. Ce qui serait un problème, c'est d'accepter la situation sans prendre de mesures correctives. Ce livre blanc est ainsi conçu pour vous aider à comprendre pourquoi la directive NIS 2 est essentielle, vous donner des lignes directrices qui vous permettront d'évaluer où vous en êtes en termes de conformité et vous fournir les éléments à prendre en compte pour votre préparation à la conformité NIS 2.

Ce livre blanc s'adresse à un large éventail de lecteurs, notamment les responsables de la sécurité de l'information, les dirigeants, décideurs et les professionnels de la cybersécurité. Vous pouvez transformer cette obligation réglementaire en une opportunité pour renforcer votre résilience et votre posture de sécurité. Ne laissez pas votre organisation dans l'incertitude, lisez, agissez et assurez-vous de prendre la trajectoire de la conformité dès maintenant !

Pourquoi la directive NIS 2 ?

Historique et contexte

Publiée en juillet 2016 et transposée en droit français en 2018, la directive NIS originale visait à renforcer la sécurité des réseaux et des systèmes d'information dans l'Union Européenne. Cette première directive a marqué un tournant dans la sécurité des réseaux et des systèmes d'information en introduisant des exigences pour les États membres et en promouvant la coopération entre eux.

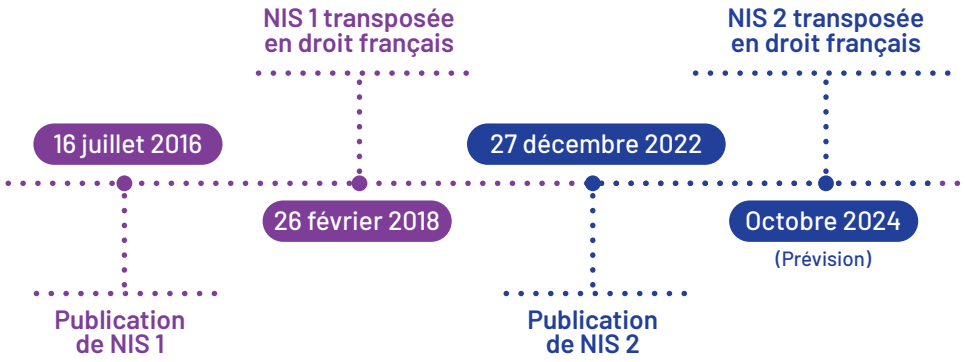
Malgré ses avancées, la directive NIS de 2016 présentait plusieurs limites :

- **Portée limitée**
  La directive NIS initiale ne couvrait pas tous les secteurs critiques et certains services essentiels n'étaient pas inclus.

- **Variabilité dans la mise en œuvre**
  Les États membres avaient une marge de manœuvre considérable dans la transposition de la directive, ce qui a conduit à une hétérogénéité considérable dans la mise en œuvre.

- **Évolution des menaces**
  Le paysage des menaces évolue rapidement, avec des attaques de plus en plus complexes et destructrices, de nouvelles cibles pour les cybercriminels, notamment les PME, les ETI et les collectivités territoriales.

Compte tenu de ces manquements, le besoin de mettre à jour la directive s'est fait ressentir, ceci afin de répondre aux nouveaux défis.



Publiée le 27 décembre 2022 au Journal Officiel de l'Union Européenne, avec une transposition en droit national prévue sous un délai de 21 mois pour chaque État membre, la directive NIS 2 s'appuie sur la précédente directive NIS pour en combler les lacunes.

> **Compte tenu de ces manquements, le besoin de mettre à jour la directive s'est fait ressentir, ceci afin de répondre aux nouveaux défis.**

Principaux points d'amélioration de NIS 2

En s'appuyant sur NIS 1, la directive NIS 2 vient renforcer la sécurité à travers de nouvelles exigences :

1. Inclusion de nouveaux secteurs

NIS 2 couvre 18 secteurs d'activité. En plus des secteurs déjà couverts par NIS 1, tels que l'énergie, les transports et la santé, NIS 2 inclut désormais des secteurs comme les services numériques, les fournisseurs de cloud computing, les services de l'administration publique, et même les petites entreprises technologiques considérées comme ayant un impact significatif sur la sécurité.

2. Exigences de sécurité renforcées

NIS 2 impose des mesures de sécurité plus strictes et robustes :

- Mesures techniques et organisationnelles : les entités doivent mettre en œuvre des contrôles de sécurité plus avancés et sophistiqués, incluant des systèmes de détection des intrusions et des protocoles de sécurité renforcés.
- Gestion des risques : adoption obligatoire d'une approche basée sur les risques pour identifier, évaluer et atténuer les risques de sécurité des systèmes d'information.

3. Meilleur processus de gestion des incidents

Les exigences de notification et de gestion des incidents ont été clarifiées et renforcées :

- Notification rapide et détaillée : obligation de signaler les incidents significatifs dans un délai strictement défini, avec des informations détaillées sur la nature, l'impact et les mesures prises pour remédier à l'incident.
- Coordination accrue : amélioration de la coopération et de la communication entre les États membres et les autorités nationales pour une réponse plus coordonnée aux incidents cyber.

4. Harmonisation et coopération européenne

NIS 2 vise à harmoniser davantage les pratiques de cybersécurité et à renforcer la coopération transfrontalière :

- Cadre harmonisé : établissement de normes de sécurité plus uniformes à travers les États membres, réduisant ainsi les disparités et les vulnérabilités au sein de l'UE.
- Partage d'informations : promotion du partage d'informations sur les menaces et les incidents de sécurité entre les entités et les autorités compétentes.

5. Sanctions plus sévères

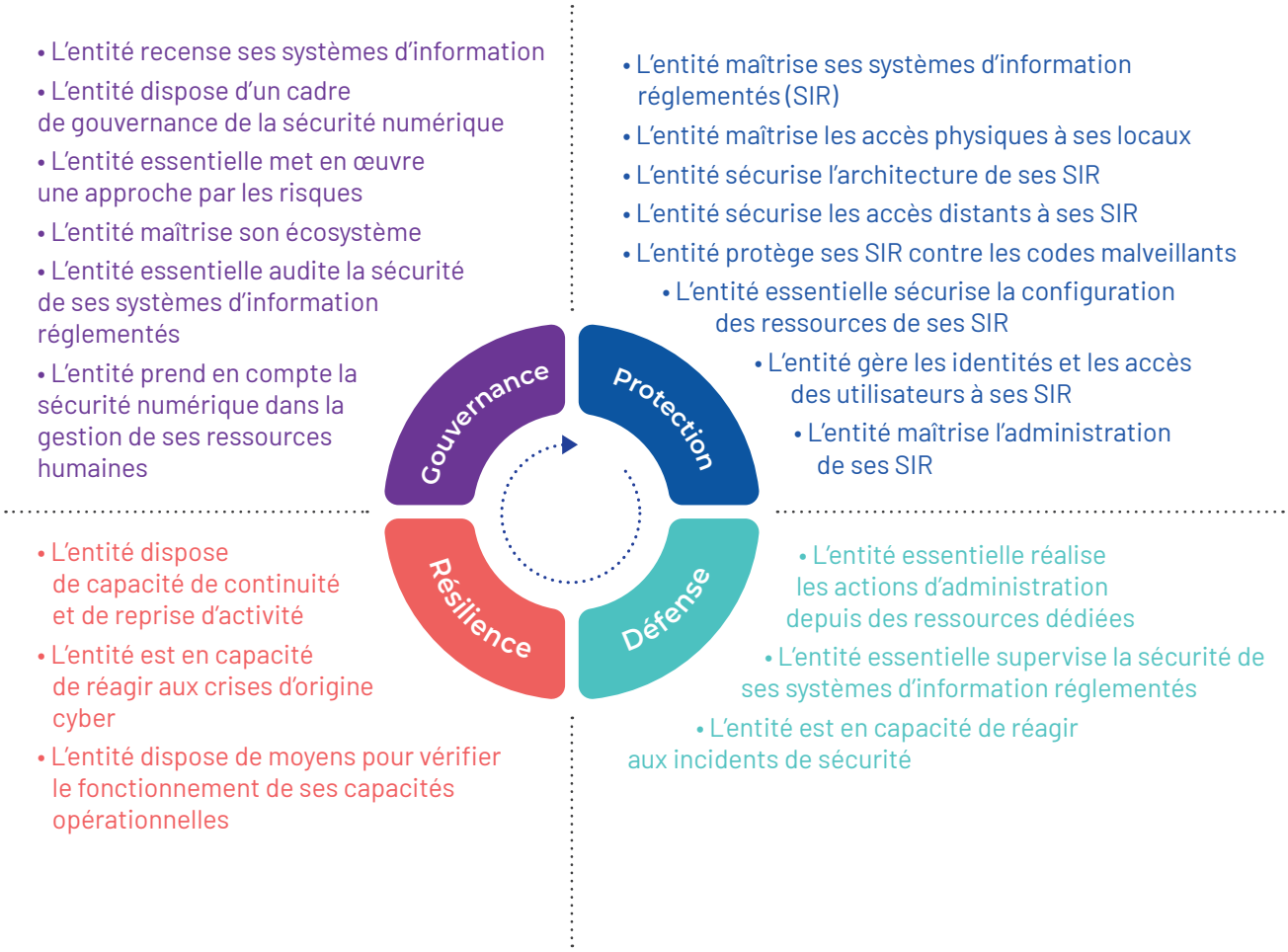
Pour garantir que les entités s'attèlent à la mise en conformité, NIS 2 introduit des sanctions :

- Augmentation du montant des amendes : les amendes pour non-conformité sont désormais plus élevées, rendant les sanctions suffisamment dissuasives pour inciter les organisations à respecter les exigences de sécurité. Ces amendes seront proportionnées aux manquements et pourront aller jusqu'au prélèvement d'un pourcentage du chiffre d'affaires de l'entité concernée (2% pour les entités essentielles et 1,4% pour les entités importantes).
- Responsabilité accrue : les dirigeants d'entreprise peuvent être tenus personnellement responsables du non-respect des obligations de sécurité.

NIS 2 vise à créer un environnement numérique plus sûr et plus résistant aux cyberattaques. Pour chaque organisation, il est impératif de comprendre ces améliorations et de se tenir prête à les mettre en œuvre. Ce livre blanc vous oriente pour anticiper votre préparation à la conformité NIS 2. **Alors, préparez-vous dès maintenant à la conformité NIS 2 !**

Les quatre piliers de la directive NIS 2

La directive NIS 2 repose sur une approche organisée autour de quatre piliers fondamentaux qui visent à renforcer la cybersécurité des entreprises et des infrastructures critiques à travers l'Europe. Ces piliers permettent de structurer les actions et obligations imposées par la directive, en mettant l'accent sur une gouvernance claire, une protection renforcée, une défense efficace et une résilience face aux cybermenaces.

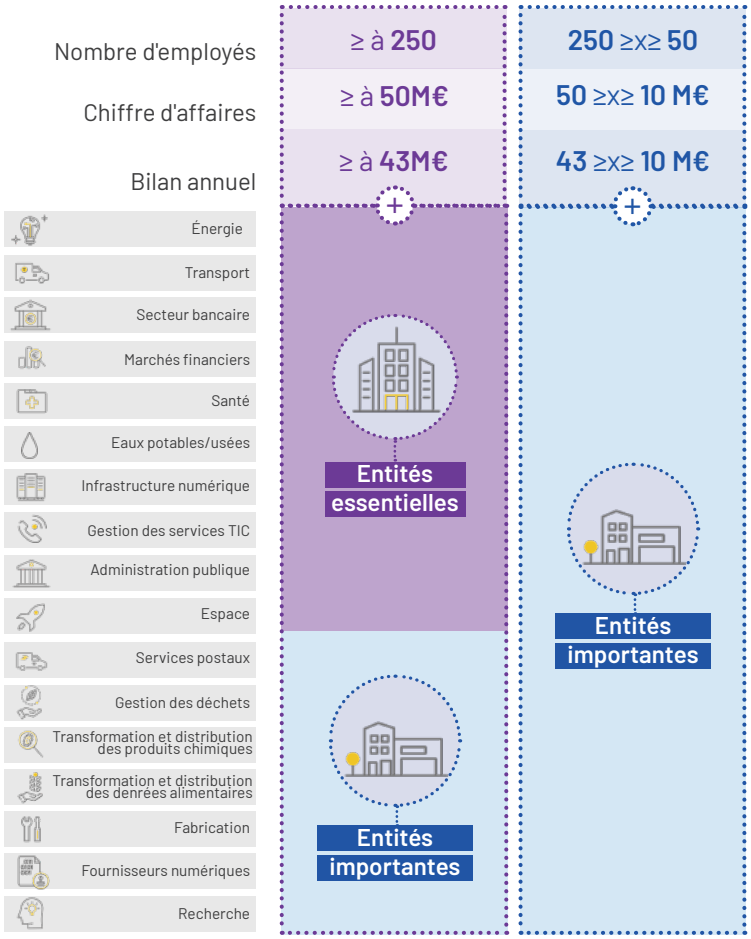


Ces piliers ne sont pas indépendants les uns des autres, mais complémentaires, formant un écosystème cohérent qui guide les organisations vers une sécurité robuste et durable. À noter que la notion de système d'information réglementé (SIR) au sens NIS 2 représente tout SI de l'entreprise recensé comme critique ou porteur d'activités critiques et/ou sensibles.

Qui est concerné par la directive NIS 2 ?

La directive NIS 2 élargit de manière significative le périmètre d'application de NIS 1. Un changement de sémantique accompagne cette évolution : le terme « opérateurs » est désormais remplacé par « entités », reflétant la portée plus large et la diversité accrue des acteurs concernés. On passe de NIS 1 qui couvrait 300 opérateurs de services essentiels à NIS 2 qui couvre 18 secteurs d'activités, au sein desquels on distingue Entités Essentielles (EE) Entités Importantes (EI), réparties dans les annexes 1 et 2 de la directive. NIS 2 inclut également les acteurs de la chaine d'approvisionnement et les services de l'administration publique.

Déterminez si votre entité est essentielle ou importante en fonction des critères ci-contre



Dans l'attente de sa transposition en droit national, qui apportera des précisions sur la classification des différentes typologies d'entités, soulignons que NIS 2 introduit une approche proportionnelle entre les EE et les EI, en particulier dans les exigences de sécurité applicables. En fonction du type d'entité (EE ou EI), l'applicabilité des exigences sera adaptée proportionnellement afin de tenir compte des ressources et des enjeux spécifiques d'une grande entreprise par rapport à ceux d'une PME.
Les sanctions, elles, pourront aller jusqu'à 2% du chiffre d'affaires mondial pour les EE et 1,4% pour les EI.

Les différentes étapes de préparation à la conformité NIS 2

La préparation à la conformité NIS 2 de son entité nécessite une approche méthodique et structurée. Surtout, restez calme ! Il n'est pas question de tout recommencer à zéro ou de tout faire en une seule fois. D'où l'intérêt de commencer au plus tôt avec ce que l'on a déjà. Quant aux actions qui ne sont pas encore très claires, planifiez-les pour les prochaines itérations. Afin d'aider votre organisation à se préparer efficacement, nous vous proposons quelques étapes-clés dans la suite de ce document.

Quel est l'état actuel de votre organisation ?

Observations

Effectuez une observation des opérations de l'entité, des différents collaborateurs impliqués, afin de comprendre le fonctionnement.

Évaluation de maturité

Envoyez des questionnaires aux représentants des différentes parties prenantes en vue d'évaluer le niveau de maturité des différents SI de votre écosystème.

Entretiens

Menez des entretiens avec des personnes à différents niveaux de l'entité.

Revue de la documentation

Recensez les documents existants (politique, procédures précédant rapport d'audit si existant,...)

Avant de vous lancer dans un quelque projet de conformité, il est crucial de savoir votre écart à l'attendu : cela vous permettra de vous projeter plus facilement.

Analyse de l'existant

Dans un premier temps, il est utile de comprendre le contexte de votre entité par des observations, des entretiens, des évaluations de maturité et une revue documentaire. Cette étape doit vous permettre de vous positionner par rapport aux questions suivantes :

- **Comment est structurée l'entité, quelles sont les activités clés et les systèmes d'information qui les supportent ?**

  Il est important de recenser vos différentes filiales le cas échéant, vos systèmes d'informations (SI) ainsi que vos activités et services pour réaliser une cartographie de l'entité. À ce stade, pensez à identifier vos SI sensibles sur la base de deux critères. D'une part par l'activité qu'ils appuient ; d'autre part, par l'impact de leur éventuelle indisponibilité sur la fourniture de services au sein de votre entité.

- **Votre entité dispose-t-elle de politiques/procédures de sécurité clairement documentées ?**
  - Politique de sécurité des systèmes d'information (PSSI),
  - Politique générale de sécurité (PGS),
  - Des plans de continuité et de reprise d'activités (PCA/PRA),
  - Plan de gestion d'incident et bien d'autres.

- **Existe-t-il une procédure de révision de ces politiques ?**

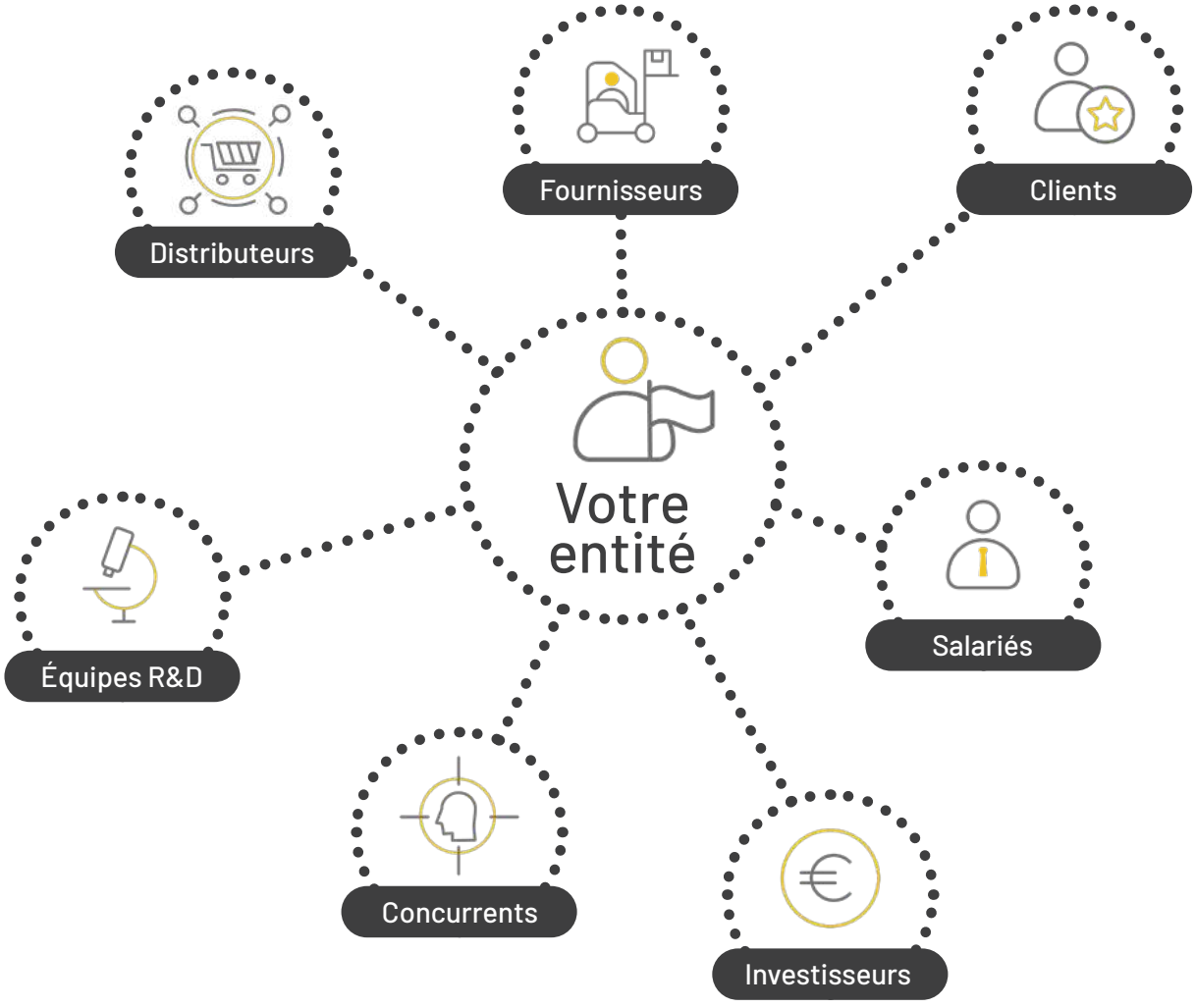
  La fréquence de revue des politiques de sécurité doit être définie. Des mises à jour peuvent être effectuées dès que le besoin se présente.

- **Quel est le niveau d'applicabilité de vos politiques ?**

  Grâce aux retours des équipes obtenus via les questionnaires préalablement transmis, vous aurez une idée de la maturité cyber de votre entité et du niveau de mise en œuvre réel de vos politiques.

Compréhension de votre écosystème

Chaque entité, dans le cadre de son activité, interagit au quotidien avec plusieurs parties prenantes, ayant des rôles à différents niveaux de la chaine d'approvisionnement.



Il est essentiel de bien comprendre l'environnement dans lequel évolue votre entité et pour y parvenir, vous pouvez :

- **Répertorier qui sont vos différentes parties prenantes :**
  il est important d'identifier avec qui votre entité interagit et d'établir une cartographie intégrant les fournisseurs et/ou sous-traitants qui contribuent à vos activités. Vous devez également vous assurer d'avoir au moins un point de contact pour chacun des acteurs avec lesquels votre entité interagit.

- **Revoir les clauses contractuelles :**
  prenez le temps d'examiner et, si besoin, de mettre à jour les clauses contractuelles qui vous lient à vos parties prenantes, et ce afin d'intégrer la sécurité numérique dans ces clauses, par exemple le plan d'assurance sécurité (PAS) et les clauses d'audit. Vous devez vous assurer que vos clauses contractuelles engagent vos fournisseurs sous-traitants à transmettre vos exigences de sécurité à leurs prestataires de façon à les intégrer jusqu'au dernier maillon de la chaîne.

- **Analyse de risque :**
  effectuez une analyse de risque qui vous permettra d'évaluer les potentielles vulnérabilités au sein de votre système ainsi que les impacts en cas d'incident. D'autre part, l'analyse de risque vous permettra d'identifier les parties prenantes susceptibles d'augmenter le niveau de menaces et de mettre en péril le bon déroulement de vos activités.

Les cyberattaques se propagent de plus en plus, avec comme point d'entrée des parties prenantes plus vulnérables qui offrent la possibilité de cibler les entités essentielles ou importantes. C'est pourquoi le périmètre d'application de NIS 2 recouvre également les fournisseurs de services numériques, les administrations publiques, les PME et bien d'autres acteurs.

Gouvernance cyber

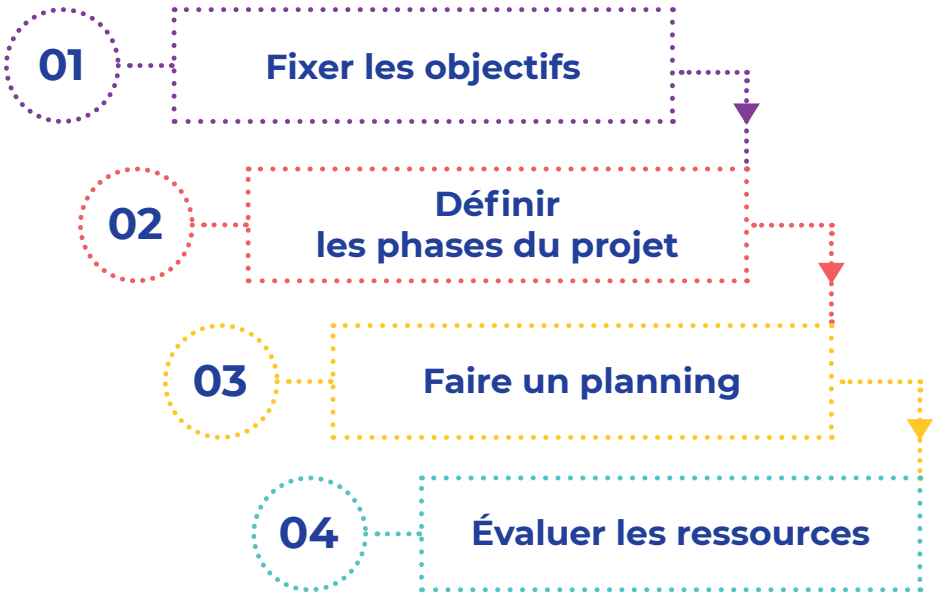
À ce niveau, il sera question de définir et de communiquer clairement qui fait quoi. Il s'agit d'une étape cruciale pour assurer la réussite de son projet de mise en conformité.

- **Attribution des responsabilités :** assurez-vous que chaque personne ou chaque équipe comprenne ses responsabilités.
- **Implication de la direction :** la gouvernance doit être claire et stratégique car si la direction n'est pas impliquée, le risque d'échec est important.
- **Coordination et communication :** la communication entre les différentes équipes d'une part et entre la direction et les équipes d'autre part doit être fluide. Sans coordination solide, vos actions pourraient s'avérer inutiles. Il est également important de prévoir dans son plan de communication, comment s'organisera la collaboration avec les autorités nationales et européennes.
- **Formation et sensibilisation :** la sensibilisation et la formation sont des missions de longue haleine. Il est essentiel de mettre en place des programmes à des fréquences bien définies, ou selon des besoins ponctuels, pour conserver un certain niveau de compétences des collaborateurs.

Mise en conformité

Plan d'action

Élaborer un plan d'action clair et structuré est la première marche à franchir pour réussir votre projet de préparation à la conformité NIS 2. Ce plan d'action doit fixer des objectifs mesurables et atteignables et détailler les différentes étapes de votre projet.



Concrètement, il faut découper votre projet en plusieurs phases, identifier et prioriser les chantiers de remédiation, définir vos axes budgétaires de dépense, faire des prévisions sur deux à trois ans et surtout garder à l'esprit que vous ne pourrez pas tout faire en une seule fois. Vous aurez besoin de faire plusieurs itérations avant d'atteindre le niveau de conformité visé.

Prévision de charges

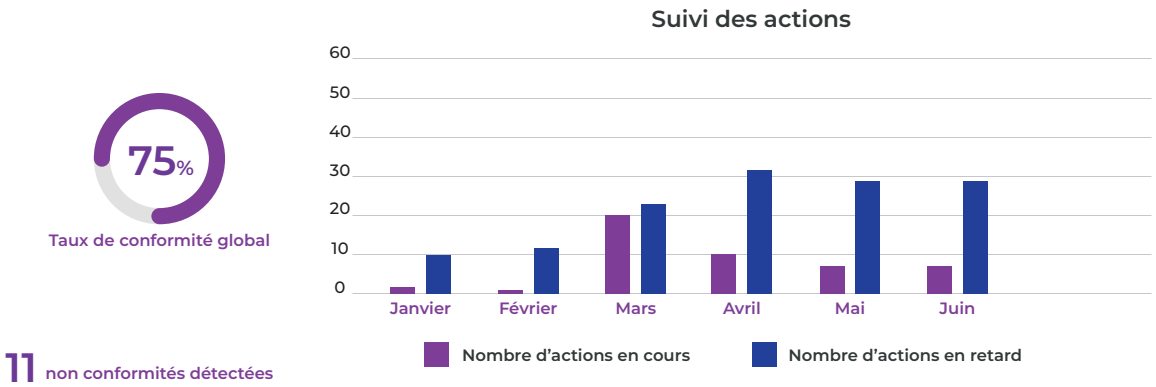
Les charges seront proportionnelles à la taille de votre entité et plus spécifiquement au périmètre choisi pour la mise en conformité.

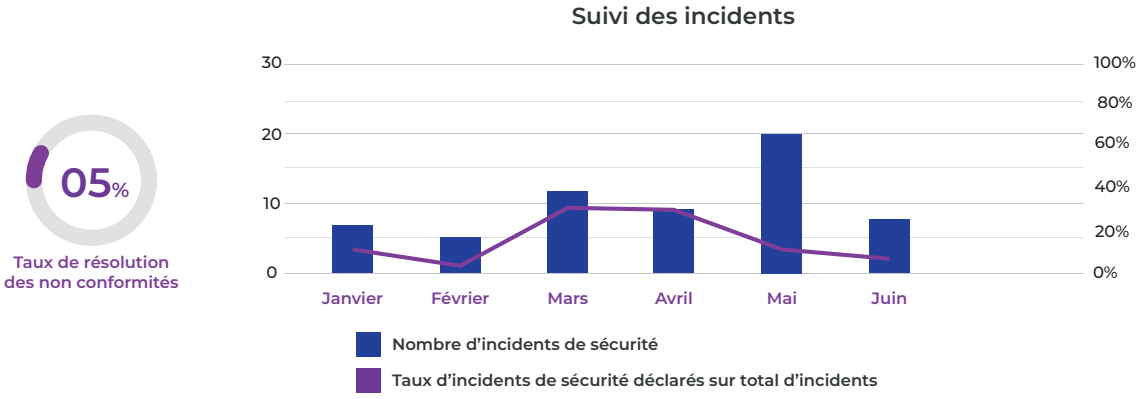
- **Outils et technologies :** choisissez les outils et/ou solutions technologiques adéquats pour faciliter au maximum votre processus de mise en conformité.
- **Formation des ressources :** prévoyez du budget pour la formation des ressources, par exemple des certifications.
- **Allocations des ressources :** pensez à la réallocation de vos équipes, évaluez le coût des ressources dédiées à la gestion du projet de mise en conformité, le coût du recrutement de nouvelles ressources si nécessaire et le coût des honoraires d'éventuels consultants.
- **Phase de préparation :** estimez la durée requise pour l'évaluation des systèmes, l'identi- - fication des écarts, et la planification des mesures de conformité.
- **Politiques et procédures :** le temps nécessaire pour élaborer/mettre à jour et formaliser les politiques de sécurité devra être pris en compte dans la planification de votre projet de mise en conformité.

Surveillance et amélioration continue

Comme mentionné précédemment, vous aurez besoin de plusieurs itérations pour atteindre le niveau de conformité requis. Il sera important de maintenir une vigilance constante afin de mettre en place un processus d'amélioration continue qui vous permettra d'atteindre le niveau de conformité visé. Vous pourrez éventuellement faire appel à un outil de gouvernance qui intègre nativement des modules de surveillance. Il s'agira par exemple de tableaux de bord, d'indicateurs de performance SSI, autant d'outils utiles pour réaliser le suivi des plans d'actions par entité en fonction de la gouvernance définie.

État d'avancement sur le semestre 1





Des indicateurs pertinents à suivre seraient le taux de conformité aux politiques de sécurité, le nombre de non-conformités, le taux de correction des non-conformités, l'avancement des plans d'action, les taux de participation aux sensibilisation et formation en cybersécurité.
De façon générale, ces indicateurs vous permettront de mesurer la performance de votre processus de mise en conformité, de vérifier que vos stratégies et votre plan d'action sont alignés, de faciliter la prise de décision et de déceler de potentielles opportunités.

Alors,
que retient-on ?

La directive NIS 2 n'est pas juste un règlement de plus ou un de trop.

La conformité à NIS 2 peut sembler être un chantier colossal, cependant il ne sera pas question de tout recommencer à zéro mais plutôt d'intégrer les éléments manquants à votre existant.
Vous n'avez pas besoin d'être parfait dès le premier jour. Ce qui compte, c'est de commencer le processus, identifier la trajectoire, les objectifs à atteindre et respecter le planning en transformant chaque défi en opportunité.
L'enjeu ici n'est pas juste d'éviter des sanctions mais de faire de cette directive un atout pour renforcer non seulement la sécurité de votre entité, celle de l'écosystème dans laquelle elle évolue et notamment la chaine d'approvisionnement.
À terme, cela renforcera sans doute la confiance de vos partenaires, parties prenantes et clients. C'est cette démarche proactive et structurée qui fera la différence et vous placera en pole position pour affronter les cybermenaces de demain.

Vous avez tout à gagner à engager au plus tôt les démarches de mise en conformité NIS 2.

L'Expertise Cybersécurité SOFTEAM

L'expertise Cyber chez SOFTEAM

Filiale de Docaposte, SOFTEAM et ses équipes Consulting ont développé une forte expertise Cybersécurité au fil des années.

Nous proposons une offre modulaire au service de la maitrise des risques, en adéquation avec les normes actuelles et réglementations applicables (RGS/NIS/LPM…).

Nous vous accompagnons avec une approche pragmatique – adaptée à votre niveau de maturité en cybersécurité afin d'identifier et de **mettre sous contrôle vos risques cyber**.

Nous intervenons lors des différentes phases de gouvernance de vos projets cybersécurité afin d'avoir une cohérence et une vision commune : **diagnostic – conseil – plan d'action**.

Notre vision NIS 2

Nos experts sont les facilitateurs de l'appropriation et l'intégration de NIS 2.

Comme toute mise en conformité, NIS 2 nécessite une phase d'appropriation contextuelle (contexte métier, proportionnalité…) afin de l'adopter et l'adapter à votre contexte, vos enjeux.

Nos experts, anciens RSSI, s'occupent de cette phase d'accompagnement et de pédagogie pour que l'intégration de la directive NIS 2 soit simple et fluide pour vous.

NIS 2 doit s'intégrer à votre gouvernance Cybersécurité (et non venir multiplier les politiques de votre entreprise). Nous vous écoutons avant de vous conseiller.

Notre équipe

Nos experts RSSI sont formés par notre directeur de l'expertise Cybersécurité, Stéphane Dubreuil, un ancien de l'ANSSI.

Des cadres expérimentés :

- Ayant déjà travaillé en environnement complexe et fortement réglementé engageant leur responsabilité
- Ayant déjà travaillé en environnement en tension (projet à plusieurs M€)

Des jeunes possédant majoritairement des doubles compétences :

- Plus de la moitié des juniors ont 2 bac+5

Une politique de certification systématique :

- Tous nos consultants passent leur certification ISO 27001 et une formation à EBIOS RM.

Annelise RIQUIER

Senior Manager du Conseil Cyber

Stéphane DUBREUIL

Directeur de l'expertise Cybersécurité

Jean-Christophe ZAPALOWICZ

Senior Manager du Conseil Cyber

SOFTEAM

SOFTEAM est le cabinet de conseils et de services de Docaposte (Groupe La Poste).

Notre mission ? Mettre le numérique au service des transitions auxquelles nos sociétés font face. Concrètement, cela se traduit dans notre attitude et dans nos engagements.
Nous sommes des partenaires de confiance pour nos clients, en adoptant une posture d'écoute active et en co-construisant des solutions qui répondent à leurs besoins spécifiques.
Nous sommes conscients que les défis auxquels nous faisons face sont complexes et évolutif : la force de notre collectif de consultants experts et engagés pour le bien commun est le socle de notre mission.

Ensemble, nous voulons faire du numérique un levier pour demain. Et cela commence justement par un bon accompagnement Cyber.

NIS 2 : bien accompagné, tout devient plus simple

Vous souhaitez échanger avec nos experts sur vos besoins d'accompagnement Cyber ?
Ils prennent vraiment le temps de vous écouter et comprendre vos enjeux,
votre environnement et vos objectifs.

Contactez directement notre équipe à practice.cyber@softeam.fr

SOFTEAM
UNE MARQUE DE DOCAPOSTE

www.softeam.com