WISER

Wide-Impact cyber SEcurity Risk framework

# Guide pour la directive sur la securite des reseaux et des systemes d'information

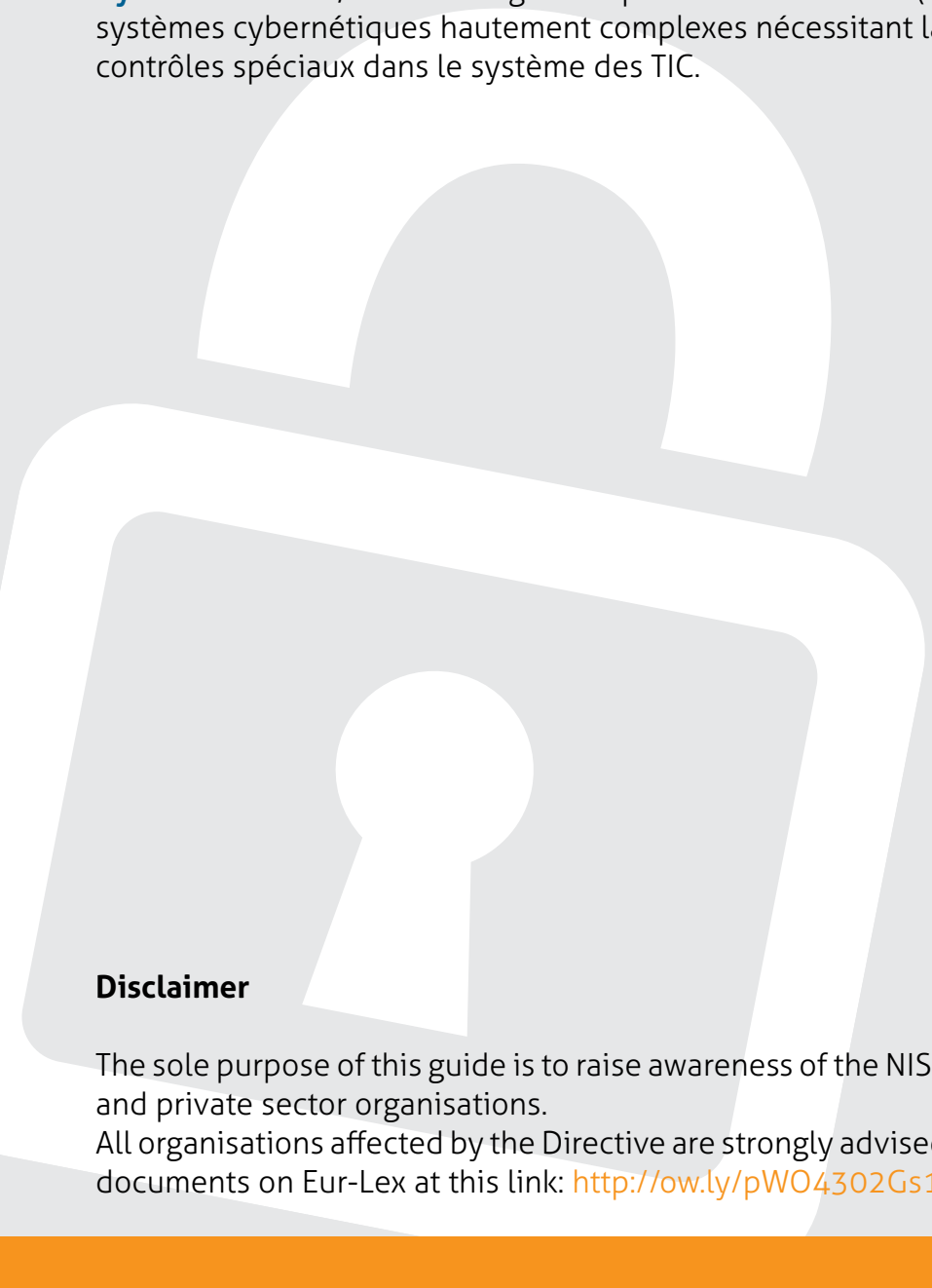
www.cyberwiser.eu | info@cyberwiser.eu | @cyberwiser

**WISER** est une initiative européenne en faveur de l'innovation menée dans le cadre d'Horizon 2020 qui place la gestion des risques informatiques au cœur même des bonnes pratiques commerciales, en profitant à de nombreux types d'entreprises, des PME aux opérateurs d'infrastructures critiques.

**CyberWISER Light**, un nouvel outil gratuit disponible en ligne pour les petites ou grandes entreprises de e-commerce. Cyber WISER Light Service les aide à avoir une approche de gestion du cyber risque et à mieux évaluer et traiter les risques pour protéger leurs actifs numériques.

**CyberWISER Essential**, une solution de gestion des risques préemballée pour les PME

**CyberWISER Plus**, a risk management platform as a service (RMaaS) pour les systèmes cybernétiques hautement complexes nécessitant la surveillance des contrôles spéciaux dans le système des TIC.



**Disclaimer**

The sole purpose of this guide is to raise awareness of the NIS Directive for public and private sector organisations.
All organisations affected by the Directive are strongly advised to read the official documents on Eur-Lex at this link: http://ow.ly/pWO4302Gs10

# Guide pour la directive sur la securite des reseaux et des systemes d'information

La directive sur la sécurité des réseaux et des systèmes d'information (NIS Directive) établit les premières règles de l'Union Européenne en matière de cyber sécurité.

L'applicabilité de la directive NIS est prévue pour août 2016. Les États membres disposeront de 21 mois pour implémenter cette directive dans leurs lois nationales et six mois pour identifier les opérateurs de services essentiels.

L'objectif de la directive est d'atteindre un niveau de sécurité élevé commun sur les réseaux et les systèmes d'information au sein de l'Union, en:

» améliorant leurs capacités en matière de sécurité au niveau national;
» augmentant la coopération au niveau de l'Union;
» rendant obligatoire la gestion des risques et la notification des incidents pour les opérateurs de services essentiels et les fournisseurs de services numériques.

## 1. Les actions des États membres pour augmenter et améliorer les capacités en matière de sécurité au niveau national

Chaque État membre adoptera une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information qui définit les objectifs stratégiques et les mesures politiques et réglementaires. La stratégie devra inclure les points suivants:

» objectifs, priorités et gouvernance de la stratégie nationale et une gouvernance permettant d'atteindre les objectifs;
» inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris;
» méthodes de coopération entre les secteurs public et privé;
» programmes de sensibilisation, d'éducation et de formation;
» projets de recherche et de développement en rapport avec la stratégie NIS;

» plan d'évaluation des risques;

» liste d'acteurs concernés par la mise en œuvre de la stratégie.

Les États membres désigneront une ou plusieurs autorités nationales compétentes chargées d'accomplir les tâches liées à la directive et surveiller son application au niveau national.

Les États membres désigneront également un référent unique qui exercera une fonction de mise en relation afin d'assurerla coopération transfrontalière avec les autorités compétentes des autres États membres et avec les mécanismes de coopération créés par la directive elle-même.

Les États membres désigneront un ou plusieurs centres de réponse aux incidents de sécurité informatique (CSIRT – Computer Security Incident Response Team).

Les CSIRT seront en charge  au moins des éléments suivants:

» suivi des incidents au niveau national;

» activation du mécanisme d'alerte précoce, diffusion de messages d'alerte, annonces et diffusion d'informations sur les risques et incidents auprès des parties intéressées;

» intervention en cas d'incident;

» analyse dynamique des risques et incidents et conscience situationnelle;

» participation au réseau des CSIRT.

## 2. Actions des États membres pour renforcer la coopération au sein de  l'Union européenne

La directive NIS établit un groupe de coopération pour soutenir et faciliter la coopération stratégique, l'échange d'informations et le développement de la confiance entre les États membres.

Elle établit également un réseau des CSIRT afin de contribuer au renforcement de la confiance entre États membres et de promouvoir une coopération opérationnelle rapide et efficace.

### *Quelles missions pour le groupe de coopération?*

Le groupe de coopération sera constitué des représentants des États membres, de la Commission ainsi que l'ENISA (Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information),  la Commission européenne agira en tant que secrétariat.

Le groupe de coopération travaillera sur la base de programmes de travail bisannuels, dans quatre différents domaines:

**Planification:**

» établir un programme de travail 18 mois après l'entrée en vigueur (Février 2018);

» préparer ensuite un programme de travail tous les deux ans.

**Pilotage:**

» fournir des orientations stratégiques pour les activités du réseau des CSIRT;

» aider les États membres à renforcer leurs capacités en matière de sécurité des réseaux et des systèmes d'information;

» aider les États membres à identifier les opérateurs essentiels de services;

» échanger sur les méthodes de notifications d'incidents;

» échanger sur les standards;

» s'engager avec les institutions, organes ou organismes de l'Union concernés;

» évaluer les stratégies nationales en matière de sécurité des réseaux et des systèmes d'information (sur la base du volontariat);

» échanger des informations et les bonnes pratiques;

» risques;

» incidents;

» sensibilisation;

» formation;

» échanger des informations et les bonnes pratiques en matière de recherche et de développement.

**Rapport d'activité:**

Tous les 1 an et demi, le groupe fournira un rapport d'évaluation de l'expérience acquise avec la coopération. Le rapport sera envoyé à la Commission en tant que contribution à la revue du fonctionnement de la directive.

### *Quel rôle aura le réseau des CSIRT?*

Le réseau des CSIRT est composé de représentants des CSIRT des États membres et du CERT-UE (L'équipe du centre de réponse aux urgences informatiques pour les institutions, organes et organismes compétents de l'Union). La Commission participera au réseau des CSIRT en qualité d'observateur. L'ENISA assurera le secrétariat et soutiendra activement la coopération entre les CSIRT.

Le réseau des CSIRT est chargé des missions suivantes:

» échanger des informations sur les services, les opérations et les capacités de coopération des CSIRT;

» échanger et traiter les informations en rapport avec des incidents (sur demande et sur la base du volontariat);
» identifier une réponse coordonnée à un incident (sur demande et sur la base du volontariat);
» aider les États membres à faire face à des incidents transfrontaliers (sur la base du volontariat);
» explorer d'autres formes de coopération opérationnelle;
» informer le groupe de coopération de ses activités et demander des orientations;
» étudier les enseignements tirés des exercices relatifs à la sécurité des réseaux et des systèmes d'information;
» à la demande d'un CSIRT donné, étudier les capacités et l'état de préparation dudit CSIRT;
» publier des lignes directrices relatives à la coopération opérationnelle.

Deux ans après l'entrée en vigueur de la directive NIS, puis ensuite tous les 18 mois, le réseau des CSIRT rédigera un rapport d'évaluation de l'expérience acquise dans le cadre de la coopération opérationnelle, y compris les conclusions et recommandations. Le rapport sera envoyé à la Commission en tant que contribution à la revue du fonctionnement de la directive.

**Obligations de gestion des risques et de notification des incidents pour les opérateurs de services essentiels et les fournisseurs de services numériques.**

*Quels sont les opérateurs de services essentiels, et quelles sont leurs obligations?*

Les opérateurs de services essentiels sont des entreprises privées ou des entités publiques ayant un rôle important dans la société et l'économie. En vertu de la directive NIS, les opérateurs de services essentiels identifiés devront prendre les mesures de sécurité appropriées et notifier les incidents graves à l'autorité nationale compétente.

Les mesures de sécurité couvrent les éléments suivants:

» prévenir les risques: mesures techniques et organisationnelles appropriées et proportionnées au risque;
» assurer la sécurité des réseaux et des systèmes d'information: les mesures doivent assurer un niveau de sécurité proportionnel aux risques que présentent le réseau et les système d'information concernés;
» gestion des incidents: Les mesures doivent prévenir et minimiser l'impact des incidents sur les systèmes d'information utilisés pour fournir les services.

*Comment les États membres identifieront les opérateurs de services essentiels?*

» Chaque État membre doit identifier les entités qui devront prendre des

mesures de sécurité appropriées et notifier les incidents de sécurité les plus graves en utilisant les critères suivants:

» l'entité doit fournir un service essentiel au maintien d'activités sociétales et/ou économiques critiques;
» la fourniture de ce service est tributaire des réseaux et des systèmes d'information;
» un incident aurait un effet disruptif important sur la fourniture dudit service.

### *Quels secteurs sont couverts par la directive?*

La directive couvrira les opérateurs dans les secteurs suivants:

» Énergie: électricité, pétrole, gaz;
» Transports: aérien, ferroviaire, routier et par voie navigable;
» Banques: établissement de crédit;
» Infrastructures de marchés financiers: exploitant de plate-forme de négociation, contreparties centrales;
» Santé: mise en place de soins de santé;
» Eau: Fourniture et distribution d'eau potable:
» Infrastructure numériques: IXP, fournisseurs de services DNS, registres de noms de domaines de haut niveau;

### *Quels types d'incidents les opérateurs de services essentiels devront-il notifier?*

La directive ne définit pas de limite à un incident important nécessitant une notification à l'autorité nationale compétente. Il définit trois paramètres qui doivent être pris en considération:

» le nombre d'utilisateurs touchés par la perturbation;
» la durée de l'incident;
» la portée géographique eu égard à la zone touchée par l'incident.

Ces paramètres peuvent être davantage clarifiés au moyen de lignes directrices adoptées par les autorités nationales compétentes agissant conjointement au sein du groupe de coopération.

### *Que sont les fournisseurs de services numériques, et quelles sont leurs obligations?*

Les entreprises numériques importantes, appelées dans la directive «fournisseurs de services numériques», devront également prendre les mesures de sécurité appropriées et notifier les incidents majeurs à l'autorité compétente.

Les mesures de sécurité couvrent les éléments suivants:

» prévenir les risques: mesures techniques et organisationnelles appropriées et proportionnelles au risque;

» assurer la sécurité des réseaux et des systèmes d'information: les mesures doivent assurer un niveau de sécurité adapté aux risques que présentent le réseau et les système d'information concernés;

» gestion des incidents: Les mesures doivent prévenir et minimiser l'impact des incidents sur les systèmes d'information utilisés pour fournir les services.

Les mesures de sécurité prises par les opérateurs de services essentiels doivent également prendre en considération certains facteurs spécifiques, à préciser ultérieurement dans un acte d'exécution de la Commission:

» la sécurité des systèmes et des installations;

» la gestion des incidents;

» la gestion de la continuité des activités;

» le suivi, l'audit et le contrôle;

» le respect des normes internationales.

### *Quels types d'incidents les fournisseurs de services numériques doivent-ils notifier?*

La directive ne définit pas les limites d'un incident important nécessitant une notification à l'autorité nationale compétente. Il définit cinq paramètres qui doivent être pris en considération:

» le nombre d'utilisateurs touchés par l'incident;

» la durée de l'incident;

» la portée géographique eu égard à la zone touchée par l'incident;

» la gravité de la perturbation du fonctionnement du service;

» l'ampleur de l'impact sur les fonctions économiques et sociétales.

Ces paramètres seront précisés par la Commission au moyen d'actes d'exécution.

### *Quels fournisseurs de services numériques la directive couvre-t-elle?*

» Les marchés en ligne – permettant la mise en place de plateformes de vente de produits ou de services en ligne;

» les services d'informatique en nuage;

» moteurs de recherche en ligne.

Toutes les entités répondant à ces définitions seront automatiquement soumises aux exigences en matière de sécurité et de notification en vertu de la directive NIS. La directive NIS ne s'applique pas aux microentreprises et petites entreprises telles qu'elles sont définies dans la recommandation

2003/361/CE de la Commission.

*Comment une approche allégée et harmonisée pour les fournisseurs de services numériques pourra-t-elle être atteinte?*

La Commission adoptera des actes d'exécution concernant les exigences de sécurité et les obligations de notifications des opérateurs de services essentiels, et ce dans l'année suivant l'adoption de la directive.

Les États membres ne seront pas en mesure d'imposer des exigences supplémentaires en matière de sécurité et de notification plus strictes sur les fournisseurs de services numériques. De plus, les autorités compétentes ne pourront exercer des activités de surveillance que lorsqu'elles disposeront de la preuve qu'un fournisseur de services numériques ne respecte pas les obligations qui lui incombent en vertu de la directive.

## Liens utiles

Directive sur la sécurité des réseaux et des systèmes d'information (NIS)

http://ow.ly/pWO4302Gs10

Marché unique numérique: cyber-sécurité

http://ow.ly/Pc9I302Gs5A

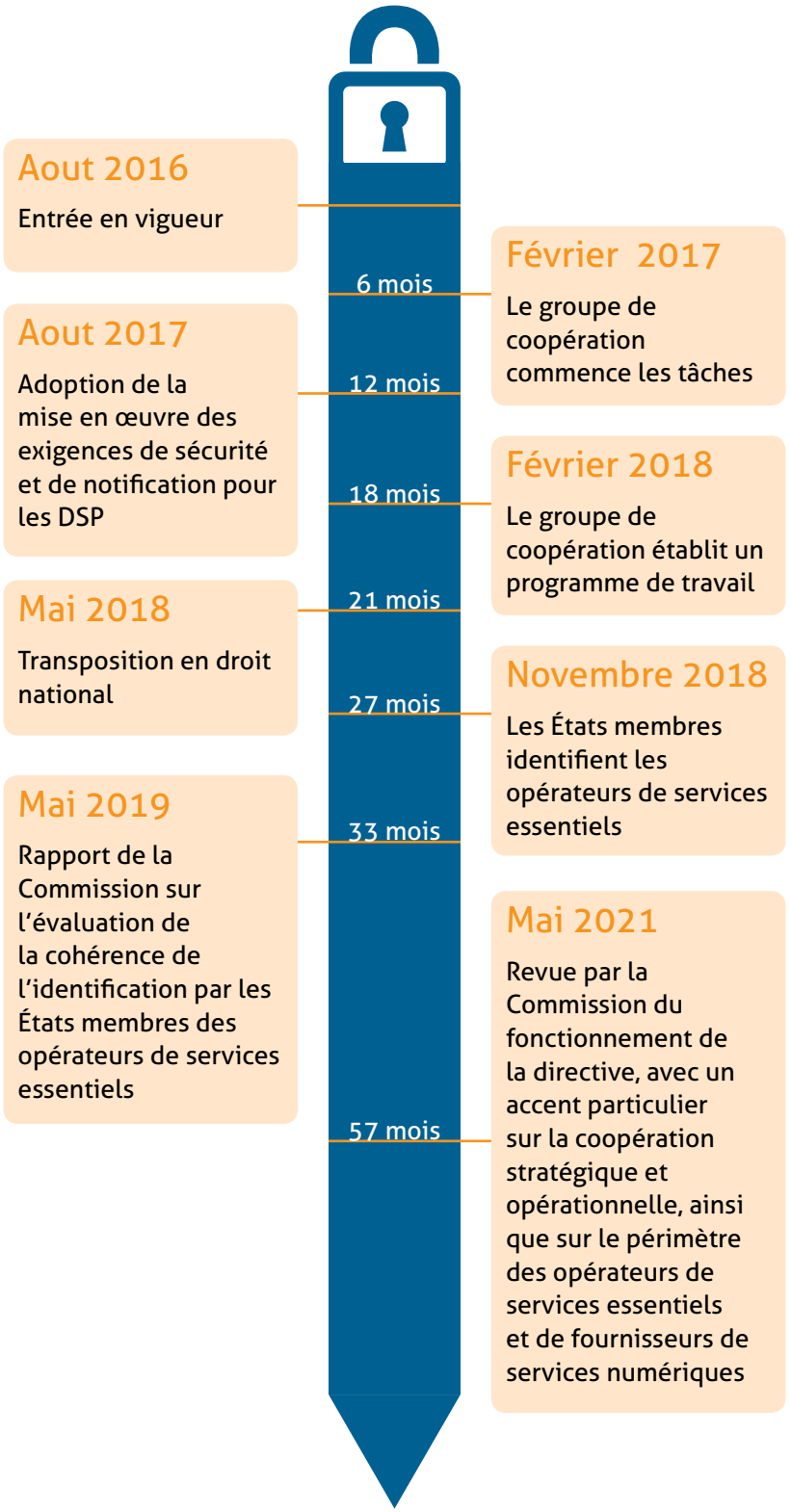
Fiche descriptive sur la cyber sécurité au sein de l'Union

http://ow.ly/YkSJ302Gs83

Communiqué de presse de la Commission Européenne sur la directive NIS approuvée par le parlement Européen

http://ow.ly/Z5Nk302Gsaf

# Quel est le calendrier de mise en œuvre de la directive?



AON Atos ENERVALIS Rexel a world of energy

SINTEF Trust-IT Trust-IT Services Ltd Communicating ICT to markets XLAB NOT IDLE

*Rejoignez la communauté des WISER d'avoir un accès gratuit à CyberWISER Light, et découvrez les dernières nouvelles et mises à jour sur le monde de la sécurité informatique.*

Abonnez-vous à la newsletter

Suivez-nous sur Twitter:

Connectez-vous sur LinkedIn:

European Commission