TRUST & Cie

Cyber Made in Provence

NIVEAU C1

NIS2, une loi de sélection naturelle ?

— Sociétés et profils impactés

Notre histoire

Trust & Cie

Trust & Cie est née du constat que la région SUD, bassin de savoirs et d'innovations, devait développer des compétences cybernétiques adéquates et disponibles pour accompagner son dynamisme économique et scientifique.

Ses fondateurs ont donc décidé de créer un cabinet d'audit régional, engagé dans une démarche de qualification PASSI et structuré pour accompagner les organisations vitales, importantes et essentielles de notre territoire dans les défis de cybersécurité et de conformité, en coordination avec leurs écosystèmes.

www.trustandcie.com

01

JUIN 2023 / KORTEX CONSULTING ET CABINET LOUIS REYNAUD FONDENT TRUST & CIE.

Pour contribuer, à leur niveau, au développement de l'expertise cyber qualifiée régionale, de proximité.

02

DES EXPERTISES RECONNUES

- Kortex Consulting, cabinet de conseil en cybersécurité et d'audit (eIDAS, PVID)
- Cabinet Louis Reynaud, premier laboratoire agréé ANSSI de la région Sud et expert auprès de l'ENISA sur les sujets de cybersécurité

03

TRUST...

Une organisation structurée selon les principes de *Security by Design* et *Security by Default*, privilégiant l'expertise, l'exigence et la haute protection de l'information,

04

... ET COMPAGNIE

Un travail permanent et en cohésion avec l'écosystème des professionnels de la cybersécurité, les institutions, les acteurs de l'enseignement et de la recherche.

Nos Services

Nos prestations sont opérées par des consultants expérimentés, disposant d'une expertise construite sur le terrain. Elles sont adaptées au public ciblé et constamment enrichies et améliorées, grâce notamment aux retours de nos clients.

—Une équipe d'experts à votre service

AUDITS DE SECURITE —
Audits d'architecture, de configuration, physiques et organisationnels, tests d'intrusions

CONSEIL EN ARCHITECTURE —
Accompagnement stratégique et opérationnel,
Préparation à la mise en conformité (RGPD, NIST…)

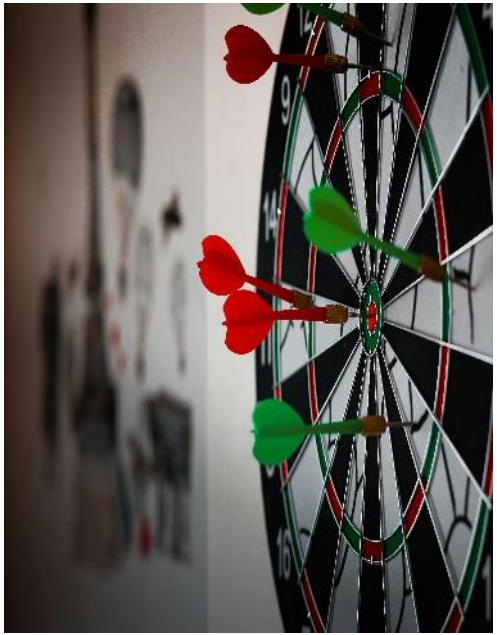
FORMATION —
Sensibilisation à la sécurité numérique,
Formation aux bonnes pratiques (ANSSI, CNIL), à la protection des données personnelles, au développement sécurisé…

Oui, nous allons encore parler de NIS2 !

En comprendre les enjeux stratégiques…

Petit rappel historique

- Des politiques européennes de cybersécurité fragmentées et peu coordonnées
- UE comme autorité harmonisatrice et régulatrice
- NIS 1 [16.07.2016] → NIS 2 [10.11.2022]

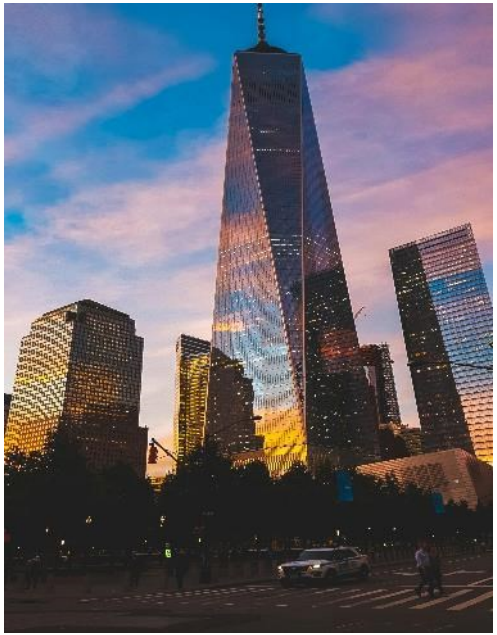


NIS2 : un périmètre étendu

Vraiment étendu...

Les secteurs couverts

- Énergie
- Transport
- Banques
- Marchés financiers
- Santé
- Eaux potables
- Infrastructures Numériques
- Fournisseurs numériques
- Eaux usées
- Gestion des services des technologies de l´information et de la communication
- Administrations publiques
- Espace
- Services postaux et de messagerie
- Gestion des déchets
- Fabrication et production de produits chimiques
- Industrie [fabrication]
- Recherche



NIS2 : un périmètre étendu

Organisations concernées

Type d´organisations

- Entités Essentielles : Grandes entreprises
- Entités Importantes : Moyennes ET Grandes entreprises

Taille des organisations

- GRANDE : > 250 employés OU CA > 50 millions d´euros
- MOYENNE : > 50 employés OU CA > 10 millions d´euros

—

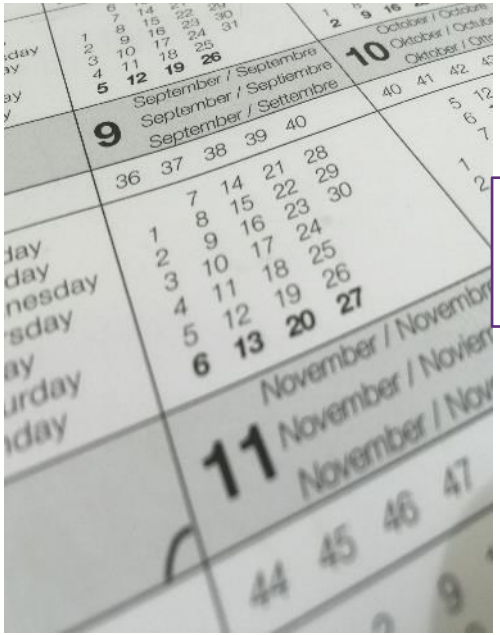
NIS2 : une volonté française

Donc une transposition scrupuleuse !

Sous la présidence française du Conseil de l´UE [Jan – Jun 2022], le comité Industrie, Recherche et Energie rédige le texte qui sera adopté le 10.11.2022 pour devenir la Directive NIS 2.

Le droit européen prime sur le droit français : la transposition prendra effet immédiatement.

—



NIS2 : c'est demain.

Planning de la transposition

Services du Premier Ministre
- Secrétariat Général du gouvernement
- Secrétariat Général des affaires européennes

Bercy
- Soumission du texte à l'AN

Assemblée Nationale
- Amendements
- Vote

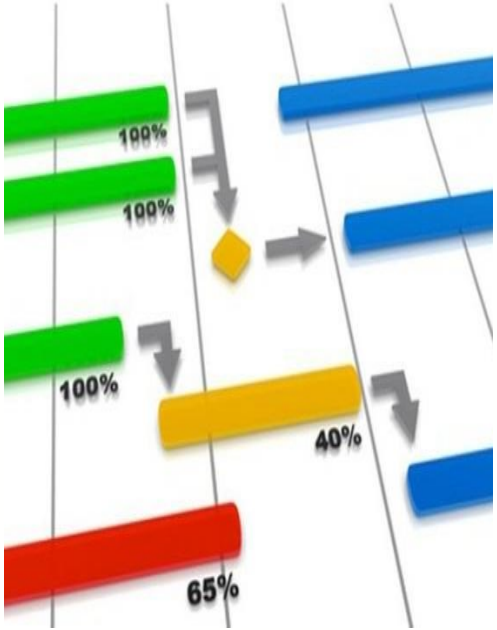
Décrets d'application

Services du Premier Ministre
- Rédaction : ANSSI

Commissions
- Affaires Européennes
- Lois Spéciales

Adoption
Transposition en droit FR

Deadline : 17.10.2024 !



NIS2 : et après-demain ?

Préparer la mise en œuvre

A partir de 2025, pour toutes les organisations concernées…

Prérogatives principales

- Gouvernance et approche par les risques [Art 20, 21.2.a, 21.2.f, 21.2.g]
- Sécurisation de la Supply chain [Art 21.2.d]
- Supervision et protection des SI [Art 21.2.b, 21.2.e]
- Gestion des accès, actifs et authentification [Art 21.2.h, 21.2.i, 21.2.j]
- Obligation de notification des incidents de sécurité [Art 23]
- Maintien en conditions opérationnelles [Art 21.1, 21.2.e]
- Continuité d´activité [Art 21.2.c]
- Obligation de formation des dirigeants et des équipes [Art 20.2]

—

La mise en œuvre

Comprendre les premiers jalons

Des thématiques empruntées à ISO 27001-2022

- Une approche basée sur les risques
- Une approche large et organisationnelle
- ISO 27001 citée comme référence dans les considérants du texte NIS 2

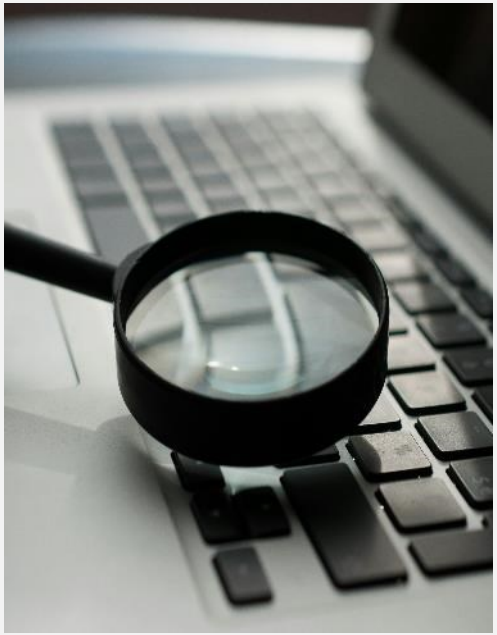
Différentes obligations que l´on soit catégorisé EE ou EI

- Un exemple quant aux différents contrôles qui seront effectués par l´ANSSI :
  - EI : contrôle ex-post –> en cas de connaissance d´une non-conformité
  - EE : contrôle ex-ante –> à la discrétion de l´ANSSI

Des questions encore en suspens

- Quel statut juridique pour l´ANSSI afin de faire appliquer les sanctions ? Pour rappel, le texte a obligation d´être contraignant !
- Quelles modalités de mise en œuvre ? Aides financières, mise à disposition de conseillers par l´ANSSI ?

—



Alors, pourquoi parler de sélection naturelle ?

Il va falloir s´adapter !

Un filet avec de plus petites mailles

- Passage de 300 OSE [NIS1] à 10 000 organisations concernées [NIS2]
- Les SI à sécuriser ne sont plus restreint aux « SI essentiels ».

Une politique volontariste = des contrôles accrus

- Sur des contraintes plus fortes [ex. notification d´incident en 24h]

Des risques pour les responsables

- Pour l´organisation : sanctions similaires à celles prévues par le RGPD
- Pour les personnes : interdiction d´exercer des responsabilités pour les dirigeants, sanctions pénales pour les RSSI

—

Sans oublier…

Un empilement de nouvelles réglementations

CRA : Cyber Resilience Act

- Cybersécurité des produits, en particulier des objets connectés

DORA : Digital Operational Resilience Act

- Sécurité des systèmes numériques du secteur de la finance : banques, compagnies d´assurance, producteurs de cryptomonnaies…

—

Crédits

- Pixabay
- Hasan Albari
- Mihai Vlasceanu
- Pixabay
- MART_PRODUCTION
- Agence Olloweb

Jean-Luc GARNIER
Mob +33 7 56 944 007

www.trustandcie.fr
contact@trustandcie.fr

TRUST

&Cie | Cyber made in Provence