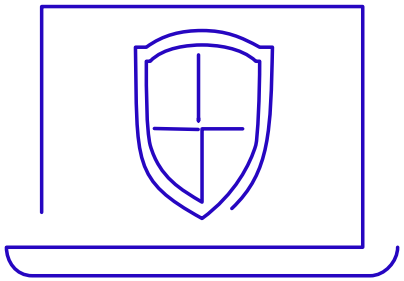


Obligations règlementaires

Secteur Transport Aérien

ORNISEC

Ayoub SABBAR, Expert Cyber

a.sabbar@ornisec.com

06 35 29 16 23

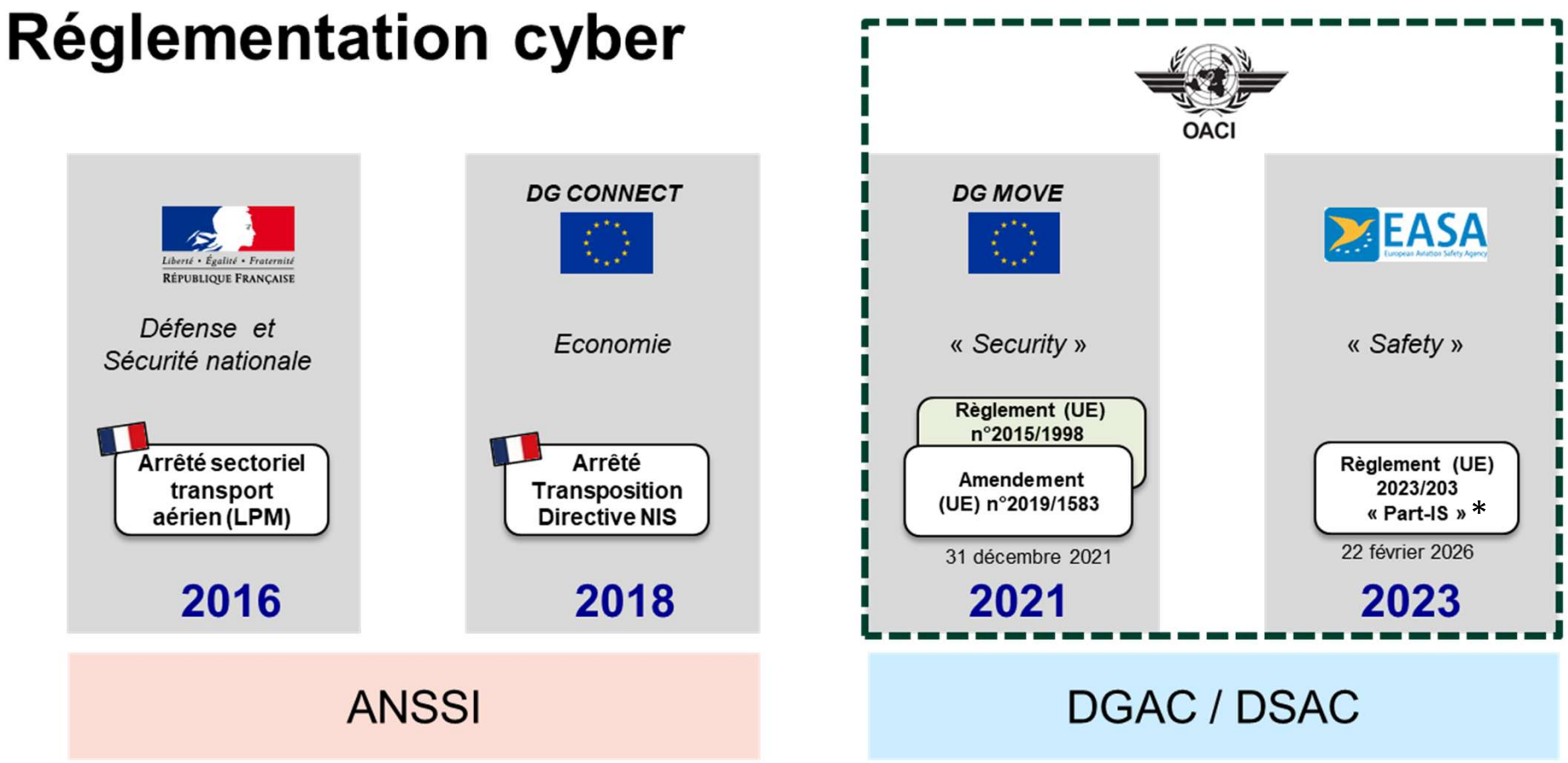
www.ornisec.com

SOMMAIRE

1.

Panorama des obligations cybersécurité

OBLIGATION CYBERSÉCURITÉ DU SECTEUR AÉRIEN



* PART IS
- EU 2023/203 pour ANSP
- EU 2022/1645 pour exploitant et services provider

ORNISEC

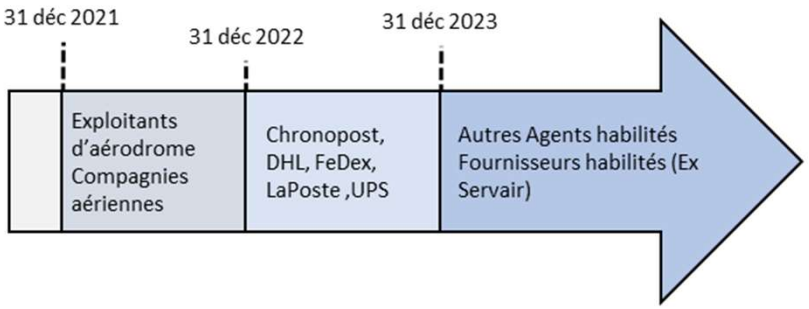
OBLIGATION CYBERSÉCURITÉ DU SECTEUR AÉRIEN

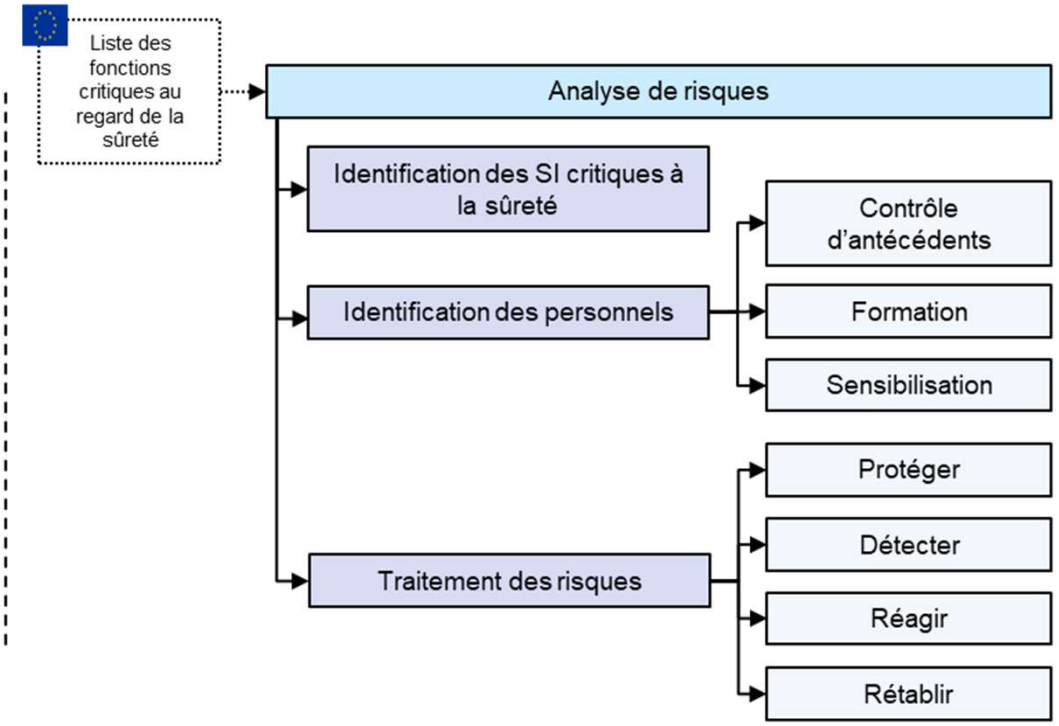
RÈGLEMENT 2015/1998

Règlement (UE) n°2015/1998 (Amendé par Règlement 2019/1583)

Cybersécurité appliquée aux fonctions **sûreté** assurées par les opérateurs / entreprises

Application du règlement (UE) n°2015/1998



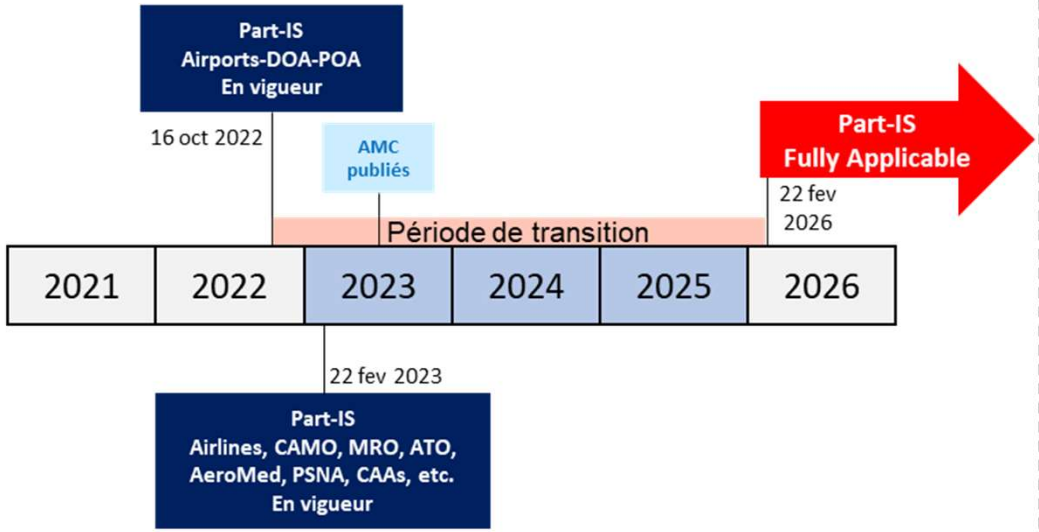


ORNISEC

OBLIGATION CYBERSÉCURITÉ DU SECTEUR AÉRIEN
RÈGLEMENT 2023/203

Règlement Part IS

Cybersécurité appliquée aux fonctions **safety** assurées par les opérateurs / entreprises



- **Système de management de la sécurité de l'information** (SMSI)
  - Définition d'une politique SSI
  - Identification des responsabilités
  - Formation
  - Gestion documentaire
  - Processus d'identification et d'évaluation des risques
  - Processus d'atténuation des risques
  - Report d'événements (interne)
  - Surveillance interne de la conformité
  - Gestion des changements (du SMSI)
  - Amélioration continue (du SMSI)
- **Report d'événements vers l'Autorité** / EASA

Articulation avec le SMS nécessaire voire intégration

ORNISEC

OBLIGATION CYBERSÉCURITÉ DU SECTEUR AÉRIEN

CADRE DE CONFORMITÉ CYBERSÉCURITÉ EN FRANCE – 3CF

- **Finalité :** Permettre aux aéroports d'initier les travaux de mise en conformité pour être prêt d'ici 2025
- **Objectif :** Rationaliser les différentes dispositions réglementaires propres à l'aviation civile et d'en faciliter ainsi la mise en œuvre.
- **Contenu :** Inspirer de l'iso 27001 et des bonnes pratiques ANSSI
- **Périmètre** : le cadre de conformité couvre à la fois :
  - Le règlement (UE) n°2015/1998 : la sécurité des SI participant à la sûreté de l'aviation civile

    Aéroports et compagnies aériennes avec agrément de sûreté
  - PART-IS : les règlements (UE) n°2022/1645 et 2023/203 : la sécurité des SI liée à la sécurité de l'aviation civile

    CAT, ATO, PSNA, FSTD, CAMO, MRO et Centre aéro médicaux

OBLIGATION CYBERSÉCURITÉ DU SECTEUR AÉRIEN

CADRE DE CONFORMITÉ CYBERSÉCURITÉ EN FRANCE – 3CF

Inspire

Intègre les exigences

Part IS partielle

RUE 2015/1998

évolue

Intègre les exigences

Part IS
Rule
AMC

Aéroports et compagnies aériennes avec agréement de sûreté

Objectifs :
- Référentiel unique
- Démarche de mise en conformité
  - Conformité au RUE 2015/1998
  - Préparation à la Part IS

Guide DSAC

Aéroports et compagnies aériennes avec agréement de sûreté

Objectifs :
- Référentiel unique
- Conformité au 1998 et Part IS

CAT, ATO, PSNA, FSTD, CAMO, MRO et Centre aéro médicaux

Objectifs :
- Conformité à la Part IS

Moyen alternatif de conformité à la Part IS ?

3CFv3 sera bientôt disponibles pour prendre en compte NISv2

ORNISEC

2.

Zoom sur la directive NISv2

Introduction à NIS 2

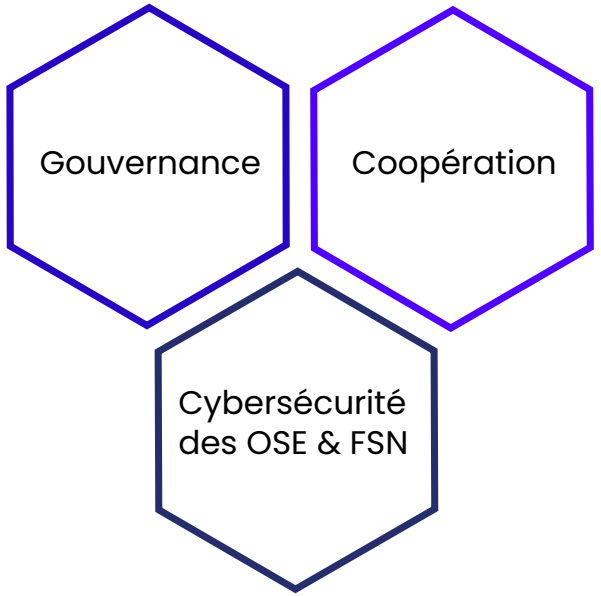
Résumé de la directive NIS 1

NIS 1 en quelques points

Objectif
Renforcer la sécurité numérique sur le marché européen pour préserver ses intérêts économiques et sociaux

Champ d'application
Tous les opérateurs de service essentiel par arrêté du Premier ministre

Date d'entrée en vigueur
26 février 2018 (Europe)



Les dispositions principales de NIS 1

Introduction à NIS 2

Les grands changements apportés par NIS 2

01

Augmentation du champ d'application de NIS

- De 300 à 15 000 entités concernées (En France).

02

Renforcement des mesures de sécurité

- Spécification et ajout de nouvelles exigences telles que l'utilisation du chiffrement, MFA, ...

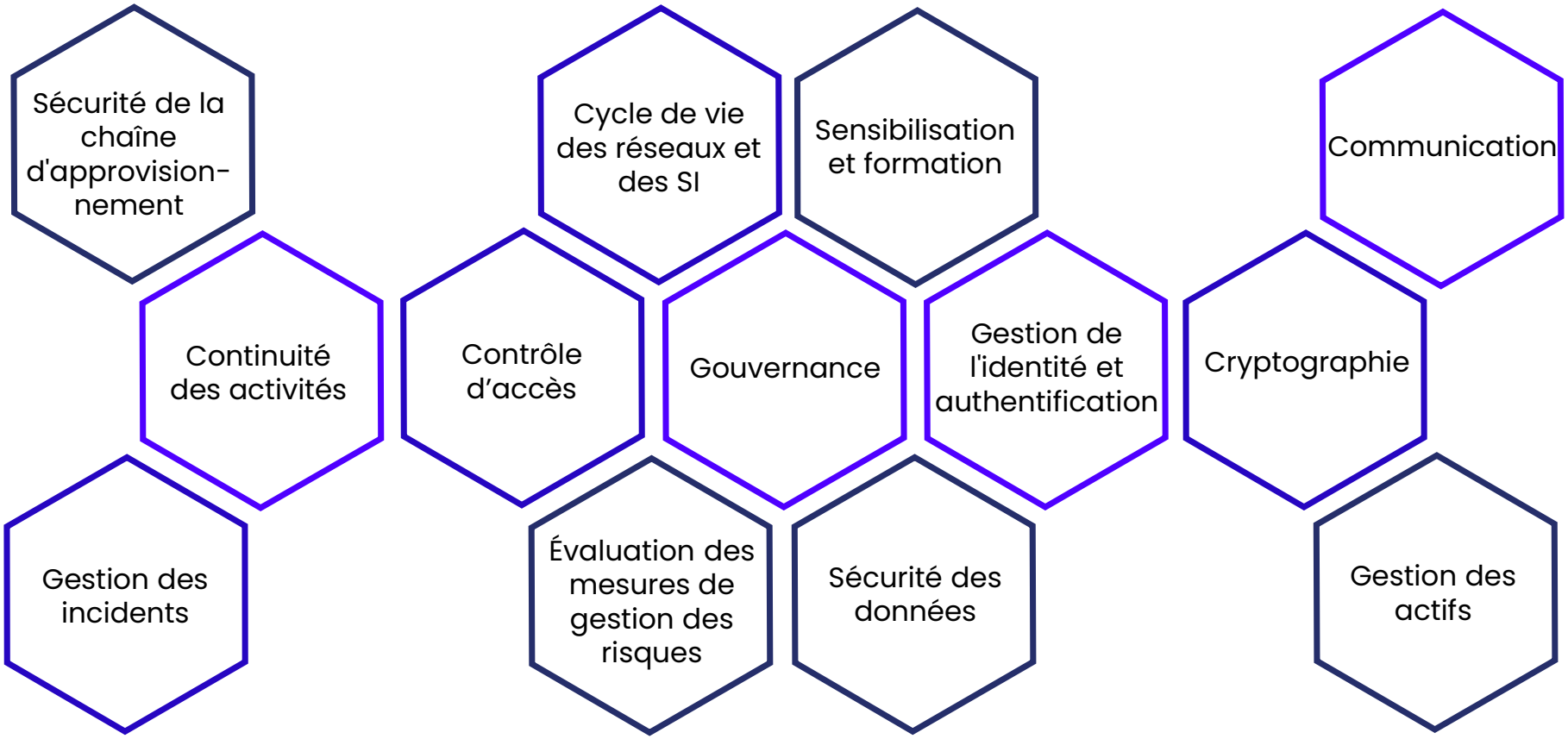
03

Intégration d'un système de proportionnalité

- Création de la notion des entités essentielles (EE) et importantes (EI).

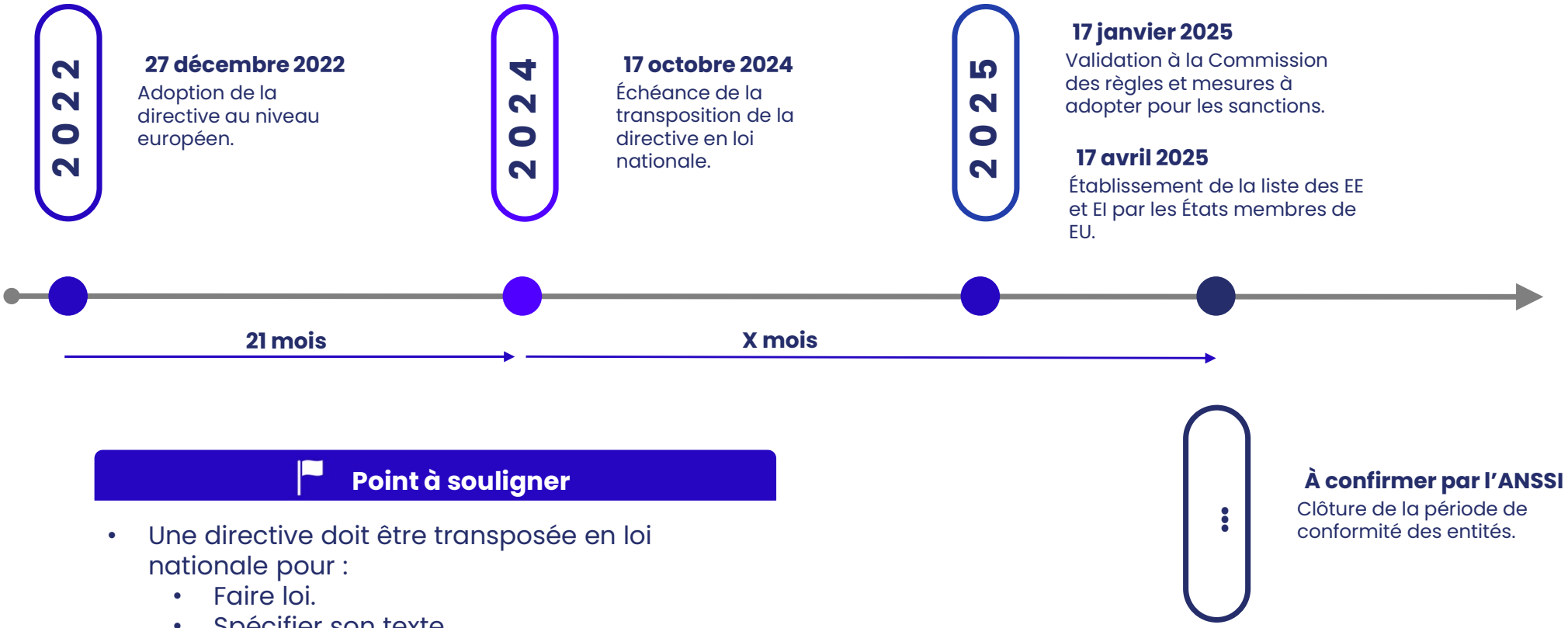
Introduction à NIS 2

Les thématiques abordées par NIS 2



Introduction à NIS 2

Le planning de la transposition



Point à souligner

- Une directive doit être transposée en loi nationale pour :
  - Faire loi.
  - Spécifier son texte.

3.

Mise en conformité à NIS 2

Mise en conformité à NIS 2

Détermination des entités concernées par NIS 2 — Méthodologie

1.
Correspondance du secteur d'activité avec ceux des annexes I & II

2.
Respect des critères de nombres d'employés et de chiffre d'affaires

3.
Détermination du type d'entité (Essentielle ou importante)

Cas particulier – Supply Chain Attack

Si l'organisation est **un sous-traitant/fournisseur ayant accès au SI** d'une entité concernée, alors **elle est directement soumise à NIS 2**.

Coup de pouce

L'ANSSI a mis à disposition un site « **MonEspaceNIS2** » avec un **test** afin de déterminer l'obligation d'une organisation à se conformer à NIS 2.

Mise en conformité à NIS 2

Détermination des entités concernées par NIS 2 — Secteurs d'activités

<table>
<tr><td rowspan="2">ANNEXE I</td><td colspan="2">Énergie</td><td colspan="2">Transports</td><td>Bancaire</td><td>Santé</td><td>Eaux</td><td>Infrastructure numérique</td><td>Administration publique</td></tr>
<tr><td>Électricité</td><td>Pétrole</td><td>Aérien</td><td>Ferroviaire</td><td>Crédit</td><td>Prestataire</td><td>Potable</td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>Gaz</td><td>Hydrogène</td><td>Eau</td><td>Routier</td><td>Marchés financiers</td><td>Recherche</td><td>Usées</td></tr>
<tr><td rowspan="3">ANNEXE II</td><td>Poste</td><td>Gestion des déchets</td><td colspan="2">Fournisseurs numériques</td><td colspan="3">Fabrication</td><td colspan="2">Gestion des services TIC</td><td>Espace</td></tr>
<tr><td>Alimentaire</td><td>Produits chimiques</td><td>Marché en ligne</td><td>Moteur de recherche</td><td>Dispositifs médicaux et in vitro</td><td>Machines et équipement n.c.a</td><td>Matériels de transport</td></tr>
<tr><td colspan="2"></td><td colspan="2">Réseaux sociaux</td><td>Électronique et optique</td><td>Automobiles</td><td>Remorques et semi-remorques</td></tr>
</table>

Mise en conformité à NIS 2

Détermination des entités concernées par NIS 2 — Nombre d'employés et CA

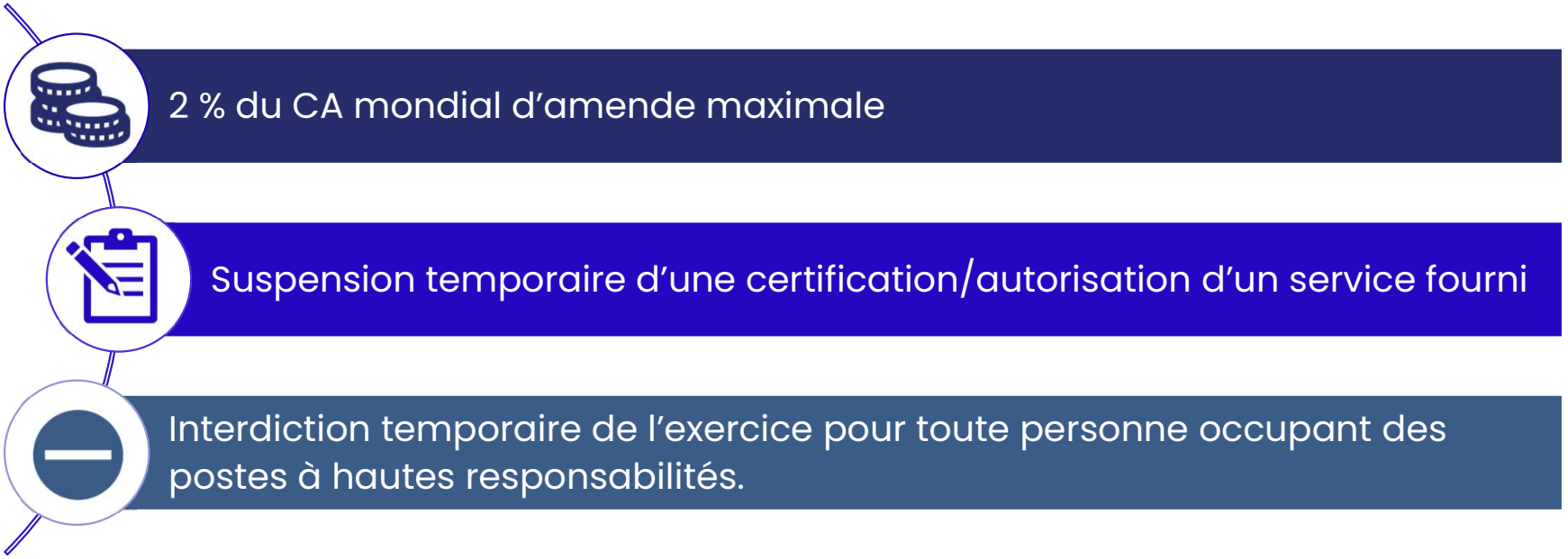
Taille de l'entité	**Nombre d'employés**	CA (Millions d'€)	**Bilan annuel (Millions d'€)**	**Annexe 1**	**Annexe 2**
Intermédiaire & Grande	x ≥ 250	y ≥ 50	z ≥ 43	Entités Essentielles	Entités Importantes
Moyenne	50 ≥ X ≥ 250	10 ≥ Y ≥ 50	10 ≥ Z ≥ 43	Entités Importantes	Entités Importantes
Micro & Petite	X < 50	Y < 10	Z < 10	Non Concernées	Non Concernées

Mise en conformité à NIS 2

Les sanctions encourues

Attention

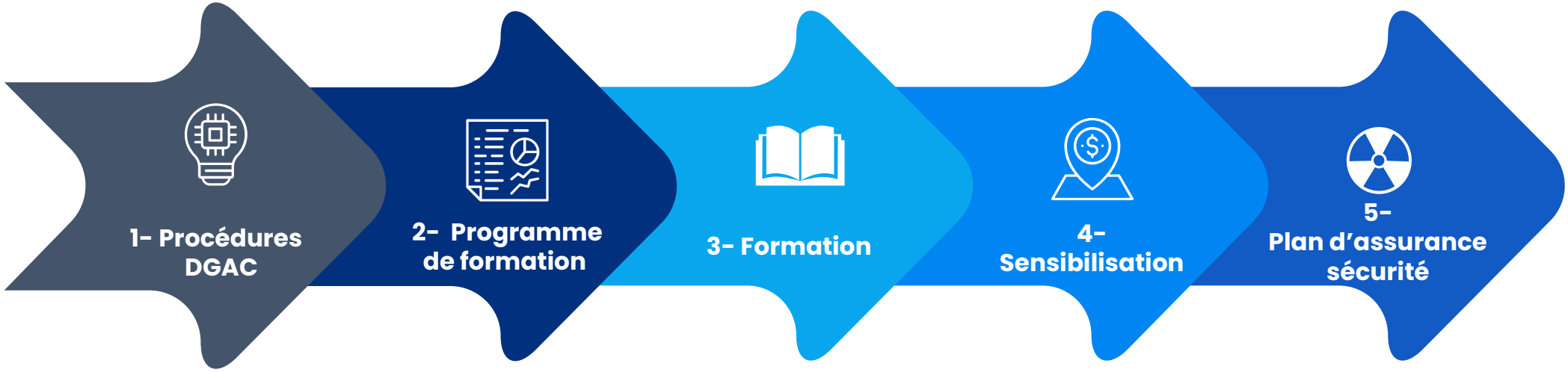
Puisque NIS 2 n'est pas encore transposée en loi nationale, alors les sanctions peuvent toujours être altérées. L'ANSSI a donné une date de dernière modification le 17 janvier 2025.



4.

Les obligations en tant que prestataires (AMOA, Intégrateur, éditeur) du secteur aérien

OBLIGATIONS CYBERSÉCURITÉ DES FOURNISSEURS - 3CF / PART IS

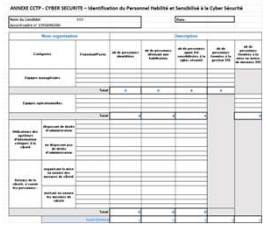


Rédaction des procédures imposées par le 3CF :

- Procédure de formation
- Procédure de sensibilisation
- Procédure de gestion des habilitations

Programme de formation :

- Lister les acteurs concernés
- Formaliser le programme de sensibilisation et de formation annuel pour chaque acteur
- Fournir le fichier Excel DGAC



Animer les 3 formations obligatoires

1. Module de Formation sécurité opérationnelle : Equipe IT/DSI
2. Module de Formation sécurité des systèmes industriels : Service technique / OT
3. Module de Formation à la gestion SSI / SMSI : Référent cyber/RSSI

(Conforme 3CF)

Animer la sensibilisation obligatoire :

- Module de formation pour l'ensemble des salariés (Conforme 3CF)

Réaliser un PAS

- Chapitre 1 : Justifier la sécurité du SI du prestataire
- Chapitre 2 : Justifier la conformité des produits avec chaque exigence 3CF côté fournisseur et des obligations avec la directive NISv2

ORNISEC

OBLIGATIONS CYBERSÉCURITÉ DES FOURNISSEURS - NISV2

Auto-déclaration sur le site de l'ANSSI

Analyse d'impact pour identifier le périmètre de la conformité (Exclusion justifiée possible)

Audit de conformité pour élaborer une feuille de route de mise en conformité sur 3 ans (délai proposé par l'ANSSI)

Lancement des travaux et suivi avec la direction

Réaliser un PAS

- Justifier la conformité des produits et du SI avec la directive NISv2

Livre Blanc

Un livre Blanc a été rédigé par les consultants ORNISEC sur les travaux de mise en conformité NISv2

Livre Blanc

Le livre blanc est disponibles en téléchargement sur le site ORNISEC https://www.ornisec.com/livre-blanc/

5.

Positionnement ORNISEC

ORNISEC, CABINET DE CONSEIL SPÉCIALISÉ DANS LE SECTEUR AÉRIEN

OFFRE D'ACCOMPAGNEMENT CLÉ EN MAIN POUR LE 3CF ET NISV2

3CF

- Produire le dossier de conformité avec le 3CF
- Formation 3CF (Qualiopi)
- Rédaction de PAS à inclure dans les AVV

1

NISv2

- Déclaration
- Identification du périmètre
- Audit de conformité
- Rapport de conformité à destination de l'ANSSI
- PAS à inclure dans AVV

2

Offre de service – Conseil & Audit en cybersécurité

Audit

- Audits d'architecture
- Audit Organisationnel et physique
- Audits de configuration
- Audits de code
- Tests d'intrusion
- Qualifié PASSI

Conseil

- Elaboration de PSSI & procédures
- Expertise sécurité & intégration
- Gestion des risques SSI
- Homologation sécurité
- Homologation RGS
- Schéma directeur
- Qualifié PACS*

Conformité

- Conformité LPM
- Conformité RGPD
- Conformité Directive NIS
- Conformité ISO27001
- Conformité HDS
- Conformité RGS
- Règlementation DGAC

Assistance RSSI et DPO (SSI)

- Gérer la sécurité opérationnelle
- Implémenter la PSSI
- Expertise sécurité
- Reporting et suivi des chantiers
- Coaching RSSI
- Réalisation des PIA - RGPD

Formation & Sensibilisation

- *Sensibilisation* : Programme, Phishing, Ateliers, QCM
- *Formation* : RSSI, Administrateur S&R, équipe industrielle, développeur et chef de projet.

Gestion de crise SSI

- Préparation : PCA/PRA, Proc. (incident, Crise)
- Exercice : Simulation de crise cybersécurité
- Réponse : Forensic, Réponse à incident
- PRIS (Qualification en cours)

* En attente de publication officielle

Ornisec est qualifiée PASSI sur les 5 portées

CERTI TRUST
CONFIDENCE IN THE DIGITAL ERA

ATTESTATION DE QUALIFICATION

ICTS France atteste par la présente que

ORNISEC
2, Le Plessix
35230 ORGERES
France

Est déclaré conforme au référentiel d'exigences publié par l'Agence Nationale de la Sécurité des Systèmes d'Information comme

Prestataire d'Audit de la Sécurité des Systèmes d'Information

(PASSI) V2.0 du 14 février 2013

En annexe du Règlement Général de Sécurité (RGS) institué par :
- Ordonnance N°2005-1516 du 8 décembre 2015 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Décret N°2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005 -1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.
- Arrêté du 13 juin 2014 portant approbation du Référentiel Général de Sécurité et précisant les modalités de mise en oeuvre de la procédure de validation des certificats électroniques.

Le Prestataire réalise les activités suivantes conformément aux exigences du référentiel PASSI v2.0 et du règlement de qualification d'ICTS France POL-7a v6.0 :

- AUDIT ORGANISATIONNEL & PHYSIQUE
- AUDIT D'ARCHITECTURE
- AUDIT DE CONFIGURATION
- TESTS D'INTRUSION
- AUDIT DE CODE SOURCE

Attestation N° **C-PASSI-072023-0CU01113-R2** Paris, le **25 juillet 2023.**
Qualification valide depuis le : **30-06-2023**
Début du cycle actuel de qualification : **30-06-2023**
Attestation valide du **30-06-2023** au **29-06-2026**
**Sujet à des évaluations de surveillance tous les 18 mois.*
L'attestation est renouvelée tous les 3 ans à la suite d'une évaluation de renouvellement.

Pierre Dewez,
Directeur Général.

ICTS France SARL
RCS Paris n° : 533 489 662
27, Place de la Madeleine
75008 Paris, France
+33 (0)7 61 56 58 37
passi@certi-trust.fr

PASSI CERTI TRUST
cofrac Accréditation n° 5-0597 CERTIFICATION DE PRODUITS ET SERVICES Liste des sites et portées disponibles sur www.cofrac.fr

Cette évaluation et l'attestation de qualification associée ont été menées dans le respect des procédures d'audit, de certification et de qualification d'ICTS France. Cette attestation peut être vérifiée en envoyant un e-mail à certification@certi-trust.com

Page 1 de 2

Ornisec est qualifiée PACS* sur les 4 portées

PREMIÈRE MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Le sous-directeur Expertise

Paris, le 19 DEC. 2023
N° 2206 /ANSSI/SDE

Monsieur le Directeur Général,

Vous avez déposé[1] une demande de qualification auprès de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) le 24 octobre 2023 en vue de faire qualifier votre service d'accompagnement et de conseil en sécurité des systèmes d'information au titre du décret n° 2015-350 du 27 mars 2015[2] et ainsi attester de sa conformité au référentiel d'exigences[3] élaboré par l'ANSSI.

Je vous prie de bien vouloir trouver en annexe la stratégie d'évaluation de ce service acceptée par l'ANSSI.

Ce courrier marque le franchissement des jalons « J0 » et « J1 » du processus de qualification d'un service[4].

Je vous rappelle que votre point de contact pour l'instruction de votre demande de qualification est Monsieur Oscar BOIZARD (oscar.boizard@ssi.gouv.fr) du bureau Qualifications et Agréments.

Je vous prie d'agréer, Monsieur le Directeur Général, l'assurance de ma considération distinguée.

Renaud LABELLE
Sous-directeur Expertise

1. Votre demande de qualification d'un service, réf. n°1892/ANSSI/SDE du 24/10/2023
2. Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. Disponible sur https://www.legifrance.gouv.fr
3. Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS), référentiel d'exigences, version 1.0 du 19 juillet 2023.
4. Processus de qualification d'un service, version en vigueur, référence QUAL_SERV_PROCESS. Disponible sur https://cyber.gouv.fr/procedures-et-formulaires-pour-la-qualification

Monsieur Ayoub SABBAR
Chief Executive Officer de ORNISEC
2 Le plessix
35230 Orgeres

51, boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél +33.1.71.75.25.25 - Télécopie +33.1.71.75.84.00

* PACS – Prestataire d'accompagnement Conseil en Sécurité - En attente de publication officielle

Merci !

Nous vous remercions pour votre écoute
Avez-vous des questions ?

AYOUB SABBAR

a.sabbar@ornisec.com

06 35 29 16 23

www.ornisec.com