MINISTÈRE
CHARGÉ
DES TRANSPORTS

Liberté
Égalité
Fraternité

osac

dgac direction générale de l'Aviation civile
DSAC

Cybersécurité
Wébinaire Attendus DSAC/OSAC
29/09/2025

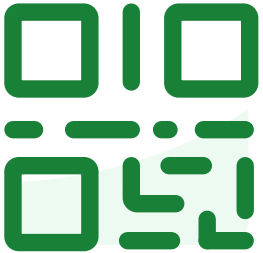
Direction de la sécurité de l'aviation civile

2 OCTOBRE 2025

MINISTÈRE CHARGÉ DES TRANSPORTS
Liberté
Égalité
Fraternité

dgac direction générale de l'Aviation civile
DSAC

osac

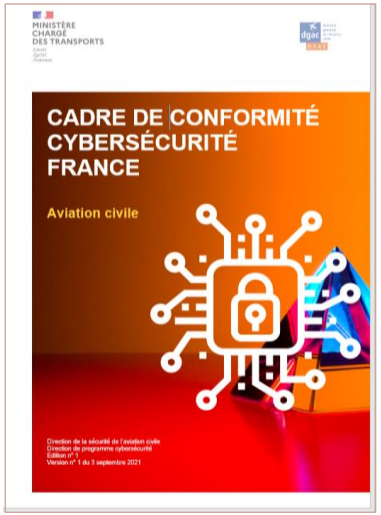


Join at slido.com
#Cyber2025

Part-IS : Principaux changements du Système de gestion

Cadre de Conformité Cyber France

- **Guide d'aide à la mise en œuvre des exigences réglementaires de cybersécurité**
  - Référentiel unique pour la conformité aux règlements 2019/1583 et Part – IS
  - Développé sur la base des AMC/GM de l'EASA
  - Approche pédagogique de la gestion des risques de cybersécurité basée sur l'ISO 27001
  - Références aux bonnes pratiques et guides : ANSSI, EUROCAE, OACI, etc.
- **Langage commun entre les autorités (DSAC/OSAC) et les organismes surveillés**
  - Document élaboré avec les opérateurs, l'industrie, les fédérations (UAF/FNAM) et l'ANSSI
  - Travail commun DSAC et OSAC



3CFv3 publié Eté 2025

Organisation SMSI

Rôles et Responsabilités (IS.I/D.OR.240)

- 3 Personnes identifiées :
  - Dirigeant Responsable
    - Mise en œuvre d'une organisation et de moyen
    - Possibilité de coordination avec une personne responsable commune au sein de l'entreprise : même niveau hiérarchique que le DR dans l'organisation
  - Responsable de la MISE EN ŒUVRE de la Part-IS : ***Nouvelle fonction***
    - en **lien direct avec le DR**
    - a l'autorité et la compétence sur la Part-IS
  - Responsable de la CONFORMITE à la Part-IS **indépendant** de celui/celle ou ceux qui la mettent en œuvre
    - Bonne pratique : Responsable identique par rapport aux exigences techniques (CMM/RSC/RQ)
    - en **lien direct avec le DR**

Organisation (IR.I/D.OR.240)

- Plusieurs formats d'organisation possibles
- Bonne pratique : ne pas modifier l'organisation déjà en place assurant déjà une mitigation des risques cyber sécurité

Politique de Sécurité

Engagement du DR (IS.I/D.OR.200)

- Engagement à mettre en œuvre des moyens adaptés de protection contre l'atteinte à la confidentialité, l'intégrité, la disponibilité et l'authenticité des informations
- Bonne pratique : Ajouter les engagements Cybersécurité aux engagements sur la sécurité des autres agréments

Politique SSI de l'engagement (IS.I/D.OR.200)

- faire de la cybersécurité une des priorités de chaque responsable
- réaliser et maintenir ses activités en conformité avec les règlements applicables ainsi qu'avec toute exigence supplémentaire spécifiée par l'organisme ;
- prendre en compte les bonnes pratiques ;
- de définir des principes de fonctionnement du SMSI intégré au SGS ainsi que des objectifs de sécurité
- garantir les principes et la mise en œuvre de la culture juste
- mettre à disposition des moyens humains et financiers nécessaires à la mise en place et au fonctionnement du système de gestion
- promouvoir en continu cette politique auprès des personnes sous sa responsabilité

Gestion des incidents de sécurité de l'information

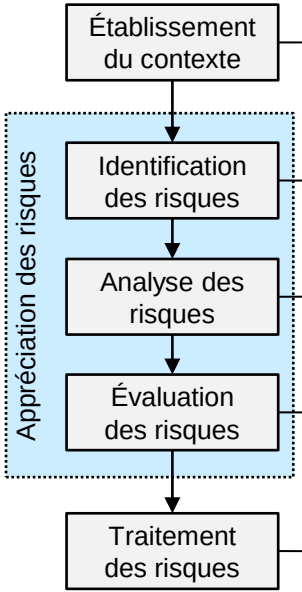
Système de notification des événements (IS.I/D.OR.215)

- Système de notification des événements Cybersécurité permettant la remontée et l'analyse
- Bonne pratique : en fonction des règles de confidentialité, l'utilisation des canaux existants pour les événements SV est possible

Gestion des incidents (IS.I/D.OR.220)

- 3 Objectifs :
  - détecter les incidents de sécurité de l'information
  - réagir à la suite d'un incident de sécurité de l'information
  - se rétablir à la suite d'un incident de sécurité de l'information
- Bonne pratique : intégrer les objectifs et méthodes dans les ERP, procédure d'utilisation d'outils de back-up

Analyse et Gestion des risques CyberSécurité



- Périmètre **IS.OR.205 (a)**
- Échelles d'analyse de risques **IS.OR.205 (c)**

- Fonctions et des interfaces **IS.OR.205 (a)**
- Événements redoutés et impacts **IS.OR.205 (c)**
- Scénarios de risque **IS.OR.205 (c)**

- Quantification des risques **IS.OR.205 (c)**
- Risque = scénario de risque (gravité ; vraisemblance) **IS.OR.205 (c)**

- Priorisation des risques **IS.OR.205 (c)**

- Actions pour le traitement des risques **IS.OR.210 (a)**
- Plan de traitement des risques **IS.OR.210 (a)**
- Évaluation des risques résiduels **IS.OR.210 (a) & IS.OR 210 (b)**

Bonne pratique :
Méthodes de modélisation d'analyse et de priorisation similaires aux risques SV
Adaptation de la probabilité d'occurrence par la vraisemblance

Intégration de l'analyse et des remontées dans les instances du Système de gestion

Assurance de la conformité

Organisation de la surveillance interne (IS.I/D.OR.200)

- Définition d'un programme de surveillance Part-IS : intégration des exigences d'organisation et de sécurité dans la vérification des exigences SG
- Vérification de l'efficacité des barrières de prévention des risques Cyber
- Bonne pratique : utilisation de l'organisation, des outils de la surveillance interne pour intégrer la surveillance Part-IS

Gestion des changements

Procédure de gestion des changement (IS.I/D.OR.255)

- Modification de la procédure de "gestion des changements non-soumis à accord préalable de l'autorité" pour intégrer des spécificités liées à la Partie IS
- Les changements suivants devraient être traités dans le cadre de cette procédure des changements non-soumis à accord préalable de l'autorité :
  - Les changements de méthodes d'évaluation du risque Cyber
  - Les changements de processus de notification des évènements
  - La modification du manuel SMSI (hors changement soumis à approbation)
- Les changements suivants sont soumis à approbation de l'autorité :
  - La chaine de responsabilité au sein du SMSI
  - La politique sécurité
  - La procédure de gestion des changements non soumis à approbation préalable

Intégration du risque Cyber à la gestion des changements (IS.I/D.OR.205)

- Modification de la procédure de gestion des changements pour intégrer l'analyse des risques cybersécurité

MINISTÈRE CHARGÉ DES TRANSPORTS
Liberté
Égalité
Fraternité

dgac direction générale de l'Aviation civile
DSAC

osac

Part-IS : Stratégie Commune DSAC-OSAC

Stratégie globale DSAC-OSAC

Analyse de la réglementation Part-IS

Un objectif d'application RBO pour concentrer les ressources sur les exploitants les plus exposés a permis de travailler sur des modalités de dispense pour certains exploitants redevables de la Part-IS (IS.IOR.200(e)).

Approche commune des métiers

Identification d'entité leader par organisme : Liste commune R4-R5-OSAC

1 métier en charge

- de l'instruction initiale
- de la surveillance du SMSI

Pour la surveillance, les entités suiveuses auditent uniquement des sondages sur la mise en œuvre de la Partie-IS dans son périmètre d'application en l'intégrant à d'autres audits.

Moyens communs pour l'instruction initiale

- Outil commun d'analyse pour les exploitants dispensés
- Attendus pour le dossier initial de mise en conformité

MINISTÈRE
CHARGÉ
DES TRANSPORTS
Liberté
Égalité
Fraternité

osac

dgac direction générale de l'Aviation civile
DSAC

PART-IS (RÉG. EXÉC. 2023/203)

Rappels sur le dépôt des demandes de dispense/mise en conformité initiale à la Part-IS

Sommaire

Dates et points clefs

La ***Part-IS*** est ***entrée en vigueur le 22 février 2023*** et ***s'appliquera à compter du 22 février 2026***: les organismes concernés (à agréments CAT ou SPO/NCC, et/ou ATO et/ou CAMO et/ou Part-145 … etc.) ont ***jusqu'au 22 octobre 2025 pour déposer leurs dossiers*** auprès de leur point de contact autorité (IEC pour la DSAC ou RS OSAC)

La suite de la présentation est composée de deux parties:

- Dépôt d'un dossier de mise en conformité initiale à la part-IS
- Dépôt d'une demande de dispense de mise en conformité à la part-IS

=> Elle adresse les points clefs à retenir par les opérateurs

1: Mise en conformité initiale à la part-IS

➔ Donne lieu à la délivrance d'une ***approbation*** de la part de OSAC et de la DSAC pour les agréments suivis sur la base de l'analyse de l'entité leader

- C'est le cas le plus courant pour les organismes certifiés
  - DSAC Quel que soit le nombre d'agréments de l'organisme un seul dossier est attendu sous METEOR
  - OSAC Un dossier par agréments est attendu. Le contenu est toutefois identique
- L'outil d'évaluation PJ2 à la communication 37760 participe à l'analyse d'exposition au risque cyber de l'exploitant

Cela implique:

- Mise en place d'un SMSI (système de management de la sécurité de l'information)
- Avec, par la suite, intégration de la vérification de la conformité de l'organisme à la part-IS aux audits SGS
- Il s'agit principalement des organismes soumis à approbation (i.e.: CAT) et/ou de typologie A3/A4 H3/H4 (et A5 (AF))

1: composition du dossier

- Demande d'approbation
- Matrice d'évaluation de la conformité conformité (PJ1 – Outil d'auto-évaluation conformité Part-IS
- Engagement du Cadre Responsable
- Référentiels :
    - Manuel du Système de gestion
    - Manuel du Système de gestion de la sécurité de l'information (SMSI)
    - CAT/SPO/NCC : La partie A1 du Manuel d'Exploitation (ou la partie du manuel système de gestion vers laquelle renvoie la partie A1)
    - ATO : le Manuel du Management de la Sécurité de l'Information (MMSI) à jour des dispositions de mise en conformité à la PART-IS
    - CAMO : manuel de l'organisme (CAME)
    - 145 : manuel de l'organisme (MOE)

Eléments à fournir par les organismes dans le cadre d'une mise en conformité initiale

1: Vos interlocuteurs – Qui fait quoi ?

Rappel « Qui fait quoi ? »:

Entité Leader : c'est l'entité de l'autorité (DSAC ou OSAC) qui réalise l'évaluation de l'ensemble des dispositions communes mises en place par les organismes pour répondre aux exigences de la Partie-IS, dans le cas où le Système de Management de la Sécurité de l'Information (SMSI) est commun à plusieurs agréments. Elle instruit les éléments transmis par l'organisme afin de s'assurer de la conformité aux exigences de la Part-IS pour l'ensemble des agréments de l'organisme.

Entité suiveuse : c'est l'entité de l'autorité (DSAC ou OSAC) qui se base sur les travaux réalisés par l'entité leader pour valider la conformité de l'organisme à la Part-IS au titre de l'agrément dont il est en charge

Exemple: Opérateur de typologie A4 avec agréments CAT/CAMO/145/ATO: R5 entité leader du fait de l'agrément CAT et OSAC entité suiveuse du fait des autres agréments (CAMO/145)

1: Profil et formation des responsables – Le CR

Cadre Responsable ou Personne responsable commune (PRC)

Vérifier une compréhension basique des exigences réglementaires européennes en matière de management de la sécurité de l'information.
N.B : cette compréhension pourra être assuré par une formation en interne, une présentation en SRB

Pour le CR/DR (ou PRC): connaissance basique de la réglementation (Part-IS) à satisfaire via par exemple la formation interne

1: Le Responsable de la mise en œuvre de la part-IS

Responsable de la mise en œuvre de la PART-IS

A l'instar des Responsables Désignés, le responsable est en charge de la supervision au quotidien de l'animation du SMSI et par la même du respect de la réglementation PART-IS. Les compétences attendues sont ainsi avant tout axées sur le domaine cybersécurité plutôt que de l'aérien. Certaines spécificités de l'aérien sont toutefois attendues :

Ainsi il convient de vérifier :

- la connaissance et la complète compréhension des exigences réglementaires européennes en matière de management de la sécurité de l'information ;
- le niveau d'information, restreint, du fonctionnement des domaines d'activité de l'organisme, du Système de gestion établi par l'organisme, des points de contacts dans les domaines opérationnels, de la culture juste et de sa promotion
- l'expérience opérationnelle liée à la sécurité de l'information (ex : responsable cybersécurité, responsable service informatique…).

Responsable de la mise en œuvre de la Part-IS équivaut à RD Cyber

=> Une connaissance fine de la réglementation et de l'opérateur chez qui il officie ainsi qu'une expérience opérationnelle SI lui sont demandées

N.B : Les principales preuves de la connaissance opérationnelle liée à la sécurité de l'information seront l'expérience dans les systèmes d'information et le niveau de poste similaire à un RD « OPS » ou « CAMO ».

La connaissance du règlement PART-IS pourra s'appuyer sur la participation à la mise en conformité à la PART-IS, sans besoin de formation complémentaire.

Les connaissances en lien avec le fonctionnement du système de gestion de l'exploitant (culture juste, référentiels, points de contact, instances) pourront s'appuyer sur une formation interne associée aux référentiels du système de gestion.

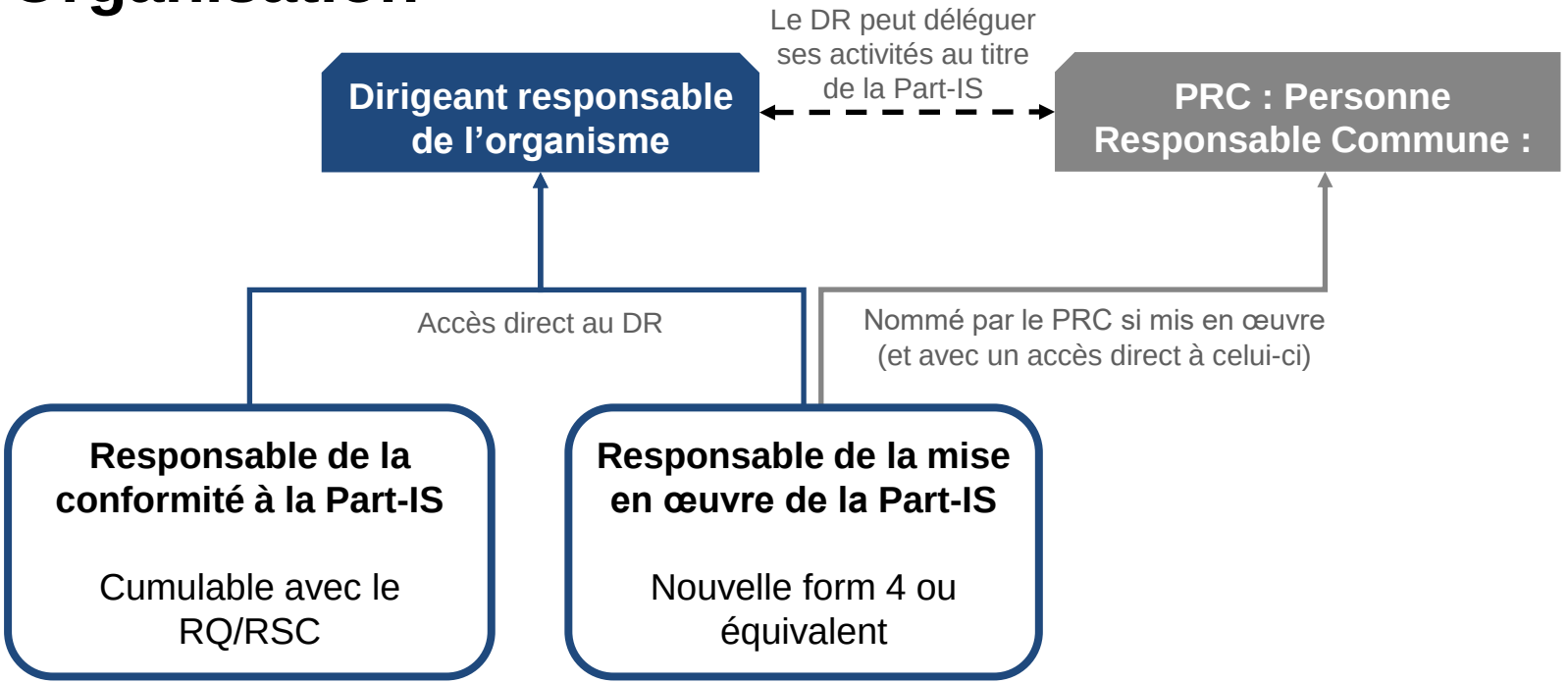
1. Le Responsable de la surveillance de la conformité

Responsable de la surveillance de la conformité En cas de cumul avec RCS « Exigences opérationnelles », vérifier - Le suivi d'une formation ou la démonstration de la connaissance des règlements Partie IS Sinon, vérifier en plus : - une connaissance du domaine d'activité de l'organisme - une connaissance du ou des Manuels de l'Organisme - avoir suivi une formation ou avoir une connaissance et avoir de l'expérience de la conduite d'audits

RSC cas 1: cumul avec casquette « AirOps »: formation à la part-IS

RSC cas 2: RSC dédié part-IS + connaissance de l'opérateur chez qui il/elle officie

1. Organisation



1. Politique de sécurité de l'information

Point clef: la politique liée à la sécurité de l'information peut être intégrée à la politique de sécurité du Système de Gestion

La politique de sécurité de l'information peut être intégrée à la politique de sécurité requise par les exigences des SG.
Les points spécifiques concernant la sécurité de l'information sont :

- faire de la cybersécurité une des priorités de chaque responsable
- réaliser et maintenir ses activités en conformité avec les règlements applicables ainsi qu'avec toute exigence supplémentaire spécifiée par l'organisme ;
- prendre en compte les bonnes pratiques ;
- de définir des principes de fonctionnement du SMSI intégré au SGS ainsi que des objectifs de sécurité ;
- garantir les principes et la mise en œuvre de la culture juste (la non-punitivité pour les personnes qui reportent un événement lié à la cybersécurité qui n'aurait pas été visible de l'organisme autrement et qui ne démontre pas des violations délibérées ou répétées aux règles) ;
- mettre à disposition des moyens humains et financiers nécessaires à la mise en place et au fonctionnement du système de gestion
- promouvoir en continu cette politique auprès des personnes sous sa responsabilité

Engagement du CR :

- Vérifier la signature de la politique et l'intégration aux référentiels

1. Procédure de gestion des changements

La procédure de gestion des changements doit prendre en compte deux nouveaux aspects : Changements en lien avec le SMSI - Vérifier l'ajout des changements en lien avec l'organisation du SMSI, et la politique Cybersécurité comme changements à approuver - Vérifier l'ajout des changements du processus de notification des événements cybersécurité, des méthodes d'analyse de risque cybersécurité, du RD Cyber Prévention des risques cybersécurité dans les changements opérationnels
- Vérifier que la procédure de gestion des changements intègre le risque cybersécurité et la conformité PART-IS aux études de changement et de risque

Point clefs: les nouveaux changements à ajouter à la procédure idoine sont ceux propres au SMSI et, globalement, l'intégration de la gestion du risque cyber

1. Gestion des événements Sécurité des Systèmes d'Information

Remontées des événements cybersécurité :
- Vérifier l'existence d'un canal de remontées des événements en interne du SMSI

Exemples : Evénement du quotidien (tentative d'intrusion, correction de bug)

Remontées des événements avec des conséquences sur la sécurité des vols :
- Vérifier l'existence d'un canal de remontées des événements cybersécurité et la mise en commun de l'analyse avec la Sécurité des vols

Exemples : Evénements avec conséquences Sécurité des vols Corruption avérée de base de données, dysfonctionnement des outils, remontée Pilote d'incohérence FM, base de données

Point clefs: moyens de remontées internes tel qu'un fichier Excel+email pour les événements de moindre gravité vs externe avec ECCAIRS pour les événements majeurs

1. Gestion des événements Sécurité des Systèmes d'Information

- Vérifier l'existence d'une méthode d'analyse de criticité, de risque cyber *Exemples :* *Description des conséquences du risque Cyber* *Matrice Gravité X Vraisemblance/Fréquence,* *Classification des applications ou outils SI* Il n'est pas nécessaire de vérifier à ce stade :
- Le contenu de la méthode d'analyse de risque cybersécurité

Point clef: mise en place d'une méthode d'analyse du risque cyber

1. Programme de surveillance interne

- Vérifier l'ajout de la mention PART-IS aux exigences à surveiller

Il n'est pas nécessaire de vérifier à ce stade :

- le contenu du programme de surveillance (découpage, cumul avec un audit du SG)
- la formation des auditeurs PART-IS

Point clef: la nécessaire mention « PART-IS » à vos exigences propres à ce règlement au sein de votre programme de surveillance interne

1. Supervision des sous-traitants

Sous-traitants participants au SMSI
- Vérifier la description des services contractés
- Vérifier l'existence d'un contrat de sous-traitance

Sous-traitants pour les fonctions opérationnelles :
Pas d'action de vérification nécessaire

Point clef: pour les sous-traitants au SMSI description services+contrat

2.1: Dispense d'appliquer l'intégralité de la Part-IS

L'outil d'évaluation PJ2 à la communication 37760 participe à l'analyse d'exposition au risque cyber de l'exploitant. Sur cette base, l'opérateur peut demander une dispense de l'application de la part-IS si l'exposition est limitée

L'opérateur doit fournir une analyse de risques quant à son exposition au risque cyber et l'impact sur la sécurité des vols

Avec une mise à jour lors d'un changement majeur dans l'organisation de son SMS et/ou de son exploitation/ses opérations

Il s'agit principalement des organismes sous régime déclaratif (i.e.: SPO/NCC; ATO, FSTDO) et/ou de typologie non complexes.

Côté autorités: La délivrance de la dispense à la PART-IS consiste à s'assurer que les risques encourus en termes de cybersécurité par un opérateur sont maitrisés par ce dernier et ne peuvent ainsi avoir de conséquences majeures sur la sécurité des vols. Cette action est formalisée par une ***autorisation*** de la part de OSAC et de la DSAC pour les agréments suivis sur la base de l'analyse de l'entité leader.

2.1: Composition du dossier

- Formulaire de demande de dispense à l'application de certaines exigences des règlements Part-IS (PJ3)
- Analyse de l'exposition au risque Cyber (PJ2)
- Engagement Cadre Responsable concernant la gestion du risque Cybersecurité (PJ3)
- Référentiels : procédure de gestion de changement (CAT, ATO)

Eléments à fournir à l'autorité

2: Eléments clefs analysés par l’autorité

- Vérification de l’engagement du CR/DR
- Précision des données de l’analyse de l’exposition au risque

➔ Examen du score de l’analyse de l’exposition au risque => cas intermédiaire cf. slides suivantes

2.2: La dispense, cas intermédiaires

Ce cas demande l'apport de l'IEC afin de s'assurer des changements récents intervenus chez l'opérateur et/par ailleurs niveau global de Sécurité des Vols chez ce dernier ➔ Le jugement de l'IEC permet de discriminer la situation la plus adaptée entre dispense et exemption.

L'analyse se fonde sur les points suivants:

- Caractère complexe ou non de l'opérateur (organisation >9 ETPs)
- CA (> 10 M€)
- Périmètre (>3 agréments)

+

- Criticité des fonctions numérisées (gestion des plans de vols par exemple)
- Prévention du risque cyber: mesures déjà en place sur les fonctions critiques
- Utilisation de la sous-traitance ou non

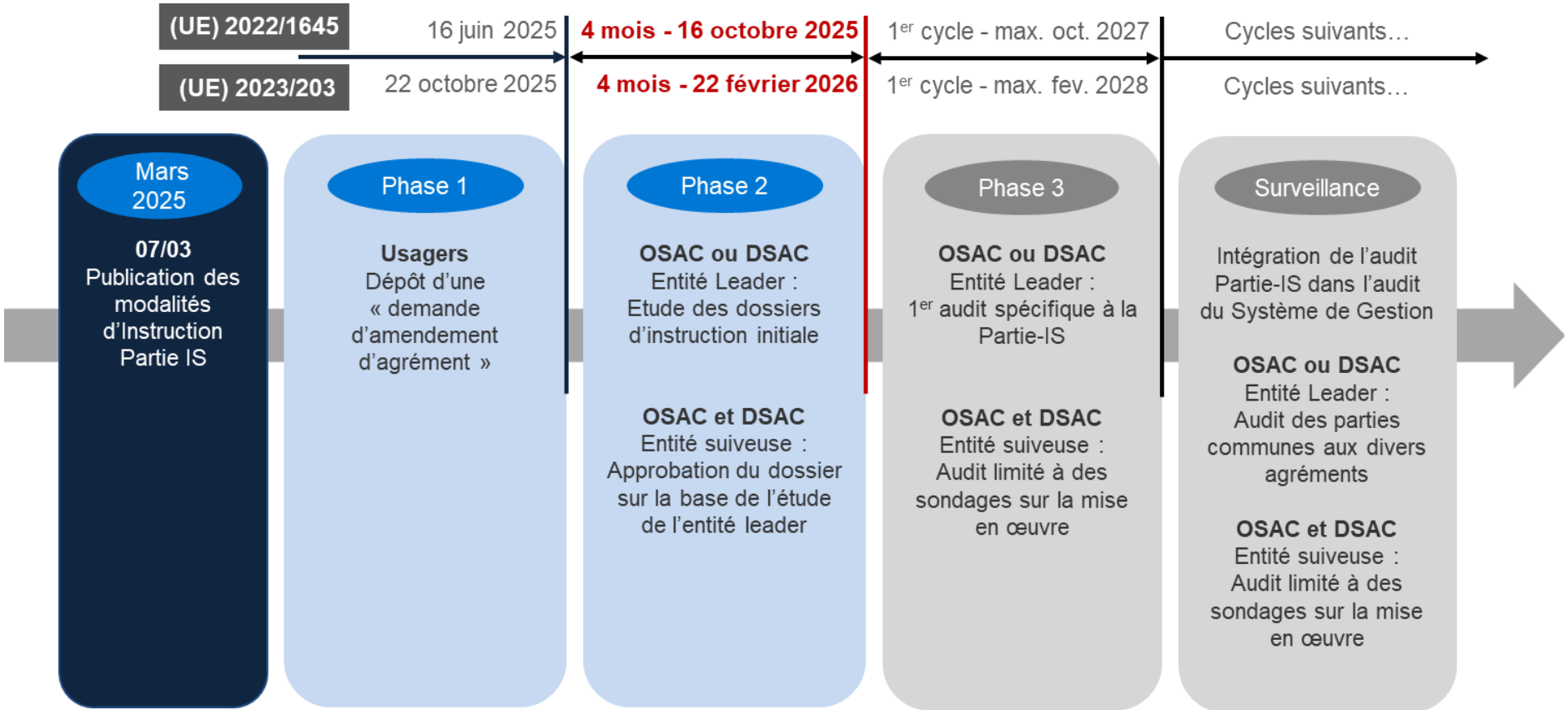
L'apport de l'Inspecteur de surveillance afin de s'assurer des changements récents intervenus chez l'opérateur et/par ailleurs niveau global de Sécurité des Vols chez ce dernier ➔ Le jugement de l'IEC permet de discriminer la situation la plus adaptée entre dispense et exemption

MINISTÈRE CHARGÉ DES TRANSPORTS
Liberté
Égalité
Fraternité

dgac
DSAC

osac

Cybersécurité
Calendrier – 2025/2026


(UE) 2022/1645
16 juin 2025
4 mois - 16 octobre 2025
1er cycle - max. oct. 2027
Cycles suivants…
(UE) 2023/203
22 octobre 2025
4 mois - 22 février 2026
1er cycle - max. fev. 2028
Cycles suivants…
Mars 2025
07/03
Publication des modalités d'Instruction Partie IS
Phase 1
Usagers
Dépôt d'une « demande d'amendement d'agrément »
Phase 2
OSAC ou DSAC
Entité Leader :
Etude des dossiers d'instruction initiale
OSAC et DSAC
Entité suiveuse :
Approbation du dossier sur la base de l'étude de l'entité leader
Phase 3
OSAC ou DSAC
Entité Leader :
1er audit spécifique à la Partie-IS
OSAC et DSAC
Entité suiveuse :
Audit limité à des sondages sur la mise en œuvre
Surveillance
Intégration de l'audit Partie-IS dans l'audit du Système de Gestion
OSAC ou DSAC
Entité Leader :
Audit des parties communes aux divers agréments
OSAC et DSAC
Entité suiveuse :
Audit limité à des sondages sur la mise en œuvre

Chronologie - Organismes

Communication Organisme

- Communication DSAC : COM#37760
- Communication OSAC : BI 2025/03
- Objectifs :
  - Modalité de mise en conformité ou de dispense : date d’envoi et attendus
  - Outils d’analyse, d’évaluation

Audience Q&A