MINISTÈRE
CHARGÉ
DES TRANSPORTS

Liberté
Égalité
Fraternité

direction générale de l'Aviation civile
dgac
DSAC

Direction générale de l'aviation civile
Direction de la sécurité de l'aviation civile
Direction technique Navigabilité et Opérations

Edité par : OSAC pour la Direction de la sécurité de l'Aviation civile

MODALITES DE MISE EN ŒUVRE DES REGLEMENTS (UE) 2022/1645 ET (UE) 2023/203 RELATIFS A LA PARTIE-IS

BULLETIN D'INFORMATION DSAC **BI 2025-03, Edition 0, version 0**

SOMMAIRE :

1. OBJET

Le présent Bulletin d'Information (BI) fait suite à la publication par l'Agence de l'Union Européenne pour la Sécurité Aérienne, l'AESA, des règlements (UE) 2022/1645 et (UE) 2023/203.

Ces règlements intègrent dans la règlementation AESA la Partie-IS, relative à la sécurité de l'information ayant un impact sur la sécurité aérienne.
Ce BI a pour but de détailler les modalités de démonstration de la conformité des organismes concernés par ces nouveaux règlements.

Ce Bulletin d'information fait l'objet des révisions suivantes :

Edition et version	Date	Modifications
Ed 0 v0	07/03/2025	Création

2. ABRÉVIATIONS

3CFv2	Cadre de Conformité Cyber France Version 2 – Guide commun DSAC/OSAC
AESA/EASA	Agence de l'Union Européenne de la Sécurité Aérienne / European Union Aviation Safety Agency
ANSSI	Agence nationale de la sécurité des systèmes d'information
AR	Autority Requirement
ATO	Approved Training Organisation
BI	Bulletin d'Information
CAMO	Continuing Airworthiness Management Organisation
CAT	Commercial Air Transport
DR	Dirigeant Responsable
ELA2	European Light Aircraft (voir Article 1 (j) du règlement (UE) No 748/2012)
FSTD	Flight Simulation Training Device
MMSI	Manuel de Management de la Sécurité de l'Information
NCC	Non-Commercial operations with Complex motor-powered aircraft
OR	Organisation Requirement
OSAC	Organisme pour la Sécurité de l'Aviation Civile
UE	Union Européenne
SGS	Système de Gestion de la Sécurité
SMSI	Système de Management de la Sécurité de l'Information
SPO	Specialised Operations

3. APPLICABILITÉ

Le présent BI s'applique aux organismes agréés suivant :

- La **Partie-21G** du règlement (UE) No 748/2012, à l'exception des organismes de production uniquement associés à la production d'aéronefs ELA2.

- La **Partie-145,** à l'exception des organismes participant uniquement à la maintenance des aéronefs conformément à la Partie-ML du règlement (UE) No 1321/2014.

- La **Partie-CAMO,** à l'exception des organismes participant uniquement à la gestion du maintien de la navigabilité des aéronefs conformément à la Partie-ML du règlement (UE) No 1321/2014.

4. RÉFÉRENCES

- Règlement Délégué (UE) 2022/1645 portant sur les modalités d'application du règlement (UE) 2018/1139 du Parlement européen et du Conseil en ce qui concerne les exigences relatives à la gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.
- Règlement d'exécution (UE) 2023/203 portant sur les modalités d'application du règlement (UE) 2018/1139 du Parlement européen et du Conseil en ce qui concerne les exigences en matière de gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.
- Règlement (UE) No 748/2012 établissant des règles d'application pour la certification de navigabilité et environnementale des aéronefs et produits, pièces et équipements associés, ainsi que pour la certification des organismes de conception et de production.
- Règlement (UE) No 1321/2014 relatif au maintien de la navigabilité des aéronefs et des produits, pièces et équipements aéronautiques, et relatif à l'agrément des organismes et des personnels participant à ces tâches.
- Guide DSAC « Cadre de Conformité Cyber France » Version 02 (3CFv2) du 30/04/2024.

5. RÉVISION

Sans objet.

6. CONTEXTE

La publication des règlements (UE) 2022/1645 et (UE) 2023/203 par l'AESA vient modifier les règlements (UE) No 748/2012 et (UE) No 1321/2014 afin d'y introduire des exigences en matière de sécurité de l'Information. Ils concernent notamment, pour les organismes surveillés par OSAC, les organismes de production, d'entretien et de gestion du maintien de la navigabilité. Ces nouveaux règlements s'appliquent de la manière suivante :

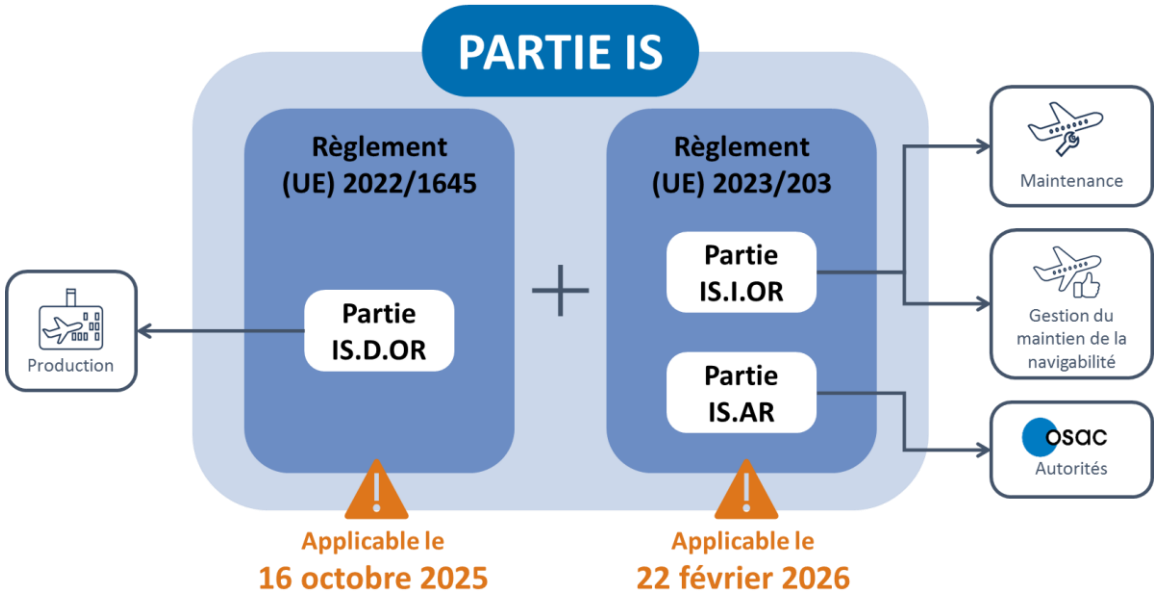

Figure 1 - Applicabilités des règlements (UE) 2022/1645 et (UE) 2023/203

Le règlement (UE) 2022/1645 est entré en vigueur le 16 octobre 2022 et sera applicable aux organismes agréés selon la Partie-21G le **16 octobre 2025**.

Le règlement (UE) 2023/203 est entré en vigueur le 22 février 2023 et sera applicable aux organismes agréés selon la Partie-145 et la Partie-CAMO ainsi qu'aux autorités compétentes le **22 février 2026**.

À compter de ces dates d'application, les organismes concernés doivent être conformes aux nouvelles exigences de la section A modifiée des règlements de référence ainsi qu'à la Partie-IS section OR dont ils sont redevables (voir schéma ci-dessus), et leur surveillance doit alors être réalisée suivant les nouvelles exigences des sections B modifiées qui leur sont applicables.

Ces nouvelles mesures nécessitent en particulier, la mise en place d'une organisation adaptée et efficace de l'organisme, en matière de gestion de la sécurité de l'information.

Dans ce cadre, la DSAC a publié un Guide (3CFv2) rédigé en concertation avec OSAC qui explicite les attendus relatifs à la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) au titre de la réglementation Partie-IS, et qui décrit les principes de base permettant d'y satisfaire.

7. INTEGRATION DU GUIDE DSAC « Cadre de Conformité Cyber France » Version 2 (3CFv2) DANS LE REFERENTIEL OSAC

Le guide DSAC « 3CFv2 », co-établi avec OSAC, uniformise les attendus de la Partie-IS pour l'ensemble des organismes concernés.

Le guide DSAC « 3CFv2 » est un moyen de conformité aux exigences s'appliquant aux organismes surveillés par OSAC :

- agréés selon la Partie-21G à l'exception des organismes de production uniquement associés à la production d'aéronefs ELA2.
- agréés selon la Partie-145 à l'exception des organismes participant uniquement à la maintenance des aéronefs conformément à la Partie-ML.
- agréés selon la Partie-CAMO à l'exception des organismes participant uniquement à la gestion du maintien de la navigabilité des aéronefs conformément à la Partie-ML.

La version en vigueur du guide « 3CFv2 » est publiée sur le site OSAC.

8. MODALITES D'INSTRUCTION INITIALE DE LA PARTIE-IS

La conformité aux exigences de la Partie-IS étant une condition du maintien des agréments des organismes concernés, ceux-ci doivent se mettre en conformité avec ces nouvelles exigences avant la date d'application et s'engager formellement auprès de leur autorité sur cette conformité.

La demande d'amendement d'agrément relatif à l'intégration de la Partie-IS devra être soumise avant les échéances suivantes, pour permettre un traitement par l'autorité avant la date d'application des règlements :

- le **vendredi 16 juin 2025** pour les organismes agréés Partie-21G et
- le **lundi 22 octobre 2025** pour les organismes agréés Partie-145 et Partie-CAMO,

soit 4 mois avant les dates d'application des règlements correspondants.

Ces demandes seront à transmettre :

- via le site METEOR de la DSAC, et/ou
- via le site internet OSAC

Pour cela, l'autorité notifiera, par courrier à chacun des organismes, les éléments à transmettre.

A ce titre les organismes sont invités à déposer un dossier de mise en conformité à la Partie-IS pour chacun de leurs agréments permettant ainsi à l'autorité :

- d'approuver l'organisation du système de gestion intégrant le SMSI ;
- d'approuver la politique de sécurité révisée afin d'y intégrer le risque « cybersécurité » ;
- d'approuver la procédure de gestion des changements pour y intégrer :
  - les changements du SMSI soumis à approbation de l'autorité (organisation du SMSI et politique de sécurité) ;
  - la réalisation d'une analyse du risque « cybersécurité » lors de ses études de sécurité pour tout changement;
- d'approuver la 1ère version du manuel SMSI après vérification de la cohérence globale de la couverture des attendus vis-à-vis du SMSI et d'absence de non-conformité manifeste ;
- d'accuser réception du changement relatif à la Partie-IS pour les autres éléments de mise en conformité non soumis à approbation préalable.

Les dossiers doivent contenir :

- Une **auto-évaluation Partie-IS** de la conformité de l'organisme incluant un engagement, signé par le dirigeant responsable, à être conforme aux dispositions de la Partie-IS (se référer au document 3CFv2 ; **disponible sur le site OSAC** dans la section « Documents pratiques ») ;
- Le **Manuel du Management de la Sécurité de l'Information (MMSI)** de l'organisme, s'il n'est pas intégré au Manuel de l'organisme ;
- Le **Manuel de l'organisme** ou les parties concernées qui intègrent les spécificités de la Partie-IS ou qui renvoient au Manuel du Management de la Sécurité de l'Information (MMSI) ;
- La **Form 2-12-50-51-60** (agréments Partie-21G, Partie-145 et Partie-CAMO) dûment renseignée, pour ce qui concerne uniquement les demandes déposées sur le site internet OSAC ;
- La **procédure de "Gestion des changements non-soumis à approbation préalable de l'autorité" ;**
- Le **justificatif (ex : CV) de la compétence/expérience des personnels** désignés au titre de la Partie-IS.

Cependant les règlements (UE) 2023/203 et (UE) 2022/1645 - Points IS.I/D.OR 200 (e), prévoient la possibilité que l'Autorité puisse dispenser un organisme, pour une période limitée dans le temps, d'appliquer certains éléments de la Partie-IS. Les modalités de dispense sont précisées au §9 du présent BI.
En cas de dispense par l'Autorité, les documents cités supra ne sont pas demandés.

Par ailleurs, dans la perspective d'une mutualisation de certains certaines actions de surveillance DSAC-OSAC, les demandes d'amendement seront à déposer :

- pour les agréments surveillés par la DSAC, sur le site METEOR via un dossier unique ;
- pour les agréments surveillés par OSAC, sur le site Internet OSAC via une demande par agrément, dont le contenu sera identique si le SMSI est commun aux différents agréments.

Ces demandes devront :

- préciser les agréments et déclarations couverts par la demande dans le titre de celle-ci (ou dans le champ prévu) ; et
- contenir les mêmes éléments, à l'exception du Manuel de l'organisme spécifique à chaque agrément.

En l'absence de réception de ces éléments dans les délais requis, une non-conformité pourra être notifiée à l'organisme, assortie, le cas échéant, de limitations d'exploitation/activités appropriées, des certificats d'agrément et/ou des déclarations de l'organisme à la date d'application du règlement (UE) 2023/1645 à savoir le 16 octobre 2025 ou du règlement (UE) 2023/203 à savoir le 22 février 2026.

Dans le cadre de l'instruction de ce changement, la DSAC ou OSAC pourra être amenée à notifier des points bloquants qu'il appartiendra à l'organisme de résoudre en apportant les actions correctives appropriées avant la date d'application de la Partie-IS.

En application de l'arrêté du 28 Décembre 2005 modifié, relatif aux redevances pour services rendus par l'Etat pour la sécurité et la sûreté de l'Aviation Civile, l'instruction de l'amendement de chacun des agréments concernés (Partie-CAMO, Partie-145, Partie-21G) sera soumise à une redevance calculée sur la base du temps passé. Un devis sera remis à l'organisme dès réception de la demande d'amendement, et la redevance devra être acquittée dans son intégralité avant l'analyse du dossier.

Pour les organismes non dispensés de la mise en conformité à la Partie-IS, à l'issue de l'instruction initiale, la vérification du maintien de la conformité aux exigences de la Partie-IS sera intégrée à la surveillance continue de l'organisme, réalisée par la DSAC (CAT, SPO, NCC, ATO, FSTD) d'une part et par OSAC (Partie-CAMO, Partie-145, Partie-21G) d'autre part.

9. MODALITES DE DISPENSE DE CERTAINES EXIGENCES DE LA PARTIE-IS

Comme abordé au chapitre précédent, les règlements (UE) 2023/203 et (UE) 2022/1645 - Points IS.I/D.OR 200 (e), prévoient la possibilité que l'Autorité puisse dispenser un organisme, pour une période limitée dans le temps, d'appliquer certains éléments de la Partie-IS. En particulier, l'organisme a la possibilité de ne pas mettre en œuvre un Système de Management de la Sécurité de l'Information (SMSI) s'il démontre, par une analyse de risque formalisée comme défini aux points IS.I/D.OR.205, qu'il présente un risque limité pour la sécurité aérienne au regard de l'exposition globale dans son activité quotidienne.

Sont potentiellement concernés par cette dispense, les organismes de type SPO, NCC, ATO, FSTD, certains CAT (notamment les moins complexes), Partie-CAMO, Partie-145 et Partie-21G.

Si l'organisme estime pouvoir prétendre à cette dispense pour un agrément donné, **en se basant sur son analyse de risque,** il peut alors en faire la demande auprès de l'Autorité concernée (DSAC ou OSAC). En cas de demande de dispense, il n'est pas nécessaire de déposer le dossier de mise en conformité à la Partie-IS.

Concernant les agréments surveillés par OSAC, les critères de base pour pouvoir prétendre à cette dispense sont, en fonction du type d'activité (basés sur les points GM1 IS.I/D.OR.200(e)):

- Partie-21G : Production uniquement d'éléments n'ayant pas de fonction « sécurité » majeure (exemple : moquette, rideaux, éléments d'aménagement intérieur …),
- Partie-145 : Travaux uniquement sur des éléments n'ayant pas de fonction « sécurité » majeure ou ne contribuant pas à l'intégrité structurale (exemple : le nettoyage, l'enlèvement des revêtements, la peinture…)
- Partie-CAMO :
    - Agrément CAMO gérant uniquement la flotte aéronef d'un exploitant considéré comme potentiellement dispensable par la DSAC (SPO, NCC, certain CAT notamment les moins complexe, etc.)
    - Agréments CAMO gérant uniquement des aéronefs en stockage ou mettant uniquement en œuvre la Sous-partie I.

L'organisme est invité à prendre connaissance des éléments d'explication ci-après et des éléments suivants, notamment l'outil qui explique la procédure à suivre :

- **Outil d'analyse de l'exposition au risque cyber disponible sur le site OSAC** dans la section « Documents pratiques » qui est un outil d'aide pour les organismes afin d'évaluer leur exposition au risque. Cette évaluation permet d'initier leur analyse de risque et d'argumenter un dossier de demande de dispense au sens des paragraphes IS.I/D.OR.200(e), si l'organisme établit qu'il répond aux critères.
- **Formulaire de demande de dispense** à l'application de certaines exigences des règlements Partie-IS, intégrant un engagement du dirigeant responsable relatif au traitement du risque cyber pouvant entraîner des conséquences sur la sécurité aérienne disponible en annexe I.

Une fois, l’outil et le formulaire complétés, ils seront à soumettre à l’OSAC, pour chacun des agréments concernés surveillés par OSAC, via l'espace client de l'organisme sur le site internet OSAC : Service : "Demande de dispense Partie IS"

Annexe I – Formulaire de demande de dispense Partie IS

Demande de dispense
à l'application de certaines exigences des règlements Partie-IS **conformément à l'IS.I/D.OR-200 (e)**

Sur la base de l'analyse de risques menée par l'organisme, le risque vis-à-vis de la sécurité *aérienne,* généré *par l'activité réalisée au titre de l'agrément XXX est limité au regard de l'exposition globale de l'organisme dans son activité quotidienne.*

En conséquence et conformément à *l'IS.I/D.OR-200 (e) je soussigné, XX, Cadre/Dirigeant responsable de [Nom de l'organisme], organisme ATO/FSTD/CAT/SPO/NCC/CAMO/145/21G[1] demande que l'exploitant soit dispensé de mettre en œuvre un Système de Management de la Sécurité de l'Information (SMSI) au titre de la Partie-IS.*

Vous trouverez en pièce justificative l'analyse de risque, effectuée dans le cadre du Système de Gestion de la sécurité (SGS) qui a amené à conclure que le risque « sécurité de l'information » impactant les missions de sécurité *aérienne de l'organisme est limité au regard de l'exposition globale de l'organisme dans son activité quotidienne.*

Ainsi, je m'engage à :

- *Gérer le risque « sécurité de l'information » comme un risque à part entière dans le cadre du SGS relatif à ces activités et donc à intégrer la gestion de la cybersécurité dans la politique SGS et dans le manuel et les procédures SGS appropriées,*
- *Me conformer aux exigences en matière de comptes rendus d'incidents énoncées dans le règlement (UE) No 376/2014,*
- *Considérer les bonnes pratiques extraites du Guide d'hygiène informatique de l'ANSSI – Niveau Standard (Voir Annexe II)* pour l'élaboration du plan d'actions ou du plan de traitement des risques *résultant des analyses de risques « sécurité de l'information » impactant la sécurité aérienne,*
- *Appliquer les dispositions de l'IS.I/D.200 (a)(13) de la Partie-IS,*
- *Réévaluer périodiquement (à l'issue du cycle d'audit de surveillance ou à une fréquence au moins égale à la durée du cycle de surveillance interne) ou à la suite d'un changement de contexte majeur, l'analyse de risque pour vérifier que les conditions d'obtention de la dispense sont toujours vérifiées,*
- *Garder à disposition de l'Autorité les éléments de preuve qui ont amené à conclure que le risque impactant les missions de* sécurité *aérienne est limité au regard de l'exposition globale de l'organisme dans son activité quotidienne.*

A [lieu], le [date]

Signature du Dirigeant Responsable

[1] *Sélectionner les mentions applicables*

Annexe II – Mesures de sécurité des systèmes d'information

Le tableau ci-dessous résume les mesures de sécurité des systèmes d'information – **Niveau STANDARD** - à considérer pour l'élaboration du plan d'actions ou du plan de traitement des risques. Elles sont extraites du **Guide d'hygiène informatique**[2] publié par l'ANSSI et constituent le socle minimal de sécurité des systèmes d'information.

	Mesures de sécurité des systèmes d'information	Standard
1	Former les équipes opérationnelles à la sécurité des systèmes d'information	X
2	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique	X
3	Maîtriser les risques de l'infogérance (sous-traitance des tâches informatiques)	X
4	Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau	X
5	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour	X
6	Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs	X
7	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés	X
8	Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateurs/administrateurs	X
9	Attribuer les bons droits sur les ressources sensibles du système d'information	X
10	Définir et vérifier des règles de choix et de dimensionnement des mots de passe	X
11	Protéger les mots de passe stockés sur les systèmes	X
12	Changer les éléments d'authentification par défaut sur les équipements et services	X
13	Privilégier lorsque c'est possible une authentification forte	X
14	Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique	X
15	Se protéger des menaces relatives à l'utilisation de supports amovibles	X
16	Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité	X
17	Activer et configurer le pare-feu local des postes de travail	X
18	Chiffrer les données sensibles transmises par voie Internet	X
19	Segmenter le réseau et mettre en place un cloisonnement entre ces zones	X
20	S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages	X
21	Utiliser des protocoles sécurisés dès qu'ils existent	X
22	Mettre en place une passerelle d'accès sécurisé à Internet	X

[2] *https://cyber.gouv.fr/publications/guide-dhygiene-informatique*

	Mesures de sécurité des systèmes d'information	Standard
23	Cloisonner les services visibles depuis Internet du reste du système d'information	X
25	Sécuriser les interconnexions réseau dédiées avec les partenaires	X
26	Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques	X
27	Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système	X
28	Utiliser un réseau dédié et cloisonné pour l'administration du système d'information	X
29	Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail	X
30	Prendre des mesures de sécurisation physique des terminaux nomades	X
31	Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable	X
32	Sécuriser la connexion réseau des postes utilisés en situation de nomadisme	X
33	Adopter des politiques de sécurité dédiées aux terminaux mobiles	X
34	Définir une politique de mise à jour des composants du système d'information	X
35	Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles	X
36	Activer et configurer les journaux des composants les plus importants	X
37	Définir et appliquer une politique de sauvegarde des composants critiques	X
~~**38**~~	~~Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives~~	~~**Sans objet**~~
39	Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel	X
40	Définir une procédure de gestion des incidents de sécurité	X