TLP:GREEN

CADRE DE CONFORMITE CYBER FRANCE

VERSION 2

Réglement d'éxécution (UE) 2015/1998
Réglement d'éxécution (UE) 2022/1645
Réglement d'éxécution (UE) 2023/203

Direction de la sécurité de l'aviation civile
Direction de programme cybersécurité
Version n° 2.0 du 30 avril 2024

Table des matières

Information

Ce document, établi par la direction de la sécurité de l'aviation civile (DSAC), présente le Cadre de Conformité Cyber France (3CF) pour l'aviation civile. Ce document, marqué **TLP:GREEN** peut donc être utilisé librement au sein de la communauté du transport aérien, sans pour autant être diffuser publiquement et sous réserve de mentionner sa paternité (source et date de la dernière mise à jour).

Pour tout commentaire ou suggestion à propos du Cadre de Conformité Cyber France (3CF), veuillez contacter la direction de programme cybersécurité de la DSAC à une des adresses suivantes :

- anne.frisch@aviation-civile.gouv.fr ;
- pierre.abdoulhadi@aviation-civile.gouv.fr.

Historique des révisions

Version	Date	Modifications
Version intermédiaire	30 juin 2021	Création du document
Version 1	3 Sept. 2021	Modifications : - § 1. Introduction - § 2. Démarche d'accompagnement - § 4.1.4. Personnels et compétence - § 5.4.4.1. Sources des non-conformités - Annexe 3 : Grille de conformité réglementaire Ajouts : - § 5.1.3. Formation - Annexe 2 : Niveaux de conformité et dispositions du 3CF
Version 2	30 avril 2024	Refonte du document afin d'y intégrer les AMC du règlement Part IS

1. Introduction

1.1. Objectif du document

Ce document propose un référentiel unique de dispositions visant à accompagner les organismes à se conformer au :

- règlement d'exécution (UE) 2015/1998 [1] modifié par le règlement d'exécution (UE) 2019/1583 de la commission du 25 septembre 2019 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile, en ce qui concerne les mesures de cybersécurité ; et/ou ;
- dispositif Part-IS :
    - Règlement délégué (UE) 2022/1645 [2] de la commission du 14 juillet 2022 portant 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 [3] de la commission du 27 octobre 2022 portant 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

1.2. Champ d'application

1.2.1. Opérateurs détenant un agrément de sûreté

Le présent document s'adresse aux **exploitants d'aérodrome** et aux **transporteurs aérien** soumis au règlement d'exécution (UE) n°2015/1998 [1].

1.2.2. Organismes détenant un agrément ou un certificat de sécurité

Le présent document s'adresse aux organismes visés par :

- les sous-sections G et J, de la section A de l'annexe I (*Part 21*) du règlement (UE) n°748/2012 [4] , à savoir ceux détenant :
    - **un agrément d'organisme de production** (*POA*) et/ou ;
    - **un agrément d'organisme de conception** (*DOA*).
- la section A de l'annexe II (Part-145) et la section A de l'annexe V (Part-CAMO) du règlement (UE) n°1321/2014 [5] , à savoir :
    - **les ateliers de maintenance** *(Part-145)*, et ;
    - **les organismes de gestion du maintien de la navigabilité** (Part-*CAMO*).
- l'annexe III (*Part-ORO*) du règlement (UE) n°965/2012 [6] , incluant :
    - **les compagnies aériennes** disposant d'un certificat de transporteur aérien.
- l'annexe VII (*Part-ORA*) du règlement (UE) n°1178/2011 [7] , à savoir :
    - **les organismes de formation des personnels de bord**, et;
    - **les centres aéro-médicaux des personnels de bord**, et ;
    - **les opérateurs de *Flight Simulation Training Devices*** (*FSTD*).
- l'annexe III (*Part ATCO.OR*) du règlement (UE) n°2015/340 [8] , à savoir :
    - **les centres de formation des contrôleurs aérien**, et ;
    - **les centres aéro-médicaux des contrôleurs aérien**.
- l'annexe III (*Part-ATM/ANS.OR*) du règlement (UE) n°2017/373 [9] , à savoir :
    - **les prestataires de service de navigation aérienne** détenant un certificat.
- l'annexe III (*Part-ADR.OR*) du règlement (UE) n°139/2014 [10] , à savoir :
    - **les exploitants d'aérodromes** détenant un certificat européen ;
    - **les prestataires de services de gestion d'aire de trafic**.
- Le règlement d'exécution (UE) 2021/664 [11], à savoir :
    - **les prestataires de services *U-space*** (*USSP*).

1.2.3. Exemption

Le présent document ne s'adresse pas

- Aux organismes de conception et de production qui sont uniquement associés à la conception et/ou à la production d'aéronefs ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) no 748/2012 [4] ;
- Aux transporteurs aériens qui participent exclusivement à l'exploitation de l'un des éléments suivants :
    - un aéronef ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) no 748/2012 [4] ;
    - des avions monomoteurs à hélice dont la configuration maximale opérationnelle en sièges passagers est inférieure ou égale à 5 et qui ne sont pas classés comme aéronefs motorisés complexes, lorsqu'ils décollent et atterrissent sur le même aérodrome ou site d'exploitation et qu'ils sont exploités selon les règles de vol à vue (VFR) de jour ;
    - des hélicoptères monomoteurs dont la configuration maximale opérationnelle en sièges passagers est inférieure ou égale à 5 et qui ne sont pas classés comme aéronefs motorisés complexes, lorsqu'ils décollent et atterrissent sur le même aérodrome ou site d'exploitation et qu'ils sont exploités en VFR de jour.
- aux organismes de formation agréés (ATO) qui participent uniquement :
    - aux activités de formation pour les aéronefs ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) no 748/2012 [4] ;
    - à la formation théorique.
- aux exploitants de simulateurs d'entraînement au vol (FSTD) qui participent uniquement à l'exploitation de FSTD pour les aéronefs ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) no 748/2012 [4] ;
- aux prestataires de services de navigation aérienne titulaires d'un certificat limité conformément au point ATM/ANS.OR.A.010 de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) 2017/373 [9] ;
- aux prestataires de services d'information de vol déclarant leurs activités conformément au point ATM/ANS.OR.A.015 de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) 2017/373 [9].

1.2.4. Dérogation

Dans cette version, le document ne s'adresse pas aux organismes disposant d'une autorisation d'application adaptée de la Part-IS au titre de l'IS.OR200 (e). Le cadre de cette dérogation d'application de la Part IS sera précisé par la DSAC au travers d'une communication METEOR à venir.

A date, elle ne concerne que les SPO/NCC.

1.3. Alignement avec d'autres dispositifs réglementaires

Concernant les organismes devant se mettre en conformité avec d'autres dispositifs réglementaires tels que :

- La loi de Programmation militaire [12] ;
- La transposition de la directive NIS v1 [13].

Ces derniers peuvent faire valoir les dispositions d'équivalence prévues par le règlement (UE) n°2015/1998 [1] et les règlements (UE) 2022/1645 [3] et 2023/203 [2] mais uniquement pour les données et systèmes relevant de la sûreté et/ou de la sécurité aérienne qui sont également :

- des systèmes d'information d'importance vitale (SIIV) ou tels que définis par le code de la défense ;
- des réseaux et systèmes d'information essentiels (SIE) tels que définis par la directive européenne de 2016 dite « NIS ».

Concernant la transposition de la directive NIS 2, la DSAC est dans l'attente de la présentation du dispositif par l'ANSSI pour se prononcer.

2. Présentation générale du document

2.1. Référentiel unique

Considérant la multiplicité des règlements, la redondance de certaines exigences et les contraintes en ressources humaines et financières, accentuées par la crise actuelle, ce document vise à fournir aux opérateurs un Cadre de Conformité de Cybersécurité France (3CF). Celui-ci a comme objectif de rationaliser les différentes dispositions réglementaires propres à l'aviation civile, applicables en France, afin de faciliter leurs mises en œuvre, au moyen d'un référentiel unique (3CF).

Le 3CF vise donc :

- à permettre la conformité :
  - au règlement (UE) n°2015/1998 [1] portant sur la sécurité de l'information pouvant affecter la sûreté aérienne ;
  - au dispositif Part-IS [2,3] portant sur la sécurité de l'information pouvant affecter la sécurité aérienne.
- à assurer la cohérence, sans en garantir la conformité, avec les dispositions nationales telles que :
  - l'arrêté sectoriel « transport aérien » [12] issu de l'article 22 de la loi de programmation militaire ;
  - le décret et les arrêtés [13]; issus de la loi de transposition de la directive *Network Information Security.*

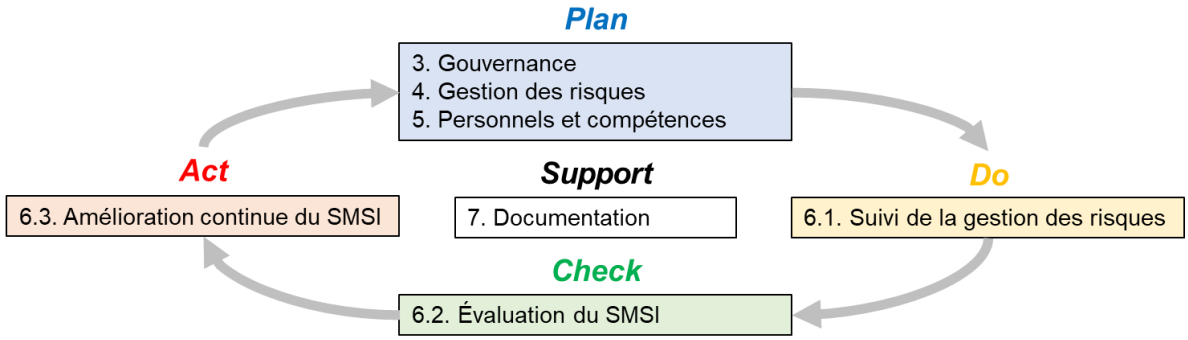
Par ailleurs, il est inspiré des bonnes pratiques telles que :

- la norme ISO 27001 [14]relative au système de management de la sécurité de l'information ;
- les guides et méthodes de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[1] ;
- les travaux menés par l'EUROCAE.

En effet, bien que les différents dispositifs réglementaires ne concernent pas les mêmes domaines du transport aérien : protection de la nation, économie, sûreté de l'aviation civile ou sécurité de l'aviation civile ; ceux-ci s'appuient sur des principes et méthodes transverses dans un objectif de sécurité de l'information. Le référentiel unique (3CF) se veut donc un outil de rationalisation des exigences.

2.2. Structure

Dans l'optique de la mise en œuvre d'un système de management de la sécurité de l'information, les chapitres du document sont à lire en ce sens :



2.3. Utilisation

Pour les organismes devant se mettre en conformité conformer :

- avec les deux règlements, l'ensemble du document est à considérer et le périmètre d'application couvre la sûreté et la sécurité aérienne ;
- uniquement avec un des règlements du dispositif Part-IS [2,3], l'ensemble du document est à considérer et le périmètre d'application couvre uniquement la sécurité aérienne ;
- uniquement avec le règlement (UE) n°2015/1998 [1], les dispositions prévues par les chapitre §4.1, §4.2, §4.3, §4.4.4, §4.5.1.1, §5. et §6.1 sont à considérer et le périmètre d'application couvre uniquement la sûreté aérienne.

Pour chaque disposition, un encart rappelle le domaine pour lequel elle s'applique : **Part-IS**, **RUE 2015/1998** et **les deux.**

La matrice de conformité précisant les dispositions du document s'appliquant selon les cas, ainsi que les définitions des principaux termes utilisés sont précisées en annexe.

[1] Publications de l'ANSSI

3. Gouvernance

3.1. Engagement du Dirigeant Responsable

Sécurité aérienne

Le Dirigeant Responsable de l'organisme s'engage à mettre en œuvre des moyens adaptés de protection contre l'atteinte à la confidentialité, l'intégrité, la disponibilité et l'authenticité des informations qui pourraient entrainer des problèmes de sécurité aérienne.

Pour ce faire, le Dirigeant Responsable s'engage à mettre en place un Système de Management de la Sécurité de l'Information (SMSI) visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la gestion des risques liés à la sécurité de l'information sur la sûreté et ou sécurité aérienne.

La lettre formalisant cet engagement du Dirigeant Responsable est intégrée ou référencée dans :
- le manuel du système de management de la sécurité de l'information, ou ;
- le manuel de l'organisme approuvé/certifié.

3.2. Politique de sécurité de l'information

3.2.1. Stratégie et objectifs de sécurité de l'information

Sécurité aérienne

Le Dirigeant Responsable définit et approuve une politique de sécurité de l'information dont découle :
- une stratégie qui décrit les intentions et l'orientation en matière de sécurité de l'information relative à la sécurité aérienne ;
- les objectifs de sécurité de l'information qu'il s'est fixé afin de mettre en œuvre cette stratégie ;
- les étapes et le plan d'actions pour atteindre ces objectifs.

3.2.2. Cohérence de la stratégie et des objectifs

Sécurité aérienne

Le Dirigeant Responsable s'assure de la cohérence entre :
- la stratégie et les objectifs de sécurité de l'information d'une part et ;
- la stratégie et les objectifs globaux de l'organisme et ceux plus spécifiques à la sécurité aérienne d'autre part.

3.2.3. Intégration ou articulation entre les systèmes de gestion

Sécurité aérienne

Le Dirigeant Responsable précise l'intégration ou l'articulation entre le SMSI et le(s) système(s) de gestion existant(s) de l'organisation. Notamment :
- le Système de Gestion de la Sécurité aérienne (SGS ou en anglais SMS Safety Management System) ;
- le cas échéant d'autres Systèmes de Management de la Sécurité de l'Information, en interaction avec le SMSI aéronautique objet de ce document, tel qu'un SMSI mutualisé au sein d'un groupe de sociétés, répondant à d'autres objectifs réglementaires, et/ou internes et/ou économiques.

3.2.4. Communication de la politique de sécurité de l'information

Sécurité aérienne

Le Dirigeant Responsable s'assure que la politique de sécurité de l'information est :
- diffusée et promue de manière appropriée :
  - au sein de son organisation ;
  - auprès de ses partenaires, notamment ses sous-traitants, ses prestataires de services et ses fournisseurs d'équipement.
- formalisée et intégrée ou référencée dans :
  - le manuel du système de management de la sécurité de l'information, ou ;
  - le manuel de l'organisme approuvé/certifié.

3.3. Gestion des ressources, rôles et responsabilités

Sécurité aérienne

Le Dirigeant Responsable :
- est capable de démontrer sa connaissance du règlement Part-IS ;
- s'assure que les ressources financières, matérielles et humaines nécessaires pour assurer la gestion des risques liés à la sécurité de l'information relative à la sécurité aérienne sont disponibles et suffisantes ;
- définit et attribue les rôles et les responsabilités en matière de gestion de l'information relative à la sécurité aérienne. Notamment, il veille à :
    - désigner une personne ou un groupe de personnes responsables :
        - de la mise en œuvre du règlement Part-IS, qui :
            - a un accès direct au Dirigeant Responsable ;
            - dispose de l'autorité et des compétences suffisantes pour exercer ses fonctions et ;
            - pour lequel une ou des personnes assurant l'intérim sont prévues en cas d'absence.
        - de la conformité au règlement Part-IS, qui :
            - est indépendant vis-à-vis de la personne ou du groupe de personnes responsables de la mise en œuvre du règlement Part-IS.
    - formaliser la désignation de ces personnes ou groupes de personnes, en précisant :
        - leur(s) titre(s), leur(s) nom(s) et leurs missions ;
        - leur lien direct avec le Dirigeant Responsable, leurs responsabilités, leurs pouvoirs et leurs moyens, au travers d'un organigramme ;
        - leurs obligations de rendre compte.
- s'assure que les rôles et responsabilités sont communiqués et connus à tous les niveaux de l'organisation, aussi bien par le personnel interne que par les partenaires extérieurs concernés.

Les éléments relatifs à la gestion des ressources, aux rôles et responsabilités sont :
- formalisés ;
- intégrés ou référencés dans :
    - le manuel du système de management de la sécurité de l'information, ou ;
    - le manuel de l'organisme approuvé/certifié.

4. Gestion des risques de sécurité de l'information

Sécurité et sûreté aérienne

Dans le cadre des activités de la gestion des risques de sécurité de l'information relative à la sûreté et/ou à la sécurité aérienne, l'organisme :

- définit les responsabilités des différents participants internes et externes ;
- définit l'articulation avec l'organisation déjà en place pour la gestion des risques relatifs à la sûreté et/ou à la sécurité aérienne ;
- précise la méthodologie ou le standard utilisée pour mener à bien ces activités :
    - Il est recommandé de mettre en œuvre une des normes ou méthodes suivantes :
        - ISO/CEI 27005 [15], Norme relative à la Gestion des risques liés à la sécurité de l'information ;
        - EBIOS Risk Manager [16] méthode d'appréciation et de traitement des risques numériques publiée par l'ANSSI ;
        - toute autre méthode conforme à la norme ISO/CEI 31000 [17], norme relative à la gestion des risques.
    - Dans le cas où l'organisme met en œuvre une autre méthodologie ou standard, il apporte la preuve que celle ou celui-ci :
        - produit des résultats :
            - reproductibles sur la base d'éléments d'entrée similaires ;
            - comparables dans le temps.
        - prend en considération des éléments d'entrée pertinents et valides ;
        - permet un affinement des résultats itératifs au fil du temps et des éléments d'entrée disponibles.
- formalise les procédures relatives à la gestion des risques, notamment à :
    - l'appréciation et au traitement des risques ;
    - la gestion des incidents de sécurité de l'information ;
    - la gestion des organismes en interface ;
    - la gestion des sous-traitants réalisant une ou des activités du SMSI.
- intègre ou fait référence à ces procédures dans :
    - le manuel du système de management de la sécurité de l'information, ou ;
    - le manuel de l'organisme approuvé/certifié, et/ou ;
    - le programme de sûreté.

Pour la suite, l'organisme s'appuie sur la méthodologie de gestion des risques qu'il a choisie pour aboutir aux conclusions. Néanmoins, sont précisées ci-après les différentes étapes et documents attendus pour être conformes aux règlements.

4.1. Établissement du contexte

Sécurité et sûreté aérienne

Afin de définir le périmètre de son analyse de risques et/ou de son SMSI, l'organisme identifie la liste des fonctions relatives à ses missions de sûreté et/ou de sécurité aérienne. Pour y parvenir, il peut s'appuyer sur :

- les listes de fonctions relatives à la sûreté et/ou sécurité aérienne disponibles en annexe[2] ;
- une pré-évaluation des risques qui identifie les fonctions les plus critiques à prendre en compte au regard de la distance et de la vraisemblance de propagation jusqu'à l'impact sur la sûreté et/ou sécurité aérienne dont on cherche à se prémunir[3].

De plus, l'organisme définit des échelles :

- de gravité relative aux conséquences en matière de sûreté et/ou de sécurité aérienne[4] ;
- de probabilité d'occurrence (ou vraisemblance) du risque ;
- les critères d'acceptation du risque propre à l'organisme[5].

[2] Les annexes ne sont pas encore définies et devraient être publiées en 2024
[3] *White paper: Identification and Classification guidance for Part-IS assets* [18]
[4] L'organisme peut s'appuyer sur les exemples suivants :
- Guide méthode EBIOS Risk Manager [16] – page 26
- ICAO Doc 9859 Safety Risk Tolerability [19]
- ICAO Doc 10108 Aviation Security Global Risk Statement [20]

[5] L'organisme peut s'appuyer sur les exemples suivants :
- Guide méthode EBIOS Risk Manager [16] – page 73
- ICAO Doc 9859 Safety Risk Tolerability [19]

4.2. Appréciation des risques

4.2.1. Identification des risques

Sécurité et sûreté aérienne

Sur la base de la liste des fonctions relatives à la sûreté et/ou sécurité aérienne de l'organisation, l'organisme identifie :

- les fonctions :
  - dont il a la responsabilité et qui sont réalisées par lui-même et pour son propre compte et/ou ;
  - qu'il met en œuvre pour le compte d'un partenaire extérieur *(interface)* et/ou;
  - dont il a la responsabilité et qui sont réalisées par un partenaire extérieur pour le compte de l'organisme considéré *(interface)*.
- les éléments qui contribuent à la réalisation de chacune des fonctions identifiées précédemment, notamment les équipements, systèmes, données et informations.

Puis, pour chaque fonction et chaque élément identifiés précédemment, l'organisme :

- associe une description ;
- identifie une ou des personnes et/ou entités responsables, qui peuvent aussi bien être internes qu'externes ;
- précise le cas échéant si celui-ci dispose d'une interface avec un tiers ainsi que la nature de cette dernière :
  - prestation de service ;
  - sous-traitance ;
  - fourniture d'équipements ;
  - prestation autre, à préciser.

L'organisme dispose d'une interface avec un autre organisme, lorsque la réalisation d'une des fonctions nécessite :

- *d'échanger des données et/ou des informations avec ce tiers ;*
- *de fournir et/ou de mettre à disposition un système, un équipement et/ou un service numérique pour ce tiers ;*
- *d'utiliser un système d'information, un équipement et/ou un service numérique fourni par ce tiers.*

Enfin, l'organisme :

- détermine pour chaque fonction identifiée, seul ou en lien avec le ou les organismes en interface concernés :
  - les événements redoutés, notamment les effets néfastes sur la sûreté et/ou sécurité aérienne consécutifs à une atteinte à la disponibilité, l'intégrité, la confidentialité et l'authenticité de la fonction ;
  - les impacts en matière de sûreté et/ou de sécurité aérienne associés à ces événements redoutés.
- établit la liste des organismes en interface précédemment identifiés.

4.2.2. Analyse de risques

Sécurité et sûreté aérienne

Ensuite, l'organisme :

- définit une échelle de vraisemblance (ou de probabilité d'occurrence) prenant en compte :
  - la vraisemblance de réalisation de l'événement redouté au niveau de l'élément du ou des systèmes d'information concerné(s) ;
  - l'efficacité des processus métier de sûreté et/ou sécurité aérienne mis en place au sein de l'organisme et pouvant bloquer, limiter ou favoriser la réalisation de l'événement redouté. *Par exemple, les barrières de protection déjà mises en place vis-à-vis de l'événement redouté*.
- identifie ses risques sur la base de l'analyse d'impacts en associant aux évènements redoutés :
  - un niveau de gravité selon l'échelle prédéfinie ;
  - un niveau de vraisemblance selon l'échelle prédéfinie ;
  - une ou des personnes et/ou entités responsables qui peuvent être au sein de l'organisme ou bien un partenaire extérieur, notamment pour les fonctions qu'il reçoit.

4.2.3. Évaluation des risques

Sécurité et sûreté aérienne

Enfin, l'organisme :

- associe à chaque risque identifié son niveau de risque selon l'échelle prédéfinie sur la base :
  - des résultats de son analyse de risques ;
  - des informations d'analyse de risques transmises dans le cadre d'une fonction réalisée par un tiers.
- établit la liste des organismes en interface présentant un risque pour la sûreté et/ou la sécurité aérienne.

4.2.4. Résultats de l'appréciation des risques

Sécurité et sûreté aérienne

L'organisme :
- formalise :
  - la liste des risques relatifs à la sûreté et/ou à la sécurité aérienne identifiés en précisant pour chacun d'entre eux :
    - la fonction associée et la ou les éventuelles interfaces ;
    - les équipements, systèmes, données et informations qui contribuent à la réalisation de la fonction associée ainsi que la ou les éventuelles interfaces ;
    - l'événement redouté associé ;
    - une ou des personnes et/ou entités responsables ;
    - le niveau de risque.
  - la liste des organismes en interface présentant un risque pour la sûreté et/ou la sécurité aérienne ;
  - le cas échéant, la liste des systèmes d'information critiques au regard de la sûreté.
- fait approuver la liste des risques relatifs à la sûreté et/ou la sécurité aérienne identifiés par son Dirigeant Responsable et/ou ses responsables des risques identifiés selon son organisation de gestion des risques ;
- conserve des informations documentées comme preuves des résultats d'appréciation des risques.

4.3. Traitement des risques

4.3.1. Mesures pour le traitement du risque

Sécurité et sûreté aérienne

Sur la base des résultats de l'appréciation des risques, l'organisme :
- définit et justifie pour chacun des risques relatifs à la sûreté et/ou à la sécurité aérienne s'il :
  - maintient le risque à condition qu'il soit acceptable en l'état ;
  - réduit le niveau de risque par l'introduction, la suppression ou la modification des mesures de sécurité de l'information ;
  - refuse le risque en évitant l'activité ou la situation qui donne lieu à un risque ;
  - partage le risque avec une autre partie capable de gérer de manière plus efficace le risque.
- détermine la ou les mesures permettant de traiter le risque conformément à l'action choisie et s'assure que celle ou celles-ci n'entrainent pas de nouveaux risques ;
- met en œuvre en temps utile et vérifie l'efficacité de ces mesures conformément aux §6.1. et §6.2.3.

Pour définir les mesures de sécurité de l'information, l'organisme peut notamment s'appuyer sur les référentiels suivants :
- Guide d'hygiène informatique de l'ANSSI [21] ;
- Norme internationale ISO/IEC 27002:2022 [22] ;
- Norme internationale ISO/ISA/IEC 62443 [23].

4.3.2. Élaboration du plan de traitement des risques

Sécurité et sûreté aérienne

L'organisme élabore un plan de traitement des risques relatifs à la sûreté et/ou à la sécurité aérienne permettant d'identifier pour chaque mesure de sécurité de l'information déterminée *supra :*
- le ou les risques qu'elle traite ;
- la priorité de mise en œuvre;
- le délai de mise en œuvre recommandé ;
- le cas échéant, les raisons ne permettant pas de les mettre en œuvre.

4.3.3. Évaluation des risques résiduels

Sécurité et sûreté aérienne

L'organisme évalue les risques résiduels, après l'application des mesures de sécurité de l'information définies dans le plan de traitement des risques. Si un risque résiduel demeure non acceptable, l'organisme le traite à nouveau, conformément au §4.3.1, jusqu'à ce que celui-ci soit acceptable.

4.3.4. Résultats du traitement des risques

Sécurité et sûreté aérienne

L'organisme :
- formalise :
  - le plan de traitement des risques relatifs à la sûreté et/ou à la sécurité aérienne ;
  - la liste des risques résiduels après application du plan de traitement des risques relatifs à la sûreté et/ou à la sécurité aérienne.
- fait approuver ces documents par le Dirigeant Responsable et/ou la (ou les) personne()s et/ou entité(s) responsable(s) des risques selon son organisation de gestion des risques ;
- conserve des informations documentées comme preuves des résultats d'appréciation des risques.

4.4. Gestion des incidents de sécurité de l'information

Sécurité et sûreté aérienne

L'organisme définit et met en œuvre des mesures techniques et organisationnelles visant à :
- détecter les types d'incidents de sécurité de l'information et identifier ceux ayant un potentiel impact sur la sûreté et /ou la sécurité aérienne ;
- réagir à la suite d'un incident de sécurité de l'information ayant un potentiel impact sur la sûreté et /ou la sécurité aérienne détecté ;
- se rétablir à la suite d'un incident de sécurité de l'information ayant un potentiel impact sur la sûreté et /ou la sécurité aérienne.

Pour y parvenir, l'organisme peut s'appuyer, par exemple sur :
- les guides et bonnes pratiques publiés par l'ANSSI ;
- les mesures précisées dans la norme ISO/CEI 27002 [22].

Sécurité aérienne

De plus dans le cadre de la gestion des incidents de sécurité de l'information relatifs à la sécurité aérienne, l'organisme prend en compte les dispositions précisées ci-après.

4.4.1. Détection des incidents de sécurité de l'information

4.4.1.1. Identification des incidents redoutés de sécurité de l'information

Sécurité aérienne

L'organisme identifie la liste des types d'incidents redoutés de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne et des impacts et conséquences associés sur la base des résultats de l'appréciation et du traitement des risques réalisés au §4.2. et §4.3.

L'organisme peut également s'appuyer sur un ou plusieurs référentiels, tels que :
- *Prestataires de détection des incidents de sécurité, sécurité - Référentiel d'exigences [24] - IV.2.1. b) ;*
- *5 standards sur la détection des incidents de sécurité [25] ;*
- *Annexe B de la norme internationale ISO/IEC 27035:2022 [26] ;*
- *ED Decision 2023/009/R - Appendix I — Examples of threat scenarios with a potential harmful impact on safety [27].*

4.4.1.2. Collecte des événements

4.4.1.2.1. Stratégie de collecte

Sécurité aérienne

Sur la base des incidents redoutés de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne, l'organisme :
- identifie les sources de collecte pertinentes au sein de son système d'information ;
- met en place une veille sur les vulnérabilités pouvant affecter son système d'information ;
- journalise les événements pertinents à la détection parmi les sources de collecte identifiées et la veille sur les vulnérabilités.

Pour y parvenir, l'organisme peut s'appuyer sur :
- *les sections IV.2.2. c) & d) du référentiel d'exigences - Prestataires de détection des incidents de sécurité [24] ;*
- *sur l'annexe A des Recommandations de sécurité pour la mise en œuvre d'un système de journalisation [28].*

4.4.1.2.2. Notification interne d'événements

Sécurité aérienne

L'organisme :
- met en place une procédure de collecte des événements qui peuvent lui être notifiés et qui satisfait aux exigences du règlement (UE) 376/2014 [29] ;
- en précise le fonctionnement, notamment :
  - les événements qui doivent être notifiés, à savoir les événements de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne ;
  - les moyens mis à disposition pour notifier un événement ;
  - les délais de notification ;
  - les conditions d'archivage, notamment au moins 5 ans.
- rend cette procédure et les moyens de notification associés accessibles aux personnes ayant besoin d'en connaitre parmi :
  - son personnel interne ;
  - les tiers pertinents dans le contexte, identifiés au §4.2.4 ;
  - tous les interlocuteurs pertinents.

L'organisme :
- peut intégrer ce système de notification interne d'événements à un système existant ;
- formalise la description de ce système et l'intègre ou y fait référence dans :
  - le manuel du système de management de la sécurité de l'information, ou ;
  - le manuel de l'organisme approuvé/certifié.

4.4.1.3. Stratégie de détection

Sécurité aérienne

L'organisme met en place une stratégie de détection qui permet de détecter les incidents redoutés de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne sur la base des sources de collecte précédentes. Aussi, l'organisme :
- définit :
  - une classification par ordre de gravité des incidents redoutés de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne ;
  - des règles de détection en :
    - s'appuyant sur :
      - la liste des incidents de sécurité redoutés de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne ;
      - des bases de connaissances acquises auprès des partenaires extérieurs ;
      - des bases de connaissances internes (audits, tests de vulnérabilités et d'intrusion) ;
      - une veille sur la menace et les vulnérabilités ;
      - l'identification d'écart de bon fonctionnement par rapport au comportement à détecter ;
      - les impacts sur les performances ;
      - les incidents de sécurité de l'information connus auprès d'autres organismes.
    - en précisant pour chaque règle :
      - les moyens mis en œuvre ;
      - une description ;
      - Le ou les incidents redoutés associés ;
      - Le niveau de gravité.
- assure la centralisation et la corrélation des événements et des vulnérabilités remontées ;
- identifie les événements ou combinaison d'évènements pouvant mener à un incident ayant un potentiel impact sur la sécurité aérienne.

4.4.1.4. Qualification

Sécurité aérienne

Lorsqu'un évènement pouvant mener à un incident de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne est détecté, l'organisme le qualifie en incident de sécurité de l'information, notamment il :

- en détermine la véracité afin d'éliminer les faux positifs ;
- identifie les équipements, systèmes, données et informations concernés par l'incident détecté ;
- identifie les conséquences en matière de sécurité aérienne et en détermine :
  - les impacts et la gravité de l'incident détecté ;
  - les causes de l'incident.
- identifie les éventuelles parties prenantes en interne et/ou les partenaires extérieurs concernés par l'incident ;
- formalise la qualification de la détection ;
- conserve des informations documentées au moins jusqu'à la prochaine qualification.

4.4.1.5. Notification

Sécurité aérienne

Pour chaque événement qualifié en incident de sécurité, l'organisme notifie :

- les personnes pertinentes au sein de son organisation pour activer les réactions appropriées ;
- le cas échéant :
  - les partenaires externes concernés selon le cadre défini au §4.5.1;
  - l'autorité selon le cadre défini au §4.4.5.

4.4.2. Réponse aux incidents de sécurité de l'information

Sécurité aérienne

L'organisme définit un mécanisme de réponse à incident qui :

- précise :
  - les rôles et les responsabilités des personnes qui activent les réactions en cas d'incident qualifié ;
  - les modalités d'information de ces personnes à la suite de la qualification d'un incident, notamment les outils et les délais.
- définit les actions immédiates à mettre en œuvre, notamment en identifiant pour chaque type d'incident redouté relatifs à la sécurité aérienne :
  - les ressources à activer au sein de l'entreprise et à l'extérieur de l'entreprise, notamment dans le cadre d'un contrat avec un Prestataire de Réponse à Incident de Sécurité (PRIS) ou de l'adhésion à un CERT ;
  - les mesures organisationnelles et techniques pouvant être mises en œuvre pour limiter la propagation d'une attaque et éviter la matérialisation du ou des incidents redoutés. Ce référentiel de mesures est tenu à jour en fonction de l'évolution du contexte ;
  - les délais de mise en œuvre de ces mesures.
- met en place une surveillance des équipements, systèmes, données et informations de son système d'information associés à l'incident détecté, et met à jour si nécessaire ce périmètre à surveiller.

4.4.3. Remédiation

Sécurité aérienne

L'organisme définit des plans de remédiation à actionner en cas d'incident, qui :

- précise les rôles et les responsabilités des personnes qui gèrent les actions de remédiation ;
- définit un ou des plans de remédiation pour chaque type d'incident redouté relatifs à la sécurité aérienne qui :
  - identifie les ressources à activer au sein de l'organisme et à l'extérieur de l'entreprise si applicable, notamment dans le cadre d'un contrat avec un Prestataire de Réponse à Incident de Sécurité (PRIS) ou de l'adhésion à un CERT ;
  - précise les actions à mettre en œuvre pour :
    - identifier le périmètre du système d'information impacté ;
    - réaliser la remédiation du système d'information impacté ;
    - s'assurer que le système d'information a retrouvé un état sûr et peut être remis en service.
  - prévoit la détermination des délais de remise en service en fonction du niveau de gravité, de la nature et du contexte de l'incident.
- produit un rapport d'incident qui sera communiqué à l'autorité selon les modalités définies au §4.4.5.

4.4.4.Résultat de la gestion des incidents de sécurité de l'information

Sécurité et sûreté aérienne

L'organisme formalise la liste des mesures techniques et organisationnelles visant à :

- détecter les incidents de sécurité de l'information ayant un potentiel impact sur la sûreté et /ou la sécurité aérienne ;
- réagir à la suite d'une incident de sécurité de l'information ayant un potentiel impact sur la sûreté et /ou la sécurité aérienne détecté ;
- se rétablir à la suite d'un incident de sécurité de l'information ayant un potentiel impact sur la sûreté et /ou la sécurité aérienne.

Sécurité aérienne

De plus dans le cadre de la gestion des incidents de sécurité relatifs à la sécurité aérienne, l'organisme formalise :

- la liste des incidents redoutés relatifs à la sécurité aérienne;
- la liste des sources de collecte, le système de veille des vulnérabilités et les événements journalisés ;
- la liste des règles de détection mises en œuvre ;
- les actions immédiates à mettre en œuvre pour chaque type d'incident redouté relatifs à la sécurité aérienne ;
- les plans de remédiation.

Enfin l'organisme conserve des informations documentées appropriées comme preuves de la gestion des incidents de sécurité de l'information.

4.4.5.Notification à l'autorité

A paraitre dans la prochaine version du 3CFv2

4.5. Gestions des risques induits par les tiers

4.5.1. Organismes en interface

4.5.1.1. Organismes présentant un risque pour la sûreté aérienne

Sûreté aérienne

Sur la base de la liste des organismes en interface présentant un risque pour la sûreté aérienne établie au §4.2, l'organisme définit un cadre de travail avec ces derniers qui :

- prévoit des règles d'échange d'information visant à préserver l'authenticité, la confidentialité et l'intégrité des informations échangées ainsi que l'anonymat des interlocuteurs s'ils le souhaitent ;
- précise les exigences à leur faire appliquer. Elles sont d'ordre :
  - règlementaire, notamment celles en matière de :
    - vérification des antécédents ;
    - sensibilisation et de formation à la sécurité de l'information.
  - contractuel, notamment :
    - la mise en œuvre de mesures de sécurité de l'information définies par l'organisme[6] ;
    - une surveillance adaptée au contexte des activités du tiers.

L'organisme conserve des informations documentées comme preuves de la gestion des organismes en interface présentant un risque pour la sûreté aérienne.

4.5.1.2. Organismes présentant un risque pour la sécurité aérienne

4.5.1.2.1. Organismes en interface détenant un agrément ou un certificat de sécurité

Sécurité aérienne

Sur la base de la liste des organismes en interface présentant un risque pour la sécurité aérienne établie au §4.2.4, l'organisme :

- identifie les tiers présentant un risque pour la sécurité aérienne et devant être conformes aux règlements Part-IS, appelées aussi contractants ;
- définit un cadre de travail avec ces derniers, qui prévoit :
  - la définition des responsabilités pour la gestion des risques partagés ;
  - un partage des hypothèses et des objectifs de sécurité sur les périmètres concernés ;
  - la notification des événements de sécurité de l'information et des vulnérabilités ayant un potentiel impact sur la sécurité aérienne conformément au §4.4.1.2.2 ;
  - des règles d'échange d'information visant à préserver l'authenticité, la confidentialité et l'intégrité des informations échangées ainsi que l'anonymat des interlocuteurs s'ils le souhaitent.

L'organisme conserve des informations documentées comme preuves de la gestion des organismes agréés ou certifiés en interfaces présentant un risque pour la sécurité aérienne.

4.5.1.2.2. Organismes en interface ne détenant pas d'agrément ou de certificat de sécurité

Sécurité aérienne

Sur la base de la liste des organismes en interface présentant un risque pour la sécurité aérienne établie au §4.2.4, l'organisme :

- identifie les tiers présentant un risque pour la sécurité aérienne et n'ayant pas d'obligation d'être conformes aux règlements Part-IS ;
- définit :
  - Lorsque cela est possible, un cadre de travail avec ces derniers qui prévoit :
    - la notification d'événements de sécurité de l'information et de vulnérabilité ayant un potentiel impact sur la sécurité aérienne conformément au §4.4.1.2.2 ;
    - des règles d'échange d'information visant à préserver l'authenticité, la confidentialité et l'intégrité des informations échangées ainsi que l'anonymat des interlocuteurs s'ils le souhaitent ;
    - la mise en œuvre de mesures de sécurité de l'information définies par l'organisme[7] ainsi qu'une surveillance adaptée au contexte des activités du tiers ;
    - Le cas échéant, un contrôle de la fiabilité du personnel conformément à la politique de contrôle de la fiabilité définie par l'organisme (§5.2).
  - Sinon, l'organisme traite ce risque dans le cadre du §4.3.

L'organisme conserve des informations documentées comme preuves de la gestion des organismes non-agréés ou non-certifiés en interface présentant un risque pour la sécurité aérienne.

[6] Pour y parvenir, l'organisme peut s'appuyer sur le référentiel AirCyber [30]

4.5.2.Sous-traitance des activités du SMSI

Sécurité aérienne

L'organisme identifie les sous-traitants œuvrant pour une ou plusieurs activités de son SMSI. Il s'agit notamment des tiers participant aux activités de :

- gestion des risques (appréciation, traitement des risques et gestion des incidents) ;
- fonctionnement du SMSI.

Dans le cas où l'organisme fait appel à un sous-traitant qualifié par l'ANSSI[7] alors ce dernier est considéré comme conforme aux exigences des règlements Part-IS (IS.OR.250) à condition que soient prévues :

- la possibilité pour l'autorité compétente d'avoir accès au sous-traitant ;
- la notification à l'organisme d'événements de sécurité de l'information et de vulnérabilité ayant un potentiel impact sur la sécurité aérienne conformément au §4.4.1.2.2.

Dans le cas contraire, l'organisme :

- mène une analyse de risque relative à la contractualisation d'une ou plusieurs de ces activités basée sur une évaluation :
  - des compétences du sous-traitant ;
  - de l'expérience du sous-traitant pour la ou les activités concernées ;
  - la fiabilité économique et technique du sous-traitant.
- élabore un contrat précisant :
  - l'organisation de la prestation :
    - les rôles et responsabilités entre l'organisme et le sous-traitant ;
    - un schéma de *reporting* clair entre l'organisme et le sous-traitant ;
    - la méthode et les outils de suivi de la prestation.
  - le périmètre de la prestation ;
  - les exigences applicables pour la ou les activités du SMSI concernées ;
  - la gestion des autorisations d'accès aux informations de l'organisme ;
  - les clauses de confidentialité ;
  - les actions possibles en cas de non-respect du contrat ;
  - la possibilité de mener des contrôles par l'organisme ;
  - la possibilité pour l'autorité compétente d'avoir accès au sous-traitant ;
  - la notification à l'organisme d'événements de sécurité de l'information et de vulnérabilité ayant un potentiel impact sur la sécurité aérienne conformément au §4.4.1.2.2.

Enfin, l'organisme :

- formalise la liste des sous-traitants œuvrant pour une ou plusieurs activités de son SMSI ;
- conserve des informations documentées comme preuves de la gestion des sous-traitants des activités du SMSI.

[7] Produits et services qualifiés par l'ANSSI

5. Personnels et compétences

5.1. Vérification des antécédents et contrôle de la fiabilité

5.1.1. Vérification des antécédents pour les personnels de sûreté aérienne

5.1.1.1. Personnel de sûreté aérienne

Sûreté aérienne

Sur la base de son analyse de risques, l'organisme identifie ou fait identifier par les tiers déterminés au §4.2.4,les personnes :

- ayant des droits d'administrateur ou un accès non surveillé et illimité aux données et systèmes de technologies de l'information et de la communication critiques utilisés aux fins de la sûreté aérienne, identifiés au §4.2., et/ou ;
- qui ont été identifiées lors de l'évaluation des risques relative à la sûreté aérienne au §4.2.

Il s'agit notamment :

- des équipes managériales, à savoir les personnes organisant, pilotant, contrôlant ou participant à la gestion des risques de sécurité de l'information pouvant affecter la sûreté aérienne; *(RSSI, DSI, Auditeur interne, responsable sûreté, etc.) ;*
- des équipes opérationnelles, à savoir les personnes définissant, planifiant et mettant en œuvre les mesures de sécurité de l'information définies au §4.3. sur les systèmes d'information critiques à la sûreté identifiés au §4.2 ;
- des administrateurs des systèmes d'information critiques à la sûreté identifiés au §4.2 ;
- des utilisateurs ayant un accès non surveillé et illimité aux données et systèmes d'information critiques à la sûreté identifiés au §4.2 ;
- Le cas échéant, des personnes et/ou entités responsables des risques relatifs à la sûreté aérienne identifiées au §4.2.

L'organisme conserve des informations documentées appropriées comme preuves de l'identification des personnels de sûreté aérienne.

5.1.1.2. Vérification renforcée des antécédents pour les personnels de sûreté aérienne

Sûreté aérienne

L'organisme applique ou fait appliquer par les tiers identifiés au §4.2.4., une vérification renforcée des antécédents des personnels de sûreté aérienne identifiés précédemment. Ainsi, il met en œuvre les actions suivantes, ou s'assure de cette mise en œuvre par les tiers. L'organisme :

- s'assure que ces personnes disposent d'une habilitation préfectorale prévue par l'article L6342-3 du code des transports, à savoir :
  - qu'ils disposent d'un titre d'accès en zone de sûreté à accès réglementé valide dont la délivrance nécessite la détention de l'habilitation préfectorale susmentionnée, ou bien ;
  - qu'ils disposent d'une habilitation sans badge valide.
- prend en considération les emplois, études et interruptions[8] éventuelles de ces personnes dans les États où elles ont résidé[9] au cours des 5 dernières années ;
- renouvelle ces vérifications à intervalles réguliers ne dépassant pas 12 mois ;
- porte une vigilance particulière sur les interruptions[6] injustifiées de ces personnes en leur demandant des explications ou justificatifs et trace le fait que cette vérification a bien été effectuée.

L'organisme :

- tient à jour une liste des personnels de sûreté ayant fait l'objet d'une vérification d'identité et détenant une habilitation valide ;
- formalise sa procédure de vérification des antécédents pour les personnels de sûreté ;
- intègre ou fait référence à cette procédure dans le programme de sûreté;
- conserve des informations documentées appropriées comme preuves de la vérification des antécédents.

[8] « Interruption » : Toute interruption de plus de vingt-huit jours dans le relevé de la formation initiale ou de la carrière.
[9] « État de résidence » : Tout pays dans lequel la personne réside en permanence depuis six mois ou plus.

5.1.2.Contrôle de la fiabilité des personnels de sécurité aérienne

Sécurité aérienne

Sur la base de son analyse de risques, l'organisme définit sa politique de contrôle de la fiabilité des personnes, dans laquelle le contrôle auquel est soumis chaque personne est proportionnel à l'impact qu'elle pourrait avoir sur la sécurité aérienne par compromission de l'intégrité, de la confidentialité ou de la disponibilité des données.

Cette politique identifie :

- des catégories de personnes en fonction du risque pour la sécurité aérienne ;
- des mesures de contrôle de la fiabilité qui :
  - établissent a minima l'identité de la personne au travers de la vérification d'un document d'identité ;
  - peuvent, selon les catégories précédemment identifiées et leur niveau de risque pour la sécurité aérienne :
    - prendre en considération les emplois, études et interruptions[9] éventuelles de ces personnes dans les États où elles ont résidé[10] au cours des 5 dernières années ;
    - amener à réaliser une vérification des antécédents selon des modalités à préciser, telles que :
      - l'habilitation préfectorale visées *supra* ;
      - la fourniture de l'extrait de casier judiciaire (bulletin numéro 3) ;
      - le dispositif de protection des secrets de Défense Nationale ;
      - tout autre dispositif existant et répondant aux objectifs de vérification des antécédents.

L'organisme :

- applique ou fait appliquer par les tiers identifiés au §4.2.4, sa politique de contrôle de la fiabilité des personnes ;
- tient à jour une liste des personnels de sécurité aérienne ayant fait l'objet d'une vérification d'identité et d'un contrôle de leur fiabilité, en précisant duquel il s'agit en fonction des risques sur la sécurité aérienne ;
- formalise la politique de contrôle de la fiabilité du personnel ;
- intègre ou fait référence à cette politique dans :
  - le manuel du système de management de la sécurité de l'information, ou ;
  - le manuel de l'organisme approuvé/certifié.
- conserve des informations documentées appropriées comme preuves du contrôle de la fiabilité du personnel :
  - tant que le personnel concerné doit faire l'objet d'une vérification d'antécédent, et ;
  - un an après la fin de l'activité justifiant le contrôle de la fiabilité.

5.1.3.Cas particuliers

5.1.3.1. Personnels soumis aux exigences de sûreté et de sécurité

Sécurité et sûreté aérienne

Dans le cas où une personne est soumise aux exigences de vérification des antécédents pour la sûreté et la sécurité aérienne, alors il doit se soumettre au dispositif le plus exigeant, à savoir celui de la sûreté.

5.1.3.2. Personnels à l'étranger

Sécurité et sûreté aérienne

Dans le cas où l'organisme emploie du personnel de nationalité étrangère ne résidant pas en France pour lequel il documente qu'il ne lui est pas légalement possible de réaliser une vérification des antécédents, alors l'organisme :

- établit l'identité de ces personnes au travers de la vérification d'un document d'identité ;
- exige de ces personnes un engagement signé de bonne conduite lors de la réalisation de missions pour le compte de l'organisme ;
- tient à jour une liste des personnels étrangers pour lesquels la vérification des antécédents n'a pu être réalisée.

5.2. Sensibilisation

Sécurité et sûreté aérienne

L'organisme met en œuvre une campagne de sensibilisation ou s'assure de cette mise en œuvre par les tiers identifiés au §4.2.4., notamment il :

- précise :
  - les moyens et ressources mis en œuvre ;
  - la fréquence de renouvellement de la campagne de sensibilisation.
- s'assure que les personnes identifiées au §5.1.1.1.et au travers de l'analyse de risques relatifs à la sécurité aérienne (§4.2.4) sont sensibilisées à la sécurité de l'information ;
- formalise le suivi de la sensibilisation et la procédure associée ;
- intègre ou fait référence à cette procédure dans :
  - le manuel du système de management de la sécurité de l'information, ou ;
  - le manuel de l'organisme approuvé/certifié, et/ou ;
  - le programme de sûreté.
- conserve des informations documentées appropriées comme preuves suivi de la sensibilisation de son personnel.

5.3. Formation

Sécurité et sûreté aérienne

L'organisme met en œuvre un programme de formation ou s'assure de cette mise en œuvre par les tiers identifiés au §4.2.4., notamment il :

- identifie les besoins au sein de son entreprise, notamment que :
  - les équipes managériales soient formées à la gestion de la sécurité de l'information en cohérence avec les tâches qui leur sont confiées ;
  - les équipes opérationnelles soient formées à la mise en œuvre des mesures de sécurité de l'information à l'état de l'art, en cohérence avec les tâches qui leur sont confiées .
- précise les moyens et ressources mis en œuvre ;
- formalise le suivi des compétences et la procédure associée ;
- intègre ou fait référence à cette procédure dans :
  - le manuel du système de management de la sécurité de l'information, ou ;
  - le manuel de l'organisme approuvé/certifié, et/ou ;
  - le programme de sûreté.
- conserve des informations documentées appropriées comme preuves de suivi de la formation de son personnel.

6. Définition et fonctionnement du SMSI

6.1. Suivi de la gestion des risques

6.1.1. Organisation du suivi de la gestion des risques

Sécurité et sûreté aérienne

L'organisme définit l'organisation du suivi de la gestion des risques et en précise :
- la structure et le positionnement ;
- les responsabilités des différents participants ;
- l'articulation avec l'organisation déjà en place pour le suivi de la gestion des risques relatifs à la sûreté et/ou à la sécurité aérienne ;
- la périodicité et/ou les événements significatifs activant cette organisation, notamment lorsque :
    - il y a un changement dans les éléments exposés à des risques liés à la sécurité de l'information ;
    - il y a un changement dans les interfaces entre l'organisme et d'autres organismes, ou dans les risques communiqués par les autres organismes ;
    - il y a un changement dans les informations ou connaissances utilisées pour le recensement, l'analyse et la classification des risques ;
    - l'analyse des incidents de sécurité de l'information a permis de tirer des enseignements.

6.1.2. Missions du suivi de la gestion des risques

Sécurité et sûreté aérienne

Périodiquement et/ou lors des événements significatifs, l'organisme :
- planifie, met en œuvre, contrôle :
    - les activités de gestion des risques :
        - appréciation des risques (§4.2) ;
        - traitement des risques (§4.3) ;
        - gestion des incidents de sécurité de l'information (§4.4) ;
        - gestion des risques induits par les tiers (§4.5).
    - la gestion des personnels et des compétences (§5) ;
    - la mise en œuvre des mesures techniques et organisationnelles :
        - du plan de traitement des risques ;
        - de détection, de réaction et de réponse à un incident de sécurité ;
        - notifiées par l'autorité compétente.
- assure le suivi des événements et incidents de sécurité de l'information.

6.1.3. Résultats du suivi de la gestion des risques

Sécurité et sûreté aérienne

L'organisme:
- produit et tient à jour des tableaux de bord de suivi :
    - des activités de gestion des risques ;
    - des personnels et des compétences ;
    - d'avancement de mise en œuvre des mesures techniques et organisationnelles ;
    - des événements et incidents de sécurité de l'information.
- informe le Dirigeant Responsable et les personnes ou entités responsables de risques des conclusions du suivi de la gestion des risques ;
- formalise la procédure relative au suivi de la gestion des risques ;
- intègre ou fait référence à cette procédure dans :
    - le manuel du système de management de la sécurité de l'information, ou ;
    - le manuel de l'organisme approuvé/certifié, et/ou ;
    - le programme de sûreté.
- conserve des informations documentées comme preuves du suivi de la gestion des risques.

6.2. Évaluation du SMSI

6.2.1. Évaluation de la conformité du SMSI

6.2.1.1. Organisation de l'évaluation de la conformité du SMSI

Sécurité aérienne

L'organisme définit l'organisation en charge de l'évaluation de la conformité et en précise :
- la structure et le positionnement ;
- les responsabilités des différents participants ;
- l'articulation avec l'organisation déjà en place pour l'évaluation de la conformité relative à la sécurité aérienne ;
- la périodicité et/ou les événements significatifs activant cette organisation.

6.2.1.2. Missions de l'évaluation de la conformité du SMSI

Sécurité aérienne

Périodiquement et/ou lors des événements significatifs et en s'appuyant sur les résultats :
- des audits internes ;
- des audits des autorités compétentes.

l'organisme :
- évalue la conformité et ;
- identifie les écarts de son SMSI par rapport aux dispositions du présent document ;
- corrige ces écarts afin de se mettre en conformité avec les exigences de la Part-IS.

6.2.1.3. Résultats de l'évaluation de la conformité du SMSI

Sécurité aérienne

L'organisme :
- produit et tient à jour un tableau de bord de suivi de la conformité et les éventuels écarts associés ;
- informe le Dirigeant Responsable et les personnes ou entités responsables des risques des conclusions de l'évaluation de la conformité du SMSI ;
- formalise la procédure relative à l'évaluation de la conformité du SMSI ;
- intègre ou fait référence à cette procédure dans :
  - le manuel du système de management de la sécurité de l'information, ou ;
  - le manuel de l'organisme approuvé/certifié.
- conserve des informations documentées comme preuves des résultats d'évaluation de la conformité du SMSI.

6.2.2. Réponse aux constatations notifiées par l'autorité compétente

Sécurité aérienne

L'organisme réagit aux constatations notifiées par l'autorité compétente au travers du processus de traitement des constatations prévus dans le cadre de son certificat/agrément.

6.2.3.Évaluation de l'efficacité et de la maturité du SMSI

6.2.3.1. Organisation de l'évaluation de l'efficacité et de la maturité du SMSI

Sécurité aérienne

L'organisme définit l'organisation en charge de l'évaluation de l'efficacité et de la maturité du SMSI et en précise :

- la structure et le positionnement ;
- les responsabilités des différents participants ;
- l'articulation avec l'organisation déjà en place pour l'évaluation du système de gestion de la sécurité aérienne ;
- la périodicité et/ou les événements significatifs activant cette organisation ;
- les indicateurs d'efficacité associés aux objectifs de sécurité définis dans la politique de sécurité de l'information ;
- le modèle de maturité du SMSI visé[10].

6.2.3.2. Missions de l'évaluation de l'efficacité et de la maturité du SMSI

Sécurité aérienne

Périodiquement et/ou lors des événements significatifs et en s'appuyant sur :

- la politique de sécurité de l'information ;
- les éléments relatifs à la gestion des ressources, aux rôles et responsabilités ;
- les tableaux de bord de suivi des activités de gestion des risques, des personnels et des compétences, et des événements et incidents de sécurité de l'information ;
- des éventuels audits techniques et organisationnels ;
- son retour d'expérience, alimenté notamment par la gestion des incidents.

L'organisme :

- évalue :
  - l'efficacité de son SMSI par rapport aux objectifs de sécurité définis dans la politique de sécurité de l'information ;
  - la maturité de son SMSI par rapport au modèle de maturité visé.Lors de ces évaluations, l'organisme porte une attention particulière aux processus relatifs :
    - à la gouvernance (§3) ;
    - aux activités de gestion des risques (§4) ainsi que leur suivi (§6.1) ;
    - à la gestion des personnels et des compétences (§5) ;
    - à l'évaluation de la conformité, de l'efficacité et de la maturité du SMSI (§6.2) ;
    - Au pilotage de l'amélioration continue (§6.3).
- identifie :
  - les écarts et/ou les manques par rapport aux objectifs de sécurité ;
  - les axes d'amélioration éventuels afin d'atteindre les niveaux de maturité du modèle visé.

6.2.3.3. Résultats de l'évaluation de l'efficacité et de la maturité du SMSI

Sécurité aérienne

L'organisme :

- produit et tient à jour des tableaux de bord de suivi de :
  - l'efficacité de son SMSI et des écarts associés ;
  - la maturité de son SMSI et des éventuels axes d'amélioration associés.
- informe le Dirigeant Responsable et les personnes ou entités responsables des risques des conclusions de l'évaluation de l'efficacité et de la maturité du SMSI ;
- formalise la procédure relative à l'évaluation de l'efficacité et de la maturité du SMSI ;
- intègre ou fait référence à cette procédure dans :
  - le manuel du système de management de la sécurité de l'information, ou ;
  - le manuel de l'organisme approuvé/certifié.
- conserve des informations documentées comme preuves des résultats de l'évaluation de l'efficacité et de la maturité du SMSI.

[10] Les modèles de maturité suivants peuvent être pris pour référence :

- Cybersecurity Capability Maturity Model (C2M2), version 1.1
- Systems Security Engineering – Capability Maturity Model (SSE-CMM)
- NIST Cybersecurity Framework (NIST CSF), version 1.1
- ATM Cybersecurity Maturity Model, edition 1

6.3. Amélioration continue du SMSI

6.3.1.1. Organisation du pilotage de l'amélioration continue du SMSI

Sécurité aérienne

L'organisme définit l'organisation du pilotage de l'amélioration continue et en précise :
- la structure et le positionnement ;
- les responsabilités des différents participants ;
- l'articulation avec l'organisation déjà en place pour le pilotage de l'amélioration continue du système de gestion de la sécurité aérienne ;
- la périodicité et/ou les événements significatifs activant cette organisation, notamment :
    - au moins 1 fois entre 2 audits de l'autorité, et/ou ;
    - les événements significatifs déclenchant la revue de direction (incident, changement de contexte etc.).

6.3.1.2. Missions du pilotage de l'amélioration continue du SMSI

Sécurité aérienne

Périodiquement et/ou lors des événements significatifs et sur la base :
- des changements de contexte de l'organisme, notamment :
    - l'évolution de la menace ;
    - un changement dans l'organisation.
- des tableaux de bord de suivi :
    - de la conformité du SMSI et des écarts associés ;
    - de l'efficacité du SMSI et des écarts associés ;
    - de la maturité du SMSI et des éventuels axes d'amélioration associés ;
    - des non-conformités notifiées par l'autorité et des actions correctives associées ;
    - des actions issues du pilotage de l'amélioration continue.

L'organisme :
- identifie :
    - les modifications à apporter au SMSI : organisation, processus, etc. ;
    - les actions correctives et préventives à mettre en œuvre ;
    - des opportunités d'amélioration continue.
- décide de les mettre en œuvre ;
- précise les délais de mises en œuvre.

6.3.1.3. Conclusions du pilotage de l'amélioration continue du SMSI

Sécurité aérienne

L'organisme :
- produit et tient à jour un tableau de bord de suivi des actions issues du pilotage de l'amélioration continue ;
- formalise la procédure relative à l'amélioration continue ;
- intègre ou fait référence à cette procédure dans :
    - le manuel du système de management de la sécurité de l'information, ou ;
    - le manuel de l'organisme approuvé/certifié.
- conserve des informations documentées comme preuves du pilotage de l'amélioration continue.

6.4. Modification du système de management de la sécurité de l'information

A paraitre dans la prochaine version du 3CFv2

7. Documentation

7.1. Gestion documentaire

A paraitre dans la prochaine version du 3CFv2

7.2. Manuel du système de gestion de la sécurité de l'information

7.2.1. Gestion du manuel SMSI

A paraitre dans la prochaine version du 3CFv2

7.2.2. Éléments du manuel

Sécurité aérienne

L'organisme intègre ou fait référence aux éléments suivants dans :

- le manuel du système de management de la sécurité de l'information, ou ;
- le manuel de l'organisme approuvé/certifié.

Documents	Chapitres 3CFv2
La lettre d'engagement du Dirigeant Responsable	3.1
La politique de sécurité de l'information	3.2
le(s) titre(s), le(s) nom(s), les missions, les obligations de rendre compte, les responsabilités et les pouvoirs des personnes visées au 3.3.	3.3
un organigramme montrant les rapports hiérarchiques en matière d'obligation de rendre compte et de responsabilité entre les personnes visées aux 3.3	
une description générale des ressources humaines, en termes d'effectifs et de catégories, et du système qui est en place pour planifier la mise à disposition du personnel	
La description du schéma de notification interne	4.4.1.2.2

Procédures	Autorité	Chapitres 3CFv2
La procédure de gestion des risques (appréciation, traitement et suivi des risques)	Mis à disposition	4.1, 4.2, 4.3 et 6.1
La procédure de gestion des incidents de sécurité de l'information	Mis à disposition	4.4
La procédure de notification à l'autorité (à venir)	Mis à disposition	4.4.5
La procédure de gestion des organismes en interface	Mis à disposition	4.5.1
La procédure de gestion des sous-traitants réalisant des activités du SMSI	Mis à disposition	4.5.2
La politique de contrôle de fiabilité du personnel	Mis à disposition	5.1.2.
La procédure de suivi de la sensibilisation	Mis à disposition	5.3
La procédure de suivi de la formation	Mis à disposition	5.4
La procédure d'évaluation de la conformité du SMSI	Mis à disposition	6.2.1
La procédure d'évaluation de l'efficacité et de la maturité du SMSI	Mis à disposition	6.2.3
La procédure d'amélioration continue	Mis à disposition	6.3
La procédure de gestion des changements du SMSI (à venir)	Approuvé	6.4
La procédure de gestion documentaire	Mis à disposition	7.1
La procédure de modification du manuel SMSI (à venir)	Mis à disposition	7.2.1

7.3. Programme de sûreté

Sûreté aérienne

L'organisme intègre ou fait référence dans son programme de sûreté aux éléments suivants :

Documents	Chapitres 3CFv2
La liste des risques au regard de la sûreté	4.2
La liste des systèmes d'information critiques à la sûreté	4.2
Le plan de traitement des risques	4.3
La liste des organismes en interface présentant un risque pour la sûreté	4.2
La liste des mesures techniques et organisationnelles visant à détecter, réagir et se rétablir à la suite d'un incident de sécurité de l'information	4.4.4

Procédures	Chapitres 3CFv2
La procédure de gestion des risques (appréciation, traitement et suivi des risques)	4.1, 4.2, 4.3 et 6.1
La procédure de gestion des organismes en interface	4.5.1
La procédure de vérification des antécédents	5.1.1
La procédure de suivi de la sensibilisation	5.3
La procédure de suivi de la formation	5.4

Annexe

Matrice de conformité

Cadre de conformité cyber France v2			Règlement 2015/1998	Part-IS.OR	AMC.IS.OR [33]
3. Gouvernance	3.1. Engagement du Dirigeant Responsable			200 (a) (1)	200 (a) (1)
	3.2. Politique de sécurité de l'information			200 (a) (1) et (d) 240 (a) (2)	
	3.3. Gestion des ressources, rôles et responsabilités			200 (a) (10) 240 (a) à (f) et (h)	240(a)(2),(a)(3) (b),(d) (f), (h)
4. Gestion des risques de sécurité de l'information	4.2. Appréciation des risques		1998 – 1.7.1, 1.7.2 et 1.7.3 AIM – DR-1-7-1 (I)	200 (a) (2) 205 (a), (b) et (c) 210 (b)	205(a) 205(b) 205(c)
	4.3. Traitement des risques		1998 – 1.7.1, 1.7.2 et 1.7.3	200 (a) (3) 210 (a) et (b)	210(a)
	4.4. Gestion des incidents de sécurité de l'information	4.4.1. Détection des incidents de sécurité de l'information		200 (a) (4) et (5) 215 (a), (b) et (e) 220 (a)	215(a)&(b) 220(a)
		4.4.2. Réponse aux incidents de sécurité de l'information		200 (a) (5) 220 (b)	220(b)
		4.4.3. Remédiation		200 (a) (5) 220 (c)	220(c)
		4.4.4. Résultat de la gestion des incidents de sécurité de l'information	1998 – 1.7.2 1998 – 1.7.3		
		4.4.5. Notification à l'autorité		200 (a) (8) 230 (a) (b) et (c)	230(a)&(b) 230(c)
	4.5. Gestion des risques induits par les tiers	4.5.1. Organismes en interface	AIM – B-2 AIM – B-4	200 (a) (9) et (13) 215 (c) et (d)	200(a)(13)
		4.5.2. Sous-traitance des activités du SMSI		235 (a) et (b)	235(a), 235(b)
5. Personnels et compétences	5.1. Vérification des antécédents et contrôle de la fiabilité		1998 – 11.1.2, 11.1.3 et 11.5.1 L. 6342-3 , 11.1.7	240 (i)	240(i)
	5.2. Sensibilisation		1998 – 11.2.8.1, 11.2.8.2 et 11.2.1.4 AIM 11-2-1-4 et 11-2-1-5	240 (h)	
	5.3. Formation		1998 – 11.2.8.1, 11.2.8.2 et 11.2.1.4 AIM 11-2-1-4 et 11-2-1-5	240 (g)	240(g)
6. Définition et fonctionnement du SMSI	6.1. Suivi de la gestion des risques		1998 – 1.7.1, 1.7.2 et 1.7.3 AIM DR 1-7-1 (II)	200 (a) (2) à (6) 205 (d)	205(d)
	6.2. Évaluation du SMSI	6.2.1. Évaluation de la conformité du SMSI		200 (a) (12)	200(a)(12)
		6.2.2. Réponse aux constatations notifiées par l'autorité compétente		200 (a) (7) 225 (a) et (b)	225
		6.2.3. Évaluation de l'efficacité et de la maturité du SMSI		260 (a)	
	6.3. Amélioration continue du SMSI			200 (b) 260 (b)	260, 260(a) 260(b)
	6.4. Modification du système de management de la sécurité de l'information			200 (c) 255 (a) et (b)	255
7. Documentation	7.1. Gestion documentaire			200 (a) (11) et (d) 245 (a),(b),(c) et(d)	245(a)(1)(vi)&(a)(5) 245(c)&(d)
	7.2. Manuel du système de gestion de la sécurité de l'information			200 (c) 250 (a) et (b)	200(c)

Définitions

L'authenticité est la propriété selon laquelle une entité est ce qu'elle revendique être		ISO/IEC 27000:2018
La **confidentialité** est la propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés		ISO/IEC 27000:2018
Un **contractant** est une entité externe ayant son propre agrément et effectuant des tâches sous couvert de ce dernier pour le compte d'une personne physique ou d'un autre organisme également agréé. Dans le cadre de la production, cet organisme est généralement désigné comme un fournisseur		Guide P-03-01 Ed0 : DSAC/OSAC
Le **Dirigeant Responsable** est la personne qui a autorité pour veiller à ce que toutes les activités de son organisme soient financées et exécutées conformément aux exigences applicables. Le dirigeant responsable est chargé d'établir et de maintenir un système de gestion efficace		RÈGLEMENT D'EXECUTION (UE) 2017/373
La **disponibilité** est la propriété d'être accessible et utilisable à la demande par une entité autorisée		ISO/IEC 27000:2018
Un **événement** lié à la sécurité de l'information est un fait détecté dans l'état d'un système, d'un service ou d'un réseau pouvant indiquer une atteinte à la politique de sécurité de l'information ou d'une défaillance des mesures de sécurité de l'information, ou une situation auparavant inconnue pouvant avoir de l'importance pour la sécurité de l'information		RÈGLEMENT DÉLÉGUÉ (UE) 2022/1645
Une **fonction** fait référence aux :	Biens essentiels	EBIOS 2010 : ANSSI
	Valeurs métier : Dans le cadre de l'étude, composante importante pour l'organisation dans l'accomplissement de sa mission. Cela peut être un service, une fonction support, une étape dans un projet et toute information ou savoir-faire associé	EBIOS RM : ANSSI
	Actifs essentiels : tout élément représentant de la valeur pour l'organisme tels que : - Les informations - Les processus et activités métier	ISO/IEC 27002:2022
Un **fournisseur** est une Entité externe fournissant des produits ou des services dont il a l'entière responsabilité		Guide P-03-01 Ed0 : DSAC/OSAC
Un **incident** est tout événement ayant un impact négatif sur la sécurité des réseaux et des systèmes d'information		Article 4, paragraphe 7, de la directive (UE) 2016/1148
L'intégrité est la propriété d'exactitude et de complétude		ISO/IEC 27000:2018
Une **interface** est limite commune à deux systèmes, permettant des échanges entre ceux-ci		LAROUSSE
Une **menace** est une violation potentielle de la sécurité de l'information qui existe lorsqu'une entité, une circonstance, une action ou un événement est susceptible de causer des dommages		RÈGLEMENT DÉLÉGUÉ (UE) 2022/1645
Un **risque** lié à la sécurité de l'information est le risque que pose, pour l'organisation des activités de l'aviation civile, les actifs, les personnes et d'autres organismes, un éventuel événement lié à la sécurité de l'information. Les risques liés à la sécurité de l'information sont associés à l'éventualité que des menaces exploitent les vulnérabilités d'un actif d'information ou d'un groupe d'actifs d'information		RÈGLEMENT DÉLÉGUÉ (UE) 2022/1645
La **sécurité aérienne** est l'état dans lequel les risques liés aux activités aéronautiques concernant, ou appuyant directement, l'exploitation des aéronefs sont réduits et maîtrisés à un niveau acceptable		Annexe 19 : OACI

La **sécurité de l'information** consiste en la préservation de la confidentialité, de l'intégrité, de l'authenticité et de la disponibilité des réseaux et des systèmes d'information	RÈGLEMENT DÉLÉGUÉ (UE) 2022/1645
Un **sous-traitant** est une entité externe exécutant des tâches spécifiées par un organisme donneur d'ordre agréé et sous couvert de l'agrément de celui-ci. La sous-traitance est l'opération par laquelle une société délègue à une autre une partie de son activité ou encore une partie d'un contrat obtenu par le donneur d'ordre. Le sous-traitant s'engage à exécuter un produit ou une tâche sur la base des instructions de l'entreprise donneuse d'ordre qui conserve la haute main sur le produit et ses caractéristiques. En cela le sous-traitant est distinct du fournisseur dans la mesure où ce dernier est totalement responsable du produit ou service qu'il propose à son client	Guide P-03-01 Ed0 : DSAC/OSAC
La **sûreté aérienne** est une combinaison des mesures ainsi que des moyens humains et matériels visant à protéger l'aviation civile contre les actes d'interventions illicites[11]. Elle vise à prévenir les actes de malveillance visant les aéronefs, leurs passagers et les membres d'équipage	Annexe 17 : OACI
Une **vulnérabilité** est une faille ou une faiblesse que présentent un actif ou un système, des procédures, une conception, une mise en œuvre ou des mesures de sécurité de l'information qui pourrait être exploitée et entraîner une atteinte à la politique de sécurité de l'information	RÈGLEMENT DÉLÉGUÉ (UE) 2022/1645
Un **système d'information** est un ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information	ISO/IEC 27000:2018

[11] Source OACI – Annexe 17

Références

[1]	Règlement d'exécution (UE) 2015/1998 de la Commission du 5 novembre 2015 fixant des mesures détaillées pour la mise en œuvre des normes de base communes dans le domaine de la sûreté de l'aviation civile
[2]	Règlement d'exécution (UE) 2023/203 de la Commission du 27 octobre 2022 portant 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
[3]	Règlement délégué (UE) 2022/1645 de la Commission du 14 juillet 2022 portant 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
[4]	Règlement (UE) n ° 748/2012 de la Commission du 3 août 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
[5]	Règlement (UE) n °1321/2014 de la Commission du 26 novembre 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
[6]	Règlement (UE) n ° 965/2012 de la Commission du 5 octobre 2012 déterminant les exigences techniques et les procédures administratives applicables aux opérations aériennes
[7]	Règlement (UE) no 1178/2011 de la Commission du 3 novembre 2011 déterminant les exigences techniques et les procédures administratives applicables au personnel navigant de l'aviation civile
[8]	Règlement (UE) 2015/340 de la Commission du 20 février 2015 déterminant les exigences techniques et les procédures administratives applicables aux licences et certificats de contrôleur de la circulation aérienne
[9]	Règlement d'exécution (UE) 2017/373 de la Commission du 1er mars 2017 établissant des exigences communes relatives aux prestataires de services de gestion du trafic aérien et de services de navigation aérienne ainsi que des autres fonctions de réseau de la gestion du trafic aérien, et à leur supervision
[10]	Règlement (UE) n ° 139/2014 de la Commission du 12 février 2014 établissant des exigences et des procédures administratives relatives aux aérodromes
[11]	Règlement d'exécution (UE) 2021/664 de la Commission du 22 avril 2021 relatif à un cadre réglementaire pour l'U-space
[12]	Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transport aérien » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense, Legifrance, Août 2016
[13]	Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, Legifrance, Mai 2018. Arrêté du 13 juin 2018 fixant les modalités des déclarations prévues aux articles 8, 11 et 20 du décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, Legifrance, Juin 2018. Arrêté du 1er août 2018 relatif au coût d'un contrôle effectué par l'Agence nationale de la sécurité des systèmes d'information en application des articles 8 et 14 de la loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, Legifrance, Août 2018 Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique, Legifrance, Septembre 2018
[14]	Norme internationale ISO/IEC 27001:2022 – Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information
[15]	Norme internationale ISO/IEC 27005:2022 – Sécurité de l'information, cybersécurité et protection de la vie privée - Préconisations pour la gestion des risques liés à la sécurité de l'information
[16]	Guides EBIOS Risk Manager, ANSSI, Version 1.5, Mars 2024
[17]	Norme internationale ISO/IEC 31000:2018 – Management du risque - Lignes directrices
[18]	White paper: Identification and Classification guidance for Part-IS assets - ED/DO-ISMS Guidance for Aviation, EUROCAE WG-72 / RTCA SC-216, 2023
[19]	ICAO Doc 9859 Safety Risk Tolerability
[20]	ICAO Doc 10108 Aviation Security Global Risk Statement
[21]	Guide d'hygiène informatique, ANSSI, Version 2.0, Septembre 2017
[22]	Norme internationale ISO/IEC 27002:2022 – Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information
[23]	Norme internationale ISA/IEC 62443 - Series of Standards
[24]	Prestataires de détection des incidents de sécurité - Référentiel d'exigences, ANSSI, 2017
[25]	Standard ETSI ISI Indicators (ISI 001-1 and Guides 001-2), ISI Event Model (ISI-002), ISI Maturity (ISI-003), ISI Event Detection (ISI-004) – 5 standards sur la détection des incidents de sécurité, ETSI,

[26]	Norme internationale ISO/IEC 27035:2023 – Technologies de l'information - Gestion des incidents de sécurité de l'information
[27]	ED Decision 2023/009/R, EASA, 2023
[28]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, note technique n° DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013, ANSSI
[29]	Règlement (UE) n °376/2014 du Parlement européen et du Conseil du 3 avril 2014 concernant les comptes rendus, l'analyse et le suivi d'événements dans l'aviation civile
[30]	Outil de Maturité AirCyber, Boostaerospace, 2023
[31]	ED-201A - Aeronautical Information System Security (AISS) Framework Guidance, EUROCAE, 2021
[32]	ED-206 - Guidance on Security Event Management, EUROCAE, 2022
[33]	P-03-01 - Instruction et surveillance des agréments d'organismes avec système de gestion, DSAC/OSAC, 2024
[34]	Easy Access Rules for Information Security, EASA, Octobre 2023

Direction générale de l'Aviation civile
Direction de la Sécurité de l'Aviation civile
50, rue Henry Farman
75720 PARIS CEDEX 15
Tél. : +33 (0)1 58 09 43 21
www.ecologie.gouv.fr