TLP:GREEN

CADRE DE CONFORMITE CYBER FRANCE

VERSION 3

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

Direction de la sécurité de l'aviation civile
Direction de programme cybersécurité
Version n° 3.0 du 11 juillet 2025

Table des matières

Information

Ce document, établi par la direction de la sécurité de l'aviation civile (DSAC) et l'organisme pour la sécurité de l'aviation civile (OSAC), 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 diffusé 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 DSAC à l'adresse suivante : dp-cyber-dsac.bf@aviation.civile.gouv.fr, et/ou ;
- l'OSAC. Pour cela, le demandeur doit rechercher le document concerné sur la page Documentation Technique et sélectionner « Demander une modification » dans la colonne Actions. Cette procédure est disponible en téléchargement sur le site internet : https://documentation.osac.aero/.

Historique des révisions

Version	Date	Modifications
Version intermédiaire	30 juin 2021	Création du document
Version 1	3 Sept. 2021	- Modifications : o § 1. Introduction o § 2. Démarche d'accompagnement o § 4.1.4. Personnels et compétence o § 5.4.4.1. Sources des non-conformités o Annexe 3 : Grille de conformité réglementaire - Ajouts : o § 5.1.3. Formation o 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 Partie – IS
Version 3	17 juin 2025	- Modifications : o § 1.2. Champs d'application o § 1.3. Équivalence entre les dispositifs réglementaires o §2. Présentation générale du document o §4.1. Établissement du contexte o §4.4.1. Détection des incidents de sécurité de l'information o § 5.1.3.2. Personnel à l'étranger o §8. Documentation o Annexe IV : Matrice de conformité o Annexe V : Définitions o Annexe VII : Références - Ajouts : o Tous : Références réglementaires o § 3.3. Personne responsable commune o § 4.2.2. Organismes relevant de la Partie ATM/ANS.OR o § 4.2.4. Organismes relevant de la Partie ATM/ANS.OR o § 4.4.5. Notification à l'autorité compétente o § 4.5.1.2.1. Notification aux DOA o §6.2.2. Réponse aux constatations notifiées par l'autorité compétente o § 6.4. Modification du SMSI o §7. Archivage o Annexe I : Bonnes pratiques o Annexe II : Fonctions essentielles sûreté aérienne o Annexe III : Fonctions essentielles sécurité aérienne o Annexe VI : Acronymes
	11 juillet 2025	Correction de typos et de mauvaises références

1. Introduction

1.1. Objectif du document

Ce document est un guide et propose un référentiel unique de dispositions visant à accompagner les organismes à se mettre en conformité 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 Partie – 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. Champs d'application

1.2.1. Opérateurs détenant un agrément de sûreté

Le présent document s'adresse aux **exploitants d'aérodrome** et aux **transporteurs aériens** 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 suivants :

Applicable	Exempté
Organismes de production (POA) relevant de l'annexe I (partie 21), section A, sous-parties G et J, du règlement (UE) n°748/2012 [4]	Organismes de production **uniquement associés à la production d'aéronefs ELA2** au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) n°748/2012 [4]
Organismes de conception (DOA) relevant de l'annexe I (partie 21), section A, sous-parties G et J, du règlement (UE) n°748/2012 [4]	Organismes de conception **uniquement associés à la conception d'aéronefs ELA2** au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) n°748/2012 [4]
Exploitants d'aérodrome et prestataires de services de gestion des aires de trafic relevant de l'annexe III (partie ADR.OR) du règlement (UE) n°139/2014 [5]	
Organismes de maintenance relevant la section A de l'annexe II (partie 145) du règlement (UE) n°1321/2014 [6]	Organismes de maintenance **participant uniquement à la maintenance des aéronefs** conformément à l'annexe V ter (**partie – ML**) du règlement (UE) n°1321/2014 [6]
Organismes responsables de la gestion du maintien de la navigabilité (CAMO) relevant de la section A de l'annexe V quater (partie CAMO) du règlement (UE) n°1321/2014 [6]	CAMO **participant uniquement à la gestion du maintien de la navigabilité des aéronefs** conformément à l'annexe V ter (partie ML) du règlement (UE) n°1321/2014 [6]

Transporteurs aériens relevant de l'annexe III (partie ORO) du règlement (UE) n°965/2012 [7]	Transporteurs aériens participant **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) n°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
Organismes de formation agréés (ATO) relevant de l'annexe VII (partie ORA) du règlement (UE) n°1178/2011 [8]	ATO participant uniquement : - aux activités de formation pour les aéronefs ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) n°748/2012 [4] - à la formation théorique.
Centres aéromédicaux du personnel navigant relevant de l'annexe VII (partie ORA) du règlement (UE) n°1178/2011 [8]	
Exploitants de simulateurs d'entraînement au vol (FSTD) relevant de l'annexe VII (partie ORA) du règlement (UE) n°1178/2011 [8]	Exploitants FSTD **participant uniquement à l'exploitation de FSTD pour les aéronefs ELA2** au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) n°748/2012 [4]
Organismes de formation des contrôleurs de la circulation aérienne (ATCO – TO) relevant de l'annexe III (partie ATCO.OR) du règlement (UE) n°2015/340 [9]	
Centres aéromédicaux ATCO relevant de l'annexe III (partie ATCO.OR) du règlement (UE) n°2015/340 [9]	
Prestataires de services de la navigation aérienne (PSNA) relevant de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) n°2017/373 [10]	Prestataires de services de navigation aérienne **titulaires d'un certificat limité** et aux prestataires de **services d'information de vol** déclarant leurs activités conformément au point ATM/ANS.OR.A.010 de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) n°2017/373 [10]
Organismes de conception de procédures de vol (FPD) relevant de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) n°2017/373 [10]	
Prestataires de services U-space Prestataires uniques de services d'informations communes soumis au règlement d'exécution (UE) n°2021/664 [11]	

1.2.3. Dispense à certaines exigences de la Partie – IS

Les règlements (UE) n°2023/203 et (UE) n°2022/1645 - IS.I/D.OR 200 (e), prévoient la possibilité que l'autorité compétente puisse dispenser un organisme, pour une période limitée dans le temps, d'appliquer certaines exigences 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 risques 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.

Le cadre de cette dérogation d'application de la Partie – IS et les critères d'éligibilité sont précisés dans les communications METEOR DSAC [12] et dans le BI OSAC 2025 – 03 [13].

Les organismes potentiellement éligibles à cette dispense sont :

- pour les organismes surveillés par la DSAC :
  - les opérateurs de travail aérien (SPO) et d'aviation générale complexe (NCC);
  - certains :
    - organismes de formation agréés (ATO) ;
    - exploitants de simulateurs d'entraînement au vol (FSTD);
    - organismes de formation des contrôleurs de la circulation aérienne (ATCO – TO) ;
    - organismes de conception de procédures de vol (FPD) ;
    - centres aéromédicaux ATCO ;
    - prestataires de services *U-Space* ;
  - les opérateurs CAT les moins complexes.
- pour les agréments surveillés par OSAC, les critères d'éligibilité à la dispense sont, en fonction du type d'activité :
  - Partie-21G : Production uniquement d'éléments n'ayant pas de fonction « sécurité » majeure ;
  - Partie-145 : Travaux uniquement sur des éléments n'ayant pas de fonction « sécurité » majeure ou ne contribuant pas à l'intégrité structurale ;
  - Partie-CAMO : les agréments CAMO gérant uniquement :
    - la flotte aéronef d'un exploitant considéré comme potentiellement dispensable par la DSAC ;
    - des aéronefs en stockage ou mettant uniquement en œuvre la Sous-partie I règlement (UE) n°1321/2014 [6]

1.3. Équivalence entre les dispositifs règlementaires

Les modalités d'application des équivalences entre les règlements Partie – IS [2,3] et le règlement (UE) 2015/1998 [1] d'une part et la transposition de la directive NIS 2 [44] d'autre part seront précisées dans la version 3.1 du Cadre de Conformité Cyber France.

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 Partie – 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 » [14] issu de l'article 22 de la loi de programmation militaire ;
  - le décret et les arrêtés [15]; issus de la loi de transposition de la directive *Network Information Security 1.*

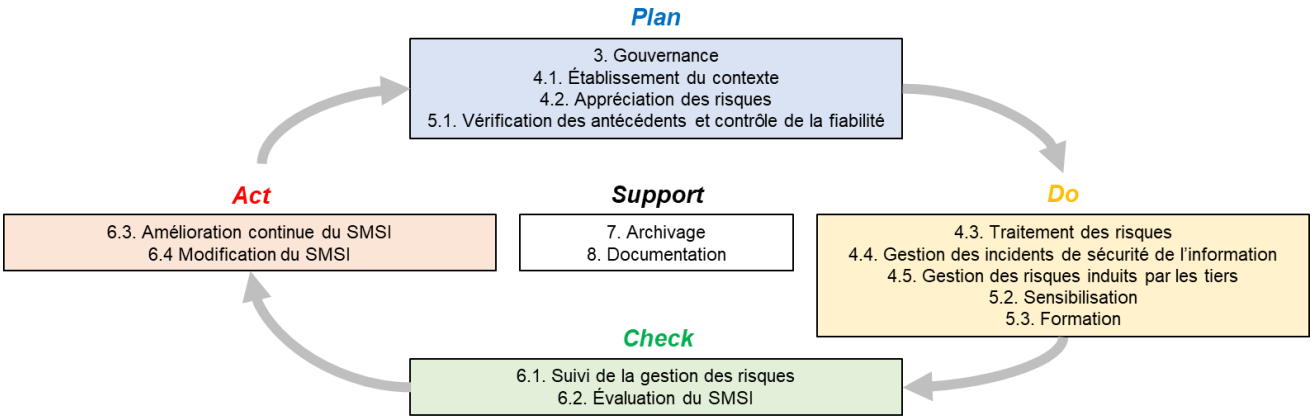
Par ailleurs, il est inspiré des bonnes pratiques telles que :

- la norme ISO 27001 [16] 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 européens et internationaux menés par l'OACI, l'EASA et 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 :



[1] Publication de l'ANSSI

2.3. Utilisation

Pour les organismes devant se mettre en conformité :

- 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 Partie – 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., §6.1 et §8.1 sont à considérer et le périmètre d'application couvre uniquement la sûreté aérienne.

Pour chaque disposition, un encart rappelle la référence réglementaire parmi :

- la **Partie – IS** [2,3] ;
- les éléments relatifs à la sûreté : **RUE 2015/1998** [1]**, l'arrêté du 11 septembre 2013** [38] relatif aux mesures de sûreté de l'aviation civile et **le code des transports** [39] **;**
- ou **les deux.**

En annexe, se trouvent :

- une liste de bonnes pratiques pour la mise en œuvre des dispositions du présent document ;
- les listes des fonctions essentielles pour l'appréciation du risque ;
- la matrice de conformité précisant les dispositions du document s'appliquant selon les cas;
- les définitions de certains termes utilisés dans le document ;
- les acronymes utilisés dans le document ;
- les références à des productions mentionnées dans le document.

2.4. Mise en œuvre

L'application de la Partie – IS est une condition de maintien des certificats/agréments des organismes.

La Part-IS exige en particulier la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) dont les principes sont similaires à ceux d'un Système de Gestion de la Sécurité (SGS) tel qu'exigé dans les règlements Partie – 21, ADR, CAMO, 145, ORO, ORA, ATCO et ATM/ANS.

Bien qu'aucun règlement n'impose d'intégrer les systèmes de management, en l'occurrence SMSI et SGS, l'organisme peut choisir de mettre en œuvre un système de gestion intégré couvrant à la fois la sécurité aérienne et la sécurité de l'information.

En fonction de l'organisation de l'organisme, cette option peut permettre d'optimiser les ressources et l'efficacité globale de la mise en œuvre de la Partie – IS, en complétant ou en adaptant les éléments existants du système de gestion de la sécurité lorsque cela est pertinent (organisations, politiques, procédures, etc.).

Dans tous les cas, l'organisme veille à articuler son SMSI avec son SGS.

3. Gouvernance

3.1. Engagement du Dirigeant Responsable

IS.I/D.OR 200 a) 1)

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.

L'engagement du Dirigeant Responsable est formalisé et intégré ou référencé dans :
- le manuel du système de management de la sécurité de l'information, ou ;
- le manuel du système de gestion de la sécurité de l'organisme.

3.2. Politique de sécurité de l'information

3.2.1. Stratégie et objectifs de sécurité de l'information

IS.I/D.OR 200 a) 1)

Le Dirigeant Responsable définit et approuve une politique de sécurité de l'information :
- qui précise le périmètre du SMSI tel que défini au §4.1 et ;
- 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

IS.I/D.OR 200 a) 1)

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

IS.I/D.OR 200 d)

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

IS.I/D.OR 240 a) 2)

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 du système de gestion de la sécurité de l'organisme.

3.3. Gestion des ressources, rôles et responsabilités

IS.I/D.OR.240 a) 1) et 3)
IS.I/D.OR 240 b), c), e) et f)

Le Dirigeant Responsable :
- est capable de démontrer sa connaissance du règlement Partie – 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 en veillant à :
    - désigner une personne ou un groupe de personnes responsables :
        - de la mise en œuvre du règlement Partie – 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 Partie – 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 du système de gestion de la sécurité de l'organisme.

IS.I/D.OR 240 d) et e)

Dans le cas où l'organisme partage des structures organisationnelles, des politiques, des processus et des procédures en matière de sécurité de l'information avec d'autres organismes ou avec des secteurs de sa propre organisation qui ne font pas partie de l'agrément ou du certificat, le Dirigeant Responsable peut déléguer ses activités à une personne responsable commune, alors :
- La personne responsable commune :
    - est nommée formellement ;
    - a un accès direct au Dirigeant Responsable ;
    - est capable de démontrer sa connaissance du règlement Partie-IS ;
    - définit et approuve la politique de sécurité de l'information ;
    - désigne une personne ou un groupe de personnes responsables de la mise en œuvre du règlement Partie – IS, qui :
        - a un accès direct à la personne responsable commune ;
        - 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.
- Le dirigeant responsable :
    - désigne formellement la personne responsable commune ;
    - endosse la politique de la personne responsable commune et s'engage à la faire appliquer sur son périmètre.
- La personne responsable commun et le dirigeant responsable :
    - établissent et sont capables de démontrer leurs connaissances du périmètre de responsabilité et les limites de l'organisation mise en place ;
    - gèrent de manière proactive les problèmes ;
    - documentent et traitent tout signe avant-coureur de non-conformité.

4. Gestion des risques de sécurité de l'information

IS.I/D.OR 205 c) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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 utilisé pour mener à bien ces activités et 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 du système de gestion de la sécurité de l'organisme, 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.

➔ Bonne pratique n°1 : Méthodologie et standard pour la gestion des risques de sécurité de l'information

4.1. Établissement du contexte

IS.I/D.OR 205 a) 1) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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, l'organisme peut s'appuyer sur les listes de fonctions essentielles fournies en annexe II et annexe III.

De plus, l'organisme définit des échelles :

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

➔ Bonne pratique n°2 : Définition du périmètre de la gestion des risques de sécurité de l'information et du SMSI

➔ Bonne pratique n°3 : Définition des échelles pour la gestion des risques

4.2. Appréciation des risques

4.2.1. Identification des risques

IS.I/D.OR 205 a) et b) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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 ;
  - clients ;
  - partenaires ;
  - 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.

➔ Bonne pratique n°4 : Détermination du socle de cybersécurité et des écarts

4.2.2. Analyse des risques

IS.I/D.OR 205 c) 1) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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.

IS.I/D.OR 205 e)

Uniquement à destination des organismes redevables de la Partie – ATM/ANS : Les organismes tenus de se conformer à la sous-partie C de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) 2017/373 remplacent l'analyse des risques par une analyse de l'impact sur leurs services dans le cadre de l'évaluation du support à la sécurité requise par le point ATM/ANS.OR.C.005.

4.2.3.Évaluation des risques

IS.I/D.OR 205 c) 1) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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

IS.I/D.OR 205 c) 2) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*
IS.I/D.OR 210 b) *AIM – DR-1-7-1 (I)*

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 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.

IS.I/D.OR 205 e)

Uniquement à destination des organismes redevables de la Partie – ATM/ANS : Les organismes tenus de se conformer à la sous-partie C de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) 2017/373 mettent les résultats de l'appréciation des risques à disposition des prestataires de services de la circulation aérienne auxquels ils fournissent des services.

Les prestataires de services de la circulation aérienne sont alors chargés d'évaluer l'impact sur la sécurité aérienne.

4.3. Traitement des risques

4.3.1. Mesures pour le traitement du risque

IS.I/D.OR 210 a) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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.

4.3.2. Élaboration du plan de traitement des risques

IS.I/D.OR 210 a) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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 ;
- le responsable de la mise en œuvre de la mesure de sécurité de l'information ;
- 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

IS.I/D.OR 210 a) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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

IS.I/D.OR 210 b) *Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3*

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

IS.I/D.OR 200 a) 5) *Règlement (UE) n°2015/1998 –1.7.2*

L'organisme définit, met en œuvre et formalise les mesures techniques et organisationnelles visant à :
- détecter les 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.

➔ Bonne pratique n°5 : Mesures de gestion des incidents de sécurité de l'information

4.4.1. Détection des incidents de sécurité de l'information

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

IS.I/D.OR 220 a)

L'organisme établit 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.

➔ Bonne pratique n°6 : Identification des incidents redoutés de sécurité de l'information

4.4.1.2. Sources de collecte des événements

4.4.1.2.1. Sources de collecte automatique d'événements

IS.I/D.OR 220 a)

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.

➔ Bonne pratique n°7 : Sources de collecte automatique des événements de sécurité de l'information

4.4.1.2.2. Report interne des événements

IS.I/D.OR 215 a), b) 1) et e)

L'organisme met en place un système de report interne des événements de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne. Ce système :
- identifie les événements qui doivent être reportés, à savoir les événements de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne ;
- précise les moyens mis à disposition pour reporter un événement ainsi que les délais ;
- est accessible aux personnes ayant besoin d'en connaitre parmi :
  - son personnel interne ;
  - les tiers pertinents dans le contexte, identifiés au §4.2.1 ;
  - tous les interlocuteurs pertinents.

L'organisme :
- peut intégrer ce système de report interne des 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 du système de gestion de la sécurité de l'organisme.

4.4.1.3. Stratégie de détection des événements

IS.I/D.OR 215 b) 3)

L'organisme met en place une stratégie de détection des événements de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne. Cette stratégie :

- définit, sur la base de son appréciation des risques, une classification par ordre de gravité des événements de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne ;
- définit des règles de détection s'appuyant sur :
  - les sources de collecte définies précédemment ;
  - la liste des incidents de sécurité redoutés identifiés précédemment ;
  - des bases de connaissances internes et externes.
- définit des règles de conservation des événements qui précisent :
  - les critères de conservation ;
  - la durée de conservation ;
  - la fréquence de réévaluation ;
  - les critères de suppression.
- assure la centralisation et la corrélation des événements ;
- permet de recenser les écarts par rapport aux valeurs de référence prédéterminées en matière de performances fonctionnelle.

➔ Bonne pratique n°8 : Définition des règles de détection des événements

4.4.1.4. Evaluation et qualification des incidents de sécurité et vulnérabilités

IS.I/D.OR 215 b) 2)

L'organisme met en place une procédure d'évaluation et de qualification des événements détectés ayant un potentiel impact sur la sécurité aérienne. Cette procédure :

- identifie le périmètre de l'événement détecté ;
- identifie les impacts et la gravité en matière de sécurité aérienne ;
- détermine les causes de l'événement détecté ;
- identifie les éventuelles parties prenantes en interne et/ou externes concernées par l'événement détecté ;
- évalue si l'événement détecté peut être qualifié en incident ou vulnérabilité.

4.4.1.5. Notification des incidents de sécurité

IS.I/D.OR 215 b) 4)
IS.I/D.OR 220 a) 2)
IS.I/D.OR 230 b) et c) 1)

Dès qu'un événement est qualifié en incident de sécurité, l'organisme notifie :

- les personnes pertinentes au sein de son organisation pour activer les réactions appropriées ;
- l'autorité compétente selon le cade défini au §4.4.4 ;
- le cas échéant les partenaires externes concernés selon le cadre défini au §4.5.1.

4.4.2.Réponse aux incidents de sécurité de l'information

IS.I/D.OR 220 b)

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, notamment les outils et les délais.
- définit les actions immédiates à mettre en œuvre et leurs délais en identifiant :
  - les ressources à activer au sein et à l'extérieur de l'organisme ;
  - 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.

➔ Bonne pratique n°9 : Définition des actions immédiates pour répondre à un incident de sécurité

4.4.3.Remédiation

IS.I/D.OR 220 c)

L'organisme définit une procédure de remédiation à la suite d'un incident de sécurité de l'information qui :
- précise les rôles et les responsabilités des personnes qui gèrent les actions de remédiation ;
- définit comment identifier le périmètre du système d'information impacté ;
- définit les actions de remédiation à mettre en œuvre pour retourner à un état sûr et en précise :
  - les priorités ;
  - les ressources à activer.
- détermine les objectifs de délais de remise en service en fonction du niveau de gravité, de la nature et du contexte de l'incident.

➔ Bonne pratique n°10 : Définition des actions de remédiation à la suite d'un incident de sécurité

4.4.4.Notification à l'autorité compétente

IS.I/D.OR 230 a), b) et c)

Lorsqu'un événement de sécurité de l'information est qualifié en incident ou vulnérabilité de sécurité de l'information ayant un potentiel impact significatif sur la sécurité aérienne, alors l'incident ou la vulnérabilité est à considérer comme un événement de sécurité aérienne.

Ainsi, l'organisme articule sa gestion des risques de sécurité de l'information avec le mécanisme de comptes rendus externes mis en place dans le cadre de son SGS ou de son processus de suivi de navigabilité.

Dans le cas où les éléments nécessaires à la notification et ceux présents dans les rapports suivants présentent une certaine sensibilité pour l'organisme, alors il transmet :
- uniquement les éléments non sensibles via ECCAIRS2 ;
- les éléments les plus sensibles par des moyens sécurisés distincts en rappelant la référence de la notification dans ECCAIRS2.

➔ Bonne pratique n°11 : Envoi sécurisé d'éléments sensibles pour la notification à l'autorité compétente

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

AIM – B-2
AIM – B-4

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 ;
        - 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

IS.I/D.OR 200 a) 13)
IS.I/D.OR 215 c) et d)

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 Partie – 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 ;
    - le report des événements de sécurité de l'information ayant un potentiel impact significatif 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.

IS.I/D.OR 230 a), b) et c)

Lorsque l'organisme dispose d'une interface avec un organisme titulaire d'un agrément de conception ou responsable de la conception d'un système ou d'un composant, alors il intègre dans son cadre de travail :

- la notification des incidents ou vulnérabilités ayant un potentiel impact significatif sur la sécurité aérienne affectant :
    - un aéronef ou un système ou élément associé, au titulaire de l'agrément de conception ;
    - un système ou un composant utilisé par l'organisme, au responsable de la conception du système ou du composant.
- la soumission d'un compte rendu :
    - au titulaire de l'agrément de conception ou à l'organisme responsable de la conception du système ou du composant ;
    - dès que possible, mais sans dépasser 72 heures à compter du moment où l'organisme a eu connaissance de la situation, sauf si des circonstances exceptionnelles l'empêchent.
- la soumission d'un rapport de suivi :
    - au titulaire de l'agrément de conception ou à l'organisme responsable de la conception du système ou du composant ;
    - précisant les mesures que l'organisme :
        - a prises ou a l'intention de prendre pour le rétablissement après l'incident et ;
        - a l'intention de prendre pour prévenir de tels incidents de sécurité de l'information.

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

IS.I/D.OR 200 a) 13)
IS.I/D.OR 215 c) et d)

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 Partie – IS ;
- définit :
  - Lorsque cela est possible, un cadre de travail avec ces derniers qui prévoit :
    - Le report des événements de sécurité de l'information ayant un potentiel impact significatif 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 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.

➔ Bonne pratique n°12 : Référentiels techniques pour la gestion des tiers

4.5.2.Sous-traitance d'activités du SMSI

IS.I/D.OR 235 a) et b)

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.

Lorsqu'il fait appel à la sous-traitance dans ce cadre, 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 significatif 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.

➔ Bonne pratique n°13 : Sous-traitance des activités du SMSI

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

Règlement (UE) n°2015/1998 – 11.1.2 c)

Sur la base de son analyse de risques, l'organisme identifie ou fait identifier par les tiers déterminés au §4.2,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

Règlement (UE) n°2015/1998 – 11.1.2 c), 11.1.3 et 11.1.7
Code des transports : L 6342-3, R 6342-32 et R 6342-33

L'organisme applique ou fait appliquer par les tiers identifiés au §4.2., 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[2] éventuelles de ces personnes dans les États où elles ont résidé[3] 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.

[2] « Interruption » : Toute interruption de plus de vingt-huit jours dans le relevé de la formation initiale ou de la carrière.
[3] « 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

IS.I/D.OR 240 i)

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 ;
    - vérifier les antécédents de ces personnes.

L'organisme :

- applique ou fait appliquer par les tiers identifiés au §4.2, 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 du système de gestion de la sécurité de l'organisme.
- 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.

➔ Bonne pratique n°14 : Vérification des antécédents pour le contrôle de la fiabilité des personnels

5.1.3.Cas particuliers

5.1.3.1. Personnels soumis aux exigences de sûreté et de sécurité

Règlement (UE) n°2015/1998 – 11.1.2 c), 11.1.3 et 11.1.7
Code des transports : L 6342-3 , R 6342-32 et R 6342-33

IS.I/D.OR 240 i)

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

Règlement (UE) n°2015/1998 – 11.1.2 c), 11.1.3 et 11.1.7
Code des transports : L 6342-3, R 6342-32 et R 6342-33

IS.I/D.OR 240 i)

Lorsqu'un organisme emploie du personnel de nationalité étrangère ne résidant pas en France pour lequel il est justifié qu'il n'est pas possible de réaliser une vérification des antécédents, alors l'organisme exige que lui soit fourni :

- une pièce d'identité officielle de l'employé permettant de vérifier son identité, et ;
- lorsqu'il est nécessaire de vérifier les antécédents :
  - un document similaire à un extrait de casier judiciaire pour les pays en mesure de fournir ce type de document ;
  - ou en l'absence de document similaire, un engagement signé par l'employé, de bonne conduite lors de la réalisation de missions pour le compte de l'organisme.

L'organisme :

- tient à jour une liste des employés étrangers pour lesquels la vérification des antécédents n'a pu être réalisée ;
- précise pour chaque employé les actions mises en œuvre pour s'assurer de leur fiabilité.

Note : Sous réserve des lois applicables, certains pays peuvent fournir sur demande de l'employeur un extrait de casier judiciaire de leurs citoyens en cours de recrutement chez cet employeur (Ex. Maroc, Inde). L'extrait du casier judiciaire fourni peut être similaire, voire plus fourni qu'un casier judiciaire français. La demande est d'autant plus facilitée lorsque l'employeur est implanté dans ce pays

5.2. Sensibilisation

Règlement (UE) n°2015/1998 – 11.2.1.4, 11.2.8.1 et 11.2.8.2
AIM 11-2-1-4 et 11-2-1-5

IS.I/D.OR 240 h)

L'organisme met en œuvre une campagne de sensibilisation ou s'assure de cette mise en œuvre par les tiers identifiés au §4.2, 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) 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 du système de gestion de la sécurité de l'organisme, et/ou ;
  - le programme de sûreté.
- conserve des informations documentées appropriées comme preuves du suivi de la sensibilisation de son personnel.

➔ Bonne pratique n°15 : Conception de sessions de sensibilisation cybersécurité

5.3. Formation

Règlement (UE) n°2015/1998 – 11.2.1.4, 11.2.8.1 et 11.2.8.2
AIM 11-2-1-4 et 11-2-1-5

IS.I/D.OR 240 g)

L'organisme met en œuvre un programme de formation ou s'assure de cette mise en œuvre par les tiers identifiés au §4.2., 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 du système de gestion de la sécurité de l'organisme, et/ou ;
  - le programme de sûreté.
- conserve des informations documentées appropriées comme preuves de suivi de la formation de son personnel.

➔ Bonne pratique n°16 : Formation cybersécurité

6. Définition et fonctionnement du SMSI

6.1. Suivi de la gestion des risques de sécurité de l'information

6.1.1. Organisation du suivi de la gestion des risques de sécurité de l'information

IS.I/D.OR 200 a) 2) à 6) et 8) à 10)
IS.I/D.OR 205 d)
Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3
AIM – DR 1-7-1 (II)

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 voire l'intégration 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 de sécurité de l'information

IS.I/D.OR 200 a) 2) à 6) et 8) à 10)
IS.I/D.OR 205 d)
Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3
AIM – DR 1-7-1 (II) et B-3

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 de sécurité de l'information

IS.I/D.OR 200 a) 2) à 6) et 8) à 10)
IS.I/D.OR 205 d)
Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3
AIM – DR 1-7-1 (II)

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 du système de gestion de la sécurité de l'organisme, 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

IS.I/D.OR 200 a) 12)

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 en s'assurant que les personnes en charge de l'évaluation soient indépendantes de celles en charge de la mise en œuvre du SMSI ;
- l'articulation voire l'intégration 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

IS.I/D.OR 200 a) 12)

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 Partie – IS.

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

IS.I/D.OR 200 a) 12)

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 du système de gestion de la sécurité de l'organisme.
- 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

IS.I/D.OR 200 a) 7)
IS.I/D.OR 225 a) et b)

L'organisme répond aux non-conformités notifiées par l'autorité compétente au travers du processus de traitement des constatations prévus dans le cadre de son certificat ou de son 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

IS.I/D.OR 260 a)

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 voire l'intégration 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.

➔ Bonne pratique n°17 : Modèle de maturité du SMSI

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

IS.I/D.OR 260 a)

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

IS.I/D.OR 260 a)

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 du système de gestion de la sécurité de l'organisme.
- conserve des informations documentées comme preuves des résultats de l'évaluation de l'efficacité et de la maturité du SMSI.

6.3. Amélioration continue du SMSI

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

IS.I/D.OR 200 b)
IS.I/D.OR 260 b)

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 voire l'intégration 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 :
    - la fréquence entre 2 audits de l'autorité compétente, et/ou ;
    - les événements significatifs déclenchant la revue de direction (incident, changement de contexte etc.).

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

IS.I/D.OR 200 b)
IS.I/D.OR 260 b)

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 compétente 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.

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

IS.I/D.OR 200 b)
IS.I/D.OR 260 b)

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 du système de gestion de la sécurité de l'organisme.
- 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

IS.I/D.OR 200 c)
IS.I/D.OR 250 c)
IS.I/D.OR 255 a)

L'organisme définit une procédure de « Gestion des modifications du SMSI non soumises à approbation ».

Cette procédure :

- est approuvée par l'autorité compétente ;
- précise la méthode de classification des changements entre ceux « soumis à approbation préalable » et ceux « soumis à notification » ;
- intègre la réalisation d'une analyse du risque « cybersécurité » pour tout changement du SMSI ;
- intègre les changements suivants :
    - Les changements de méthodes d'analyse du risque « cybersécurité » pour tout changement SMSI ;
    - Les changements de processus de notification des évènements ;
    - La modification du manuel SMSI (hors changement soumis à approbation).

L'organisme peut intégrer cette procédure à celle déjà existante dans le SGS.

IS.I/D.OR 200 c)
IS.I/D.OR 250 c)
IS.I/D.OR 255 b)

Les modifications suivantes sont soumises à l'approbation de l'autorité compétente :

- Les changements majeurs de la chaine de responsabilité au sein du SMSI, faisant apparaître :
    - le responsable SMSI ;
    - le responsable de la conformité du SMSI ;
    - le cas échéant, la personne responsable commune.
- Les changements majeurs de la politique de sécurité de l'information ayant un impact potentiel sur la sécurité aérienne ;
- Les changements majeurs relatifs à la procédure de « Gestion des modifications du SMSI non soumises à approbation ».

L'organisme intègre ou fait référence à ces modifications soumises à approbation de l'autorité compétente dans :

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

7. Archivage

7.1. Procédure de conservation des enregistrements

IS.I/D.OR 200 a) 11)
IS.I/D.OR 245 c) et d)

L'organisme :
- met à jour sa procédure de conservation des enregistrements pour :
  - intégrer les éléments précisés au §7.2 ;
  - intégrer des moyens de protection proportionnels à la sensibilité des documents et au besoin de disponibilité ;
  - prévoir la destruction de ces documents et la mise au rebut des moyens de stockage utilisés lorsque l'archivage n'est plus nécessaire. La sécurisation des destructions et mises au rebut est proportionnelle à la sensibilité des documents et contenus des moyens de stockage concernés.
- intègre la gestion de ces documents dans le périmètre de son SMSI ;
- intègre ou fait référence à cette procédure dans :
  - le manuel du système de management de la sécurité de l'information, ou ;
  - le manuel du système de gestion de la sécurité de l'organisme.

7.2. Enregistrements à conserver

IS.I/D.OR 200 a) 11)
IS.I/D.OR 245 a) et b)

Documents	Durée d'archivage
Tout agrément ou certificat délivré par l'autorité compétente	Au moins 5 ans après la fin de validité de l'agrément ou du certificat
Toute autorisation de dispense délivrée par l'autorité compétente ainsi que le formulaire de dispense associé	Au moins 5 ans après la fin de validité de la dispense
Les contrats relatifs à la sous-traitance des activités du SMSI	Au moins 5 ans après la modification ou la fin du contrat
Les documents relatifs aux processus clés de gestion des risques de sécurité de l'information - Appréciation, traitement des risques et suivi de la gestion des risques - Gestion des incidents de sécurité de l'information - Gestion des risques induits par les tiers - Gestion des personnels et des compétences - Évaluation du SMSI	Au moins 5 ans après la création du document
Les documents relatifs à l'appréciation des risques : - Les échelles de gravité et de vraisemblance (ou occurrence) - Les critères d'acceptation du risque - Liste des risques de sécurité de l'information relatifs à la sécurité aérienne et les informations associées - Liste des organismes en interface présentant un risque pour la sécurité aérienne	Au moins 5 ans après la création du document
Les documents relatifs au traitement des risques : - Le plan de traitement des risques - La liste des risques résiduels après application du plan de traitement	Au moins 5 ans après la création du document
Les documents relatifs au report interne des événements et des vulnérabilités de sécurité de l'information	Au moins 5 ans après la création du document
Les documents relatifs à la notification externe	Au moins 5 ans après la création du document
Les documents relatifs aux événements liés à la sécurité de l'information qui pourraient devoir être réévalués pour révéler des incidents ou des vulnérabilités en matière de sécurité de l'information non détectés	La durée de rétention est celle précisée dans les procédures de gestion des incidents (§4.4.1.3)
Les documents relatifs aux qualifications et à l'expérience liées à la sécurité de l'information du personnel	Tant que la personne travaille pour l'organisme ET au moins 3 ans après que la personne a quitté l'organisme

8. Documentation

8.1. Programme de sûreté

Règlement (UE) n°2015/1998 – 1.7.1, 1.7.2 et 1.7.3

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

Documents	Chapitres 3CFv3
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
Tous les documents relatifs aux processus, procédures, rôles et responsabilités clés mis en œuvre pour se mettre en conformité au règlement (UE) n°2015/1998 [1]	

➔ Bonne pratique n°18 : Exemples d'éléments ou de références dans le programme de sûreté

8.2. Manuel de management de la sécurité de l'information

IS.I/D.OR 250 a) et d)

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 du système de gestion de la sécurité de l'organisme.

Documents	Chapitres 3CFv3
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 système de report interne des événements de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne	4.4.1.2.2
La procédure de gestion des sous-traitants réalisant des activités du SMSI	4.5.2
La procédure de gestion des modifications du SMSI non soumise à approbation	6.4
Tous les documents relatifs aux processus, procédures, rôles et responsabilités clés mis en œuvre pour se mettre en conformité aux règlements Partie – IS [2,3]	

➔ Bonne pratique n°19 : Exemples d'éléments ou de références dans le manuel SMSI ou de l'organisme approuvé/certifié

Annexes

Annexe I : Bonnes pratiques

Bonne pratique n°1 : Méthodologie et standard pour la gestion des risques de sécurité de l'information

Dans le cadre de la gestion de ces risques de sécurité de l'information, il est recommandé de s'appuyer sur une méthodologie ou un standard reconnu pour mener à bien ses activités de gestion des risques. De cette manière l'organisme n'aura pas à prouver la conformité de la méthodologie ou du standard utilisé. Ci-après une liste non exhaustive de méthodologies ou standards reconnus :

- EBIOS Risk Manager : Cette méthode, développée par l'ANSSI est souvent utilisée dans l'écosystème français et permet l'articulation avec les méthodes d'analyse de risques issues de la sécurité aérienne :
  - Guides EBIOS Risk Manager, ANSSI, Version 1.5, Mars 2024 [17].
- ISO/CEI 27005 : Standard international de gestion des risques liés à la sécurité de l'information largement reconnu et éprouvé :
  - 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 [18].
- Méthodologie d'analyse de risque OACI/ GCRC : Méthode développée par l'OACI et publiée dans le document GCRC permettant l'intégration de la cybersécurité dans les méthodes de gestion des risques de sécurité aérienne, ou de sûreté aérienne, ou de capacité/efficacité de la navigation aérienne :
  - Méthodologie d'analyse de risque OACI/ GCRC [19].
- Toute autre méthode conforme à la norme ISO/CEI 31000, norme relative à la gestion des risques :
  - Norme internationale ISO/IEC 31000:2018 – Management du risque - Lignes directrices [20].

Bonne pratique n°2 : Définition du périmètre de la gestion des risques de sécurité de l'information et du SMSI

Afin de définir le périmètre de son analyse de risques et/ou de son SMSI, il est recommandé de s'appuyer sur :

- les listes de fonctions relatives à la sûreté et/ou sécurité aérienne précisées en annexe II et annexe III ;
- 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 :
  - White paper: Identification and Classification guidance for Partie – IS assets - ED/DO-ISMS Guidance for Aviation, EUROCAE WG-72 / RTCA SC-216, 2023. [21] *Le document est disponible sur demande.*

Bonne pratique n°3 : Définition des échelles pour la gestion des risques

Dans le cadre de la gestion des risques de sécurité de l'information, il est nécessaire de définir différentes échelles qui permettent une comparaison des résultats à chaque itération. Afin d'y parvenir, il est recommandé de s'appuyer sur les référentiels suivants ou de s'en inspirer :

- Guides EBIOS Risk Manager, ANSSI, Version 1.5, Mars 2024 [17] – page 26 ;
- ICAO Doc 9859 Safety Risk Tolerability [22] ;
- ICAO Doc 10108 Aviation Security Global Risk Statement [23].

Bonne pratique n°4 : Détermination du socle de cybersécurité et des écarts

Lors de l'identification des risques, il est recommandé de :

- définir son **socle de sécurité**, à savoir l'ensemble des référentiels de cybersécurité s'appliquant aux activités de l'organisme. Ces référentiels peuvent être :
  - des règles d'hygiène informatique et bonnes pratiques de sécurité [24] : guides de recommandations de l'ANSSI, règles de sécurité internes à l'organisation, etc. ;
  - des normes : ISO/IEC 27002:2022 [25], etc. ;
  - des dispositifs règlementaires techniques : Loi de Programmation Militaire, Transposition des directives NIS 1 et 2, l'II 901, l'IGI 1300, etc.
- identifier les écarts par rapport à ce socle de cybersécurité afin d'avoir une image claire de sa situation en matière de protection aux risques de sécurité de l'information et ainsi mieux déterminer les risques pesant sur l'organisme.

De plus, le socle de sécurité est alimenté lors de chaque itération d'appréciation et de traitement des risques. Il est donc recommandé d'adopter une stratégie en augmentant progressivement le niveau des exigences de ce socle de cybersécurité :

- Étape 1 : Considérer le guide d'hygiène de l'ANSSI comme socle de cybersécurité de base et viser la conformité aux 42 mesures :
  - Guide d'hygiène informatique, ANSSI, Version 2.0, Septembre 2017 [24].
- Étape 2 : Considérer un référentiel plus exigeant telles que :
  - les mesures de la Norme internationale ISO/IEC 27002:2022 [25] ;
  - les mesures de la Norme internationale ISO/ISA/IEC 62443 [26] ;
  - les mesures techniques de la Loi de Programmation Militaire [14] si applicables ;
  - les mesures techniques des transpositions des directives NIS 1 [15] et/ou 2 [42] si applicables.

Bonne pratiques n°5 : Mesures de gestion des incidents de sécurité de l'information

Afin de déterminer les mesures techniques et organisationnelles visant à détecter, réagir et se rétablir à la suite d'un incident, il est recommandé de s'appuyer sur les référentiels suivants :

- les guides et bonnes pratiques publiées par l'ANSSI ;
- les mesures de la Norme internationale ISO/IEC 27002:2022 [25]
- ED-206 - Guidance on Security Event Management, EUROCAE, 2022 [27]

Bonne pratiques n°6 : Identification des incidents redoutés de sécurité de l'information

Afin d'identifier les incidents redoutés de sécurité de l'information ayant un potentiel impact sur la sécurité aérienne, il est recommandé de s'appuyer sur un ou plusieurs référentiels, tels que :

- Les événements devant obligatoirement être notifiés à l'autorité précisés dans le règlement (UE) 2015/1018 ;
- Prestataires de détection des incidents de sécurité - Référentiel d'exigences, ANSSI, 2017 – IV.2.2. b) [28] ;
- 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 [29] ;
- Norme internationale ISO/IEC 27035:2023 – Technologies de l'information - Gestion des incidents de sécurité de l'information – Annexe B [30] ;
- ED Decision 2023/009/R - Appendix I – Examples of threat scenarios with a potential harmful impact on safety [31] ;
- Mitre Attack – Référence les tactiques et techniques mises en œuvre dans le cadre de scénarios d'attaques.

Bonne pratique n°7 : Sources de collecte automatique des événements de sécurité de l'information

Lors de la mise en place d'une stratégie de collecte des événements de sécurité de l'information, il est recommandé de s'appuyer sur les référentiels suivants :

- Prestataires de détection des incidents de sécurité - Référentiel d'exigences, ANSSI, 2017 – IV.2.2. c) [28] ;
- Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, version 2 ,2022, ANSSI [32] ;
- ED-206 - Guidance on Security Event Management, EUROCAE, 2022 [27].

Bonne pratique n°8 : Définition des règles de détection

Lors de la définition des règles de détection, il est recommandé de :

- s'appuyer sur des bases de connaissances :
  - internes :
    - Les résultats d'audits ;
    - Les tests d'intrusion, les balayages de vulnérabilités et les risques liés aux évènements redoutés.
  - externes :
    - Une veille sur la menace et les vulnérabilités ;
    - Les incidents de sécurité de l'information connus auprès d'autres organismes ;
    - Les bases de connaissance acquises auprès des partenaires extérieurs.
- De formaliser ces règles, en précisant pour chacune d'entre elles :
  - les moyens mis en œuvre pour détecter le ou les événements ;
  - une description de la règle ;
  - Le ou les incidents redoutés que la règle vise à détecter ;
  - Le niveau de gravité du ou des événements à détecter.

Bonne pratique n°9 : Actions immédiates pour répondre à un incident de sécurité de l'information

Lors de la définition des actions immédiates à mettre en œuvre pour répondre à un incident de sécurité, il est recommandé d'identifier :

- les ressources à activer au sein et à l'extérieur de l'entreprise, notamment dans le cadre :
  - d'un *Security Operation Center* ;
  - d'un contrat avec un Prestataire de Réponse à Incident de Sécurité (PRIS) qualifié par l'ANSSI : https://cyber.gouv.fr/produits-services-qualifies;
  - ou de l'adhésion à un CERT :
    - CERT Aviation France[4] ;
    - CERT – FR[5] ;
    - CSIRT[6].
- Les mesures techniques et organisationnelles pouvant être mises en œuvre pour limiter la propagation d'une attaque et éviter la matérialisation du ou des incidents redoutés. L'organisme peut s'appuyer sur :
  - Guide ANSSI cyberattaques et remédiation : Piloter la remédiation [33] – page 33 – 34 – 35 ;
  - ED-206 - Guidance on Security Event Management, EUROCAE, 2022 [27] ;
  - Guidance on Aviation Cybersecurity Incident Response & Recovery – OACI (à paraitre).

Bonne pratique n°10 : Définition des actions de remédiation à la suite d'un incident de sécurité

Lors de l'élaboration de la procédure de remédiation, il est recommandé de s'appuyer sur :

- Guide ANSSI cyberattaques et remédiation : Piloter la remédiation [33] ;
- ED-206 - Guidance on Security Event Management, EUROCAE, 2022 [27] ;
- Guidance on Aviation Cybersecurity Incident Response & Recovery – OACI (à paraitre).

Bonne pratique n°11 : Envoi sécurisé d'éléments sensibles pour la notification à l'autorité compétente

Lorsque l'organisme estime que des éléments sensibles doivent être transmis à l'autorité compétente, il est recommandé de :

- chiffrer les éléments via une solution sécurisée :
  - Conteneur Zed ! avec un mot de passe unique et robuste.
- transmettre le secret et la clé pour accéder au secret par 2 moyens de communication différents :
  - Secret : Conteneur Zed ! par mail ;
  - Clé : Mot de passe par :
    - une application de messagerie chiffrée, ou ;
    - en mode dégradé par SMS, téléphone ou main propre.

L'organisme se rapproche de l'entité en charge de son certificat/agrément (DSAC – IR, DSAC – EC et/ou OSAC) pour définir les modalités d'envoi sécurisé.

[4] CERT Aviation France : https://www.cert-aviation.fr/
[5] CERT – FR : https://www.cert.ssi.gouv.fr/
[6] CSIRT Territoriaux : https://cyber.gouv.fr/csirt-territoriaux

Bonne pratique n°12 : Référentiels techniques pour la gestion des tiers

Dans le cadre de la gestion des tiers, il est recommandé de s'appuyer sur des référentiels d'exigences techniques tels que :

- Outil de Maturité AirCyber, Boostaerospace, 2023 [34] ;
- Standard ISO 27001 [16].

Bonne pratique n°13 : Sous-traitance des activités du SMSI

En France, l'ANSSI délivre des qualifications à des société de service, qui offrent des garanties de qualité de prestation en matière de sécurité de l'information aux clients qui font appels à eux. La liste de ces prestataires et des référentiels auxquels ils doivent se mettre en conformité sont disponibles sur le site de l'ANSSI : https://cyber.gouv.fr/produits-services-qualifies.

Si un organisme sous-traite certaines activités de son SMSI, il est recommandé de faire appel à un prestataire qualifié par l'ANSSI. Ce dernier est alors considéré comme conforme aux exigences des règlements Partie – IS (IS.I/D.OR.250) à condition que soient également prévues :

- la possibilité pour l'autorité compétente d'avoir accès au sous-traitant ;
- le report 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.

Bonne pratique n°14 : Vérification des antécédents pour le contrôle de la fiabilité des personnels

Lorsque la politique conclut qu'il est nécessaire pour l'organisme de vérifier les antécédents de certaines personnes, il est recommandé de s'appuyer sur des dispositifs existants tels que :

- l'habilitation préfectorale accordée dans le cadre de la délivrance d'un titre de circulation aéroportuaire ;
- la fourniture de l'extrait de casier judiciaire (bulletin numéro 3) ;
- le dispositif de protection des secrets de Défense Nationale, lorsque le statut de l'organisme le permet ;
- tout autre dispositif existant et répondant aux objectifs de contrôle de la fiabilité.

Bonne pratique n°15 : Conception de sessions de sensibilisation cybersécurité

Lors de l'élaboration des sessions de sensibilisation pour ses personnels, il est recommandé de s'appuyer sur le guide de conception de sessions de sensibilisation cybersécurité de la DSAC [35].

Bonne pratique n°16 : Conception du programme de formation pour les personnels

Lors de l'élaboration du programme de formation pour ses personnels, il est recommandé de s'appuyer sur le guide de formation cybersécurité de la DSAC [36].

Bonne pratique n°17 : Modèle de maturité du SMSI

Dans le cadre de l'évaluation de la maturité de son SMSI, il est recommandé que l'organisme s'appuie sur un des modèles de maturité suivants :

- Cybersecurity Capability Maturity Model (C2M2), version 2.0 ;
- Cybersecurity Capability Maturity Integration ;
- Systems Security Engineering – Capability Maturity Model (SSE-CMM) ;
- NIST Cybersecurity Framework (NIST CSF), version 1.1 ;
- ATM Cybersecurity Maturity Model, edition 1 ;
- Standard ISO/IEC 27004:2016 - Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation.

Bonne pratique n°18 : Exemples d'éléments ou de références dans le programme de sûreté

Ci-après une liste non-exhaustive des éléments qui peuvent figurer ou être référencés dans le programme de sûreté.

Procédures	Chapitres 3CFv3
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

Bonne pratique n°19 : Exemples d'éléments ou de références dans le manuel SMSI ou de l'organisme approuvé/certifié

Ci-après une liste non-exhaustive des éléments qui peuvent figurer ou être référencés dans le manuel SMSI ou de l'organisme approuvé/certifié.

Procédures	Chapitres 3CFv3
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 incidents de sécurité de l'information	4.4
La procédure de notification à l'autorité compétente	4.4.5
La procédure de gestion des organismes en interface	4.5.1
La procédure de gestion des sous-traitants réalisant des activités du SMSI	4.5.2
La politique de contrôle de fiabilité du personnel	5.1.2.
La procédure de suivi de la sensibilisation	5.3
La procédure de suivi de la formation	5.4
La procédure d'évaluation de la conformité du SMSI	6.2.1
La procédure d'évaluation de l'efficacité et de la maturité du SMSI	6.2.3
La procédure d'amélioration continue	6.3
La procédure de gestion de l'archivage	7.1

Annexe II : Fonctions essentielles sûreté pour l'appréciation des risques

Fonctions	Exemples de composants (Systèmes d'information & procédures)	Règlement (UE) n°2015/1998
Contrôle des accès en partie critique	**Systèmes contribuant au contrôle des accès des personnes:** - Système de contrôle d'accès automatisés (RFiD, QR code, biométrie, etc.) ; - Système de vidéosurveillance ; - Système d'alarme (notamment pour la périmétrie ou les portes frontières).	1.2 Contrôle des accès 4.2 Protection des passagers et des bagages de cabine
Contrôle des accès des véhicules en partie critique	**Systèmes contribuant au contrôle des accès des véhicules :** Système de contrôle d'accès automatique pour les véhicules (ex : lecture de plaque).	1.2 Contrôle des accès
Inspection/filtrage des passagers et bagages cabine	**Systèmes contribuant à détecter l'intrusion d'objets prohibés par les passagers et dans les bagages cabines :** - Portique de détection de métaux (*WTMD*) ; - *Body scanner* ; - Équipement de radioscopie (*RX*) ; - Système de détection d'explosifs (*EDS*) ; - Équipement de détection de traces d'explosifs (*ETD*) ; - Équipement d'inspection filtrage des liquides, aérosols et gels (*LEDs*) ; - Analyseur de chaussures (*ShSc*).	4.1 Inspection/filtrage des passagers et des bagages de cabine
Inspection/filtrage, protection et réconciliation des bagages de soute	**Systèmes contribuant à détecter l'intrusion d'objets prohibés dans les bagages de soute :** - Équipement de radioscopie (*RX*) ; - Système de détection d'explosifs (*EDS*).	5.1 Inspection/filtrage des bagages de soute
	Systèmes et procédures contribuant à la réconciliation des passagers et bagages de soute - Système de *check in* à l'aéroport ; - Système de *check in* en ligne	5.3 Procédure de vérification de concordance entre passagers et bagages
	Systèmes et procédures contribuant à éviter ou à détecter l'accès non autorisé à des bagages de soute sécurisés : - Système de contrôle d'accès automatisés (RFiD, QR code, biométrie, etc.) ; - Système de vidéosurveillance ; - Système d'alarme.	5.2 Protection des bagages de soute
Inspection/filtrage des personnels	**Systèmes contribuant à détecter l'intrusion d'objets prohibés par les personnes autres que des passagers :** - Portique de détection de métaux (*WTMD*) ; - *Body scanner* ; - Équipement de radioscopie (*RX*) ; - Système de détection d'explosifs (*EDS*) ; - Équipement de détection de traces d'explosifs (*ETD*) ; - Équipement d'inspection filtrage des liquides, aérosols et gels (*LEDs*).	1.3 Inspection/filtrage des personnes autres que les passagers et des objets qu'elles transportent
Inspection/Filtrage des fournitures, des courriers et des matériels	**Systèmes contribuant à détecter l'intrusion d'objets prohibés** - Équipement de radioscopie (*RX*) ; - Système de détection d'explosifs (*EDS*) ; - Équipement de détection de traces d'explosifs (*ETD*).	6.1 Contrôles de sûreté 6.3 Agents habilités 7.1 Courrier des transporteurs aériens et matériel des transporteurs aériens destinés à être chargés sur un aéronef 8.1 Contrôles de sûreté 9.1 Contrôles de sûreté
Protection des entrepôts de fret et de fournitures sécurisés	**Systèmes et procédures contribuant à éviter ou à détecter l'accès non autorisé au fret et aux fournitures sécurisés :** - Système de contrôle d'accès automatisés ; - Système de vidéosurveillance ; - Système d'alarme.	1 Sûreté dans les aéroports 6 Fret et courrier 8 Approvisionnement de bord (Selon les organisations concernées) 9.2 Protection des fournitures d'aéroports

Protection de l'information (Physique ou logique)	**Systèmes et procédures de traitement et de stockage des données relatives à la vérification des antécédents et aux droits d'accès**	1.2 Contrôle des accès 6.3 Agents habilités 6.4 Chargeurs connus 8.1 Contrôles de sûreté 11.1 Recrutement
	Systèmes et procédures de traitement et de stockage des données relatives aux acteurs de la chaine d'approvisionnement - Base de données de l'Union sur la sûreté de la chaîne d'approvisionnement ; - Liste des fournisseurs connus ; - Listes des fournisseurs habilités.	6.3 Agents habilités 6.4 Chargeurs connus 8.1 Contrôles de sûreté 9.1 Contrôles de sûreté
	Systèmes et procédures de traitement et stockage des documents confidentiels Exemples de documents confidentiels : - Programme de sûreté de l'aérodrome ; - Programme de sûreté de du transporteur aérien ; - Programmes de sûreté des sociétés de sûreté ; - Instructions relatives aux agents de sûreté.	3 Sûreté des aéronefs 4 Passagers et bagages de cabine 5 Bagage de soute 6 Fret et courrier 7 Courrier de transporteur aérien et matériel de transporteur aérien 8 Approvisionnement de bord 9 Fournitures destinées aux aéroports
Détection et interception de drones	**Systèmes de protection contre l'intrusion de drones**	N/A

Annexe III : Fonctions essentielles sécurité aérienne pour l'appréciation des risques

Organismes de production (POA)

Fonctions	Sous-fonctions	Objectifs
Gérer la configuration et la conformité des produits	Gérer la configuration des aéronefs, des composants et des systèmes critiques*	Garantir que la configuration des aéronefs et composants reste conforme à la conception (définition approuvée)
	Assurer la conformité des produits et des composants à la conception approuvée et émettre le certificat de conformité ou le certificat libératoire autorisé	Vérifier et attester que les produits et composants respectent les définitions approuvées.
Maîtriser la qualité de la production	Industrialiser et gérer la production des aéronefs ou composants critiques*	Mettre en œuvre et contrôler les processus de fabrication pour garantir des produits et des composants conformes.
	Assurer la robustesse et la traçabilité des opérations critiques*	Garantir que toutes les opérations critiques* sont traçables (et tracées) et conformes aux exigences de sécurité.
	Gérer l'approvisionnement des pièces et matériaux critiques* et assurer la bonne réalisation des procédés sous-traités	S'assurer que les pièces et composant approvisionnés ou que les procédés sous-traités correspondent bien à la conception (définition approuvée)
	Contrôler la traçabilité des pièces et des matériaux critiques*	Vérifier que les pièces et matériaux critiques* répondent à la conception (définition approuvée)
Tester, valider et corriger les non-conformités	Tester et valider le produit et ses composants	Réaliser des tests pour garantir la conformité des produits et composants aux exigences de sécurité et/ou à la conception (définition approuvée)
	Gérer les non-conformités et mettre en œuvre les actions correctives	Identifier et corriger les anomalies détectées dans les processus de production.

**sont considérées comme "critiques" les composants, les systèmes ou les opérations évalués comme critiques lors de l'analyse de risque au titre du système de gestion de la sécurité (SGS) par l'organisme.*

Organismes de conception (DOA)

Fonctions	Sous-fonctions	Objectifs
Concevoir, développer et gérer l'architecture des systèmes	Définir l'architecture et la configuration globale de l'aéronef ou du système	Concevoir l'architecture et les configurations pour garantir leur intégration et répondre aux exigences
	Gérer la configuration, les évolutions, et les données techniques	Suivre les configurations et diffuser les données pour garantir la conformité réglementaire.
	Développer, intégrer et valider les logiciels et systèmes embarqués	Concevoir, intégrer et tester les logiciels et systèmes embarqués pour garantir leur bon fonctionnement.
	Tester et valider les fonctions de l'aéronef ou du système	Vérifier que toutes les fonctions respectent les exigences de navigabilité et de sécurité.
Gérer les moyens de conception et de test		S'assurer que les outils et systèmes de conception sont disponibles, fonctionnels et conformes aux spécifications.
Gérer les processus de certification		Organiser et vérifier les processus de certification pour s'assurer de la conformité réglementaire.

Exploitants d'aérodromes

Fonctions	Sous-fonctions	Objectifs
Gestion des opérations aéroportuaires et du trafic	Maintenir les aires de manœuvre et de trafic	Maintenir l'aire de manœuvre et l'aire de trafic afin de garantir l'arrivée et le départ des avions en toute sécurité
	Gérer les autorisations de circulation	Gérer les autorisations de circulation (Aire de trafic, Aire de manœuvre, Piétons, véhicules)
	Gérer les allocations des postes de stationnement	Gérer l'allocation des postes de stationnement
Protection et maintenance des infrastructures aéroportuaires	Sécuriser les surfaces	Sécuriser les surfaces de protection et les abords de l'aérodrome
	Fournir le balisage lumineux	Assurer le fonctionnement du balisage lumineux et la transmission du bon état de fonctionnement à la tour
Gestion des incendies		Assurer l'intervention des pompiers en cas d'incidents
Gestion des données aéronautiques		Gérer les données et informations aéronautiques

Organismes de maintenance (Partie – 145)

Fonctions	Sous-fonctions	Objectifs
Gérer la documentation, les processus, et les équipements de maintenance	Gérer la documentation approuvée et les consignes de navigabilité	Organiser et suivre les documents approuvés et consignes pour garantir leur conformité et leur mise en œuvre
	Gérer les outils et équipements utilisés pour la maintenance	Garantir la disponibilité, l'entretien, et la conformité des outils de maintenance
	Assurer la traçabilité des interventions de maintenance	Enregistrer toutes les interventions pour garantir un historique complet et intègre
	Gérer l'approvisionnement en pièces et systèmes, les contrôler et les stocker	Vérifier que les pièces et composants sont conformes avant leur utilisation dans les aéronefs.
Réaliser et inspecter les activités de maintenance	Effectuer la maintenance des aéronefs et de leurs composants	Réaliser les tâches de maintenance nécessaires pour garantir la sécurité et la navigabilité des aéronefs
	Inspecter et certifier les travaux de maintenance	Vérifier la conformité des travaux et délivrer les approbations pour remise en service
	Gérer les non-conformités et mettre en œuvre des actions correctives	Identifier et résoudre les anomalies détectées pour prévenir les risques de sécurité

Organismes responsables de la gestion du maintien de la navigabilité (CAMO)

Fonctions	Sous-fonctions	Objectifs
Assurer la navigabilité continue des aéronefs	Suivre la navigabilité des aéronefs	S'assurer que les aéronefs respectent en permanence les exigences réglementaires de navigabilité
	Gérer et mettre en œuvre les consignes de navigabilité	Suivre et appliquer les directives réglementaires pour garantir la sécurité des aéronefs.
	Gérer les modifications et réparations approuvées	S'assurer que toutes les modifications et réparations respectent les normes de navigabilité
	Maintenir la documentation technique et réglementaire	Veiller à ce que la documentation soit complète, à jour et conforme aux exigences réglementaires
Planifier et superviser les activités de maintenance	Élaborer et gérer le programme d'entretien des aéronefs	Définir, approuver et mettre à jour le programme d'entretien en tenant compte des réglementations.
	Coordonner les activités de maintenance	Planifier et coordonner les interventions de maintenance avec les MOA et d'autres entités.
	Contrôler la traçabilité des opérations de maintenance	Garantir que les travaux de maintenance sont enregistrés avec une traçabilité complète.

Transporteurs aériens (CAT/SPO/NCC)

Fonctions	Sous-fonctions	Objectifs
Gestion des aéronefs et des équipages	Évaluation des compétences et traçabilité de la formation des équipages (PNT et PNC)	Evaluer les compétences et tracer la formation des équipages (PNT et PNC)
	Programmation des aéronefs et des équipages	Programmer les aéronefs et les équipages
	Régulation des aéronefs et des équipages	Réguler les aéronefs et les équipages
Préparation des vols	Élaboration du plan de vol	Elaborer le plan de vol opérationnel
	Dépose du plan de vol ATC	Déposer le plan de vol ATC
	Devis de masse et centrage et performances avions	Etablir le devis de masse et centrage et calculer les performances avions
	Transmission du dossier de vol aux pilotes	Transmettre le dossier de vol aux pilotes
Gestion des données et documentation cockpit	Accès aux informations nécessaires au vol	Permettre aux pilotes d'accéder en vol aux informations nécessaires (information météo, NOTAM, etc.)
	Affichage des cartes de navigation et d'aérodromes	S'assurer que les cartes de navigation et les outils associés sont disponibles, à jour et intègres
	Accès à la documentation et aux procédures d'urgence en vol	Permettre aux pilotes d'accéder en vol à la documentation intégrant les procédures d'urgence

Organismes de formation agréés (ATO) & Exploitants de simulateur d'entraînement au vol (FSTD)

Fonctions	Sous-fonctions	Objectifs
Gérer les données de formation pilote	Gérer les programmes de formation en vol	Fournir au stagiaire pilote un programme de formation en vol exhaustif et intègre
	Gérer les supports de formation pilote théorique	Fournir au stagiaire pilote un support de formation théorique intègre et répondant aux exigences règlementaires
	Tracer les parcours de formation	Assurer la traçabilité et la progression de la formation suivie par chaque stagiaire pilote
Gérer les aéronefs utilisés pour la formation pilote		Mettre à disposition des aéronefs répondant aux exigences de sécurité, pour la formation en vol des stagiaires pilotes
Gérer les simulateurs de vol utilisés pour la formation pilote		Mettre à disposition les simulateurs d'entraînement au vol (FSTD) répondant aux exigences de sécurité pour la formation des stagiaires pilotes

Centres aéromédicaux du personnel naviguant et ATCO

Fonctions	Sous-fonctions	Objectifs
Assurer la réalisation et la qualité des examens médicaux réglementaires pour les pilotes et contrôleurs aériens	Effectuer les examens médicaux réglementaires des pilotes et des contrôleurs aériens	Vérifier que les pilotes et les contrôleurs aériens remplissent les critères médicaux nécessaires à l'exercice de leurs fonctions et délivrer un certificat d'aptitude
	Disposer d'un matériel médical conforme aux normes aéromédicales et correctement calibré pour la réalisation des examens	Garantir la précision et la fiabilité des examens médicaux grâce à un matériel conforme aux exigences réglementaires.
	Assurer la traçabilité et protéger les données des examens médicaux et des certificats d'aptitude.	Assurer un suivi rigoureux des examens, ainsi que l'intégrité et la confidentialité des données médicales

Organismes de formation des contrôleurs de la circulation aérienne (ATCO)

Fonctions	Sous-fonctions	Objectifs
Gérer les données de formation ATCO	Gérer les programmes de formation ATCO	Fournir au stagiaire ATCO un programme de formation exhaustif et intègre
	Gérer les supports de formation théorique ATCO	Fournir au stagiaire ATCO un support de formation théorique intègre et répondant aux exigences règlementaires
	Tracer les parcours de formation	Assurer la traçabilité et la progression de la formation suivie par chaque stagiaire ATCO
Gérer les simulateurs ATC utilisés pour la formation ATCO		Mettre à disposition de simulateurs ATC répondant aux exigences de sécurité pour la formation pratiques des stagiaires ATCO

Prestataires de service de navigation aérienne (ANSP)

Fonctions	Sous-fonctions	Objectifs
Gestion du trafic aérien (ATM)	Services de la circulation aérienne (ATS)	Assurer la sécurité, la régularité et l'efficacité des vols (inclut l'ATC, le service d'alerte, l'information de vol)
	Gestion des flux de trafic aérien (ATFM)	Equilibrer la demande et capacité des services de gestion du trafic afin de prévenir les congestions et de minimiser les retards
	Gestion de l'espace aérien (ASM)	Gérer stratégiquement et tactiquement l'espace aérien pour assurer son utilisation efficace et sécurisée
Communication, Navigation, Surveillance (CNS)	Communication (COM)	Assurer l'échange efficace d'informations entre les contrôleurs aériens et les pilotes pour maintenir un trafic aérien sûr et ordonné.
	Navigation (NAV)	Permettre aux aéronefs de déterminer leur position avec précision et de suivre des trajectoires de vol prédéfinies.
	Surveillance (SUR)	Permettre de surveiller la position des aéronefs en temps réel afin d'assurer la séparation sécurisée entre eux.
Fourniture d'informations météorologiques (MET)		Fournir les conditions météorologiques et des alertes en temps réel aux aéronefs et aux contrôleurs
Service d'information aéronautique (AIS)		Collecter, gérer, diffuser les informations nécessaires à la sécurité, à la régularité et à l'efficacité de la navigation aérienne

Prestataires de services U-Space (USSP)

Fonctions	Sous-fonctions	Objectifs
Développer et mettre en œuvre les moyens pour fournir les services U-space		Concevoir, déployer et assurer la maintenance des moyens techniques indispensables à la fourniture des services U-space aux exploitants de drones
Fournir les services U-space aux exploitants de drones		Garantir la disponibilité et l'efficacité des services U-space pour permettre des opérations de drones sûres et conformes à la réglementation.

Organismes de conception de procédures de vol (FPD)

Fonctions	Sous-fonctions	Objectifs
Concevoir et valider les procédures de vol	Concevoir des procédures respectant la réglementation	Garantir que les procédures de vol respectent la réglementation tout en prenant en compte les contraintes opérationnelles
	Valider et vérifier les procédures avant mise en œuvre	Assurer que les procédures conçues sont conformes aux exigences de sécurité et adaptées aux contraintes opérationnelles

Annexe IV : Matrice de conformité

Cadre de conformité cyber France v3			Règ. (UE) 2015/1998 [1] Règ. (CE) 300/2008 [37] AIM [38] Code des transports [39]	Partie – IS.I/D.OR	AMC IS.I.OR [40]
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)	200 a) 1) 240 a) 2)
	3.3. Gestion des ressources, rôles et responsabilités			240 a) 1) et 3) 240 b) à (f) 240 (h)	240 a) 3) et b) 240 d), f) et h)
4. Gestion des risques de sécurité de l'information			1998 – 1.7.1, 1.7.2 et 1.7.3	205 c)	
	4.1. Établissement du contexte		1998 – 1.7.1, 1.7.2 et 1.7.3	205 a) 1)	
	4.2. Appréciation des risques		1998 – 1.7.1, 1.7.2 et 1.7.3 AIM – DR-1-7-1 (I)	205 a), b), c) et e) 210 b)	205 a), b), c) et e)
	4.3. Traitement des risques		1998 – 1.7.1, 1.7.2 et 1.7.3	210 a) et b)	210 a)
	4.4. Gestion des incidents de sécurité de l'information		1998 –1.7.2	200 a) 5)	
		4.4.1. Détection des incidents de sécurité de l'information		215 a), b), et e) 220 a) 230 b) et c) 1)	215 a) et b) 220 a)
		4.4.2. Réponse aux incidents de sécurité de l'information		220 b)	220 b)
		4.4.3. Remédiation		220 c)	220 c)
		4.4.4. Notification à l'autorité compétente		230 a), b) et c)	230 a) et 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) 13) 215 c) et d) 230 a), b) et c)	200 a) 13)
		4.5.2. Sous-traitance des activités du SMSI		235 a) et b)	235 a) et b)
5. Personnels et compétences	5.1. Vérification des antécédents et contrôle de la fiabilité		1998 – 11.1.2 c), 11.1.3, 1998 – 11.1.7 CT – L6342-3,R6342-32&33	240 i)	240 i)
	5.2. Sensibilisation		1998 – 11.2.1.4, 11.2.8.1 et 11.2.8.2 AIM 11-2-1-4 et 11-2-1-5	240 h)	
	5.3. Formation		1998 – 11.2.1.4, 11.2.8.1 et 11.2.8.2 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 de sécurité de l'information		1998 – 1.7.1, 1.7.2 et 1.7.3 AIM DR 1-7-1 (II) et B-3	200 a) 2) à 6) 200 a) 8) à 10) 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)	260 260 a)
	6.3. Amélioration continue du SMSI			200 b) 260 b)	260 260 b)
	6.4. Modification du système de management de la sécurité de l'information			200 c) 250 c) 255 a) et b)	200 c) 255
7. Archivage	7.1. Procédure de conservation des enregistrements			200 a) 11) 245 c) et d)	245 c) et d)
	7.2. Enregistrements à conserver			200 a) 11) 245 a) et b)	245 a) 1) vi) et a) 5)
8. Documentation	8.1. Programme de sûreté		1998 – 1.7.1, 1.7.2 et 1.7.3 300 – 12,13 et 14		
	8.2. Manuel de management de la sécurité de l'information			250 a) et d)	
Communications DSAC [12] **BI OSAC 2025 – 03** [13]				200 e) 250 b)	200 e)

Annexe V : Définitions

L'authenticité est la propriété selon laquelle une entité est ce qu'elle revendique être		ISO/IEC 27000:2018 [41]
L'autorité nationale compétente (autorité compétente) : une ou plusieurs entités désignées par un État membre, investies des pouvoirs nécessaires et auxquelles des responsabilités ont été attribuées pour l'exécution des tâches de certification, de supervision et de contrôle de l'application conformément au présent règlement et conformément aux actes délégués et actes d'exécution adoptés sur la base de celui-ci, ainsi qu'au règlement (CE) no 549/2004.		RÈGLEMENT (UE) 2018/1139 [42]
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 [41]
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 [43]
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 [10]
La **disponibilité** est la propriété d'être accessible et utilisable à la demande par une entité autorisée		ISO/IEC 27000:2018 [41]
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 [3]
Une **fonction essentielle** fait référence aux :	Biens essentiels	EBIOS RM [17]
	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 [17]
	Actifs essentiels : tout élément représentant de la valeur pour l'organisme tels que : - Les informations - Les processus et activités métier	ISO/IEC 27002:2022 [25]
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 [43]
Un **incident** est un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles		DIRECTIVE (UE) 2022/2555 [44]
L'intégrité est la propriété d'exactitude et de complétude		ISO/IEC 27000:2018 [41]
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 [3]
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 [3]
Les **réseaux et systèmes d'information** sont définis comme : a) un réseau de communications électroniques au sens de l'article 2, point a), de la directive 2002/21/CE ; b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques ; ou c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance		DIRECTIVE (UE) 2022/2555 [44]

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 : ICAO [45]
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 [3]
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 [43]
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. Elle vise à prévenir les actes de malveillance visant les aéronefs, leurs passagers et les membres d'équipage	Annexe 17 : ICAO [46]
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 [3]

Annexe VI : Acronymes

3CF	Cadre de conformité cyber France
AIM	Arrêté InterMinistériel
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ATCO – TO	Air Traffic COntroller - Training Organisation – Organismes de formation des contrôleurs de la circulation aérienne
ATM/ANS	Air Traffic Management / Air Navigation System
BI OSAC	Bulletin Information OSAC
CAMO	Continuing Airworthiness Management Organisation – Organisme de gestion de maintien de la navigabilité
CAT	Certificate of Air Transport - Certificat de Transporteur Aérien
CE (EC)	Commission Européenne (European Commission)
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DOA	Design Organisation Approval
DR	Dirigeant Responsable
DSAC **DSAC – EC** **DSAC – IR**	Direction de la Sécurité de l'Aviation Civile Direction de la Sécurité de l'Aviation Civile – Échelon Central Direction de la Sécurité de l'Aviation Civile – InterRégionale
DSI	Direction des Systèmes d'Information
EASA / AESA	European Aviation Safety Agency / Agence Européenne de la Sécurité Aérienne
ECCAIRS	European Co-ordination Center for Accident and Incident Reporting Systems
EUROCAE	European Organisation for Civil Aviation Equipment
FDP	Flight Procedure Design Organisation – Organisme de conception de procédures de vol
FSTD	Flight Simulation Training Device
IGI	Instruction Générale Interministérielle
II	Instruction Interministérielle
METEOR	Module d'Échange et de TÉlétransmission avec les ORganismes
NCC	Non Commercial Complex – Exploitation d'aéronefs à motorisation complexe à des fins non commerciales
NIS	Network and Information Security
OACI / ICAO	Organisation de l'Aviation Civile Internationale – International Civil Aviation Organisation
POA	Production Organisation Approval
PSNA	Prestataire de Services de la Navigation Aérienne
RSSI	Responsable de la Sécurité des Systèmes d'Information
SGS / SMS	Système de Gestion de la Sécurité – Safety Management System
SMSI / ISMS	Système de Management de la Sécurité de l'Information – Information Security Management System
SPO	Specialised Operations – Exploitations spécialisées
UE	Union Européenne

Annexe VII : 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) 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) 139/2014 de la Commission du 12 février 2014 établissant des exigences et des procédures administratives relatives aux aérodromes
[6]	Règlement (UE) 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
[7]	Règlement (UE) 965/2012 de la Commission du 5 octobre 2012 déterminant les exigences techniques et les procédures administratives applicables aux opérations aériennes
[8]	Règlement (UE) 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
[9]	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
[10]	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
[11]	Règlement d'exécution (UE) 2021/664 de la Commission du 22 avril 2021 relatif à un cadre réglementaire pour l'U-space
[12]	Communication Partie – IS DSAC - METEOR - Aéroport : n°37820 - Navigation aérienne : n°37940 - Compagnie aérienne et organisme de formation : n°37760 - Centre aéromédicaux : Courrier 25-011/DSAC/PN et 25-075/DSAC/ANA
[13]	BI OSAC 2025-03 : Modalités de mise en œuvre des règlements (UE) 2022/1645 et (UE) 2023/203 relatifs à la Partie – IS
[14]	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, Légifrance, Août 2016
[15]	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
[16]	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
[17]	Guides EBIOS Risk Manager, ANSSI, Version 1.5, Mars 2024
[18]	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
[19]	Méthodologie d'analyse de risque OACI/ GCRC – Juin 2025 (RESTRICTED)
[20]	Norme internationale ISO/IEC 31000:2018 – Management du risque - Lignes directrices
[21]	White paper: Identification and Classification guidance for Part-IS assets - ED/DO-ISMS Guidance for Aviation, EUROCAE WG-72 / RTCA SC-216, 2023
[22]	ICAO Doc 9859 Safety Risk Tolerability
[23]	ICAO Doc 10108 Aviation Security Global Risk Statement
[24]	Guide d'hygiène informatique, ANSSI, Version 2.0, Septembre 2017

[25]	Norme internationale ISO/IEC 27002:2022 – Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information
[26]	Norme internationale ISA/IEC 62443 - Series of Standards
[27]	ED-206 - Guidance on Security Event Management, EUROCAE, 2022
[28]	Prestataires de détection des incidents de sécurité - Référentiel d'exigences, ANSSI, 2017
[29]	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,
[30]	Norme internationale ISO/IEC 27035:2023 – Technologies de l'information - Gestion des incidents de sécurité de l'information
[31]	ED Decision 2023/009/R, EASA, 2023
[32]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, version 2, ANSSI, 2022
[33]	Guides ANSSI cyberattaques et remédiation : Piloter la remédiation d'un incident cyber, ANSSI, 2025
[34]	Outil de Maturité AirCyber, Boostaerospace, 2023
[35]	Guide de conception de sessions de sensibilisation cybersécurité_v1_DSAC_2021
[36]	Guide de formation cybersécurité_v1_DSAC_2021
[37]	Règlement (CE) 300/2008 du parlement européen et du conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile
[38]	Arrêté du 11 septembre 2013 relatif aux mesures de sûreté de l'aviation civile
[39]	Code des transports
[40]	Easy Access Rules for Information Security, EASA, Juin 2024
[41]	Norme internationale ISO/IEC ISO/IEC 27000:2018
[42]	Règlement (UE) 2018/1139 du parlement européen et du conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile
[43]	P-03-01 - Instruction et surveillance des agréments d'organismes avec système de gestion, DSAC/OSAC, 2024
[44]	Directive (UE) 2022/2555 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union
[45]	Annexe 19 : OACI
[46]	Annexe 17 : OACI

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