MINISTÈRE
CHARGÉ
DES TRANSPORTS

Liberté
Égalité
Fraternité

dgac direction générale de l'Aviation civile
DSAC

CADRE DE CONFORMITÉ CYBERSÉCURITÉ FRANCE

Aviation civile

Direction de la sécurité de l'aviation civile
Direction de programme cybersécurité
Édition nº 1
Version n° 1 du 3 septembre 2021

Informations

Ce document, établi par la direction de la sécurité de l'aviation civile (DSAC), présente le Cadre de Conformité Cyber France (3CF) pour l'aviation civile.

Il peut être utilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour).

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

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

Historique des révisions

Edition et Version	Date	Modifications
Edition1 - Version intermédiaire	30 juin 2021	Création du document
Edition1 Version1 (Ed1-v1)	3 Sept. 2021	Modifications : - § 1. Introduction : - § 2. Démarche d'accompagnement - § 4.1.4. Personnels et compétence - § 5.4.4.1. Sources des non-conformités - Annexe 3 : Grille de conformité réglementaire Ajouts : - § 5.1.3. Formation - Annexe 2 : Niveaux de conformité et dispositions du 3CF

Approbation du document

Nom	Responsabilité	Date	Visa
Pierre **ABDOULHADI** Adjoint à la directrice de programme cybersécurité – DSAC	Rédacteur	3 Sept. 2021	OK
Anne **FRISCH** Directrice de programme cybersécurité – DSAC	Vérificateur	3 Sept. 2021	OK
Patrick **CIPRIANI** Directeur de la sécurité de l'aviation civile - DSAC	Approbateur	3 Sept. 2021	OK

Sommaire

Table des illustrations

1. Introduction

1.1. Contexte

Par son rôle dans la défense et la sécurité nationale, et par l'importance qu'il représente pour l'économie de la Nation, le transport aérien est concerné depuis 2016 par des dispositions nationales en matière de cybersécurité.

Ces dispositions sont issues :

- d'une part de l'article 22 de la loi de programmation militaire (LPM) et
- d'autre part de la loi de transposition de la directive européenne *Network and Information Security* (NIS).

En conséquence, certains acteurs du transport aérien désignés Opérateurs d'Importance Vitale (OIV) ou Opérateur de Service Essentiel (OSE), doivent se conformer à des règles de sécurité des systèmes d'information.

En outre, l'ensemble des acteurs du transport aérien seront bientôt soumis à 2 évolutions réglementaires majeures, propres au secteur aérien :

- l'amendement (UE) n°2019/1583 [1] au règlement (UE) n°2015/1998 fixant les normes de base commune en matière de sûreté, qui vise à sécuriser les systèmes d'information contribuant à la sûreté de l'aviation civile, applicable au 31 Décembre 2021 ;
- le règlement (UE) *Part IS* [2], en projet actuellement, qui vise à sécuriser les systèmes d'information contribuant à la sécurité de l'aviation civile qui devrait être adopté en décembre 2022 pour une application en décembre 2023

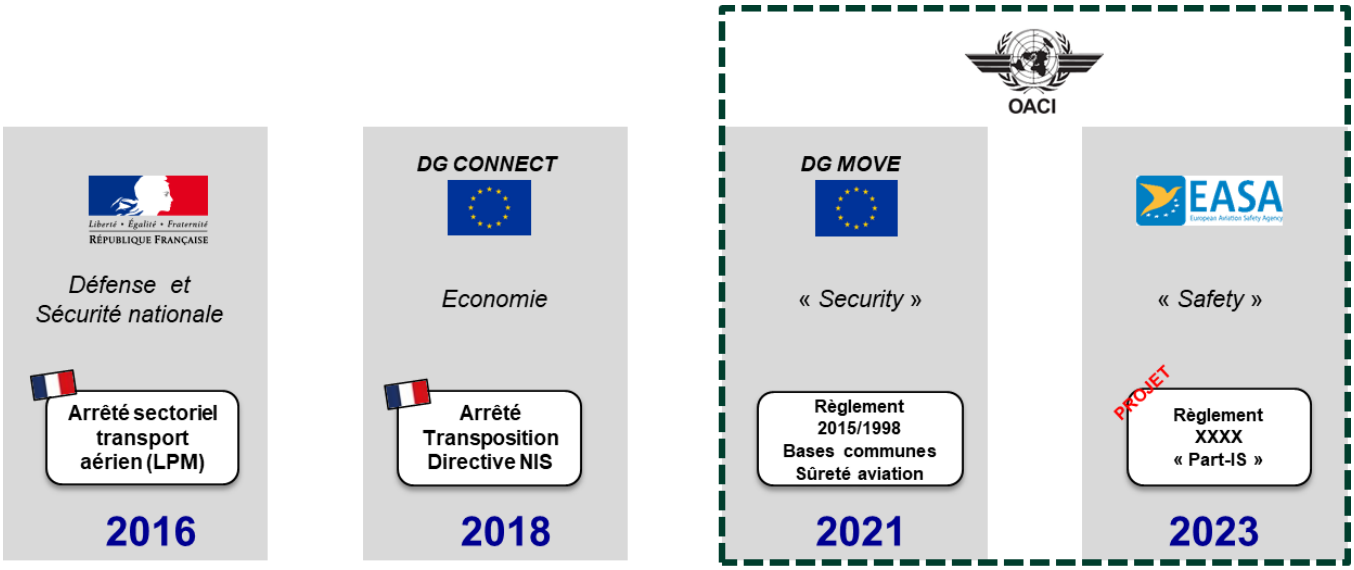

Figure 1 : Dispositions réglementaires dans le domaine du transport aérien

1.2. Objectifs du cadre de conformité cyber France

1.2.1. 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 **C**adre de **C**onformité de **C**ybersécurité **F**rance (3CF en abrégé). 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] pour les mesures portant sur la sécurité des systèmes d'information participant à la sûreté de l'aviation civile ;
  - au futur règlement (UE) *Part IS* [2] portant sur la sécurité des systèmes d'information liés à la sécurité de l'aviation civile ;
- à assurer la cohérence, sans en garantir la conformité, avec les dispositions nationales telles que :
  - l'arrêté sectoriel « transport aérien » [3] issu de l'article 22 de la loi de programmation militaire, désigné comme « arrêté sectoriel du transport aérien »;
  - le décret [4] et les arrêtés [5,6 et 7] issus de la loi de transposition de la directive *Network Information Security* (NIS), désignés comme « transposition de la directive NIS ».

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

- la norme ISO 27001 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).

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 des systèmes d'information. Le référentiel unique (3CF) se veut donc un outil de rationalisation des exigences.

1.2.2. Harmonisation et cohérence européenne

Dans un souci d'harmonisation et de cohérence européenne, et afin d'éviter toute distorsion concurrentielle ce document franco-français à l'origine, est développé en étroite coordination avec plusieurs autorités européennes, homologues de la DGAC/DSAC. Il fait l'objet de consultation auprès des opérateurs concernés (exploitants d'aérodrome et compagnies aériennes) et des associations qui les représentent (FNAM et UAF). Dans sa version anglaise, il sera présenté, entre autres à l'Agence Européenne pour la Sécurité de l'Aviation (AESA) dans le cadre des travaux d'élaboration des *Acceptable Means of Compliance* (AMC).

1.2.3. Accompagnement vers les conformités

Par ailleurs, compte tenu de la diversité de maturité cybersécurité des opérateurs visés par les règlements et de la complexité de la matière, ce document (3CF) propose également une démarche d'accompagnement vers la conformité aux différents règlements. Notamment, pour les opérateurs devant se conformer aux 2 règlements cybersécurité du transport aérien, applicables à des dates différentes.

1.2.4. Principe de mise en œuvre

Le présent document fournit aux opérateur un cadre de conformité, qui, s'il est appliqué, donne l'assurance d'être conforme au règlement (UE) n°2015/1998 [1] et, au règlement (UE) *Part-IS* [2] lorsque celui-ci sera applicable.

En outre, l'opérateur désigné OIV ou OSE, a l'assurance que le cadre de conformité cyber est cohérent et ne présente donc pas de contradiction avec les exigences LPM et NIS. Pour autant, à lui tout seul, le 3CF ne permet pas d'assurer la conformité aux exigences LPM et NIS.

1.3. Opérateurs concernés

Les règlements cybersécurité transport aérien étant applicables à des dates et à des acteurs différents, le cadre de conformité cyber France se décline en 2 versions.

1.3.1. Version 1

Le présent document constitue la version 1 du cadre de conformité cyber France et permet la conformité au règlement (UE) n°2015/1998 [1] en préparant celle au futur au règlement (UE) *Part-IS* [2].

Il s'adresse donc aux **exploitants d'aérodrome** et **aux compagnies aériennes** devant mettre en œuvre les mesures de sûreté prévues par le règlement (UE) n°2015/1998 [1].

1.3.2. Version 2

La seconde version du document quant à elle, sera publiée lorsque le règlement (UE) *Part-IS* [2] sera adopté et permettra les conformités au règlement (UE) n°2015/1998 [1] et règlement (UE) *Part-IS* [2].

Outre les opérateurs identifiés ci-dessus, elle s'adressera également aux organismes visés par :

- les sous-sections G et J, de la section A de l'annexe I (*Part 21*) du règlement (UE) n°748/2012 [8], à savoir ceux détenant :
  - **un agrément d'organisme de production** (*POA*) et/ou ;
  - **un agrément d'organisme de conception** (*DOA*)
- la section A de l'annexe II (Part-145) et la section A de l'annexe V (Part-CAMO) du règlement (UE) n°1321/2014 [9], à savoir :
  - **les ateliers de maintenance**, et ;
  - **les organismes de gestion du maintien de la navigabilité** (*CAMO*).
- l'annexe III (*Part-ORO*) du règlement (UE) n°965/2012 [10], à savoir :
  - **les compagnies aériennes** disposant d'un certificat d'exploitation.
- l'annexe VII (*Part-ORA*) du règlement (UE) n°1178/2011 [11], à savoir :
  - **les organismes de formation des personnels de bord**, et;
  - **les centres aéro-médicaux des personnels de bord**, et ;
  - **les opérateurs de *Flight Simulation Training Devices*** (*FSTD*).
- l'annexe III (*Part ATCO.OR*) du règlement (UE) n°2015/340 [12], à savoir :
  - **les centres de formation des contrôleurs aérien**, et ;
  - **les centres aéro-médicaux des contrôleurs aérien**.
- l'annexe III (*Part-ATM/ANS.OR*) du règlement (UE) n°2017/373 [13], à savoir :
  - **les prestataires de service de navigation aérienne** détenant un certificat.
- l'annexe III (*Part-ADR.OR*) du règlement (UE) n°139/2014 [14], à savoir :
  - **les exploitants d'aérodromes** détenant un certificat européen ;
  - **les prestataires de services de gestion d'aire de trafic**.
- le futur règlement relatif aux **prestataires de services *U-space*** (*USSP*).

1.4. Contenu du document

Le document est organisé de la façon suivante :

- Le chapitre 2 présente la démarche d'accompagnement proposée par la DSAC, notamment les niveaux de conformité et les dispositions associées ;
- Le chapitre 3 s'intéresse à la gouvernance en matière de cybersécurité, à savoir la manière de structurer les activités liées à la cybersécurité au travers d'une organisation adaptée ;
- Le chapitre 4 décrit les prérequis nécessaires pour d'une part structurer la gestion de la sécurité des systèmes d'information et d'autre part assurer la conformité avec le règlement (UE) n°2015/1998 [1];
- Le chapitre 5 aborde les exigences nécessaires à la mise en œuvre d'un système de management de la sécurité de l'information, répondant partiellement aux exigences du futur règlement (UE) *Part IS* [2]. Il s'agit d'une évolution de la démarche de gestion de la sécurité des systèmes d'information.

Si le 3ème chapitre s'adresse particulièrement à la direction de l'opérateur, les 2ème, 4ème et 5ème chapitres quant à eux s'adressent aux équipes en charge de l'organisation, du pilotage et de la mise en œuvre des mesures de sécurité des systèmes d'information.

1.5. Conventions de lecture

Dans le document, les termes suivants doivent être compris dans ce sens :

- **La sécurité des systèmes d'information** (SSI) est l'ensemble des moyens techniques, organisationnels, juridiques et humains participant à la protection de la confidentialité, de l'intégrité et de la disponibilité des systèmes d'information[1] ;

- **La cybersécurité** est l'état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles[1] ;

- **La sûreté** est une combinaison des mesures ainsi que des moyens humains et matériels visant à protéger l'aviation civile contre les actes d'interventions illicites[2]. Elle vise à prévenir les actes de malveillance (d'**origine intentionnelle** donc) visant les aéronefs, leurs passagers et les membres d'équipage ;

- **La sécurité de l'aviation civile** 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[3]. Dans les faits, il s'agit des risques ayant une origine **non intentionnelle** (erreur humaine, phénomène naturel imprévisible, etc.).

[1] Source : ANSSI

[2] Source OACI – Annexe 17

[3] Source OACI – Annexe 19

2. Démarche d'accompagnement

2.1. Niveaux de conformité

2.1.1. Définition des niveaux de conformité

La démarche proposée vise à accompagner les opérateurs de leur niveau actuel en matière de cybersécurité, vers la conformité au règlement (UE) n°2015/1998 [1] jusqu'à la conformité au règlement (UE) *Part IS* [2]. Afin d'y parvenir 4 niveaux de conformité progressifs, caractérisés par des principes et des mesures de sécurité des systèmes d'information, ont été identifiés.

Dans sa 1ère version, le périmètre d'application du cadre de conformité cyber France est limité au domaine de la sûreté, relevant du règlement (UE) n°2015/1998 [1]. L'objectif à terme étant de l'étendre au domaine de la sécurité de l'aviation civile, les niveaux de conformité intègrent donc certaines dispositions non exigées par le règlement (UE) n°2015/1998 [1] mais permettant de préparer la conformité au règlement (UE) *Part IS* [2].

Ainsi, un 5ème niveau de conformité, nommé Niveau 4' (*quatre prime*) est défini. Celui-ci présente les mêmes dispositions que le niveau 4, à la différence qu'elles s'appliquent aux domaines de la sûreté **et** de la sécurité de l'aviation.

Les niveaux de conformité peuvent être compris dans ce sens :

- Niveau 1 : Gestion de la sécurité des systèmes d'information standard dans le domaine de la sûreté ;
- Niveau 2 : Gestion de la sécurité des systèmes d'information avancée dans le domaine de la sûreté ;
- Niveau 3 : Système de management de la sécurité de l'information allégé dans le domaine de la sûreté ;
- Niveau 4 : Système de management de la sécurité de l'information dans le domaine de la sûreté ;
- Niveau 4' : Système de management de la sécurité de l'information dans le domaine de la sûreté et de la sécurité de l'aviation.

A noter, que ce niveau 4' (*quatre prime*) ne permet pas la conformité totale au règlement (UE) *Part IS* [2]. En effet, à date, il n'est pas encore adopté et les moyens acceptables de conformité ne sont pas encore élaborés.

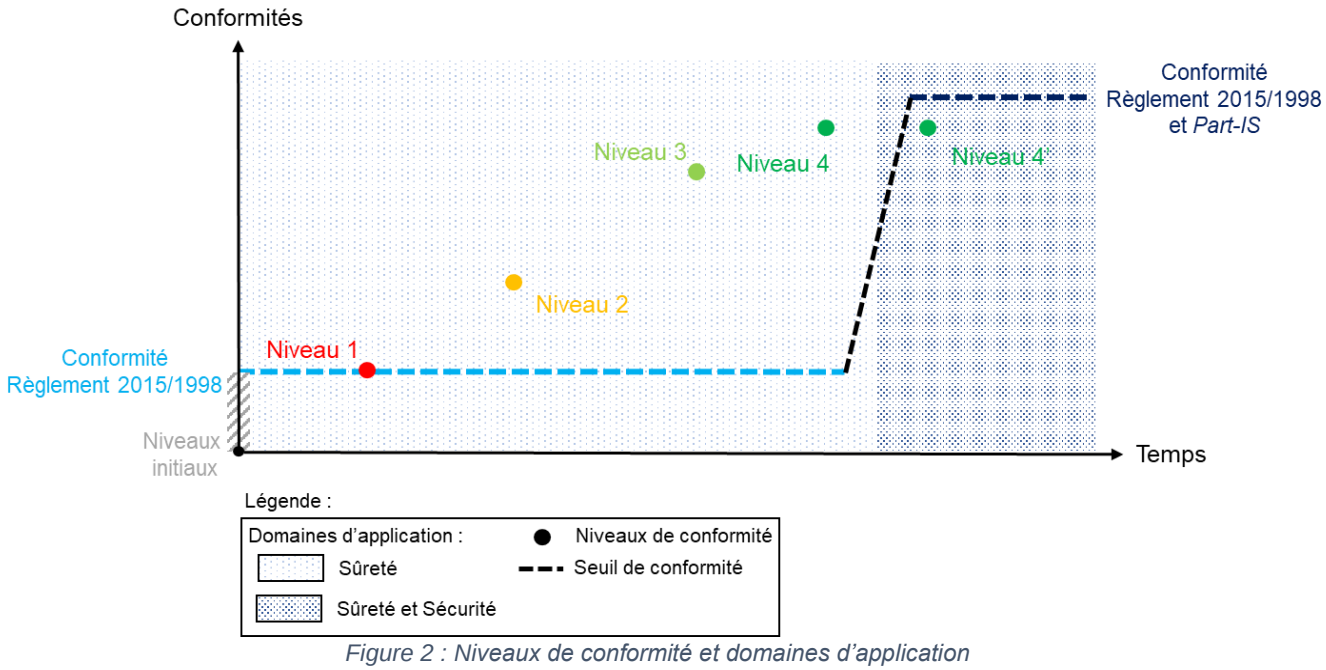

Figure 2 : Niveaux de conformité et domaines d'application

2.1.2.Convention de lecture des niveaux de conformité

2.1.2.1. Numérotation

La convention de numérotation correspond à des niveaux de conformité par rapport au document 3CF, à ne pas confondre avec les niveaux de non-conformité relatifs à la réglementation, utilisés dans les audits sûreté et de sécurité.

2.1.2.2. Atteinte d'un niveau de conformité

Concrètement, chaque section du document présente un ou plusieurs niveaux de conformité. Pour atteindre un niveau de conformité, l'opérateur doit mettre en œuvre les dispositions précisées dans chaque paragraphe et celles-ci sont cumulatives. Le tableau des niveaux de conformité et des dispositions en annexe[4] illustre cette logique.

Par exemple, pour atteindre le niveau 1, l'opérateur met en œuvre les dispositions de niveau 1 uniquement ; tandis que pour atteindre le niveau 3, il met en œuvre toutes les dispositions des niveaux 1,2 et 3.

2.1.3.Conformité réglementaire

La grille de conformité réglementaire, disponible en annexe[5], présente les différentes sections du 3CF en fonction :

- des exigences cybersécurité du règlement (UE) n°2015/1998 [1] ;
- des exigences connues à date du règlement (UE) *Part IS* [2].

Un opérateur est donc conforme au règlement (UE) n°2015/1998 [1] s'il répond aux dispositions, au moins de niveau 1, précisées dans les sections du 3CF, associées aux exigences du dit-règlement.

En pratique, pour être conforme, l'opérateur doit mettre en œuvre les dispositions du 3CF, au moins de niveau 1, suivantes :

- § 4.1.4. Personnels et compétences ;
- § 4.2.2. Appréciation des risques ;
- § 4.2.3.1.1. Élaboration du plan d'actions
- § 4.2.4. Mise en œuvre des mesures de sécurité des systèmes d'information ;
- § 5.4.4. Réaction aux non-conformités.

[4] Annexe 2 : Niveaux de conformité et dispositions du 3CF

[5] Annexe 3 : Grille de conformité réglementaire

2.2. Application de la démarche

La démarche proposée se décompose en 5 étapes :

- Étape A : L'opérateur fait un état des lieux de sa conformité au regard du règlement (UE) n°2015/1998 [1] et vise ainsi le niveau de conformité le plus adapté à son organisme en ayant l'assurance qu'il sera conforme à *minima* avec le règlement applicable ;
- Étape B, C et D : L'opérateur élève progressivement son niveau de maturité en s'appuyant sur ses travaux précédents et gagne ainsi en maturité cyber ;
- Étape E : A ce stade, l'opérateur dispose d'un Système de Management de la Sécurité de l'Information (SMSI), appliqué au domaine de la sûreté. Cette étape consiste à étendre le périmètre au domaine de la sécurité de l'aviation civile, et ainsi à se rapprocher de la conformité au futur règlement (UE) *Part IS* [2] ;
- Les étapes suivantes seront détaillées dans la version 2 du document.

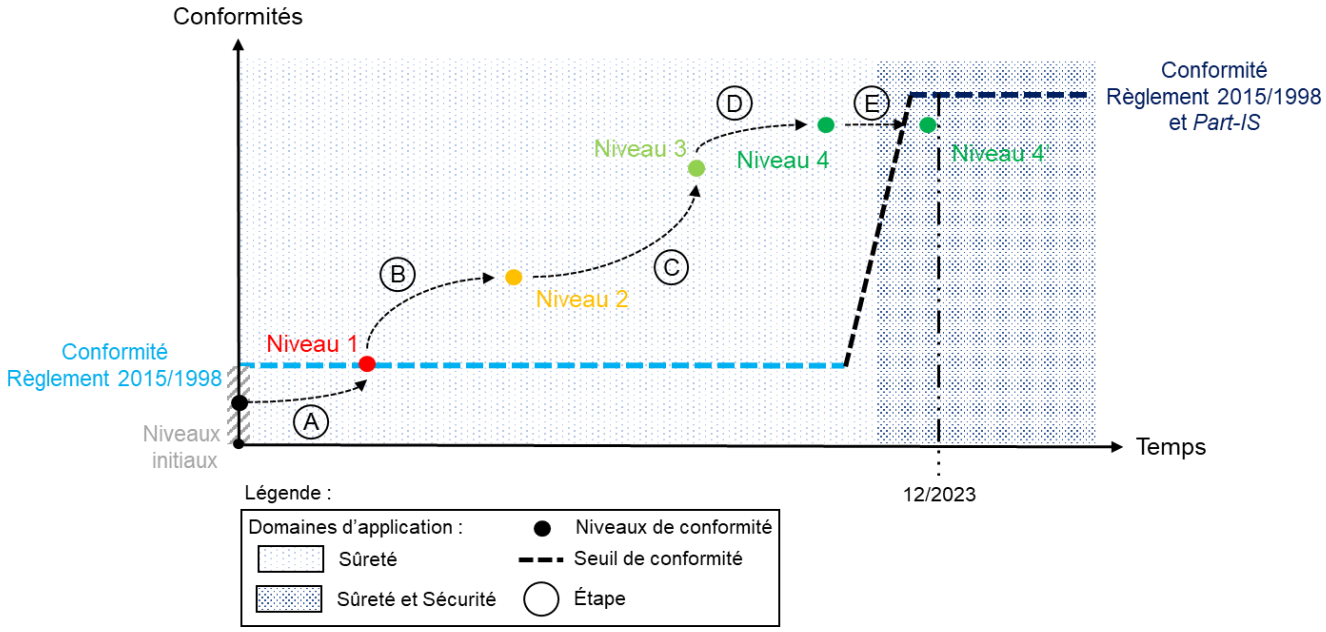

Figure 3 : Application de la démarche mise en conformité progressive

A noter que, les efforts et le temps nécessaires au passage d'un niveau à un autre, dépendent de la maturité ainsi que des moyens mis en œuvre par l'opérateur. Il convient donc que celui-ci définisse au préalable son plan de travail sur la base de ces niveaux de conformité avec comme objectif la mise en œuvre du niveau de conformité 4' (*quatre prime*) en décembre 2023[6].

[6] Date non officielle, à confirmer

3. Gouvernance

3.1. Engagement de la direction

Conformité niveau 1 et plus :

La direction s'engage à assurer la protection des systèmes d'information critiques au regard de la sûreté de l'aviation civile, contre toute atteinte à la confidentialité, l'intégrité et la disponibilité de ces systèmes et des informations qu'ils contiennent et / ou traitent.

Conformité niveau 3 et plus :

Pour ce faire, la direction 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 le niveau de cybersécurité des systèmes d'information critiques au regard de la sûreté dont elle a la responsabilité.

3.2. Stratégie et objectifs

Conformité niveau 3 et plus :

De plus, la direction établit et approuve :

- une stratégie qui décrit son ambition globale en matière de cybersécurité ;
- les objectifs pour y parvenir ;
- les étapes et le plan d'actions pour atteindre ces objectifs.

3.3. Gestion des ressources, rôles et responsabilités de la sécurité des systèmes d'information

Conformité niveau 1 et plus :

La direction s'assure que :

- les ressources nécessaires pour assurer la gestion des risques liés à la sécurité des systèmes d'information sont disponibles ;
- les rôles et responsabilités concernés par la sécurité des systèmes d'information, à tous niveaux de l'organisation :
    - du personnel interne ;
    - du personnel externe (prestataires, fournisseurs, etc.).

  sont formalisés, attribués, approuvés, communiqués et connus au sein de l'organisation.

3.4. Approbation

Conformité niveau 1 et plus :

La direction approuve formellement :

- la liste des systèmes d'informations critiques à la sûreté de l'aviation civile identifiés ;
- le plan d'actions de mise en œuvre des mesures de sécurité des systèmes d'information ;
- les politiques et procédures de sécurité des systèmes d'information.

Conformité niveau 2 et plus :

En outre, la direction approuve formellement le compte-rendu d'appréciation des risques.

Conformité niveau 3 et plus :

Enfin, la direction accepte formellement, à chaque révision de l'appréciation des risques, les risques résiduels pesant sur le périmètre du système de management de la sécurité de l'information sur la base :

- d'une appréciation des risques ;
- du plan de traitement des risques.

3.5. Système de management de la sécurité de l'information

Conformité niveau 3 et plus :

La direction :

- s'appuie sur et approuve formellement un système de management de la sécurité de l'information (SMSI) et les documents associés pour mettre en œuvre la stratégie et atteindre les objectifs ;
- s'engage à satisfaire aux exigences applicables en matière de sécurité des systèmes d'information ;
- s'engage à œuvrer pour l'amélioration continue du SMSI ;
- désigne qui a la responsabilité et l'autorité de s'assurer que le SMSI est conforme aux exigences du présent document et à la déclinaison qui en est faite pour l'entreprise ;
- s'assure que la personne désignée ci-dessus dispose des moyens, des ressources nécessaires et du statut adapté à la réalisation de cette mission.

La direction s'engage à participer aux revues de direction afin de s'assurer que le SMSI est toujours approprié, adapté et efficace.

Lors de ces revues, la direction prend des décisions relatives :

- aux opportunités d'amélioration continue et ;
- à d'éventuels changements à apporter au SMSI.

3.6. Cohérence de la stratégie, des objectifs et du SMSI

Conformité niveau 3 et plus :

La direction s'assure de la cohérence et de l'intégration ou de l'articulation de la stratégie, des objectifs SSI et du SMSI avec :

- la stratégie, les objectifs et les risques globaux de l'organisation ;
- le(s) système(s) de management existant(s) de l'organisation.

4. Gestion de la sécurité des systèmes d'information

4.1. Organisation de la sécurité des systèmes d'information

4.1.1. Missions et enjeux

Conformité niveau 1 et plus :

L'opérateur identifie les missions critiques au regard de la sûreté de l'aviation civile.

4.1.2. Besoins et attentes prestataires et fournisseurs

Conformité niveau 1 et plus :

L'opérateur identifie :

- les prestataires de services et fournisseurs d'équipements auxquels il fait appel dans le cadre de la mise en œuvre des missions critiques au regard de la sûreté de l'aviation civile, et ;
- les exigences relatives à la sécurité des systèmes d'information à leur faire appliquer. Elles sont d'ordre :
    - règlementaire, notamment celles en matière de contrôle d'antécédents, de sensibilisation et de formation ;
    - contractuel et garantissent que les prestataires et fournisseurs appliquent les mesures de cybersécurité définies et mises en œuvre par l'opérateur[7].

4.1.3. Politiques et procédures

Conformité niveau 1 et plus 2 :

L'opérateur :

- définit les politiques et procédures pour la mise en œuvre des mesures de sécurité des systèmes d'information, notamment celles de niveau standard[8] précisées en Annexe 1 ;
- s'assure que ces documents sont approuvés par la direction, diffusés et communiqués aux personnels ainsi qu'aux prestataires et fournisseurs le cas échéant.

Conformité niveau 3 et plus :

Puis, l'opérateur définit les politiques et procédures pour la mise en œuvre des mesures de sécurité des systèmes d'information, notamment celles de niveau renforcé.

[7] Règle 3 du guide d'hygiène informatique de l'ANSSI [15]

[8] Règles 16, 10, 34, 35 37 et 40 du guide d'hygiène informatique de l'ANSSI [15]

4.1.4.Personnels et compétences

4.1.4.1. Identification des personnes

Conformité niveau 1 et plus :

L'opérateur identifie ou fait identifier par les parties intéressées concernées :

- les équipes managériales, à savoir les personnes organisant et pilotant la sécurité des systèmes d'information critiques à la sûreté ;
- les équipes opérationnelles, à savoir les personnes définissant, planifiant et mettant en œuvre les mesures de sécurité sur les systèmes d'information critiques à la sûreté ;
- les utilisateurs des systèmes d'information critiques à la sûreté :
  - disposant de droits d'administrateur ;
  - ne disposant pas de droits d'administrateur.
- les acteurs de la sûreté, à savoir les personnes :
  - organisant la mise en œuvre des mesures de sûreté ;
  - mettant en œuvre les mesures de sûreté.

4.1.4.2. Vérification des antécédents

Conformité niveau 1 et plus :

L'opérateur applique ou fait appliquer par les parties intéressées, une vérification renforcée des antécédents des personnes identifiées au § 4.1.4.1.

Ainsi, l'opérateur

- s'assure que ces personnes disposent d'une habilitation préfectorale prévue par l'article L6342-3 du code des transports [16], 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.
- prend en considération les emplois, études et interruptions éventuelles de ces personnes dans les États où elles ont résidé au cours des 5 dernières années ;
- conserve des informations documentées appropriées comme preuves.

4.1.4.3. Sensibilisation et formation

Conformité niveau 1 et plus :

L'opérateur :

- s'assure que :
  - toutes les personnes identifiées précédemment sont sensibilisées à la cybersécurité[9] ;
  - les équipes managériales sont formées à la gestion de la sécurité des systèmes d'information en cohérence avec les tâches qui leur sont confiées[10]. ;
  - les équipes opérationnelles sont formées à la mise en œuvre des mesures de sécurité à l'état de l'art, en cohérence avec les tâches qui leur sont confiées[11].
- conserve des informations documentées appropriées comme preuves.

[9]Guide de conception de sessions de sensibilisation cybersécurité [17]

[10]Guide de formation cybersécurité [18] - § 2.1.

[11]Guide de formation cybersécurité [18] - § 2.2.

4.2. Gestions des risques

4.2.1. Méthodologie de gestion des risques

Dans le cadre de la gestion des risques, l'opérateur réalise une **appréciation des risques**, sur laquelle il s'appuie pour définir le **traitement des risques** approprié.

Conformité niveau 1 et plus :

L'opérateur gère les risques en s'appuyant sur une des normes ou des méthodes suivantes :

- ISO/CEI 27005 [20],Norme relative à la Gestion des risques liés à la sécurité de l'information ;
- EBIOS *Risk Manager* [21] méthode d'appréciation et de traitement des risques numériques publiée par l'ANSSI ;
- toute autre méthode conforme à la norme ISO/CEI 31000, norme relative à la gestion des risques.

4.2.2. Appréciation des risques

4.2.2.1. Activités d'appréciation des risques

Conformité niveau 1 et plus :

Sur la base des missions établies précédemment, l'opérateur :

- identifie les fonctions critiques au regard de la sûreté de l'aviation civile[12];
- réalise une analyse d'impacts[13] sur la sûreté en cas de perte de confidentialité, d'intégrité et/ou de disponibilité des fonctions identifiées ;
- identifie les événements redoutés et leur niveau de gravité.

Conformité niveau 2 et plus :

De plus, l'opérateur :

- établit des critères de risque, notamment :
  - les critères d'acceptation des risques ;
  - les critères d'appréciation des risques.
- identifie les risques sur la base de son analyse d'impact ;
- mène une analyse des risques visant à déterminer les niveaux de risques associés ;
- évalue les risques visant à :
  - comparer les résultats de l'analyse de risque avec les critères de risques ;
  - prioriser les risques analysés.

Conformité niveau 4 :

Enfin, l'opérateur associe à chaque risque identifié son propriétaire ou responsable

[12] Fonctions critiques au regard de la sûreté du transport aérien [19]

[13] L'analyse d'impact correspond à :

- l'identification des menaces, des vulnérabilités et des conséquences dans l'ISO 27005 :2018 [20]
- l'atelier 1 : cadrage et socle de sécurité de la Méthode EBIOS *Risk Manager* [21] ;

4.2.2.2. Résultats de l'appréciation des risques

Conformité niveau 1 et plus :

Sur la base de l'analyse d'impact ou de l'appréciation des risques, l'opérateur identifie les systèmes d'information critiques à la sûreté et conserve des informations documentées comme preuves.

Conformité niveau 2 et plus :

En outre, l'opérateur :

- produit un compte-rendu des résultats de l'appréciation des risques détaillant :
  - les conclusions des différentes activités, notamment la liste des risques appréciés et classés par ordre de priorité, en fonction des critères d'évaluation des risques définis ;
  - la liste des systèmes d'information critiques à la sûreté de l'aviation civile, identifiés**.**
- conserve des informations documentées comme preuves des résultats d'appréciation des risques.

4.2.3.Traitement des risques

4.2.3.1. Activités du traitement des risques

4.2.3.1.1. Élaboration du plan d'actions

Conformité niveau 1 et plus :

L'opérateur élabore un plan d'actions de mise en œuvre des 38 mesures de sécurité des systèmes d'information standards détaillées dans l'annexe 1 ; et précisant

- les priorités ;
- les délais de mise en œuvre ;
- le cas échéant, les raisons ne permettant pas de mettre en œuvre la mesure de sécurité des systèmes d'information.

Conformité niveau 3 et plus :

En outre, l'opérateur complète le plan d'actions avec les 19 mesures de sécurité des systèmes d'information renforcées détaillées dans l'annexe 1

4.2.3.1.2. Actions et mesures complémentaires pour le traitement du risque

Conformité niveau 3 et plus :

Sur la base des résultats de l'appréciation des risque, l'opérateur définit pour chacun des risques s'il :

- maintient le risque, dans le cas où il considère que le risque identifié est acceptable en l'état ;
- réduit le niveau de risque par l'introduction, la suppression ou la modification des mesures de sécurité des systèmes d'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,

afin que le risque résiduel puisse être réapprécié et jugé acceptable.

L'opérateur détermine alors, la ou les mesures complémentaires permettant de traiter le risque conformément à l'action choisie.

4.2.3.1.3. Élaboration du plan de traitement des risques

Conformité niveau 3 et plus :

L'opérateur élabore un plan de traitement des risques permettant d'identifier :

- Les mesures de sécurité des systèmes d'information :
  - du plan d'action ;
  - complémentaires déterminées *supra* et les risques qu'elles traitent.
- leurs priorités et ;
- leurs délais de mise en œuvre ;
- le cas échéant, les raisons ne permettant pas de les mettre en œuvre.

4.2.3.1.4. Évaluation des risques résiduels

Conformité niveau 3 et plus :

L'opérateur évalue les risques résiduels, après l'application des mesures de sécurité des systèmes d'information définies dans le plan de traitement des risques.

4.2.3.1.5. Approbation des risques

Conformité niveau 1 et plus :

L'opérateur formalise l'approbation par la direction :
- de la liste des systèmes d'informations critiques à la sûreté de l'aviation civile identifiés ;
- du plan d'actions de mise en œuvre des mesures de sécurité des systèmes d'information.

Conformité niveau 2 et plus :

En outre, l'opérateur formalise l'approbation par la direction du compte-rendu d'appréciation des risques.

Conformité niveau 3 et plus :

Puis, l'opérateur formalise :
- l'approbation du plan de traitement des risques ;
- l'acceptation des risques résiduels, auprès de la direction.

Conformité niveau 4 :

Enfin, l'opérateur formalise l'acceptation des risques résiduels, auprès des propriétaires ou responsables des risques.

4.2.3.2. Résultats du traitement des risques

Conformité niveau 1 et plus :

L'opérateur :
- produit un rapport comprenant :
  - la liste approuvée des systèmes d'informations critiques à la sûreté tels qu'identifiés ;
  - le plan d'actions approuvé relatif à la mise en œuvre des mesures de sécurité des systèmes d'information.
- conserve des informations documentées comme preuves des résultats du traitement des risques.

Conformité niveau 2 et plus :

Puis, l'opérateur complète le rapport approuvé en incluant le compte-rendu d'appréciation des risques.

Conformité niveau 3 et plus :

Enfin l'opérateur complète le rapport avec :
- le plan approuvé de traitement des risques ;
- l'évaluation des risques résiduels acceptés.

4.2.4.Mise en œuvre des mesures de sécurité des systèmes d'information

Conformité niveau 1 et plus :

L'opérateur :

- met en œuvre :
  - les mesures standards[14] 1,2 et 4[15], et ;
  - au moins 10% des mesures identifiées dans le plan d'action ;
- produit un tableau de bord de suivi d'avancement du plan d'actions ;
- conserve des informations documentées comme preuves des résultats de la gestion des risques.

Conformité niveau 2 et plus :

En outre, l'opérateur met en œuvre au moins 50% des mesures identifiées dans le plan d'actions.

Conformité niveau 3 et plus :

Puis, l'opérateur applique les mesures de sécurité des systèmes d'information en s'appuyant sur la mise en œuvre du SMSI détaillée au § 5.3.

[14] Voir Annexe 1 – Mesures de sécurité des systèmes d'information

[15] Ces mesures de sécurité sont imposées par le règlement (UE) n°2015/1998 [1]

5. Système de management de la sécurité de l'information

5.1. Définition du SMSI

5.1.1. Stratégie du SMSI

5.1.1.1. Missions et enjeux

Conformité niveau 3 et plus :

Outre les dispositions prévues au § 4.1.1. du présent document, l'opérateur identifie en fonction des missions, les enjeux externes et internes pertinents qui influent sur la capacité à obtenir le(s) résultat(s) attendu(s) du SMSI, notamment :

- les contraintes externes :
  - le règlements (UE) n°2015/1998 [1] ;
  - les lois et textes nationaux : Loi de programmation militaire, loi de transposition de la directive NIS – Décrets et Arrêtés associés, le cas échéant ;
  - les exigences contractuelles, le cas échéant.
- les contraintes internes.

5.1.1.2. Besoin et attentes des parties intéressées

Conformité niveau 3 et plus :

Outre les dispositions prévues au 4.1.2. relatives aux prestataires et fournisseurs, l'opérateur identifie :

- les parties intéressées concernées par le système de management de la sécurité de l'information :
  - les clients ;
  - les partenaires qui sont :
    - les organisations avec lesquelles elle échange des informations pour assurer les missions critiques au regard de la sûreté ;
    - les prestataires de services et fournisseurs d'équipements ;
    - toute autre personne ou organisation susceptible d'affecter ou d'être affectée par une décision ou une activité du SMSI ;
    - les autorités compétentes.
- les exigences relatives à la sécurité des systèmes d'information à faire appliquer aux parties intéressées. Elles sont d'ordre :
  - règlementaire, notamment celles en matière de contrôle d'antécédent, de sensibilisation et de formation ;
  - contractuel et garantissent que les parties intéressées appliquent les exigences de cybersécurité définies et mises en œuvre par l'opérateur[16].

5.1.1.3. Domaine d'application et périmètre

Conformité niveau 3 et plus :

L'opérateur détermine le domaine d'application du SMSI, à savoir les limites et l'applicabilité. Pour ce faire, il prend en compte :

- les enjeux externes et internes ;
- les exigences ;
- les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.

[16] Règle 3 du guide d'hygiène informatique de l'ANSSI [8]

5.1.1.4. Interface avec les autres systèmes de management

Conformité niveau 3 et plus :

L'opérateur établit et formalise l'articulation entre le SMSI et les autres systèmes de management existants, qui peuvent être :

- un Système de Gestion de la Sécurité de l'aviation civile (*Safety Management System, SMS*) ;
- un Système de Gestion de la Sûreté (*Security Management System, SeMS).*

Cette articulation est plus ou moins naturelle à établir en fonction du choix de l'opérateur, à savoir :

- établir un SMSI indépendamment des autres systèmes de management existants, ou bien ;
- intégrer le SMSI à aux systèmes de management existants, dans le cadre d'un système de management intégré. Dans ce cas, l'opérateur décrit l'articulation entre le SMSI et les autres systèmes de management en particulier avec son système de gestion de la sécurité (SGS).

5.1.2.Formation

Conformité niveau 4 :

Outre les dispositions prévues au § 4.1.4.3, l'opérateur :

- s'assure que les équipes managériales sont formées à :
  - l'audit interne d'un SMSI ;
  - la gestion des incidents de cybersécurité, en cohérence avec les tâches qui leur sont confiées[17].
- conserve des informations documentées appropriées comme preuves.

5.1.3.Documentation

Conformité niveau 3 et plus :

L'opérateur décrit à travers une procédure de gestion documentaire, la manière dont il maîtrise les informations documentées :

La procédure de gestion documentaire précise :

- l'identification des types d'informations à documenter (imposé réglementairement ou jugé nécessaires à l'efficacité du système de management de la sécurité de l'information) ;
- les dispositions à appliquer lors de la création et de la mise à jour des informations documentées de l'opérateur. En particulier, l'opérateur s'assure que les éléments suivants sont appropriés :
  - identification et description (par exemple titre, date, auteur, numéro de référence) ;
  - format (par exemple langue, version logicielle, graphique) et support (par exemple papier, électronique) ;
  - examen et approbation du caractère approprié et pertinent des informations.
- l'objectif du contrôle exercé par l'opérateur, à savoir s'assurer que les informations documentées sont :
  - disponibles et conviennent à l'utilisation, où et quand elles sont nécessaires ;
  - correctement protégées (par exemple de toute perte de confidentialité, utilisation inappropriée ou perte d'intégrité).
- le contrôle exercé concerne, quand applicables :
  - la distribution, l'accès, la récupération et l'utilisation ;
  - le stockage et la conservation, y compris la préservation de la lisibilité ;
  - le contrôle des modifications;
  - la durée de conservation et suppression.
- les informations documentées d'origine externe que l'opérateur juge nécessaires à la planification et au fonctionnement du SMSI sont identifiées et maîtrisées.

[17] Guide de formation cybersécurité [18] - § 2.3. et § 2.4.

5.1.4. Communication

Conformité niveau 3 et plus :

L'opérateur détermine les besoins de communication interne et externe pertinents pour le SMSI, et notamment :
- sur quels sujets communiquer ;
- à quels moments communiquer ;
- avec qui communiquer ;
- qui doit communiquer ;
- les processus par lesquels la communication doit s'effectuer.

5.2. Planification du SMSI

Conformité niveau 3 et plus :

L'opérateur planifie le SMSI en s'appuyant sur la gestion des risques de niveau de conformité 3 et plus.

5.3. Mise en œuvre du SMSI

5.3.1. Organisation de la gestion des risques

Conformité niveau 3 et plus :

L'opérateur définit l'organisation de la gestion des risques et en précise :
- la structure et le positionnement ;
- les responsabilités des différents participants ;
- la périodicité et/ou les événements significatifs déclenchant une réunion ;
- les différents indicateurs de suivi d'avancement du plan de traitement des risques.

5.3.2. Missions de la gestion des risques

Conformité niveau 3 et plus :

Au travers de cette organisation, l'opérateur :
- procède à une réappréciation des risques et/ou ;
- planifie et met en œuvre :
  - les mesures standards[18] 1 et 4 et renforcée 2 ;
  - au moins 70% des mesures standards;
  - au moins 20% des mesures renforcées ;
  - les mesures complémentaires identifiées dans le plan de traitement des risques.
- contrôle l'avancée du plan de traitement des risques.

Conformité niveau 4 :

En outre, l'opérateur planifie et met en œuvre :
- au moins 80% des mesures standards;
- au moins 50% des mesures renforcées.

5.3.3. Résultats de la gestion des risques

Conformité niveau 3 et plus :

L'opérateur :
- produit un tableau de bord de suivi d'avancement du plan de traitement des risques ;
- conserve des informations documentées comme preuves des résultats de la gestion des risques.

[18] Voir Annexe 1 – Mesures de sécurité

5.4. Évaluation et amélioration du SMSI

5.4.1. Évaluation des performances de sécurité

5.4.1.1. Organisation de l'évaluation des performances de sécurité

Conformité niveau 4 :

L'opérateur définit l'organisation de l'évaluation des performances et précise :
- la structure et le positionnement ;
- les responsabilités des différents participants ;
- la périodicité et/ou les événements significatifs déclenchant une réunion ;
- les indicateurs :
    - de conformité du système de management de la sécurité de l'information ;
    - d'efficacité de la sécurité.

5.4.1.2. Missions de l'évaluation des performances

Conformité niveau 4 :

Au travers de cette organisation, l'opérateur évalue l'efficacité :
- de la gestion des risques :
    - Appréciation des risques ;
    - Traitement des risques.
- des mesures inscrites dans le plan de traitement des risques.

Par rapport :
- aux objectifs de sécurité des systèmes d'information définis dans la stratégie ;
- au retour d'expérience de la gestion des incidents.

En s'appuyant sur :
- les résultats :
    - des audits internes ;
    - des audits des autorités compétentes.
- son retour d'expérience.

5.4.1.3. Résultats de l'évaluation des performances

Conformité niveau 4 :

L'opérateur :
- produit un tableau de bord de suivi des performances de sécurité ;
- conserve des informations documentées comme preuves des résultats d'évaluation des performances.

5.4.2. Audits internes

5.4.2.1. Objectifs des audits internes

Conformité niveau 4 :

L'opérateur réalise des audits internes visant à évaluer :
- la conformité :
  - avec le présent document, du SMSI ;
  - des systèmes d'information critiques au regard de la sûreté avec les mesures prévues dans le plan de traitement du risque.
- la mise en œuvre efficace et la tenue à jour du SMSI.

5.4.2.2. Programme d'audits

Conformité niveau 4 :

L'opérateur définit un ou plusieurs programmes d'audits, prenant en compte :
- la démarche d'appréciation des risques ;
- la démarche de traitement des risques ;
- les résultats des audits précédents.

et précise :
- la fréquence, les méthodes et les responsabilités des audits ;
- les exigences de planification ;
- l'élaboration des rapports.

De plus l'opérateur :
- définit les critères d'audits et les périmètres de chaque audit ;
- sélectionne des auditeurs qui assurent l'objectivité et l'impartialité du processus d'audit.

5.4.2.3. Suivi du programme d'audit

Conformité niveau 4 :

L'opérateur assure le suivi du programme d'audit au sein du dispositif d'évaluation des performances.

5.4.2.4. Résultats des audits internes

Conformité niveau 4 :

L'opérateur :
- produit un tableau de bord de suivi du ou des programmes d'audits internes ;
- enrichit les tableaux de bord de suivis :
  - des performances de sécurité ;
  - des non-conformités et actions correctives avec les résultats des audits internes ;
- s'assure qu'il est rendu compte des résultats des audits à la direction concernée ;
- conserve des informations documentées comme preuves de la mise en œuvre du ou des programme(s) d'audit et des résultats d'audit.

5.4.3.Revue de direction

5.4.3.1. Revue de direction

Conformité niveau 3 et plus :

L'opérateur définit et précise :
- l'organisation et le positionnement de la revue de direction ;
- les responsabilités des différents participants ;
- la périodicité :
  - au moins 1 fois entre 2 audits de l'autorité, et/ou ;
  - les événements significatifs déclenchant la revue de direction (incident, changement de contexte etc.).

5.4.3.2. Missions de la revue de direction

Conformité niveau 3 et plus :

Sur la base :
- des changements de contexte de l'opérateur, notamment :
  - l'évolution de la menace ;
  - un changement de l'organisation ;
  - des changements des besoins et attentes des parties intéressées ;
  - une modification du domaine d'application.
- des résultats de l'appréciation des risques ;
- des tableaux de bord de suivi d'avancement du plan de traitement des risques.

L'opérateur identifie et décide des :
- actions préventives à mettre en œuvre ;
- modifications à apporter au SMSI : Organisation, besoins et attentes des parties intéressées, et du domaine d'application.

Conformité niveau 4 :

Pour prendre ses décisions, l'opérateur s'appuie également sur :
- des tableaux de bord de suivi d'avancement du plan de traitement des risques, des performances de sécurité et des actions correctives ;
- des résultats d'audits.

5.4.3.3. Conclusions de la revue de direction

Conformité niveau 3 et plus :

L'opérateur conserve des informations documentées comme preuves des conclusions des revues de direction.

5.4.4.Réaction aux non-conformités

5.4.4.1. Sources des non-conformités

Conformité niveau 1 et plus :

L'opérateur réagit aux non-conformités notifiées par les autorités compétentes.

Conformité niveau 4 :

L'opérateur réagit aux non-conformités :
- identifiées lors :
  - de l'évaluation des performances ;
  - des audits internes ;
  - de la gestion des incidents,
- notifiées par :
  - ses parties intéressées, en particulier les clients et les partenaires (fournisseurs, sous-traitants, etc.) ;
  - l'autorité compétente dans le cadre de sa surveillance, la DSAC.

5.4.4.2. Traitement des non-conformités

Conformité niveau 4 :

Lorsqu'une non-conformité est détectée, l'opérateur en :
- traite les conséquences ;
- identifie :
  - la ou les causes ;
  - si des non-conformités similaires existent ou pourraient se produire.

Sur la base de cette analyse, l'opérateur :
- détermine l'action corrective associée comme par exemple :
  - aucune action ;
  - un ajout, une suppression ou une modification d'une mesure de traitement du risque ;
  - une modification du système de management de la sécurité de l'information.
- planifie sa mise en œuvre ;
- évalue son efficacité.

5.4.4.3. Suivi des non-conformités

Conformité niveau 4 :

L'opérateur assure le suivi des non-conformités au sein du dispositif d'évaluation des performances et lors des revues de direction.

5.4.4.4. Résultat de la réaction aux non-conformités

Conformité niveau 4 :

L'opérateur produit un tableau de bord de suivi des non-conformités et actions correctives qui précise :
- la non-conformité et l'action corrective associée ;
- le statut de mise en œuvre et les délais ;
- l'évaluation de son efficacité.

L'opérateur conserve des informations documentées comme preuves des réactions à une non-conformité.

6. Cas particuliers des OIV et des OSE

Concernant le règlement (UE) n°2015/1998 [1] les OIV et OSE peuvent faire valoir la mesure d'équivalence prévue par ledit règlement mais uniquement pour les données et systèmes critiques relevant de la sûreté de l'aviation civile qui sont également :

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

Cependant cette équivalence ne s'applique pas pour les exigences règlementaires relatives à la vérification des antécédents. En effet, ils doivent s'y soumettre au même titre que les autres opérateurs.

Concernant le futur règlement (UE) *Part IS* [2], les OIV et les OSE ayant déjà mené des travaux en matière de sécurité des systèmes d'information dans le cadre des dispositifs LPM et NIS, peuvent s'appuyer dessus pour la mise en œuvre du SMSI, à condition d'avoir pris en considération les enjeux en matière de sécurité de l'aviation civile dans leurs démarches.

Concrètement, les OIV et les OSE peuvent s'appuyer sur

- leur PSSI pour la définition du SMSI et l'évaluation des performances ;
- leur analyse d'impacts ou leur démarche globale d'analyse de risques pour l'appréciation des risques ;
- les mesures de sécurité des systèmes d'information déjà mises en œuvre pour le traitement du risque. Ils n'ont pas obligation d'appliquer des mesures complémentaires ;
- leurs audits prévus dans le cadre de la LPM et de la NIS pour l'évaluation de leurs performances.

Annexe 1 - Mesures de sécurité des systèmes d'information

Le tableau ci-dessous présente les mesures de sécurité des systèmes d'information à considérer pour l'élaboration du plan d'actions ou du plan de traitement des risques. Elles sont extraites du Guide d'hygiène informatique [15] publié par l'ANSSI et constituent le socle minimal de sécurité des systèmes d'information. Deux niveaux d'implémentation y sont identifiés :

- Standard pour les niveaux de conformité 1 et 2 ;
- Renforcé pour les niveaux de conformité 3 et plus.

Le guide ne spécifie pas comment les mesures doivent être mises en œuvre, car cela dépend de chaque opérateur, mais fait référence à d'autres guides et référentiels de l'ANSSI qui apportent des indications.

A noter que certaines mesures ne sont pas pertinentes dans le domaine du transport aérien, elles ont été supprimées. D'autres mesures, quant à elles, relèvent de l'organisation de la sécurité des systèmes d'information ou de la gestion du risque et sont donc explicitement citées dans les chapitres du document traitant ces sujets. Une référence au dit chapitre est alors faite.

	Mesures de sécurité des systèmes d'information	Standard	Renforcé	§
1	Former les équipes opérationnelles à la sécurité des systèmes d'information			§4.1.4. §5.1.2
2	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique			§4.1.4.
3	Maîtriser les risques de l'infogérance			§4.1.2. §5.1.1.2.
4	Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau			§4.2.2.2.
5	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour			
6	Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs			§4.1.3.
7	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés			
8	Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateurs/administrateurs			
9	Attribuer les bons droits sur les ressources sensibles du système d'information			
10	Définir et vérifier des règles de choix et de dimensionnement des mots de passe			§4.1.3.
11	Protéger les mots de passe stockés sur les systèmes			
12	Changer les éléments d'authentification par défaut sur les équipements et services			
13	Privilégier lorsque c'est possible une authentification forte			
14	Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique			§4.1.3.
15	Se protéger des menaces relatives à l'utilisation de supports amovibles			
16	Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité			
17	Activer et configurer le pare-feu local des postes de travail			
18	Chiffrer les données sensibles transmises par voie Internet			
19	Segmenter le réseau et mettre en place un cloisonnement entre ces zones			
20	S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages			
21	Utiliser des protocoles sécurisés dès qu'ils existent			

22	Mettre en place une passerelle d'accès sécurisé à Internet			
	Mesures de sécurité	**Standard**	**Renforcé**	**§**
23	Cloisonner les services visibles depuis Internet du reste du système d'information			
25	Sécuriser les interconnexions réseau dédiées avec les partenaires			
26	Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques			
27	Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système			
28	Utiliser un réseau dédié et cloisonné pour l'administration du système d'information			
29	Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail			
30	Prendre des mesures de sécurisation physique des terminaux nomades			
31	Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable			
32	Sécuriser la connexion réseau des postes utilisés en situation de nomadisme			
33	Adopter des politiques de sécurité dédiées aux terminaux mobiles			
34	Définir une politique de mise à jour des composants du système d'information			§4.1.3.
35	Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles			§4.1.3.
36	Activer et configurer les journaux des composants les plus importants			
37	Définir et appliquer une politique de sauvegarde des composants critiques			§4.1.3.
38	Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives			§5.4.
39	Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel			§3.3
40	Définir une procédure de gestion des incidents de sécurité			§4.1.3.

Annexe 2 – Niveaux de conformité et dispositions du 3CF

Chapitres du 3CF			Niveaux de conformité au 3CF			
			N. 1	N. 2	N. 3	N. 4
3. Gouvernance	3.1. Engagement de la direction					
	3.2. Stratégie et objectifs					
	3.3. Gestion des ressources, rôles et responsabilités de la sécurité des systèmes d'information					
	3.4. Approbation					
	3.5. Système de management de la sécurité de l'information					
	3.6. Cohérence de la stratégie, des objectifs et du SMSI					
4. Gestion de la sécurité de l'information	4.1. Organisation de la sécurité des systèmes d'information	4.1.1. Missions et enjeux				
		4.1.2. Besoin et attentes des parties intéressées				
		4.1.3. Politiques et procédures				
		4.1.4. Personnels et compétences				
	4.2. Gestions des risques	4.2.1. Méthodologie de gestion des risques				
		4.2.2. Appréciation des risques				
		4.2.3.1.1. Élaboration du plan d'actions				
		4.2.3.1.2. Actions et mesures complémentaires pour le traitement du risque				
		4.2.3.1.3. Élaboration du plan de traitement des risques				
		4.2.3.1.4. Évaluation des risques résiduels				
		4.2.3.1.5. Approbation des risques				
		4.2.4. Mise en œuvre des mesures de sécurité des systèmes d'information				
5. Système de management de la sécurité de l'information	5.1. Définition du SMSI	5.1.1.1. Missions et enjeux				
		5.1.1.2. Besoin et attentes des parties intéressées				
		5.1.1.3. Domaine d'application et périmètre				
		5.1.1.4. Interface avec les autres systèmes de management				
		5.1.2. Formation				
		5.1.3. Documentation				
		5.1.4. Communication				
	5.2. Planification du SMSI					
	5.3.2. Missions de la gestion des risques					
	5.4. Évaluation et amélioration du SMSI	5.4.1. Évaluation des performances de sécurité				
		5.4.2. Audits internes				
		5.4.3. Revue de direction				
		5.4.4. Réaction aux non-conformités				

Disposition de niveau 1

Disposition de niveau 2

Disposition de niveau 3

Disposition de niveau 4

Pas de disposition

Annexe 3 - Grille de conformité réglementaire

Chapitres du 3CF			Règlement (UE) n°2015/1998	Règlement (UE) *Part IS*
3. Gouvernance	3.1. Engagement de la direction			
	3.2. Stratégie et objectifs			
	3.3. Gestion des ressources, rôles et responsabilités de la sécurité des systèmes d'information			
	3.4. Approbation			
	3.5. Système de management de la sécurité de l'information			
	3.6. Cohérence de la stratégie, des objectifs et du SMSI			
4. Gestion de la sécurité de l'information	4.1. Organisation de la sécurité des systèmes d'information	4.1.1. Missions et enjeux		
		4.1.2. Besoin et attentes des parties intéressées		
		4.1.3. Politiques et procédures		
		4.1.4. Personnels et compétences		
	4.2. Gestions des risques	4.2.1. Méthodologie de gestion des risques		
		4.2.2. Appréciation des risques		
		4.2.3.1.1. Élaboration du plan d'actions		
		4.2.3.1.2. Actions et mesures complémentaires pour le traitement du risque		
		4.2.3.1.3. Élaboration du plan de traitement des risques		
		4.2.3.1.4. Évaluation des risques résiduels		
		4.2.3.1.5. Approbation des risques		
		4.2.4. Mise en œuvre des mesures de sécurité des systèmes d'information		
5. Système de management de la sécurité de l'information	5.1. Définition du SMSI	5.1.1.1. Missions et enjeux		
		5.1.1.2. Besoin et attentes des parties intéressées		
		5.1.1.3. Domaine d'application et périmètre		
		5.1.1.4. Interface avec les autres systèmes de management		
		5.1.2. Formation		
		5.1.3. Documentation		
		5.1.4. Communication		
	5.2. Planification du SMSI			
	5.3.2. Missions de la gestion des risques			
	5.4. Évaluation et amélioration du SMSI	5.4.1. Évaluation des performances de sécurité		
		5.4.2. Audits internes		
		5.4.3. Revue de direction		
		5.4.4. Réaction aux non-conformités		

Exigences du règlement (UE) n°2015/1998

Exigences du règlement (UE) *Part IS*, connues à date

Terminologie

Acronymes	Significations
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CAMO	*Continuing Airworthiness Management Organisation*
DOA	*Design Organisation Approval*
DSAC	Direction de la Sécurité de l'Aviation Civile
FNAM	Fédération Nationale de l'Aviation Marchande
FSTD	*Flight Simulation Training Device*
LPM	Loi de Programmation Militaire
NIS	*Network and Information Security*
OIV	Opérateur d'Importance Vitale
OSE	Opérateur de Service Essentiel
Part - IS	*Part - Information Security*
POA	*Production Organisation Approval*
SeMS	*Security Management System* - Système de management de la sûreté
SGS	Système de Gestion de la Sécurité (de l'aviation civile)
SIE	Système d'Information Essentiel
SIIV	Système d'Information d'Importance Vitale
SMSI	Système de Management de la Sécurité de l'Information
SSI	Sécurité des Systèmes d'Information
UAF	Union des Aéroports Français
UE	Union Européenne
UAS	*Unmanned Aircraft system* - Systèmes d'aéronefs sans équipage à bord
U-Space	Une zone géographique UAS désignée par les États membres, dans laquelle les exploitations d'UAS ne sont autorisées qu'avec l'appui de services U-spac
USSP	*U-space Service Provider* - Un service *U-space* est un service reposant sur des services numériques et l'automatisation de fonctions, conçu pour garantir à un grand nombre d'*UAS* un accès sécurisé, sûr et efficace à l'espace aérien *U-space*

Bibliographie

[1] *Règlement d'exécution (UE) 2019/1583 de la commission du 25 septembre 2019 modifiant le règlement d'exécution (UE) 2015/1998 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*, Union Européenne, Septembre 2019.

[2] *Règlement (UE) Part-IS*, Union Européenne, Opinion en cours à l'EASA

[3] *Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transport aérien » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense*, Legifrance, Août 2016.

[4] *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.

[5] *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.

[6] *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.

[7] *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.

[8] *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,* Union Européenne, Aout 2012.

[9] *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 tâche,* Union Européenne, Novembre 2014.

[10] *Règlement (UE) 965/2012 de la commission du 5 octobre 2012 déterminant les exigences techniques et les procédures administratives applicables aux opérations aériennes conformément au règlement (CE) no 216/2008 du Parlement européen et du Conseil,* Union Européenne, Octobre 2012.

[11] *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 conformément au règlement (CE) no 216/2008 du Parlement européen et du Conseil,* Union Européenne, Novembre 2011.

[12] *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 conformément au règlement (CE) n ° 216/2008 du Parlement européen et du Conseil, modifiant le règlement d'exécution (UE) n ° 923/2012 de la Commission et abrogeant le règlement (UE) n ° 805/2011 de la Commission,* Union Européenne, Février 2015.

[13] *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, abrogeant le règlement (CE) 482/2008, les règlements d'exécution (UE) 1034/2011, (UE) 1035/2011 et (UE) 2016/1377 et modifiant le règlement (UE) 677/2011,* Union Européenne, Mars 2017.

[14] *Règlement (UE) 139/2014 de la commission du 12 février 2014 établissant des exigences et des procédures administratives relatives aux aérodromes conformément au règlement (CE) 216/2008 du Parlement européen et du Conseil,* Union Européenne, Février 2014.

[15] *Guide d'hygiène informatique*, ANSSI, Version 2.0, Septembre 2017.

[16] *Code des transports*, Legifrance, Avril 2021.

[17] *Guide de conception de sessions de sensibilisation cybersécurité*, DSAC, Version1.0, Septembre 2021

[18] *Guide de formation cybersécurité*, DSAC, Version1.0, Septembre 2021

[19] *Fonctions critiques au regard de la sûreté du transport aérien,* DSAC, Version 1.0, Septembre 2021

[20] *ISO/CEI 27005 : 2018 – Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information*.

[21] *Guide EBIOS Risk Manager*, ANSSI, Version 1.1, Décembre 2018.

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