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 imposées aux organismes relevant des règlements (UE) nº 748/2012 et (UE) nº 139/2014 de la Commission et modifiant les règlements (UE) nº 748/2012 et (UE) nº 139/2014 de la Commission

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le 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 et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) nº 2111/2005, (CE) nº 1008/2008, (UE) nº 996/2010, (UE) nº 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) nº 552/2004 et (CE) nº 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) nº 3922/91 du Conseil ([1]), et notamment son article 19, paragraphe 1, point g), et son article 39, paragraphe 1, point b),

considérant ce qui suit:

(1) Conformément aux exigences essentielles énoncées à l'annexe II, point 3.1 b), du règlement (UE) 2018/1139, les organismes de conception et de production sont tenus de mettre en œuvre et d'entretenir un système de gestion afin d'assurer la gestion des risques pour la sécurité.

(2) En outre, conformément aux exigences essentielles énoncées à l'annexe VII, points 2.2.1 et 5.2, du règlement (UE) 2018/1139, les exploitants d'aérodrome et les prestataires de services de gestion d'aire de trafic sont tenus de mettre en œuvre et de maintenir un système de gestion afin d'assurer la gestion des risques pour la sécurité.

(3) Les risques pour la sécurité visés aux considérants 1 et 2 peuvent provenir de sources diverses, parmi lesquelles des défauts de conception et d'entretien, des aspects liés aux performances humaines, des menaces pour l'environnement et des menaces relatives à la sécurité de l'information. Par conséquent, les systèmes de gestion mis en œuvre par les organismes visés aux considérants 1 et 2 devraient tenir compte non seulement des risques pour la sécurité découlant d'événements fortuits, mais aussi de ceux découlant de menaces relatives à la sécurité de l'information lorsque des failles existantes peuvent être exploitées par des personnes animées d'intentions malveillantes. Ces risques liés à la sécurité de l'information ne cessent de croître dans le contexte de l'aviation civile, les systèmes d'information actuels étant de plus en plus interconnectés et ciblés par des acteurs malveillants.

(4) Les risques associés à ces systèmes d'information ne se limitent pas à d'éventuelles attaques dans le cyberespace, mais comprennent également des menaces pesant sur les processus et procédures ainsi que sur les performances des êtres humains.

(5) De nombreux organismes recourent déjà à des normes internationales, telles que la norme ISO 27001, pour assurer la sécurité des données et des informations numériques. Il est possible que ces normes ne tiennent pas pleinement compte de toutes les spécificités de l'aviation civile.

(6) Il convient, dès lors, d'établir des exigences pour la gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.

(7) Il est essentiel que ces exigences couvrent les différents domaines de l'aviation et leurs interfaces car l'aviation constitue un système de systèmes fortement interconnecté. Par conséquent, elles devraient s'appliquer à tous les organismes qui sont déjà tenus de disposer d'un système de gestion conforme à la législation existante de l'Union en matière de sécurité aérienne.

(8) Les exigences énoncées dans le présent règlement devraient être appliquées de manière cohérente dans tous les domaines de l'aviation, en réduisant au minimum les répercussions sur la législation de l'Union en matière de sécurité aérienne déjà applicable à ces domaines.

([1]) JO L 212 du 22.8.2018, p. 1.

(9) Les exigences fixées dans le présent règlement devraient être sans préjudice des exigences en matière de sécurité de l'information et de cybersécurité énoncées au point 1.7 de l'annexe du règlement d'exécution (UE) 2015/1998 de la Commission ([2]) et à l'article 14 de la directive (UE) 2016/1148 du Parlement européen et du Conseil ([3]).

(10) La définition relative à la sécurité de l'information aux fins du présent acte juridique ne devrait pas être interprétée comme s'écartant de celle relative à la sécurité des réseaux et des systèmes d'information figurant dans la directive (UE) 2016/1148.

(11) Afin d'éviter la duplication des exigences légales, lorsque des organismes relevant du présent règlement sont déjà soumis à des exigences de sécurité découlant d'autres actes de l'Union visés au considérant 9, dont l'effet équivaut à celui des dispositions du présent règlement, le respect de ces exigences de sécurité devrait valoir respect des exigences fixées dans le présent règlement.

(12) Les organismes relevant du présent règlement qui sont déjà soumis aux exigences de sécurité découlant du règlement d'exécution (UE) 2015/1998 devraient également se conformer aux exigences de l'annexe I (partie IS.D.OR.230 «Système de comptes rendus externe en matière de sécurité de l'information») du présent règlement, dès lors que le règlement d'exécution (UE) 2015/1998 ne contient aucune disposition liée aux comptes rendus externes des incidents relatifs à la sécurité de l'information.

(13) Il convient de modifier les règlements (UE) n° 748/2012 ([4]) et (UE) n° 139/2014 ([5]) de la Commission de manière à assurer le lien entre les systèmes de gestion prescrits par les règlements énumérés ci-dessus et les exigences en matière de gestion de la sécurité de l'information prévues par le présent règlement.

(14) Afin de donner aux organismes un délai suffisant pour se conformer aux nouvelles règles et procédures instaurées par le présent règlement, il convient que celui-ci entre en application 3 ans après la date d'entrée en vigueur.

(15) Les exigences fixées par le présent règlement sont fondées sur l'avis n° 03/2021 ([6]) émis par l'Agence conformément à l'article 75, paragraphe 2, points b) et c), et à l'article 76, paragraphe 1, du règlement (UE) 2018/1139.

(16) Conformément à l'article 128, paragraphe 4, du règlement (UE) 2018/1139, la Commission a consulté les experts désignés par chaque État membre, dans le respect des principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer» ([7]),

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Objet

Le présent règlement énonce les exigences auxquelles doivent satisfaire les organismes visés à l'article 2 pour déterminer et gérer les risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne et d'affecter les données et systèmes de technologies de l'information et de la communication utilisés aux fins de l'aviation civile, pour détecter les événements liés à la sécurité de l'information et pour déterminer ceux qui sont considérés comme des incidents de sécurité de l'information susceptibles d'avoir des répercussions sur la sécurité aérienne, réagir à ces incidents de sécurité de l'information et garantir le rétablissement après incident.

([2]) 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 (JO L 299 du 14.11.2015, p. 1).

([3]) Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

([4]) Règlement (UE) n° 748/2012 de la Commission du 3 août 2012 établissant des règles d'application pour la certification de navigabilité et environnementale des aéronefs et produits, pièces et équipements associés, ainsi que pour la certification des organismes de conception et de production (JO L 224 du 21.8.2012, p. 1).

([5]) Règlement (UE) n° 139/2014 de la Commission du 12 février 2014 établissant des exigences et des procédures administratives relatives aux aérodromes conformément au règlement (CE) n° 216/2008 du Parlement européen et du Conseil (JO L 44 du 14.2.2014, p. 1).

([6]) https://www.easa.europa.eu/document-library/opinions

([7]) JO L 123 du 12.5.2016, p. 1.

Article 2

Champ d'application

1. Le présent règlement s'applique aux organismes suivants:

a) organismes de production et organismes de conception relevant de l'annexe I (partie 21), section A, sous-parties G et J, du règlement (UE) nº 748/2012, à l'exception des organismes de conception et de production qui sont uniquement associés à la conception et/ou à la production d'aéronefs ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) nº 748/2012;

b) exploitants d'aérodrome et prestataires de services de gestion des aires de trafic relevant de l'annexe III «Partie exigences applicables aux organismes (partie ADR.OR)» du règlement (UE) nº 139/2014.

2. Le présent règlement est sans préjudice des exigences en matière de sécurité de l'information et de cybersécurité énoncées au point 1.7 de l'annexe du règlement d'exécution (UE) 2015/1998 et à l'article 14 de la directive (UE) 2016/1148.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) «sécurité de l'information»: la préservation de la confidentialité, de l'intégrité, de l'authenticité et de la disponibilité des réseaux et des systèmes d'information;

2) «événement lié à la sécurité de l'information»: 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;

3) «incident»: tout événement ayant un impact négatif sur la sécurité des réseaux et des systèmes d'information au sens de l'article 4, paragraphe 7, de la directive (UE) 2016/1148;

4) «risque lié à la sécurité de l'information»: 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;

5) «menace»: 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;

6) «vulnérabilité»: 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.

Article 4

Exigences découlant d'autres dispositions législatives de l'Union

1. Lorsqu'un organisme visé à l'article 2 satisfait à des exigences de sécurité énoncées à l'article 14 de la directive (UE) 2016/1148 qui sont équivalentes aux exigences fixées dans le présent règlement, le respect desdites exigences de sécurité vaut respect des exigences fixées dans le présent règlement.

2. Lorsqu'un organisme visé à l'article 2 est un exploitant ou une entité visée dans les programmes nationaux de sûreté de l'aviation civile des États membres établis conformément à l'article 10 du règlement (CE) nº 300/2008 du Parlement européen et du Conseil ([8]), les exigences de cybersécurité figurant au point 1.7 de l'annexe du règlement d'exécution (UE) 2015/1998 sont considérées comme équivalentes aux exigences fixées dans le présent règlement, sauf en ce qui concerne le point IS.D.OR.230 de l'annexe du présent règlement, qui doit être respecté.

([8]) Règlement (CE) nº 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 et abrogeant le règlement (CE) nº 2320/2002 (JO L 97 du 9.4.2008, p. 72).

3. La Commission, après consultation de l'AESA et du groupe de coopération visé à l'article 11 de la directive (UE) 2016/1148, peut publier des lignes directrices pour l'évaluation de l'équivalence des exigences fixées dans le présent règlement et dans la directive (UE) 2016/1148.

Article 5

Autorité compétente

1. L'autorité chargée de certifier et de contrôler le respect du présent règlement est:

a) à l'égard des organismes visés à l'article 2, point a), l'autorité compétente désignée conformément à l'annexe I (partie 21) du règlement (UE) nº 748/2012;

b) à l'égard des organismes visés à l'article 2, point b), l'autorité compétente désignée conformément à l'annexe III (partie ADR.OR) du règlement (UE) nº 139/2014.

2. Les États membres peuvent, aux fins du présent règlement, désigner une entité indépendante et autonome chargée de remplir le rôle et les responsabilités assignés aux autorités compétentes visées au paragraphe 1. Dans ce cas, des mesures de coordination sont établies entre cette entité et les autorités compétentes visées au paragraphe 1, afin d'assurer une surveillance efficace de toutes les exigences auxquelles l'organisme est tenu de satisfaire.

Article 6

Modification du règlement (UE) nº 748/2012

L'annexe I (partie 21) du règlement (UE) nº 748/2012 est modifiée comme suit:

1) La table des matières est modifiée comme suit:

a) le titre suivant est inséré après le titre 21.A.139:

«**21.A.139A Système de gestion de la sécurité de l'information**»;

b) le titre suivant est inséré après le titre 21.A.239:

«**21.A.239A Système de gestion de la sécurité de l'information**».

2) Le point 21.A.139A suivant est inséré après le point 21.A.139:

«**21.A.139A Système de gestion de la sécurité de l'information**

Outre le système de gestion de la production requis par le point 21.A.139, l'organisme de production établit, met en œuvre et tient à jour un système de gestion de la sécurité de l'information conformément au règlement délégué (UE) 2022/1645 de la Commission (*) afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.

(*) 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 imposées aux organismes relevant des règlements (UE) nº 748/2012 et (UE) nº 139/2014 de la Commission et modifiant les règlements (UE) nº 748/2012 et (UE) nº 139/2014 de la Commission (JO L 248 du 26.9.2022, p. 18).».

3) Le point 21.A.239A suivant est inséré après le point 21.A.239:

«**21.A.239A Système de gestion de la sécurité de l'information**

Outre le système de gestion de la conception requis par le point 21.A.239, l'organisme de conception établit, met en œuvre et tient à jour un système de gestion de la sécurité de l'information conformément au règlement délégué (UE) 2022/1645 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.».

Article 7

Modification du règlement (UE) nº 139/2014

L'annexe III (partie ADR.OR) du règlement (UE) nº 139/2014 est modifiée comme suit:

1) Le point suivant ADR.OR.D.005A est inséré après le point ADR.OR.D.005:

«**ADR.OR.D.005A Système de gestion de la sécurité de l'information**

L'exploitant d'aérodrome établit, met en œuvre et tient à jour un système de gestion de la sécurité de l'information conformément au règlement délégué (UE) 2022/1645 de la Commission (*) afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.

(*) 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 imposées aux organismes relevant des règlements (UE) nº 748/2012 et (UE) nº 139/2014 de la Commission et modifiant les règlements (UE) nº 748/2012 et (UE) nº 139/2014 de la Commission (JO L 248 du 26.9.2022, p. 18).».

2) Le point ADR.OR.D.007 est remplacé par le texte suivant:

«**ADR.OR.D.007 Gestion des données et des informations aéronautiques**

a) Dans le cadre de son système de gestion, l'exploitant d'aérodrome met en œuvre et tient à jour un système de gestion de la qualité couvrant les activités suivantes:

1) ses activités liées aux données aéronautiques;

2) ses activités de fourniture d'informations aéronautiques.

b) Dans le cadre de son système de gestion, l'exploitant d'aérodrome établit un système de gestion de la sûreté afin de garantir la sécurité des données opérationnelles qu'il reçoit, produit ou utilise d'une autre manière, de sorte que l'accès à ces données opérationnelles soit réservé aux seules personnes autorisées.

c) Le système de gestion de la sûreté définit les éléments suivants:

1) les procédures relatives à l'évaluation et à l'atténuation des risques dans le domaine de la sécurité des données, à la surveillance et à l'amélioration de la sûreté, aux évaluations de la sûreté et à la diffusion des enseignements;

2) les moyens destinés à déceler les manquements à la sûreté et à alerter le personnel par des signaux d'avertissement appropriés;

3) les moyens de contrôler les effets des manquements à la sûreté et d'identifier les mesures de rétablissement et les procédures d'atténuation permettant d'en éviter la réapparition.

d) L'exploitant d'aérodrome s'assure de l'habilitation de sûreté de son personnel en ce qui concerne la sécurité des données aéronautiques.

e) Les aspects relatifs à la sécurité de l'information sont gérés conformément au point ADR.OR.D.005A.».

3) Le point suivant ADR.OR.F.045A est inséré après le point ADR.OR.F.045:

«**ADR.OR.F.045A Système de gestion de la sécurité de l'information**

L'organisme chargé de la fourniture des services de gestion des aires de trafic établit, met en œuvre et tient à jour un système de gestion de la sécurité de l'information conformément au règlement délégué (UE) 2022/1645 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.».

Article 8

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il entre en application le 16 octobre 2025.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 14 juillet 2022.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

SÉCURITÉ DE L'INFORMATION — EXIGENCES APPLICABLES À L'ORGANISME

[PARTIE-IS.D.OR]

IS.D.OR.100 Champ d'application

IS.D.OR.200 Système de gestion de la sécurité de l'information

IS.D.OR.205 Évaluation des risques liés à la sécurité de l'information

IS.D.OR.210 Traitement des risques liés à la sécurité de l'information

IS.D.OR.215 Système de comptes rendus interne en matière de sécurité de l'information

IS.D.OR.220 Incidents de sécurité de l'information — détection, réaction et rétablissement

IS.D.OR.225 Réponse aux constatations notifiées par l'autorité compétente

IS.D.OR.230 Système de comptes rendus externe en matière de sécurité de l'information

IS.D.OR.235 Sous-traitance des activités de gestion de la sécurité de l'information

IS.D.OR.240 Exigences en matière de personnel

IS.D.OR.245 Archivage

IS.D.OR.250 Manuel de gestion de la sécurité de l'information (MGSI)

IS.D.OR.255 Modification du système de gestion de la sécurité de l'information

IS.D.OR.260 Amélioration constante

IS.D.OR.100 Champ d'application

La présente partie établit les exigences auxquelles doivent satisfaire les organismes visés à l'article 2 du présent règlement.

IS.D.OR.200 Système de gestion de la sécurité de l'information (SGSI)

a) Afin d'atteindre les objectifs énoncés à l'article 1er, l'organisme doit établir, mettre en œuvre et tenir à jour un système de gestion de la sécurité de l'information (SGSI) qui garantit que l'organisme:

1) met en place une politique en matière de sécurité de l'information définissant les principes généraux de l'organisme en ce qui concerne l'incidence potentielle des risques liés à la sécurité de l'information sur la sécurité aérienne;

2) recense et analyse les risques liés à la sécurité de l'information conformément au point IS.D.OR.205;

3) définit et met en œuvre des mesures de traitement des risques liés à la sécurité de l'information conformément au point IS.D.OR.210;

4) met en œuvre un système de comptes rendus interne en matière de sécurité de l'information conformément au point IS.D.OR.215;

5) définit et met en œuvre, conformément au point IS.D.OR.220, les mesures requises pour détecter les événements liés à la sécurité de l'information, recense les événements qui sont considérés comme des incidents susceptibles d'avoir des répercussions sur la sécurité aérienne, sauf dans les cas autorisés par le point IS.D.OR.205 e), réagit à ces incidents de sécurité de l'information et garantit le rétablissement après incident;

6) met en œuvre les mesures qui ont été notifiées par l'autorité compétente en réaction immédiate à un incident de sécurité de l'information ou à une vulnérabilité ayant une incidence sur la sécurité aérienne;

7) prend les mesures qui s'imposent, conformément au point IS.D.OR.225, pour remédier aux constatations notifiées par l'autorité compétente;

8) met en œuvre un système de comptes rendus externe conformément au point IS.D.OR.230 pour permettre à l'autorité compétente de prendre les mesures qui s'imposent;

9) satisfait aux exigences énoncées au point IS.D.OR.235 lorsqu'il sous-traite une partie des activités visées au point IS.D.OR.200 à d'autres organismes;

10) satisfait aux exigences en matière de personnel énoncées au point IS.D.OR.240;

11) satisfait aux exigences en matière d'archivage énoncées au point IS.D.OR.245;

12) vérifie que l'organisme respecte les exigences du présent règlement et fournit un retour d'information sur les constatations au dirigeant responsable ou, dans le cas des organismes de conception, au responsable de l'organisme de conception, afin de garantir la mise en œuvre effective des mesures correctives;

13) protège, sans préjudice des exigences applicables en matière de comptes rendus des incidents, la confidentialité de toute information que l'organisme aurait reçue d'autres organismes, en fonction de son niveau de sensibilité.

b) Afin de satisfaire en permanence aux exigences visées à l'article 1er, l'organisme doit mettre en œuvre un processus d'amélioration constante conformément au point IS.D.OR.260.

c) L'organisme doit documenter, conformément au point IS.D.OR.250, tous les processus, procédures, rôles et responsabilités clés requis pour se conformer au point IS.D.OR.200 a) et établir un processus de modification de cette documentation. Les modifications apportées à ces processus, procédures, rôles et responsabilités doivent être gérées conformément au point IS.D.OR.255.

d) Les processus, procédures, rôles et responsabilités établis par l'organisme pour se conformer au point IS.D.OR.200 a) doivent correspondre à la nature et à la complexité de ses activités, sur la base d'une évaluation des risques liés à la sécurité de l'information inhérents à ces activités, et peuvent être intégrés dans d'autres systèmes de gestion existants déjà mis en œuvre par l'organisme.

e) Sans préjudice de l'obligation de se conformer aux exigences en matière de comptes rendus énoncées dans le règlement (UE) nº 376/2014 du Parlement européen et du Conseil [1] et aux exigences du point IS.D.OR.200 a), point 13), l'organisme peut recevoir l'autorisation de l'autorité compétente de ne pas mettre en œuvre les exigences visées aux points a) à d) et les exigences connexes énoncées aux points IS.D.OR.205 à IS.D.OR.260 s'il démontre à la satisfaction de cette autorité que ses activités, ses installations et ses ressources, ainsi que les services qu'il exploite, fournit, reçoit et gère ne présentent aucun risque en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne, ni pour lui-même ni pour d'autres organismes. L'autorisation doit reposer sur une évaluation documentée des risques liés à la sécurité de l'information effectuée par l'organisme ou un tiers conformément au point IS.D.OR.205 et examinée et approuvée par son autorité compétente.

L'autorité compétente examinera le maintien de la validité de cette autorisation à l'issue du cycle d'audit de supervision applicable et chaque fois que des modifications sont mises en œuvre dans le cadre des travaux de l'organisme.

IS.D.OR.205 Évaluation des risques liés à la sécurité de l'information

a) L'organisme doit recenser tous ceux de ses éléments qui sont susceptibles d'être exposés à des risques liés à la sécurité de l'information. Il s'agit notamment des éléments suivants:

1) les activités, installations et ressources de l'organisme, ainsi que les services qu'il exploite, fournit, reçoit ou gère;

2) les équipements, systèmes, données et informations qui contribuent au fonctionnement des éléments énumérés au point 1).

b) L'organisme doit déterminer les interfaces qu'il partage avec d'autres organismes et qui pourraient entraîner une exposition mutuelle à des risques liés à la sécurité de l'information.

c) En ce qui concerne les éléments et interfaces visés aux points a) et b), l'organisme doit recenser les risques liés à la sécurité de l'information qui pourraient avoir une incidence sur la sécurité aérienne. Pour chaque risque recensé, l'organisme doit:

1) attribuer un niveau de risque selon une classification prédéfinie qu'il a établie;

[1] Règlement (UE) nº 376/2014 du Parlement européen et du Conseil du 3 avril 2014 concernant les comptes rendus, l'analyse et le suivi d'événements dans l'aviation civile, modifiant le règlement (UE) nº 996/2010 du Parlement européen et du Conseil et abrogeant la directive 2003/42/CE du Parlement européen et du Conseil et les règlements de la Commission (CE) nº 1321/2007 et (CE) nº 1330/2007 (JO L 122 du 24.4.2014, p. 18).

2) associer chaque risque et son niveau à l'élément ou à l'interface correspondant(e) déterminé(e) conformément aux points a) et b).

La classification prédéfinie visée au point 1) doit tenir compte du risque de réalisation du scénario de menace et de la gravité de ses conséquences pour la sécurité. Sur la base de cette classification, et compte tenu du fait que l'organisme dispose ou non d'un processus de gestion des risques structuré et reproductible pour les opérations, l'organisme doit être en mesure d'établir si le risque est acceptable ou s'il doit être traité conformément au point IS.D.OR.210.

Afin de faciliter la comparabilité des évaluations des risques, l'attribution du niveau de risque conformément au point 1) doit tenir compte des informations pertinentes obtenues en coordination avec les organismes visés au point b).

d) L'organisme examine et met à jour l'évaluation des risques effectuée conformément aux points a), b) et c) dans l'une des situations suivantes:

1) il y a un changement dans les éléments exposés à des risques liés à la sécurité de l'information;

2) il y a un changement dans les interfaces entre l'organisme et d'autres organismes, ou dans les risques communiqués par les autres organismes;

3) il y a un changement dans les informations ou connaissances utilisées pour le recensement, l'analyse et la classification des risques;

4) l'analyse des incidents de sécurité de l'information a permis de tirer des enseignements.

IS.D.OR.210 Traitement des risques liés à la sécurité de l'information

a) L'organisme doit élaborer des mesures pour faire face aux risques inacceptables recensés conformément au point IS.D.OR.205, les mettre en œuvre en temps utile et vérifier le maintien de leur efficacité. Ces mesures doivent permettre à l'organisme:

1) de contrôler les circonstances qui contribuent à la réalisation effective du scénario de menace;

2) de diminuer les conséquences sur la sécurité aérienne liées à la concrétisation du scénario de menace;

3) d'éviter les risques.

Ces mesures ne doivent pas introduire de nouveaux risques potentiels inacceptables pour la sécurité aérienne.

b) La personne visée aux points IS.D.OR.240 a) et b), et les autres membres du personnel de l'organisme concernés doivent être informés des résultats de l'évaluation des risques effectuée conformément au point IS.D.OR.205, des scénarios de menace correspondants et des mesures à mettre en œuvre.

L'organisme doit également informer les organismes avec lesquels il partage une interface conformément au point IS.D.OR.205 b) de tout risque commun à tous les organismes.

IS.D.OR.215 Système de comptes rendus interne en matière de sécurité de l'information

a) L'organisme établit un système de comptes rendus interne permettant le recensement et l'évaluation des événements liés à la sécurité de l'information, y compris ceux qui doivent être signalés conformément au point IS.D.OR.230.

b) Ce système et la procédure visée au point IS.D.OR.220 doivent permettre à l'organisme:

1) de recenser les événements signalés conformément au point a) qui sont considérés comme des incidents de sécurité de l'information ou des vulnérabilités susceptibles d'avoir une incidence sur la sécurité aérienne;

2) de déterminer les causes des incidents de sécurité de l'information et des vulnérabilités recensés conformément au point 1) et les facteurs qui y contribuent, et de les traiter dans le cadre du processus de gestion des risques liés à la sécurité de l'information conformément aux points IS.D.OR.205 et IS.D.OR.220;

3) de procéder à une évaluation de toutes les informations connues et pertinentes relatives aux incidents de sécurité de l'information et aux vulnérabilités recensés conformément au point 1);

4) de veiller à la mise en œuvre d'une méthode de diffusion des informations en interne, en tant que de besoin.

c) Tout organisme sous-traitant susceptible d'exposer l'organisme à des risques liés à la sécurité de l'information pouvant avoir une incidence sur la sécurité aérienne est tenu de lui rendre compte des événements liés à la sécurité de l'information. Ces comptes rendus doivent être soumis selon les procédures établies dans les arrangements contractuels spécifiques et être évalués conformément au point b).

d) L'organisme doit coopérer dans le cadre des enquêtes avec tout autre organisme qui a contribué de manière significative à la sécurité de l'information dans le cadre de ses propres activités.

e) L'organisme peut intégrer ce système de comptes rendus à d'autres systèmes de comptes rendus qu'il a déjà mis en œuvre.

IS.D.OR.220 Incidents de sécurité de l'information — détection, réaction et rétablissement

a) Sur la base des résultats de l'évaluation des risques effectuée conformément au point IS.D.OR.205 et des résultats du traitement des risques effectué conformément au point IS.D.OR.210, l'organisme doit mettre en œuvre des mesures pour détecter les incidents et les vulnérabilités qui indiquent une possible concrétisation de risques inacceptables et qui peuvent avoir une incidence potentielle sur la sécurité aérienne. Ces mesures de détection doivent permettre à l'organisme:

1) de recenser les écarts par rapport aux valeurs de base prédéterminées en matière de performances fonctionnelles;

2) de déclencher des signaux d'avertissement pour activer les mesures de réaction appropriées, en cas d'écart.

b) L'organisme doit mettre en œuvre des mesures pour réagir à tout événement recensé conformément au point a) qui peut se transformer ou s'est transformé en incident de sécurité de l'information. Ces mesures de réaction doivent permettre à l'organisme:

1) de déclencher la réaction aux signaux d'avertissement visés au point a) 2) en activant des ressources et des actions prédéfinies;

2) de contenir la propagation d'une attaque et d'éviter la pleine concrétisation d'un scénario de menace;

3) de contrôler le mode de défaillance des éléments affectés définis au point IS.D.OR.205 a).

c) L'organisme doit mettre en œuvre des mesures visant au rétablissement à la suite d'incidents de sécurité de l'information, y compris, le cas échéant, des mesures d'urgence. Ces mesures de rétablissement doivent permettre à l'organisme:

1) de supprimer la situation qui est à l'origine de l'incident ou de la limiter à un niveau tolérable;

2) d'assurer que les éléments affectés définis au point IS.D.OR.205 a) retrouvent un état garantissant la sécurité dans un délai de rétablissement défini précédemment par l'organisme.

IS.D.OR.225 Réponse aux constatations notifiées par l'autorité compétente

a) Après réception de la notification des constatations présentée par l'autorité compétente, l'organisme doit:

1) déterminer la cause ou les causes profondes des cas de non-conformité ainsi que les facteurs qui y contribuent;

2) définir un plan d'actions correctives;

3) démontrer la correction du défaut de conformité à la satisfaction de l'autorité compétente.

b) Les actions visées au point a) doivent être mises en œuvre dans le délai convenu avec l'autorité compétente.

IS.D.OR.230 Système de comptes rendus externe en matière de sécurité de l'information

a) L'organisme doit mettre en œuvre un système de comptes rendus en matière de sécurité de l'information qui satisfait aux exigences du règlement (UE) n° 376/2014 et de ses actes délégués et d'exécution si ce règlement lui est applicable.

b) Sans préjudice des obligations du règlement (UE) nº 376/2014, l'organisme doit veiller à ce que tout incident ou vulnérabilité en matière de sécurité de l'information susceptible de représenter un risque important pour la sécurité aérienne soit signalé à son autorité compétente. En outre:

1) lorsqu'un tel incident ou une telle vulnérabilité affecte un aéronef ou un système ou élément associé, l'organisme doit également en rendre compte au titulaire de l'agrément de conception;

2) lorsqu'un tel incident ou une telle vulnérabilité affecte un système ou un composant utilisé par l'organisme, celui-ci doit en rendre compte à l'organisme responsable de la conception du système ou du composant.

c) L'organisme doit rendre compte de la situation visée au point b) comme suit:

1) une notification doit être soumise à l'autorité compétente et, le cas échéant, au titulaire de l'agrément de conception ou à l'organisme responsable de la conception du système ou du composant, dès que l'organisme a connaissance de la situation;

2) un compte rendu doit être soumis à l'autorité compétente et, le cas échéant, 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.

Le compte rendu est établi sous la forme définie par l'autorité compétente et contient toutes les informations pertinentes sur la situation dont l'organisme a connaissance;

3) un rapport de suivi précisant les mesures que l'organisme a prises ou a l'intention de prendre pour le rétablissement après l'incident et les mesures qu'il a l'intention de prendre pour prévenir de tels incidents de sécurité de l'information à l'avenir doit être présenté à l'autorité compétente et, le cas échéant, au titulaire de l'agrément de conception ou à l'organisme responsable de la conception du système ou du composant.

Le rapport de suivi doit être présenté dès que ces mesures ont été définies et être établi selon la forme prévue par l'autorité compétente.

IS.D.OR.235 Sous-traitance des activités de gestion de la sécurité de l'information

a) Lorsqu'il sous-traite une partie des activités visées au point IS.D.OR.200 à d'autres organismes, l'organisme veille à ce que les activités sous-traitées soient conformes aux exigences du présent règlement et que l'organisme sous-traitant travaille sous sa supervision. L'organisme doit faire en sorte que les risques associés aux activités sous-traitées soient gérés de manière appropriée.

b) L'organisme doit veiller à ce que l'autorité compétente puisse, sur demande, avoir accès à l'organisme sous-traitant afin de déterminer le respect constant des exigences applicables énoncées dans le présent règlement.

IS.D.OR.240 Exigences en matière de personnel

a) Le dirigeant responsable de l'organisme ou, dans le cas des organismes de conception, le responsable de l'organisme de conception désigné conformément au règlement (UE) nº 748/2012 et au règlement (UE) nº 139/2014 pour les organismes visés à l'article 2, paragraphe 1, points a) et b), du présent règlement, détient les droits statutaires pour assurer que toutes les activités requises par le présent règlement peuvent être financées et exécutées. Cette personne doit:

1) veiller à ce que toutes les ressources nécessaires soient disponibles pour se conformer aux exigences du présent règlement;

2) établir et promouvoir la politique en matière de sécurité de l'information visée au point IS.D.OR.200 a), point 1);

3) démontrer qu'il a une vision d'ensemble du présent règlement.

b) Le dirigeant responsable ou, dans le cas des organismes de conception, le responsable de l'organisme de conception, doit désigner une personne ou un groupe de personnes chargées de s'assurer que l'organisme respecte les exigences du présent règlement, et doit définir l'étendue de leurs compétences. Cette personne ou ce groupe de personnes doit rendre compte directement au dirigeant responsable ou, dans le cas des organismes de conception, au responsable de l'organisme de conception, et doit posséder les connaissances, les qualifications et l'expérience appropriées pour s'acquitter de ses responsabilités. Les procédures doivent établir qui supplée une personne particulière dans le cas d'une absence de longue durée de cette personne.

c) Le dirigeant responsable ou, dans le cas des organismes de conception, le responsable de l'organisme de conception, doit désigner une personne ou un groupe de personnes chargées de gérer la fonction de contrôle de la conformité visée au point IS.D.OR.200 a), point 12).

d) Lorsque 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 domaines de sa propre organisation qui ne font pas partie de l'agrément ou de la déclaration, le dirigeant responsable ou, dans le cas des organismes de conception, le responsable de l'organisme de conception, peut déléguer ses activités à une personne responsable commune.

Dans ce cas, des mesures de coordination doivent être établies entre le dirigeant responsable de l'organisme ou, dans le cas des organismes de conception, le responsable de l'organisme de conception, et la personne responsable commune afin de garantir une intégration adéquate de la gestion de la sécurité de l'information au sein de l'organisme.

e) Le dirigeant responsable ou le responsable de l'organisme de conception, ou la personne responsable commune visée au point d), doit détenir les droits statutaires pour établir et maintenir les structures organisationnelles, les politiques, les processus et les procédures nécessaires à la mise en œuvre du point IS.D.OR.200.

f) L'organisme doit avoir mis en place un processus garantissant qu'il dispose d'un personnel suffisant pour mener à bien les activités couvertes par la présente annexe.

g) L'organisme doit mettre en place un processus garantissant que le personnel visé au point f) possède les compétences nécessaires pour accomplir ses tâches.

h) L'organisme doit avoir mis en place un processus permettant de garantir que le personnel est informé des responsabilités liées aux rôles et tâches assignés.

i) L'organisme doit veiller à ce que l'identité et la fiabilité du personnel ayant accès aux systèmes d'information et aux données soumises aux exigences du présent règlement soient établies de manière appropriée.

IS.D.OR.245 Archivage

a) L'organisme doit conserver des archives sur ses activités de gestion de la sécurité de l'information.

1) L'organisme doit veiller à ce que les documents suivants soient archivés et traçables:

i) tout agrément reçu et toute évaluation connexe des risques liés à la sécurité de l'information conformément au point IS.D.OR.200 e);

ii) les contrats portant sur les activités visées au point IS.D.OR.200 a), point 9);

iii) les documents relatifs aux processus clés visés au point IS.D.OR.200 d);

iv) les documents relatifs aux risques recensés dans l'évaluation des risques visée au point IS.D.OR.205 ainsi que les mesures connexes de traitement des risques visées au point IS.D.OR.210;

v) les documents relatifs aux incidents et vulnérabilités liés à la sécurité de l'information signalés conformément aux systèmes de comptes rendus visés aux points IS.D.OR.215 et IS.D.OR.230;

vi) 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.

2) Les documents visés au point 1) i) doivent être conservés au moins 5 ans après que l'agrément a perdu sa validité.

3) Les documents visés au point 1) ii) doivent être conservés au moins 5 ans après la modification ou la résiliation du contrat.

4) Les documents visés aux points 1) iii), iv) et v), doivent être conservés pendant une période d'au moins 5 ans.

5) Les documents visés au point 1) vi) doivent être conservés jusqu'à ce que ces événements liés à la sécurité de l'information aient été réévalués selon une périodicité définie dans une procédure établie par l'organisme.

b) L'organisme doit conserver les documents relatifs aux qualifications et à l'expérience de son propre personnel participant aux activités de gestion de la sécurité de l'information.

1) Les documents relatifs aux qualifications et à l'expérience du personnel doivent être conservés aussi longtemps que la personne travaille pour l'organisme et pendant au moins 3 ans après que la personne a quitté l'organisme.

2) À leur demande, les membres du personnel doivent avoir accès à leurs dossiers individuels. En outre, à leur demande, l'organisme doit leur fournir une copie de leurs dossiers individuels lorsqu'ils quittent l'organisme.

c) Le format des dossiers doit être défini dans les procédures de l'organisme.

d) Les documents doivent être stockés de manière à ne pas être endommagés, altérés ou dérobés, les informations étant signalées, le cas échéant, en fonction de leur niveau de classification de sécurité. L'organisme doit veiller à ce que les documents soient stockés de manière à garantir l'intégrité, l'authenticité et l'accès autorisé.

IS.D.OR.250 Manuel de gestion de la sécurité de l'information (MGSI)

a) L'organisme doit mettre à la disposition de l'autorité compétente un manuel de gestion de la sécurité de l'information (MGSI) et, le cas échéant, tous manuels et procédures associés auxquels il renvoie, contenant:

1) une déclaration signée par le dirigeant responsable ou, dans le cas des organismes de conception, par le responsable de l'organisme de conception, confirmant que l'organisme travaillera à tout moment conformément à la présente annexe et au MGSI. Si le dirigeant responsable ou, dans le cas des organismes de conception, le responsable de l'organisme de conception, n'est pas le directeur général de l'organisme, alors le directeur général doit contresigner la déclaration;

2) le(s) titre(s), le(s) nom(s), les missions, les obligations de rendre compte, les responsabilités et les pouvoirs de la ou des personnes visées aux points IS.D.OR.240 b) et c);

3) le titre, le nom, les missions, les obligations de rendre compte, les responsabilités et les pouvoirs de la personne responsable commune visée au point IS.D.OR.240 d), le cas échéant;

4) la politique en matière de sécurité de l'information de l'organisme visée au point IS.D.OR.200 a), point 1);

5) 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, comme requis au point IS.D.OR.240 d);

6) le(s) titre(s), le(s) nom(s), les missions, les obligations de rendre compte, les responsabilités et les pouvoirs des personnes clés chargées de la mise en œuvre du point IS.D.OR.200, y compris la ou les personnes responsables de la fonction de contrôle de la conformité visée au point IS.D.OR.200 a), point 12);

7) un organigramme montrant les rapports hiérarchiques en matière d'obligation de rendre compte et de responsabilité entre les personnes visées aux points 2) et 6);

8) la description du système de comptes rendus interne visé au point IS.D.OR.215;

9) les procédures qui précisent comment l'organisme garantit le respect de la présente partie, et notamment:

i) la documentation visée au point IS.D.OR.200 c);

ii) les procédures qui définissent la manière dont l'organisme contrôle les activités sous-traitées visées au point IS.D.OR.200 a), point 9);

iii) la procédure de modification du MGSI définie au point c);

10) des informations détaillées sur les autres moyens de mise en conformité actuellement approuvés.

b) La première édition du MGSI doit être approuvée et une copie doit être conservée par l'autorité compétente. Le MGSI doit être modifié en tant que de besoin pour conserver une description à jour du SGSI de l'organisme. Une copie de toute modification du MGSI doit être fournie à l'autorité compétente.

c) Les modifications apportées au SGSI doivent être gérées selon une procédure établie par l'organisme. Toute modification qui n'entre pas dans le champ d'application de cette procédure et toute modification liée aux modifications visées au point IS.D.OR.255 b) doivent être approuvées par l'autorité compétente.

d) L'organisme peut intégrer le MGSI à d'autres spécifications de gestion ou manuels qu'il détient, à condition qu'il existe une référence croisée claire indiquant quelles parties des spécifications de gestion ou du manuel correspondent aux différentes exigences énoncées dans la présente annexe.

IS.D.OR.255 Modification du système de gestion de la sécurité de l'information

a) Les modifications apportées au SGSI peuvent être gérées et notifiées à l'autorité compétente dans le cadre d'une procédure élaborée par l'organisme. Cette procédure doit être approuvée par l'autorité compétente.

b) En ce qui concerne les modifications du SGSI non couvertes par la procédure visée au point a), l'organisme doit demander et obtenir une approbation délivrée par l'autorité compétente.

En ce qui concerne ces modifications:

1) la demande doit être soumise avant que ne soient apportées de telles modifications, afin de permettre à l'autorité compétente de déterminer le respect constant du présent règlement et de modifier, au besoin, le certificat d'organisme ainsi que les termes de l'agrément correspondants qui y sont joints;

2) l'organisme doit mettre à la disposition de l'autorité compétente toute information qu'elle demande pour évaluer la modification;

3) la modification ne doit être mise en œuvre qu'après réception de l'approbation formelle de l'autorité compétente;

4) l'organisme doit exercer ses activités dans les conditions prescrites par l'autorité compétente pendant la mise en œuvre de ces modifications.

IS.D.OR.260 Amélioration constante

a) L'organisme doit évaluer, à l'aide d'indicateurs de performance adéquats, l'efficacité et la maturité du SGSI. Cette évaluation doit être effectuée selon un calendrier prédéfini par l'organisme ou à la suite d'un incident de sécurité de l'information.

b) Si des manquements sont constatés à la suite de l'évaluation effectuée conformément au point a), l'organisme doit prendre les mesures d'amélioration nécessaires pour garantir que le SGSI continue de respecter les exigences applicables et maintient les risques liés à la sécurité de l'information à un niveau acceptable. En outre, l'organisme réévalue les éléments du SGSI concernés par les mesures adoptées.