II

*(Actes non législatifs)*

# RÈGLEMENTS

## RÈGLEMENT D'EXÉCUTION (UE) 2023/203 DE LA COMMISSION

**du 27 octobre 2022**

**portant modalités d'application du règlement (UE) 2018/1139 du Parlement européen et du Conseil en ce qui concerne les exigences en matière de gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne pour les organismes relevant des règlements (UE) nº 1321/2014, (UE) nº 965/2012, (UE) nº 1178/2011 et (UE) 2015/340 de la Commission, des règlements d'exécution (UE) 2017/373 et (UE) 2021/664 de la Commission, et pour les autorités compétentes relevant des règlements (UE) nº 748/2012, (UE) nº 1321/2014, (UE) nº 965/2012, (UE) nº 1178/2011, (UE) 2015/340 et (UE) nº 139/2014 de la Commission, des règlements d'exécution (UE) 2017/373 et (UE) 2021/664 de la Commission, et modifiant les règlements (UE) nº 1178/2011, (UE) nº 748/2012, (UE) nº 965/2012, (UE) nº 139/2014, (UE) nº 1321/2014 et (UE) 2015/340 de la Commission, et les règlements d'exécution (UE) 2017/373 et (UE) 2021/664 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 17, paragraphe 1, point b), son article 27, paragraphe 1, point a), son article 31, paragraphe 1, point b), son article 43, paragraphe 1, point b), son article 53, paragraphe 1, point a), et son article 62, paragraphe 15, point c),

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 responsables de la gestion du maintien de la navigabilité et les organismes responsables de la maintenance 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 IV, points 3.3.b) et 5 b), du règlement (UE) 2018/1139, les organismes de formation des pilotes, les organismes de formation des membres d'équipage de cabine, les centres aéromédicaux pour les membres d'équipage et les exploitants de simulateurs d'entraînement au vol sont tenus de mettre en œuvre et d'entretenir un système de gestion afin d'assurer la gestion des risques pour la sécurité.

(3) En outre, conformément aux exigences essentielles énoncées à l'annexe V, point 8.1 c), du règlement (UE) 2018/1139, les transporteurs aériens sont tenus de mettre en œuvre et d'entretenir un système de gestion afin d'assurer la gestion des risques pour la sécurité.

(4) Qui plus est, conformément aux exigences essentielles énoncées à l'annexe VIII, points 5.1 c) et 5.4 b), du règlement (UE) 2018/1139, les prestataires de services de gestion du trafic aérien et de services de navigation aérienne, les prestataires de services U-space et les prestataires uniques de services d'informations communes, ainsi que les organismes de formation et les centres aéromédicaux pour les contrôleurs de la circulation aérienne doivent mettre en œuvre et entretenir un système de gestion afin d'assurer la gestion des risques pour la sécurité.

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

(5) Ces risques pour la sécurité peuvent provenir de sources diverses, telles que des défauts de conception et d'entretien, des aspects liés aux performances humaines, des menaces environnementales et des menaces relatives à la sécurité de l'information. Par conséquent, les systèmes de gestion mis en œuvre par l'Agence de l'Union européenne pour la sécurité aérienne (ci-après l'«Agence»), les autorités nationales compétentes et les organismes visés aux considérants ci-dessus 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.

(6) 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.

(7) 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. 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.

(8) Il est essentiel que ces exigences couvrent tous les 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 et autorités compétentes relevant des règlements (UE) n° 748/2012 ([2]), (UE) n° 1321/2014 ([3]), (UE) n° 965/2012 ([4]), (UE) n° 1178/2011 ([5]), (UE) 2015/340 ([6]) et (UE) n° 139/2014 ([7]) de la Commission et du règlement d'exécution (UE) 2021/664 de la Commission ([8]), ainsi qu'à ceux qui sont déjà tenus de disposer d'un système de gestion conformément à la législation de l'Union en vigueur en matière de sécurité aérienne. Toutefois, certains organismes devraient être exclus du champ d'application du présent règlement afin de garantir une proportionnalité appropriée, les risques liés à la sécurité de l'information qu'ils représentent pour le système aéronautique étant moins élevés.

(9) Les exigences énoncées dans le présent règlement devraient garantir une application 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.

([2]) 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).

([3]) Règlement (UE) n° 1321/2014 de la Commission du 26 novembre 2014 relatif au maintien de la navigabilité des aéronefs et des produits, pièces et équipements aéronautiques, et relatif à l'agrément des organismes et des personnels participant à ces tâches (JO L 362 du 17.12.2014, p. 1).

([4]) Règlement (UE) n° 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) n° 216/2008 du Parlement européen et du Conseil (JO L 296 du 25.10.2012, p. 1).

([5]) Règlement (UE) n° 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) n° 216/2008 du Parlement européen et du Conseil (JO L 311 du 25.11.2011, p. 1).

([6]) 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 (JO L 63 du 6.3.2015, p. 1).

([7]) 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).

([8]) Règlement d'exécution (UE) 2021/664 de la Commission du 22 avril 2021 relatif à un cadre réglementaire pour l'U-space (JO L 139 du 23.4.2021, p. 161).

(10) 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 ([9]) et à l'article 14 de la directive (UE) 2016/1148 du Parlement européen et du Conseil ([10]).

(11) Les exigences de sécurité énoncées aux articles 33 à 43 du titre V «Sécurité du programme» du règlement (UE) 2021/696 du Parlement européen et du Conseil ([11]) sont considérées comme équivalentes aux exigences énoncées dans le présent règlement, sauf en ce qui concerne le point IS.I.OR.230 de l'annexe II du présent règlement, qui devrait être respecté.

(12) Afin de garantir la sécurité juridique, l'interprétation du terme «sécurité de l'information» tel que défini dans le présent règlement, qui reflète son utilisation commune dans l'aviation civile à l'échelle mondiale, devrait être considérée comme cohérente avec celle de l'expression «sécurité des réseaux et des systèmes d'information» telle que définie à l'article 4, point 2), de la directive (UE) 2016/1148. La définition de la sécurité de l'information aux fins du présent règlement 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.

(13) 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'actes de l'Union visés aux considérants 10 et 11, 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.

(14) Les organismes relevant du présent règlement qui sont déjà soumis aux exigences de sécurité découlant du règlement d'exécution (UE) 2015/1998 ou du règlement (UE) 2021/696, ou des deux, devraient également se conformer aux exigences de l'annexe II (partie IS.I.OR.230 «Système de comptes rendus externes en matière de sécurité de l'information») du présent règlement, dès lors qu'aucun des deux premiers règlements ne contient de disposition liée aux comptes rendus externes des incidents relatifs à la sécurité de l'information.

(15) Par souci d'exhaustivité, il convient de modifier les règlements (UE) n° 1178/2011, (UE) n° 748/2012, (UE) n° 965/2012, (UE) n° 139/2014, (UE) n° 1321/2014 et (UE) 2015/340 et les règlements d'exécution (UE) 2017/373 ([12]) et (UE) 2021/664 afin d'introduire les exigences relatives aux systèmes de gestion de la sécurité de l'information prévues dans le présent règlement, ainsi que celles relatives aux systèmes de gestion qui y sont énoncées, et de définir les exigences applicables aux autorités compétentes en ce qui concerne la surveillance des organismes mettant en œuvre les exigences susmentionnées en matière de gestion de la sécurité de l'information.

(16) Afin de donner aux organismes suffisamment de temps pour assurer le respect des nouvelles règles et procédures, le présent règlement devrait s'appliquer 3 ans après son entrée en vigueur, sauf pour le prestataire de services de navigation aérienne du système européen de navigation par recouvrement géostationnaire (EGNOS) défini dans le règlement d'exécution (UE) 2017/373, pour lequel, en raison de l'homologation de sécurité en cours du système et des services EGNOS conformément au règlement (UE) 2021/696, il devrait devenir applicable à partir du 1er janvier 2026.

(17) Les exigences définies dans le présent règlement sont fondées sur l'avis n° 03/2021 ([13]) 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.

([9]) 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).

([10]) 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).

([11]) Règlement (UE) 2021/696 du Parlement européen et du Conseil du 28 avril 2021 établissant le programme spatial de l'Union et l'Agence de l'Union européenne pour le programme spatial et abrogeant les règlements (UE) n° 912/2010, (UE) n° 1285/2013 et (UE) n° 377/2014 et la décision n° 541/2014/UE. (JO L 170du 12.5.2021, p. 69).

([12]) 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) n° 482/2008, les règlements d'exécution (UE) n° 1034/2011, (UE) n° 1035/2011 et (UE) 2016/1377 et modifiant le règlement (UE) n° 677/2011 (JO L 62 du 8.3.2017, p. 1).

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

(18) Les exigences définies dans le présent règlement sont conformes à l'avis du comité pour l'application des règles communes de sécurité dans le domaine de l'aviation civile institué par l'article 127 du règlement (UE) 2018/1139,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

*Article premier*

**Objet**

Le présent règlement définit les exigences auxquelles doivent satisfaire les organismes et les autorités compétentes pour:

a) 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 systèmes et les données de technologies de l'information et de la communication utilisés aux fins de l'aviation civile;

b) détecter les événements liés à la sécurité de l'information et déterminer ceux qui sont considérés comme des incidents de sécurité de l'information susceptibles d'avoir des répercussions sur la sécurité aérienne;

c) réagir à ces incidents de sécurité de l'information et garantir le rétablissement après incident.

*Article 2*

**Champ d'application**

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

a) les organismes de maintenance relevant la section A de l'annexe II (partie 145) du règlement (UE) n° 1321/2014, à l'exception de ceux qui participent uniquement à la maintenance des aéronefs conformément à l'annexe V *ter* (partie ML) du règlement (UE) n° 1321/2014;

b) les organismes responsables de la gestion du maintien de la navigabilité (CAMO) relevant de la section A de l'annexe V *quater* (partie CAMO) du règlement (UE) n° 1321/2014, à l'exception de ceux qui participent uniquement à la gestion du maintien de la navigabilité des aéronefs conformément à l'annexe V *ter* (partie ML) du règlement (UE) n° 1321/2014;

c) les transporteurs aériens relevant de l'annexe III (partie ORO) du règlement (UE) n° 965/2012, à l'exception de ceux qui participent exclusivement à l'exploitation de l'un des éléments suivants:

i) un aéronef ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) n° 748/2012;

ii) des avions monomoteurs à hélice dont la configuration maximale opérationnelle en sièges passagers est inférieure ou égale à 5 et qui ne sont pas classés comme aéronefs motorisés complexes, lorsqu'ils décollent et atterrissent sur le même aérodrome ou site d'exploitation et qu'ils sont exploités selon les règles de vol à vue (VFR) de jour;

iii) des hélicoptères monomoteurs dont la configuration maximale opérationnelle en sièges passagers est inférieure ou égale à 5 et qui ne sont pas classés comme aéronefs motorisés complexes, lorsqu'ils décollent et atterrissent sur le même aérodrome ou site d'exploitation et qu'ils sont exploités en VFR de jour:

d) les organismes de formation agréés (ATO) relevant de l'annexe VII (partie ORA) du règlement (UE) n° 1178/2011, à l'exception de ceux qui participent uniquement aux activités de formation pour les aéronefs ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) n° 748/2012, ou qui participent uniquement à la formation théorique;

e) les centres aéromédicaux du personnel navigant relevant de l'annexe VII (partie ORA) du règlement (UE) n° 1178/2011;

f) les exploitants de simulateurs d'entraînement au vol (FSTD) relevant de l'annexe VII (partie ORA) du règlement (UE) n° 1178/2011, à l'exception de ceux qui participent uniquement à l'exploitation de FSTD pour les aéronefs ELA2 au sens de l'article 1er, paragraphe 2, point j), du règlement (UE) n° 748/2012;

g) les organismes de formation des contrôleurs de la circulation aérienne (ATCO) et les centres aéromédicaux ATCO relevant de l'annexe III (partie ATCO.OR) du règlement (UE) 2015/340;

h) les organismes relevant de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) 2017/373, à l'exception des prestataires de services suivants:

i) les prestataires de services de navigation aérienne titulaires d'un certificat limité conformément au point ATM/ANS.OR.A.010 de ladite annexe;

ii) les prestataires de services d'information de vol déclarant leurs activités conformément au point ATM/ANS.OR.A.015 de ladite annexe;

i) les prestataires de services U-space et les prestataires uniques de services d'informations communes soumis au règlement d'exécution (UE) 2021/664.

2. Le présent règlement s'applique aux autorités compétentes, y compris l'Agence de l'Union européenne pour la sécurité aérienne (ci-après l'«Agence»), visées à l'article 6 du présent règlement et à l'article 5 du règlement délégué (UE) 2022/1645 de la Commission ([14]).

3. Le présent règlement s'applique également à l'autorité compétente responsable de la délivrance, de la prolongation, de la modification, de la suspension ou du retrait des licences de maintenance d'aéronefs conformément à l'annexe III (partie 66) du règlement (UE) n° 1321/2014.

4. 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 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 réel 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;

([14]) 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) n° 748/2012 et (UE) n° 139/2014 de la Commission et modifiant les règlements (UE) n° 748/2012 et (UE) n° 139/2014 de la Commission (JO L 248 du 26.9.2022, p. 18).

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 applicables aux organismes et aux autorités compétentes**

1. Les organismes visés à l'article 2, paragraphe 1, se conforment aux exigences de l'annexe II (partie IS.I.OR) du présent règlement.

2. Les autorités compétentes visées à l'article 2, paragraphes 2 et 3, se conforment aux exigences de l'annexe I (partie IS.AR) du présent règlement.

*Article 5*

**Exigences découlant d'autres dispositions législatives de l'Union**

1. Lorsqu'un organisme visé à l'article 2, paragraphe 1, satisfait à des exigences de sécurité fixées conformément 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, paragraphe 1, 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) n° 300/2008 du Parlement européen et du Conseil ([15]). 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.I.OR.230 de l'annexe II du présent règlement, qui est respecté en tant que tel.

3. Lorsque l'organisme visé à l'article 2, paragraphe 1, est le prestataire de services de navigation aérienne du système européen de navigation par recouvrement géostationnaire (EGNOS) visé dans le règlement (UE) 2021/696, les exigences de sécurité énoncées aux articles 33 à 43 du titre V dudit règlement sont considérées comme équivalentes aux exigences énoncées dans le présent règlement, sauf en ce qui concerne le point IS.I.OR.230 de l'annexe II du présent règlement, qui est respecté en tant que tel.

4. La Commission, après consultation de l'Agence 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 6*

**Autorité compétente**

1. Sans préjudice des tâches confiées au conseil d'homologation de sécurité visé à l'article 36 du règlement (UE) 2021/696, 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, paragraphe 1, point a), l'autorité compétente désignée conformément à l'annexe II (partie 145) du règlement (UE) n° 1321/2014;

b) à l'égard des organismes visés à l'article 2, paragraphe 1, point b), l'autorité compétente désignée conformément à l'annexe V *quater* (partie CAMO) du règlement (UE) n° 1321/2014;

([15]) Règlement (CE) n° 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) n° 2320/2002 (JO L 97 du 9.4.2008, p. 72).

c) à l'égard des organismes visés à l'article 2, paragraphe 1, point c), l'autorité compétente désignée conformément à l'annexe III (partie ORO) du règlement (UE) n° 965/2012;

d) à l'égard des organismes visés à l'article 2, paragraphe 1, points d) à f), l'autorité compétente désignée conformément à l'annexe VII (partie ORA) du règlement (UE) n° 1178/2011;

e) à l'égard des organismes visés à l'article 2, paragraphe 1, point g), l'autorité compétente désignée conformément à l'article 6, paragraphe 2, du règlement (UE) 2015/340;

f) à l'égard des organismes visés à l'article 2, paragraphe 1, point h), l'autorité compétente désignée conformément à l'article 4, paragraphe 1, du règlement d'exécution (UE) 2017/373;

g) à l'égard des organismes visés à l'article 2, paragraphe 1, point i), l'autorité compétente désignée conformément à l'article 14, paragraphe 1 ou 2, selon le cas, du règlement d'exécution (UE) 2021/664.

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.

3. L'Agence coopère dans le strict respect des règles applicables en matière de confidentialité, de protection des données à caractère personnel et de protection des informations classifiées avec l'Agence de l'Union européenne pour le programme spatial (EUSPA) et le conseil d'homologation de sécurité visé à l'article 36 du règlement (UE) 2021/696 afin d'assurer une surveillance efficace des exigences applicables au prestataire de services de navigation aérienne EGNOS.

*Article 7*

**Communication d'informations pertinentes aux autorités compétentes en matière de sécurité des réseaux et des systèmes d'information (SRI)**

Les autorités compétentes au titre du présent règlement communiquent sans retard au point de contact unique désigné conformément à l'article 8 de la directive (UE) 2016/1148 toute information pertinente contenue dans les notifications soumises conformément au point IS.I.OR.230 de l'annexe II du présent règlement et au point IS.D.OR.230 de l'annexe I du règlement délégué (UE) 2022/1645 par les opérateurs de services essentiels identifiés conformément à l'article 5 de la directive (UE) 2016/1148.

*Article 8*

**Modification du règlement (UE) n° 1178/2011**

Les annexes VI (partie ARA) et VII (partie ORA) du règlement (UE) n° 1178/2011 sont modifiées conformément à l'annexe III du présent règlement.

*Article 9*

**Modification du règlement (UE) n° 748/2012**

L'annexe I (partie 21) du règlement (UE) n° 748/2012 est modifiée conformément à l'annexe IV du présent règlement.

*Article 10*

**Modification du règlement (UE) n° 965/2012**

Les annexes II (partie ARO) et III (partie ORO) du règlement (UE) n° 965/2012 sont modifiées conformément à l'annexe V du présent règlement.

*Article 11*

**Modification du règlement (UE) n° 139/2014**

L'annexe II (partie ADR.AR) du règlement (UE) n° 139/2014 est modifiée conformément à l'annexe VI du présent règlement.

*Article 12*

**Modification du règlement (UE) n° 1321/2014**

Les annexes II (partie 145), III (partie 66) et V *quater* (partie CAMO) du règlement (UE) n° 1321/2014 sont modifiées conformément à l'annexe VII du présent règlement.

*Article 13*

**Modification du règlement (UE) 2015/340**

Les annexes II (partie ATCO.AR) et III (partie ATCO.OR) du règlement (UE) 2015/340 sont modifiées conformément à l'annexe VIII du présent règlement.

*Article 14*

**Modification du règlement d'exécution (UE) 2017/373**

Les annexes II (partie ATM/ANS.AR) et III (partie ATM/ANS.OR) du règlement d'exécution (UE) 2017/373 sont modifiées conformément à l'annexe IX du présent règlement.

*Article 15*

**Modification du règlement d'exécution (UE) 2021/664**

Le règlement d'exécution (UE) 2021/664 est modifié comme suit:

1) À l'article 15, paragraphe 1, le point f) est remplacé par le texte suivant:

«f) qu'ils mettent en œuvre et entretiennent un système de gestion de la sûreté conformément à l'annexe III, sous-partie D, point ATM/ANS.OR.D.010, du règlement d'exécution (UE) 2017/373 et un système de gestion de la sécurité de l'information conformément à l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203;».

2) À l'article 18, le point l) suivant est ajouté:

«l) établissent, mettent en œuvre et entretiennent un système de gestion de la sécurité de l'information conformément à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203.».

*Article 16*

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

Il est applicable à compter du 22 février 2026.

Toutefois, dans le cas du prestataire de services de navigation aérienne EGNOS relevant du règlement d'exécution (UE) 2017/373, il s'applique à compter du 1er janvier 2026.

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

Fait à Bruxelles, le 27 octobre 2022.

*Par la Commission*
*La présidente*
Ursula VON DER LEYEN

*ANNEXE I*

**SÉCURITÉ DE L'INFORMATION — EXIGENCES APPLICABLES À L'AUTORITÉ**

**[PARTIE-IS.AR]**

IS.AR.100 Champ d'application

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

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

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

IS.AR.215 Incidents de sécurité de l'information — détection, réaction et rétablissement

IS.AR.220 Sous-traitance des activités de gestion de la sécurité de l'information

IS.AR.225 Exigences en matière de personnel

IS.AR.230 Archivage

IS.AR.235 Amélioration constante

**IS.AR.100 Champ d'application**

La présente partie établit les exigences en matière de gestion auxquelles doivent satisfaire les autorités compétentes visées à l'article 2, paragraphe 2, du présent règlement.

Les exigences auxquelles doivent satisfaire ces autorités compétentes pour l'exercice de leurs activités de certification, de supervision et de contrôle de l'application figurent dans les règlements visés à l'article 2, paragraphe 1, du présent règlement et à l'article 2 du règlement délégué (UE) 2022/1645.

**IS.AR.200 Système de gestion de la sécurité de l'information (SGSI)**

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

1) met en place une politique en matière de sécurité de l'information définissant les principes généraux de l'autorité compétente 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.AR.205;

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

4) définit et met en œuvre, conformément au point IS.AR.215, 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, réagit à ces incidents de sécurité de l'information et garantit le rétablissement après incident;

5) satisfait aux exigences énoncées au point IS.AR.220 lorsqu'il sous-traite une partie des activités décrites au point IS.AR.200 à d'autres organismes;

6) satisfait aux exigences en matière de personnel énoncées au point IS.AR.225;

7) satisfait aux exigences en matière d'archivage énoncées au point IS.AR.230;

8) vérifie que son propre organisme respecte les exigences du présent règlement et fournit à la personne visée au point IS.AR.225 a) un retour d'information sur les constatations afin de garantir la mise en œuvre effective des mesures correctives;

9) protège la confidentialité des informations dont elle dispose au sujet des organismes soumis à sa supervision ainsi que des informations reçues par l'intermédiaire des systèmes de comptes rendus externes de l'organisme établis conformément au point IS.I.OR.230 de l'annexe II (partie IS.I.OR) du présent règlement et au point IS.D.OR.230 de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645;

10) notifie à l'Agence les modifications qui ont une incidence sur la capacité de l'autorité compétente à s'acquitter de ses tâches et à exercer ses responsabilités telles que définies dans le présent règlement;

11) définit et met en œuvre des procédures pour partager, le cas échéant, de manière pratique et en temps utile, les informations pertinentes pour aider les autres autorités compétentes et agences, ainsi que les organismes soumis au présent règlement, à procéder à des évaluations efficaces des risques de sécurité liés à leurs activités.

b) Afin de satisfaire en permanence aux exigences visées à l'article 1er, l'autorité compétente doit mettre en œuvre un processus d'amélioration constante conformément au point IS.AR.235.

c) L'autorité compétente doit documenter l'ensemble des processus, procédures, rôles et responsabilités clés requis pour se conformer au point IS.AR.200 a) et établir un processus de modification de cette documentation.

d) Les processus, procédures, rôles et responsabilités établis par l'autorité compétente pour se conformer au point IS.AR.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'autorité compétente.

**IS.AR.205 Évaluation des risques liés à la sécurité de l'information**

a) L'autorité compétente doit recenser tous les éléments de son propre organisme qui sont susceptibles d'être exposés à des risques liés à la sécurité de l'information. Ces éléments sont notamment les suivants:

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

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

b) L'autorité compétente doit déterminer les interfaces que son propre organisme 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'autorité compétente 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'autorité compétente doit:

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

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'autorité compétente dispose ou non d'un processus de gestion des risques structuré et reproductible pour les opérations, l'autorité compétente doit être en mesure d'établir si le risque est acceptable ou s'il doit être traité conformément au point IS.AR.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'autorité compétente examine et met à jour l'évaluation des risques effectuée conformément aux points a), b) et c) dans l'un des cas suivants:

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 de l'autorité compétente 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.AR.210 Traitement des risques liés à la sécurité de l'information**

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

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 au point IS.AR.225 a), et les autres membres du personnel de l'autorité compétente concernés doivent être informés des résultats de l'évaluation des risques effectuée conformément au point IS.AR.205, des scénarios de menace correspondants et des mesures à mettre en œuvre.

L'autorité compétente doit également informer les organismes avec lesquels elle partage une interface conformément au point IS.AR.205 b) de tout risque commun à l'autorité compétente et à l'organisme.

**IS.AR.215 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.AR.205 et des résultats du traitement des risques effectué conformément au point IS.AR.210, l'autorité compétente doit mettre en œuvre des mesures pour détecter les événements 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'autorité compétente:

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'autorité compétente 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'autorité compétente:

1) de déclencher la réaction de son propre organisme 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.AR.205 a).

c) L'autorité compétente 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'autorité compétente:

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.AR.205 a) retrouvent un état garantissant la sécurité dans un délai de rétablissement préalablement défini par son propre organisme.

**IS.AR.220 Sous-traitance des activités de gestion de la sécurité de l'information**

Lorsqu'elle sous-traite une partie des activités visées au point IS.AR.200 à d'autres organismes, l'autorité compétente 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'autorité compétente doit faire en sorte que les risques associés aux activités sous-traitées soient gérés de manière appropriée.

**IS.AR.225 Exigences en matière de personnel**

L'autorité compétente doit:

a) disposer d'une personne habilitée à établir et à entretenir les structures organisationnelles, les politiques, les processus et les procédures nécessaires à la mise en œuvre du présent règlement.

Cette personne doit:

1) être habilitée à accéder à toutes les ressources nécessaires pour permettre à l'autorité compétente d'accomplir toutes les tâches requises par le présent règlement;

2) disposer de la délégation de pouvoir nécessaire à l'accomplissement des tâches qui lui sont assignées;

b) avoir mis en place un processus garantissant que l'autorité compétente dispose d'un personnel suffisant pour mener à bien les activités couvertes par la présente annexe;

c) avoir mis en place un processus garantissant que le personnel visé au point b) possède les compétences nécessaires pour accomplir ses tâches;

d) avoir mis en place un processus permettant de garantir que le personnel est informé des responsabilités liées aux rôles et tâches assignés;

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

**IS.AR.230 Archivage**

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

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

i) les contrats portant sur les activités visées au point IS.AR.200 a), point 5);

ii) les documents relatifs aux processus clés visés au point IS.AR.200 d);

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

iv) 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 la modification ou la résiliation du contrat.

3) Les documents visés aux points 1) ii) et 1 iii) doivent être conservés pendant une période d'au moins 5 ans.

4) Les documents visés au point 1) iv) 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'autorité compétente.

b) L'autorité compétente 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'autorité compétente et pendant au moins 3 ans après que la personne a quitté l'autorité compétente.

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

c) Le format des dossiers est défini dans les procédures de l'autorité compétente.

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'autorité compétente doit veiller à ce que les documents soient stockés de manière à garantir l'intégrité, l'authenticité et l'accès autorisé.

**IS.AR.235 Amélioration constante**

a) L'autorité compétente doit évaluer, à l'aide d'indicateurs de performance adéquats, l'efficacité et la maturité de son propre SGSI. Cette évaluation doit être effectuée selon un calendrier prédéfini par l'autorité compétente 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'autorité compétente 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'autorité compétente réévalue les éléments du SGSI concernés par les mesures adoptées.

*ANNEXE II*

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

**[PARTIE-IS.I.OR]**

IS.I.OR.100 Champ d'application

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

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

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

IS.I.OR.215 Système de comptes rendus internes en matière de sécurité de l'information

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

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

IS.I.OR.230 Système de comptes rendus externes en matière de sécurité de l'information

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

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

IS.I.OR.245 Archivage

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

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

IS.I.OR.260 Amélioration constante

**IS.I.OR.100 Champ d'application**

La présente partie établit les exigences auxquelles doivent satisfaire les organismes visés à l'article 2, paragraphe 1, du présent règlement.

**IS.I.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 entretenir 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.I.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.I.OR.210;

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

5) définit et met en œuvre, conformément au point IS.I.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.I.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 ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne;

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

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

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

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

11) satisfait aux exigences en matière d'archivage énoncées au point IS.I.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 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.I.OR.260.

c) L'organisme doit documenter, conformément au point IS.I.OR.250, tous les processus, procédures, rôles et responsabilités clés requis pour se conformer au point IS.I.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.I.OR.255.

d) Les processus, procédures, rôles et responsabilités établis par l'organisme pour se conformer au point IS.I.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 et aux exigences du point IS.I.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), ni les exigences connexes figurant aux points IS.I.OR.205 à IS.I.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.I.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.I.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;

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.I.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, selon le cas, c) ou e), 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.

e) Par dérogation au point c), les organismes tenus de se conformer à la sous-partie C de l'annexe III (partie ATM/ANS.OR) du règlement d'exécution (UE) 2017/373 remplacent l'analyse de l'impact sur la sécurité aérienne par une analyse de l'impact sur leurs services dans le cadre de l'évaluation du support à la sécurité requise par le point ATM/ANS.OR.C.005. Cette évaluation du support à la sécurité est mise à la disposition des prestataires de services de la circulation aérienne auxquels ils fournissent des services et ces prestataires de services de la circulation aérienne sont chargés d'évaluer l'impact sur la sécurité aérienne.

**IS.I.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.I.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.I.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.I.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.I.OR.205 b) de tout risque commun aux deux organismes.

**IS.I.OR.215 Système de comptes rendus internes en matière de sécurité de l'information**

a) L'organisme doit établir un système de comptes rendus internes 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.I.OR.230.

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

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

2) de déterminer les causes des incidents et des vulnérabilités en matière de sécurité de l'information 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.I.OR.205 et IS.I.OR.220;

3) de procéder à une évaluation de toutes les informations connues et pertinentes relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information 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 rendre compte à celui-ci 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.I.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.I.OR.205 et des résultats du traitement des risques effectué conformément au point IS.I.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 référence 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.I.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.I.OR.205 a) retrouvent un état garantissant la sécurité dans un délai de rétablissement défini précédemment par l'organisme.

**IS.I.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.I.OR.230 Système de comptes rendus externes 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) n° 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.I.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.I.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.I.OR.240 Exigences en matière de personnel**

a) Le dirigeant responsable de l'organisme désigné conformément aux règlements (UE) n° 1321/2014, (UE) n° 965/2012, (UE) n° 1178/2011 et (UE) 2015/340, au règlement d'exécution (UE) 2017/373 ou au règlement d'exécution (UE) 2021/664, selon le cas, visé à l'article 2, paragraphe 1, du présent règlement, détient les droits statutaires pour faire en sorte que toutes les activités requises par le présent règlement puissent être financées et exécutées. Cette personne doit:

1) veiller à ce que toutes les ressources nécessaires soient disponibles pour assurer la conformité aux exigences du présent règlement;

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

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

b) Le dirigeant responsable 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 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 doit désigner une personne ou un groupe de personnes chargées de gérer la fonction de contrôle de la conformité visée au point IS.I.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 secteurs de sa propre organisation qui ne font pas partie de l'agrément ou de la déclaration, le dirigeant responsable 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 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 la personne responsable commune visée au point d) doit détenir les droits statutaires pour établir et entretenir les structures organisationnelles, les politiques, les processus et les procédures nécessaires à la mise en œuvre du point IS.I.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.I.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.I.OR.200 e);

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

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

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

v) les documents relatifs aux incidents et vulnérabilités en matière de sécurité de l'information signalés conformément aux systèmes de comptes rendus visés aux points IS.I.OR.215 et IS.I.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.I.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 confirmant que l'organisme travaillera en permanence conformément à la présente annexe et au MGSI. Lorsque le dirigeant responsable n'est pas le président de l'organisme, le président de l'organisme contresigne 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.I.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.I.OR.240 d), le cas échéant;

4) la politique en matière de sécurité de l'information de l'organisme visée au point IS.I.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.I.OR.240;

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.I.OR.200, y compris la ou les personnes responsables de la fonction de contrôle de la conformité visée au point IS.I.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 internes visé au point IS.I.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.I.OR.200 c);

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

iii) la procédure de modification du MGSI visée 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 MGSI doivent être gérées selon une procédure établie par l'organisme. Les modifications qui n'entrent pas dans le champ d'application de cette procédure et les modifications liées aux modifications visées au point IS.I.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.I.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.I.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.

*ANNEXE III*

Les annexes VI (partie ARA) et VII (partie ORA) du règlement (UE) n° 1178/2011 sont modifiées comme suit:

1) L'annexe VI (partie ARA) est modifiée comme suit:

a) au point ARA.GEN.125, le point c) suivant est ajouté:

«c) L'autorité compétente de l'État membre fournit dès que possible à l'Agence les informations pertinentes en matière de sécurité provenant des rapports sur la sécurité de l'information qu'elle a reçus en application du point IS.I.OR.230 de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203.»;

b) le point ARA.GEN.135A suivant est inséré après le point ARA.GEN.135:

«**ARA.GEN.135A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne**

a) L'autorité compétente met en œuvre un système permettant de recueillir, d'analyser et de diffuser de manière appropriée les informations relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne qui sont signalés par les organismes. Ce système est mis en œuvre en coordination avec toutes les autres autorités compétentes en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre afin d'améliorer la coordination et la compatibilité des systèmes de comptes rendus.

b) L'Agence met en œuvre un système visant à analyser de manière appropriée toute information pertinente en matière de sécurité reçue conformément au point ARA.GEN.125 c) et à fournir dans les meilleurs délais aux États membres et à la Commission toute information, notamment des recommandations ou des actions correctives à mettre en œuvre, utile pour leur permettre de réagir en temps opportun à un incident ou à une vulnérabilité en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne ayant trait à des produits, des pièces, des équipements non fixes, des personnes ou des organismes soumis au règlement (UE) 2018/1139 et à ses actes délégués et d'exécution.

c) Dès réception des informations auxquelles il est fait référence aux points a) et b), l'autorité compétente prend des mesures appropriées pour traiter l'incidence potentielle sur la sécurité aérienne de l'incident ou de la vulnérabilité en matière de sécurité de l'information.

d) Les mesures prises en application du point c) sont immédiatement notifiées à l'ensemble des personnes ou des organismes qui sont tenus de s'y conformer en vertu du règlement (UE) 2018/1139 et de ses actes délégués et d'exécution. L'autorité compétente de l'État membre notifie également ces mesures à l'Agence et, lorsqu'une action conjuguée est nécessaire, aux autorités compétentes des autres États membres concernés.»;

c) au point ARA.GEN.200, le point e) suivant est ajouté:

«e) Outre les exigences énoncées au point a), le système de gestion établi et entretenu par l'autorité compétente doit être conforme à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

d) le point ARA.GEN.205 est modifié comme suit:

i) le titre est remplacé par le texte suivant:

«**ARA.GEN.205 Attribution de tâches**»;

ii) le point c) suivant est ajouté:

«c) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ORA.GEN.200A, l'autorité compétente peut confier des tâches à des entités qualifiées conformément au point a), ou à toute autorité compétente en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre. Lors de l'attribution de tâches, l'autorité compétente s'assure:

1) que tous les aspects liés à la sécurité aérienne sont coordonnés et pris en considération par l'entité qualifiée ou l'autorité concernée;

2) que les résultats des activités de certification et de supervision menées par l'entité qualifiée ou l'autorité concernée sont intégrés dans les dossiers généraux de certification et de supervision de l'organisme;

3) que son propre système de gestion de la sécurité de l'information établi conformément au point ARA.GEN.200 e) englobe toutes les tâches de certification et de supervision continue effectuées pour son compte.»;

e) au point ARA.GEN.300, le point g) suivant est ajouté:

«g) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ORA.GEN.200A, outre le respect des points a) à f), l'autorité compétente examine tout agrément accordé en vertu du point IS.I.OR.200 e) du présent règlement ou du point IS.D.OR.200 e) du règlement délégué (UE) 2022/1645 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.»;

f) le point ARA.GEN.330A suivant est inséré après le point ARA.GEN.330:

«**ARA.GEN.330A Modification du système de gestion de la sécurité de l'information**

a) En ce qui concerne les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.I.OR.255 a) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point ARA.GEN.300. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point ARA.GEN.350.

b) En ce qui concerne les autres modifications nécessitant une demande d'approbation conformément au point IS.I.OR.255 b) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification.».

2) L'annexe VII (partie ORA) est modifiée comme suit:

le point ORA.GEN.200A suivant est inséré après le point ORA.GEN.200:

«**ORA.GEN.200A Système de gestion de la sécurité de l'information**

Outre le système de gestion visé au point ORA.GEN.200, l'organisme établit, met en œuvre et entretient un système de gestion de la sécurité de l'information conformément au règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.».

*ANNEXE IV*

L'annexe I (partie 21) du règlement (UE) n° 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.B.20:

«21.B.20A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne»;

b) le titre du point 21.B.30 est remplacé par le texte suivant:

«21.B.30 Attribution de tâches»;

c) le titre suivant est inséré après le titre 21.B.240:

«21.B.240A Modification du système de gestion de la sécurité de l'information»;

d) le titre suivant est inséré après le titre 21.B.435:

«21.B.435A Modification du système de gestion de la sécurité de l'information».

2) Au point 21.B.15, le point c) suivant est ajouté:

«c) L'autorité compétente de l'État membre fournit dès que possible à l'Agence les informations pertinentes en matière de sécurité provenant des rapports sur la sécurité de l'information qu'elle a reçus en application du point IS.D.OR.230 de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645.».

3) Le point suivant 21.B.20A est inséré après le point 21.B.20:

**«21.B.20A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne**

a) L'autorité compétente met en œuvre un système permettant de recueillir, d'analyser et de diffuser de manière appropriée les informations relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne qui sont signalés par les organismes. Ce système est mis en œuvre en coordination avec toutes les autres autorités compétentes en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre afin d'améliorer la coordination et la compatibilité des systèmes de comptes rendus.

b) L'Agence met en œuvre un système visant à analyser de manière appropriée toute information pertinente en matière de sécurité reçue conformément au point 21.B.15 c) et à fournir dans les meilleurs délais aux États membres et à la Commission toute information, notamment des recommandations ou des actions correctives à mettre en œuvre, utile pour leur permettre de réagir en temps opportun à un incident ou à une vulnérabilité en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne ayant trait à des produits, des pièces, des équipements non fixes, des personnes ou des organismes soumis au règlement (UE) 2018/1139 et à ses actes délégués et d'exécution.

c) Dès réception des informations auxquelles il est fait référence aux points a) et b), l'autorité compétente prend des mesures appropriées pour traiter l'incidence potentielle sur la sécurité aérienne de l'incident ou de la vulnérabilité en matière de sécurité de l'information.

d) Les mesures prises en application du point c) sont immédiatement notifiées à l'ensemble des personnes ou des organismes qui sont tenus de s'y conformer en vertu du règlement (UE) 2018/1139 et de ses actes délégués et d'exécution. L'autorité compétente de l'État membre notifie également ces mesures à l'Agence et, lorsqu'une action conjuguée est nécessaire, aux autorités compétentes des autres États membres concernés.».

4) Au point 21.B.25, le point e) suivant est ajouté:

«e) Outre les exigences énoncées au point a), le système de gestion établi et entretenu par l'autorité compétente doit être conforme à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.».

5) Le point 21.B.30 est modifié comme suit:

a) le titre est remplacé par le texte suivant:

**«21.B.30 Attribution de tâches»;**

b) le point c) suivant est ajouté:

«c) Pour la certification et la supervision de la conformité de l'organisme avec les points 21.A.139A et 21.A.239A, l'autorité compétente peut confier des tâches à des entités qualifiées conformément au point a), ou à toute autorité compétente en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre. Lors de l'attribution de tâches, l'autorité compétente s'assure:

1) que tous les aspects liés à la sécurité aérienne sont coordonnés et pris en considération par l'entité qualifiée ou l'autorité concernée;

2) que les résultats des activités de certification et de supervision menées par l'entité qualifiée ou l'autorité concernée sont intégrés dans les dossiers généraux de certification et de supervision de l'organisme;

3) que son propre système de gestion de la sécurité de l'information établi conformément au point 21.B.25 e) englobe toutes les tâches de certification et de supervision continue effectuées pour son compte.».

6) Au point 21.B.221, le point g) suivant est ajouté:

«g) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point 21.A.139A, outre le respect des points a) à f), l'autorité compétente examine tout agrément accordé en vertu du point IS.I.OR.200 e) du présent règlement ou du point IS.D.OR.200 e) du règlement délégué (UE) 2022/1645 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.».

7) Le point suivant 21.B.240A est inséré après le point 21.B.240:

«**21.B.240A Modification du système de gestion de la sécurité de l'information**

a) Pour les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.D.OR.255 a) de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point 21.B.221. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point 21.B.225.

b) Pour les autres modifications nécessitant une demande d'approbation conformément au point IS.D.OR.255 b) de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification.».

8) Au point 21.B.431, le point d) suivant est ajouté:

«d) Pour la certification et la supervision de la conformité de l'organisme avec le point 21.A.239A, outre la conformité aux points a) à c), l'autorité compétente doit respecter les principes suivants:

1) l'autorité compétente examine les interfaces et les risques correspondants recensés conformément au point IS.D.OR.205 b) de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645 par chaque organisme soumis à sa supervision;

2) si des divergences sont constatées dans les interfaces mutuelles et les risques correspondants recensés par différents organismes, l'autorité compétente doit les examiner avec les organismes concernés et, si nécessaire, établir les constatations nécessaires pour garantir la mise en œuvre de mesures correctives;

3) lorsque la documentation examinée conformément au point 2) révèle l'existence de risques significatifs liés aux interfaces avec des organismes soumis à la supervision d'une autorité compétente différente au sein du même État membre, ces informations doivent être communiquées à l'autorité compétente correspondante.».

9) Le point suivant 21.B.435A est inséré après le point 21.B.435:

«**21.B.435A Modification du système de gestion de la sécurité de l'information**

a) Pour les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.D.OR.255 a) de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point 21.B.431. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point 21.B.433.

b) Pour les autres modifications nécessitant une demande d'approbation conformément au point IS.D.OR.255 b) de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification..».

*ANNEXE V*

Les annexes II (partie ARO) et III (partie ORO) du règlement (UE) n° 965/2012 sont modifiées comme suit:

1) L'annexe II (partie ARO) est modifiée comme suit:

a) au point ARO.GEN.125, le point c) suivant est ajouté:

«c) L'autorité compétente de l'État membre fournit dès que possible à l'Agence les informations pertinentes en matière de sécurité provenant des rapports sur la sécurité de l'information qu'elle a reçus en application du point IS.I.OR.230 de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203.»;

b) le point ARO.GEN.135A suivant est inséré après le point ARO.GEN.135:

«**ARO.GEN.135A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne**

a) L'autorité compétente met en œuvre un système permettant de recueillir, d'analyser et de diffuser de manière appropriée les informations relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne qui sont signalés par les organismes. Ce système est mis en œuvre en coordination avec toutes les autres autorités compétentes en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre afin d'améliorer la coordination et la compatibilité des systèmes de comptes rendus.

b) L'Agence met en œuvre un système visant à analyser de manière appropriée toute information pertinente en matière de sécurité reçue conformément au point ARO.GEN.125 c) et à fournir dans les meilleurs délais aux États membres et à la Commission toute information, notamment des recommandations ou des actions correctives à mettre en œuvre, utile pour leur permettre de réagir en temps opportun à un incident ou à une vulnérabilité en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne ayant trait à des produits, des pièces, des équipements non fixes, des personnes ou des organismes soumis au règlement (UE) 2018/1139 et à ses actes délégués et d'exécution.

c) Dès réception des informations auxquelles il est fait référence aux points a) et b), l'autorité compétente prend des mesures appropriées pour traiter l'incidence potentielle sur la sécurité aérienne de l'incident ou de la vulnérabilité en matière de sécurité de l'information.

d) Les mesures prises en application du point c) sont immédiatement notifiées à l'ensemble des personnes ou des organismes qui sont tenus de s'y conformer en vertu du règlement (UE) 2018/1139 et de ses actes délégués et d'exécution. L'autorité compétente de l'État membre notifie également ces mesures à l'Agence et, lorsqu'une action conjuguée est nécessaire, aux autorités compétentes des autres États membres concernés.»;

c) au point ARO.GEN.200, le point e) suivant est ajouté:

«e) Outre les exigences énoncées au point a), le système de gestion établi et entretenu par l'autorité compétente doit être conforme à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

d) le point ARO.GEN.205 est modifié comme suit:

i) le titre est remplacé par le texte suivant:

«**ARO.GEN.205 Attribution de tâches**»;

ii) le point c) suivant est ajouté:

«c) Pour la certification et la supervision de la conformité de l'organisme avec le point ORO.GEN.200A, l'autorité compétente peut confier des tâches à des entités qualifiées conformément au point a), ou à toute autorité compétente en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre. Lors de l'attribution de tâches, l'autorité compétente s'assure:

1) que tous les aspects liés à la sécurité aérienne sont coordonnés et pris en considération par l'entité qualifiée ou l'autorité concernée;

2) que les résultats des activités de certification et de supervision menées par l'entité qualifiée ou l'autorité concernée sont intégrés dans les dossiers généraux de certification et de supervision de l'organisme;

3) que son propre système de gestion de la sécurité de l'information établi conformément au point ARO.GEN.200 e) englobe toutes les tâches de certification et de supervision continue effectuées pour son compte.»;

e) au point ARO.GEN.300, le point g) suivant est ajouté:

«g) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ORO.GEN.200A, outre le respect des points a) à f), l'autorité compétente examine tout agrément accordé en vertu du point IS.I.OR.200 e) du présent règlement ou du point IS.D.OR.200 e) du règlement délégué (UE) 2022/1645 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.»;

f) le point ARO.GEN.330A suivant est inséré après le point ARO.GEN.330:

«**ARO.GEN.330A Modification du système de gestion de la sécurité de l'information**

a) Pour les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.I.OR.255 a) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point ARO.GEN.300. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point ARO.GEN.350.

b) Pour les autres modifications nécessitant une demande d'approbation conformément au point IS.I.OR.255 b) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification.».

2) L'annexe III (partie ORO) est modifiée comme suit:

le point ORO.GEN.200A suivant est inséré après le point ORO.GEN.200:

«**ORO.GEN.200A Système de gestion de la sécurité de l'information**

Outre le système de gestion visé au point ORO.GEN.200, l'exploitant établit, met en œuvre et entretient un système de gestion de la sécurité de l'information conformément au règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.».

*ANNEXE VI*

L'annexe II (partie ADR.AR) du règlement (UE) n° 139/2014 est modifiée comme suit:

1) Au point ADR.AR.A.025, le point c) suivant est ajouté:

«c) L'autorité compétente de l'État membre fournit dès que possible à l'Agence les informations pertinentes en matière de sécurité provenant des rapports sur la sécurité de l'information qu'elle a reçus en application du point IS.D.OR.230 de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645.».

2) Le point ADR.AR.A.030A suivant est inséré après le point ADR.AR.A.030:

«**ADR.AR.A.030A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne**

a) L'autorité compétente met en œuvre un système permettant de recueillir, d'analyser et de diffuser de manière appropriée les informations relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne qui sont signalés par les organismes. Ce système est mis en œuvre en coordination avec toutes les autres autorités compétentes en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre afin d'améliorer la coordination et la compatibilité des systèmes de comptes rendus.

b) L'Agence met en œuvre un système visant à analyser de manière appropriée toute information pertinente en matière de sécurité reçue conformément au point ADR.AR.A.025 c) et à fournir dans les meilleurs délais aux États membres et à la Commission toute information, notamment des recommandations ou des actions correctives à mettre en œuvre, utile pour leur permettre de réagir en temps opportun à un incident ou à une vulnérabilité en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne ayant trait à des produits, des pièces, des équipements non fixes, des personnes ou des organismes soumis au règlement (UE) 2018/1139 et à ses actes délégués et d'exécution.

c) Dès réception des informations auxquelles il est fait référence aux points a) et b), l'autorité compétente prend des mesures appropriées pour traiter l'incidence potentielle sur la sécurité aérienne de l'incident ou de la vulnérabilité en matière de sécurité de l'information.

d) Les mesures prises en application du point c) sont immédiatement notifiées à l'ensemble des personnes ou des organismes qui sont tenus de s'y conformer en vertu du règlement (UE) 2018/1139 et de ses actes délégués et d'exécution. L'autorité compétente de l'État membre notifie également ces mesures à l'Agence et, lorsqu'une action conjuguée est nécessaire, aux autorités compétentes des autres États membres concernés.».

3) Au point ADR.AR.B.005, le point d) suivant est ajouté:

«d) Outre les exigences énoncées au point a), le système de gestion établi et entretenu par l'autorité compétente doit être conforme à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.».

4) Le point ADR.AR.B.010 est modifié comme suit:

i) le titre est remplacé par le texte suivant:

«**ADR.AR.B.010 Attribution de tâches**»;

ii) le point c) suivant est ajouté:

«c) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ADR.OR.D.005A, l'autorité compétente peut confier des tâches à des entités qualifiées conformément au point a), ou à toute autorité compétente en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre. Lors de l'attribution de tâches, l'autorité compétente s'assure:

1) que tous les aspects liés à la sécurité aérienne sont coordonnés et pris en considération par l'entité qualifiée ou l'autorité concernée;

2) que les résultats des activités de certification et de supervision menées par l'entité qualifiée ou l'autorité concernée sont intégrés dans les dossiers généraux de certification et de supervision de l'organisme;

3) que son propre système de gestion de la sécurité de l'information établi conformément au point ADR.AR.B.005 e) englobe toutes les tâches de certification et de supervision continue effectuées pour son compte.».

5) Au point ADR.AR.C.005, le point f) suivant est ajouté:

«f) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ADR.OR.D.005A, outre le respect des points a) à e), l'autorité compétente examine tout agrément accordé en vertu du point IS.I.OR.200 e) du présent règlement ou du point IS.D.OR.200 e) du règlement délégué (UE) 2022/1645 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.».

6) Le point suivant ADR.AR.C.040A est inséré après le point ADR.AR.C.040:

«**ADR.AR.C.040A Modification du système de gestion de la sécurité de l'information**

a) En ce qui concerne les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.D.OR.255 a) de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point ADR.AR.C.005. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point ADR.AR.C.055.

b) En ce qui concerne les autres modifications nécessitant une demande d'approbation conformément au point IS.D.OR.255 b) de l'annexe (partie IS.D.OR) du règlement délégué (UE) 2022/1645:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification.».

*ANNEXE VII*

Les annexes II (partie 145), III (partie 66) et V *quater* (partie CAMO) du règlement (UE) n° 1321/2014 sont modifiées comme suit:

1) L'annexe II (partie 145) est modifiée comme suit:

a) la table des matières est modifiée comme suit:

i) le titre suivant est inséré après le titre 145.A.200:

«145.A.200A Système de gestion de la sécurité de l'information»;

ii) le titre suivant est inséré après le titre 145.B.135:

«145.B.135A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne»;

iii) le titre du point 145.B.205 est remplacé par le texte suivant:

«145.B.205 Attribution de tâches»;

iv) le titre suivant est inséré après le titre 145.B.330:

«145.B.330A Modification du système de gestion de la sécurité de l'information»;

b) le point suivant 145.A.200A est inséré après le point 145.A.200:

«145.A.200A **Système de gestion de la sécurité de l'information**

Outre le système de gestion visé au point 145.A.200, l'organisme de maintenance établit, met en œuvre et entretient un système de gestion de la sécurité de l'information conformément au règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

c) au point 145.B.125, le point c) suivant est ajouté:

«c) L'autorité compétente de l'État membre fournit dès que possible à l'Agence les informations pertinentes en matière de sécurité provenant des rapports sur la sécurité de l'information qu'elle a reçus en application du point IS.I.OR.230 de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203.»;

d) le point suivant 145.B.135A est inséré après le point 145.B.135:

«145.B.135A **Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne**

a) L'autorité compétente met en œuvre un système permettant de recueillir, d'analyser et de diffuser de manière appropriée les informations relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne qui sont signalés par les organismes. Ce système est mis en œuvre en coordination avec toutes les autres autorités compétentes en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre afin d'améliorer la coordination et la compatibilité des systèmes de comptes rendus.

b) L'Agence met en œuvre un système visant à analyser de manière appropriée toute information pertinente en matière de sécurité reçue conformément au point 145.B.125 c) et à fournir dans les meilleurs délais aux États membres et à la Commission toute information, notamment des recommandations ou des actions correctives à mettre en œuvre, utile pour leur permettre de réagir en temps opportun à un incident ou à une vulnérabilité en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne ayant trait à des produits, des pièces, des équipements non fixes, des personnes ou des organismes soumis au règlement (UE) 2018/1139 et à ses actes délégués et d'exécution.

c) Dès réception des informations auxquelles il est fait référence aux points a) et b), l'autorité compétente prend des mesures appropriées pour traiter l'incidence potentielle sur la sécurité aérienne de l'incident ou de la vulnérabilité en matière de sécurité de l'information.

d) Les mesures prises en application du point c) sont immédiatement notifiées à l'ensemble des personnes ou des organismes qui sont tenus de s'y conformer en vertu du règlement (UE) 2018/1139 et de ses actes délégués et d'exécution. L'autorité compétente de l'État membre notifie également ces mesures à l'Agence et, lorsqu'une action conjuguée est nécessaire, aux autorités compétentes des autres États membres concernés.»;

e) au point 145.B.200, le point e) suivant est ajouté:

«e) Outre les exigences énoncées au point a), le système de gestion établi et entretenu par l'autorité compétente doit être conforme à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

f) le point 145.B.205 est modifié comme suit:

i) le titre est remplacé par le texte suivant:

«145.B.205 **Attribution de tâches**»;

ii) le point c) suivant est ajouté:

«c) Pour la certification et la supervision de la conformité de l'organisme avec le point 145.A.200A, l'autorité compétente peut confier des tâches à des entités qualifiées conformément au point a), ou à toute autorité compétente en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre. Lors de l'attribution de tâches, l'autorité compétente s'assure:

1) que tous les aspects liés à la sécurité aérienne sont coordonnés et pris en considération par l'entité qualifiée ou l'autorité concernée;

2) que les résultats des activités de certification et de supervision menées par l'entité qualifiée ou l'autorité concernée sont intégrés dans les dossiers généraux de certification et de supervision de l'organisme;

3) que son propre système de gestion de la sécurité de l'information établi conformément au point 145.B.200 e) englobe toutes les tâches de certification et de supervision continue effectuées pour son compte.»;

g) au point 145.B.300, le point g) suivant est ajouté:

«g) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point 145.A.200A, outre le respect des points a) à f), l'autorité compétente examine tout agrément accordé en vertu du point IS.I.OR.200 e) du présent règlement ou du point IS.D.OR.200 e) du règlement délégué (UE) 2022/1645 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.»;

h) le point suivant 145.B.330A est inséré après le point 145.B.330:

«145.B.330A **Modification du système de gestion de la sécurité de l'information**

a) Pour les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.I.OR.255 a) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point 145.B.300. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point 145.B.350.

b) Pour les autres modifications nécessitant une demande d'approbation conformément au point IS.I.OR.255 b) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification.».

2) L'annexe III (partie 66) est modifiée comme suit:

a) dans la table des matières, le titre suivant est inséré après le titre 66.B.10:

«66.B.15 Système de gestion de la sécurité de l'information»;

b) le point 66.B.15 suivant est inséré après le point 66.B.10:

«66.B.15 **Système de gestion de la sécurité de l'information**

L'autorité compétente établit, met en œuvre et entretient un système de gestion de la sécurité de l'information conformément à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.».

3) L'annexe V *quater* (partie CAMO) est modifiée comme suit:

a) la table des matières est modifiée comme suit:

i) le titre suivant est inséré après le titre CAMO.A.200:

«CAMO.A.200A Système de gestion de la sécurité de l'information»;

ii) le titre suivant est inséré après le titre CAMO.B.135:

«CAMO.B.135A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne»;

iii) le titre du point CAMO.B.205 est remplacé par le texte suivant:

«CAMO.B.205 Attribution de tâches»;

iv) le titre suivant est inséré après le titre CAMO.B.330:

«CAMO.B.330A Modification du système de gestion de la sécurité de l'information»;

b) le point CAMO.A.200A suivant est inséré après le point CAMO.A.200:

«CAMO.A.200A **Système de gestion de la sécurité de l'information**

Outre le système de gestion visé au point CAMO.A.200, l'organisme établit, met en œuvre et entretient un système de gestion de la sécurité de l'information conformément au règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

c) au point CAMO.B.125, le point c) suivant est ajouté:

«c) L'autorité compétente de l'État membre fournit dès que possible à l'Agence les informations pertinentes en matière de sécurité provenant des rapports sur la sécurité de l'information qu'elle a reçus en application du point IS.I.OR.230 de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203.»;

d) le point CAMO.B.135A suivant est inséré après le point CAMO.B.135:

«CAMO.B.135A **Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne**

a) L'autorité compétente met en œuvre un système permettant de recueillir, d'analyser et de diffuser de manière appropriée les informations relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne qui sont signalés par les organismes. Ce système est mis en œuvre en coordination avec toutes les autres autorités compétentes en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre afin d'améliorer la coordination et la compatibilité des systèmes de comptes rendus.

b) L'Agence met en œuvre un système visant à analyser de manière appropriée toute information pertinente en matière de sécurité reçue conformément au point CAMO.B.125 c) et à fournir dans les meilleurs délais aux États membres et à la Commission toute information, notamment des recommandations ou des actions correctives à mettre en œuvre, utile pour leur permettre de réagir en temps opportun à un incident ou à une vulnérabilité en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne ayant trait à des produits, des pièces, des équipements non fixes, des personnes ou des organismes soumis au règlement (UE) 2018/1139 et à ses actes délégués et d'exécution.

c) Dès réception des informations auxquelles il est fait référence aux points a) et b), l'autorité compétente prend des mesures appropriées pour traiter l'incidence potentielle sur la sécurité aérienne de l'incident ou de la vulnérabilité en matière de sécurité de l'information.

d) Les mesures prises en application du point c) sont immédiatement notifiées à l'ensemble des personnes ou des organismes qui sont tenus de s'y conformer en vertu du règlement (UE) 2018/1139 et de ses actes délégués et d'exécution. L'autorité compétente de l'État membre notifie également ces mesures à l'Agence et, lorsqu'une action conjuguée est nécessaire, aux autorités compétentes des autres États membres concernés.»;

e) au point CAMO.B.200, le point e) suivant est ajouté:

«e) Outre les exigences énoncées au point a), le système de gestion établi et entretenu par l'autorité compétente doit être conforme à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

f) le point CAMO.B.205 est modifié comme suit:

i) le titre est remplacé par le texte suivant:

«CAMO.B.205 **Attribution de tâches**»;

ii) le point c) suivant est ajouté:

«c) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point CAMO.A.200A, l'autorité compétente peut confier des tâches à des entités qualifiées conformément au point a), ou à toute autorité compétente en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre. Lors de l'attribution de tâches, l'autorité compétente s'assure:

1) que tous les aspects liés à la sécurité aérienne sont coordonnés et pris en considération par l'entité qualifiée ou l'autorité concernée;

2) que les résultats des activités de certification et de supervision menées par l'entité qualifiée ou l'autorité concernée sont intégrés dans les dossiers généraux de certification et de supervision de l'organisme;

3) que son propre système de gestion de la sécurité de l'information établi conformément au point CAMO.B.200 e) englobe toutes les tâches de certification et de supervision continue effectuées pour son compte.»;

g) au point CAMO.B.300, le point g) suivant est ajouté:

«g) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point CAMO.A.200A, outre le respect des points a) à f), l'autorité compétente examine tout agrément accordé en vertu du point IS.I.OR.200 e) du présent règlement ou du point IS.D.OR.200 e) du règlement délégué (UE) 2022/1645 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.»;

h) le point CAMO.B.330A suivant est inséré après le point CAMO.B.330:

«CAMO.B.330A **Modification du système de gestion de la sécurité de l'information**

a) Pour les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.I.OR.255 a) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point CAMO.B.300. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point CAMO.B.350.

b) Pour les autres modifications nécessitant une demande d'approbation conformément au point IS.I.OR.255 b) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification.».

*ANNEXE VIII*

Les annexes II (partie ATCO.AR) et III (partie ATCO.OR) du règlement (UE) 2015/340 sont modifiées comme suit:

1) L'annexe II (partie ATCO.AR) est modifiée comme suit:

a) au point ATCO.AR.A.020, le point c) suivant est ajouté:

«c) L'autorité compétente de l'État membre fournit dès que possible à l'Agence les informations pertinentes en matière de sécurité provenant des rapports sur la sécurité de l'information qu'elle a reçus en application du point IS.I.OR.230 de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203.»;

b) le point ATCO.AR.A.025A suivant est inséré après le point ATCO.AR.A.025:

«**ATCO.AR.A.025A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne**

a) L'autorité compétente met en œuvre un système permettant de recueillir, d'analyser et de diffuser de manière appropriée les informations relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne qui sont signalés par les organismes. Ce système est mis en œuvre en coordination avec toutes les autres autorités compétentes en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre afin d'améliorer la coordination et la compatibilité des systèmes de comptes rendus.

b) L'Agence met en œuvre un système visant à analyser de manière appropriée toute information pertinente en matière de sécurité reçue conformément au point ATCO.AR.A.020 et à fournir dans les meilleurs délais aux États membres et à la Commission toute information, notamment des recommandations ou des actions correctives à mettre en œuvre, utile pour leur permettre de réagir en temps opportun à un incident ou à une vulnérabilité en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne ayant trait à des produits, des pièces, des équipements non fixes, des personnes ou des organismes soumis au règlement (UE) 2018/1139 et à ses actes délégués et d'exécution.

c) Dès réception des informations auxquelles il est fait référence aux points a) et b), l'autorité compétente prend des mesures appropriées pour traiter l'incidence potentielle sur la sécurité aérienne de l'incident ou de la vulnérabilité en matière de sécurité de l'information.

d) Les mesures prises en application du point c) sont immédiatement notifiées à l'ensemble des personnes ou des organismes qui sont tenus de s'y conformer en vertu du règlement (UE) 2018/1139 et de ses actes délégués et d'exécution. L'autorité compétente de l'État membre notifie également ces mesures à l'Agence et, lorsqu'une action conjuguée est nécessaire, aux autorités compétentes des autres États membres concernés.»;

c) au point ATCO.AR.B.001, le point e) suivant est ajouté:

«e) Outre les exigences énoncées au point a), le système de gestion établi et entretenu par l'autorité compétente doit être conforme à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

d) le point ATCO.AR.B.005 est modifié comme suit:

i) le titre est remplacé par le texte suivant:

«**ATCO.AR.B.005 Attribution de tâches**»;

ii) le point c) suivant est ajouté:

«c) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ATCO.OR.C.001A, l'autorité compétente peut confier des tâches à des entités qualifiées conformément au point a), ou à toute autorité compétente en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre. Lors de l'attribution de tâches, l'autorité compétente s'assure:

1) que tous les aspects liés à la sécurité aérienne sont coordonnés et pris en considération par l'entité qualifiée ou l'autorité concernée;

2) que les résultats des activités de certification et de supervision menées par l'entité qualifiée ou l'autorité concernée sont intégrés dans les dossiers généraux de certification et de supervision de l'organisme;

3) que son propre système de gestion de la sécurité de l'information établi conformément au point ATCO.AR.B.001 e) englobe toutes les tâches de certification et de supervision continue effectuées pour son compte.»;

e) au point ATCO.AR.C.001, le point f) suivant est ajouté:

«f) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ATCO.OR.C.001A, outre le respect des points a) à e), l'autorité compétente examine tout agrément accordé en vertu du point IS.I.OR.200 e) du présent règlement ou du point IS.D.OR.200 e) du règlement délégué (UE) 2022/1645 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.»;

f) le point ATCO.AR.E.010A suivant est inséré après le point ATCO.AR.E.010:

«**ATCO.AR.E.010A Modification du système de gestion de la sécurité de l'information**

a) En ce qui concerne les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.I.OR.255 a) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point ATCO.AR.C.001. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point ATCO.AR.C.010.

b) En ce qui concerne les autres modifications nécessitant une demande d'approbation conformément au point IS.I.OR.255 b) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification.».

2) L'annexe III (partie ATCO.OR) est modifiée comme suit:

le point ATCO.OR.C.001A suivant est inséré après le point ATCO.OR.C.001:

«**ATCO.OR.C.001A Système de gestion de la sécurité de l'information**

Outre le système de gestion visé au point ATCO.OR.C.001, l'organisme de formation établit, met en œuvre et entretient un système de gestion de la sécurité de l'information conformément au règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.».

*ANNEXE IX*

Les annexes II (partie ATM/ANS.AR) et III (partie ATM/ANS.OR) du règlement d'exécution (UE) 2017/373 sont modifiées comme suit:

1) L'annexe II (partie ATM/ANS.AR) est modifiée comme suit:

a) au point ATM/ANS.AR.A.020, le point c) suivant est ajouté:

«c) L'autorité compétente de l'État membre fournit dès que possible à l'Agence les informations pertinentes en matière de sécurité provenant des rapports sur la sécurité de l'information qu'elle a reçus en application du point IS.I.OR.230 de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203.»;

b) le point ATM/ANS.AR.A.025A suivant est inséré après le point ATM/ANS.AR.A.025:

«**ATM/ANS.AR.A.025A Réaction immédiate à un incident ou à une vulnérabilité en matière de sécurité de l'information ayant une incidence sur la sécurité aérienne**

a) L'autorité compétente met en œuvre un système permettant de recueillir, d'analyser et de diffuser de manière appropriée les informations relatives aux incidents et aux vulnérabilités en matière de sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne qui sont signalés par les organismes. Ce système est mis en œuvre en coordination avec toutes les autres autorités compétentes en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre afin d'améliorer la coordination et la compatibilité des systèmes de comptes rendus.

b) L'Agence met en œuvre un système visant à analyser de manière appropriée toute information pertinente en matière de sécurité reçue conformément au point ATM/ANS.AR.A.020 c) et à fournir dans les meilleurs délais aux États membres et à la Commission toute information, notamment des recommandations ou des actions correctives à mettre en œuvre, utile pour leur permettre de réagir en temps opportun à un incident ou à une vulnérabilité en matière de sécurité de l'information susceptible d'avoir une incidence sur la sécurité aérienne ayant trait à des produits, des pièces, des équipements non fixes, des personnes ou des organismes soumis au règlement (UE) 2018/1139 et à ses actes délégués et d'exécution.

c) Dès réception des informations auxquelles il est fait référence aux points a) et b), l'autorité compétente prend des mesures appropriées pour traiter l'incidence potentielle sur la sécurité aérienne de l'incident ou de la vulnérabilité en matière de sécurité de l'information.

d) Les mesures prises en application du point c) sont immédiatement notifiées à l'ensemble des personnes ou des organismes qui sont tenus de s'y conformer en vertu du règlement (UE) 2018/1139 et de ses actes délégués et d'exécution. L'autorité compétente de l'État membre notifie également ces mesures à l'Agence et, lorsqu'une action conjuguée est nécessaire, aux autorités compétentes des autres États membres concernés.»;

c) au point ATM/ANS.AR.B.001, le point e) suivant est ajouté:

«e) Outre les exigences énoncées au point a), le système de gestion établi et entretenu par l'autorité compétente doit être conforme à l'annexe I (partie IS.AR) du règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

d) le point ATM/ANS.AR.B.005 est modifié comme suit:

i) le titre est remplacé par le texte suivant:

«**ATM/ANS.AR.B.005 Attribution de tâches**»;

ii) le point c) suivant est ajouté:

«c) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ATM/ANS.OR.B.005A, l'autorité compétente peut confier des tâches à des entités qualifiées conformément au point a), ou à toute autorité compétente en matière de sécurité de l'information ou de cybersécurité au sein de l'État membre. Lors de l'attribution de tâches, l'autorité compétente s'assure:

1) que tous les aspects liés à la sécurité aérienne sont coordonnés et pris en considération par l'entité qualifiée ou l'autorité concernée;

2) que les résultats des activités de certification et de supervision menées par l'entité qualifiée ou l'autorité concernée sont intégrés dans les dossiers généraux de certification et de supervision de l'organisme;

3) que son propre système de gestion de la sécurité de l'information établi conformément au point ATM/ANS.AR.B.001 e) englobe toutes les tâches de certification et de supervision continue effectuées pour son compte.»;

e) au point ATM/ANS.AR.C.010, le point d) suivant est ajouté:

«d) En ce qui concerne la certification et la supervision de la conformité de l'organisme avec le point ATM/ANS.OR.B.005A, outre le respect des points a) à c), l'autorité compétente examine tout agrément accordé en vertu du point IS.I.OR.200 e) du présent règlement ou du point IS.D.OR.200 e) du règlement délégué (UE) 2022/1645 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.»;

f) le point ATM/ANS.AR.C.025A suivant est inséré après le point ATM/ANS.AR.C.025:

«**ATM/ANS.AR.C.025A Modification du système de gestion de la sécurité de l'information**

a) Pour les modifications gérées et notifiées à l'autorité compétente conformément à la procédure définie au point IS.I.OR.255 a) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203, l'autorité compétente inclut l'examen de ces modifications dans sa supervision continue conformément aux principes énoncés au point ATM/ANS.AR.C.010. En cas de constatation d'une non-conformité, l'autorité compétente en informe l'organisme, demande de nouvelles modifications et agit conformément au point ATM/ANS.AR.C.050.

b) En ce qui concerne les autres modifications nécessitant une demande d'approbation conformément au point IS.I.OR.255 b) de l'annexe II (partie IS.I.OR) du règlement d'exécution (UE) 2023/203:

1) dès la réception de la demande de modification, l'autorité compétente vérifie que l'organisme satisfait aux exigences applicables avant de donner son approbation;

2) l'autorité compétente définit les conditions dans lesquelles l'organisme peut exercer ses activités pendant la mise en œuvre de la modification;

3) si elle est assurée que l'organisme satisfait aux exigences applicables, l'autorité compétente approuve la modification.».

2) L'annexe III (partie ATM/ANS.OR) est modifiée comme suit:

a) le point ATM/ANS.OR.B.005A suivant est inséré après le point ATM/ANS.OR.B.005:

«**ATM/ANS.OR.B.005A Système de gestion de la sécurité de l'information**

Outre le système de gestion visé au point ATM/ANS.OR.B.005, le prestataire de services établit, met en œuvre et entretient un système de gestion de la sécurité de l'information conformément au règlement d'exécution (UE) 2023/203 afin d'assurer la bonne gestion des risques liés à la sécurité de l'information susceptibles d'avoir une incidence sur la sécurité aérienne.»;

b) le point ATM/ANS.OR.D.010 est remplacé par le texte suivant:

«**ATM/ANS.OR.D.010 Gestion de la sûreté**

a) Les prestataires de services de navigation aérienne et de gestion des courants de trafic aérien et le gestionnaire de réseau établissent, en tant que partie intégrante de leur système de gestion tel que requis au point ATM/ANS.OR.B.005, un système de gestion de la sûreté afin de garantir:

1) la sûreté de leurs installations et de leur personnel de manière à prévenir toute interférence illicite dans la fourniture des services;

2) la sûreté des données opérationnelles qu'ils reçoivent, produisent ou utilisent, de manière que leur accès soit réservé aux seules personnes autorisées.

b) Le système de gestion de la sûreté définit:

1) le processus et les procédures relatifs à l'évaluation et à l'atténuation des risques dans le domaine de la sûreté, 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 recenser, superviser et 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.

c) Les prestataires de services de navigation aérienne et de gestion des courants de trafic aérien et le gestionnaire de réseau garantissent, s'il y a lieu, l'habilitation de sûreté de leur personnel et travaillent en coordination avec les autorités civiles et militaires compétentes pour assurer la sûreté de leurs installations, de leur personnel et de leurs données.

d) Les aspects relatifs à la sécurité de l'information sont gérés conformément au point ATM/ANS.OR.B.005A.».