II

(Non-legislative acts)

REGULATIONS

COMMISSION IMPLEMENTING REGULATION (EU) 2023/203

of 27 October 2022

laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340 and (EU) No 139/2014, Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664 and amending Commission Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340, and Commission Implementing Regulations (EU) 2017/373 and (EU) 2021/664

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 ([1]), and in particular Articles 17(1) point (b), 27(1) point (a), 31(1) point (b), 43(1) point (b), 53(1) point (a) and 62(15) point (c) thereof

Whereas:

(1) In accordance with the essential requirements set out in Annex II, point 3.1(b), to Regulation (EU) 2018/1139, continuing airworthiness management organisations and maintenance organisations are to implement and maintain a management system to manage safety risks.

(2) In addition, in accordance with the essential requirements set out in Annex IV, point 3.3(b) and point 5(b), to Regulation (EU) 2018/1139, pilot training organisations, cabin crew training organisations, aero-medical centres for aircrew and operators of flight simulation training devices are to implement and maintain a management system to manage safety risks.

(3) Moreover, in accordance with the essential requirements set out in Annex V, point 8.1(c), to Regulation (EU) 2018/1139, air operators are to implement and maintain a management system to manage safety risks.

(4) Furthermore, in accordance with the essential requirements set out in Annex VIII, point 5.1(c) and point 5.4(b), to Regulation (EU) 2018/1139, air traffic management and air navigation service providers, U-space service providers and single common information service providers, and training organisations and aero-medical centres for air traffic controllers are to implement and maintain a management system to manage safety risks.

([1]) OJ L 212, 22.8.2018, p. 1.

(5) Those safety risks may derive from different sources, such as design and maintenance flaws, human performance aspects, environmental threats and information security threats. Therefore, the management systems implemented by the European Union Aviation Safety Agency ('the Agency') and the national competent authorities and organisations referred to in the recitals above, should take into account not only safety risks stemming from random events, but also safety risks deriving from information security threats where existing flaws may be exploited by individuals with a malicious intent. Those information security risks are constantly increasing in the civil aviation environment as the current information systems are becoming more and more interconnected, and increasingly becoming the target of malicious actors.

(6) The risks associated with those information systems are not limited to possible attacks to the cyberspace, but encompass also threats, which may affect processes and procedures as well as the performance of human beings.

(7) A significant number of organisations already use international standards, such as ISO 27001, in order to address the security of digital information and data. Those standards may not fully address all the specificities of civil aviation. Therefore, it is appropriate to set out requirements for the management of information security risks with a potential impact on aviation safety.

(8) It is essential that those requirements cover all aviation domains and their interfaces, since aviation is a highly interconnected system of systems. Therefore, they should apply to all the organisations and competent authorities covered by Commission Regulations (EU) No 748/2012 ([2]), (EU) No 1321/2014 ([3]), (EU) No 965/2012 ([4]), (EU) No 1178/2011 ([5]), (EU) 2015/340 ([6]), (EU) No 139/2014 ([7]) and Commission Implementing Regulation (EU) 2021/664 ([8]), also those that are already required to have a management system in accordance with the existing Union aviation safety legislation. However, some organisations should be excluded from the scope of this Regulation in order to ensure appropriate proportionality to the lower information security risks they pose to the aviation system.

(9) The requirements laid down in this Regulation should ensure a consistent implementation across all aviation domains, while creating a minimal impact on the Union aviation safety legislation already applicable to those domains.

([2]) Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations (OJ L 224, 21.8.2012, p. 1).

([3]) Commission Regulation (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks (Recast) (OJ L 362, 17.12.2014, p. 1).

([4]) Commission Regulation (EU) No 965/2012 of 5 October 2012 laying down technical requirements and administrative procedures related to air operations pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 296, 25.10.2012, p. 1).

([5]) Commission Regulation (EU) No 1178/2011 of 3 November 2011 laying down technical requirements and administrative procedures related to civil aviation aircrew pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 311, 25.11.2011, p. 1).

([6]) Commission Regulation (EU) 2015/340 of 20 February 2015 laying down technical requirements and administrative procedures relating to air traffic controllers' licences and certificates pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council, amending Commission Implementing Regulation (EU) No 923/2012 and repealing Commission Regulation (EU) No 805/2011 (OJ L 63, 6.3.2015, p. 1).

([7]) Commission Regulation (EU) No 139/2014 of 12 February 2014 laying down requirements and administrative procedures related to aerodromes pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 44, 14.2.2014, p. 1).

([8]) Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (OJ L 139, 23.4.2021, p. 161).

(10) The requirements laid down in this Regulation should be without prejudice to information security and cybersecurity requirements laid down in Point 1.7 of the Annex to Commission Implementing Regulation (EU) 2015/1998 ([9]) and in Article 14 of Directive (EU) 2016/1148 of the European Parliament and of the Council ([10]).

(11) The security requirements laid down in Articles 33 to 43 of Title V 'Security of the Programme' of Regulation (EU) 2021/696 of the European Parliament and of the Council ([11]) are considered to be equivalent with the requirements laid down in this Regulation, except as regards point IS.I.OR.230 of Annex II to this Regulation which should be complied with.

(12) In order to provide legal certainty, the interpretation of the term 'information security' as defined in this Regulation, reflecting its common use in civil aviation globally, should be considered as being consistent with that of the term 'security of network and information systems' as defined in Article 4(2) of Directive (EU) 2016/1148. The definition of information security used for the purposes of this Regulation should not be interpreted as divergent from the definition of security of network and information systems laid down in Directive (EU) 2016/1148.

(13) In order to avoid duplication of legal requirements, where organisations covered by this Regulation are already subject to security requirements arising from Union acts referred to in recitals (10) and (11) which are in their effect equivalent to the provisions laid down in this Regulation, compliance with those security requirements should be considered to constitute compliance with the requirements laid down in this Regulation.

(14) Organisations covered by this Regulation that are already subject to security requirements arising from Implementing Regulation (EU) 2015/1998 or Regulation (EU) 2021/696, or both, should also comply with the requirements of Annex II (Part IS.I.OR.230 'Information security external reporting scheme') to this Regulation as neither Regulation contains provisions related to external reporting of information security incidents.

(15) For the sake of completeness, Regulations (EU) No 1178/2011, (EU) No 748/2012, (EU) No 965/2012, (EU) No 139/2014, (EU) No 1321/2014, (EU) 2015/340 and Implementing Regulations (EU) 2017/373 ([12]) and (EU) 2021/664 should be amended in order to introduce the information security management system requirements prescribed in this Regulation together with the management systems set out therein, and to set out the competent authorities' requirements as regards the oversight of organisations implementing the aforementioned information security management requirements.

(16) In order to provide organisations with sufficient time to ensure compliance with the new rules and procedures, this Regulation should apply 3 years after its entry into force, except for the air navigation service provider of the European Geostationary Navigation Overlay Service (EGNOS) defined in Implementing Regulation (EU) 2017/373, where due to the ongoing security accreditation of the EGNOS system and services in line with Regulation (EU) 2021/696, it should become applicable from 1 January 2026.

(17) The requirements laid down in this Regulation are based on Opinion No 03/2021 ([13]), issued by the Agency in accordance with Article 75(2) points (b) and (c) and Article 76(1) of Regulation (EU) 2018/1139.

([9]) Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (OJ L 299, 14.11.2015, p. 1).

([10]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

([11]) Regulation (EU) 2021/696 of the European Parliament and of the Council of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU (OJ L 170, 12.5.2021, p. 69).

([12]) Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011 (OJ L 62, 8.3.2017, p. 1).

([13]) https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

(18) The requirements laid down in this Regulation are in accordance with the opinion of the Committee for the application of common safety rules in the field of civil aviation established by Article 127 of Regulation (EU) 2018/1139,

HAS ADOPTED THIS REGULATION:

Article 1

Subject matter

This Regulation sets out the requirements to be met by the organisations and competent authorities in order:

(a) to identify and manage information security risks with potential impact on aviation safety which could affect information and communication technology systems and data used for civil aviation purposes,

(b) to detect information security events and identify those which are considered information security incidents with potential impact on aviation safety,

(c) to respond to, and recover from, those information security incidents.

Article 2

Scope

1. This Regulation applies to the following organisations:

(a) maintenance organisations subject to Section A of Annex II (Part-145) to Regulation (EU) No 1321/2014, except those solely involved in the maintenance of aircraft in accordance with Annex Vb (Part-ML) to Regulation (EU) No 1321/2014;

(b) continuing airworthiness management organisations (CAMOs) subject to Section A of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014, except those solely involved in the continuing airworthiness management of aircraft in accordance with Annex Vb (Part-ML) to Regulation (EU) No 1321/2014;

(c) air operators subject to Annex III (Part-ORO) to Regulation (EU) No 965/2012, except those solely involved in the operation of any of the following:

(i) an ELA 2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012;

(ii) single-engine propeller-driven aeroplanes with a Maximum Operational Passenger Seating Configuration of 5 or less that are not classified as complex motor-powered aircraft, when taking off and landing at the same aerodrome or operating site and operating under Visual Flight Rules (VFR) by day rules;

(iii) single-engine helicopters with a Maximum Operational Passenger Seating Configuration of 5 or less that are not classified as complex motor-powered aircraft, when taking off and landing at the same aerodrome or operating site and operating under VFR by day rules.

(d) approved training organisations (ATOs) subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011, except those solely involved in training activities of ELA2 aircraft as defined in Article 1(2), point (j) of Regulation (EU) No 748/2012, or solely involved in theoretical training;

(e) aircrew aero-medical centres subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011;

(f) flight simulation training device (FSTD) operators subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011, except those solely involved in the operation of FSTDs for ELA2 aircraft as defined in Article 1 (2), point (j) of Regulation (EU) No 748/2012;

(g) air traffic controller training organisations (ATCO TOs) and ATCO aero-medical centres subject to Annex III (Part ATCO.OR) to Regulation (EU) 2015/340;

(h) organisations subject to Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373, except the following service providers:

(i) air navigation service providers holding a limited certificate in accordance with point ATM/ANS.OR.A.010 of that Annex;

(ii) flight information service providers declaring their activities in accordance with point ATM/ANS.OR.A.015 of that Annex;

(i) U-space service providers and single common information service providers subject to Implementing Regulation (EU) 2021/664.

2. This Regulation applies to the competent authorities, including the European Union Aviation Safety Agency ('the Agency'), referred to Article 6 of this Regulation and in Article 5 of Commission Delegated Regulation (EU) 2022/1645 ([14]).

3. This Regulation also applies to the competent authority responsible for the issuance, continuation, change, suspension or revocation of aircraft maintenance licences in accordance with Annex III (Part-66) to Regulation (EU) No 1321/2014.

4. This Regulation is without prejudice to information security and cybersecurity requirements laid down in point 1.7 of the Annex to Implementing Regulation (EU) 2015/1998 and in Article 14 of Directive (EU) 2016/1148.

Article 3

Definitions

For the purpose of this Regulation, the following definitions shall apply:

(1) 'information security' means the preservation of confidentiality, integrity, authenticity and availability of network and information systems;

(2) 'information security event' means an identified occurrence of a system, service or network state indicating a possible breach of the information security policy or failure of information security controls, or a previously unknown situation that can be relevant for information security;

(3) 'incident' means any event having an actual adverse effect on the security of network and information systems as defined in Article 4(7) of Directive (EU) 2016/1148;

(4) 'information security risk' means the risk to organisational civil aviation operations, assets, individuals, and other organisations due to the potential of an information security event. Information security risks are associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets;

([14]) Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 (OJ L 248, 26.9.2022, p. 18).

(5) 'threat' means a potential violation of information security which exists when there is an entity, circumstance, action or event that could cause harm;

(6) 'vulnerability' means a flaw or weakness in an asset or a system, procedures, design, implementation, or information security measures that could be exploited and results in a breach or violation of the information security policy.

Article 4

Requirements for organisations and competent authorities

1. The organisations referred to in Article 2(1) shall comply with the requirements of Annex II (Part-IS.I.OR) to this Regulation.

2. The competent authorities referred to in Article 2(2) and (3) shall comply with the requirements of Annex I (Part-IS.AR) to this Regulation.

Article 5

Requirements arising from other Union legislation

1. Where an organisation referred to in Article 2(1) complies with security requirements laid down in accordance with Article 14 of Directive (EU) 2016/1148 that are equivalent to the requirements laid down in this Regulation, compliance with those security requirements shall be considered to constitute compliance with the requirements laid down in this Regulation.

2. Where an organisation referred to in Article 2(1) is an operator or an entity referred to in the national civil aviation security programmes of Member States laid down in accordance with Article 10 of Regulation (EC) No 300/2008 of the European Parliament and of the Council ([15]), the cybersecurity requirements contained in point 1.7 of the Annex to Implementing Regulation (EU) 2015/1998 shall be considered to be equivalent with the requirements laid down in this Regulation, except as regards point IS.I.OR.230 of Annex II to this Regulation that shall be complied with as such.

3. Where the organisation referred to in Article 2(1) is the air navigation service provider of the European Geostationary Navigation Overlay Service (EGNOS) referred to in Regulation (EU) 2021/696, the security requirements contained in Articles 33 to 43 of Title V of that Regulation are considered to be equivalent with the requirements laid down in this Regulation, except as regards point IS.I.OR.230 of Annex II to this Regulation that shall be complied with as such.

4. The Commission, after consulting the Agency and the Cooperation Group referred to in Article 11 of Directive (EU) 2016/1148, may issue guidelines for the assessment of the equivalence of requirements laid down in this Regulation and Directive (EU) 2016/1148.

Article 6

Competent authority

1. Without prejudice to the tasks entrusted to the Security Accreditation Board (SAB) referred to in Article 36 of Regulation (EU) 2021/696, the authority responsible for certifying and overseeing compliance with this Regulation shall be:

(a) with regard to organisations referred to in Article 2(1), point (a), the competent authority designated in accordance with Annex II (Part-145) to Regulation (EU) No 1321/2014;

(b) with regard to organisations referred to in Article 2(1), point (b), the competent authority designated in accordance with Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014;

([15]) Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

(c) with regard to organisations referred to in Article 2(1), point (c), the competent authority designated in accordance with Annex III (Part-ORO) to Regulation (EU) No 965/2012;

(d) with regard to organisations referred to in Article 2(1), points (d) to (f), the competent authority designated in accordance with Annex VII (Part-ORA) to Regulation (EU) No 1178/2011;

(e) with regard to organisations referred to in Article 2(1), point (g), the competent authority designated in accordance with Article 6(2) of Regulation (EU) 2015/340;

(f) with regard to organisations referred to in Article 2(1), point (h), the competent authority designated in accordance with Article 4(1) of Implementing Regulation (EU) 2017/373;

(g) with regard to organisations referred to in Article 2(1), point (i), the competent authority designated in accordance with Article 14(1) or 14(2), as applicable, of Implementing Regulation (EU) 2021/664.

2. Member States may, for the purposes of this Regulation, designate an independent and autonomous entity to fulfil the assigned role and responsibilities of the competent authorities referred to in paragraph 1. In that case, coordination measures shall be established between that entity and the competent authorities, as referred to in paragraph 1, to ensure effective oversight of all the requirements to be met by the organisation.

3. The Agency shall cooperate in full compliance with the applicable rules on secrecy, protection of personal data and protection of classified information with the European Union Agency for the Space Programme (EUSPA), and the SAB referred to in Article 36 of Regulation (EU) 2021/696 in order to ensure effective oversight of the requirements applicable to EGNOS air navigation service provider.

Article 7

Submission of relevant information to NIS competent authorities

Competent authorities under this Regulation shall inform, without undue delay, the single point of contact designated in accordance with Article 8 of Directive (EU) 2016/1148 of any relevant information included in notifications submitted pursuant to point IS.I.OR.230 of Annex II to this Regulation and point IS.D.OR.230 of Annex I to Delegated Regulation (EU) 2022/1645 by operators of essential services identified in accordance with Article 5 of Directive (EU) 2016/1148.

Article 8

Amendment to Regulation (EU) No 1178/2011

Annexes VI (Part-ARA) and VII (Part-ORA) to Regulation (EU) No 1178/2011 are amended in accordance with Annex III to this Regulation.

Article 9

Amendment to Regulation (EU) No 748/2012

Annex I (Part 21) to Regulation (EU) No 748/2012 is amended in accordance with Annex IV to this Regulation.

Article 10

Amendment to Regulation (EU) No 965/2012

Annexes II (Part-ARO) and III (Part-ORO) to Regulation (EU) No 965/2012 are amended in accordance with Annex V to this Regulation.

Article 11

Amendment to Regulation (EU) No 139/2014

Annex II (Part-ADR.AR) to Regulation (EU) No 139/2014 is amended in accordance with Annex VI to this Regulation.

Article 12

Amendment to Regulation (EU) No 1321/2014

Annexes II (Part-145), III (Part-66) and Vc (Part-CAMO) to Regulation (EU) No 1321/2014 are amended in accordance with Annex VII to this Regulation.

Article 13

Amendment to Regulation (EU) 2015/340

Annexes II (Part ATCO.AR) and III (Part ATCO.OR) to Regulation (EU) 2015/340 are amended in accordance with Annex VIII to this Regulation.

Article 14

Amendment to Implementing Regulation (EU) 2017/373

Annexes II (Part-ATM/ANS.AR) and III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 are amended in accordance with Annex IX to this Regulation.

Article 15

Amendment to Implementing Regulation (EU) 2021/664

Implementing Regulation (EU) 2021/664 is amended as follows:

(1) in Article 15(1), point(f) is replaced by the following:

'(f) implement and maintain a security management system in accordance with point ATM/ANS.OR.D.010 in Subpart D of Annex III to Implementing Regulation (EU) 2017/373 and an information security management system in accordance with Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203;';

(2) in Article 18, the following point (l) is added:

'(l) establish, implement and maintain an information security management system in accordance with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203.'.

Article 16

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from 22 February 2026.

However, as regards the case of the EGNOS air navigation service provider subject to Implementing Regulation (EU) 2017/373 it shall apply from 1 January 2026.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27 October 2022.

For the Commission
The President
Ursula VON DER LEYEN

ANNEX I

INFORMATION SECURITY – AUTHORITY REQUIREMENTS

[PART-IS.AR]

IS.AR.100 Scope

IS.AR.200 Information security management system (ISMS)

IS.AR.205 Information security risk assessment

IS.AR.210 Information security risk treatment

IS.AR.215 Information security incidents – detection, response, and recovery

IS.AR.220 Contracting of information security management activities

IS.AR.225 Personnel requirements

IS.AR.230 Record-keeping

IS.AR.235 Continuous improvement

IS.AR.100 Scope

This Part establishes the management requirements to be met by the competent authorities referred to in Article 2(2) of this Regulation.

The requirements to be met by those competent authorities for the performance of their certification, oversight and enforcement activities are contained in the Regulations referred to in Article 2(1) of this Regulation and in Article 2 of Delegated Regulation (EU) 2022/1645.

IS.AR.200 Information security management system (ISMS)

(a) In order to achieve the objectives set out in Article 1, the competent authority shall set up, implement and maintain an information security management system (ISMS) which ensures that the competent authority:

(1) establishes a policy on information security setting out the overall principles of the competent authority with regard to the potential impact of information security risks on aviation safety;

(2) identifies and reviews information security risks in accordance with point IS.AR.205;

(3) defines and implements information security risk treatment measures in accordance with point IS.AR.210;

(4) defines and implements, in accordance with point IS.AR.215, the measures required to detect information security events, identifies those which are considered incidents with a potential impact on aviation safety, and responds to, and recovers from, those information security incidents;

(5) complies with the requirements contained in point IS.AR.220 when contracting any part of the activities described in point IS.AR.200 to other organisations;

(6) complies with the personnel requirements contained in point IS.AR.225;

(7) complies with the record-keeping requirements contained in point IS.AR.230;

(8) monitors compliance of its own organisation with the requirements of this Regulation and provides feedback on findings to the person referred to in point IS.AR.225 (a) to ensure effective implementation of corrective actions;

(9) protects the confidentiality of any information that the competent authority may have related to organisations subject to its oversight and the information received through the organisation's external reporting schemes established in accordance with point IS.I.OR.230 of Annex II (Part-IS.I.OR) to this Regulation and point IS.D.OR.230 of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645;

(10) notifies the Agency of changes that affect the capacity of the competent authority to perform its tasks and discharge its responsibilities as defined in this Regulation;

(11) defines and implements procedures to share, as appropriate and in a practical and timely manner, relevant information to assist other competent authorities and agencies, as well as organisations subject to this Regulation, to conduct effective security risk assessments relating to their activities.

(b) In order to continuously meet the requirements referred to in Article 1, the competent authority shall implement a continuous improvement process in accordance with point IS.AR.235.

(c) The competent authority shall document all key processes, procedures, roles and responsibilities required to comply with point IS.AR.200(a) and establish a process for amending this documentation.

(d) The processes, procedures, roles and responsibilities established by the competent authority in order to comply with point IS.AR.200(a) shall correspond to the nature and complexity of its activities, based on an assessment of the information security risks inherent to those activities, and may be integrated within other existing management systems already implemented by the competent authority.

IS.AR.205 Information security risk assessment

(a) The competent authority shall identify all the elements of its own organisation which could be exposed to information security risks. This shall include:

(1) the competent authority's activities, facilities and resources, and the services the competent authority operates, provides, receives or maintains;

(2) the equipment, systems, data and information that contribute to the functioning of the elements referred to in point (1)

(b) The competent authority shall identify the interfaces that its own organisation has with other organisations, and which could result in the mutual exposure to information security risks.

(c) For the elements and interfaces referred to in points (a) and (b), the competent authority shall identify the information security risks which may have a potential impact on aviation safety.

For each identified risk, the competent authority shall:

(1) assign a risk level according to a predefined classification established by the competent authority;

(2) associate each risk and its level with the corresponding element or interface identified in accordance with points (a) and (b).

The predefined classification referred to in point (1) shall take into account the potential of occurrence of the threat scenario and the severity of its safety consequences. Through this classification, and taking into account whether the competent authority has a structured and repeatable risk management process for operations, the competent authority shall be able to establish whether the risk is acceptable or needs to be treated in accordance with point IS.AR.210.

In order to facilitate the mutual comparability of risks assessments, the assignment of the risk level per point (1) shall take into account relevant information acquired in coordination with the organisations referred to in point (b).

(d) The competent authority shall review and update the risk assessment carried out in accordance with points (a), (b) and (c) in any of the following cases:

(1) there is a change in the elements subject to information security risks;

(2) there is a change in the interfaces between the competent authority's organisation and other organisations, or in the risks communicated by the other organisations;

(3) there is a change in the information or knowledge used for the identification, analysis and classification of risks;

(4) there are lessons learnt from the analysis of information security incidents.

IS.AR.210 Information security risk treatment

(a) The competent authority shall develop measures to address unacceptable risks identified in accordance with point IS.AR.205, shall implement them in a timely manner and shall check their continued effectiveness. Those measures shall enable the competent authority to:

(1) control the circumstances that contribute to the effective occurrence of the threat scenario;

(2) reduce the consequences to aviation safety associated with the materialisation of the threat scenario;

(3) avoid the risks.

Those measures shall not introduce any new potential unacceptable risks to aviation safety.

(b) The person referred to in point IS.AR.225 (a) and other affected personnel of the competent authority shall be informed of the outcome of the risk assessment carried out in accordance with point IS.AR.205, the corresponding threat scenarios and the measures to be implemented.

The competent authority shall also inform organisations with which it has an interface in accordance with point IS.AR.205 (b) of any risk shared between competent authority and the organisation.

IS.AR.215 Information security incidents – detection, response and recovery

(a) Based on the outcome of the risk assessment carried out in accordance with point IS.AR.205 and the outcome of the risk treatment performed in accordance with point IS.AR.210, the competent authority shall implement measures to detect events that indicate the potential materialisation of unacceptable risks and which may have a potential impact on aviation safety. Those detection measures shall enable the competent authority to:

(1) identify deviations from predetermined functional performance baselines;

(2) trigger warnings to activate proper response measures, in case of any deviation.

(b) The competent authority shall implement measures to respond to any event conditions identified in accordance with point (a) that may develop or have developed into an information security incident. Those response measures shall enable the competent authority to:

(1) initiate the reaction of its own organisation to the warnings referred to in point (a)(2) by activating predefined resources and course of actions;

(2) contain the spread of an attack and avoid the full materialisation of a threat scenario;

(3) control the failure mode of the affected elements defined in point IS.AR.205(a).

(c) The competent authority shall implement measures aimed at recovering from information security incidents, including emergency measures, if needed. Those recovery measures shall enable the competent authority to:

(1) remove the condition that caused the incident, or constrain it to a tolerable level;

(2) restore a safe state of the affected elements defined in point IS.AR.205(a) within a recovery time previously defined by its own organisation.

IS.AR.220 Contracting of information security management activities

The competent authority shall ensure that when contracting any part of the activities referred to in point IS.AR.200 to other organisations, the contracted activities comply with the requirements of this Regulation and the contracted organisation works under its oversight. The competent authority shall ensure that the risks associated with the contracted activities are appropriately managed.

IS.AR.225 Personnel requirements

The competent authority shall:

(a) have a person who has the authority to establish and maintain the organisational structures, policies, processes, and procedures necessary to implement this Regulation.

This person shall:

(1) have authority to fully access the resources necessary for the competent authority to perform all the tasks required by this Regulation;

(2) possess the delegation of power required to perform the assigned duties;

(b) have a process in place to ensure that they have sufficient personnel on duty to perform the activities covered by this Annex;

(c) have a process in place to ensure that the personnel referred to in point (b) have the necessary competence to perform their tasks;

(d) have a process in place to ensure that personnel acknowledge the responsibilities associated with the assigned roles and tasks;

(e) ensure that the identity and trustworthiness of the personnel who have access to information systems and data subject to the requirements of this Regulation are appropriately established.

IS.AR.230 Record-keeping

(a) The competent authority shall keep records of its information security management activities

(1) The competent authority shall ensure that the following records are archived and traceable:

(i) contracts for activities referred to in point IS.AR.200(a)(5);

(ii) records of the key processes referred to in point IS.AR.200(d);

(iii) records of the risks identified in the risk assessment referred to in point IS.AR.205 along with the associated risk treatment measures referred to in point IS.AR.210;

(iv) records of information security events which may need to be reassessed to reveal undetected information security incidents or vulnerabilities.

(2) The records referred to in point (1)(i) shall be retained at least until 5 years after the contract has been amended or terminated.

(3) The records referred to in point (1)(ii) and (iii) shall be retained at least for a period of 5 years.

(4) The records referred to in point (1)(iv) shall be retained until those information security events have been reassessed in accordance with a periodicity defined in a procedure established by the competent authority.

(b) The competent authority shall keep records of qualification and experience of its own staff involved in information security management activities

(1) The personnel's qualification and experience records shall be retained for as long as the person works for the competent authority, and for at least 3 years after the person has left the competent authority.

(2) Members of the staff shall, upon their request, be given access to their individual records. In addition, upon their request, the competent authority shall provide them with a copy of their individual records on leaving the competent authority.

(c) The format of the records shall be specified in the competent authority's procedures.

(d) Records shall be stored in a manner that ensures protection from damage, alteration and theft, with information being identified, when required, according to its security classification level. The competent authority shall ensure that the records are stored using means to ensure integrity, authenticity and authorised access.

IS.AR.235 Continuous improvement

(a) The competent authority shall assess, using adequate performance indicators, the effectiveness and maturity of its own ISMS. The assessment shall be performed on a predefined calendar basis defined by the competent authority or following an information security incident.

(b) If deficiencies are found following the assessment carried out in accordance with point (a), the competent authority shall take the necessary improvement measures to ensure that the ISMS continues to comply with the applicable requirements and maintains the information security risks at an acceptable level. In addition, the competent authority shall reassess those elements of the ISMS affected by the adopted measures.

ANNEX II

INFORMATION SECURITY – ORGANISATION REQUIREMENTS

[PART-IS.I.OR]

IS.I.OR.100 Scope

IS.I.OR.200 Information security management system (ISMS)

IS.I.OR.205 Information security risk assessment

IS.I.OR.210 Information security risk treatment

IS.I.OR.215 Information security internal reporting scheme

IS.I.OR.220 Information security incidents – detection, response, and recovery

IS.I.OR.225 Response to findings notified by the competent authority

IS.I.OR.230 Information security external reporting scheme

IS.I.OR.235 Contracting of information security management activities

IS.I.OR.240 Personnel requirements

IS.I.OR.245 Record-keeping

IS.I.OR.250 Information security management manual (ISMM)

IS.I.OR.255 Changes to the information security management system

IS.I.OR.260 Continuous improvement

IS.I.OR.100 Scope

This Part establishes the requirements to be met by the organisations referred to in Article 2(1) of this Regulation.

IS.I.OR.200 Information security management system (ISMS)

(a) In order to achieve the objectives set out in Article 1, the organisation shall set up, implement and maintain an information security management system (ISMS) which ensures that the organisation:

(1) establishes a policy on information security setting out the overall principles of the organisation with regard to the potential impact of information security risks on aviation safety;

(2) identifies and reviews information security risks in accordance with point IS.I.OR.205;

(3) defines and implements information security risk treatment measures in accordance with point IS.I.OR.210;

(4) implements an information security internal reporting scheme in accordance with point IS.I.OR.215;

(5) defines and implements, in accordance with point IS.I.OR.220, the measures required to detect information security events, identifies those events which are considered incidents with a potential impact on aviation safety except as permitted by point IS.I.OR.205(e), and responds to, and recovers from, those information security incidents;

(6) implements the measures that have been notified by the competent authority as an immediate reaction to an information security incident or vulnerability with an impact on aviation safety;

(7) takes appropriate action, in accordance with point IS.I.OR.225, to address findings notified by the competent authority;

(8) implements an external reporting scheme in accordance with point IS.I.OR.230 in order to enable the competent authority to take appropriate actions;

(9) complies with the requirements contained in point IS.I.OR.235 when contracting any part of the activities referred to in point IS.I.OR.200 to other organisations;

(10) complies with the personnel requirements laid down in point IS.I.OR.240;

(11) complies with the record-keeping requirements laid down in point IS.I.OR.245;

(12) monitors compliance of the organisation with the requirements of this Regulation and provides feedback on findings to the accountable manager to ensure effective implementation of corrective actions;

(13) protects, without prejudice to applicable incident reporting requirements, the confidentiality of any information that the organisation may have received from other organisations, according to its level of sensitivity.

(b) In order to continuously meet the requirements referred to in Article 1, the organisation shall implement a continuous improvement process in accordance with point IS.I.OR.260.

(c) The organisation shall document, in accordance with point IS.I.OR.250, all key processes, procedures, roles and responsibilities required to comply with point IS.I.OR.200(a), and shall establish a process for amending that documentation. Changes to those processes, procedures, roles and responsibilities shall be managed in accordance with point IS.I.OR.255.

(d) The processes, procedures, roles and responsibilities established by the organisation in order to comply with point IS.I.OR.200(a) shall correspond to the nature and complexity of its activities, based on an assessment of the information security risks inherent to those activities, and may be integrated within other existing management systems already implemented by the organisation.

(e) Without prejudice to the obligation to comply with the reporting requirements laid down in Regulation (EU) No 376/2014 and the requirements laid down in point IS.I.OR.200 (a)(13), the organisation may be approved by the competent authority not to implement the requirements referred to in points (a) to (d) and the related requirements contained in points IS.I.OR.205 through IS.I.OR.260, if it demonstrates to the satisfaction of that authority that its activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose any information security risks with a potential impact on aviation safety neither to itself nor to other organisations. The approval shall be based on a documented information security risk assessment carried out by the organisation or a third party in accordance with point IS.I.OR.205 and reviewed and approved by its competent authority.

The continued validity of that approval will be reviewed by the competent authority following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.

IS.I.OR.205 Information security risk assessment

(a) The organisation shall identify all its elements which could be exposed to information security risks. That shall include:

(1) the organisation's activities, facilities and resources, as well as the services the organisation operates, provides, receives or maintains;

(2) the equipment, systems, data and information that contribute to the functioning of the elements listed in point (1).

(b) The organisation shall identify the interfaces that it has with other organisations, and which could result in the mutual exposure to information security risks.

(c) With regard to the elements and interfaces referred to in points (a) and (b), the organisation shall identify the information security risks which may have a potential impact on aviation safety. For each identified risk, the organisation shall:

(1) assign a risk level according to a predefined classification established by the organisation;

(2) associate each risk and its level with the corresponding element or interface identified in accordance with points (a) and (b).

The predefined classification referred to in point (1) shall take into account the potential of occurrence of the threat scenario and the severity of its safety consequences. Based on that classification, and taking into account whether the organisation has a structured and repeatable risk management process for operations, the organisation shall be able to establish whether the risk is acceptable or needs to be treated in accordance with point IS.I.OR.210.

In order to facilitate the mutual comparability of risks assessments, the assignment of the risk level pursuant to point (1) shall take into account relevant information acquired in coordination with the organisations referred to in point (b).

(d) The organisation shall review and update the risk assessment carried out in accordance with points (a), (b) and, as applicable, points (c) or (e), in any of the following situations:

(1) there is a change in the elements subject to information security risks;

(2) there is a change in the interfaces between the organisation and other organisations, or in the risks communicated by the other organisations;

(3) there is a change in the information or knowledge used for the identification, analysis and classification of risks;

(4) there are lessons learnt from the analysis of information security incidents.

(e) By derogation from point (c), organisations required to comply with Subpart C of Annex III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 shall replace the analysis of the impact on aviation safety by an analysis of the impact on their services as per the safety support assessment required by point ATM/ANS.OR.C.005. This safety support assessment shall be made available to the air traffic service providers to whom they provide services and those air traffic service providers shall be responsible for evaluating the impact on aviation safety.

IS.I.OR.210 Information security risk treatment

(a) The organisation shall develop measures to address unacceptable risks identified in accordance with point IS.I.OR.205, implement them in a timely manner and check their continued effectiveness. Those measures shall enable the organisation to:

(1) control the circumstances that contribute to the effective occurrence of the threat scenario;

(2) reduce the consequences on aviation safety associated with the materialisation of the threat scenario;

(3) avoid the risks.

Those measures shall not introduce any new potential unacceptable risks to aviation safety.

(b) The person referred to in point IS.I.OR.240 (a) and (b) and other affected personnel of the organisation shall be informed of the outcome of the risk assessment carried out in accordance with point IS.I.OR.205, the corresponding threat scenarios and the measures to be implemented.

The organisation shall also inform organisations with which it has an interface in accordance with point IS.I.OR.205(b) of any risk shared between both organisations.

IS.I.OR.215 Information security internal reporting scheme

(a) The organisation shall establish an internal reporting scheme to enable the collection and evaluation of information security events, including those to be reported pursuant to point IS.I.OR.230.

(b) That scheme and the process referred to in point IS.I.OR.220 shall enable the organisation to:

(1) identify which of the events reported pursuant to point (a) are considered information security incidents or vulnerabilities with a potential impact on aviation safety;

(2) identify the causes of, and contributing factors to, the information security incidents and vulnerabilities identified in accordance with point (1), and address them as part of the information security risk management process in accordance with points IS.I.OR.205 and IS.I.OR.220;

(3) ensure an evaluation of all known, relevant information relating to the information security incidents and vulnerabilities identified in accordance with point (1);

(4) ensure the implementation of a method to distribute internally the information as necessary.

(c) Any contracted organisation which may expose the organisation to information security risks with a potential impact on aviation safety shall be required to report information security events to the organisation. Those reports shall be submitted using the procedures established in the specific contractual arrangements and shall be evaluated in accordance with point (b).

(d) The organisation shall cooperate on investigations with any other organisation that has a significant contribution to the information security of its own activities.

(e) The organisation may integrate that reporting scheme with other reporting schemes it has already implemented.

IS.I.OR.220 Information security incidents – detection, response and recovery

(a) Based on the outcome of the risk assessment carried out in accordance with point IS.I.OR.205 and the outcome of the risk treatment performed in accordance with point IS.I.OR.210, the organisation shall implement measures to detect incidents and vulnerabilities that indicate the potential materialisation of unacceptable risks and which may have a potential impact on aviation safety. Those detection measures shall enable the organisation to:

(1) identify deviations from predetermined functional performance baselines;

(2) trigger warnings to activate proper response measures, in case of any deviation.

(b) The organisation shall implement measures to respond to any event conditions identified in accordance with point (a) that may develop or have developed into an information security incident. Those response measures shall enable the organisation to:

(1) initiate the reaction to the warnings referred to in point (a)(2) by activating predefined resources and course of actions;

(2) contain the spread of an attack and avoid the full materialisation of a threat scenario;

(3) control the failure mode of the affected elements defined in point IS.I.OR.205(a).

(c) The organisation shall implement measures aimed at recovering from information security incidents, including emergency measures, if needed. Those recovery measures shall enable the organisation to:

(1) remove the condition that caused the incident, or constrain it to a tolerable level;

(2) reach a safe state of the affected elements defined in point IS.I.OR.205(a) within a recovery time previously defined by the organisation.

IS.I.OR.225 Response to findings notified by the competent authority

(a) After receipt of the notification of findings submitted by the competent authority, the organisation shall:

(1) identify the root cause or causes of, and contributing factors to, the non-compliance;

(2) define a corrective action plan;

(3) demonstrate the correction of the non-compliance to the satisfaction of the competent authority.

(b) The actions referred to in point (a) shall be carried out within the period agreed with the competent authority.

IS.I.OR.230 Information security external reporting scheme

(a) The organisation shall implement an information security reporting system that complies with the requirements laid down in Regulation (EU) No 376/2014 and its delegated and implementing acts if that Regulation is applicable to the organisation.

(b) Without prejudice to the obligations of Regulation (EU) No 376/2014, the organisation shall ensure that any information security incident or vulnerability, which may represent a significant risk to aviation safety, is reported to their competent authority. Furthermore:

(1) Where such an incident or vulnerability affects an aircraft or associated system or component, the organisation shall also report it to the design approval holder;

(2) Where such an incident or vulnerability affects a system or constituent used by the organisation, the organisation shall report it to the organisation responsible for the design of the system or constituent.

(c) The organisation shall report the conditions referred to in point (b) as follows:

(1) a notification shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, as soon as the condition has been known to the organisation;

(2) a report shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, as soon as possible, but not exceeding 72 hours from the time the condition has been known to the organisation, unless exceptional circumstances prevent this.

The report shall be made in the form defined by the competent authority and shall contain all relevant information about the condition known to the organisation;

(3) a follow-up report shall be submitted to the competent authority and, if applicable, to the design approval holder or to the organisation responsible for the design of the system or constituent, providing details of the actions the organisation has taken or intends to take to recover from the incident and the actions it intends to take to prevent similar information security incidents in the future.

The follow-up report shall be submitted as soon as those actions have been identified, and shall be produced in the form defined by the competent authority.

IS.I.OR.235 Contracting of information security management activities

(a) The organisation shall ensure that when contracting any part of the activities referred to in point IS.I.OR.200 to other organisations, the contracted activities comply with the requirements of this Regulation and the contracted organisation works under its oversight. The organisation shall ensure that the risks associated with the contracted activities are appropriately managed.

(b) The organisation shall ensure that the competent authority can have access upon request to the contracted organisation to determine continued compliance with the applicable requirements laid down in this Regulation.

IS.I.OR.240 Personnel requirements

(a) The accountable manager of the organisation designated in accordance with Regulations (EU) No 1321/2014, (EU) No 965/2012, (EU) No 1178/2011, (EU) 2015/340, Implementing Regulation (EU) 2017/373 or Implementing Regulation (EU) 2021/664 as applicable referred to in Article 2(1) of this Regulation shall have corporate authority to ensure that all activities required by this Regulation can be financed and carried out. That person shall:

(1) ensure that all necessary resources are available to comply with the requirements of this Regulation;

(2) establish and promote the information security policy referred to in point IS.I.OR.200(a)(1);

(3) demonstrate a basic understanding of this Regulation.

(b) The accountable manager shall appoint a person or group of persons to ensure that the organisation complies with the requirements of this Regulation, and shall define the extent of their authority. That person or group of persons shall report directly to the accountable manager, and shall have the appropriate knowledge, background and experience to discharge their responsibilities. It shall be determined in the procedures who deputises for a particular person in the case of lengthy absence of that person.

(c) The accountable manager shall appoint a person or group of persons with the responsibility to manage the compliance monitoring function referred to in point IS.I.OR.200(a)(12).

(d) Where the organisation shares information security organisational structures, policies, processes and procedures with other organisations or with areas of their own organisation which are not part of the approval or declaration, the accountable manager may delegate its activities to a common responsible person.

In such a case, coordination measures shall be established between the accountable manager of the organisation and the common responsible person to ensure adequate integration of the information security management within the organisation.

(e) The accountable manager or the common responsible person referred to in (d) shall have corporate authority to establish and maintain the organisational structures, policies, processes and procedures necessary to implement point IS.I.OR.200.

(f) The organisation shall have a process in place to ensure that they have sufficient personnel on duty to carry out the activities covered by this Annex.

(g) The organisation shall have a process in place to ensure that the personnel referred to in point (f) have the necessary competence to perform their tasks.

(h) The organisation shall have a process in place to ensure that personnel acknowledge the responsibilities associated with the assigned roles and tasks.

(i) The organisation shall ensure that the identity and trustworthiness of the personnel who have access to information systems and data subject to the requirements of this Regulation are appropriately established.

IS.I.OR.245 Record-keeping

(a) *The organisation shall keep records of its information security management activities*

(1) The organisation shall ensure that the following records are archived and traceable:

(i) any approval received and any associated information security risk assessment in accordance with point IS.I.OR.200(e);

(ii) contracts for activities referred to in point IS.I.OR.200(a)(9);

(iii) records of the key processes referred to in point IS.I.OR.200(d);

(iv) records of the risks identified in the risk assessment referred to in point IS.I.OR.205 along with the associated risk treatment measures referred to in point IS.I.OR.210;

(v) records of information security incidents and vulnerabilities reported in accordance with the reporting schemes referred to in points IS.I.OR.215 and IS.I.OR.230;

(vi) records of those information security events which may need to be reassessed to reveal undetected information security incidents or vulnerabilities.

(2) The records referred to in point (1)(i) shall be retained at least until 5 years after the approval has lost its validity.

(3) The records referred to in point (1)(ii) shall be retained at least until 5 years after the contract has been amended or terminated.

(4) The records referred to point (1)(iii), (iv) and (v) shall be retained at least for a period of 5 years.

(5) The records referred to in point (1)(vi) shall be retained until those information security events have been reassessed in accordance with a periodicity defined in a procedure established by the organisation.

(b) *The organisation shall keep records of qualification and experience of its own staff involved in information security management activities*

(1) The personnel's qualification and experience records shall be retained for as long as the person works for the organisation, and for at least 3 years after the person has left the organisation.

(2) Members of the staff shall, upon their request, be given access to their individual records. In addition, upon their request, the organisation shall provide them with a copy of their individual records on leaving the organisation.

(c) The format of the records shall be specified in the organisation's procedures.

(d) Records shall be stored in a manner that ensures protection from damage, alteration and theft, with information being identified, when required, according to its security classification level. The organisation shall ensure that the records are stored using means to ensure integrity, authenticity and authorised access.

IS.I.OR.250 Information security management manual (ISMM)

(a) The organisation shall make available to the competent authority an information security management manual (ISMM) and, where applicable, any referenced associated manuals and procedures, containing:

(1) a statement signed by the accountable manager confirming that the organisation will at all times work in accordance with this Annex and with the ISMM. If the accountable manager is not the chief executive officer (CEO) of the organisation, then the CEO shall countersign the statement;

(2) the title(s), name(s), duties, accountabilities, responsibilities and authorities of the person or persons defined in point IS.I.OR.240(b) and (c);

(3) the title, name, duties, accountabilities, responsibilities and authority of the common responsible person defined in point IS.I.OR.240(d), if applicable;

(4) the information security policy of the organisation as referred to in point IS.I.OR.200(a)(1);

(5) a general description of the number and categories of staff and of the system in place to plan the availability of staff as required by point IS.I.OR.240;

(6) the title(s), name(s), duties, accountabilities, responsibilities and authorities of the key persons responsible for the implementation of point IS.I.OR.200, including the person or persons responsible for the compliance monitoring function referred to in point IS.I.OR.200(a)(12);

(7) an organisation chart showing the associated chains of accountability and responsibility for the persons referred to in points (2) and (6);

(8) the description of the internal reporting scheme referred to in point IS.I.OR.215;

(9) the procedures that specify how the organisation ensures compliance with this Part, and in particular:

(i) the documentation referred to in point IS.I.OR.200(c);

(ii) the procedures that define how the organisation controls any contracted activities as referred to in point IS.I.OR.200(a)(9);

(iii) the ISMM amendment procedure referred to in in point (c);

(10) the details of currently approved alternative means of compliance.

(b) The initial issue of the ISMM shall be approved and a copy shall be retained by the competent authority. The ISMM shall be amended as necessary to remain an up-to-date description of the ISMS of the organisation. A copy of any amendments to the ISMM shall be provided to the competent authority.

(c) Amendments to the ISMM shall be managed in a procedure established by the organisation. Any amendments that are not included within the scope of this procedure and any amendments related to the changes referred to in point IS.I.OR.255(b) shall be approved by the competent authority.

(d) The organisation may integrate the ISMM with other management expositions or manuals it holds, provided there is a clear cross reference that indicates which portions of the management exposition or manual correspond to the different requirements contained in this Annex.

IS.I.OR.255 Changes to the information security management system

(a) Changes to the ISMS may be managed and notified to the competent authority in a procedure developed by the organisation. This procedure shall be approved by the competent authority.

(b) With regard to changes to the ISMS not covered by the procedure referred to in point (a), the organisation shall apply for and obtain an approval issued by the competent authority.

With regard to those changes:

(1) the application shall be submitted before any such change takes place, in order to enable the competent authority to determine continued compliance with this Regulation and to amend, if necessary, the organisation certificate and related terms of approval attached to it;

(2) the organisation shall make available to the competent authority any information it requests to evaluate the change;

(3) the change shall be implemented only upon receipt of a formal approval by the competent authority;

(4) the organisation shall operate under the conditions prescribed by the competent authority during the implementation of such changes.

IS.I.OR.260 Continuous improvement

(a) The organisation shall assess, using adequate performance indicators, the effectiveness and maturity of the ISMS. That assessment shall be carried out on a calendar basis predefined by the organisation or following an information security incident.

(b) If deficiencies are found following the assessment carried out in accordance with point (a), the organisation shall take the necessary improvement measures to ensure that the ISMS continues to comply with the applicable requirements and maintains the information security risks at an acceptable level. In addition, the organisation shall reassess those elements of the ISMS affected by the adopted measures.

ANNEX III

Annexes VI (Part-ARA) and VII (Part-ORA) to Regulation (EU) No 1178/2011 are amended as follows:

(1) Annex VI (Part-ARA) is amended as follows:

(a) in point 'ARA.GEN.125, the following point (c) is added:

'(c) The competent authority of the Member State shall provide the Agency as soon as possible with safety-significant information stemming from the information security reports it has received pursuant to point IS.I.OR.230 of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203.';

(b) the following point ARA.GEN.135A is inserted after point ARA.GEN.135:

'**ARA.GEN.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety**

(a) The competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety that are reported by organisations. This shall be done in coordination with any other relevant authorities responsible for information security or cybersecurity within the Member State to increase the coordination and compatibility of reporting schemes.

(b) The Agency shall implement a system to appropriately analyse any relevant safety-significant information received in accordance with point ARA.GEN.125(c), and without undue delay provide the Member States and the Commission with any information, including recommendations or corrective actions to be taken, necessary for them to react in a timely manner to an information security incident or vulnerability with a potential impact on aviation safety involving products, parts, non-installed equipment, persons or organisations subject to Regulation (EU) 2018/1139 and its delegated and implementing acts.

(c) Upon receiving the information referred to in points (a) and (b), the competent authority shall take adequate measures to address the potential impact on aviation safety of the information security incident or vulnerability.

(d) Measures taken in accordance with point (c) shall immediately be notified to all persons or organisations that shall comply with them under Regulation (EU) 2018/1139 and its delegated and implementing acts. The competent authority of the Member State shall also notify those measures to the Agency and, when combined action is required, the competent authorities of the other Member States concerned.';

(c) in point ARA.GEN.200, the following point (e) is added:

'(e) In addition to the requirements contained in point (a), the management system established and maintained by the competent authority shall comply with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(d) point ARA.GEN.205 is amended as follows:

(i) the heading is replaced by the following:

'**ARA.GEN.205 Allocation of tasks**';

(ii) the following point (c) is added:

'(c) With regard to the certification and oversight of the organisation's compliance with point ORA.GEN.200A, the competent authority may allocate tasks to qualified entities in accordance with point (a), or to any relevant authority responsible for information security or cybersecurity within the Member State. When allocating tasks, the competent authority shall ensure that:

(1) all aspects related to aviation safety are coordinated and taken into account by the qualified entity or relevant authority;

(2) the results of the certification and oversight activities performed by the qualified entity or relevant authority are integrated in the overall certification and oversight files of the organisation;

(3) its own information security management system established in accordance with point ARA.GEN.200(e) covers all the certification and continuing oversight tasks performed on its behalf.';

(e) in point ARA.GEN.300, the following point (g) is added:

'(g) With regard to the certification and oversight of the organisation's compliance with point ORA.GEN.200A, in addition to complying with points (a) to (f), the competent authority shall review any approval granted under point IS.I.OR.200(e) of this Regulation or point IS.D.OR.200(e) of Delegated Regulation (EU) 2022/1645 following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.'

(f) the following point ARA.GEN.330A is inserted after point ARA.GEN.330:

'**ARA.GEN.330A Changes to the information security management system**

(a) With regard to changes managed and notified to the competent authority in accordance with the procedure set out in point IS.I.OR.255(a) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point ARA.GEN.300. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point ARA.GEN.350.

(b) With regard to other changes requiring an application for approval in accordance with point IS.I.OR.255(b) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.';

(2) Annex VII (Part-ORA) is amended as follows:

The following point ORA.GEN.200A is inserted after point ORA.GEN.200:

'**ORA.GEN.200A Information security management system**

In addition to the management system referred to in point ORA.GEN.200, the organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.'.

ANNEX IV

Annex I (Part 21) to Regulation (EU) No 748/2012 is amended as follows:

(1) the Table of Contents is amended as follows:

(a) the following heading is inserted after heading 21.B.20:

'21.B.20A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety';

(b) the heading of point 21.B.30 is replaced by the following:

'21.B.30 Allocation of tasks';

(c) the following heading is inserted after heading 21.B.240:

'21.B.240A Changes to the information security management system';

(d) the following heading is inserted after heading 21.B.435:

'21.B.435A Changes to the information security management system';

(2) in point 21.B.15, the following point (c) is added:

'(c) The competent authority of the Member State shall provide the Agency as soon as possible with safety-significant information stemming from the information security reports it has received pursuant to point IS.D.OR.230 of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645.';

(3) the following point 21.B.20A is inserted after point 21.B.20:

'21.B.20A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety

(a) The competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety that are reported by organisations. This shall be done in coordination with any other relevant authorities responsible for information security or cybersecurity within the Member State to increase the coordination and compatibility of reporting schemes.

(b) The Agency shall implement a system to appropriately analyse any relevant safety-significant information received in accordance with point 21.B.15(c), and without undue delay provide the Member States and the Commission with any information, including recommendations or corrective actions to be taken, necessary for them to react in a timely manner to an information security incident or vulnerability with a potential impact on aviation safety involving products, parts, non-installed equipment, persons or organisations subject to Regulation (EU) 2018/1139 and its delegated and implementing acts.

(c) Upon receiving the information referred to in points (a) and (b), the competent authority shall take adequate measures to address the potential impact on aviation safety of the information security incident or vulnerability.

(d) Measures taken in accordance with point (c) shall immediately be notified to all persons or organisations that shall comply with them under Regulation (EU) 2018/1139 and its delegated and implementing acts. The competent authority of the Member State shall also notify those measures to the Agency and, when combined action is required, the competent authorities of the other Member States concerned.';

(4) in point 21.B.25, the following point (e) is added:

'(e) In addition to the requirements contained in point (a), the management system established and maintained by the competent authority shall comply with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(5) point 21.B.30 is amended as follows:

(a) the heading is replaced by the following:

'21.B.30 Allocation of tasks';

(b) the following point (c) is added:

'(c) For the certification and oversight of the organisation's compliance with points 21.A.139A and 21.A.239A, the competent authority may allocate tasks to qualified entities in accordance with point (a), or to any relevant authority responsible for information security or cybersecurity within the Member State. When allocating tasks, the competent authority shall ensure that:

(1) all aspects related to aviation safety are coordinated and taken into account by the qualified entity or relevant authority;

(2) the results of the certification and oversight activities performed by the qualified entity or relevant authority are integrated in the overall certification and oversight files of the organisation;

(3) its own information security management system established in accordance with point 21.B.25(e) covers all the certification and continuing oversight tasks performed on its behalf.';

(6) in point 21.B.221, the following point (g) is added:

'(g) With regard to the certification and oversight of the organisation's compliance with point 21.A.139A, in addition to complying with points (a) to (f), the competent authority shall review any approval granted under point IS.I.OR.200(e) of this Regulation or point IS.D.OR.200(e) of Delegated Regulation (EU) 2022/1645 following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.'

(7) the following point 21.B.240A is inserted after point 21.B.240:

'**21.B.240A Changes to the information security management system**

(a) For changes managed and notified to the competent authority in accordance with the procedure set out in point IS.D.OR.255(a) of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point 21.B.221. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point 21.B.225.

(b) For other changes requiring an application for approval in accordance with point IS.D.OR.255(b) of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.';

(8) in point 21.B.431, the following point (d) is added:

'(d) For the certification and oversight of the organisation's compliance with point 21.A.239A, in addition to complying with points (a) to (c), the competent authority shall comply with the following principles:

(1) the competent authority shall review the interfaces and associated risks identified in accordance with point IS.D.OR.205(b) of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645 by each organisation subject to its oversight;

(2) if discrepancies are found in the mutual interfaces and associated risks identified by different organisations, the competent authority shall review them with the affected organisations and, if necessary, raise appropriate findings to ensure the implementation of corrective actions;

(3) where the documentation reviewed under point (2) reveals the existence of significant risks associated with interfaces with organisations subject to the oversight of a different competent authority within the same Member State, this information shall be communicated to the corresponding competent authority.';

(9) the following point 21.B.435A is inserted after point 21.B.435:

'**21.B.435A Changes to the information security management system**

(a) For changes managed and notified to the competent authority in accordance with the procedure set out in point IS.D.OR.255(a) of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point 21.B.431. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point 21.B.433.

(b) For other changes requiring an application for approval in accordance with point IS.D.OR.255(b) of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.'.

ANNEX V

Annexes II (Part-ARO) and III (Part-ORO) to Regulation (EU) No 965/2012 are amended as follows:

(1) Annex II (Part-ARO) is amended as follows:

(a) in point ARO.GEN.125, the following point (c) is added:

'(c) The competent authority of the Member State shall provide the Agency as soon as possible with safety-significant information stemming from the information security reports it has received pursuant to point IS.I.OR.230 of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203.';

(b) the following point ARO.GEN.135A is inserted after point ARO.GEN.135:

'**ARO.GEN.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety**

(a) The competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety that are reported by organisations. This shall be done in coordination with any other relevant authorities responsible for information security or cybersecurity within the Member State to increase the coordination and compatibility of reporting schemes.

(b) The Agency shall implement a system to appropriately analyse any relevant safety-significant information received in accordance with point ARO.GEN.125(c), and without undue delay provide the Member States and the Commission with any information, including recommendations or corrective actions to be taken, necessary for them to react in a timely manner to an information security incident or vulnerability with a potential impact on aviation safety involving products, parts, non-installed equipment, persons or organisations subject to Regulation (EU) 2018/1139 and its delegated and implementing acts.

(c) Upon receiving the information referred to in points (a) and (b), the competent authority shall take adequate measures to address the potential impact on aviation safety of the information security incident or vulnerability.

(d) Measures taken in accordance with point (c) shall immediately be notified to all persons or organisations that shall comply with them under Regulation (EU) 2018/1139 and its delegated and implementing acts. The competent authority of the Member State shall also notify those measures to the Agency and, when combined action is required, the competent authorities of the other Member States concerned.';

(c) in point ARO.GEN.200, the following point (e) is added:

'(e) In addition to the requirements contained in point (a), the management system established and maintained by the competent authority shall comply with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(d) point ARO.GEN.205 is amended as follows:

(i) the heading is replaced by the following:

'**ARO.GEN.205 Allocation of tasks**';

(ii) the following point (c) is added:

'(c) For the certification and oversight of the organisation's compliance with point ORO.GEN.200A, the competent authority may allocate tasks to qualified entities in accordance with point (a), or to any relevant authority responsible for information security or cybersecurity within the Member State. When allocating tasks, the competent authority shall ensure that:

(1) all aspects related to aviation safety are coordinated and taken into account by the qualified entity or relevant authority;

(2) the results of the certification and oversight activities performed by the qualified entity or relevant authority are integrated in the overall certification and oversight files of the organisation;

(3) its own information security management system established in accordance with point ARO.GEN.200(e) covers all the certification and continuing oversight tasks performed on its behalf.';

(e) in point ARO.GEN.300, the following point (g) is added:

'(g) With regard to the certification and oversight of the organisation's compliance with point ORO.GEN.200A, in addition to complying with points (a) to (f), the competent authority shall review any approval granted under point IS.I.OR.200(e) of this Regulation or point IS.D.OR.200(e) of Delegated Regulation (EU) 2022/1645 following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.'

(f) the following point ARO.GEN.330A is inserted after point ARO.GEN.330:

'**ARO.GEN.330A Changes to the information security management system**

(a) For changes managed and notified to the competent authority in accordance with the procedure set out in point IS.I.OR.255(a) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point ARO.GEN.300. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point ARO.GEN.350.

(b) For other changes requiring an application for approval in accordance with point IS.I.OR.255(b) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.';

(2) Annex III (Part-ORO) is amended as follows:

the following point ORO.GEN.200A is inserted after point ORO.GEN.200:

'**ORO.GEN.200A Information security management system**

In addition to the management system referred to in point ORO.GEN.200, the operator shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.'.

ANNEX VI

Annex II (Part-ADR.AR) to Regulation (EU) No 139/2014 is amended as follows:

(1) in point ADR.AR.A.025, the following point (c) is added:

'(c) The competent authority of the Member State shall provide the Agency as soon as possible with safety-significant information stemming from the information security reports it has received pursuant to point IS.D.OR.230 of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645.';

(2) the following point ADR.AR.A.030A is inserted after point ADR.AR.A.030:

'**ADR.AR.A.030A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety**

(a) The competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety that are reported by organisations. This shall be done in coordination with any other relevant authorities responsible for information security or cybersecurity within the Member State to increase the coordination and compatibility of reporting schemes.

(b) The Agency shall implement a system to appropriately analyse any relevant safety-significant information received in accordance with point ADR.AR.A.025(c), and without undue delay provide the Member States and the Commission with any information, including recommendations or corrective actions to be taken, necessary for them to react in a timely manner to an information security incident or vulnerability with a potential impact on aviation safety involving products, parts, non-installed equipment, persons or organisations subject to Regulation (EU) 2018/1139 and its delegated and implementing acts.

(c) Upon receiving the information referred to in points (a) and (b), the competent authority shall take adequate measures to address the potential impact on aviation safety of the information security incident or vulnerability.

(d) Measures taken in accordance with point (c) shall immediately be notified to all persons or organisations that shall comply with them under Regulation (EU) 2018/1139 and its delegated and implementing acts. The competent authority of the Member State shall also notify those measures to the Agency and, when combined action is required, the competent authorities of the other Member States concerned.';

(3) in point ADR.AR.B.005, the following point (d) is added:

'(d) In addition to the requirements contained in point (a), the management system established and maintained by the competent authority shall comply with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(4) point ADR.AR.B.010 is amended as follows:

(i) the heading is replaced by the following:

'**ADR.AR.B.010 Allocation of tasks**';

(ii) the following point (c) is added:

'(c) With regard to the certification and oversight of the organisation's compliance with point ADR.OR.D.005A, the competent authority may allocate tasks to qualified entities in accordance with point (a), or to any relevant authority responsible for information security or cybersecurity within the Member State. When allocating tasks, the competent authority shall ensure that:

(1) all aspects related to aviation safety are coordinated and taken into account by the qualified entity or relevant authority;

(2) the results of the certification and oversight activities performed by the qualified entity or relevant authority are integrated in the overall certification and oversight files of the organisation;

(3) its own information security management system established in accordance with point ADR.AR.B.005(e) covers all the certification and continuing oversight tasks performed on its behalf.';

(5) in point ADR.AR.C.005, the following point (f) is added:

'(f) With regard to the certification and oversight of the organisation's compliance with point ADR.OR.D.005A, in addition to complying with points (a) to (e), the competent authority shall review any approval granted under point IS.I.OR.200(e) of this Regulation or point IS.D.OR.200(e) of Delegated Regulation (EU) 2022/1645 following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.'

(6) the following point ADR.AR.C.040A is inserted after point ADR.AR.C.040:

'**ADR.AR.C.040A Changes to the information security management system**

(a) With regard to changes managed and notified to the competent authority in accordance with the procedure set out in point IS.D.OR.255(a) of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point ADR.AR.C.005. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point ADR.AR.C.055.

(b) With regard to other changes requiring an application for approval in accordance with point IS.D.OR.255(b) of the Annex (Part-IS.D.OR) to Delegated Regulation (EU) 2022/1645:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.'.

ANNEX VII

Annexes II (Part-145), III (Part-66) and Vc (Part-CAMO) to Regulation (EU) No 1321/2014 are amended as follows:

(1) Annex II (Part-145) is amended as follows:

(a) the Table of Contents is amended as follows:

(i) the following heading is inserted after heading 145.A.200:

'145.A.200A Information security management system';

(ii) the following heading is inserted after heading 145.B.135:

'145.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety';

(iii) the heading of point 145.B.205 is replaced by the following:

'145.B.205 Allocation of tasks';

(iv) the following heading is inserted after heading 145.B.330:

'145.B.330A Changes to the information security management system';

(b) the following point 145.A.200A is inserted after point 145.A.200:

'145.A.200A **Information security management system**

In addition to the management system referred to in point 145.A.200, the maintenance organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(c) in point 145.B.125, the following point (c) is added:

'(c) The competent authority of the Member State shall provide the Agency as soon as possible with safety-significant information stemming from the information security reports it has received pursuant to point IS.I.OR.230 of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203';

(d) the following point 145.B.135A is inserted after point 145.B.135:

'145.B.135A **Immediate reaction to an information security incident or vulnerability with an impact on aviation safety**

(a) The competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety that are reported by organisations. This shall be done in coordination with any other relevant authorities responsible for information security or cybersecurity within the Member State to increase the coordination and compatibility of reporting schemes.

(b) The Agency shall implement a system to appropriately analyse any relevant safety-significant information received in accordance with point 145.B.125(c), and without undue delay provide the Member States and the Commission with any information, including recommendations or corrective actions to be taken, necessary for them to react in a timely manner to an information security incident or vulnerability with a potential impact on aviation safety involving products, parts, non-installed equipment, persons or organisations subject to Regulation (EU) 2018/1139 and its delegated and implementing acts.

(c) Upon receiving the information referred to in points (a) and (b), the competent authority shall take adequate measures to address the potential impact on aviation safety of the information security incident or vulnerability.

(d) Measures taken in accordance with point (c) shall immediately be notified to all persons or organisations that shall comply with them under Regulation (EU) 2018/1139 and its delegated and implementing acts. The competent authority of the Member State shall also notify those measures to the Agency and, when combined action is required, the competent authorities of the other Member States concerned.';

(e) in point 145.B.200, the following point (e) is added:

'(e) In addition to the requirements contained in point (a), the management system established and maintained by the competent authority shall comply with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(f) point 145.B.205 is amended as follows:

(i) the heading is replaced by the following:

'145.B.205 **Allocation of tasks**';

(ii) the following point (c) is added:

'(c) For the certification and oversight of the organisation's compliance with point 145.A.200A, the competent authority may allocate tasks to qualified entities in accordance with point (a), or to any relevant authority responsible for information security or cybersecurity within the Member State. When allocating tasks, the competent authority shall ensure that:

(1) all aspects related to aviation safety are coordinated and taken into account by the qualified entity or relevant authority;

(2) the results of the certification and oversight activities performed by the qualified entity or relevant authority are integrated in the overall certification and oversight files of the organisation;

(3) its own information security management system established in accordance with point 145.B.200(e) covers all the certification and continuing oversight tasks performed on its behalf.';

(g) in point 145.B.300, the following point (g) is added:

'(g) With regard to the certification and oversight of the organisation's compliance with point 145.A.200A, in addition to complying with points (a) to (f), the competent authority shall review any approval granted under point IS.I.OR.200(e) of this Regulation or point IS.D.OR.200(e) of Delegated Regulation (EU) 2022/1645 following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.';

(h) the following point 145.B.330A is inserted after point 145.B.330:

'145.B.330A **Changes to the information security management system**

(a) For changes managed and notified to the competent authority in accordance with the procedure set out in point IS.I.OR.255(a) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point 145.B.300. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point 145.B.350.

(b) For other changes requiring an application for approval in accordance with point IS.I.OR.255(b) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.';

(2) Annex III (Part-66) is amended as follows:

(a) in the Table of Contents, the following heading is inserted after heading 66.B.10:

'66.B.15 Information security management system';

(b) the following point 66.B.15 is inserted after point 66.B.10:

'66.B.15 **Information security management system**

The competent authority shall establish, implement and maintain an information security management system in accordance with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(3) Annex Vc (Part-CAMO) is amended as follows:

(a) the Table of Contents is amended as follows:

(i) the following heading is inserted after heading CAMO.A.200:

'CAMO.A.200A Information security management system';

(ii) the following heading is inserted after heading CAMO.B.135:

'CAMO.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety';

(iii) the heading of point CAMO.B.205 is replaced by the following:

'CAMO.B.205 Allocation of tasks';

(iv) the following heading is inserted after heading CAMO.B.330:

'CAMO.B.330A Changes to the information security management system';

(b) the following point CAMO.A.200A is inserted after point CAMO.A.200:

'CAMO.A.200A **Information security management system**

In addition to the management system referred to in point CAMO.A.200, the organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(c) in point CAMO.B.125, the following point (c) is added:

'(c) The competent authority of the Member State shall provide the Agency as soon as possible with safety-significant information stemming from the information security reports it has received pursuant to point IS.I.OR.230 of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203.';

(d) the following point CAMO.B.135A is inserted after CAMO.B.135:

'CAMO.B.135A **Immediate reaction to an information security incident or vulnerability with an impact on aviation safety**

(a) The competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety that are reported by organisations. This shall be done in coordination with any other relevant authorities responsible for information security or cybersecurity within the Member State to increase the coordination and compatibility of reporting schemes.

(b) The Agency shall implement a system to appropriately analyse any relevant safety-significant information received in accordance with point CAMO.B.125(c), and without undue delay provide the Member States and the Commission with any information, including recommendations or corrective actions to be taken, necessary for them to react in a timely manner to an information security incident or vulnerability with a potential impact on aviation safety involving products, parts, non-installed equipment, persons or organisations subject to Regulation (EU) 2018/1139 and its delegated and implementing acts.

(c) Upon receiving the information referred to in points (a) and (b), the competent authority shall take adequate measures to address the potential impact on aviation safety of the information security incident or vulnerability.

(d) Measures taken in accordance with point (c) shall immediately be notified to all persons or organisations that shall comply with them under Regulation (EU) 2018/1139 and its delegated and implementing acts. The competent authority of the Member State shall also notify those measures to the Agency and, when combined action is required, the competent authorities of the other Member States concerned.';

(e) in point CAMO.B.200, the following point (e) is added:

'(e) In addition to the requirements contained in point (a), the management system established and maintained by the competent authority shall comply with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(f) point CAMO.B.205 is amended as follows:

(i) the heading is replaced by the following:

'CAMO.B.205 **Allocation of tasks**';

(ii) the following point (c) is added:

'(c) With regard to the certification and oversight of the organisation's compliance with point CAMO.A.200A, the competent authority may allocate tasks to qualified entities in accordance with point (a), or to any relevant authority responsible for information security or cybersecurity within the Member State. When allocating tasks, the competent authority shall ensure that:

(1) all aspects related to aviation safety are coordinated and taken into account by the qualified entity or relevant authority;

(2) the results of the certification and oversight activities performed by the qualified entity or relevant authority are integrated in the overall certification and oversight files of the organisation;

(3) its own information security management system established in accordance with point CAMO.B.200(e) covers all the certification and continuing oversight tasks performed on its behalf.';

(g) in point CAMO.B.300, the following point (g) is added:

'(g) With regard to the certification and oversight of the organisation's compliance with point CAMO.A.200A, in addition to complying with points (a) to (f), the competent authority shall review any approval granted under point IS.I.OR.200(e) of this Regulation or point IS.D.OR.200(e) of Delegated Regulation (EU) 2022/1645 following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.'

(h) the following point CAMO.B.330A is inserted after point CAMO.B.330:

'CAMO.B.330A **Changes to the information security management system**

(a) For changes managed and notified to the competent authority in accordance with the procedure set out in point IS.I.OR.255(a) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point CAMO.B.300. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point CAMO.B.350.

(b) For other changes requiring an application for approval in accordance with point IS.I.OR.255(b) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.'.

ANNEX VIII

Annexes II (Part ATCO.AR) and III (Part ATCO.OR) to Regulation (EU) 2015/340 are amended as follows:

(1) Annex II (Part ATCO.AR) is amended as follows:

(a) in point ATCO.AR.A.020, the following point (c) is added:

'(c) The competent authority of the Member State shall provide the Agency as soon as possible with safety-significant information stemming from the information security reports it has received pursuant to point IS.I.OR.230 of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203.';

(b) the following point ATCO.AR.A.025A is inserted after point ATCO.AR.A.025:

'**ATCO.AR.A.025A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety**

(a) The competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety that are reported by organisations. This shall be done in coordination with any other relevant authorities responsible for information security or cybersecurity within the Member State to increase the coordination and compatibility of reporting schemes.

(b) The Agency shall implement a system to appropriately analyse any relevant safety-significant information received in accordance with point ATCO.AR.A.020, and without undue delay provide the Member States and the Commission with any information, including recommendations or corrective actions to be taken, necessary for them to react in a timely manner to an information security incident or vulnerability with a potential impact on aviation safety involving products, parts, non-installed equipment, persons or organisations subject to Regulation (EU) 2018/1139 and its delegated and implementing acts.

(c) Upon receiving the information referred to in points (a) and (b), the competent authority shall take adequate measures to address the potential impact on aviation safety of the information security incident or vulnerability.

(d) Measures taken in accordance with point (c) shall immediately be notified to all persons or organisations that shall comply with them under Regulation (EU) 2018/1139 and its delegated and implementing acts. The competent authority of the Member State shall also notify those measures to the Agency and, when combined action is required, the competent authorities of the other Member States concerned.';

(c) in point ATCO.AR.B.001, the following point (e) is added:

'(e) In addition to the requirements contained in point (a), the management system established and maintained by the competent authority shall comply with Annex I (Part-IS.AR) to Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(d) point ATCO.AR.B.005 is amended as follows:

(i) the heading is replaced by the following:

'**ATCO.AR.B.005 Allocation of tasks**';

(ii) the following point (c) is added:

'(c) With regard to the certification and oversight of the organisation's compliance with point ATCO.OR.C.001A, the competent authority may allocate tasks to qualified entities in accordance with point (a), or to any relevant authority responsible for information security or cybersecurity within the Member State. When allocating tasks, the competent authority shall ensure that:

(1) all aspects related to aviation safety are coordinated and taken into account by the qualified entity or relevant authority;

(2) the results of the certification and oversight activities performed by the qualified entity or relevant authority are integrated in the overall certification and oversight files of the organisation;

(3) its own information security management system established in accordance with point ATCO.AR.B.001(e) covers all the certification and continuing oversight tasks performed on its behalf.';

(e) in point ATCO.AR.C.001, the following point (f) is added:

'(f) With regard to the certification and oversight of the organisation's compliance with point ATCO.OR.C.001A, in addition to complying with points (a) to (e), the competent authority shall review any approval granted under point IS.I.OR.200(e) of this Regulation or point IS.D.OR.200(e) of Delegated Regulation (EU) 2022/1645 following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.'

(f) the following point ATCO.AR.E.010A is inserted after point ATCO.AR.E.010:

'**ATCO.AR.E.010A Changes to the information security management system**

(a) With regard to changes managed and notified to the competent authority in accordance with the procedure set out in point IS.I.OR.255(a) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point ATCO.AR.C.001. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point ATCO.AR.C.010.

(b) With regard to other changes requiring an application for approval in accordance with point IS.I.OR.255(b) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.';

(2) Annex III (Part ATCO.OR) is amended as follows:

The following point ATCO.OR.C.001A is inserted after point ATCO.OR.C.001:

'**ATCO.OR.C.001A Information security management system**

In addition to the management system referred to in point ATCO.OR.C.001, the training organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.'.

ANNEX IX

Annexes II (Part-ATM/ANS.AR) and III (Part-ATM/ANS.OR) to Implementing Regulation (EU) 2017/373 are amended as follows:

(1) Annex II (Part-ATM/ANS.AR) is amended as follows:

(a) in point ATM/ANS.AR.A.020, the following point (c) is added:

'(c) The competent authority of the Member State shall provide the Agency as soon as possible with safety-significant information stemming from the information security reports it has received pursuant to point IS.I.OR.230 of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203.';

(b) the following point ATM/ANS.AR.A.025A is inserted after point ATM/ANS.AR.A.025:

'**ATM/ANS.AR.A.025A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety**

(a) The competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security incidents and vulnerabilities with a potential impact on aviation safety that are reported by organisations. This shall be done in coordination with any other relevant authorities responsible for information security or cybersecurity within the Member State to increase the coordination and compatibility of reporting schemes.

(b) The Agency shall implement a system to appropriately analyse any relevant safety-significant information received in accordance with point ATM/ANS.AR.A.020(c), and without undue delay provide the Member States and the Commission with any information, including recommendations or corrective actions to be taken, necessary for them to react in a timely manner to an information security incident or vulnerability with a potential impact on aviation safety involving products, parts, non-installed equipment, persons or organisations subject to Regulation (EU) 2018/1139 and its delegated and implementing acts.

(c) Upon receiving the information referred to in points (a) and (b), the competent authority shall take adequate measures to address the potential impact on aviation safety of the information security incident or vulnerability.

(d) Measures taken in accordance with point (c) shall immediately be notified to all persons or organisations that shall comply with them under Regulation (EU) 2018/1139 and its delegated and implementing acts. The competent authority of the Member State shall also notify those measures to the Agency and, when combined action is required, the competent authorities of the other Member States concerned.';

(c) in point ATM/ANS.AR.B.001, the following point (e) is added:

'(e) In addition to the requirements contained in point (a), the management system established and maintained by the competent authority shall comply with Annex I (Part-IS.AR) of Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(d) point ATM/ANS.AR.B.005 is amended as follows:

(i) the heading is replaced by the following:

'**ATM/ANS.AR.B.005 Allocation of tasks**';

(ii) The following point (c) is added:

'(c) With regard to the certification and oversight of the organisation's compliance with point ATM/ANS.OR.B.005A, the competent authority may allocate tasks to qualified entities in accordance with point (a), or to any relevant authority responsible for information security or cybersecurity within the Member State. When allocating tasks, the competent authority shall ensure that:

(1) all aspects related to aviation safety are coordinated and taken into account by the qualified entity or relevant authority;

(2) the results of the certification and oversight activities performed by the qualified entity or relevant authority are integrated in the overall certification and oversight files of the organisation;

(3) its own information security management system established in accordance with point ATM/ANS.AR.B.001(e) covers all the certification and continuing oversight tasks performed on its behalf.';

(e) in point ATM/ANS.AR.C.010, the following point (d) is added:

'(d) With regard to the certification and oversight of the organisation's compliance with point ATM/ANS.OR.B.005A, in addition to complying with points (a) to (c), the competent authority shall review any approval granted under point IS.I.OR.200(e) of this Regulation or point IS.D.OR.200(e) of Delegated Regulation (EU) 2022/1645 following the applicable oversight audit cycle and whenever changes are implemented in the scope of work of the organisation.'

(f) the following point ATM/ANS.AR.C.025A is inserted after point ATM/ANS.AR.C.025:

'**ATM/ANS.AR.C.025A Changes to the information security management system**

(a) For changes managed and notified to the competent authority in accordance with the procedure set out in point IS.I.OR.255(a) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles laid down in point ATM/ANS.AR.C.010. If any non-compliance is found, the competent authority shall notify the organisation thereof, request further changes and act in accordance with point ATM/ANS.AR.C.050.

(b) With regard to other changes requiring an application for approval in accordance with point IS.I.OR.255(b) of Annex II (Part-IS.I.OR) to Implementing Regulation (EU) 2023/203:

(1) upon receiving the application for the change, the competent authority shall check the organisation's compliance with the applicable requirements before issuing the approval;

(2) the competent authority shall establish the conditions under which the organisation may operate during the implementation of the change;

(3) if it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.';

(2) Annex III (Part-ATM/ANS.OR) is amended as follows:

(a) the following point ATM/ANS.OR.B.005A is inserted after point ATM/ANS.OR.B.005:

'**ATM/ANS.OR.B.005A Information security management system**

In addition to the management system referred to in point ATM/ANS.OR.B.005, the service provider shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 2023/203 in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(b) point ATM/ANS.OR.D.010 is replaced by the following:

'**ATM/ANS.OR.D.010 Security management**

(a) Air navigation services and air traffic flow management providers and the Network Manager shall, as an integral part of their management system as required in point ATM/ANS.OR.B.005, establish a security management system to ensure:

(1) the security of their facilities and personnel so as to prevent unlawful interference with the provision of services;

(2) the security of operational data they receive, or produce, or otherwise employ, so that access to it is restricted only to those authorised.

(b) The security management system shall define:

(1) the process and procedures relating to security risk assessment and mitigation, security monitoring and improvement, security reviews and lesson dissemination;

(2) the means designed to identify, monitor and detect security breaches and to alert personnel with appropriate security warnings;

(3) the means to control the effects of security breaches and to identify recovery action and mitigation procedures to prevent re-occurrence.

(c) Air navigation services and air traffic flow management providers and the Network Manager shall ensure the security clearance of their personnel, if appropriate, and coordinate with the relevant civil and military authorities to ensure the security of their facilities, personnel and data.

(d) The aspects related to information security shall be managed in accordance with point ATM/ANS.OR.B.005A.'.