EUROPEAN
COMMISSION

Brussels, XXX
[…](2021) XXX draft

ANNEX I TO EASA OPINION 03 -2021

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

amending Commission Regulations (EU) No 748/2012, No 1321/2014, No 965/2012, No 1178/2011, 2015/340, 2017/373, No 139/2014 and 2021/664 as regards the introduction of 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, No 965/2012, No 1178/2011, 2015/340, 2017/373 and 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, No 1321/2014, No 965/2012, No 1178/2011, 2015/340, 2017/373, No 139/2014 and 2021/664

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

amending Commission Regulations (EU) No 748/2012, No 1321/2014, No 965/2012, No 1178/2011, 2015/340, 2017/373, No 139/2014 and 2021/664 as regards the introduction of 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, No 965/2012, No 1178/2011, 2015/340, 2017/373 and 2021/664, and for competent authorities covered by Commission Regulations (EU) No 748/2012, No 1321/2014, No 965/2012, No 1178/2011, 2015/340, 2017/373, No 139/2014 and 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), 27(1), 31(1), 43(1), 53(1) and 62(15)(c) thereof,

Whereas:

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

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

(3) Furthermore, in accordance with the essential requirements set out in Annex V to Regulation (EU) 2018/1139, aircraft operators shall implement and maintain a management system to manage safety risks.

(4) Furthermore, in accordance with the essential requirements set out in Annex VIII 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 shall implement and maintain a management system to manage safety risks.

(5) Finally, in accordance with Article 62(15)(c) of Regulation (EU) 2018/1139, the Commission shall adopt implementing acts laying down the provisions concerning the rules and procedures for the administration and management systems of the Agency and national competent authorities relating to the exercise of the certification, oversight and enforcement tasks.

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

(6) The management systems implemented by the Agency, national competent authorities and organisations to manage safety risks need to take into account not only those risks stemming for random events, but also those where existing flaws may be exploited by individuals with a malicious intent.

(7) This type of risks is 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.

(8) The risks associated with these information systems are not limited to possible attacks to the cyberspace, but encompass threats which are both digital and analogue.

(9) A significant number of organisations already use international standards, such as ISO 27001, which deal with the management of information security risks.

(10) As a consequence, it is appropriate to introduce requirements for the management of information security risks, without limiting them to cybersecurity risks.

(11) It is essential that these requirements cover all aviation domains and their interfaces since aviation is a highly interconnected system of systems. As a consequence, they shall apply to all the organisations and competent authorities that are already required to have a management system in accordance with the existing aviation safety regulations.

(12) The measures provided for in this Regulation need to contribute to the creation of a seamless and consistent regulatory framework where the interfaces between security and safety are appropriately covered, and where special attention is paid at avoiding gaps, loopholes and duplications with other information security and cybersecurity requirements such as those contained in Commission Implementing Regulation (EU) 2015/1998 ([2]) and in the national requirements stemming from Directive (EU) 2016/1148 (NIS Directive) ([3]).

(13) The measures related to information security and cybersecurity stemming from the NIS Directive, Commission Implementing Regulation (EU) 2015/1998 and this Regulation should be coordinated at national levels to avoid gaps and duplications of obligations.

(14) It is therefore appropriate that, where organisations covered by this Regulation are subject to cybersecurity or information security requirements arising from other EU or national legislation, the competent authority defined according to this Regulation should have the possibility to replace compliance with the requirements of this Regulation by compliance with elements contained in other EU or national legislation, provided that such requirements are at least equivalent in effect to the obligations laid down in this Regulation. In such a case, the competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

(15) In addition, in the particular case of airport operators, air carriers and entities as defined in the national civil aviation security programmes of Member States, it is appropriate that the competent authority responsible for the certification and oversight of the organisation's compliance with this Regulation should have the possibility to replace compliance with the requirements contained in this Regulation, except those related to

([2]) 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).

([3]) 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).

the information security external reporting schemes, by compliance with elements of the cybersecurity requirements contained in the Annex to Commission Implementing Regulation (EU) 2015/1998. In such a case, the competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

(16) Furthermore, it is also appropriate that even if the competent authority decides not to use the options described in the previous two recitals, the affected organisations should still have the possibility to use compliance methods developed under the cybersecurity or information security requirements of those EU or national legislations as a means to comply with the requirements of this Regulation, In such a case, the organisation shall demonstrate to their competent authority that with those compliance methods the organisation fully meets the requirements and objectives of this Regulation.

(17) The measures provided for in this Regulation need to ensure a consistent implementation across all aviation domains, while creating a minimal impact on the existing rules already applicable to those domains.

(18) The measures provided for in this Regulation need to be proportional to the risks incurred by the different organisations.

(19) The measures provided for in this Regulation need to follow a performance- and risk-based approach.

(20) The measures provided for in this Regulation need to ensure that organisations and authorities can integrate any new management system requirements with other existing management systems they may have.

(21) A sufficient transition period should be provided for organisations and authorities to ensure their compliance with the new rules and procedures introduced by this Regulation.

(22) The measures provided for in this Regulation are based on Opinion No 03/2021, issued by the European Union Aviation Safety Agency in accordance with Article 75(2)(b) and (c) and Article 76(1) of Regulation (EU) 2018/1139.

(23) The measures provided for in this Regulation are in accordance with the opinion of the committee established by Article 127 of Regulation (EU) 2018/1139,

HAS ADOPTED THIS REGULATION:

Article 1

Annex I (Part 21) to Commission Regulation (EU) No 748/2012 ([4]) is amended as follows:

(1) in the ‘Contents’, the following new points are added:

- ‘21.B.20A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety’
- ‘21.B.240A Changes to the information security management system’
- ‘21.B.435A Changes to the information security management system’;

([4]) 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).

(2) in the ‘Contents’, the title of point ‘21.B.30 Allocation of tasks to qualified entities’ is amended as follows:

‘21.B.30 Allocation of tasks’;

(3) in ‘Section B’, a new point (c) is added to point ‘21.B.15 Information to the Agency’ as follows:

‘(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.OR.230 of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX.’;

(4) in ‘Section B’, a new point 21.B.20A is added as follows:

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

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, 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 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 European 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 (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 (c) shall immediately be notified to all persons or organisations that need to 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.’;

(5) in ‘Section B’, a new point (e) is added to point ‘21.B.25 Management system’ as follows:

‘(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) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.’;

(6) In ‘Section B’, in point ‘21.B.30 Allocation of tasks to qualified entities’:

(i) the title is replaced as follows:

‘21.B.30 Allocation of tasks’;

(ii) a new point (c) is added as follows:

‘(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 (e) of point 21.B.25 covers all the certification and continuing oversight tasks performed on its behalf.’;

(7) In ‘Section B’, a new point (g) is added to point ‘21.B.221 Oversight principles’ as follows:

‘(g) For the certification and oversight of the organisation’s compliance with point 21.A.139A, in addition to complying with points (a) through (f), 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.OR.205(b) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (g)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.’;

(8) in ‘Section B’, a new point 21.B.240A is added as follows:

‘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 described in point IS.OR.255(a) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles

set forth in point 21.B.221. If any non-compliance is found, the competent authority shall notify the organisation, 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.OR.255(b) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX:

(1) upon receiving the application for the change, the competent authority shall verify 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) when it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.';

(9) in 'Section B', a new point (d) is added to point '21.B.431 Oversight principles' as follows:

'(d) For the certification and oversight of the organisation's compliance with point 21.A.239A, in addition to complying with points (a) through (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.OR.205(b) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (d)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.'

(10) in 'Section B', a new point 21.B.435A is added as follows:

'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 described in point IS.OR.255(a) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles set forth in point 21.B.431. If any non-compliance is found, the competent authority shall notify the organisation, 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.OR.255(b) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX:

(1) upon receiving the application for the change, the competent authority shall verify 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) when it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.'.

Article 2

Annex II (Part-145) to Commission Regulation (EU) No 1321/2014 ([5]) is amended as follows:

(1) in the 'CONTENTS', the following new points are added:

- '145.A.200A Information security management system'
- '145.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety'
- '145.B.330A Changes to the information security management system';

(2) in the 'CONTENTS', the title of point '145.B.205 Allocation of tasks to qualified entities' is replaced as follows:

'145.B.205 Allocation of tasks';

(3) in 'Section A', a new point 145.A.200A is added as follows:

'145.A.200A Information security management system

In addition to the management system required by point 145.A.200, the maintenance organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(4) in 'Section B', a new point (c) is added to point '145.B.125 Information to the Agency' as follows:

'(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.OR.230 of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX.';

(5) in 'Section B', a new point 145.B.135A is added as follows:

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

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, 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 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 European Commission

([5]) 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 ((OJ L 362, 17.12.2014, p. 1).

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 (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 (c) shall immediately be notified to all persons or organisations that need to 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.';

(6) in 'Section B', a new point (e) is added to point '145.B.200 Management System' as follows:

'(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) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(7) in 'Section B', in point '145.B.205 Allocation of tasks to qualified entities':

(i) the title is replaced as follows:

'145.B.205 Allocation of tasks';

(ii) a new point (c) is added as follows:

'(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 (e) of point 145.B.200 covers all the certification and continuing oversight tasks performed on its behalf.';

(8) in 'Section B', a new point (g) is added to point '145.B.300 Oversight principles' as follows:

‘(g) For the certification and oversight of the organisation’s compliance with point 145.A.200A, in addition to complying with points (a) through (f), 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.OR.205(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (g)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.’;

(9) in ‘Section B’, a new point 145.B.330A is added as follows:

‘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 described in point IS.OR.255(a) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles set forth in point 145.B.300. If any non-compliance is found, the competent authority shall notify the organisation, 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.OR.255(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX:

(1) upon receiving the application for the change, the competent authority shall verify 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) when it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.’.

Article 3

Annex III (Part-66) to Commission Regulation (EU) No 1321/2014 is amended as follows:

(1) in the ‘Contents’, the following new point is added:

‘66.B.15 Information security management system’

(2) In ‘Section B’, a new point 66.B.15 is added as follows:

‘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) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.’.

Article 4

Annex Vc (Part-CAMO) to Commission Regulation (EU) No 1321/2014 is amended as follows:

(1) in the 'Contents', the following new points are added:

- 'CAMO.A.200A Information security management system'
- 'CAMO.B.135A Immediate reaction to an information security incident or vulnerability with an impact on aviation safety'
- 'CAMO.B.330A Changes to the information security management system';

(2) in the 'Contents', the title of point 'CAMO.B.205 Allocation of tasks to qualified entities' is replaced as follows:

'CAMO.B.205 Allocation of tasks';

(3) in 'Section A', a new point CAMO.A.200A is added as follows:

'CAMO.A.200A Information security management system

In addition to the management system required by point CAMO.A.200, the organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(4) in 'Section B', a new point (c) is added to point 'CAMO.B.125 Information to the Agency' as follows:

'(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.OR.230 of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX.'

(5) in 'Section B', a new point CAMO.B.135A is added as follows:

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

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, 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 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 European 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 (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 (c) shall immediately be notified to all persons or organisations that need to 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.';

(6) in 'Section B', a new point (e) is added to point 'CAMO.B.200 Management System' as follows:

'(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) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(7) in 'Section B', in point 'CAMO.B.205 Allocation of tasks to qualified entities':

(i) the title is replaced as follows:

'CAMO.B.205 Allocation of tasks'

(ii) a new point (c) is added as follows:

'(c) For 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 (e) of point CAMO.B.200 covers all the certification and continuing oversight tasks performed on its behalf.';

(8) in 'Section B', a new point (g) is added to point CAMO.B.300 Oversight principles' as follows:

(g) For the certification and oversight of the organisation's compliance with point CAMO.A.200A, in addition to complying with points (a) through (f), 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.OR.205(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (g)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.';

(9) in 'Section B', a new point CAMO.B.330A is added as follows:

'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 described in point IS.OR.255(a) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles set forth in point CAMO.B.300. If any non-compliance is found, the competent authority shall notify the organisation, 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.OR.255(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX:

(1) upon receiving the application for the change, the competent authority shall verify 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) when it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.'.

Article 5

Annex II (Part-ARO) to Commission Regulation (EU) No 965/2012 ([6]) is amended as follows:

(1) a new point (c) is added to point 'ARO.GEN.125 Information to the Agency' as follows:

'(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.OR.230 of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX.';

(2) a new point ARO.GEN.135A is added as follows:

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

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, 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 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 European 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 (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 (c) shall immediately be notified to all persons or organisations that need to 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) a new point (e) is added to point 'ARO.GEN.200 Management System' as follows:

'(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) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

([6]) 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).

(4) in point ‘ARO.GEN.205 Allocation of tasks to qualified entities’:

(i) the title is replaced as follows:

‘ARO.GEN.205 Allocation of tasks’;

(ii) a new point (c) is added as follows:

‘(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 (e) of point ARO.GEN.200 covers all the certification and continuing oversight tasks performed on its behalf.’;

(5) a new point (g) is added to point ‘ARO.GEN.300 Oversight’ as follows:

‘(g) For the certification and oversight of the organisation’s compliance with point ORO.GEN.200A, in addition to complying with points (a) through (f), 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.OR.205(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (g)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.’;

(6) a new point ARO.GEN.330A is added as follows:

‘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 described in point IS.OR.255(a) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the

principles set forth in point ARO.GEN.300. If any non-compliance is found, the competent authority shall notify the organisation, 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.OR.255(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX:

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

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

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

Article 6

A new point ORO.GEN.200A is added to Annex III (Part-ORO) to Commission Regulation (EU) No 965/2012:

‘ORO.GEN.200A Information security management system

In addition to the management system required by point ORO.GEN.200, the operator shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.’.

Article 7

Annex VI (Part-ARA) to Commission Regulation (EU) No 1178/2011 ([7]) is amended as follows:

(1) a new point (c) is added to point 'ARA.GEN.125 Information to the Agency' as follows:

'(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.OR.230 of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX.';

(2) a new point ARA.GEN.135A is added as follows:

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

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, 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 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 European 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 (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 (c) shall immediately be notified to all persons or organisations that need to 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) a new point (e) is added to point 'ARA.GEN.200 Management System' as follows:

'(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

([7]) 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).

(Part-IS.AR) to Implementing Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(4) in point 'ARA.GEN.205 Allocation of tasks to qualified entities':

(i) the title is replaced as follows:

'ARA.GEN.205 Allocation of tasks';

(ii) a new point (c) is added as follows:

'(c) For 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 (e) of point ARA.GEN.200 covers all the certification and continuing oversight tasks performed on its behalf.';

(5) a new point (g) is added to point 'ARA.GEN.300 Oversight' as follows:

'(g) For the certification and oversight of the organisation's compliance with point ORA.GEN.200A, in addition to complying with points (a) through (f), 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.OR.205(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (g)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.';

(6) a new point ARA.GEN.330A is added as follows:

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

(a) For changes managed and notified to the competent authority in accordance with the procedure described in point IS.OR.255(a) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles set forth in point ARA.GEN.300. If any non-compliance is found, the competent authority shall notify the organisation, request further changes and act in accordance with point ARA.GEN.350.

(b) For other changes requiring an application for approval in accordance with point IS.OR.255(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX:

(1) upon receiving the application for the change, the competent authority shall verify 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) when it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.'.

Article 8

A new point ORA.GEN.200A is added to Annex VII (Part-ORA) to Commission Regulation (EU) No 1178/2011 as follows:

‘ORA.GEN.200A Information security management system

In addition to the management system required by point ORA.GEN.200, the organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.’.

Article 9

Annex II (Part ATCO.AR) to Commission Regulation (EU) 2015/340 ([8]) is amended as follows:

(1) a new point (c) is added to point 'ATCO.AR.A.020 Information to the Agency' as follows:

'(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.OR.230 of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX.';

(2) a new point ATCO.AR.A.025A is added as follows:

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

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, 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 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 European 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 (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 (c) shall immediately be notified to all persons or organisations that need to 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) a new point (e) is added to point 'ATCO.AR.B.001 Management System' as follows:

'(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) 202X/XXXX in order to ensure the

([8]) 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).

proper management of information security risks which may have an impact on aviation safety.';

(4) in point 'ATCO.AR.B.005 Allocation of tasks to qualified entities':

(i) the title is replaced as follows:

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

(ii) a new point (c) is added as follows:

'(c) For 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 (e) of point ATCO.AR.B.001 covers all the certification and continuing oversight tasks performed on its behalf.';

(5) a new point (f) is added to point 'ATCO.AR.C.001 Oversight' as follows:

'(f) For the certification and oversight of the organisation's compliance with point ATCO.OR.C.001A, in addition to complying with points (a) through (e), 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.OR.205(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (f)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.';

(6) A new point ATCO.AR.E.010A is added as follows:

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

(a) For changes managed and notified to the competent authority in accordance with the procedure described in point IS.OR.255(a) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles set forth in point ATCO.AR.C.001. If any non-compliance is found, the competent authority shall notify the organisation, request further changes and act in accordance with point ATCO.AR.C.010.

(b) For other changes requiring an application for approval in accordance with point IS.OR.255(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX:

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

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

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

Article 10

A new point ATCO.OR.C.001A is added to Annex III (Part ATCO.OR) to Commission Regulation (EU) 2015/340 as follows:

‘ATCO.OR.C.001A Information security management system

In addition to the management system required by point ATCO.OR.C.001, the training organisation shall establish, implement and maintain an information security management system in accordance with Implementing Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.’.

Article 11

Annex II (Part-ATM/ANS.AR) to Commission Regulation (EU) 2017/373 ([9]) is amended as follows:

(1) a new point (c) is added to point 'ATM/ANS.AR.A.020 Information to the Agency' as follows:

'(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.OR.230 of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX.';

(2) a new point ATM/ANS.AR.A.025A is added as follows:

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

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, 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 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 European 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 (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 (c) shall immediately be notified to all persons or organisations that need to 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.';

([9]) 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).

(3) a new point (e) is added to point 'ATM/ANS.AR.B.001 Management System' as follows:

'(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) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(4) in point 'ATM/ANS.AR.B.005 Allocation of tasks to qualified entities':

(i) the title is replaced as follows:

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

(ii) a new point (c) is added as follows:

'(c) For 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 (e) of point ATM/ANS.AR.B.001 covers all the certification and continuing oversight tasks performed on its behalf.';

(5) a new point (d) is added to point 'ATM/ANS.AR.C.010 Oversight' as follows:

'(d) For the certification and oversight of the organisation's compliance with point ATM/ANS.OR.B.005A, in addition to complying with points (a) through (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.OR.205(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (d)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.';

(6) a new point ATM/ANS.AR.C.025A is added as follows:

‘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 described in point IS.OR.255(a) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles set forth in point ATM/ANS.AR.C.010. If any non-compliance is found, the competent authority shall notify the organisation, request further changes and act in accordance with point ATM/ANS.AR.C.050.

(b) For other changes requiring an application for approval in accordance with point IS.OR.255(b) of Annex II (Part-IS.OR) to Implementing Regulation (EU) 202X/XXXX:

(a) upon receiving the application for the change, the competent authority shall verify the organisation’s compliance with the applicable requirements before issuing the approval;

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

(c) when it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.’.

Article 12

Annex III (Part-ATM/ANS.OR) to Commission Regulation (EU) 2017/373 is amended as follows:

(1) a new point ATM/ANS.OR.B.005A is added as follows:

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

In addition to the management system required by 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) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(2) point 'ATM/ANS.OR.D.010 Security Management' 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.'

Article 13

Annex II (Part-ADR.AR) to Commission Regulation (EU) No 139/2014 ([10]) is amended as follows:

(1) a new point (c) is added to point 'ADR.AR.A.025 Information to the Agency' as follows:

'(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.OR.230 of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX.';

(2) a new point ADR.AR.A.030A is added as follows:

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

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, 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 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 European 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 (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 (c) shall immediately be notified to all persons or organisations that need to 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) a new point (d) is added to point 'ADR.AR.B.005 Management System' as follows:

'(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

([10]) 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).

(Part-IS.AR) to Implementing Regulation (EU) 202X/XXXX in order to ensure the proper management of information security risks which may have an impact on aviation safety.';

(4) in point 'ADR.AR.B.010 Allocation of tasks to qualified entities':

(i) the title is replaced as follows:

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

(ii) a new point (c) is added as follows:

'(c) For 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 (e) of point ADR.AR.B.005 covers all the certification and continuing oversight tasks performed on its behalf.';

(5) a new point (f) is added to point 'ADR.AR.C.005 Oversight' as follows:

'(f) For the certification and oversight of the organisation's compliance with point ADR.OR.D.005A, in addition to complying with points (a) through (e), 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.OR.205(b) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX by each organisation under 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) When the documentation reviewed under point (f)(2) shows the existence of significant risks associated with interfaces with organisations under the oversight of a different competent authority within the same Member State, this information shall be shared with the corresponding competent authority.';

(6) a new point ADR.AR.C.040A is added as follows:

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

(a) For changes managed and notified to the competent authority in accordance with the procedure described in point IS.OR.255(a) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX, the competent authority shall include the review of such changes in its continuing oversight in accordance with the principles set forth in point ADR.AR.C.005. If any non-compliance is found, the competent authority shall notify the organisation, request further changes and act in accordance with point ADR.AR.C.055.

(b) For other changes requiring an application for approval in accordance with point IS.OR.255(b) of Annex I (Part-IS.OR) to Delegated Regulation (EU) 202X/XXXX:

(1) upon receiving the application for the change, the competent authority shall verify 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) when it is satisfied that the organisation complies with the applicable requirements, the competent authority shall approve the change.'.

Article 14

Commission Regulation (EU) No 2021/664 ([11]) is amended as follows:

(1) point(f) of paragraph (1) of Article 15 is replaced as follows:

'(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.OR) to Implementing Regulation (EU) 202X/XXXX;';

(2) a new paragraph (l) is added to Article 18 as follows:

'(l) establish, implement and maintain an information security management system in accordance with Annex I (Part-IS.AR) to Implementing Regulation (EU) 202X/XXXX.'

Article 15

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 [*OP please insert date:* ***1 year*** *after the date of entry into force*].

Organisations may correct any findings of non-compliance related to points 145.A.200A, CAMO.A.200A, ORO.GEN.200A, ORA.GEN.200A, ATCO.OR.C.001A and ATM/ANS.OR.B.005A until ***[****OP please insert date:* ***2 years*** *after the date of entry into force****]*** or until the date established by the competent authority for the correction of the finding, whichever comes later.

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

Done at Brussels,

For the Commission
The President
Ursula VON DER LEYEN

([11]) Commission Implementing Regulation (EU) No 2021/664 of 22 April 2021 on a regulatory framework for the U-space (OJ L 139, 23.4.2021, p. 161).