European Union Aviation Safety Agency

Opinion No 03/2021

Management of information security risks

RELATED NPA/CRD: 2019-07 — RMT.0720

EXECUTIVE SUMMARY

The objective of this Opinion is to efficiently contribute to the protection of the aviation system from information security risks, and to make it more resilient to information security events and incidents. To achieve this objective, this Opinion proposes the introduction of provisions for the identification and management of information security risks which could affect information and communication technology systems and data used for civil aviation purposes, detecting information security events, identifying those which are considered information security incidents, and responding to, and recovering from, those information security incidents to a level commensurate with their impact on aviation safety.

These provisions shall apply to competent authorities and organisations in all aviation domains (i.e. production and design organisations, air operators, maintenance organisations, continuing airworthiness management organisations (CAMOs), training organisations, aero-medical centres, operators of flight simulation training devices (FSTDs), air traffic management/air navigation services (ATM/ANS) providers, U-space service providers and single common information service providers, aerodrome operators and apron management service providers), shall include high-level, performance-based requirements, and shall be supported by acceptable means of compliance (AMC), guidance material (GM), and industry standards.

This Opinion proposes a new Implementing Regulation and a new Delegated Regulation (depending on the specific aviation domains covered) regarding information security management systems for organisations and competent authorities.

In addition, this Opinion proposes amendments to Commission Regulations (EU) No 748/2012, No 1321/2014, 2017/373, 2015/340, No 139/2014, No 1178/2011, No 965/2012 and 2021/664, in order to introduce requirements to comply with the proposed new Implementing and Delegated Regulations described above, and to add the elements necessary for the competent authorities to perform their certification and oversight activities.

NOTE: For the purpose of this Opinion, '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.

Domain:	Impact of security on safety		
Affected rules:	Commission Regulations (EU) No 748/2012, No 1321/2014, 2017/373, 2015/340, No 139/2014, No 1178/2011, No 965/2012 and 2021/664		
Affected stakeholders:	DOA holders and POA holders; AOC holders (CAT); maintenance organisations; CAMOs; training organisations; aero-medical centres; operators of flight simulation training devices (FSTDs); ATM/ANS providers; U-space service providers and single common information service providers; aerodrome operators; apron management service providers; Member States		
Driver:	Safety	Rulemaking group:	No (instead, the European Strategic Coordination Platform (ESCP) for Cybersecurity in Aviation was consulted)
Impact assessment:	Light	Rulemaking Procedure:	Standard

16.1.2019	27.5.2019	11.6.2021	2022/Q3	2022/Q3

Table of contents

1. About this Opinion

1.1. How this Opinion was developed

The European Union Aviation Safety Agency (EASA) developed this Opinion in line with Regulation (EU) 2018/1139[1] ('Basic Regulation') and the Rulemaking Procedure[2].

This rulemaking activity is included in the European Plan for Aviation Safety (EPAS) for 2021–2025 under rulemaking task (RMT).0720 and has been performed in consultation with the European Strategic Coordination Platform (ESCP) for Cybersecurity in Aviation[3]. The scope and timescales of the task were defined in the related Term of Reference[4].

The related NPA 2019-07 'Management of information security risks'[5] was published on 27 May 2019, with all interested parties being consulted during a 4-month period, from 27 May to 27 September 2019. 757 comments were received from interested parties, including industry, national aviation authorities (NAAs), and social partners.

EASA has addressed and responded to the comments received on the NPA. It reviewed the comments received with the support of the ESCP through meetings and further consultation conducted per email. The comments received and EASA's responses to them are presented in Comment-Response Document (CRD) 2019-07 that is expected to be published one month after the publication of this Opinion.

Due to the complexity of the matter and the extremely wide range of EU institutions/agencies/organisations, competent authorities, stakeholders, and international regulatory partners affected, this RMT has been developed in close coordination, consultation and discussion with the ESCP.

The ESCP includes:

— an Executive Committee (ESCP-EC) at the higher level; and

— a Technical Advisory Committee (ESCP-TAC) at the technical level, with different work streams, to discuss various matters (ESCP governance matters, EU information security strategy, regulatory actions, consistency of risk assessment processes, etc.).

---

1 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 (OJ L 212, 22.8.2018, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1535612134845&uri=CELEX:32018R1139).

2 EASA is bound to follow a structured rulemaking process as required by Article 115(1) of Regulation (EU) 2018/1139. Such a process has been adopted by the EASA Management Board (MB) and is referred to as the 'Rulemaking Procedure'. See MB Decision No 18-2015 of 15 December 2015 replacing Decision 01/2012 concerning the procedure to be applied by EASA for the issuing of opinions, certification specifications and guidance material (http://www.easa.europa.eu/the-agency/management-board/decisions/easa-mb-decision-18-2015-rulemaking-procedure).

3 https://www.easa.europa.eu/sites/default/files/dfu/ESCP%20Charter%20V2.0%20February%202019.pdf

4 https://www.easa.europa.eu/document-library/terms-of-reference-and-group-compositions/tor-rmt0720

5 https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-07

The ESCP has been meeting since July 2017, and is composed of representatives from the following organisations:

— **Members**

- European Commission (DG-MOVE, DG-CNECT, DG-GROW and DG-HOME);
- other EU agencies and organisations:
  - European External Action Service (EEAS);
  - European Union Agency for Law Enforcement Cooperation (Europol);
  - European Union Aviation Safety Agency (EASA);
  - European Union Agency for Network Information Security (ENISA);
  - Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU);
  - EUROCONTROL;
  - SESAR Deployment Manager;
  - SESAR Joint Undertaking;
  - European Defence Agency (EDA);
- Six European States (Finland, France, Poland, Romania, Sweden, and the UK);
- European Civil Aviation Conference (ECAC);
- Aviation industry associations:
  - AeroSpace and Defence Industries Association Europe (ASD);
  - Airlines for Europe (A4E);
  - Airports Council International — Europe (ACI);
  - Civil Air Navigation Services Organisation — Europe (CANSO);
  - European Cockpit Association (ECA);
  - European Helicopter Association (EHA);
  - European Independent Maintenance Group (EIMG);
  - European Regional Airlines Association (ERAA);
  - European Transport Workers' Federation (ETF);
  - General Aviation Manufacturers (GAMA);
  - International Air Transport Association — Europe (IATA).

— **Observers**

- International Civil Aviation Organization (ICAO);
- Federal Aviation Administration (FAA), Transport Canada Civil Aviation (TCCA) and Israel CAA;

- North Atlantic Treaty Organization (NATO);
- Aerospace Industries Association of America (AIA);
- Aerospace Industries Association of Canada (AIAC);
- Aviation Information Sharing and Analysis Center (A-ISAC);
- European Business Aviation Association (EBAA).

EASA developed the *final* text of this Opinion and the draft regulations based on the input of the public consultation and on the input of the consultation with the ESCP. The draft regulations are published on the Official Publication of EASA[6].

The major milestones of this RMT are presented on the cover page.

1.2. The next steps

This Opinion proposes two new regulations (one implementing act and one delegated act) introducing requirements for the management of information security risks, events, and incidents for competent authorities and for organisations in all aviation domains.

It also proposes amendments (through one implementing act and one delegated act) to the already existing Commission Regulations (EU) No 748/2012, No 1321/2014, 2017/373, 2015/340, No 139/2014, No 1178/2011, No 965/2012 and 2021/664. The purpose of these amendments is to introduce requirements to comply with the information security management requirements introduced in the new Implementing and Delegated Regulations described above, and to add the elements necessary for the competent authorities to perform their certification and oversight activities.

This Opinion is submitted to the European Commission, which will use it as a technical basis to prepare EU regulations.

The Decision that contains the related AMC and GM will be published by EASA when the related regulations are adopted by the European Commission.

6 http://easa.europa.eu/document-library/opinions

2. In summary — why and what

2.1. Why we need to amend the rules — issue/rationale

The current European aviation safety regulatory framework contains a series of requirements which are aimed at reducing the likelihood of an accident happening. These requirements include, among other things:

— comprehensive requirements for the certification of aircraft, engines, propellers, parts and non-installed equipment;

— comprehensive requirements for the continuing airworthiness of aircraft, including duplicated inspections for critical areas/systems;

— comprehensive requirements for the approval of organisations, complemented by periodic audits performed by the competent authority;

— independent quality systems or organisational reviews within all approved organisations;

— periodic airworthiness reviews performed on every aircraft to ensure the continued validity of the certificate of airworthiness;

— an aircraft continuing airworthiness monitoring programme implemented by the competent authority of the State of Registry of the aircraft; and

— requirements for the coordination between the competent authorities of the different Member States.

This combination of requirements results in that even if an error, mistake and/or deficiency happens, it should not create a hazardous situation that could result in an accident or serious incident. Consequently, an accident or serious incident would only happen in the remote random event of several deficiencies taking place simultaneously and, by chance, aligning themselves.

The concern, however, is that for information security purposes, not enough focus may have been put in properly addressing the situation where existing flaws in different areas are aligned on purpose and exploited by individuals with a malicious intent, no longer being a random event. Such a risk is constantly increasing in the civil aviation environment as the current aeronautical information systems are becoming more and more interconnected, with several major elements interacting with the aircraft as well as with each other, such as:

— original equipment manufacturers (OEMs) and their supply chain;

— air operators (e.g. airlines), including their aircrew and ground personnel;

— providers of groundhandling services;

— aerodrome operators;

— maintenance organisations;

— passengers;

— ATM/ANS providers;

— communication service providers (CSPs) and satellite service providers (SSPs);

— third parties that have access to non-protected aviation transmissions.

This is where information security risks, events and incidents come into play, and addressing them is the objective of this RMT.

NOTE: For the purpose of this Opinion, '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.

These information security risks have the potential to generate events that can have direct consequences on the safety of flight. Therefore, the interactions between information security management systems (ISMS) and safety management systems (SMS) (or safety support assessments performed in accordance with point ATM/ANS.OR.C.005) are relevant for addressing information security risks, events and incidents. Nevertheless, certain adaptations are necessary in relation to the security aspects, especially regarding the concept of 'vulnerabilities', the 'notion of intent' and the existence of sensitive classified information.

These adaptations need to consider the fact that information security breaches are based on various motives, such as the intent and desire to access information, to damage systems, to disrupt operations, or to threaten human lives. In other words, there are persons or entities that are intentionally looking for weaknesses in various systems, including aviation systems, that can be exploited with the aim of creating harm. These potential weaknesses are not always known to the operators or other entities in civil aviation. Furthermore, in some cases, the exploitation of weaknesses, although, when assessed individually, they could appear harmless, may be intentionally combined to create a certain damage, potentially having catastrophic effects. In other cases, weaknesses could be inadvertently exploited by malware spreading beyond their intended target, especially when good information security practices are neglected, and thus have a negative effect on civil aviation. Weaknesses can also be very different in nature: some relate to hardware, some to software, some to processes, and some even to the physical security of a given system.

When weaknesses can be exploited, they are called vulnerabilities. Timely reaction to known vulnerabilities adapted to the situation and system concerned (especially for safety-relevant systems) is essential to prevent potential attackers, who may have very different profiles and who can adapt quickly to the environment, from exploiting them or combining them with other vulnerabilities.

In addition, the adaptations also need to consider those cases where attacks are performed for other purposes, not necessarily targeting aviation, but which may cause collateral damage on aviation safety.

In doing so, it is of paramount importance that aviation safety-related systems are adequately protected from information security risks while continuing to ensure aviation safety.

It is important to put this in a context where currently there are other EU legislative acts, outside the scope of the Basic Regulation, that contain provisions related to information security for civil aviation.

These are the following:

— Directive (EU) 2016/1148[7] of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (also called 'the NIS Directive'),

— Regulation (EU) 2015/1998[8] of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security.

However, these EU legislative acts are not intended to address the safety impact of information security risks in the aviation domain in a comprehensive manner for the following reasons:

— They are not focused on the impact that the information security risks may have on aviation safety:

- The NIS Directive is focused on preventing significant disruption of essential services to society and economic activities.
- Regulation (EU) 2015/1998 is focused on preventive cybersecurity measures within the scope of aviation security.

— They do not cover all aviation domains and stakeholders:

- The NIS Directive only covers those operators of essential services defined by each Member State. This means that:
  - not all aviation domains may be covered. For example, it is perfectly possible that in a particular Member State, ATM/ANS organisations, aerodromes and air operators are covered, but maintenance organisations and aircraft manufacturers are not;
  - even for a particular aviation domain, only certain individual stakeholders may have been defined as operators of essential services by the Member State. For example, only the larger airports and air operators.

  Furthermore, the criteria used to identify those operators of essential services vary among the different Member States.

  Nevertheless, it must be noted that the Commission has already proposed a new version of the NIS Directive (NIS 2.0) aiming to address some of those shortcomings, in particular the fact that Member States have applied the notion of 'operator of essential services' differently.
- Regulation (EU) 2015/1998 applies to all airports or parts of airports, all operators, including air carriers, that provide services at airports, and all entities that apply aviation security standards and that operate from premises located inside or outside airport premises and provide goods and/or services to or through airports with the objective of setting the common rules and common basic standards on aviation security. Therefore,

[7] 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) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148).

[8] 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) (https://eur-lex.europa.eu/eli/reg_impl/2015/1998/oj).

it does not cover all the possible entities whose dealings might have an impact on aviation safety.

Therefore, additional rules to fill in existing gaps are needed to address the safety impact of information security risks in a comprehensive and standardised manner across all civil aviation domains. This Opinion proposes these additional rules, while ensuring that the different legislative acts are consistent with and complementary to each other in the effort to holistically address the safety impact of information security risks, avoiding thus duplications, gaps and inconsistencies.

2.2. What we want to achieve — objectives

The overall objectives of the EASA system are defined in Article 1 of the Basic Regulation. This proposal will contribute to the achievement of the overall objectives by addressing the issues outlined in Section 2.1.

The specific objective of this Opinion is to efficiently contribute to the protection of the aviation system from information security risks, events and incidents and their consequences by ensuring that organisations and authorities involved in the safety of civil aviation activities are able to:

— identify and manage information security risks which could affect information and communication technology systems and data used for civil aviation purposes;

— detect information security events identifying those which are considered information security incidents; and

— respond to, and recover from, those information security incidents,

to a level commensurate with their impact on aviation safety.

This is important not only in order to address those risks, events and incidents at organisational level, but also for capturing lessons learned which could be used to improve the system of processes that support aviation safety (e.g. future standards development, certification and oversight activities, etc.).

During the discussions of the ESCP, the following aspects were considered essential in order to achieve the objectives of this Opinion:

— To focus on the impact that information security threats and events could have on safety, regardless of whether this safety impact comes from an attack affecting the aircraft or an attack affecting the normal functioning of the European Aviation Traffic Management Network (EATMN).

— To cover all aviation domains and their interfaces since aviation is a system of systems.

— To ensure that the proposed requirements contribute to the creation of a seamless and consistent regulatory framework where the interfaces between security and safety are appropriately covered, paying special attention at avoiding gaps, loopholes and duplications with Commission Implementing Regulation (EU) 2015/1998 and with the national security requirements stemming from the NIS Directive.

— To ensure that the proposed requirements minimally impact the existing rules that are applicable to the different aviation domains.

— To ensure that any proposed requirements are proportional to the risks incurred by the different organisations.

— To ensure that the proposed requirements are flexible enough to avoid frequent revisions, taking a high-level, performance- and risk-based approach, where AMC & GM material and existing industry standards play a significant role in defining best practices.

— To ensure that organisations and authorities can integrate any new management system requirements with other existing management systems they may have.

— To balance the urgency of the task with the efforts aimed at promoting a harmonised approach at international level.

2.3. How we want to achieve it — overview of the proposals

Taking the above into consideration, this Opinion proposes the following:

A. OBJECTIVE AND SCOPE OF THE PROPOSED RULE

— **This Opinion introduces requirements to be met by organisations involved in civil aviation activities, and by competent authorities, in order to:**

- identify and manage information security risks which could affect information and communication technology systems and data used for civil aviation purposes,
- detect information security events identifying those which are considered information security incidents, and
- respond to, and recover from, those information security incidents

to a level commensurate with their impact to aviation safety.

— **The focus is on the impact on aviation safety, regardless of whether this safety impact comes from an attack affecting the aircraft or an attack affecting the normal functioning of the EATMN.**

It must be noted that the EATMN is defined in Regulation (EC) No 552/2004[9] as follows:

- systems and procedures for airspace management;
- systems and procedures for air traffic flow management;
- systems and procedures for air traffic services, in particular flight data processing systems, surveillance data processing systems and human–machine interface systems;
- communications systems and procedures for ground-to-ground, air-to-ground and air-to-air communications;
- navigation systems and procedures;
- surveillance systems and procedures;
- systems and procedures for aeronautical information services; and

[9] Regulation (EC) No 552/2004 of the European Parliament and of the Council of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation) (OJ L 96, 31.3.2004, p. 26) (https://eur-lex.europa.eu/search.html?scope=EURLEX&text=552%2F2004&lang=en&type=quick&qid=1619616124120).

- systems and procedures for the use of meteorological information.

However, the Basic Regulation states the following:

'Since the rules necessary for the interoperability of the European air traffic management network (EATMN) are either contained in this Regulation or will be contained in delegated or implementing acts adopted on the basis thereof, Regulation (EC) No 552/2004 of the European Parliament and of the Council should be repealed. However, a certain period of time will be required before necessary delegated and implementing acts can be prepared, adopted and can start to apply.'

As a consequence, the elements of the EATMN may change as the new delegated and implementing acts are progressively being introduced.

— **The proposed requirements apply to the following organisations and to the competent authorities responsible for their certification and oversight:**

- approved production and design organisations subject to Subparts G and J respectively of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012[10]
- maintenance organisations subject to Section A of Annex II (Part-145) to Regulation (EU) No 1321/2014[11]
- continuing airworthiness management organisations subject to Section A of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014
- air operators subject to Annex III (Part-ORO) to Regulation (EU) No 965/2012[12]
- aircrew training organisations (ATOs), aircrew aero-medical centres (AeMCs) and FSTD operators subject to Annex VII (Part-ORA) to Regulation (EU) No 1178/2011[13]
- ATCO training organisations (ATCO TOs) and ATCO aero-medical centres (AeMCs) subject to Annex III (Part ATCO.OR) to Regulation (EU) 2015/340[14]
- ATS, MET, AIS, DAT, CNS, ATFM and ASM providers and the Network Manager subject to Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373[15]

[10] 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)(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R0748).

[11] 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) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R1321).

[12] 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) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R0965).

[13] 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) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011R1178).

[14] 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) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R0340).

[15] 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

- aerodrome operators and apron management service providers subject to Annex III (Part-ADR.OR) to Regulation (EU) No 139/2014[16]
- U-space service providers and single common information service providers subject to Regulation (EU) 2021/664[17]

The proposed requirements also apply to the competent authority responsible for the issuance, continuation, change, suspension or revocation of aircraft maintenance licences as per Annex III (Part-66) to Regulation (EU) No 1321/2014.

— **The following organisations have been excluded from the proposed rule in order to ensure appropriate proportionality to the lower safety risks they pose to the aviation system:**

NOTE 1: Once the proposed regulation is adopted and implemented, and as part of the normal regulatory review process, EASA will review not only whether improvements to the requirements are needed, but also whether there is a need to introduce specific provisions for the exempted organisations that do not imply the introduction of a full ISMS for them (which could be disproportional). This could lead to the introduction of some specific provisions in their existing rules to address specific areas of risk.

NOTE 2: For the purpose of the following exemptions, an ELA2 aircraft is a manned European Light Aircraft[18], as defined in paragraph 2(j) of Article 1 of Regulation (EU) No 748/2012.

- design organisations that are solely involved in the design of ELA2 aircraft
- organisations involved in the design of 'Unmanned Aircraft Systems (UAS)' operated in the 'specific' category, when not required to comply with Subpart J of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012
- production organisations that are covered by Subpart F of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012 (production without production organisation approval (POA))

---

and amending Regulation (EU) No 677/2011 (OJ L 62, 8.3.2017, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0373).

[16] 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) (https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32014R0139).

[17] Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space (OJ L 139, 23.4.2021, p. 161) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0664).

[18] 'ELA2 aircraft' means the following manned European Light Aircraft:

(i) an aeroplane with a Maximum Take-off Mass (MTOM) of 2 000 kg or less that is not classified as complex motor-powered aircraft;

(ii) a sailplane or powered sailplane of 2 000kg MTOM or less;

(iii) a balloon;

(iv) a hot air airship;

(v) a gas airship complying with all of the following characteristics:

— 3 % maximum static heaviness,

— Non-vectored thrust (except reverse thrust),

— Conventional and simple design of: structure, control system and ballonet system,

— Non-power assisted controls;

(vi) a Very Light Rotorcraft.

- organisations producing UAS operated in the 'specific' category, when not required to comply with Subparts F or G of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012
- organisations that perform maintenance and continuing airworthiness management activities in accordance with Annex Vd (Part-CAO) to Regulation (EU) No 1321/2014
- organisations that are responsible for the training of maintenance certifying staff in accordance with Annex IV (Part-147) to Regulation (EU) No 1321/2014
- aircrew training organisations (ATOs) that are required to comply with Annex VII (Part-ORA) to Regulation (EU) No 1178/2011, if they are solely involved in theoretical training activities
- aircrew training organisations (ATOs) that are required to comply with Annex VII (Part-ORA) to Regulation (EU) No 1178/2011, if they are solely involved in training activities of ELA2 aircraft
- declared training organisations (DTOs) that are required to comply with Regulation (EU) No 1178/2011
- air operators that are required to comply with Annex III (Part-ORO) to Regulation (EU) No 965/2012, if they are solely involved in the operation of ELA2 aircraft
- air operators that are not required to comply with Annex III (Part-ORO) to Regulation (EU) No 965/2012
- FSTD operators that are required to comply with Annex VII (Part-ORA) to Regulation (EU) No 1178/2011, if they are solely related to ELA2 aircraft
- air navigation service providers holding a limited certificate in accordance with point ATM/ANS.OR.A.010 of Annex III to Regulation (EU) 2017/373
- flight information service providers declaring their activities in accordance with point ATM/ANS.OR.A.015 of Annex III to Regulation (EU) 2017/373

In addition, this regulation will not be applicable to organisations covered by the future Annex 'Part-21 Light' that is expected to be introduced in Regulation (EU) No 748/2012 as a result of the Opinion that EASA intends to publish in the coming months in the context of the activities of RMT.0727.

— A provision has been introduced in IS.OR.200(e), permitting the organisation to be exempted by the competent authority from implementing an ISMS if it demonstrates to the satisfaction of such 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 an impact on safety neither to itself nor to other organisations. This approval shall be based on a documented information security risk assessment performed by the organisation in accordance with IS.OR.205 and reviewed and approved by its competent authority.

The continued validity of this approval shall 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.

— **Applicability to organisations and authorities affected by Regulation (EU) 2021/664 (U-space Regulation)**

In Opinion No 01/2020, EASA proposed:

- requirements for the use of the U-space airspace by UAS operators (additional to those contained in Regulation (EU) 2019/947);
- requirements for U-space service providers and single common information service providers; and
- requirements for the competent authorities responsible for the oversight of U-space service providers and single common information service providers.

In the particular case of the above-mentioned competent authorities, Opinion No 01/2020 included a requirement for the authority to implement an ISMS.

However, during the committee procedure for the adoption of the U-space regulation, it was decided to remove the ISMS requirement at that stage and incorporate it through this Opinion, which is specific to information security for all aviation domains. This would ensure full consistency with all the other aviation domains and would ensure that all the details for the appropriate implementation of the ISMS would be available at the time of entry into force.

Based on the above, this Opinion includes a proposal to amend Article 18 of Regulation (EU) 2021/664 in order to include the requirement for the authority to implement an information security management system complying with Part-IS.AR.

In the case of the U-space service providers and single common information service providers, this Opinion includes a proposal to amend Article 15 of Regulation (EU) 2021/664 in order to include the requirement for the organisation to implement an information security management system complying with Part-IS.OR.

In the case of UAS operators, and as it is explained later in this Opinion, this information security regulation will not be applicable to those in the ‘open’ and ‘specific’ categories. The decision on whether or not it will be applicable in the future to those in the ‘certified’ category will be taken through the ongoing RMT.0230.

— **Applicability to groundhandling service providers**

The decision on whether the provisions contained in this Opinion will be extended or not in the future to groundhandling service providers and their competent authorities will be part of the activities of the ongoing RMT.0728, through which the organisational requirements for groundhandling service providers are being developed.

— **Applicability to operators of UASs**

- Operators of UASs in the 'open' and 'specific' categories have been excluded from the applicability of this regulation.

  According to Commission Regulation (EU) 2019/947, operators of UASs in the 'open' category do not require either an authorisation or a declaration in order to operate the UAS.

  On the other hand, for operators of UASs in the 'specific' category, such a(n) authorisation or declaration is needed. Also, these operators have the option to obtain a 'Light UAS Operator Certificate (LUC)' on the basis of implementing a safety management system, which provides them with the privilege to self-authorise their operations.

  However, even in the most restrictive case of a non-standard scenario, the authorisation can also be granted by the competent authority without the obligation to implement any management system or obtain an LUC. In order to obtain such an authorisation, the development of an operational risk assessment, the application of mitigating measures, the development of an operations manual, and a procedure for the coordination with the relevant air traffic control (ATC) unit (if affecting controlled airspace) are sufficient.

  For those reasons, these operators have been exempted from the rules proposed through this Opinion, and, in particular, from implementing an ISMS.

- Operation of UASs in the 'certified' category

  The decision on whether the provisions contained in this Opinion will be extended or not in the future to operators of UASs in the 'certified' category and their competent authorities will be part of the activities of the ongoing RMT.0230, though which all the requirements for this category of UASs are being developed.

— **Third-country operators that are required to comply with Regulation (EU) No 452/2014[19]**

These operators have been excluded from the scope of the proposed regulation. Nevertheless, these operators will be subject to the requirements contained in the

[19] Commission Regulation (EU) No 452/2014 of 29 April 2014 laying down technical requirements and administrative procedures related to air operations of third country operators pursuant to Regulation (EC) No 216/2008 of the European Parliament and of the Council (OJ L 133, 6.5.2014, p. 12) (https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32014R0452).

amendments introduced in Regulation (EU) 2015/1998 through the amending Regulation (EU) 2019/1583[20] (new point 1.7 in the Annex to Regulation (EU) 2015/1998).

— **Organisations in third countries that are currently covered by bilateral Safety Agreements with the EU**

The proposed regulation does not apply to organisations currently covered by a Safety Agreement signed between their country and the EU. However, this does not preclude the possibility for a future re-negotiation of those Safety Agreements in order to include certain provisions related to the management of information security risks.

It is important to note that even if those third-country organisations are not subject to the requirements of the proposed rule, this does not preclude that the persons or organisations in Europe that are subject to this rule may impose certain contractual requirements when buying those products from the third-country organisations.

The reason for that is that those EU organisations will have to address information security risks coming from the interfaces they have with other organisations or because of the products they use. Nevertheless, it must be noted that these are organisational requirements, not product certification requirements. So, the question is not whether the product acquired from the third-country organisation is appropriately certified (this is the subject of the appropriate certification process). It is about the risks coming from the third-country organisation if it does not manage information security risks appropriately and this impacts the product (e.g. not properly addressing in-service experience, not having sufficient staff to address information security risks at organisational level, etc.).

In any case, the oversight of the EU organisation subject to the rules will be performed by the EU Member State competent authority or, if applicable, by EASA. As part of this oversight, the competent authority will check how the organisation manages the risks coming from their suppliers.

— **It is important to note that the proposed requirements do not apply to organisations for which there are no organisation requirements within the existing rules.** Therefore, the proposed requirements will not be directly applicable to organisations that work as contractors under the control and accountability of other organisations for which the rule is applicable. It will be the responsibility of the contracting organisations to take into account the information security risks associated with their contracted organisations and establish appropriate provisions in the contracts in order to address those risks.

— **Finally, the proposed requirements do not apply to those organisations that are outside the scope of the Basic Regulation.** This is, for example, the case for those aerodromes that have been exempted by the Member States in accordance with Article 2(7) of the Basic Regulation. This provision allows the Member States to exempt from the Basic Regulation the design, maintenance and operation of an aerodrome, and the safety-

[20] Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures (OJ L 246, 26.09.2019, p. 15) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2019.246.01.0015.01.ENG&toc=OJ%3AL%3A2019%3A246%3ATOC).

related equipment used at that aerodrome, where that aerodrome handles no more than 10 000 commercial air transport passengers per year and no more than 850 movements related to cargo operations per year, and provided that the Member States concerned ensure that such exemption does not endanger compliance with the essential requirements referred to in Article 33 of the Basic Regulation.

B. LEGAL BASIS FOR THE PROPOSED REQUIREMENTS

Due to the fact that this Opinion proposes requirements to be met by organisations and competent authorities in all aviation domains, and as required by the Basic Regulation for each of these domains, it has been necessary to split those requirements into delegated acts and implementing acts:

— Delegated acts applicable to:

- design and production organisations, as per Article 19(1) of the Basic Regulation
- aerodrome operators and apron management service providers, as per Article 39(1) of the Basic Regulation

— Implementing acts applicable to:

- the competent authorities (including EASA), as per Article 62(15)(c) of the Basic Regulation
- CAMOs and maintenance organisations, as per Article 17(1) of the Basic Regulation
- pilot training organisations, cabin crew training organisations, aero-medical centres for aircrew and operators of FSTDs, as per Article 27(1) of the Basic Regulation
- aircraft operators, as per Article 31(1) of the Basic Regulation
- ATM/ANS providers, as per Article 43(1) of the Basic Regulation
- U-space service providers and single common information service providers, as per Article 43(1) of the Basic Regulation
- training organisations and aero-medical centres for air traffic controllers, as per Article 53(1) of the Basic Regulation

Based on the above, the following Regulations have been proposed as Annexes I, II, III and IV to this Opinion:

— Annex I: An Implementing Regulation amending all the existing rules applicable to:

- competent authorities in all domains; and
- organisations in all domains, except for design and production organisations, aerodrome operators and apron management service providers, for which the existing rules are amended via the corresponding Delegated Act contained in Annex III.

The purpose of the amendments contained in Annex I is to introduce requirements for authorities and organisations to comply with the new Part-IS.AR and Part-IS.OR requirements (which are contained in Annex II), and to add the elements necessary for the competent authorities to perform their certification and oversight activities.

— Annex II: An Implementing Regulation introducing the new information security regulation (Part-IS.AR and Part-IS.OR) for:

- competent authorities in all domains; and
- organisations in all domains, except for design and production organisations, aerodrome operators and apron management service providers, which are covered via the corresponding Delegated Act contained in Annex IV.

— Annex III: A Delegated Regulation amending the existing rules applicable to design and production organisations, aerodrome operators and apron management service providers.

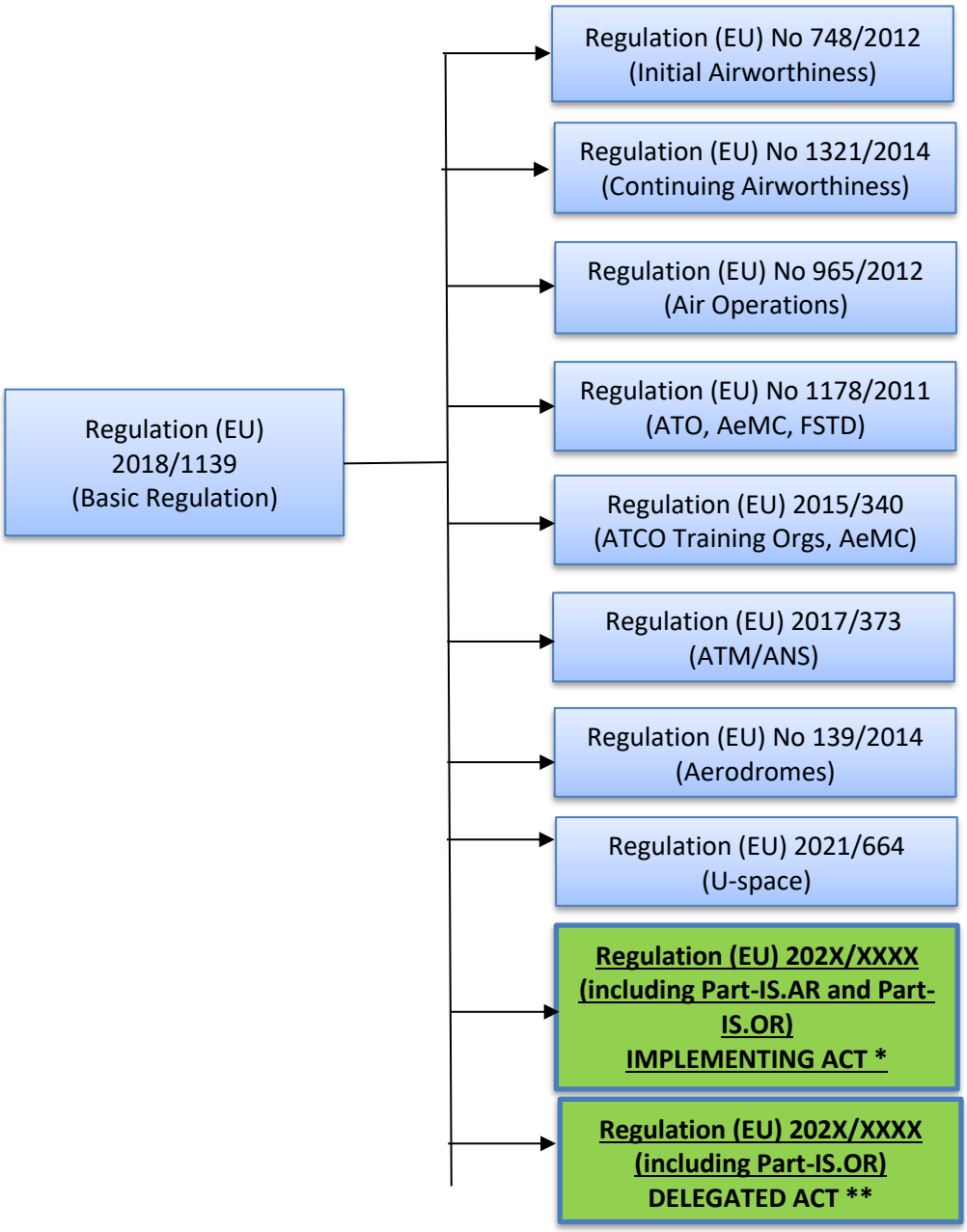
The purpose of the amendments contained in Annex III is to introduce requirements for those organisations to comply with the new Part-IS.OR requirements (which are contained in Annex IV).

— Annex IV: A Delegated Regulation introducing the new information security regulation (Part-IS.OR) for design and production organisations, aerodrome operators and apron management service providers.

It is important to note that, although there are two regulations (an Implementing Act and a Delegated Act) containing Part-IS.OR (ref. Annexes II and IV), with each one of them applicable to a different set of organisations, both Part-IS requirements are almost identical. The split has been done for the purpose of complying with the legal requirements of the Basic Regulation.

C. STRUCTURE OF THE PROPOSED RULE

— This Opinion proposes the introduction of two regulations (one Implementing Act and one Delegated Act). These regulations apply across different aviation domains and, therefore, could be seen as 'horizontal' rules. In addition, appropriate cross-references to these 'horizontal' rules have been introduced in the existing rules.



* Implementing Act for competent authorities in all domains and for all organisations except for design and production organisations, aerodrome operators and apron management service providers.

** Delegated Act for design and production organisations, aerodrome operators and apron management service providers.

— This structure, where the ISMS requirements for authorities and organisations have been introduced in 'horizontal' rules, provides the following benefits:

- It ensures consistency of information security requirements across different domains.
- There is no need for a separate organisation approval, certificate or declaration. The organisation approval, certificate or declaration will cover the requirements of the current approval and the requirements of the corresponding 'horizontal' information security rule.
- Minimal changes are necessary to the existing rules, which will reduce the impact on those rules and the possibility of interference with other RMTs.
- It facilitates the extension of the information security requirements to other domains in the future if necessary (e.g. groundhandling services, operators of UASs in the 'certified' category, etc.).

— However, it is important to note that the authority requirements for the certification and oversight of the ISMS of the different organisations have not been introduced in the 'horizontal' rules. Instead, they have been integrated in the certification and oversight requirements already contained in the existing rules for each domain. This applies to the following aspects**:**

- information to the Agency;
- immediate reaction to an information security incident with a safety impact;
- allocation of tasks;
- changes to the ISMS (of the organisation); and
- oversight principles.

It must be noted that the other option, which was widely favoured during the discussions in the ESCP, of introducing the authority certification and oversight requirements in Part-IS.AR would have been better in making more visible the need for consistency of oversight approaches among the authorities responsible for each aviation domain.

This option mostly relied on introducing in Part-IS.AR cross-references to the equivalent requirements already contained in the existing rules, indicating that the authority would need to comply with them but with a focus placed on information security aspects affecting safety. This would have been complemented with the introduction in Part-IS.AR of some specific information security provisions which did not have an equivalent in the existing rules.

However, EASA eventually discarded this option for the following reasons:

- It would result in the introduction of a very large number of cross-references to the equivalent requirements already contained in the existing rules, indicating that the authority would need to comply with them but with a focus placed on information security aspects affecting safety.

- This, in addition to being too general and too vague to be properly implemented, would not have been accurate enough because the equivalent requirements contained in the existing rules are not identical across the different domains and, in addition, some of the requirements contained in them are not relevant to information security.
- Furthermore, any AMC & GM that would have been developed in connection with those requirements would have required to be split between AMC & GM associated with Part-IS.AR and AMC & GM associated with the existing rules. The AMC & GM related to those requirements where cross-references were introduced, would need to be associated with the existing rules. However, those AMC & GM related to specific information security provisions directly introduced in Part-IS.AR would need to be associated with Part-IS.AR.

— Regarding the content of Part-IS.AR and Part-IS.OR:

- Part-IS.AR (which is included in the Implementing Act) contains the requirements for the ISMS of the competent authority.
- Part-IS.OR (which is included in both the Implementing Act and in the Delegated Act, depending on the type of organisation) contains the requirements for the ISMS of the organisations.

Part-IS.AR (Authority Requirements):

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

Part-IS.OR (Organisation Requirements):

IS.OR.100 Scope
IS.OR.200 Information security management system (ISMS)
IS.OR.205 Information security risk assessment
IS.OR.210 Information security risk treatment
IS.OR.215 Information security internal reporting scheme
IS.OR.220 Information security incidents — detection, response, and recovery
IS.OR.225 Response to findings notified by the competent authority
IS.OR.230 Information security external reporting scheme
IS.OR.235 Contracting of information security management activities
IS.OR.240 Personnel requirements
IS.OR.245 Record-keeping
IS.OR.250 Information security management manual (ISMM)
IS.OR.255 Changes to the information security management system
IS.OR.260 Continuous improvement

D. COMPETENT AUTHORITY

— This Opinion proposes that the competent authority responsible for the certification and oversight of each organisation's compliance with this Regulation shall be the one established in accordance with the current regulations applicable to each organisation.

In those cases where the competent authority is not EASA, those regulations require the Member State to nominate one or more competent authorities for the certification and oversight of the applicable requirements. This allows the Member State to nominate as competent authority for the certification and oversight of the requirements contained in this Regulation the same entity already responsible for the certification and oversight of the requirements contained in the regulations detailed in Article 2(1)(a) through (1)(i), or a different entity.

If the Member State decides to nominate a different entity, coordination measures shall be established between those entities to ensure effective oversight of all the requirements to be met by the organisation.

— The proposed requirements include provisions to allow the competent authority to allocate certification and oversight tasks to other entities (for example, to qualified entities or to a national information security agency). However, in such a case, the

competent authority and the allocated organisation must coordinate the aspects related to aviation safety. Furthermore, the competent authority must integrate the results of the certification and oversight activities performed on their behalf by other entities into the overall certification and oversight files of the organisation.

These provisions facilitate the access by the competent authority to additional information security expertise, and provide flexibility to the State in order to create a national safety and information security organisational structure that fits their needs.

— EASA will be the competent authority for the oversight of the proposed information security requirements for the cases foreseen in the following articles of the Basic Regulation:

- Article 64(1) 'Reallocation of responsibility upon request of Member States'
- Article 65 'Reallocation of responsibility upon request of organisations operating in more than one Member State'
- Article 77(2) 'Airworthiness and environmental certification'
- Article 78 'Aircrew certification'
- Article 80(1) 'ATM/ANS'
- Article 81 'Air traffic controller training organisations certification'

Particular attention has been given to the European Geostationary Navigation Overlay Service (EGNOS), for which EASA is the competent authority for its safety approval, including in the requirements proposed by this Opinion. Appropriate provisions have been introduced in order to avoid duplication of oversight activities with those performed by the Security Accreditation Board (SAB) responsible for the oversight of the EGNOS security requirements established by the European Commission.

E. CONSISTENCY WITH OTHER LEGISLATIVE ACTS

— Taking into account that a number of organisations are already subject to cybersecurity or information security requirements arising from other EU or national legislation (e.g. national implementation of the NIS Directive and Regulation (EU) 2015/1998) or will be affected by future evolutions of the NIS Directive, the following provisions have been introduced in order to minimise gaps and duplications and ensure consistency of oversight regimes:

- The possibility has been provided for the competent authority 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, and that this competent authority coordinates with any other relevant authorities to ensure coordinated or compatible oversight regimes.

  It must be noted that the sentence '*provided that such requirements are at least equivalent in effect to the obligations laid down in this Regulation*' is similar to the one contained in point 1.2.7 of the NIS Directive.

- In the particular case of airport operators, air carriers and entities as defined in the national civil aviation security programmes of Member States, and although the point above could also be applied, an additional possibility has been provided for the competent authority to replace compliance with the requirements contained in this Regulation, except those related to the information security external reporting scheme required by point IS.OR.230 of Annex I to this Regulation, by compliance with elements of the cybersecurity requirements contained in the Annex to Implementing Regulation (EU) 2015/1998. In such a case, this competent authority shall coordinate with any other relevant authorities to ensure coordinated or compatible oversight regimes.

  It must be noted that the requirements related to the information security external reporting scheme have been excluded from this option because there are no equivalent provisions in the Annex to Regulation (EU) 2015/1998.

  It must also be noted that this possibility given to the competent authority is similar to the reciprocal provision contained in point 1.7.5 of Annex I to Regulation (EU) 2015/1998, which reads as follows:

  'Where airport operators, air carriers and entities as defined in the national civil aviation security programme are subjected to separate cybersecurity requirements arising from other EU or national legislation, the appropriate authority may replace compliance with the requirements of this regulation by compliance with the elements contained in the other EU or national legislation. The appropriate authority shall coordinate with any other relevant competent authorities to ensure coordinated or compatible oversight regimes.'

- Finally, for those cases where the competent authority has decided not to use the options provided above, the possibility is given to the affected organisations to use compliance methods developed under the cybersecurity or information security requirements of those EU or national legislation as a means to comply with the requirements of this Regulation, provided that the organisation demonstrates to their competent authority that with those compliance methods the organisation fully meets the requirements and objectives of this Regulation.

F. PERFORMANCE- AND RISK-BASED APPROACH

— The regulations proposed through this Opinion have been developed taking a high-level, performance- and risk-based approach, where AMC & GM material and industry standards will play a significant role in defining best practices.

— Regarding the AMC & GM material that will support the implementation of the proposed regulations, and which will be published by EASA once the applicable regulations are adopted by the European Commission, they are currently being developed in coordination with the ESCP.

These discussions have already identified the need to develop AMC and GM to address the following specific issues:

- Objective of the rule
  - Address the need to cover not only the digital aspects of information security (which is the main focus) but also the physical aspects.
  - Provide guidance explaining that the impact on safety may come not only because of a direct impact on the aircraft but also by affecting the EATMN.
- Definitions

  Although a number of definitions have been introduced in the proposed regulations, it may be necessary to introduce specific definitions in the AMC & GM for terms which are used with different meanings depending on the context of the paragraphs where they are used.
- Small organisations

  AMC and GM are needed on how to implement an ISMS for small organisations; in particular, for organisations such as certain small aerodromes, where certain elements of the EATMN may not be applicable or may be performed by other organisations.
- Temporary exemption of certain organisations from the requirement to have an ISMS

  AMC and GM are needed on how to perform the 'information security risk assessment' required by IS.OR.200(e) in order to demonstrate to the competent authority that the organisation's activities, facilities and resources, as well as the services it operates, provides, receives and maintains, do not pose any information security risks with an impact on safety neither to itself nor to other organisations.
- Identification of interfaces with other organisations

  AMC and GM are needed on how to identify the interfaces (also called 'functional chains') with other organisations with which the organisation shares information security risks, as well as on commonly shared and understood criteria for performing the risk assessments and for sharing information on residual risks.
- Risks attributed to aviation staff and evaluation of competence

  With the proposed requirements, the organisations will have to evaluate the information security risks that could be attributed to the roles, responsibilities, activities, actions assigned to their aviation staff (e.g. aircrew, mechanics, air traffic controllers, etc.).

  AMC and GM may be needed in order to provide more details on how the risk assessment should be done, how to design a tailored competence scheme and how to define appropriate access controls to the different systems and information.

- Information security risk assessments

  It is necessary to develop material covering, among other aspects, the following:

  - the identification of threat scenarios;
  - the determination of level of risks, including the threat potential and safety consequences; and
  - the determination of acceptability of risks.

  AMC and GM are also needed on the approach to be taken when performing risk assessments in the case of legacy aircraft and other legacy systems and technologies.

- Information security risk treatment

  It is necessary to develop material covering, among other aspects, the following:

  - the level of urgency to implement the measures;
  - the proportionality of the measures to the severity of the safety consequences; and
  - the assessment of the effectiveness of the measures.

- Information security incidents — detection, response and recovery

  It is necessary to develop material covering, among other aspects, the following:

  - the establishment of functional performance baselines, from which deviations have to be identified;
  - the scope of the detection, response and recovery measures; and
  - the criteria to follow when developing detection, response and recovery measures.

- Maturity, performance and continuous improvement
  - It may be necessary to define in the AMC & GM different levels of maturity and performance for each requirement of the rule and define what level is considered sufficient in order to meet the specific objectives of the particular requirement. This could be particularly important in order to make clear the level expected at the end of the transition period of the future rule.
  - It is necessary to develop material covering, among other aspects, the following:
    - performance targets and indicators that would allow evaluating the capability of the organisation;
    - gathering, archiving and analysis of collected metrics of activities; and
    - the implementation of process or design improvements.

- Information security external reporting scheme
    - AMC and GM are needed to explain how to evaluate which incidents and vulnerabilities should be reported and which not.
    - AMC and GM are needed in order to determine when an incident is considered to be 'known to the organisation', for the purpose of defining the starting point of the 72-hour reporting limit. During the development of this material, material contained in the future standard jointly developed by EUROCAE and RTCA on 'ED-ISEM Guidance on Information Security Event Management (ISEM)' and in AMC 21.A.3A(b)(2) to Annex I (Part-21) of Regulation (EU) No 748/2012 may be useful.
    - AMC and GM are needed on the expected reaction times depending on the criticality of the incident.
    - AMC and GM are necessary on the type of information contained in the external reports.
    - AMC and GM may be needed on the possibility of using the European Coordination Centre for Accident and Incident Reporting Systems (ECCAIRS) for the external reporting.
- Information to the Agency

  Regarding this requirement, which has been integrated in the equivalent provisions contained in the existing rules, and where the competent authority of the Member State is required to provide EASA with safety-significant information stemming from the information security reports it has received, it is necessary to provide examples of 'safety-significant information'.
- Contracted activities

  AMC and GM are needed on the level of involvement (LoI) that the organisations should exercise in the oversight of the activities performed by the contracted organisations and on the evaluation of risks associated with these contracted activities.

  Guidance is needed to explain the difference between the provisions related to the contracting of activities required by Part-IS (e.g. management of risks, reporting, record record-keeping, etc.), and the control of suppliers and contracted operational activities.
- Comparability matrix between Part-IS and certain international standards

  A comparability matrix should be included in the AMC & GM comparing the ISO 27000 standards and the requirements of Part-IS.

  This should include the identification, for each requirement of Part-IS, of which provisions of ISO 27000 could be used to meet them (totally or partially), and when not sufficient, which additional actions should be performed.

Depending on time constraints for the publication of the AMC & GM once the regulations are adopted, similar comparability matrices could be developed for other standards.

G. INTEGRATION WITH OTHER MANAGEMENT SYSTEMS

Points IS.AR.200(d) and IS.OR.200(d) give the possibility to competent authorities and organisations to integrate the ISMS proposed through this Opinion with other existing management systems they may already have (e.g. safety management system, security management system, etc.).

H. ENTRY INTO FORCE AND TRANSITIONAL MEASURES

In order to provide a sufficient transition period that allows organisations and authorities to comply with the new rules and procedures, the following provisions have been proposed through this Opinion:

— The regulation would enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

— However, the regulation would not apply until 1 year after the date of entry into force. This would be the point at which the competent authorities would have to start performing the oversight of organisations' compliance with the new requirements.

— In addition, organisations may correct any findings of non-compliance raised by the authority until 2 years after the date of entry into force of the regulation or until the date established by the competent authority, whichever comes later.

2.4. What are the stakeholders' views — outcome of the consultation

In total, 757 comments were received during the consultation phase of NPA 2019-07, which took place from 27 May 2019 to 27 September 2019.

The distribution of comments across the different aviation domains was the following:

— European authorities: 221 comments

— FAA: 34 comments

— Eurocontrol: 4 comments

— Airports: 105 comments

— European manufacturers and design organisations: 122 comments

— US manufacturers (including General Aviation): 10 comments

— Brazilian manufacturers: 15 comments

— Canadian manufacturers: 1 comment

— ATM/ANS: 81 comments

— Airlines: 67 comments

— Business Aviation: 47 comments

— General Aviation (EU): 20 comments

— European associations for aviation personnel: 4 comments

— Training organisations: 1 comment

— Maintenance organisations: 1 comment

— Private persons: 24 comments

Although the responses to those comments are presented in Comment-Response Document (CRD) 2019-07 that is expected to be published one month after the publication of this Opinion, the following is a summary of the main issues raised:

— The need for an information security regulation

- A number of comments questioned the need for a specific regulation and proposed the use of the ISO 27000 standard instead.
- A number of comments expressed the need for appropriate proportionality of the rules.

— The affected and exempted organisations

A number of comments from the FAA and US industry organisations raised the concern that the proposed regulation would directly or indirectly impact US organisations and the oversight activities performed by the FAA. In particular, they requested that the management of risks associated with CS-23 aircraft be removed from the scope of the regulation.

In addition, there was a wide range of comments , in some cases contradicting each other, regarding specific organisations which should be exempted or included within the scope. Some examples are the following:

- The rule should also apply to non-approved organisations (e.g. SITA, AMADEUS).
- Include groundhandling service providers within the scope.
- Exempt production organisations producing only parts and appliances.
- Use a different criterion for the exemptions (not the ELA2 category).
- Exempt small ATOs, FSTD operators, etc.
- Eliminate all exemptions and replace them by adequate proportionality of the rule.
- Exemptions should be based on the complexity of organisations.
- Exempt small drones in the ‘certified’ category.
- Include drones in the ‘specific’ category (with LUC).

— The definitions contained in the proposed regulation

A significant number of comments were received proposing additional terms to be defined, as well as alternative wording for those which had already been included in the NPA.

— The content of the ISMS and its integration with other management systems

- A number of comments emphasised the need to align as much as possible with existing SMS rules.

- A significant number of comments were received on the specific elements of the ISMS, the elements of the organisations which should be covered by the risk assessment (e.g. facilities, activities, resources, equipment, systems, data, etc.) and the terms used (e.g. risks, events, incidents, threats, vulnerabilities, etc.).

— Which should be the competent authority responsible for the new information security requirements

- In general, the proposal contained in the NPA that the current competent authority for each organisation (typically the NAA) would be also responsible for the oversight of the organisations subject to the new requirements was supported.
- A number comments raised the concern that the current NAAs may not have sufficient staff with the appropriate qualifications to perform oversight on information security matters.
- A small number of Member States raised concerns about how the proposed requirements would affect their current national organisational structures, in particular in relation to the hierarchy between the NAA, the national cybersecurity agencies and the ministries responsible for them.
- Some comments were received indicating that even if the authority is the NAA, EASA could still be denied access to certain information, if it is sensitive.

— The consistency with the NIS Directive and Regulation (EU) 2015/1998, and the approach to follow regarding operators of essential services

- There were comments, especially from some authorities, saying that the organisations affected by the NIS Directive should also comply with the new information security requirements. Otherwise, there would be a lack of standardisation in the Member States and unfair competition. Furthermore, in some cases, this may result in operators of essential services having to comply with less strict requirements than operators of non-essential services.
- A very high number of comments emphasised the need for compatible regulatory and oversight regimes between the future EU rules, the NIS Directive and Regulation (EU) 2015/1998, as well as the need for avoidance of duplicated oversight for those organisations covered by more than one legislative act.

— The reporting requirements

- There was a significant emphasis on avoiding duplication of reporting schemes.
- Some comments requested the inclusion of a list of information security reportable conditions in Regulation (EU) No 376/2014[21].
- Some comments requested the definition of the template for reporting to be left to the Member States, so that they can use the same template they already use for reporting under the NIS Directive.

[21] Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007 (OJ L 122, 24.4.2014, p. 18) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0376&qid=1619720051833).

— The type of material which should be included in the AMC & GM

- There were a significant number of comments requesting a public consultation of the future AMC and GM.
- A significant number of comments proposed the performance of an appropriate gap analysis and the production of a comparability matrix between the future EU rules and ISO 27001
- There was also a proposal to accept compliance with ICAO Annex 17 as equivalent to compliance with this regulation.
- A significant number of comments requested the development of AMC and GM on how to implement an ISMS for small organisations, possibly using compliance checklists and specific forms.
- Other aspects where there was a significant number of comments requesting AMC and GM were the following:
    - Staffing needs, qualifications, level of competence and training.
    - The evaluation of risks attributed to aviation staff.
    - How to address legacy aircraft.
    - The special case of organisations holding several approvals but having a common department dedicated to information security management.
    - Incident reporting mechanisms, timelines and forms.
    - Coordination with suppliers and contracted organisations.

Survey launched on 14 September 2020

After the closing of the comment period for NPA 2019-07 on 27 September 2019, EASA and the ESCP initiated the evaluation and discussion of the comments to ensure that they were properly addressed.

Given that by the summer of 2020 there were still important issues where a compromise needed to be reached, EASA launched a survey.

This survey was sent on 14 September 2020 to the ESCP participants, and it was responded by 8 industry associations, 4 industry organisations, 2 European agencies and 16 authorities.

Based on the result of the survey and the subsequent discussions within the ESCP, EASA decided the following:

— **The availability of AMC and GM**

In order to not delay the publication of the Opinion, while still giving enough visibility to the ESCP of the upcoming material before agreeing on the content of the Opinion, EASA decided to:

- develop objectives, and include them in the rule as performance-based requirements, for those requirements which are more performance- and risk-based (IS.AR.205, 210 and 215; IS.OR.205, 210 and 220), and

- develop AMC with criteria on how to meet those objectives, and have a sufficiently mature version of them that would allow the ESCP to agree on the appropriateness of the requirements and objectives before this Opinion was issued. Additional discussions will take place in the coming months within the ESCP to finalise the AMC and GM.

— **The terms 'information security' and 'cybersecurity' and the acronym to be used for this rule**

EASA decided to use the term 'information security' across this Opinion because the risks associated with information systems are not limited to possible attacks to the cyberspace, but encompass threats which are both digital and analogue. The only references to the term 'cybersecurity' in the proposed regulations are those where there are references to other legislative acts dealing with cybersecurity, such as Regulation (EU) 2015/1998.

EASA also decided to use the acronym 'IS', standing for 'information security', for the naming of 'Part-IS', since other possible options were either creating confusion about the meaning or colliding with acronyms already used in the aviation domain.

— **The need for consistency with other legislative acts (e.g. NIS Directive, Regulation (EU) 2015/1998)**

In order to achieve a uniform level of safety and a level playing field across all the Member States, EASA decided that all the organisations within the scope of this proposed regulation would have to comply with it. This would also apply to those organisations that already comply with other cybersecurity or information security provisions in the NIS Directive and/or Regulation (EU) 2015/1998.

However, based on further feedback received after this survey, EASA has eventually included provisions that would allow the competent authority to replace, for the affected organisations, the requirements of the future safety rules by elements of the national implementation of the NIS Directive and/or Regulation (EU) 2015/1998 (or future evolutions), under certain conditions (refer to point 2.3.E 'Consistency with other legislative acts' of this Opinion).

— **Which authority will be the competent authority responsible for the implementation of the proposed rule**

EASA decided that the competent authority that is already responsible for the organisation (as per the already existing rules) becomes also responsible for the implementation and enforcement of the new requirements proposed through this Opinion. This way a single authority is responsible for the organisation, ensuring thus that all the aspects related to aviation safety are appropriately considered.

Nevertheless, provisions have been included to allow the competent authority to allocate certification and oversight tasks to other entities (for example, to qualified entities or to a national information security agency), subject to appropriate coordination between them. These provisions should facilitate the access of the competent authority to additional information security expertise, and provides Member States with the flexibility to create a national safety and information security organisational structure that fits their needs.

2.5. What are the expected benefits and drawbacks of the proposal

In Section 4.3 of NPA 2019-07, EASA selected the following options in order to perform the corresponding impact assessment:

Option No	*Short title*	**Description**
0	Baseline scenario	No policy change (no change to the rules; risks remain as outlined in the issue analysis).
1	Introduce requirements for the management of information security risks	Introduce requirements related to aeronautical information systems security, with the following features: — The proposed rule would have the form of a 'horizontal rule' applicable to all aviation domains, with some organisations being exempted (permanently or temporarily) in order to ensure proportionality to the lower risks involved. — The rule would contain high-level, performance- and risk-based requirements, and would be complemented by AMC and GM as well as industry standards. — The competent authority for the information security elements would be the NAA that is already responsible for the implementation and enforcement of the current implementing rules applicable to the organisation. — Organisations identified by a Member State as operators of essential services in accordance with the NIS Directive would be able to replace compliance with the organisation requirements contained in this Regulation by compliance with the elements contained in the nationally transposed Article 14 of the NIS Directive under certain conditions. — Organisations and competent authorities would be given the possibility to integrate the new information security management system (ISMS) into other existing management systems they may already have.

The impact of those options was analysed in Section 4.4 of NPA 2019-07 and the conclusion provided in Section 4.5 was to take on board Option 1 indicated above.

Nevertheless, as a result of the public consultation performed through NPA 2019-07 and further surveys and discussions within ESCP and with affected parties, the following changes have been introduced in this Opinion:

— Instead of mandating that the competent authority responsible for the oversight of the organisation´s compliance with the new rule to be the same authority that is already responsible for the oversight of the organisation´s compliance with the current rules, this will be just an option for the Member State. The other option will be for the Member State to choose a different authority, but in that case coordination measures shall be established between both authorities to ensure effective oversight of all the requirements to be met by the organisation.

  This additional option will require further coordination since several authorities will be involved in the approval of the organisation. However, it will provide greater flexibility to the Member

States when defining their national organisational structures for the oversight of safety, security and essential services matters.

— The text proposed in NPA 2019-07 allowed those organisations identified by a Member State as operators of essential services in accordance with the NIS Directive to replace compliance with the organisation requirements contained in this Regulation by compliance with the elements contained in the nationally transposed Article 14 of the NIS Directive under certain conditions.

However, EASA has eventually included provisions that would allow the competent authority to replace, for the affected organisations, the requirements of the future safety rules not only by elements of the national implementation of the NIS Directive (or future evolutions) but also of Regulation (EU) 2015/1998, under certain conditions (refer to point 2.3.E 'Consistency with other legislative acts' of this Opinion).

In addition, a number of measures have been introduced to reduce the impact on the affected organisations, such as:

- The affected organisations may use compliance methods developed under other cybersecurity or information security legislative acts in order to show compliance with the requirements proposed through this Opinion, if they meet the safety objectives of the future rule.
- Provisions have been introduced requiring appropriate coordination between the competent authority defined in this Regulation and other relevant authorities responsible for information security or cybersecurity within the Member State.
- The proposed rules have been developed having considered maximum use of international standards widely used by affected organisations.

Based on the above, the expected benefits and drawbacks of the regulations proposed in this Opinion, and the mitigating measures for those drawbacks, are the following:

2.5.1. The expected benefits

— A more systematic and standardised approach across all aviation domains when identifying the areas exposed to information security risks which could impact safety, by performing risk assessments, developing and implementing measures to protect their critical systems, data and processes, identifying vulnerabilities and information security incidents and taking actions to mitigate them.

— A more coordinated approach between the different authorities within each Member State, which will promote more effective and efficient organisational structures within the Member States, more consistent regulatory and oversight policies, and an improved coordination when addressing safety and security matters.

— A wider collaboration and exchange of information between organisations and authorities, and a more complete picture of safety risks across the European aviation system due to the incorporation of information security data through the corresponding reporting mechanisms.

— Increased skills and competence of the organisation staff, which should improve the overall productivity, efficiency and effectiveness of the organisations.

— Increase of employment opportunities and better economic conditions for the qualified personnel available in the labour market.

— Increased business opportunities for educational institutions and training organisations.

— Possible decrease of insurance costs.

As a summary, the measures introduced through this Opinion should contribute to:

— an increased level of safety, protecting the aviation system from information security risks and making it more resilient to information security events and incidents;

— an economic benefit for the organisations since the liability costs, as well as the operational and reputational damage caused by incidents and accidents could be otherwise very high; and

— an enhanced internal market and competitiveness due to the inclusion of standardised requirements for all aviation organisations in the different aviation domains.

2.5.2. The expected drawbacks

— Aviation organisations and authorities may find difficulties in having access to a sufficient number of qualified personnel, possibly at increased cost.

This impact is expected to be reduced, at least in the case of competent authorities, since this Opinion includes provisions to allow them to allocate certification and oversight tasks to other entities which could have more competent staff for information security matters (e.g. national information security agencies).

— There will be an economic impact caused by the need for the organisations to implement the new requirements. This impact will largely depend on how robust their current management systems are when addressing information security risks.

— Some large organisations, considered as operators of essential services by their Member States, may have already implemented ISMS and event notification measures similar to the ones proposed by this Opinion.

This impact would be significantly mitigated by the measures introduced through this Opinion, such as:

- The possibility given to the competent authority to replace, for the affected organisations, the requirements of the future safety rules not only by elements of the national implementation of the NIS Directive (or future evolutions) or Regulation (EU) 2015/1998, under certain conditions (refer to point 2.3.E ‘Consistency with other legislative acts’ of this Opinion).
- the possibility for the affected organisations to use compliance methods developed under other cybersecurity or information security legislative acts in order to show compliance with the requirements proposed through this Opinion,
- the need for coordination between the different authorities within the Member States so that there is no duplication of oversight activities; and
- the significant use that will be made in the AMC & GM of international standards which are already used by those organisations.

— Other organisations, even when not covered by the NIS Directive, may have already implemented, at least partially, measures to address information security risks. This could be especially the case of aircraft manufacturers, aerodromes and ATM/ANS organisations. For these organisations, there would be an economic impact due to the need to introduce some changes in order to fully comply with the proposed requirements.

Nevertheless, this should be limited by the significant use that will be made in the AMC & GM of international standards which are already used by those organisations.

— The organisations that have not implemented any procedures and processes for the management of information security risks will suffer the highest cost for the implementation of the proposed measures. This is expected to be the case for smaller organisations, which may not have paid special attention to the information security risks to which they are exposed as well as to the risks they expose other stakeholders to. Nevertheless, this economic impact should be mitigated by the fact that the future AMC and GM will take due account of the proportionality aspects linked to smaller organisations by providing details on what would be sufficient for a small organisation in order to implement an ISMS.

— Furthermore, the costs described above will be mitigated by the transition measures introduced for the applicability and compliance with the new requirements, which would delay the applicability of the rule for 1 year after the rule adoption, and would provide 1 additional year for organisations to close any findings of compliance with the new rules.

2.6. How we monitor and evaluate the rules

Monitoring is a continuous and systematic process of data collection and analysis about the implementation/application of a rule/activity. It generates factual information for future possible evaluations and impact assessments, and also helps to identify actual implementation problems. With respect to this proposal, EASA would suggest monitoring various elements with the indicators proposed below:

What to monitor	How to monitor	Who should monitor	How often to monitor
How effective is the coordination between the competent authority and other relevant authorities responsible for information security or cybersecurity risks within the Member State	Audits/feedback from Member States	EASA	Once the rule is applicable. Recurrence to be defined.
How many Member States have decided to use the newly adopted EU rule as a	Audits/feedback from Member States	EASA	Once the rule is applicable.

Lex Specialis for compliance with the NIS Directive and Regulation (EU) 2015/1998			Recurrence to be defined.
Number and trend of information security occurrences or vulnerabilities reported by organisations, split by risk classification.	Occurrence records in the European Central Repository (ECR) and information collected at Member State level	EASA/competent authority — with the support of the Network of Analysts (NoA) and the Network of Cybersecurity Analysts (NoCA)	On a recurrent basis, e.g. once a year.
Number and level of findings related to the implementation of Part-IS.AR and Part-IS.OR.	Audits	Competent authorities/EASA	On a recurrent basis, e.g. once a year.

Cologne, 11 June 2021

Patrick KY
Executive Director

3. References

3.1. Affected regulations

— 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)

— 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)

— 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)

— 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)

— 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)

— 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)

  NOTE: The future evolution of the current Regulation (EU) No 73/2010 of 26 January 2010 laying down the requirements on the quality of aeronautical data and aeronautical information for the single European sky (OJ L 23, 27.1.2010, p. 6) has been also considered.

— 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)

— 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)

3.2. Related decisions

AMC & GM to the Regulations listed in Section 3.1.

3.3. Other reference documents

The following (non-exhaustive) list includes documents that have been considered during the development of this Opinion:

— Amendment 16 to ICAO Annex 17 adopted by the Council on 14 March 2018

— Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 104, 19.7.2016, p. 1)

— Regulation (EU) No 376/2014 of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the Council and repealing Directive 2003/42/EC of the European Parliament and of the Council and Commission Regulations (EC) No 1321/2007 and (EC) No 1330/2007 (OJ L 122, 24.4.2014, p. 18)

— Regulation (EU) 2015/1018 of 29 June 2015 laying down a list classifying occurrences in civil aviation to be mandatorily reported according to Regulation (EU) No 376/2014 of the European Parliament and of the Council (OJ L 163, 30.6.2015, p. 1)

— Regulation (EC) No 552/2004 of 10 March 2004 on the interoperability of the European Air Traffic Management network (the interoperability Regulation) (OJ L 96, 31.3.2004, p. 26)

— Regulation (EU) No 73/2010 of 26 January 2010 laying down the requirements on the quality of aeronautical data and aeronautical information for the single European sky (OJ L 23, 27.1.2010, p. 6)

— Regulation (EC) No 300/2008 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)

— 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)

— ISO 27000 Series on ‘information security management systems (ISMS)’ standards

— ISO 31000 Series on ‘risk management’ standards

— CEN — EN 16495 on standards for ‘Air Traffic Management — Information security for organisations supporting civil aviation operations’

— ECAC Document 30 ‘Recommendations on cyber security and supporting Guidance Material’

4. Related document

CRD 2019-07 'Management of information security risks'