European Union Aviation Safety Agency

Notice of Proposed Amendment 2019-07

Management of information security risks

RMT.0720

EXECUTIVE SUMMARY

The objective of this rulemaking task (RMT) is to efficiently contribute to the protection of the aviation system from cyberattacks and their consequences. To achieve this objective, this Notice of Proposed Amendments (NPA) proposes the introduction of provisions for the management of information security risks related to aeronautical information systems used in civil aviation. These provisions shall apply to competent authorities and organisations in all aviation domains (i.e. design, production, management of continuing airworthiness, maintenance, air operations, aircrew, air traffic management/air navigation services (ATM/ANS), and aerodromes), shall include high-level, performance-based requirements, and shall be supported by acceptable means of compliance (AMC), guidance material (GM), and industry standards.

NOTE: For the purpose of this NPA, information security risks are those that may compromise the confidentiality, integrity and availability of information being stored, transmitted or processed through the aeronautical information systems used in civil aviation.

Action area:	Emerging issues — safety and security		
Affected rules:	Regulations (EU) No 748/2012, No 1321/2014, 2017/373, 2015/340, No 139/2014, No 1178/2011 and No 965/2012 and related AMC and GM		
Affected stakeholders:	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); ATM/ANS providers; aerodrome operators; apron management service providers; Member States		
Driver:	Safety	**Rulemaking group:**	No
Impact assessment:	Light	**Rulemaking Procedure:**	Standard

Table of contents

1. About this NPA

1.1. How this NPA was developed

The European Union Aviation Safety Agency (EASA) developed this NPA 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) under RMT.0720. The text of this NPA has been developed by EASA in consultation with the European Strategic Coordination Platform (ESCP) for Cybersecurity in Aviation[3]. It is hereby submitted to all interested parties[4] for consultation.

1.2. How to comment on this NPA

Please submit your comments using the automated **Comment-Response Tool (CRT)** available at **http://hub.easa.europa.eu/crt/**[5].

The deadline for submission of comments is **27 September 2019**.

1.3. The next steps

Following the closing of the public commenting period, EASA will review all the comments received in coordination with the ESCP.

Based on the comments received, EASA will consider the need to issue amendments to Regulations (EU) No 748/2012[6], No 1321/2014[7], 2017/373[8], 2015/340[9], No 139/2014[10], No 1178/2011[11] and No 965/2012[12] as well as the need to develop new implementing and/or delegated regulations, and, if necessary, issue an opinion. A summary of the comments received will be provided in the Opinion.

---

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 In accordance with Article 115 of Regulation (EU) 2018/1139, and Articles 6(3) and 7 of the Rulemaking Procedure.

5 In case of technical problems, please contact the CRT webmaster (crt@easa.europa.eu).

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

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

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

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

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

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

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

The Opinion would be submitted to the European Commission, which will use it as a technical basis in order to take a decision on whether or not to amend the abovementioned Regulations.

If the Commission decides that the Regulations should be amended, EASA will further issue one or more Decisions amending the AMC and GM to comply with the amendments introduced into the Regulations.

The comments received on this NPA and the EASA responses to them will be reflected in a comment-response document (CRD). The CRD will be appended to the Opinion.

2. In summary — why and what

2.1. Why we need to change 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 allows 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. As a consequence, an accident or serious incident would only happen in the remote random event of several deficiencies happening simultaneously and, by chance, aligning themselves.

The concern, however, is that 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 and aeronautical information services (AIS) 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 come into play, and addressing them is the objective of this RMT.

NOTE: For the purpose of this NPA, information security risks are those that may compromise the confidentiality, integrity and availability of information being stored, transmitted or processed through the aeronautical information systems used in civil aviation.

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 and safety management systems (SMS) may be relevant for addressing information security risks. Nevertheless, certain adaptations are necessary in order to take into account the security aspects, in particular in relation to the concept of 'vulnerabilities' and the 'notion of intent' as well as the existence of sensitive information.

These adaptations need to take into account the fact that there is the intent and desire to damage aviation systems, to disrupt operations, or to threaten human lives. In other words, there are persons or entities that are intentionally looking for weaknesses in the system that can be exploited with the aim of creating harm. These potential weaknesses are not always known to the operators. Furthermore, in some cases, weaknesses may be intentionally combined to create a certain damage, potentially having in such cases catastrophic effects, although, when assessed individually, they could appear harmless. In other cases, weaknesses could be inadvertently exploited by malware spreading beyond their intended target, especially when good information security practices are neglected. Weaknesses can also be very different in nature: some related 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 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.

It is important to put this in a context where currently there are two EU regulatory frameworks, outside the scope of the Basic Regulation, that contain provisions related to information security.

These are the following:

— 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[13] (also called 'the NIS Directive'),

— Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security[14].

[13] 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/PDF/?uri=CELEX:32016L1148&qid=1557415901561&from=EN).

[14] 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/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1998&qid=1557416043097&from=EN).

However, these regulatory frameworks do not 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 aviation security.
— They do not cover all aviation domains and stakeholders:
  — The NIS Directive only covers those essential services defined by each Member State. As a consequence:
    — not all the aviation domains may be covered. For example, it is perfectly possible that in a particular Member State, ATM/ANS organisations, aerodromes and airlines 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 essential services by the Member State. For example, only the larger airports and airlines.

    Furthermore, the criteria used to identify those essential services will vary among the different Member States.
  — 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 that operate from premises located inside or outside airport premises and provide goods and/or services to or through airports with the objective to set the common rules and common basic standards on aviation security. Therefore, it does not cover all the possible entities whose dealings might have an impact on aviation safety.

Therefore, new rules are needed to address the safety impact of information security risks in a comprehensive and standardised manner across all the aviation domains.

At the same time, it is clear that, when developing these new requirements, it is essential to ensure that the different frameworks are complementary to each other in the effort to address safety and security matters, avoiding any duplications, inconsistencies or gaps.

Coming now to the question of what is the best timing to propose these amendments to the European aviation safety rules, the following has been taken into account:

— The fact that the NIS Directive is an EU directive and not an EU regulation means that it is not directly applicable in the Member States. Instead, it needs to be transposed into each national regulatory system.

  Also, according to the NIS Directive, it was only recently when the Member States were required to transpose it into their national systems, with a first deadline set for 9 May 2018 for the adoption and publication of the laws, regulations and administrative provisions necessary to comply with the NIS Directive, and a second deadline set for 9 November 2018 for the identification of the operators of essential services with an establishment on their territory.
— In addition to that, the Member States would need to establish in due time appropriate and detailed requirements and policies in order to comply with the requirements of the NIS Directive, in particular with its Article 14 where it is required that Member States ensure that operators of essential services manage the network and information security risks and notify

those incidents that have a significant impact on the continuity of the essential services provided.

Taking the above into account, one option considered was not to develop any new rules until the NIS Directive is fully transposed and implemented by all the Member States. This would allow to clearly know the detailed national requirements in each Member State before deciding on the detailed content of any future regulation.

However, the drawbacks of doing so were the following:

— Since the provisions contained in the NIS Directive are of a high level, the resulting detailed requirements and policies that would eventually be introduced in each Member State will vary across all the Member States. Therefore, waiting until all the Member States have fully transposed and implemented the NIS Directive created the risk of starting to work on the future rules when a fully non-standardised landscape, with very divergent requirements, had been already implemented across the EU.

— Furthermore, the slow pace at which some Member States have been transposing the NIS Directive and defining the detailed requirements and policies seemed to indicate that it could take several years until the work for the future aviation information security rules could start, which did not align with the urgency of the issue at stake.

Information on the state of play in the transposition and implementation of the NIS Directive across the Member States can be found at:

https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive

These drawbacks could be avoided by not delaying the RMT, since the national authorities responsible for the transposition of the NIS Directive would be able to use the material being developed in this RMT for the purpose of defining their national requirements and policies for the essential services in the aviation domain.

This would facilitate the standardisation of national requirements for essential services across the Member States, with the additional benefit of being aligned with the requirements that are being developed for all aviation domains in this RMT.

Considering the above, EASA decided not to delay this RMT.

Related safety issues

There are no safety recommendations (SRs) addressed to EASA pertinent to the scope of this RMT.

Exemptions[15] in accordance with Article 70 'Safeguard provisions'/Article 71 'Flexibility provisions' and/or Article 76 'Agency measures' of the Basic Regulation

There have been no exemptions pertinent to the scope of this RMT.

[15] Exemptions that have an impact on the development of this RMT's content and refer to:
- Article 70(1): Measures taken as an immediate reaction to a safety problem;
- Article 71(1): Limited in scope and duration exemptions from substantive requirements laid down in the Basic Regulation and its implementing rules in the event of urgent unforeseeable affecting persons or urgent operational needs of those persons;
- Article 71(3): Derogation from the rule(s) implementing the Basic Regulation where an equivalent level of protection to that attained by the application of the said rules can be achieved by other means;
- Article 76(7): Individual flight time specifications schemes deviating from the applicable certification specifications which ensure compliance with essential requirements and, as appropriate, the related implementing rules.

Alternative means of compliance (AltMoC) relevant to the scope of this RMT

There have been no AltMoC pertinent to the scope of this RMT.

ICAO and third-country references relevant to the scope of this RMT

Amendment 16 to ICAO Annex 17 adopted by the Council on 14 March 2018, and in particular its point 4.9 'Measures relating to cyber threats' has been considered during the development of this RMT.

References to differences between the scope of this RMT and ICAO SARPs, FARs, etc.

The proposed rules are aligned with the ICAO framework.

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 RMT is to efficiently contribute to the protection of the aviation system from cyberattacks and their consequences by ensuring that organisations and authorities involved in civil aviation activities are able to identify, protect from, detect, respond to and recover from those information security incidents that could potentially affect aviation safety.

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

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 is being developed in close coordination as well as full consultation and discussion with the ESCP.

This ESCP includes:

— an Executive Committee (ESCP-EC) at the higher, political 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, coherence and consistency of risk management processes, etc.).

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 Member 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:**
  - ICAO,
  - FAA and TCCA,
  - NATO,
  - Aerospace Industries Association of America (AIA),
  - Aerospace Industries Association of Canada (AIAC).

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

- The need to focus on the impact that information security threats and events could have on safety, regardless of whether this safety impact comes from a direct effect on the aircraft or as an indirect effect by affecting the normal functioning of the European Aviation Traffic Management Network (EATMN).
- The need to cover all aviation domains and their interfaces, since aviation is a system of systems.

— The need 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.

— The need to ensure compliance with related ICAO standards.

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

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

— The need 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.

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

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

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

A. OBJECTIVE AND SCOPE OF THE PROPOSED RULE

— **This NPA introduces requirements to be met by organisations involved in civil aviation activities, as well as by their competent authorities, in order to identify, protect from, detect, respond to and recover from those information security incidents which could potentially affect aviation safety.**

— **The focus is on the impact on aviation safety, regardless of whether this comes from a direct effect on the aircraft or as an indirect effect by affecting the normal functioning of the European Aviation Traffic Management Network (EATMN).**

NOTE: The EATMN is defined in Regulation (EC) No 552/2004[16] 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;

[16] 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/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0552&qid=1557420528736&from=EN).

- 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;
- systems and procedures for the use of meteorological information.

— **The legal basis for the introduction of these requirements is contained in the Basic Regulation, and in particular in its Article 62 paragraph (15)(c) and in Annexes II, IV, V, VII and VIII, which contain requirements for competent authorities and organisations regarding the implementation of management systems.**

— **These proposed requirements apply to the competent authorities and to the following organisations:**

- production organisations and design organisations that are required to comply with Subparts G and J respectively of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012[17]
- maintenance organisations that are required to comply with Section A of Annex II (Part-145) to Regulation (EU) No 1321/2014[18]
- continuing airworthiness management organisations that are required to comply with Section A of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014 (as per Opinion No 06/2016[19])
- air operators that are required to comply with Annex III (Part-ORO) to Regulation (EU) No 965/2012[20]
- aircrew training organisations (ATOs), aircrew aero-medical centres (AeMCs) and FSTD operators that are required to comply with Annex VII (Part-ORA) to Regulation (EU) No 1178/2011[21]
- ATCO training organisations (ATCO TOs) and ATCO aero-medical centres (AeMCs) that are required to comply with Annex III (Part ATCO.OR) to Regulation (EU) 2015/340[22]
- ATS, MET, AIS, DAT, CNS, ATFM and ASM providers and the Network Manager that are required to comply with Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373[23]

[17] https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32012R0748

[18] https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32014R1321

[19] Opinion No 06/2016 'Embodiment of safety management system (SMS) requirements into Commission Regulation (EU) No 1321/2014 — SMS in Part-M' (https://www.easa.europa.eu/document-library/opinions/opinion-062016).

[20] https://eur-lex.europa.eu/eli/reg/2012/965/2014-02-17

[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02011R1178-20140403

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

[23] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R0373

NOTE: Although Regulation (EU) 2017/373 is not fully applicable yet, it will be before EASA issues the final Opinion associated to this NPA.

— aerodrome operators and apron management service providers (as per Opinion No 02/2014[24]) that are required to comply with Annex III (Part-ADR.OR) to Regulation (EU) No 139/2014[25]

— **In order to ensure appropriate proportionality of the risks involved, the proposed requirements shall not apply to the following organisations:**

NOTE: An ELA2 aircraft is a manned European Light Aircraft[26], as defined in paragraph 2(j) of Article 1 of Regulation (EU) No 748/2012.

— production organisations and design organisations that are required to comply with Subparts G and J respectively of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012, if they are solely involved in the design and production of ELA2 aircraft

— 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))

— organisations that demonstrate their design capability in accordance with alternative procedures to Subpart J of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012

— organisations that perform maintenance and continuing airworthiness activities in accordance with Annex Vd (Part-CAO) to Regulation (EU) No 1321/2014 (as per Opinion No 05/2016[27])

— 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

---

[24] Opinion No 02/2014 'Requirements for apron management services at aerodromes' (https://www.easa.europa.eu/document-library/opinions/opinion-022014).

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0139

[26] '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 2 000 kg 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.

[27] https://www.easa.europa.eu/document-library/opinions/opinion-052016

— 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

— operators of unmanned aircraft systems (UASs) that belong to the 'open' and 'specific' categories (as per Opinion No 01/2018[28])

NOTE: According to Opinion No 01/2018, operators of UASs in the 'open' category do not require neither an authorisation nor a declaration in order to operate the UAS.

For operators of UASs in the 'specific' category, such authorisation or declaration is needed. And these operators have the option to obtain a 'Light UAS Operator Certificate (LUC)' on the basis of implementing a safety management system which will provide them 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 authorisation it suffices with 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).

For those reasons, these operators have been exempted from the rules proposed in this NPA, and in particular, from implementing an ISMS. However, this approach may be different in the future when rules are developed for operators of UASs in the 'certified' category.

In addition, a provision has been introduced in AISSS.OR.200(e), permitting the organisation to be temporarily exempted by the competent authority from implementing an ISMS if it demonstrates to the satisfaction of the competent authority that its activities, facilities and resources, as well as the equipment, systems and services it provides, maintains and operates, do not pose any information security risks neither to itself nor to other organisations. This exemption shall be based on a documented safety

[28] Opinion No 01/2018 'Unmanned aircraft system (UAS) operations in the 'open' and 'specific' categories' (https://www.easa.europa.eu/document-library/opinions/opinion-012018).

assessment performed by the organisation, and reviewed and approved by its competent authority.

This exemption will have a maximum duration of 1 year, and can be reissued for subsequent periods, each for a maximum of 1 year, on the basis of a new documented safety assessment as described above for each exemption and for each subsequent period.

— **In the case of third-country operators that are required to comply with Regulation (EU) No 452/2014[29], EASA decided that the new rule shall not apply to them. Nevertheless, these operators will be subject to the requirements imposed by the different Member States as a result of the provisions of point 4.9 'Measures relating to cyber threats' of Annex 17 to the ICAO Convention.**

— **It is important to note that the proposed requirements do not apply to organisations for which there are no organisation requirements within the existing implementing 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 there are organisation requirements. These organisations will have to take into account the information security risks associated to their contracted organisations and establish appropriate provisions in the contracts in order to address those risks.

— **Furthermore, the proposed requirements do not apply to those organisations which are outside the scope of the Basic Regulation.** This is, for example, the case of 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-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.

[29] https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32014R0452

B. STRUCTURE OF THE PROPOSED RULE

— **This NPA proposes the introduction of a new rule directly stemming from the Basic Regulation, which will address information security risks and will be applicable to all aviation domains** (airworthiness, operations, ATM/ANS, aerodromes, etc.). **Therefore, it could be seen as a 'horizontal' information security rule.**

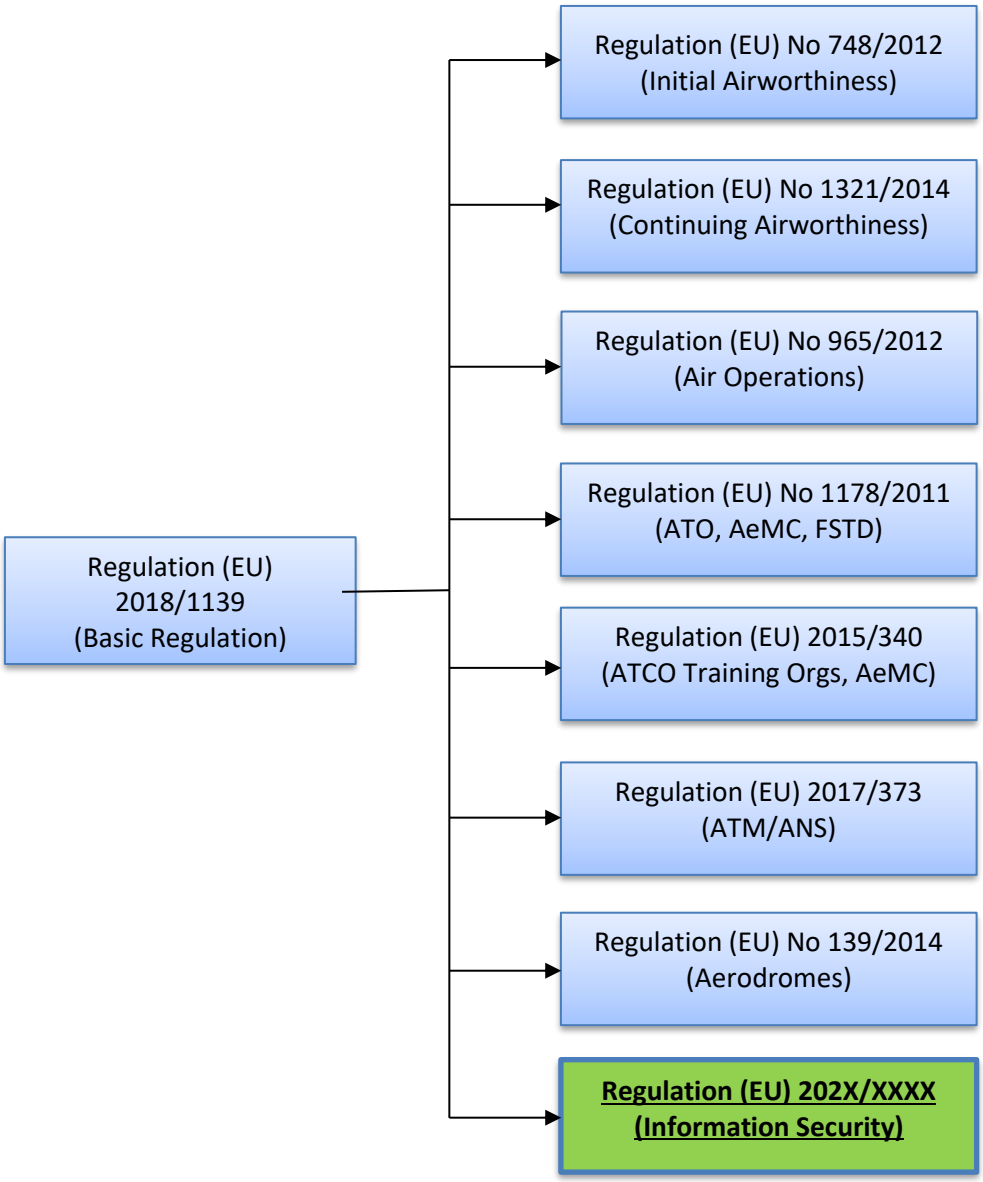
NOTE: In this NPA, this 'horizontal' rule applies to all aviation domains. However, in the final deliverable of this RMT (i.e. Opinion), EASA will divide this 'horizontal' rule in three sets of rules:

— one for those organisations for which the Basic Regulation provides that the detailed rules need to be adopted by means of delegated acts;

— one for those organisations for which the Basic Regulation provides that the detailed rules need to be adopted by means of implementing acts; and

— another one for all the competent authorities since, according to Article 62(15)(c) of the Basic Regulation, the detailed rules for their management systems need to be adopted by means of implementing acts.

In any case, it is envisaged that both rules applicable to organisations are identical.



— **This new draft regulation proposed in this NPA contains:**

  — **a 'cover regulation' (preamble and enacting terms (articles))** that contains the provisions related to objectives, scope, definitions, means of compliance, competent authority, and entry into force;

  — **an Annex I 'Part-AISS.AR — Authority Requirements' and an Annex II 'Part-AISS.OR — Organisation Requirements'** with the detailed authority and organisation requirements, including, among other things, the need to implement an information security management system (ISMS) and internal/external reporting schemes.

— **The requirements contained in this 'horizontal' information security rule will complement those related to management systems already contained in other implementing rules that are applicable to the affected organisations. As a consequence, they do not require a separate approval certificate/declaration. The organisation approval certificate/declaration will cover the requirements of the current approval and the requirements of the 'horizontal' rule.**

  For consistency purposes, cross references will be introduced in the existing implementing rules applicable to each domain in order to state that the organisations and competent authorities are also required to comply with the new 'horizontal' rule requirements in order to maintain their approval/declaration.

  Furthermore, for those domains where the existing implementing rules already include certain provisions related to information security (such as ATM/ANS and aerodromes), amendments have been proposed since those provisions will be superseded by the new 'horizontal' rule.

C. COMPETENT AUTHORITY

— **This NPA proposes that the competent authority that is already responsible for the organisation (for the already existing implementing rules) become also responsible for the implementation and enforcement of the new requirements proposed in this NPA.**

  This allows to have a single authority responsible for the organisation, ensuring that all the aspects related to aviation safety are appropriately considered. This also prevents disputes between different authorities regarding the validity of the organisation approval certificate.

  It also allows EASA to fulfil its standardisation oversight obligations on this competent authority. This would have been more difficult if the competent authority for the new requirements was, for example, a national information security agency responsible for the implementation of the national transposition of the NIS Directive, where there would likely be restrictions for EASA to access the necessary information in order to perform audits.

— **The proposed requirements include provisions to allow the competent authority to delegate tasks to qualified entities (for example, to a national information security**

agency). However, the requirements to be met by the organisation and by the qualified entity are still the ones contained in Part-AISS.OR and Part-AISS.AR respectively, and the responsibility remains with the competent authority, especially in order to ensure that the audits performed by the qualified entity take due consideration of the safety aspects.

This facilitates the access by the competent authority to additional information security expertise, and it provides flexibility to the State in order to create a national safety and security organisational structure that fits their needs.

— **EASA will be the competent authority for the 'horizontal' information security rule 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'**

Particular attention has been given to Pan-European approved organisations (like it is the case of EGNOS), for which the Security Accreditation Board (SAB) defined in Article 11 of Regulation (EU) No 512/2014[30] has certain functions when defining the security requirements to be met by the organisation. In those cases, appropriate coordination measures will need to be established between EASA and the SAB.

D. CONSISTENCY WITH OTHER REGULATORY FRAMEWORKS

— **Directive (EU) 2016/1148 (NIS Directive):**

  — **In order not to interfere with the national implementation of the NIS Directive, the proposed 'horizontal' rule gives the possibility to those organisations which have been identified as operators of essential services to not comply with Part-AISS.OR and, instead, comply with the nationally transposed Article 14 of the NIS Directive.** The only condition is that the competent authority that is responsible for the 'horizontal' information security rule (the NAA) and the competent authority that is responsible for the implementation of the nationally transposed NIS Directive shall coordinate the aspects related to aviation safety.

  — **Regarding the EASA standardisation oversight inspections, they will be performed only for the NAA, in order to verify how the NAA has implemented all the requirements related to the aviation safety approval of the organisation (the existing implementing rules).** For the elements related to information security, EASA will check how the NAA and the authority that is responsible for the national

[30] Regulation (EU) No 512/2014 of the European Parliament and of the Council of 16 April 2014 amending Regulation (EU) No 912/2010 setting up the European GNSS Agency (OJ L 150, 20.5.2014, p. 72) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0512&qid=1557739879640&from=EN).

transposition of the NIS Directive coordinate. However, EASA will not audit the authority that is responsible for the national transposition of the NIS Directive. If EASA finds that the coordination between the authorities is inappropriate, it will raise a finding in accordance with the applicable requirements.

— **Regulation (EU) 2015/1998 (aviation security) and Amendment 16 to ICAO Annex 17:**

— **The latest Amendment 16 to ICAO Annex 17, which became applicable in November 2018, has elevated certain provisions on measures relating to cyberthreats (point 4.9.1) from the category of 'recommendations' to the category of 'standards'.** This point now reads as follows:

'4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.'

— **In order to align with those new standards, the European Commission is currently in the process of amending Regulation (EU) 2015/1998.**

However, taking into account the scope of Regulation (EU) 2015/1998, and in particular its focus on aviation security and its link to the national civil aviation security programmes, it can be anticipated that the scope of these amendments may not cover all aviation domains and stakeholders, and may not fully address the effects on aviation safety.

— **On the other side, the 'horizontal' information security rule proposed in this NPA, as mentioned above, covers all aviation domains and it focuses on the effects on aviation safety.**

The above means that the 'horizontal' rule and Regulation (EU) 2015/1998 can be seen as complementary in order to achieve the objective to fully cover the safety and security aspects for the widest possible scope of organisations.

In order to achieve this, and in order to avoid duplications and inconsistencies, the 'horizontal' rule proposed in this NPA has also been developed with the aim to be fully aligned with the new 4.9.1 standard that is contained in Amendment 16 to ICAO Annex 17 whenever it relates to aviation safety, and it has been done in coordination with the efforts of the European Commission to amend Regulation (EU) 2015/1998.

— Taking into account those synergies, it can be anticipated that the information security management system developed by one organisation in order to meet the requirements of the 'horizontal' information security rule proposed in this NPA may be used totally or in part to meet the requirements of the amended Regulation (EU) 2015/1998.

And vice versa, it may be possible that certain elements of the organisation management system, which were developed in order to comply with Regulation

(EU) 2015/1998, could be used as a means to comply with the 'horizontal' information security rule.

E. PERFORMANCE- AND RISK-BASED APPROACH

— **The proposed 'horizontal' rule has been drafted by taking a high-level, performance- and risk-based approach, where AMC/GM material and existing industry standards will play a significant role in defining best practices.**

— **AMC/GM material and relevant industry standards:**

— The detailed content of the AMC/GM material will be developed during the coming months in coordination with the ESCP.

— This AMC/GM material will contain means and guidance on how to comply with the requirements contained in the 'horizontal' rule proposed in this NPA.

— For the purpose of developing the AMC/GM material, use will be made of the material contained in existing standards and best practices, such as:

— 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'.

— Existing material that is available within the Member States for the implementation of the NIS Directive will be considered during the development phase of the AMC/GM. If such material is found during the ESCP discussions to be useful for the wider aviation sector (not only within a particular Member State), it may be introduced in the AMC/GM so that it can be used by the relevant stakeholders in all Member States.

— The AMC/GM material may contain references to other industry standards, such as, for example:

— EUROCAE ED-201 'Aeronautical Information System Security (AISS) Framework Guidance';

— EUROCAE ED-205 'Process Standard for Security Certification and Declaration of Air Traffic Management/Air Navigation Services (ATM/ANS) Ground Systems'.

— **Although detailed discussions within the ESCP in relation to the AMC/GM material still have to take place, the need is already anticipated to develop AMC/GM material for the following key subjects:**

— **For Article 1 'Objective':**

What is the meaning of 'information security incidents which could potentially affect aviation safety':

Guidance is needed to explain that the effect on safety is regardless of whether it comes from a direct effect on the aircraft or as an indirect effect by affecting the normal functioning of the European Aviation Traffic Management Network (EATMN).

— **For Article 4 'Competent authority':**

What is the coordination expected between authorities:

AMC and GM is needed to explain what are the expectations as regards coordination between authorities for the following cases:

— when the NAA that is responsible for the organisation delegates certain tasks to qualified entities (such as a national information security agency);

— when, for organisations that provide essential services, the requirements followed are not those contained in Part-AISS.OR but those resulting from the nationally transposed Article 14 of the NIS Directive.

The AMC and GM should also cover the need for the State to define how to solve disputes between the different competent authorities.

— **For point AISS.OR.200 and AISS.AR.200 'Information security management system (ISMS)':**

Identification of interfaces with other organisations and performance of risk assessments:

AMC and GM is 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.

The outcome of the work performed within the ESCP Shared Trans-Organisational Risk Management (STORM) Work Stream will be essential for this.

Risk assessment of contracted activities:

AMC and GM is needed for the risk assessment of contracted activities, since the approved organisation will have to take into account the information security risks associated to their contracted activities and establish appropriate provisions in the contracts in order to address those risks.

Legacy aircraft and other legacy systems and technologies:

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

Small organisations:

AMC and GM is 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.

Maturity models:

AMC and GM is needed to provide examples of maturity models for each aviation domain (ATM/ANS, aerodromes, airworthiness, etc.). These maturity models should be useful, for example, for the following purposes:

— comparing the organisation to how it looked in the past, to track improvements over time;

— comparing the organisation to how it should look in the future after a road map of improvements has been completed;

— comparing the organisation's practices with other organisations, in order to develop and share good practices;

— assessing suppliers and supply chain maturity.

All the above is important in order to evaluate the risks associated to the organisations with which the organisation has an interface (STORM).

Refer to Appendix I for a draft example of a Maturity Matrix for the ATM/ANS domain. This matrix contains different subjects to be assessed as well as reference to examples of acceptable standards.

NOTE: This is just a draft example that may need to be further reviewed during the development of the AMC/GM material.

Risks attributed to aviation staff and evaluation of competences:

With the proposed requirements, the organisations will have to evaluate the information security risks that could be attributed to the activities and actions performed by their aviation staff (e.g. aircrew, mechanics, air traffic controllers, etc.), as well as identify whether they need additional training and skills.

AMC and GM may be needed in order to provide more details on how the risk exposure assessment should be done, and how to design a tailored competence scheme.

Temporary exemption of certain organisations from the requirement to have an ISMS:

AMC and GM is needed on how to perform the 'safety assessment' required by AISS.OR.200(e) in order to demonstrate to the competent authority that the organisation's activities, facilities and resources, as well as the equipment, systems and services it provides, maintains and operates, do not pose any information security risks neither to itself nor to other organisations.

— **For point AISS.OR.310 'External information security reporting scheme':**

Scope of reporting activities and associated procedures:

AMC and GM is needed on what should be reported and how.

— **For point AISS.OR.400 'Contracted activities':**

Control of contracted activities:

GM is needed to explain that this point relates to contracting of activities which are within the scope of the organisation, and not to the supply chain of products and systems (which are covered under point AISS.OR.200(a)(6)).

AMC is 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 to these contracted activities.

Particular reference should be included for the case of, for example, certain communication providers or groundhandling services providers who work as contractors under the control and accountability of the organisation.

F. INTEGRATION WITH OTHER MANAGEMENT SYSTEMS

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

G. ENTRY INTO FORCE AND TRANSITIONAL MEASURES

— Taking into account the publication date of this NPA and the need to evaluate the comments received during the public consultation phase, EASA expects to submit an Opinion (containing a final draft rule proposal) to the European Commission during the summer of 2020.

— Considering the need for such Opinion to undergo the corresponding adoption process at the European Commission, with the involvement of the Member States, it is not expected that the rule be adopted before the summer of 2021.

— Shortly after adoption, the rule should enter into force. However, certain transitional measures may need to be introduced in order to provide for some time for the implementation of the new rule by the authorities and organisations. A phased approach could be followed, depending on the different timing where authorities and organisations could be ready to apply the different requirements.

Request to stakeholders:

Stakeholders are invited to provide proposals on what would be a reasonable duration for such transitional measures.

A proposal received so far from some industry participants in the ESCP include the following:

— **Phase 1: Gap analysis (12 months)**

Key actions: Compare the existing security management system of the organisation with the Part-AISS ISMS requirements (including AMC) that are applicable to the organisation.

Objective: Identify the missing elements.

— **Phase 2: Definition, planning and preparation (18 months)**

Key actions: Have the security policy and objectives approved by the accountable manager and communicated inside the organisation. Establish responsibilities and support. Have an approved ISMS implementation plan.

Objective: Identify what needs to be done and by whom.

— **Phase 3: Development and deployment (24 months)**

Key actions: Establish data collection to feed security risk management and security assurance. Get security risk control and security performance assessment operational. Ensure training and security promotion.

Objective: Develop security culture and become compliant with the Part-AISS ISMS requirements.

Deliverable: Statement of compliance with Part-AISS (i.e. 24 months after the date of entry into force of the Regulation).

— **Phase 4: Continuous improvement**

Key action: Based on security performance monitoring and measurement, enhance ISMS performance by dedicated action plans.

Objective: Ensure ISMS performance and try to become even better.

— The AMC and GM material associated to the rule will be adopted by EASA immediately after the adoption of the rule by the European Commission.

2.4. What are the expected benefits and drawbacks of the proposals

NOTE: This is a summary of the expected benefits and drawbacks. For more details, please refer to the impact assessment (IA) in Section 4.

The expected benefits are the following:

- A more robust management system that ensures that organisations across all aviation domains systematically identify the areas exposed to information security risks, perform appropriate risk assessments, develop and implement measures to protect their critical systems, data and processes, continuously identify vulnerabilities and information security risks and take actions to mitigate them.
- An enhanced internal market and competitiveness due to the inclusion of standardised requirements for all aviation organisations in the different aviation domains.
- A more coordinated approach between different organisations within all the aviation domains, where the interfaces and the shared risks are properly evaluated.
- A more coordinated oversight approach between the different authorities in each Member State (NAAs, national information security authorities, ministries, etc.), which should reduce the total number of audits and the amount of conflicting requirements, facilitating a comprehensive approach where safety and security aspects are properly considered.
- Better defined internal and external reporting schemes that will facilitate the sharing of information, both inside the organisations as well as among organisations and authorities, at national and European level.
- Possible decrease of insurance costs.
- Increased skills and competences of the organisation staff, which should improve the overall productivity and efficiency of the organisations.
- Increase of employment opportunities and better economic conditions for the qualified personnel available in the labour market.
- Increase of business opportunities for educational institutions and organisations.

The expected drawbacks are the following:

- Aviation organisations may find difficulties in having access to a sufficient number of qualified personnel, possibly at increased cost.
- 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 information security management systems and event notification measures similar to the ones proposed by this NPA. These organisations should not be significantly impacted, moreover taking into account the possibility given to them in this NPA to replace the requirements of Part-AISS.OR by the requirements stemming from the nationally transposed NIS Directive.
- Other organisations, even when not affected 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, the economic impact will be of a medium scale due to the need to introduce some changes in order to fully comply with the proposed requirements.

— It will be those organisations which have not implemented any procedures and processes for the management of information security risks that will suffer the highest cost for the implementation of the proposed measures. This is expected to be the case of 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 NPA proposals, as well as the future AMC and GM material, are going to properly take into account the proportionality aspects linked to smaller organisations.

— Furthermore, the costs described above are expected to be mitigated by the introduction of appropriate transitional measures for the application of the proposed rules.

3. Proposed amendments

The text of the amendment is arranged to show deleted text, new or amended text as shown below:

— deleted text is ~~struck through~~;

— new or amended text is highlighted in blue;

— an ellipsis '[…]' indicates that the rest of the text is unchanged.

3.1. Draft regulation

Regulation (EU) No 748/2012 is amended as follows:

NOTE: This text already takes into account the amendments proposed in NPA 2019-05 'Embodiment of safety management system (SMS) requirements into Part-145 and Part 21'[31]

ANNEX I

PART 21

[…]

Contents

[…]

SUBPART G — PRODUCTION ORGANISATION APPROVAL

[…]

21.A.146 Information security

[…]

SUBPART J — DESIGN ORGANISATION APPROVAL

[…]

21.A.246 Information security

[…]

SECTION A

TECHNICAL REQUIREMENTS

[…]

SUBPART G — PRODUCTION ORGANISATION APPROVAL

[…]

21.A.146 Information security

The production organisation shall comply with Regulation (EU) 202X/XXXX.

[…]

31 https://www.easa.europa.eu/document-library/notices-of-proposed-amendment/npa-2019-05

SUBPART H — DESIGN ORGANISATION APPROVAL

[…]

21.A.246 Information security

The design organisation shall comply with Regulation (EU) 202X/XXXX.

[…]

SECTION B

PROCEDURES FOR COMPETENT AUTHORITIES

21.B.5 Scope

~~(a) This Section establishes the procedure for the competent authority of the Member State when exercising its tasks and responsibilities concerned with the issuance, maintenance, amendment, suspension and revocation of certificates, approvals and authorisations referred to in this Annex I (Part 21).~~

~~(b) The Agency shall develop in accordance with Article 19 of Regulation (EC) No 216/2008 certification specifications and guidance material to assist Member States in the implementation of this Section.~~

This Section, together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX, establish the administrative and management system requirements to be followed by the competent authority that is in charge of the implementation and enforcement of Section A of this Annex.

Regulation (EU) No 1321/2014 is amended as follows:

NOTE: This text already takes into account the amendments that are expected to be adopted to Regulation (EU) No 1321/2014 as a result of the proposals contained in Opinion No 05/2016 and Opinion No 06/2016, which are currently in the adoption process at the European Commission.

It also takes into account the amendments proposed in NPA 2019-05 'Embodiment of safety management system (SMS) requirements into Part-145 and Part 21'.

ANNEX II

(PART-145)

CONTENTS

[…]

145.A.72 Information security

[…]

SECTION A

TECHNICAL REQUIREMENTS

[…]

145.A.72 Information security

The maintenance organisation shall comply with Regulation (EU) 202X/XXXX.

[…]

SECTION B

PROCEDURE FOR COMPETENT AUTHORITIES

145.B.01 Scope

~~This section establishes the administrative procedures which the competent authority shall follow when exercising its tasks and responsibilities regarding issuance, continuation, change, suspension or revocation of approvals of maintenance organisations under this Annex (Part-145).~~

This Section, together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX, establish the administrative and management system requirements to be followed by the competent authority that is in charge of the implementation and enforcement of Section A of this Annex.

ANNEX Vc

[PART-CAMO]

CONTENTS

SECTION A

ORGANISATION REQUIREMENTS

[…]

CAMO.A.330 Information security

The continuing airworthiness management organisation shall comply with Regulation (EU) 202X/XXXX.

SECTION B

AUTHORITY REQUIREMENTS

CAMO.B.005 Scope

This ~~s~~Section, together with the requirements contained in Annex I (Part-AISS.AR) to Regulation 202X/XXXX, establish~~es~~ the administrative and management system requirements to be followed by the competent authority that is in charge of the implementation and enforcement of Section A of this Annex.

Regulation (EU) No 965/2012 is amended as follows:

ANNEX II

AUTHORITY REQUIREMENTS FOR AIR OPERATIONS

[PART-ARO]

ARO.GEN.005 Scope

This Annex, together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX, establish~~es~~ the requirements for the administration and management system to be fulfilled by the Agency and the Member States for the implementation and enforcement of Regulation ~~(EC) No 216/2008~~ (EU) 2018/1139 and its Implementing and Delegated Rules regarding civil aviation air operations.

[…]

ANNEX III

ORGANISATION REQUIREMENTS FOR AIR OPERATIONS

[PART-ORO]

[…]

ORO.SEC.110 Information security

Air operators listed under point ORO.GEN.005 shall comply with Regulation (EU) 202X/XXXX.

Regulation (EU) No 1178/2011 is amended as follows:

ANNEX VI

AUTHORITY REQUIREMENTS FOR AIRCREW

[PART-ARA]

[…]

ARA.GEN.110 Information security

This Annex, together with the requirements contained in Annex I (Part-AISS.AR) to Regulation 202X/XXXX, establish the requirements for the administration and management system to be fulfilled by the Agency and the Member States for the implementation and enforcement of Regulation (EU) 2018/1139 and its implementing and delegated acts regarding aircrew.

[…]

ANNEX VII

ORGANISATION REQUIREMENTS FOR AIRCREW

[PART-ORA]

[…]

ORA.GEN.225 Information security

The organisation shall comply with Regulation (EU) 202X/XXXX.

[…]

Regulation (EU) 2015/340 is amended as follows:

ANNEX II

PART ATCO.AR

REQUIREMENTS FOR COMPETENT AUTHORITIES

[…]

ATCO.AR.A.001 Scope

This Part, set out in this Annex, together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX, establish~~es~~ the administrative requirements applicable to the competent authorities with responsibility for the issue, maintenance, suspension or revocation of licences, ratings, endorsements and medical certificates for air traffic controllers and certification and oversight of training organisations and aero-medical centres.

[…]

ANNEX III

PART ATCO.OR

REQUIREMENTS FOR AIR TRAFFIC CONTROLLER TRAINING ORGANISATIONS AND AERO-MEDICAL CENTRES

[…]

ATCO.OR.C.030 Information security

Training organisations shall comply with Regulation (EU) 202X/XXXX.

[…]

ATCO.OR.E.001 Aero-medical centres

Aero-medical centres (AeMCs) shall apply the provisions of Subparts ORA.GEN and ORA.AeMC of Annex VII to Commission Regulation (EU) No 290/2012 ([1]), with:

(a) all references to class 1 to be replaced with class 3; and

(b) all references to Part MED to be replaced with Part ATCO.MED.

In addition, they shall comply with Regulation (EU) 202X/XXXX.

Regulation (EU) 2017/373 is amended as follows:

ANNEX II

REQUIREMENTS FOR COMPETENT AUTHORITIES — OVERSIGHT OF SERVICES AND OTHER ATM NETWORK FUNCTIONS

(Part-ATM/ANS.AR)

[…]

ATM/ANS.AR.A.001 Scope

This Annex, together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX, establish~~es~~ the requirements for the administration and management systems of the competent authorities responsible for certification, oversight and enforcement in respect of the application of the requirements set out in Annexes III to XIII by the service providers in accordance with Article 6.

[…]

ANNEX III

COMMON REQUIREMENTS FOR SERVICE PROVIDERS

(Part-ATM/ANS.OR)

[…]

ATM/ANS.OR.B.040 Information security

Service providers shall comply with Regulation (EU) 202X/XXXX.

[…]

ATM/ANS.OR.D.010 Security management

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

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

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

(b) The security management system shall define:

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

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

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

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

~~(d) Air navigation services and air traffic flow management providers and the Network Manager shall take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cyber security threats which may have an unlawful interference with the provision of their service.~~

(d) The aspects related to information security, and in particular those related to aeronautical data and aeronautical information, shall be managed in accordance with point ATM/ANS.OR.B.040.

Regulation (EU) No 139/2014 is amended as follows:

ANNEX II

Part Authority Requirements — Aerodromes (Part-ADR.AR)

[…]

ADR.AR.A.001 Scope

This Annex, together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX, establish~~es~~ the requirements for the Competent Authorities involved in the certification and oversight of aerodromes, aerodrome operators and apron management service providers.

[…]

ANNEX III

Part Organisation Requirements — Aerodrome Operators (Part-ADR.OR)

[…]

ADR.OR.D.007 Management of aeronautical data and aeronautical information

NOTE: This text already takes into account the amendments that are expected to be adopted to Regulation (EU) No 139/2014 as a result of the proposals contained in Opinion No 02/2018[32], which is currently in the adoption process at the European Commission.

(a) As part of its management system, the aerodrome operator shall implement and maintain a quality management system covering the following activities:

(1) its aeronautical data activities; and

(2) its aeronautical information provision activities.

~~(b) The aerodrome operator shall, as part of its management system, establish a security management system to ensure the security of operational data it receives, or produces, or otherwise employs, so that access to that operational data is restricted only to those authorised.~~

~~(c) The security management system shall define the following elements:~~

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

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

[32] Opinion No 02/2018 'Specific requirements for providers of meteorological services, aeronautical information services/aeronautical information management, and flight procedure design services; common rules for airspace structure design' (https://www.easa.europa.eu/document-library/opinions/opinion-022018).

~~(3) the means of controlling the effects of security breaches and of identifying recovery action and mitigation procedures to prevent reoccurrence.~~

~~(d) The aerodrome operator shall ensure the security clearance of its personnel with respect to aeronautical data security.~~

~~(e) The aerodrome operator shall take the necessary measures to protect its aeronautical data against cyber security threats.~~

(d) The aspects related to information security, and in particular those related to aeronautical data and aeronautical information, shall be managed in accordance with point ADR.OR.D.035.

[…]

ADR.OR.D.035 Information security

The aerodrome operator shall comply with Regulation (EU) 202X/XXXX.

[…]

COMMISSION REGULATION (EU) 202X/XXXX

of XX Month 202X

on the introduction of organisation requirements for the management of information security risks related to aeronautical information systems used in civil aviation

(Text with EEA relevance)

[PREAMBLE]

Article 1

Objective

This Regulation establishes the requirements to be met by organisations and competent authorities involved in civil aviation activities in order to identify, protect from, detect, respond to and recover from those information security incidents which could potentially affect aviation safety.

Article 2

Scope

1. This Regulation applies to:
   (a) production organisations and design organisations that are required to comply with Subparts G and J respectively of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012;
   (b) maintenance organisations that are required to comply with Section A of Annex II (Part-145) to Regulation (EU) No 1321/2014;
   (c) continuing airworthiness management organisations (CAMOs) that are required to comply with Section A of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014;
   (d) air operators that are required to comply with Annex III (Part-ORO) to Regulation (EU) No 965/2012;
   (e) aircrew training organisations (ATOs), aircrew aero-medical centres and FSTD operators that are required to comply with Annex VII (Part-ORA) to Regulation (EU) No 1178/2011;
   (f) air traffic controller training organisations (ATCO TOs) and ATCO aero-medical centres that are required to comply with Annex III (Part ATCO.OR) to Regulation (EU) 2015/340;
   (g) ATS, MET, AIS, DAT, CNS, ATFM and ASM providers and the Network Manager that are required to comply with Annex III (Part-ATM/ANS.OR) to Regulation (EU) 2017/373;
   (h) aerodrome operators and apron management service providers that are required to comply with Annex III (Part-ADR.OR) to Regulation (EU) No 139/2014.
2. By way of derogation from paragraph 1, this Regulation shall not apply to the following organisations:
   (a) production organisations and design organisations that are required to comply with Subparts G and J respectively of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012, if they are solely involved in the design and production of ELA2 aircraft;
   (b) 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;

(c) 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;

(d) 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;

(e) 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.

3. By way of derogation from paragraph 1, organisations listed in paragraph 1 that have been identified by a Member State as operators of essential services in accordance with the nationally transposed Directive (EU) 2016/1148 may replace compliance with the organisation requirements contained in Annex II (Part-AISS.OR) to this Regulation by compliance with the elements contained in the national transposition of Article 14 of Directive (EU) 2016/1148, provided the competent authority that is responsible for this Regulation and the competent authority that is defined in the nationally transposed Directive (EU) 2016/1148 establish an agreement to coordinate the aspects that impact on aviation safety.

4. This Regulation also applies to the authorities that are responsible for the implementation and enforcement of the regulations listed in paragraph 1.

Article 3

Definitions

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

(a) ‘accountable manager’ means the same person who already performs in the organisation the functions of the accountable manager, or in the case of design organisations the functions of the head of the design organisation, in accordance with the corresponding regulation detailed in Article 2(1);

(b) ‘contracted activities’ means any activity within the scope of the approved organisation’s operations, in accordance with the terms of an approval or certificate, that is performed by other organisations that are either themselves certified to carry out such activity or, if not certified, work under the oversight of the approved organisation;

(c) ‘ELA2 aircraft’ means a manned European Light Aircraft as defined in Article 1 of Regulation (EU) No 748/2012;

(d) ‘information security’ means the preservation of confidentiality, integrity and availability of information;

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

(f) ‘information security incident’ means a single or a series of unwanted or unexpected information security events which could potentially affect aviation safety;

(g) ‘information security risk’ means the risk to organisational operations, assets, individuals and other organisations due to the potential of an information security breach;

(h) ‘security control’ means a measure, including any process, policy, device, practice or other action, that modifies a risk.

(i) 'threat' means the potential cause of an unwanted incident, which can result in harm to a system or organisation;

(j) 'vulnerability' means a weakness of an asset or a security control that can be exploited by one or more threats or inadvertent action.

Article 4

Competent authority

Without prejudice to the tasks related to aviation security entrusted to the Security Accreditation Board (SAB) defined in Article 11 of Regulation (EU) No 512/2014 in the case of European Global Navigation Satellite Systems (GNSS), the competent authority responsible for the implementation and enforcement of this Regulation shall be the same as the competent authority that is already responsible for the implementation and enforcement of the corresponding regulation detailed in Article 2(1).

Article 5

Entry into force

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

It shall apply from [*XX months after date of entry into force*].

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

ANNEX I

AERONAUTICAL INFORMATION SYSTEM SECURITY — AUTHORITY REQUIREMENTS

[PART-AISS.AR]

AISS.AR.005 Objective

This Section establishes the administrative and management system requirements to be followed by the competent authorities that are in charge of the implementation and enforcement of the organisation requirements contained in Annex II (Part-AISS.OR) to this Regulation.

AISS.AR.100 Personnel requirements

(a) The competent authority shall have a process in place to plan the availability of staff to ensure that it has sufficient and appropriately qualified staff to perform the activities related to Annex I (Part-AISS.AR) to this Regulation.

(b) The competent authority shall have a process in place to check a person's identity and previous experience, including, where legally permissible, any criminal records, as part of the assessment of an individual's suitability to implement a security control and/or for unescorted access to sensitive areas within the competent authority's organisation.

(c) The competent authority shall establish the competences that are required for competent authority personnel involved in the aviation information systems security roles and shall have a process in place to manage those competences. In addition to the necessary expertise related to the job function, competence must include an understanding of information security management.

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

(a) The competent authority shall establish, implement, maintain and continuously improve the information security management system (ISMS) aimed at identifying, protecting from, detecting, responding to and recovering from any information security incident within the objective of Article 1.

The ISMS shall:

(1) define the lines of responsibility and accountability throughout its organisation, including the direct accountability of the top management;

(2) contain an information security policy which describes the overall philosophies and principles of the organisation with regard to information security;

(3) identify the organisation activities, facilities and resources, the systems it operates and maintains and the services it provides, which could be exposed to information security risks;

(4) identify the interfaces with other organisations with which it shares information security risks;

(5) take into account the information security risks inherent to the organisation facilities and activities, to the systems it operates and maintains, to the services it provides, and to its interactions with other organisations;

(6) take into account the information security risks inherent to the use of equipment, systems and services provided to the organisation;

(7) identify the critical information and communications technology systems, data and processes used for civil aviation purposes;

(8) perform information security risk assessments, both initially and when changes to the security environment occur, of all identified critical systems, data and processes;

(9) based on the outputs of the risks assessments, the ISMS shall:

(i) develop and implement measures to protect the critical systems, data and processes; and

(ii) continuously identify vulnerabilities and information security risks to the critical systems, data and processes, take actions to mitigate any unacceptable risks and exploitable vulnerabilities, and verify the continued effectiveness of the protection of critical systems, data and processes;

(10) describe how the organisation ensures that personnel have the skills and competences to perform their tasks;

(11) include documentation of all management system key processes and procedures, including a process for making personnel aware of their responsibilities and the procedure for amending this documentation;

(12) include a function to monitor compliance of the organisation with the relevant requirements, which shall include a feedback system of findings to the top management to ensure effective implementation of corrective actions as necessary; and

(13) protect the confidentiality of any information that the ISMS may contain related to particular organisations, as well as the information received through the external and internal reporting schemes.

(b) The ISMS shall correspond to the nature and complexity of the competent authority and its

activities.

(c) The performance and effectiveness of the ISMS shall be assessed at planned intervals, and appropriate action shall be taken in a timely manner to address inefficiencies and improve its overall performance.

(d) The competent authority of the Member State shall notify the Agency of changes that affect its capability to perform its tasks and discharge its responsibilities as defined in this Regulation.

(e) The competent authority may integrate the ISMS with other management systems it has already implemented.

AISS.AR.400 Allocation of tasks to qualified entities

(a) Tasks related to the implementation of this Regulation may be allocated by the competent authority to qualified entities as described in Article 69 of Regulation (EU) 2018/1139.

(b) The competent authority shall ensure that the identification of information security risks, the information security risk assessment process and the internal audit process required by AISS.AR.200(a)(5), (a)(6), (a)(9) and (c) cover all certification or continuing oversight tasks performed by the qualified entities on its behalf.

AISS.AR.500 Record keeping

(a) The competent authority shall establish a system of record keeping where information is identified according to its security classification level. The record-keeping system shall allow adequate storage, accessibility, and reliable traceability of:

(1) the documented policies and procedures of its ISMS;

(2) the training, qualification, and authorisation of the personnel referred to in AISS.AR.100;

(3) the allocation of tasks to qualified entities, covering the elements required by AISS.AR.400, as well as the details of the allocated tasks;

(4) continuing oversight of certified organisations, including:

(i) all assessment, audit and inspection records;

(ii) any exemption issued in accordance with AISS.OR.200(e) together with the records of the safety assessment;

iii) a copy of the oversight programme listing the dates when audits are due and when audits were carried out;

(iv) copies of all formal correspondence;

(v) details of findings, corrective actions, date of action closure, any exemption and enforcement actions;

(vi) any assessment, audit and inspection reports issued by another competent authority;

(vii) copies of all organisation ISMMs and amendments to them; and

(viii) copies of any other document approved by the competent authority;

(5) the evaluation and notification to the Agency of alternative means of compliance proposed by organisations, and the assessment of the alternative means of compliance used by the competent authority itself;

(6) safety information and follow-up measures in accordance with AISS.AR.620; and

(7) the use of flexibility provisions in accordance with Regulation (EU) 2018/1139.

(b) All records shall be kept for a minimum period of 5 years while ensuring compliance with applicable data protection law.

AISS.AR.600 Oversight

NOTE: This text already takes into account the amendments proposed in NPA 2019-05 'Embodiment of safety management system (SMS) requirements into Part-145 and Part 21'.

The competent authority shall comply with the following requirements:

(a) for production organisations: point 21.B.221 of Section B of Annex I (Part 21) to Regulation (EU) No 748/2012;

(b) for design organisations: point 21.B.431 of Section B of Annex I (Part 21) to Regulation (EU) No 748/2012;

(c) for maintenance organisations: point 145.B.300 of Section B of Annex II (Part-145) to Regulation (EU) No 1321/2014;

(d) for continuing airworthiness management organisations (CAMOs): point CAMO.B.300 of Section B of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014;

(e) for air operators: point ARO.GEN.300 of Annex II (Part-ARO) to Regulation (EU) No 965/2012;

(f) for aircrew training organisations (ATOs), aircrew and ATCO aero-medical centres and FSTD operators: point ARA.GEN.300 of Annex VI (Part-ARA) to Regulation (EU) No 1178/2011;

(g) for air traffic controller training organisations (ATCO TOs): point ATCO.AR.C.001 of Annex II (Part ATCO.AR) to Regulation (EU) 2015/340;

(h) for providers of air traffic services (ATS), meteorological services (MET), aeronautical information services (AIS), data services (DAT), communications, navigation and surveillance services (CNS), air traffic flow management services (ATFM) and aviation services management (ASM) and the Network Manager: point ATM/ANS.AR.C.010 of Annex II (Part-ATM/ANS.AR) to Regulation (EU) 2017/373;

(i) for aerodrome operators and apron management service providers: point ADR.AR.C.005 of Annex II (Part-ADR.AR) to Regulation (EU) No 139/2014.

AISS.AR.610 Oversight programme

NOTE: This text already takes into account the amendments proposed in NPA 2019-05 'Embodiment of safety management system (SMS) requirements into Part-145 and Part 21'.

The competent authority shall comply with the following requirements:

(a) for production organisations: point 21.B.222 of Section B of Annex I (Part 21) to Regulation (EU) No 748/2012;

(b) for design organisations: point 21.B.432 of Section B of Annex I (Part 21) to Regulation (EU) No 748/2012;

(c) for maintenance organisations: point 145.B.305 of Section B of Annex II (Part-145) to Regulation

(EU) No 1321/2014;

(d) for continuing airworthiness management organisations: point CAMO.B.305 of Section B of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014;

(e) for air operators: point ARO.GEN.305 of Annex II (Part-ARO) to Regulation (EU) No 965/2012;

(f) for aircrew training organisations (ATOs), aircrew and ATCO aero-medical centres and FSTD operators: point ARA.GEN.305 of Annex VI (Part-ARA) to Regulation (EU) No 1178/2011;

(g) for air traffic controller training organisations (ATCO TOs): point ATCO.AR.C.005 of Annex II (Part ATCO.AR) to Regulation (EU) 2015/340;

(h) for providers of air traffic services (ATS), meteorological services (MET), aeronautical information services (AIS), data services (DAT), communications, navigation and surveillance services (CNS), air traffic flow management services (ATFM) and aviation services management (ASM) and the Network Manager: point ATM/ANS.AR.C.015 of Annex II (Part-ATM/ANS.AR) to Regulation (EU) 2017/373;

(i) for aerodrome operators and apron management service providers: point ADR.AR.C.010 of Annex II (Part-ADR.AR) to Regulation (EU) No 139/2014.

AISS.AR.620 Information to the Agency

(a) The competent authority of the Member State shall without undue delay notify the Agency in case of any significant problems with the implementation of this Regulation.

(b) The competent authority of the Member State shall provide the Agency with safety-significant information stemming from the information security reports it has received pursuant to point AISS.OR.310.

AISS.AR.630 Immediate reaction to an information security problem with safety impact

(a) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, the competent authority shall implement a system to appropriately collect, analyse, and disseminate information related to information security problems with safety impact.

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

(c) Upon receiving the information referred to in (a) and (b), the competent authority shall take adequate measures to address the information security problem with safety impact.

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

AISS.AR.800 Assessment of changes to organisations

NOTE: This text already takes into account the amendments proposed in NPA 2019-05 'Embodiment of safety management system (SMS) requirements into Part-145 and Part 21'.

The competent authority shall comply with the following requirements:

(a) for production organisations: point 21.B.240 of Section B of Annex I (Part 21) to Regulation (EU) No 748/2012;

(b) for design organisations: point 21.B.435 of Section B of Annex I (Part 21) to Regulation (EU) No 748/2012;

(c) for maintenance organisations: point 145.B.330 of Section B of Annex II (Part-145) to Regulation (EU) No 1321/2014;

(d) for continuing airworthiness management organisations (CAMOs): point CAMO.B.330 of Section B of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014;

(e) for air operators: point ARO.GEN.330 of Annex II (Part-ARO) to Regulation (EU) No 965/2012;

(f) for aircrew training organisations (ATOs), aircrew and ATCO aero-medical centres and FSTD operators: point ARA.GEN.330 of Annex VI (Part-ARA) to Regulation (EU) No 1178/2011;

(g) for air traffic controller training organisations (ATCO TOs): point ATCO.AR.E.010 of Annex II (Part ATCO.AR) to Regulation (EU) 2015/340;

(h) for providers of air traffic services (ATS), meteorological services (MET), aeronautical information services (AIS), data services (DAT), communications, navigation and surveillance services (CNS), air traffic flow management services (ATFM) and aviation services management (ASM) and the Network Manager: points ATM/ANS.AR.C.025, ATM/ANS.AR.C.030, ATM/ANS.AR.C.035 and ATM/ANS.AR.C.040 of Annex II (Part-ATM/ANS.AR) to Regulation (EU) 2017/373;

(i) for aerodrome operators and apron management service providers: point ADR.AR.C.040 of Annex II (Part-ADR.AR) to Regulation (EU) No 139/2014.

AISS.AR.900 Findings and corrective actions

NOTE: This text already takes into account the amendments proposed in NPA 2019-05 'Embodiment of safety management system (SMS) requirements into Part-145 and Part 21'.

Regarding findings and corrective actions, the competent authority shall comply with the following requirements:

(a) for production organisations: point 21.B.225 of Section B of Annex I (Part 21) to Regulation (EU) No 748/2012;

(b) for design organisations: point 21.B.433 of Section B of Annex I (Part 21) to Regulation (EU) No 748/2012;

(c) for maintenance organisations: point 145.B.350 of Section B of Annex II (Part-145) to Regulation (EU) No 1321/2014;

(d) for continuing airworthiness management organisations (CAMOs): point CAMO.B.350 of Section B of Annex Vc (Part-CAMO) to Regulation (EU) No 1321/2014;

(e) for air operators: points ARO.GEN.350, ARO.GEN.355 and ARO.GEN.360 of Annex II (Part-ARO)

to Regulation (EU) No 965/2012;

(f) for aircrew training organisations (ATOs), aircrew and ATCO aero-medical centres and FSTD operators: points ARA.GEN.350 and ARA.GEN.355 of Annex VI (Part-ARA) to Regulation (EU) No 1178/2011;

(g) for air traffic controller training organisations (ATCO TOs): points ATCO.AR.C.010 and ATCO.AR.E.015 of Annex II (Part ATCO.AR) to Regulation (EU) 2015/340;

(h) for providers of air traffic services (ATS), meteorological services (MET), aeronautical information services (AIS), data services (DAT), communications, navigation and surveillance services (CNS), air traffic flow management services (ATFM) and aviation services management (ASM) and the Network Manager: point ATM/ANS.AR.C.050 of Annex II (Part-ATM/ANS.AR) to Regulation (EU) 2017/373;

(i) for aerodrome operators and apron management service providers: point ADR.AR.C.055 of Annex II (Part-ADR.AR) to Regulation (EU) No 139/2014.

ANNEX II

AERONAUTICAL INFORMATION SYSTEM SECURITY — ORGANISATION REQUIREMENTS

[PART-AISS.OR]

AISS.OR.005 Scope

The requirements contained in this Section apply to the organisations listed in Article 2 of this Regulation.

AISS.OR.100 Personnel requirements

(a) The accountable manager of the organisation shall have corporate authority to establish and maintain the organisation's information security management system and shall be responsible for:

(1) ensuring that all necessary resources are available to manage information security in accordance with Annex II (Part-AISS.OR) to this Regulation;

(2) establishing and promoting the information security policy specified in point AISS.OR.200;

(3) nominating a person, or group of persons, who are ultimately responsible to the accountable manager, with the responsibility for managing the compliance monitoring function as part of the information security management system;

(4) nominating a person, or group of persons, who are ultimately responsible to the accountable manager, with the responsibility for managing the development, administration, and maintenance of effective information security management processes as part of the management system;

(5) ensuring that the person, or group of persons, nominated in accordance with points AISS.OR.100(a)(3) and (a)(4) have direct access to the accountable manager so that the accountable manager is kept properly informed of compliance and information security matters; and

(6) demonstrating a basic understanding of Annex II (Part-AISS.OR) to this Regulation.

(b) The person, or group of persons, nominated in accordance with points AISS.OR.100(a)(3) and (4) shall demonstrate relevant knowledge, background, and satisfactory experience related to aviation information system security and demonstrate a working knowledge of this Part.

(c) The organisation shall have a process in place to plan the availability of staff to ensure that the organisation has sufficient and appropriately qualified staff to perform the activities related to Annex II (Part-AISS.OR) to this Regulation.

(d) The organisation shall have a process in place to check a person's identity and previous experience, including, where legally permissible, any criminal records, as part of the assessment of an individual's suitability to implement a security control and/or for unescorted access to sensitive areas within the organisation.

(e) The organisation shall establish the competences required for personnel involved in the aviation information systems security roles and shall have a process in place to manage those competences. In addition to the necessary expertise related to the job function, competence must include an understanding of information security management.

AISS.OR.200 Information security management system (ISMS)

(a) The organisation shall establish, implement, maintain and continuously improve the information security management system (ISMS) aimed at identifying, protecting from, detecting, responding to and recovering from any information security incident within the objective of Article 1.

The ISMS shall:

(1) define the lines of responsibility and accountability throughout the organisation, including the direct accountability of the accountable manager;

(2) contain an information security policy which describes the overall philosophies and principles of the organisation with regard to information security;

(3) identify the organisation activities, facilities and resources, as well as the equipment, systems and services it provides, maintains and operates, which could be exposed to information security risks;

(4) identify the interfaces with other organisations with which it shares information security

risks;

(5) take into account the information security risks inherent to the organisation facilities and activities, to the equipment, systems and services it provides, maintains and operates, and to its interactions with other organisations;

(6) take into account the information security risks inherent to the use of equipment, systems and services provided to the organisation;

(7) identify the critical information and communications technology systems, data and processes used for civil aviation purposes;

(8) perform information security risk assessments, both initially and when changes to the security environment occur, of all identified critical systems, data and processes;

(9) based on the outputs of the risks assessments, the ISMS shall:

(i) develop and implement measures to protect the critical systems, data and processes; and

(ii) continuously identify vulnerabilities and information security risks to the critical systems, data and processes, take actions to mitigate any unacceptable risks and exploitable vulnerabilities, and verify the continued effectiveness of the protection of critical systems, data and processes;

(10) describe how the organisation ensures that personnel have the skills and competences to perform their tasks;

(11) include documentation of all management system key processes and procedures, including a process for making personnel aware of their responsibilities and the procedure for amending this documentation;

(12) include a function to monitor compliance of the organisation with the relevant requirements, which shall include a feedback system of findings to the accountable manager to ensure effective implementation of corrective actions as necessary; and

(13) implement security measures that have been notified by the competent authority of the Member State or the Agency under AISS.AR.630.

(b) The ISMS shall correspond to the risks inherent to the nature and complexity of the organisation and its activities.

(c) The performance and effectiveness of the ISMS shall be assessed at planned intervals, and appropriate action shall be taken in a timely manner to address inefficiencies and improve its overall performance.

(d) The organisation may integrate the ISMS with other management systems it has already implemented.

(e) By way of derogation from paragraphs (a), (b), (c) and (d), the organisation may be exempted by the competent authority from implementing an ISMS if it demonstrates to the satisfaction of such competent authority that its activities, facilities and resources, as well as the equipment, systems and services it provides, maintains and operates, do not pose any information security risks neither to itself nor to other organisations. This exemption shall be based on a documented safety assessment performed by the organisation, and reviewed and approved by its competent authority.

This exemption will have a maximum duration of 1 year, and can be reissued for subsequent periods, each for a maximum of 1 year, on the basis of a new documented safety assessment as described above for each exemption and for each subsequent period.

AISS.OR.300 Information security internal reporting scheme

(a) As part of its information security management system, the organisation shall establish an internal reporting scheme to enable the assessment of information security events and vulnerabilities of equipment, process and services.

(b) Through this scheme, the organisation shall:

(1) identify the causes of and contributing factors to any information security incident and address them as part of the information security risk management;

(2) ensure the evaluation of all known relevant information relating to information security incidents and deviation from procedures and implement a method to circulate the information as necessary.

(c) Any subcontracted organisation shall be able to report through the organisation's internal information security reporting scheme.

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

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

AISS.OR.310 Information security external reporting scheme

(a) As part of its information security management system, the organisation shall implement an information security reporting system that meets the requirements laid down in Regulation (EU) No 376/2014 and its delegated and implementing acts, if such regulation is applicable to the organisation.

(b) Without prejudice to point (a), the organisation shall ensure that any information security incident which may endanger an aircraft, its occupants or any other person(s) is reported to their competent authority.

(c) Without prejudice to Regulation (EU) No 376/2014 and its delegated and implementing acts, the reports referred to in points (a) and (b) shall be made in a form and manner established by the competent authority and shall contain all pertinent information about the condition known to the organisation.

Request to stakeholders:

Regarding point (c), stakeholders are invited to provide feedback on whether EASA should develop (possibly in the AMC and GM) a template with the format and structure of the reports, or it should be left to the competent authorities.

(d) A notification shall be submitted to the competent authority as soon as the condition has been known to the organisation, with a report complying with point (c) being submitted to the competent authority within 72 hours.

(e) Where relevant, the organisation shall produce a follow-up report to provide details of actions it has taken or intends to take to recover from the incident and actions it intends to take to prevent similar information security incidents in the future, as soon as these actions have been identified. This report shall be produced in a form and manner established by the competent authority.

AISS.OR.400 Contracted activities

(a) The organisation shall ensure that when contracting any part of its activities to external organisations, the contracted activity conforms to the requirements of this Regulation. The approved organisation shall also ensure that any risks associated with such activities are part of the organisation's information security management system (ISMS).

(b) When the organisation contracts any part of its activities to an organisation that is not itself certified in accordance with this Regulation to carry out such activities, it shall ensure that the contracted organisation works under its oversight. The organisation shall ensure that the competent authority is given access to the contracted organisation to determine continued compliance with the applicable requirements under this Regulation.

AISS.OR.500 Record keeping

(a) Records of the information security management system (ISMS) and contracted activities:

(1) The organisation shall ensure that the following records are retained, stored and traceable:

(i) any exemption received in accordance with AISS.OR.200(e) together with the records of the safety assessment;

(ii) records of the management system key processes as defined in AISS.OR.200;

(iii) contracts for activities defined in AISS.OR.400;

(iv) records of events that reveal unauthorised interference with aeronautical information systems.

(2) The records specified under (1) shall be retained for a minimum period of 5 years.

(b) Personnel records:

(1) The organisation shall ensure that the records of qualification and experience of personnel involved in information security management and compliance monitoring are retained.

(2) The records specified under (1) shall be retained for as long as the person works for the organisation, and for at least 3 years after the person has left the organisation.

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

(d) Records shall be stored in a manner that ensures protection from damage, alteration and theft, with information being identified, when required, according to its security classification level. The organisation shall ensure that the events described under (a)(1)(iii) are stored using appropriate means to ensure integrity, authenticity and authorised access.

AISS.OR.700 Information security management manual (ISMM)

(a) The organisation shall provide the competent authority with the ISMM and, where applicable, any referenced associated manuals and procedures that contain:

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

(2) the information security policy of the organisation as defined in AISS.OR.200(a)(2);

(3) a general description of the staff and of the system in place to plan the availability of staff as required by AISS.OR.100(c);

(4) the title(s), name(s), duties, accountabilities, responsibilities and authorities of the person(s) referred to in point AISS.OR.100(a)(3);

(5) an organisation chart showing the associated chains of accountability and responsibility between all the person(s) referred to in point AISS.OR.100(a)(3);

(6) the description of the internal reporting scheme as required by AISS.OR.300;

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

(i) the documentation of the management system key processes as required by AISS.OR.200;

(ii) the procedures that define how the organisation controls any contracted activities as required by AISS.OR.400;

(iii) the ISMM amendment procedure;

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

(b) The ISMM shall be amended as necessary to remain an up-to-date description of the organisation, and a copy of it shall be provided to the competent authority.

(c) Amendments to the ISMM shall be managed as defined in the procedure referred to in (a)(7)(iii).

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

AISS.OR.800 Changes to the organisation

(a) Changes to the reporting lines between the personnel, nominated in accordance with AISS.OR.100(a)(3) and (a)(4), and the accountable manager shall be subject to prior approval by the competent authority.

(b) Other changes may be managed and notified to the competent authority as defined in a procedure developed by the organisation and approved by the competent authority.

(c) Except for changes managed in accordance with a procedure approved by the competent authority as described in (b), the organisation shall apply for and obtain an approval issued by the competent authority. The application shall be submitted before any such change takes place, in order to enable the competent authority to determine continued compliance with Regulation (EU) 2018/1139 and its delegated and implementing acts and to amend, if necessary, the organisation certificate and related terms of approval attached to it.

The organisation shall make available to the competent authority any information it requests to evaluate the change.

The change shall be implemented only upon receipt of a formal approval by the competent authority in accordance with AISS.AR.800.

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

AISS.OR.900 Findings

(a) After receipt of the notification of findings according to AISS.AR.900, the organisation shall:

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

(2) define a corrective action plan; and

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

(b) The actions required by paragraph (a) shall be performed within the period agreed with that competent authority as defined in AISS.AR.900.

4. Impact assessment (IA)

4.1. What is the issue

Please refer to Section 2.1.

4.2. What we want to achieve — objectives

Please refer to Section 2.2.

4.3. How it could be achieved — options

During the discussions within the European Strategic Coordination Platform (ESCP), a number of fundamental questions were raised, which led to different options being considered, with some of them discarded.

Q1: Who should be the competent authority for the approval and oversight of the new requirements?

Since the requirements proposed in this NPA apply to organisations for which there are organisation requirements in the existing implementing rules, this means that there is already a competent authority that is responsible for the oversight of the organisation. This is either EASA or the national aviation authority (NAA).

And the question was who should be the competent authority for the additional information security elements proposed in this NPA.

In the case of organisations that are directly approved by EASA, the conclusion during the ESCP discussions was that it was reasonable that EASA would be also the authority for the information security requirements proposed in this NPA. The only issue raised was in relation to Pan-European organisations (such as EGNOS), for which the Security Accreditation Board (SAB) defined in Article 11 of Regulation (EU) No 512/2014 has certain functions when defining the security requirements to be met by the organisations. In those cases, appropriate coordination measures will need to be established between EASA and the SAB.

However, in the case of organisations which are under the responsibility of a competent authority of a Member State, the situation was not so simple because the Member States may have already defined other competent authorities for the requirements imposed by other regulatory frameworks (such as the NIS Directive and Regulation (EU) 2015/1998). This competent authority in some Member States could be, for example, the national cybersecurity agency while in others it could be a particular ministry or a civil aviation authority.

The following two options were considered in order to define who would be the competent authority responsible for the implementation and enforcement of the requirements proposed in this NPA:

— Option 1: Leave to the Member States the decision of who would be the authority for the information security elements. This would provide them, for example, with the possibility to give this responsibility to the authority responsible for the NIS Directive.

— Option 2: Require that the competent authority for the information security elements is the NAA already responsible for the current EASA safety approval (or declaration) held by the organisation.

When evaluating Option 1, it soon became evident that this would result in a situation where the organisation would be under the responsibility of two authorities: the NAA for the elements of the current EASA implementing rules and, for example, a national cybersecurity agency for the information security elements proposed in this NPA. This raised the concern of creating the following problems:

— Possible disputes between the two authorities regarding the continued validity of the organisation approval, due to the importance placed by each authority on the findings raised during their audits. Solving this issue may have required to create two approval certificates for the organisation, one issued by each authority.

— Possible inconsistent approach during the oversight performed by both authorities, not properly taking into account the interfaces between safety and security.

— It would have been very difficult for EASA, if not impossible, to audit the activities performed by the national cybersecurity agency due to possible access restrictions to the necessary information.

Eventually, Option 1 was discarded. The selected Option 2 allows having a single authority (the NAA) responsible for all the elements applicable to the organisation, ensuring that all the aspects related to aviation safety are appropriately considered.

In addition, and in order to provide sufficient flexibility to the Member States, provisions have been introduced in AISS.AR.400 'Allocation of tasks to qualified entities' in order to allow the NAA to delegate tasks, for example, to a national cybersecurity agency already responsible for the implementation of the national transposition of the NIS Directive. However, the requirements to be met by the organisation and by the qualified entity are still the ones contained in Part-AISS.OR and Part-AISS.AR respectively, and the responsibility remains with the competent authority, especially in order to ensure that the audits performed by the qualified entity take appropriate consideration of the safety aspects.

Regarding the standardisation of oversight activities, EASA will perform oversight only on the NAA, in order to verify how the NAA has implemented all the requirements related to the aviation safety approval of the organisation. For the information security elements, if a national cybersecurity agency (or equivalent) is involved, EASA will check how the NAA and the national cybersecurity agency (or equivalent) coordinate. However, EASA will not audit the national cybersecurity agency (or equivalent). If EASA finds that coordination is inappropriate when auditing the NAA, it will raise a finding in accordance with the applicable requirements.

Q2: How to avoid duplication of requirements and oversight with the NIS Directive?

During the discussions of the ESCP, it became clear that those organisations which have been defined as operators of essential services by the respective Member States are already implementing requirements related to information security management systems (ISMS) and events reporting as a result of the national implementation of the NIS Directive.

In order not to create duplication of requirements and in order not to interfere with how the Member States implement the NIS Directive across the different sectors (energy, banking, aviation, etc.), the proposed 'horizontal' rule gives the possibility to those organisations which have been identified as operators of essential services not to comply with Part-AISS.OR and, instead, comply with the national transposition of Article 14 of the NIS Directive. The only condition is that the competent authority responsible for the 'horizontal' information security rule (the NAA) and the competent authority responsible for the implementation of the nationally transposed NIS Directive shall coordinate the aspects related to aviation safety.

Obviously, the drawback of this approach is that the requirements imposed on those operators of essential services by the nationally transposed NIS Directive may vary from Member State to Member State, creating a lack of standardisation.

This is something that could be solved and even prevented if the competent authorities, which in many cases are still defining detailed requirements and policies for their operators of essential aviation services, use the material that is being developed in this RMT for that purpose.

This would promote the standardisation of national requirements for essential services across the Member States, with the additional benefit of being aligned with the requirements that are being developed for all aviation domains in this RMT.

Q3: Which aviation domains and stakeholders should be covered by the proposed rule?

The general criterion followed has been to make the proposed rule applicable to those organisations that currently have requirements for a management system in the existing implementing rules in place, as well as to those organisations for which such requirements are currently in the adoption process at the European Commission or under development in other EASA RMTs.

And in order to ensure adequate proportionality of the risks involved, the following organisations have been excluded:

— production organisations and design organisations that are required to comply with Subparts G and J respectively of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012, if they are solely involved in the design and production of ELA2 aircraft;

— 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);

— organisations that demonstrate their design capability in accordance with alternative procedures to Subpart J of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012;

— organisations that perform maintenance and continuing airworthiness activities in accordance with Annex Vd (Part-CAO) to Regulation (EU) No 1321/2014 (as per Opinion No 05/2016);

— 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 (ATO) 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) in accordance 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;

— operators of unmanned aircraft systems (UASs) that belong to the ‘open’ and ‘specific’ categories (as per Opinion No 01/2018).

NOTE: According to Opinion No 01/2018, operators of UASs in the 'open' category do not require neither an authorisation nor a declaration in order to operate the UAS.

For operators of UASs in the 'specific' category, such authorisation or declaration is needed. And these operators have the option to obtain a 'Light UAS Operator Certificate (LUC)' on the basis of implementing a safety management system which will provide them 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 authorisation it suffices with 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).

For those reasons, these operators have been exempted from the rules proposed in this NPA, and in particular, from implementing an ISMS. However, this approach may be different in the future when rules are developed for operators of UASs in the 'certified' category.

In addition, a provision has been introduced in AISSS.OR.200(e), permitting the organisation to be temporarily exempted by the competent authority from implementing an ISMS if it demonstrates to the satisfaction of such competent authority that its activities, facilities and resources, as well as the equipment, systems and services it provides, maintains and operates, do not pose any information security risks neither to itself nor to other organisations. This exemption shall be based on a documented safety assessment performed by the organisation, and reviewed and approved by its competent authority.

This exemption will have a maximum duration of 1 year, and can be reissued for subsequent periods, each for a maximum of 1 year, on the basis of a new documented safety assessment as described above for each exemption and for each subsequent period.

In the case of third-country operators that are required to comply with Regulation (EU) No 452/2014, EASA has decided not to apply the new rule to them. Nevertheless, these operators will be subject to the requirements imposed by the different Member States as a result of the provisions of point 4.9 'Measures relating to cyber threats' of Annex 17 to the ICAO Convention.

Q4: What should be the structure of the proposed rule?

The following two options were considered:

— Option 1: Introduce requirements for the management of information security risks in each of the existing implementing rules for the different aviation domains.

— Option 2: Create a 'horizontal' information security rule applicable to all aviation domains, and introduce cross references to this 'horizontal' rule in the existing implementing rules.

Eventually, the option of creating a 'horizontal' rule (Option 2) was selected and Option 1 was discarded for the following reasons:

— Creating a single regulation that covers all the aviation domains ensures the consistency of the requirements and the treatment of aviation as a system of systems. This is essential in the information security domain due to the extremely high degree of interconnections between the different stakeholders.

Furthermore, this 'horizontal' rule could become the spearhead of future efforts for a wider implementation of 'horizontal' rules in areas other than information security.

— This single regulation creates a much lower impact, since the changes to the existing implementing rules are limited to the introduction of some cross references. In addition, it prevents interference with any current or future RMT affecting the existing implement rules, since they will not contain the information security requirements. This also facilitates the future adoption process of the requirements proposed in this NPA at the European Commission.

NOTE: In this NPA, this 'horizontal' rule applies to all aviation domains. However, in the final deliverable of this RMT (i.e. Opinion), EASA will divide this 'horizontal' rule in three sets of rules:

— one for those organisations for which the Basic Regulation provides that the detailed rules need to be adopted by means of delegated acts;

— one for those organisations for which the Basic Regulation provides that the detailed rules need to be adopted by means of implementing acts; and

— another one for all the competent authorities since, according to Article 62(15)(c) of the Basic Regulation, the detailed rules for their management systems need to be adopted by means of implementing acts.

In any case, it is envisaged that both rules applicable to organisations are identical.

Q5: Performance- and risk-based rules or prescriptive rules?

During the discussions in the ESCP, it soon became clear that it would be very difficult to properly address the information security risks faced by the aviation community through the introduction of prescriptive rules. Prescriptive rules would not provide enough flexibility in order to cover the very different risks and realities faced by the different organisations and, in addition, they would very soon become obsolete in view of the extremely quick evolution of the information security risk landscape.

As a result, it was agreed to follow a high-level, performance- and risk-based approach for the development of the rules, assigning a very significant importance to the development of appropriate AMC and GM material as well as to the use of industry standards. The available standards will have to be scrutinised during the development phase of the AMC and GM material in order to identify which ones are appropriate.

Q6: How to ensure integration of the new requirements with other management systems?

From the beginning of the discussions in the ESCP, the importance of ensuring the highest possible integration of management systems was clear. Many organisations have already in

place management systems for safety and for security, and many of them would be willing to integrate any new information security management system (ISMS) that is being developed.

As a result, the first proposal discussed involved merging the ISMS requirements being developed with the management system requirements that already exist in other implementing rules. However, this option raised the following concerns:

— Currently, only the implementing rules for some aviation domains contain requirements for a management system. This is the case of:

  — Regulation (EU) No 965/2012 (air operations),

  — Regulation (EU) No 1178/2011 (aircrew),

  — Regulation (EU) 2017/373 (ATM/ANS),

  — Regulation (EU) No 139/2014 (aerodromes),

  — Regulation (EU) 2015/340 (air traffic controllers).

  However, for the other domains the management system requirements are either in the adoption process at the European Commission or under development through other RMTs. This is the case of:

  — Regulation (EU) No 748/2012 (design and production organisations),

  — Regulation (EU) No 1321/2014 (continuing airworthiness management organisations and Part-145 maintenance organisations).

  Furthermore, the existing management system requirements are not identical (neither in terms of content nor in terms of structure) across the different implementing rules.

— This means that merging the future ISMS requirements into the existing implementing rules would have the following disadvantages:

  — The merging would have been possible only for some aviation domains, and this with the very high impact created by the full amendment of those implementing rules and by the significant interference with any ongoing or future rulemaking activity affecting such implementing rules.

  — For the other domains, where the management system is currently under the comitology process or under rulemaking action, the merging would have created a very significant interference with the ongoing processes.

  — It would have meant to abandon the idea of creating a 'horizontal' rule for the ISMS covering all aviation domains.

Taking into account those concerns, this option was discarded and, instead, it was decided to create a 'horizontal' information security rule where the ISMS structure and content would be as close as possible to the management systems that already exist in some implementing rules.

In addition, it was decided to introduce in points AISS.OR.200(d) and AISS.AR.200(e) the possibility for organisations and competent authorities to integrate the information security management system (ISMS) proposed in this NPA with other existing management systems they may already have.

As a result of the analysis above, the selected policy options were the following:

Table 1: Selected policy options

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 Annex II (Part-AISS.OR) to 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.

4.4. What are the impacts

4.4.1. Safety impact

Option 0 would result in the continuation of the safety risks described under Section 2.1, which are constantly increasing as a result of the current aviation information systems becoming more and more interconnected and as a result of the increased potential for malicious individuals and organisations to cause damage. This increase of risks will be lower for organisations that have a mature information security management system (ISMS) and higher for those organisations that do not have such a mature management system.

As a consequence, it could be said that Option 0 would have medium negative safety impact.

Option 1 is expected to have a **positive safety impact** for the following reasons:

— The introduction of an ISMS will ensure that organisations across all aviation domains systematically identify the areas exposed to information security risks, perform appropriate risk assessments, develop and implement measures to protect their critical systems, data and processes, continuously identify vulnerabilities and information security risks and take actions to mitigate them.

— The introduction of internal and external reporting schemes will facilitate the sharing of information, both inside the organisations as well as among organisations and authorities.

— The introduction of coordination requirements between the different authorities within each Member State and the efforts made to ensure consistency of regulatory and oversight requirements with the other regulatory frameworks (NIS Directive and Regulation (EU) 2015/1998) will ensure a comprehensive approach where all the aspects related to safety and security are properly considered.

This positive impact will be lower for organisations that already have a mature ISMS in place and higher for those that do not have a mature one. This means that the average positive safety impact of Option 1 is medium.

So, comparing Option 0 (medium negative) to Option 1 (medium positive), there is a high positive safety impact for Option 1 compared to Option 0.

4.4.2. Environmental impact

No environmental impacts are expected with both Options 0 and 1.

4.4.3. Social impact

Option 0 would result in a **high negative social impact** created by an increasing lack of trust that the public would have in air travel because of the real (or perceived) increase of risks. This increasing lack of thrust could be in relation to a particular organisation (the public may not want to fly with a particular airline, for example) or to the entire aviation sector (if the risks are perceived to affect the whole aviation system, such as risks affecting air traffic management).

Option 1 would have the following positive impacts:

— It allows to maintain the current trust (and even increase it) that the public has in air travel.

— It is expected to generate an increase of employment opportunities and better economic conditions for the qualified personnel available in the labour market, due to the need of a number of organisations to increase their efforts and resources in order to properly implement a robust ISMS.

— It is also expected to create an increase of opportunities for educational institutions and organisations.

So, compared to Option 0, Option 1 would bring a high positive social impact.

4.4.4. Economic impact

Option 0 would result in constantly increasing economic costs due to the information security incidents that may result from the increase of risks and not having a robust ISMS. Taking into account the huge cost of even a single major information security event, not only because of the direct effect on the activities of the organisation but also because of the impact on its reputation, this increase of costs will be much higher for organisations that do not have a mature ISMS.

Some examples of cost estimations of actual cyberattacks, which included a number of companies in the transport sector, can be found at the following links:

— NotPetya cyberattack (June 2017):
  — https://www.bbc.com/news/technology-41336086
  — https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#7be5f8514f9a

In addition, a study on the cost of cybercrime can be found at the following link:

  — https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Option 0 is, therefore, expected to have a high negative economic impact.

Option 1:

The economic impact on the organisations will largely depend on how robust their current ISMSs are when addressing information security risks.

Some large organisations, considered as operators of essential services by their Member States, may have already implemented ISMSs and event notification measures similar to the ones proposed by this NPA. These organisations should not be significantly impacted, moreover taking into account the possibility given to them in this NPA to replace the requirements of Part-AISS.OR by the requirements stemming from the nationally transposed NIS Directive.

Other organisations, even when not affected 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, the economic impact will be of a medium scale, due to the need to fully adapt their existing management processes to the new requirements.

It will be those organisations which have not implemented any procedures and processes for the management of information security risks that will suffer the highest cost for the implementation of the proposed measures. Among other things, they will have to:

— identify the areas which could be exposed to information security risks;

— identify the interfaces with other organisations with which they share information security risks;

— identify the critical information and communications technology systems, data and processes they use;

— perform information security risk assessments of all identified critical systems, data and processes;

— develop and implement measures to protect the critical systems, data and processes;

— continuously identify vulnerabilities and information security risks to the critical systems, data and processes, take actions to mitigate any unacceptable risks and exploitable vulnerabilities, and verify the continued effectiveness of critical systems, data and processes protection; and

— ensure that personnel have the skills and competences to perform their tasks.

This is expected to be the case for those organisations which have not 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 NPA proposals, as well as the future AMC and GM material, are going to properly take into account the proportionality aspects linked to smaller organisations, with a significant number of those organisations being exempted from the proposed rules.

In addition, it must be considered that certain organisations may find difficulties in having access to a sufficient number of qualified personnel, possibly at increased costs.

So, it could be said that the negative economic impact of implementing the measures proposed in this NPA will vary from low to high depending on the maturity of the organisations, with the average negative impact being medium.

Notwithstanding the anticipated economic costs described above, these costs may be spread over time by the introduction of appropriate transitional measures for the application of the proposed rules.

In addition, it is the opinion of EASA that these negative impacts should be outweighed by the much higher economic benefits resulting from the following:

— A much more robust management system capable of identifying, protecting from, detecting, responding to and recovering from those information security incidents which could potentially affect aviation safety.

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

— A more coordinated approach between different organisations within all the aviation domains, where the interfaces and the shared risks are properly evaluated.

— A much more coordinated oversight approach between the different authorities in each Member State (national information security authorities, ministries, civil aviation authorities, etc.), which should reduce the total number of audits and the amount of conflicting requirements, facilitating a comprehensive approach where safety and security aspects are properly considered.

— A more coordinated approach to event reporting, allowing a much wider information sharing between organisations and Member States, both at national and European level, should they be willing to share such information.

— Possible decrease of insurance costs.

All the above should significantly reduce the risks for organisations to suffer major information security incidents, and will put them in a position to rapidly react to such incidents which still happen anyway. Taking into account the huge cost of even a single major information security event, not only because of the direct effect on the activities of the organisation but also because of the impact on its

reputation, the associated economic benefits of fully implementing the requirements proposed by this NPA should significantly outweigh any implementation costs incurred.

In addition, the following aspects need to be highlighted:

— The proposed requirements are in line with the Basic Regulation, in particular with the efforts to properly address the interfaces between security and safety.

— The fact that the proposed rule has a 'horizontal' character (applies to all aviation domains) could be seen as supporting the efforts for a 'better regulation' and a first step to apply the same approach to areas other than information security.

— The proposed requirements contribute to the growth of the internal market and its competitiveness, since they include standardised requirements for all aviation organisations in the different aviation domains.

— Organisations located in the USA, Canada and Brazil, when covered by an existing bilateral agreement with the EU, are not affected by the rules proposed in this NPA. However, this does not prevent that, in the future, there may be an evaluation between the signatories of the respective bilateral agreements for the purpose of identifying whether there is a need to introduce certain special conditions associated to the requirements proposed in this NPA.

— The proposed requirements, which have been widely coordinated within the ESCP, should contribute to the harmonisation of the requirements at global level.

This means that the medium negative economic impact described above for implementing the measures proposed in this NPA will be more than outweighed by the high economic benefit of reducing the likelihood of suffering information security incidents. This would give an overall low positive economic impact for Option 1.

So, taking into account the high negative effect of Option 0 and the overall low positive impact of Option 1, the comparison would give a high positive impact for Option 1 (compared to Option 0).

4.4.5. General Aviation and proportionality issues

Option 0 would not have any impact on General Aviation.

Option 1:

In order to ensure appropriate proportionality of the risks involved and to address the concerns from the General Aviation community, the requirements proposed in this NPA shall not apply to the following organisations:

— production organisations and design organisations that are required to comply with Subparts G and J respectively of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012, if they are solely involved in the design and production of ELA2 aircraft;

— 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);

— organisations that demonstrate their design capability in accordance with alternative procedures to Subpart J of Section A of Annex I (Part 21) to Regulation (EU) No 748/2012;

— organisations that perform maintenance and continuing airworthiness activities in accordance with Annex Vd (Part-CAO) to Regulation (EU) No 1321/2014 (as per Opinion No 05/2016);

— 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;

— operators of unmanned aircraft systems (UASs) that belong to the 'open' and 'specific' categories (as per Opinion No 01/2018).

In addition, a provision has been introduced in point AISSS.OR.200(e) that permits the organisation to be temporarily exempted by the competent authority from implementing an ISMS if it demonstrates to the satisfaction of such competent authority that its activities, facilities and resources, as well as the equipment, systems and services it provides, maintains and operates, do not pose any information security risks neither to itself nor to other organisations. This exemption shall be based on a documented safety assessment performed by the organisation, and reviewed and approved by its competent authority.

This exemption will have a maximum duration of 1 year, and can be reissued for subsequent periods, each for a maximum of 1 year, on the basis of a new documented safety assessment as described above for each exemption and for each subsequent period.

Based on the above, neutral proportionality impacts are expected for Option 1 compared to Option 0.

4.5. Conclusion

The value '0' (zero) assigned in the table below to the impacts generated by Option 0 is the reference baseline of a situation where safety risks and associated costs are constantly increasing. And the values assigned to the impacts of Option 1 are either positive or negative effects against that baseline, that is, comparing Option 1 to Option 0.

Table 2 — Summary of impacts per criteria and option

Type of impact	Option 0	Option 1
	No policy change	***Introduce requirements related to the security of aeronautical information systems***
Safety	0	+++
Social	0	+++
Economic	0	+++/–
Proportionality	0	0
Total	**0**	**++**

Based on the impact assessment described above, it is concluded that the preferred option is Option 1, that is to propose a new regulation that shall:

— require organisations to manage the impact of information security risks on aviation safety by taking a system-of-systems approach where all the interfaces between the different actors are taken into account;

— ensure that only one authority is responsible in the Member State for the full organisation approval (including the proposed information security requirements), but still allowing this authority to delegate, under its responsibility, tasks to other organisations (such as a national cybersecurity agency);

— avoid duplication of requirements, giving the possibility to those organisations which have been identified as operators of essential services not to comply with Part-AISS.OR and, instead, comply with the nationally transposed Article 14 of the NIS Directive;

— be applicable to all those organisations for which the current implementing rules contain requirements for a management system, as well as to those organisations for which such requirements are currently in the adoption process at the European Commission or under development in other EASA RMTs;

— ensure adequate proportionality of the risks involved by excluding those organisations that are subject to lower risks;

— avoid a significant impact on the existing implementing rules and interference with ongoing RMTs by taking the format of a separate 'horizontal' rule;

— allow for adequate flexibility for organisations and authorities and avoids frequent rule amendments by introducing high-level, performance- and risk-based requirements supported by AMC and GM material and industry standards;

— ensure that organisations and authorities can integrate the new requirements into other existing management systems they may already have.

Therefore, compared to Option 0, Option 1 is expected to bring high positive safety and social impacts and medium positive economic impacts.

Request to stakeholders

Stakeholders are invited to provide:

- **quantified justification elements on the possible impacts (e.g. economic, social, safety) of the options proposed, or alternatively to propose a justified solution to the issue;**
- **any other information they may find necessary to bring to the attention of EASA; as a result, the relevant parts of the IA might be modified on a case-by-case basis.**

4.6. Monitoring and evaluation

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; it also helps to identify actual implementation problems. With respect to this proposal, EASA would suggest monitoring various elements looking at short and medium term. Indeed, there are elements that should be monitored as soon as the rules are implemented and others for which some years would need to pass before the outcome could be measured. A proposal on indicators to be checked is presented below:

What to monitor	How to monitor	Who should monitor	How often to monitor
How the different Member States have defined the competent authorities for safety and security and how coordination is performed.	Audits/Feedback from Member States	EASA	Once the rule is applicable. Recurrence to be defined.
How many Member States have decided to make use of Article 2(4), replacing compliance with Part-AISS.OR by compliance with the NIS Directive.	Audits/Feedback from Member States	EASA	Once the rule is applicable. Recurrence to be defined.
Number of information security incidents reported by organisations affected by this initiative, split by severity/risk.	ECCAIRS — the split in severity/risk should allow to distinguish the improvement of reporting versus the improvement of safety performance	EASA/competent authority — with the support of the Network of Analyst (NoA)	On a recurrent basis, e.g. once a year.
Number and level of findings related to the implementation of Part-AISS.AR and Part-AISS.OR.	Audits	Competent authorities/EASA	On a recurrent basis, e.g. once a year.

5. Proposed actions to support implementation

— Full discussion and coordination with the European Strategic Coordination Platform (ESCP), as described in Section 2.3

— Focused communication for all the advisory body meetings (MAB, SAB, TeB, TEC)

— EASA Circulars

(Primarily targeted audience: competent authorities, industry)

— Detailed explanation with clarification and indicated hints on the EASA web

(Industry, competent authorities)

— Dedicated thematic workshop/sessions

(Industry, competent authorities)

— Series of thematic events organised on the regional principle

(Industry, competent authorities)

6. References

6.1. 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: 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)

6.2. Affected decisions

— AMC & GM to the regulations listed in Section 6.1.

6.3. Other reference documents

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

— 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'

7. Appendix I: 'Draft example of a maturity matrix for the ATM/ANS domain'

NOTE: It is published separately and contains a draft example that may need to be further reviewed during the development of the AMC/GM material.