EASA
European Union Aviation Safety Agency

NPA 2019-07 “Management of Information Security Risks”

Juan Anton
Cybersecurity in Aviation & Emerging Risks Section Manager

2nd July 2019
EASA Workshop on NPA 2019-07

Your safety is our mission.

An Agency of the European Union

Summary of the rulemaking activity and associated steps

Summary of the rulemaking activity and associated steps

- **Rulemaking task RMT.0720: included in the EPAS (European Plan for Aviation Safety)**
  - Preliminary Impact Assessment (PIA) issued on 17 July 2017.
  - Terms of Reference (ToR) published on 16 January 2019.
  - NPA 2019-07 published on 27 May 2019.
    - Public Consultation on the EASA website until 27 September 2019.
    - Comments to be submitted through the Comment-Response Tool (CRT) at: **http://hub.easa.europa.eu/crt/**
  - Opinion expected by summer 2020.
  - Entry into force: once adopted by the European Commission (not expected before second half of 2021).
  - Expected to include transition measures to facilitate implementation.

Why we need to develop new rules

Information security risks are constantly increasing

- **Information systems are becoming increasingly complex and interconnected, and a more frequent target of cyber-crime.**
  - Weaknesses in one organisation, product or system can have an impact on different stakeholders, largely amplifying the impact of a cyber attack.
  - These weaknesses are not always known by the operators.
  - They can be combined and exploited with malicious intent:
    - Different attacker profiles:
      - Sponsored by certain States for political/economic reasons.
      - Activists seeking publicity for their cause.
      - Criminals looking for economic benefits.
    - Not always necessarily targeting aviation, but producing a collateral damage.

Current EASA rules only partially address information security risks

- **The current EASA aviation regulatory framework is mostly focused on reducing the likelihood of accidents resulting from non-intentional acts:**
  - Includes different safety layers.
  - Accidents would only occur when several simultaneous deficiencies/errors randomly align themselves: very remote and fortuitous event.

- **Not enough focus on safety risks resulting from intentional acts.**
  - Existing flaws are exploited with malicious intent. Not a random event.
  - Traditional safety layers may not be sufficient to address these risks.
  - Current requirements only in the following areas:
    - Technical requirements for aircraft/engine certification
    - Organisation requirements for ATM/ANS and Aerodromes

Two other EU frameworks partially address information security (NIS Directive 2016/1148, Aviation Security Reg. 2015/1998)

- **They are not focused on the impact on aviation safety**
  - **NIS Directive:** focus on preventing disruption of essential systems (social and economic impact).
  - **Reg. 2015/1998:** focus on aviation security.
- **They do not cover all aviation domains and stakeholders**
  - **NIS Directive:** Only the essential services defined by each Member State.
    - Only some aviation domains, and not all stakeholders within those domains.
    - Different in each Member State.
  - **Reg. 2015/1998:** Applies only to:
    - Airports or parts of airports.
    - Operators (including air operators) and entities that provide services or goods to or through those airports.

Why we do it now, without waiting to the full implementation of the NIS Directive

Addressing aviation information security risks is an urgent matter

- **NIS Directive applicability:**
  - **9 May 2018:** Member States to adopt and publish the national laws, regulations and administrative procedures to transpose the NIS Directive.
  - **9 November 2018:** Member States to identify the operators of essential services affected by those requirements.

- **Current state of implementation of the NIS Directive:**
  - Some Member States have still not transposed the NIS Directive.
  - Very different speeds of implementation across the Member States.

Waiting for full implementation of the NIS Directive would mean several years before we could start this rulemaking task.

There is a need to ensure a level playing field across Europe

→ **Non-standardised implementation of the NIS Directive:**

→ Different approaches to the definition of essential services.

→ Very different levels of implementation across the Member States.

Waiting for full implementation of NIS Directive would mean starting this rulemaking task when a fully non-standardised landscape is already implemented across the EU. Instead:

→ The discussions on this rulemaking task already started in July 2017.

→ This allows Member States to take into account the material being developed in this task in order to define their policies for implementation of the NIS Directive for the essential services in the aviation domain.

→ **This promotes standardisation and consistency of both frameworks.**

What is the objective of this task

Objective of this rulemaking task

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, detect, respond and recover

from those information security incidents that could affect safety

How the task has been discussed and coordinated

The European Strategic Coordination Platform (ESCP)

- **Members:**
  - European Commission *(DG-MOVE, DG-CNECT, DG-GROW and DG-HOME)*
  - Other EU Agencies and Organisations *(EEAS, EUROPOL, EASA, ENISA, CERT-EU, EUROCONTROL, SESAR)*
  - European Defence Agency
  - States *(ECAC plus 6 EU individual Member States: Finland, France, Poland, Romania, Sweden, UK)*
  - EU relevant Aviation industry associations *(ASD, A4E, ACI, CANSO, ECA, EHA, EIMG, ERAA, ETF, GAMA, IATA)*
- **Observers:**
  - ICAO, FAA, TCCA, AIA, AIAC, NATO

The ESCP has been meeting regularly for the last 2 years

Key elements to achieve the objectives of this task

Key elements agreed during the ESCP discussions:

- → **Focus on the impact of information security threats and events on safety** *(directly on the aircraft or on the European Traffic Management Network)*
- → **Need to cover all aviation domains and interfaces** *(system-of systems)*
- → **Consistency with NIS Directive and Reg. 2015/1998** *(no gaps, loopholes or duplications)*
- → **Compliance with ICAO standards.**
- → **Minimize the impact on existing EASA regulations.**
- → **Proportionality to the risks incurred by the different organisations.**
- → **High-level, performance/risk-based rules supported by AMC/GM and industry standards.**
- → **Make possible for organisations and authorities to integrate the Information Security Management System (ISMS) with other management systems.**

THE PROPOSED RULE

Objective and scope of the proposed rule

Legal basis for introducing the proposed requirements

- **The Basic Regulation (EU) 2018/1139 contains requirements for authorities and organisations regarding implementation of management systems.**
  - Article 62, point (15)(c): For competent authorities
  - Annex II, points 3.1(b): For organisations involved in airworthiness
  - Annex IV, points 3.3(b) and 5(b): For aircrew training organisations and Aeromedical Centres
  - Annex V: points 8.1(c) and 8.4(d): For air operators
  - Annex VII points 2.2.1, 4.2.1 and 5.2: For aerodrome operators, groundhandling services providers and apron management services providers
  - Annex VIII, points 5.1(c), 5.4(b) and 6,1(b): For ATM/ANS service providers and ATC training organisations and Aeromedical Centres.
- **This NPA proposes requirements to ensure that those management systems cover information security risks with an impact on safety.**

Objective of the proposed rule (Article 1)

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.***

Objective of the proposed rule (Article 1)

- **Focus on the impact on aviation safety:**
  - Cyber incident directly affecting the aircraft.
  - Cyber incident affecting the normal functioning of the EATMN (European Aviation Traffic Management Network).

EATMN defined in Reg. (EC) No 552/2004. Includes systems and procedures for:

- Airspace and air traffic flow management,
- Air traffic services,
- Communications, navigation and surveillance,
- Aeronautical information services,
- Meteorological information.

Scope of applicability (Article 2)

- Competent authorities.

- POA and DOA approval holders.
- Part-145 maintenance organisations.
- Part-CAMO organisations (Opinion 06/2016).
- Air operators covered by Part-ORO.
- Aircrew training organisations (ATOs) and aircrew Aeromedical Centres.
- ATCO training organisations and ATCO Aeromedical Centres.
- ATS, MET, AIS, DAT, CNS, ATFM and ASM providers and the Network Manager.
- Aerodrome operators and apron management service providers.

Exempted organisations

- Production organisations not holding POA approval
- Organisations with alternative procedures for design (no DOA approval)
- Future Part-CAO organisations (Opinion 05/2016).
- Part-147 training organisations.
- Declared training organisations.
- ATOs providing only theoretical training.
- Private operators of other than complex motor-powered aircraft.
- TCO operators (they will still be subject to national requirements resulting from point 4.9 "Measures relating to cyber threats" of ICAO Annex 17).
- Operators of UAS in the "open" and "specific" categories (in the future, for the "certified category", the exemption may not apply).
- POAs, DOAs, ATOs, FSTD operators and air operators, when solely dealing with ELA2 aircraft (most aeroplanes below 2000Kg MTOM, very light rotorcraft, sailplanes, balloons and airships).

Other exemptions (on a case-by-case)

- **AISS.OR.200(e):**
  - The organisation can be exempted by the competent authority.
  - The organisations needs to demonstrate that its activities, facilities and services do not pose cyber risks to itself nor to other organisations.
  - This shall be based on a documented safety assessment approved by the authority.
  - The duration of the exemption is maximum 1 year.
  - It can be extended for periods of 1 year each on the basis of new safety assessments.

Structure of the proposed rule

Options 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.

Option selected

- **Option selected:** Create a “horizontal” information security rule applicable to all aviation domains, and introduce cross references to this “horizontal” rule in the existing implementing rules.

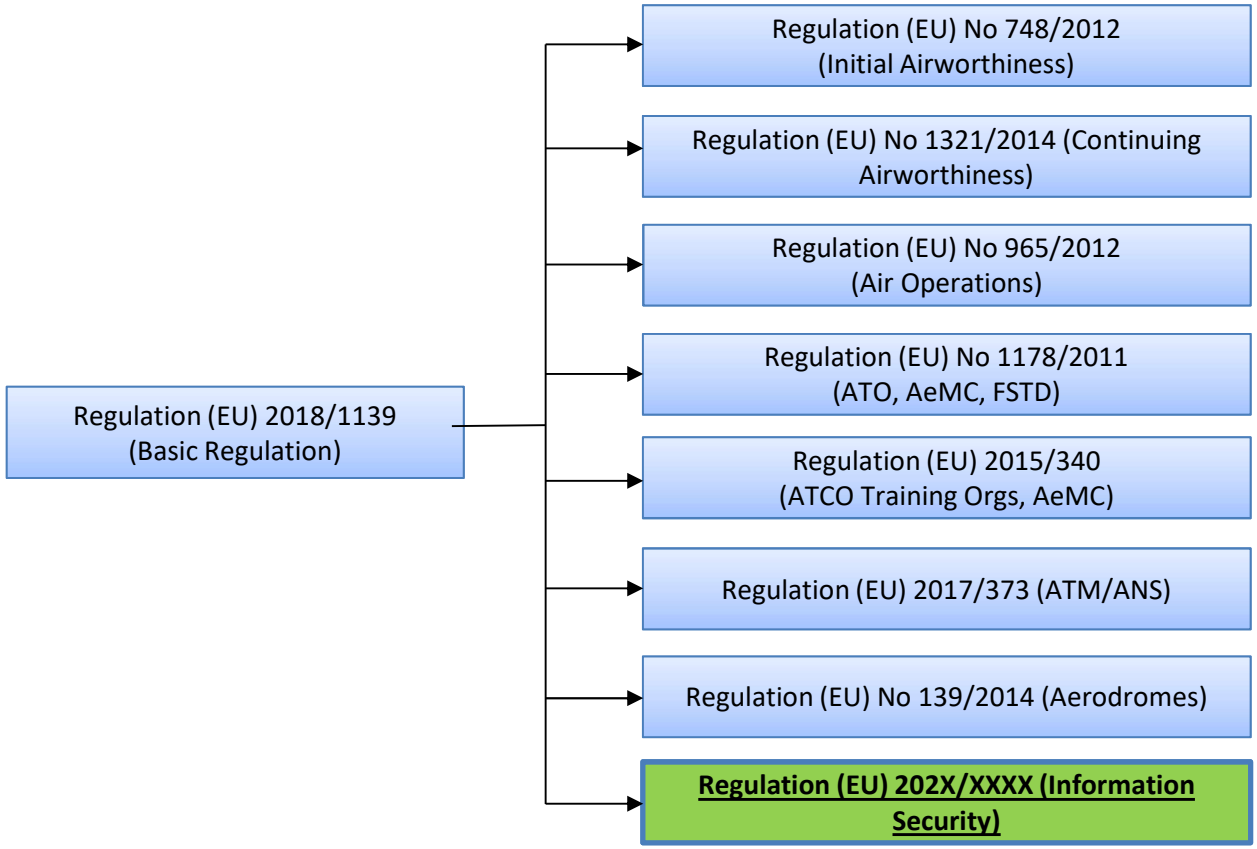
- **Reasons:**
  - Allows consistency of requirements across the different domains.
  - Reduces the changes to the existing rules, limiting them to the introduction of some cross-references to the “horizontal” rule.
  - Prevents interference with other current or future rulemaking tasks affecting the existing rules.
  - Facilitates the future adoption process at the Commission of the proposed rules.

Option selected

- **Key aspects of the "horizontal" rule:**
  - The proposed requirements complement those related to management systems already contained in the existing organisation implementing rules. 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.**
  - 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 separate rules** *(for legal reasons since they follow different adoption processes):*
    - one for **organisations** for which the rules will be adopted by means of **delegated acts**;
    - one for **organisations** for which the rules will be adopted by means of **implementing acts**;
    - one for the **competent authorities** since, according to Article 62(15)(c) of the Basic Regulation, the detailed rules for their management systems are adopted by means of **implementing acts**.

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

The “horizontal” rule within the EASA regulatory framework



Structure of the “horizontal” rule

- **Separate regulation with similar structure as other Implementing Rules:**
  - **Cover Regulation**, including:
    - Objectives, scope, definitions, competent authority and entry into force.
  - **Annex I “Part-AISS.AR — Authority Requirements”**
  - **Annex II “Part-AISS.OR — Organisation Requirements”**

Structure of the “horizontal” rule

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)

Article 1

Objective

……..

Article 2

Scope

……..

Article 3

Definitions

……..

Article 4

Competent authority

……..

Article 5

Entry into force

……..

Structure of the “horizontal” rule

ANNEX I

AERONAUTICAL INFORMATION SYSTEM SECURITY — AUTHORITY REQUIREMENTS

[PART-AISS.AR]

AISS.AR.005	Objective
AISS.AR.100	Personnel requirements
AISS.AR.200	Information security management system (ISMS)
AISS.AR.400	Allocation of tasks to qualified entities
AISS.AR.500	Record keeping
AISS.AR.600	Oversight
AISS.AR.610	Oversight programme
AISS.AR.620	Information to the Agency
AISS.AR.630	Immediate reaction to an information security problem with safety impact
AISS.AR.800	Assessment of changes to organisations
AISS.AR.900	Findings and corrective actions

Structure of the “horizontal” rule

ANNEX II

AERONAUTICAL INFORMATION SYSTEM SECURITY — ORGANISATION REQUIREMENTS

[PART-AISS.OR]

AISS.OR.005 Scope

AISS.OR.100 Personnel requirements

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

AISS.OR.300 Information security internal reporting scheme

AISS.OR.310 Information security external reporting scheme

AISS.OR.400 Contracted activities

AISS.OR.500 Record keeping

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

AISS.OR.800 Changes to the organisation

AISS.OR.900 Findings

Cross-references in the existing Implementing Rules

- **Regulation (EU) No 748/2012 (Initial Airworthiness):**
  - **In Part-21, Section A, Subpart G "Production Organisation Approval"**:
    - **New point 21.A.146 "Information Security": The production organisation shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-21, Section B, Subpart H "Design Organisation Approval"**:
    - **New point 21.A.246 "Information Security": The design organisation shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-21, Section B:**
    - **Point 21.B.5 "Scope" amended to read:**

      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.

Cross-references in the existing Implementing Rules

- **Regulation (EU) No 1321/2014 (Continuing Airworthiness):**
  - **In Part-145, Section A**:
    - **New point 145.A.72 "Information Security": The maintenance organisation shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-145, Section B:**
    - **Point 145.B.01 "Scope" amended to read:**

      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.

Cross-references in the existing Implementing Rules

- **Regulation (EU) No 1321/2014 (Continuing Airworthiness):**
  - **In Part-CAMO, Section A**:
    - **New point CAMO.A.330 "Information Security": The continuing airworthiness management organisation shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-145, Section B:**
    - **Point CAMO.B.005 "Scope" amended to read:**

      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.

Cross-references in the existing Implementing Rules

- **Regulation (EU) No 965/2012 (Air Operations):**
  - **In Part-ORO**:
    - **New point ORO.SEC.110 "Information Security": Air operators listed under point ORO.GEN.005 shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-ARO:**
    - **Point ARO.GEN.005 "Scope" amended to read:**

      This Annex, **together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 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 Rules regarding civil aviation air operations.

Cross-references in the existing Implementing Rules

- **Regulation (EU) No 1178/2011 (Aircrew):**
  - **In Part-ORA**:
    - **New point ORA.GEN.225 "Information Security": The organisation shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-ARA:**
    - **New point ARA.GEN.110 ~~"Information Security~~" "Scope":**

      This Annex, **together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 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 Rules regarding aircrew.

Cross-references in the existing Implementing Rules

→ **Regulation (EU) 2015/340 (ATCO):**

→ **In Part-ATCO.OR**:

→ **New point ATCO.OR.C.030 "Information Security": Training organisations shall comply with Regulation (EU) 202X/XXXX.**

→ Point ATCO.OR.E.001 "Aero-medical centres" amended to add:

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

→ **In Part-ATCO.AR:**

→ **Point ATCO.AR.A.001 "Scope" amended to read:**

This Part, set out in this Annex, **together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX,** establish 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.

Cross-references in the existing Implementing Rules

- **Regulation (EU) 2017/373 (ATM/ANS):**
  - **In Part-ATM/ANS.OR**:
    - **New point ATM/ANS.OR.B.040 "Information Security": Service providers shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-ATM/ANS.AR:**
    - **Point ATM/ANS.AR.A.001 "Scope" amended to read:**

      This Annex, **together with the requirements contained in Annex I (Part-AISS.AR) to Regulation (EU) 202X/XXXX,** establishes 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.

Cross-references in the existing Implementing Rules

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.

Cross-references in the existing Implementing Rules

- **Regulation (EU) No 139/2014 (Aerodromes):**
  - **In Part-ADR.OR**:
    - **New point ADR.OR.D.035 "Information Security": The aerodrome operator shall comply with Regulation (EU) 202X/XXXX.**
  - **In Part-ADR.AR:**
    - **Point ADR.AR.A.001 "Scope" amended to read:**

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

Cross-references in the existing Implementing Rules

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

(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;~~

~~(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.

Competent Authority responsible for the implementation and oversight of the proposed requirements

Options considered

- **When EASA is the authority for the current approval of the organisation:**
  - EASA would be also the competent authority for the elements of the proposed rule.
  - Special case: For Pan-European organisations such as EGNOS, coordination measures between EASA and the SAB (Security Accreditation Board) will need to be defined.

- **When a competent authority of a Member State is currently responsible for the oversight of the organisation:**
  - **Option 1:** Leave to the Member State the decision of who will be the competent authority for the proposed rule (could be different from the one already responsible for the current EASA safety approval (or declaration) of the organization).
  - **Option 2:** The authority for the proposed rule would be the same as the one responsible for the current EASA safety approval (or declaration) of the organization.

Option selected

- **Option selected:** The authority for the proposed rule would be the same as the one responsible for the current EASA safety approval (or declaration) of the organization.

- **Reasons:**
  - Prevents disputes between 2 authorities responsible for the approval of the organisation, and avoids the need to create 2 approval certificates for the organisation.
  - Permits a consistent oversight approach for all aspects related to aviation safety (including cyber), in particular for the management systems held by the organisation.
  - Permits EASA to perform its audit activities on the competent authority (may not be possible if a national cybersecurity agency is responsible, because of information access restrictions)

Delegation of oversight activities

- **AISS.AR.400 "Qualified entities":** This allows the competent authority to delegate tasks, for example, to a national cybersecurity agency (possibly responsible for the implementation of the NIS Directive).
  - This facilitates the access by the competent authority to additional information security expertise
  - This provides flexibility to the State in order to create a national safety and security organisational structure that fits their needs.

NOTE: The responsibility remains on the competent authority. Especially to ensure that the audits performed by the qualified entity take due account of the safety aspects.

EASA standardisation activities

- **EASA will perform its oversight activities on the competent authority.** This oversight will include also the elements related to information security.

- If the competent authority has delegated certain tasks on, for example, a national cybersecurity agency, EASA will check how they coordinate. EASA will not audit the national cybersecurity agency.

Consistency with the NIS Directive (EU) 2016/1148

Consistency with NIS Directive (for essential services)

- **NIS Directive, Article 14:**
  - **Point 1:** "Member States shall ensure that operators of essential services take……technical and organisational measures to manage the risks posed to the security of network and information systems….."
  - **Point 2:** "Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of network and information systems…..with a view to ensuring the continuity of those services."
  - **Point 3:** "Member States shall ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide….."

- **NIS Directive, Article 1:**
  - **Point 7:** This point allows to replace the requirements contained in the NIS Directive by those of a sector-specific Union legal act if such requirements are at least equivalent to those in the NIS Directive.

Options considered

- **Option of requiring the essential services to comply both with the NIS Directive and the requirements proposed in this NPA:**
  - This would have meant a duplication of requirements, sometimes not fully compatible, as well as duplication of authorities and oversight activities.

- **Option of replacing the requirements of Article 14 of the NIS Directive by the future requirements proposed in this NPA:**
  - This would not happen until the proposed rules are adopted (not before 2021).
  - Would mean a change of regulatory framework for essential services who may have been already applying the NIS Directive since 2018.

- **Option of considering that meeting the requirements of Article 14 of the NIS Directive would be acceptable instead of complying with the requirements proposed in this NPA:**
  - **<u>This was the option selected.</u>**

Option selected

- **Option selected:** Meeting the requirements of Article 14 of the NIS Directive would be acceptable for essential services, instead of complying with the requirements proposed in this NPA. **With one condition:**
  - The competent authority responsible for the safety approval (EASA rules) and the competent authority for the NIS Directive shall establish an agreement to coordinate the aspects impacting aviation safety.

- **Benefits:**
  - Prevents duplication of requirements and permits essential services to continue with their established practices related to information security.
  - Ensures coordination between authorities.
  - Prevents interference on how the Member States implement the NIS Directive across the different sectors (energy, banking, transport, etc) and define their authority structures.

Option selected

- → **Drawback:**
  - → **Possible lack of standardisation across the EU:** The requirements imposed on essential services as a result of the NIS Directive currently vary across the different Member States.
  - → **Envisaged solution:**
    - → For the upcoming Acceptable Means of Compliance (AMC) and Guidance Material (GM) associated to this rule, EASA and the ESCP will review existing policies used by those Member States which are more advanced in the implementation of the NIS Directive.
      - → <u>This will allow to use that material across all the EU Member States and for all stakeholders (not only for essential services)</u>
    - → Since many Member States are still defining detailed requirements and policies for their operators of aviation essential services, they could benefit from aligning them with the AMC/GM material (and associated Industry Standards) being developed in this rulemaking task.
      - → <u>This would promote standardisation of requirements and policies across the EU for the implementation of the NIS Directive, aligning them with the ones being developed in this task for the full aviation sector.</u>

Consistency with Regulation (EU) 2015/1998

Regulation (EU) 2015/1998

- **Focuses on aviation security.**
- **Applies only to:**
  - Airports or parts of airports.
  - Operators (including air operators) and entities that provide services or goods to or through those airports.
- **It is in the process of being amended to align with Amendment 16 to ICAO Annex 17:**
  - Point 4.9.1 of ICAO Annex 17 on measures relating to cyber-threats, has become a "standard" applicable since November 2018:

    "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."
- **Appropriate coordination has been performed to ensure consistency between the rules proposed in the NPA and Regulation (EU) 2015/1998.**

Performance- and risk-based approach

Performance- and risk-based approach

- **Objective:**
  - Ensure the flexibility of the rules.
  - Ensure that they don't need frequent amendments in view of the fast evolution of cybersecurity risks.

- **The role of Acceptable Means of Compliance (AMC), Guidance Material (GM) and Industry Standards:**
  - The rule contains high-level, performance-and risk-based requirements.
  - It will be supplemented by detailed AMC and GM material, which will contain references to certain Industry Standards.

AMC's and GMs

- **For their development, use will be made of:**
  - 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'.
  - Material available in the Member States for the implementation of the NIS Directive, if found appropriate for the wider aviation sector (not just for essential services).
  - References may be introduced to certain Industry Standards, such as:
    - EUROCAE ED-201 and EUROCAE ED-205

AMC's and GMs

- **Development calendar:**
  - The detailed discussions in the ESCP started at the end of May 2019.
  - The AMC/GM should be ready at the beginning of 2021, so they can considered by the Commission and Member States before adopting the future rule.
  - Any amendments to the existing Industry Standards and any new Industry Standards need to be ready when the future rule is adopted by the Commission, so the different stakeholders can use them in the implementation of the future rule.

Integration with other management systems

Options considered

→ **Option 1 (discarded): merge the ISMS requirements proposed in this NPA with the management systems currently existing in other EASA Implementing Rules.**

Drawbacks:

→ Only some aviation domains currently have requirements for management systems (Air operations, aircrew, ATCOs, ATM/ANS and aerodromes)

→ For other domains they are still under development:

→ Design and Production Organisations (NPA 2019-05)

→ Part-145 maintenance organisations (NPA 2019-05)

→ Continuing Airworthiness Management Organisations (Opinion 06/2015)

→ Those management system requirements are not identical across the different Implementing Rules (neither in terms of content nor structure).

→ **Merging would mean:**

→ Only possible for some aviation domains.

→ Interference with ongoing and future rulemaking activities affecting those rules.

→ Abandon the idea of having aligned cyber requirements across all the aviation domains.

Options considered

- **Option 2 (selected):**
  - Create an “horizontal” rule, with cross-reference in the domain-specific implementing rules
  - Make the structure and content of the “horizontal” rule as close as possible to the existing management system requirements in the other rules.
  - Introduce in AISS.OR.200(d) and AISS.AR.200(e) the possibility for organisations and authorities to integrate the different management systems.

Benefits:

- Ensures consistency across all domains.
- Minimises the impact on existing rules and current and future rulemaking activities.
- Facilitates the integration of management systems by authorities and organisations.

Entry into force and transition measures

Entry into Force and transition measures

- → NPA 2019-07 published on 27 May 2019.
  - → Public Consultation on the EASA website until 27 September 2019.
  - → Comments to be submitted through the Comment-Response Tool (CRT) at:
    http://hub.easa.europa.eu/crt/
- → Opinion expected by summer 2020.
- → Entry into force: once adopted by the European Commission (not expected before second half of 2021).
- → Expected to include transition measures to facilitate implementation. A phased approach could be followed depending on the different timing where authorities and organisations could be ready to apply the different requirements.

STAKEHOLDERS REQUESTED TO PROVIDE FEEDBACK

Impact Assessment

Impact Assessment

- **Safety impact: HIGHTLY POSITIVE due to:**
  - Organisations and authorities will have a robust management system to address cyber risks.
  - Reporting systems will facilitate information sharing.
  - Improved coordination between safety and security authorities within the Member States.

Impact Assessment

- **Social impact: HIGHTLY POSITIVE due to:**
  - Increases the public trust in travelling by air.
  - Generates employment opportunities and better conditions for qualified personnel available in the market.
  - Generates increased opportunities for educational institutions and organisations.

Impact Assessment

- **Proportionality impact: NO IMPACT expected due to:**
  - General Aviation organisations and other organisations with lower risks have been excluded from the rule.
  - Possibility for the organization to get a temporary exemption (which can be extended) if it demonstrates to the NAA, with a documented assessment, that its activities do not pose information security risks.

Impact Assessment

- **Economic impact**:
  - **Negative impact compared to doing nothing: MEDIUM**
    - There will be an economic cost of implementation that will depend on the current maturity of the organisation (and how they are currently managing cyber risks).
    - Organisations may have difficulties finding qualified personnel (will depend on the market availability).
  - **Positive impact compared to doing nothing: VERY HIGH**
    - A more robust management system, better information sharing and better coordination between safety and security authorities will significantly reduce the risk and impact of suffering cyber attacks and the huge associated costs (operational and reputational).
    - Increased staff skills and competences should improve the overall productivity and efficiency of the organization.
    - Possible decrease in insurance costs.

Your comments are welcome

Please submit them **by 27 September 2019** through the Comment-Response Tool (CRT) at:

http://hub.easa.europa.eu/crt/

EASA
European Union Aviation Safety Agency

EASA Workshop on NPA 2019-07

Questions

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union