EASA
European Union Aviation Safety Agency

Workshop 4: “Regulatory requirements for organisations”

Juan Anton
Cybersecurity in Aviation & Emerging Risks Section Manager

5th – 7th February 2020
Workshop on Cybersecurity in Aviation
Aviation Partnership Project
Sri Lanka

Your safety is our mission.

An Agency of the European Union

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.
    - →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 services (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.

THE PROPOSED RULE

Key elements agreed during the ESCP discussions:

- → **Introduce common requirements for an Information Security Management System (ISMS) and reporting of incidents.**
- → **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.**

Scope of applicability

→ Competent authorities.

→ POA (production) and DOA (design) approval holders.

→ Part-145 maintenance organisations.

→ Part-CAMO continuing airworthiness management organisations.

→ Air operators covered by Part-ORO (commercial and/or larger aircraft).

→ Aircrew training organisations (ATOs) and aircrew Aeromedical Centres.

→ ATCO training organisations and ATCO Aeromedical Centres.

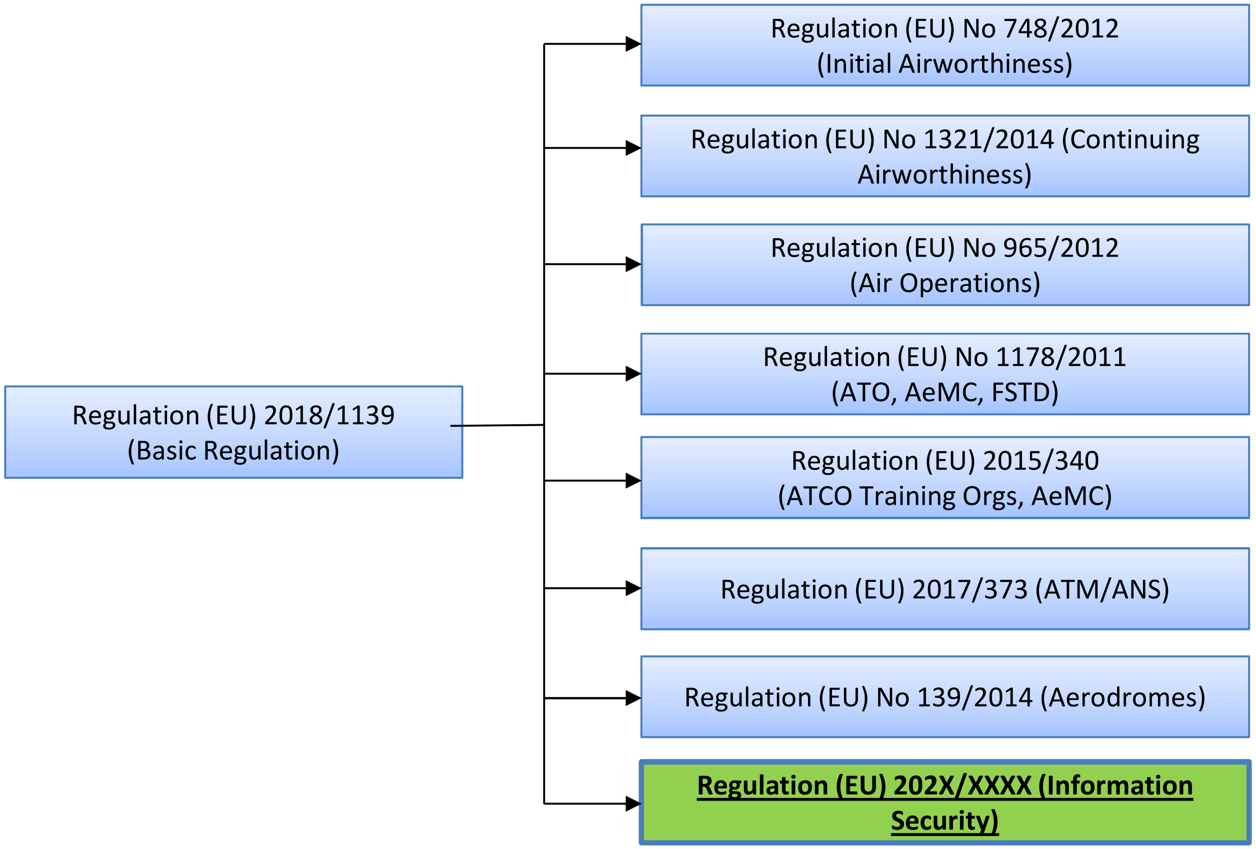
→ ATS, MET, AIS, DAT, CNS, ATFM and ASM providers and the Network Manager.

→ Aerodrome operators and apron management service providers.

Exempted organisations

- Production and Design organisations not holding an approval (alternative procedures)
- Part-CAO organisations (they deal with lighter aircraft).
- Part-147 maintenance training organisations.
- Declared training organisations (for pilot licences of lighter aircraft)
- 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).

The Cybersecurity rule within the EASA regulatory framework



Regulation (EU) 2018/1139 (Basic Regulation)

Regulation (EU) No 748/2012 (Initial Airworthiness)

Regulation (EU) No 1321/2014 (Continuing Airworthiness)

Regulation (EU) No 965/2012 (Air Operations)

Regulation (EU) No 1178/2011 (ATO, AeMC, FSTD)

Regulation (EU) 2015/340 (ATCO Training Orgs, AeMC)

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

Regulation (EU) No 139/2014 (Aerodromes)

Regulation (EU) 202X/XXXX (Information Security)

Cross-references in the existing Implementing Rules

- **AN EXAMPLE: 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.

Structure of the 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 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

Some key elements of the ISMS (AISS.OR.200)

- **Establish, implement, maintain and continuously improve an ISMS. This ISMS shall (among other aspects):**
  - **Identify the organisation activities, facilities and resources, and the equipment, systems and services it provides, maintains and operates, which could be exposed to cyber risks.**
  - Identify the **interfaces with other organisations** with which it shares cyber risks.
  - Identify their **critical information and communication technology systems.**
  - Perform **information security risk assessments** (initially and when changes occur).
  - Develop and implement measures to **protect critical systems, data and processes.**
  - **Identify vulnerabilities and mitigate any unacceptable risks and vulnerabilities.**
  - Ensure that **personnel have the competences and skills** to perform their tasks.

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

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 ended on 27 September 2019.

- Opinion expected by summer 2020.

- Entry into force: once adopted by the European Commission (not expected before end 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.

EASA

European Union Aviation Safety Agency

Questions

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union