ICAO

SAFE SKIES.
SUSTAINABLE FUTURE.

Session 6

Aviation Cybersecurity Oversight

Mr. Philippe MORIO

Cybersecurity expert, ICAO (TTX leader)

Mr. Leonardo Boszczowski

Regional Officer, Aviation Security and Facilitation, SAM (Facilitator)

Ms. Esther Nistal Cabanas

AVSEC auditor AESA (Spain) & Risk Expert. Coordinator of R&D Transport Projects at Isdefe

Mr. Peral Pecharroman, José Maria

Regional Officer Aviation Security and Facilitation, ICAO NACC (Facilitator)

Mr. Douglas Williamson

Director of Information Technology, Jamaica Civil Aviation Authority, Jamaica

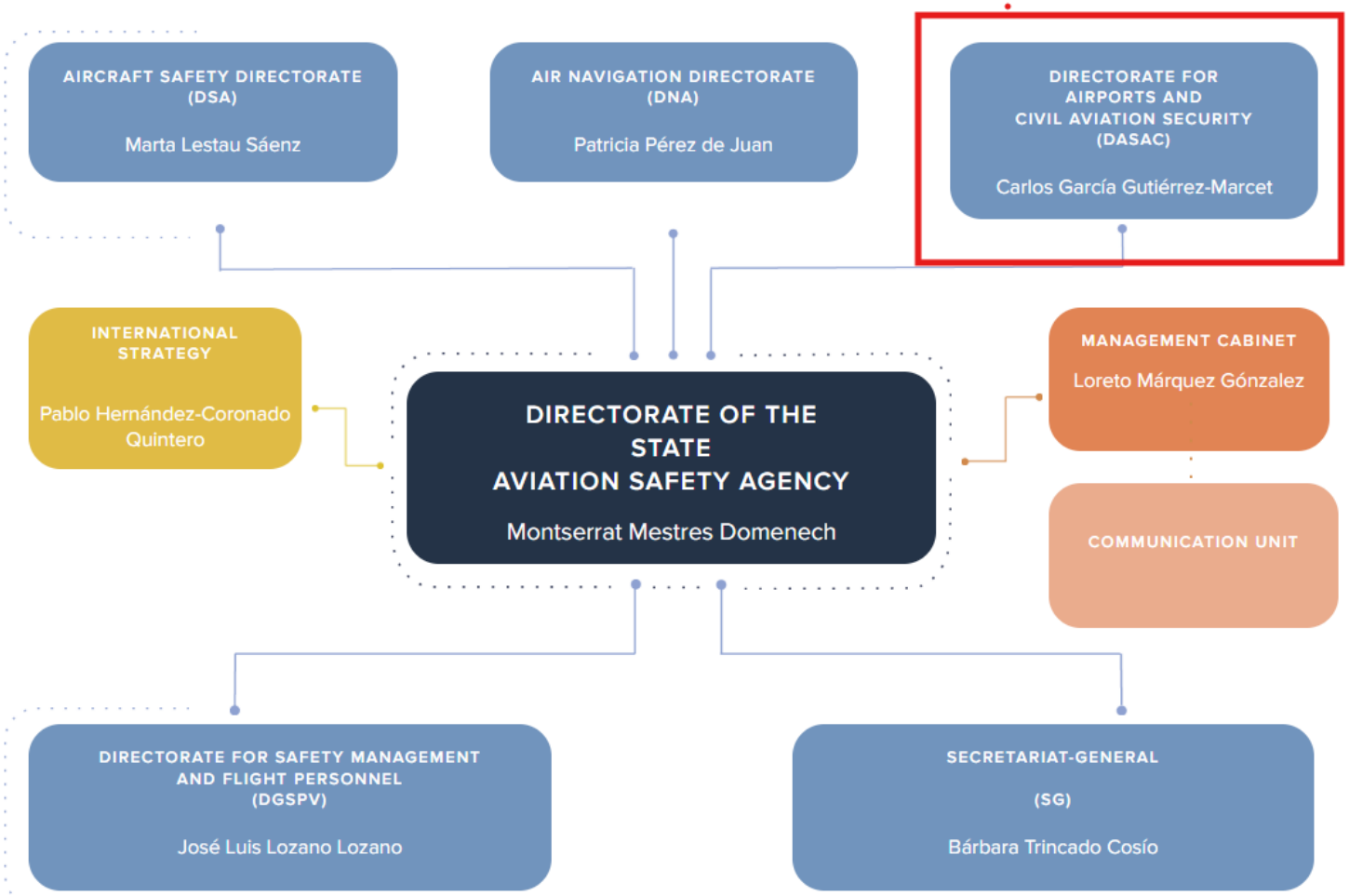
AESA – Spanish Air Safety and Security Agency

- AESA is the civil aviation oversight Authority to comply with ICAO SARPs and EU regulation
- 400 civil servants plus external consultants, as myself
- It is a separate body from Spanish DGAC

AESA – Spanish Air Safety and Security Agency

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

Organisation chart



- AESA is organized in Directorates, to attend SAFETY inspections
- However, SECURITY is considered to be “transversal”
- So Civil Aviation Security Directorate is responsible for performing Security inspections, regardless the type of entity.
- It includes cybersecurity inspections

ICAO

CYBERSECURITY REGULATIONS

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

Regulation	Object and Scope	Application Area	Comment	Appropriate Autority in SPAIN	Entry into Force
Annex 17 ICAO 4.9.1	Standards for aviation security, including cybersecurity	Global aviation sector	Developed by ICAO, ensuring global consistency	EASA	2018?
EU Regulation 1583/2019	Detailed measures for aviation security and cybersecurity	EU member states entities, obligated by Regulation 300/20203 Leave ATM entities aside	Develop by European Commission: Focuses on harmonizing security measures across the EU	EASA	2020
NIS2 Directives	Measures for cybersecurity across critical sectors	EU member states entities	First EU-wide legislation on cybersecurity	National Cybersecurity Authority	2024
National Security Scheme	Legal framework for information security in Spain	Any public entity in Spain (and their supply chain!!!!!!)	Specific to Spain, ensuring national security	National Cybersecurity Authority	2022
PART-IS	Information Security System	EU member states aviation entities: Airports, air carriers, ATM entities, CAMOs, etc	Develop by EASA	EASA	2025-2026

ICAO

European Regulatory Framework

NIS 1 (2016)

First EU framework for essential service operators, including air transport.

NIS 2 (2022)

Broader scope with enhanced requirements. National transposition by October 2024. October 2024.

AVSEC Regulation 1583/2019

EU delegated regulation on cybersecurity in civil aviation, effective since December December 2020.

PART IS (EASA)

Embeds cybersecurity into Safety Management Systems. Applicable from 2025 and 2026 2025 and 2026

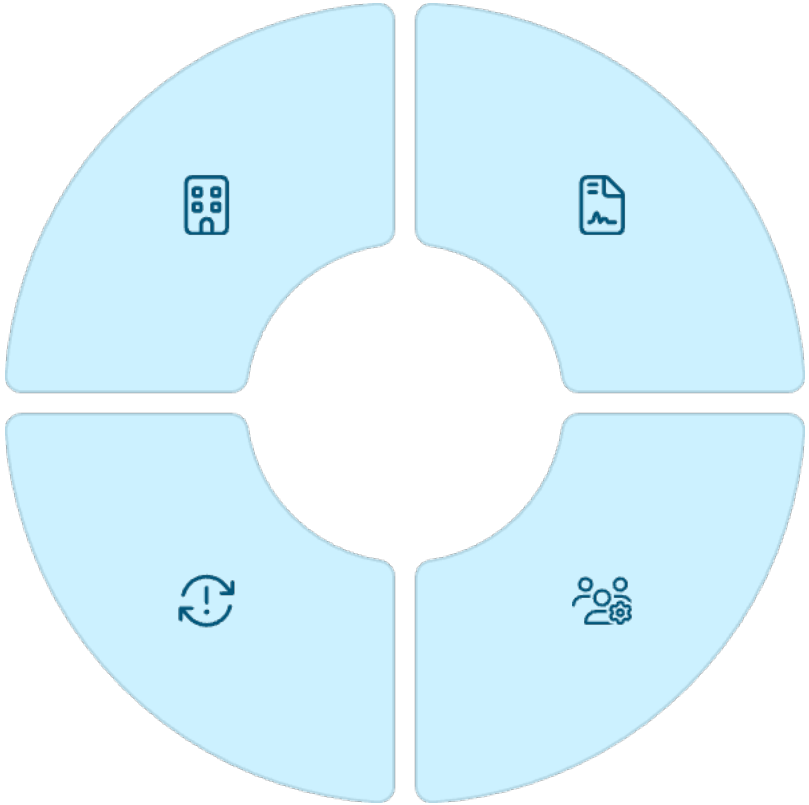
Spanish National Framework

National Security Framework (ENS)

Core framework for ICT systems in public sector, extended to essential service providers.

Integrated Oversight by AESA

Alignment with AVSEC and PART-IS through through coordinated mechanisms.



NIS 2 Transposition

New Cybersecurity Law for all critical sectors, including Aviation, within Transport.

National Regulation was expected in 2024. Not approved yet. We have a consolidated draft

Coordination Bodies

AESA (Aviation Safety), CNPIC (Critical Infrastructure), and INCIBE work together.

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019 vs Annex 17

- **Standard 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 a few words:

- IDENTIFY CRITICAL SYSTEMS
- PERFORM A RISK ASSESSMENT
- IMPLEMENT CONTROLS

Recommended Practice 4.9.2

Recommendation— Each Contracting State should ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures should include, inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with the risk assessment carried out by its relevant national authorities.

In a few words:

-IMPLEMENTED CONTROLS HAVE TO ADDRESS:

C CONFIDENCIALITY

I INTEGRITY

A AVAILABILITY

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION

- **1. 0.6. The appropriate authority shall establish and implement procedures to share, as appropriate and in a practical and timely manner, relevant information to assist other national authorities and agencies, airport operators, air carriers and other entities concerned, to conduct effective security risk assessments relating to their operations.**

IN PRACTICE

- AESA has agreements with other national appropriate authorities. NATIONAL CRIPTOLOGIC CENTRE. We perform joint inspections
- AESA is in permanent contact with the industry through
  - Forums
  - Working Groups
  - Workshops & Training initiatives
  - Functional mailbox

ICAO

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION

- **1.7.1. The appropriate authority shall ensure that airport operators, air carriers and entities as defined in the national civil aviation security programme identify and protect their critical information and communications technology systems and data from cyber-attacks which could affect the security of civil aviation.**

IN PRACTICE

- AESA has helped the entities to identify their “critical systems” **AVSEC related.**
- AESA has provided a list, as a sample list. Entities can and must enlarge the list
- Critical systems with an impact on SAFETY have not been identified by AESA. Every entity HAS TO IDENTIFY those systems to meet PART-IS requirements. Coming soon.

ICAO

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION 1.7.1 CRITICAL SYSTEMS IDENTIFICACTION

IN PRACTICE. OVERSIGHT TIPS AND FINDINGS

CRITICAL FUNCTION	OBJECTIVE
Personnel access control to ZRS/ZC	Prevent unauthorized personnel access, aiming to introduce prohibited items to ZC
Vehicle access control to ZRS/ZC	Prevent unauthorized vehicle access, aiming to introduce prohibited items to ZC
Inspection of persons other than passengers and the objects they carry to ZRS/ZC	Prevent the introduction of prohibited items to ZC
Aircraft protection in an area other than ZRS/ZC	Protection of the aircraft and its operations
Inspection of passengers, belongings, and hand luggage	Prevent the introduction of prohibited items to ZC
Inspection of hold luggage, protection, and reconciliation	Prevent the introduction of prohibited items to ZC
Inspection of cargo/on-board supplies	Prevent the introduction of IEDs in unsecured cargo

CRITICAL FUNCTION	OBJECTIVE
Reception and review of cargo. Issuance and transmission of security status and other relevant data	Prevent the introduction of IEDs in the secure cargo supply chain
Protection in warehouse of secure cargo/on-board secure supplies	Prevent the introduction of IEDs in secure cargo (warehouse)
Protection of secure cargo/on-board supplies throughout the process (not warehouse)	Prevent the introduction of IEDs in the secure cargo supply chain
Inspection and protection of CO-MAIL and CO-MAT	Prevent the introduction of prohibited items to Z, aiming to protect the aircraft and its operations
Protection of AVSEC information	Protection of information that could facilitate an act of unlawful interference if known. Protection of classified information
Detection and interception of UAS	Detection and interception of UAS

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION

7.2. Airport operators, air carriers and entities shall identify in their security programme, or any relevant document cross-referenced in the security programme, the critical information and communications technology systems and data described in 1.7.1. The security programme, or any relevant document cross-referenced in the security programme shall detail the measures to ensure the protection from, detection of, response to and recovery from cyber-attacks, as described in 1.7.1.

IN PRACTICE

- AESA accepts: either a separate Cybersecurity Program or a specific mention within the Security Program to policies, protocols, documents
- AESA asks for specific examples of
  - 1 Protection from cyber attacks (controls); 2 Detection of cyber attacks; 3 Response to cyberattacks; 4 mitigation measures to reduce the impact of cyberattacks in time (THIS IS NOT A BUSINESS CONTINUITY MEASURE)

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION 7.2 CYBER MEASURES

IN PRACTICE. OVERSIGHT TIPS AND FINDINGS

- There is always a Cyber Program or mention to cyber documents, but
- Important items missing:
  - Specific measures to detect cyberattacks
  - Specific protocols to Response to cyberattacks

PROVISION

7.3. The detailed measures to protect such systems and data from unlawful interference shall be identified, developed and implemented in accordance with a risk assessment carried out by the airport operator, air carrier or entity as appropriate.

IN PRACTICE

- AESA asks for a detailed RISK ASSESSMENT
- AESA accepts internationally well known methods
  - Magerite
  - Arli-SI
  - ISO 27005
  - Cramm
  - Mehari
  - SP800-30

PROVISION 7.3 RISK ASSESSMENT

IN PRACTICE. OVERSIGH TIPS

- Main entities use Magerit or ISO 27005. Make AESA oversight activities easier
- If entities decide to use proprietary or purposed-built methodologies, AESA work is more complicated. Takes to time check and understand.
- Most common deficiencies that result from an incomplete or erroneous risk assessment
  - Critical systems and Risk Assessment items do not match
  - Impact parameter deem to be consider extremely too low in many occasions
  - Risk appetite not clearly defined
  - Risk treatment endorsed by the Hierarchy missing

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION

7.4 Where a specific authority or agency is competent for measures related to cyber threats within a single Member State, this authority or agency may be designated as competent for the coordination and/or monitoring of the cyber-related provisions in this Regulation

IN PRACTICE

- AESA is the Appropriate Authority for this matters
- It is defined in the NASP
- However works in close coordination with “other” cyber authorities in Spain. There are a few

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION

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

IN PRACTICE

- AESA does joint cyber inspections with OCC, Ministry of Interior
- Some entities are critical infrastructure (main airports) or essential operators (big airlines, or those who serve operations from the islands in Spain)
- We try no to bother the entities twice if possible. We share the findings. We learn from each other, since the scope of our inspections is different by complementary

ICAO

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION

11.1.2 Persons having administrator rights or unsupervised and unlimited access to critical information and communications technology systems and data used for civil aviation security purposes as described in 1.7.1 in accordance with the national aviation security programme, or having been otherwise identified in the risk assessment in accordance with 1.7.3.

Unless otherwise specified in this Regulation, whether an enhanced or a standard background check has to be completed shall be determined by the appropriate authority in accordance with applicable national rules.

IN PRACTICE

- The entity has to identify the role of administrator and designate the persons
- AESA asks for the list of administrators
- The administrators have to be subject to a BACKGROUND CHECK. Aesa checks the process.

ICAO

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019 vs Annex 17

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

PROVISION

11.2.8.1 Persons implementing the measures as laid down in point 1.7.2 shall have the skills and aptitudes required to carry out their designated tasks effectively. They shall be made aware of relevant cyber risks on a need-to-know basis..

IN PRACTICE

- Almost every body in the aviation sector deals with a critical system. So almost everybody needs training in cyber
- Entities are free to train the contents they want
- However AESA has produced training material to help them
- We check the the number of employees that have received the basic traning

PROVISION

11.2.8.2 Persons having access to data or systems shall receive appropriate and specific job related training commensurate with their role and responsibilities, including being made aware of relevant risks where their job function requires this. The appropriate authority, or the authority or agency as laid down in point 1.7.4 shall specify or approve the content of the course.

IN PRACTICE

- This training is much more specialised than 11.2.8.1
- AESA has produced the minimun content of the course. It is included in the NSTP
- During the inspections we check if the administrators have received the specialised traning. We asked for their training records.

AVIATION CYBERSECURITY OVERSIGHT IN SPAIN. NATIONAL PROVISONS NOT IN REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

NATIONAL PROVISION

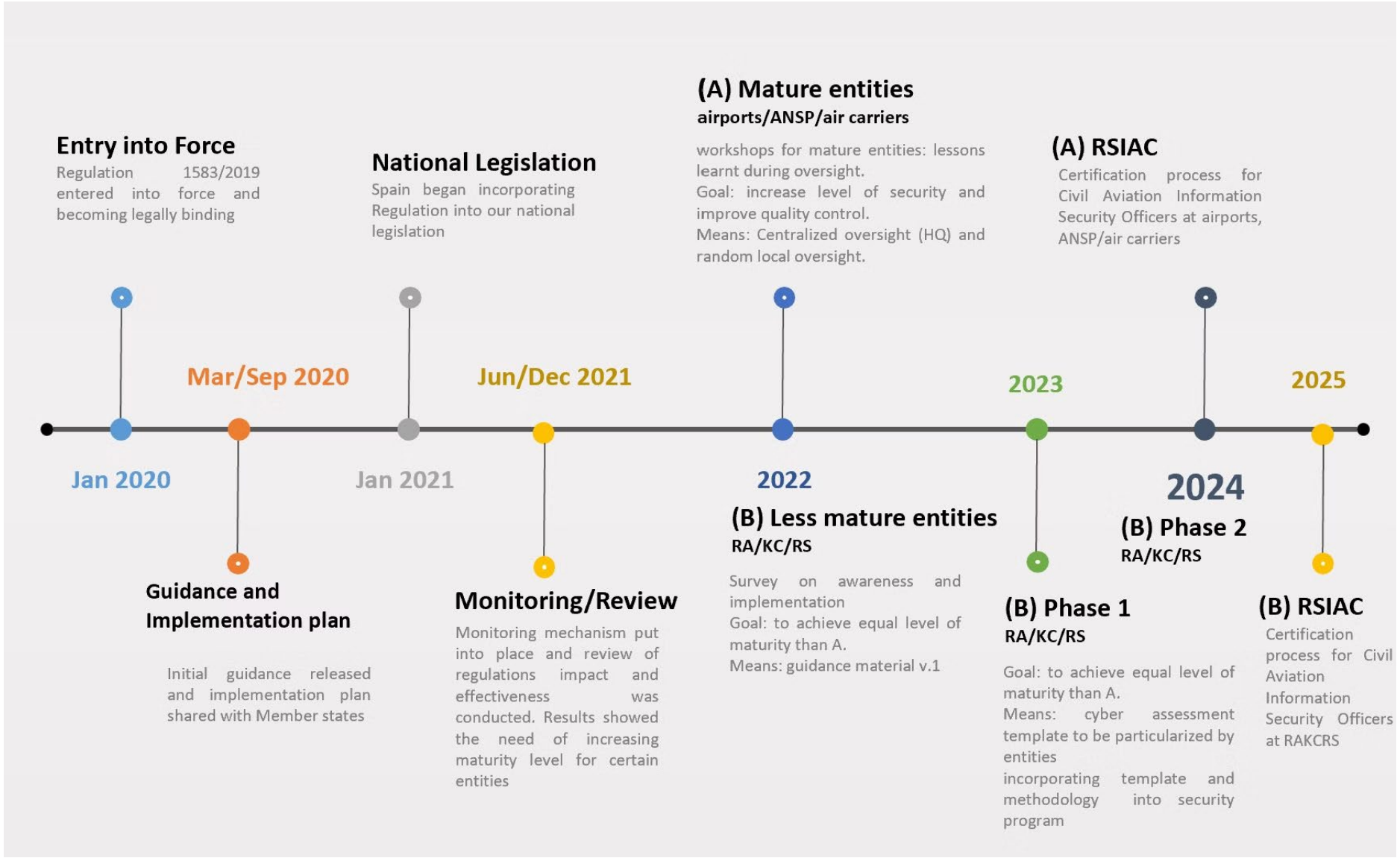
SA-16 4.1.1 Has the entity apointed an Information Security Officer? RSIAC

SA-16 4.1.2 Has the entity informed AESA?

IN PRACTICE

- AESA has certified the main entities RSIACs
  - Big Airlines
  - Main Airport Operator
  - Main ANSPs
- We have a roadmap to certify more RSIACs
  - RAs, KCs, small Airlines, not regular commercial

AVIATION CYBERSECURITY OVERSIGHT IN EUROPE
REGULATION 1583/2019 . SPANISH ROADMAP



AVIATION CYBERSECURITY OVERSIGHT IN SPAIN. NATIONAL PROVISONS NOT IN REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

NATIONAL PROVISION

SA-16 4.4.6 Has the entity identified third parties with access to Critical Systems

IN PRACTICE

- AESA asks for the list of providers

AVIATION CYBERSECURITY OVERSIGHT IN SPAIN. NATIONAL PROVISONS NOT IN REGULATION 1583/2019

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

NATIONAL PROVISION

SA-16 4.6.1 Has the entity a procedure to report potential cyber incidents to the Appropriate Authority?

IN PRACTICE

- AESA checks wether there is a procedure
- AESA asks for real incidents, and actual communitations to the CERT

NATIONAL PROVISION

SA-16 4.6.1 Has the entity a procedure to report potential cyber incidents to the Appropriate Authority?

IN PRACTICE

- AESA checks wether there is a procedure
- AESA asks for real incidents, and actual communitations to the CERT

Main Regulatory Requirements and Evidence

Regulatory Requirement	Evidence to Request	Key Audit Questions
1.0.6. Information Sharing	Documentation of exchange of information information with other authorities and entities.	Does the entity share relevant information information with other stakeholders? Is there there an established procedure for the exchange of information?
1.7.1-1.7.3. Identification and Protection of of Critical Systems	Security program, risk assessments, technical technical documentation of the systems.	Have critical information systems been identified? Is there an inventory of these systems? Have risk assessments been carried out? Have adequate security measures been implemented?
11.1.1-11.1.2. Recruitment	Hiring policies, background check records, job descriptions.	Are background checks conducted for personnel with access to critical systems? Do the verification procedures comply with legal requirements?
11.2.8. Training	Training plans, attendance records, training materials.	Is information security training provided to staff? Is the training appropriate for each employee's role? Are regular evaluations of the training carried out?

AVIATION CYBERSECURITY OVERSIGHT IN SPAIN. THE WAY FORWARD

PART-IS IMPLEMENTATION

- **information security measures with impact on safety**
- **joint risk assessment Safety and Security?**
- **joint inspections Safety and Security?**

REGULATION 1583/2019 MATURITY

- identification of critical functions/critical systems: AESA will be more demanding. more detail needed
- risk assessment methodologies: AESA will study in depth the methodologies presented
- risk treatment: AESA will ask for continuous improvement
- training courses: AESA will inspect the contents, to make sure are up to date
- Ready to apply the sanctioning regime allowed by the regulation?

THANK YOU

SSCC.SECRETARIAT-CCSA.SECRETARIAT@TC.GC.CA

HTTPS://TC.CANADA.CA/EN/INITIATIVES/SAFER-SKIES-INITIATIVE/SAFER-SKIES-CONSULTATIVE-COMMITTEE

Twitter: @icaoavsec | Linkedin: @ICAO AVSEC FAL | www.icao.int