EASA PART-IS

IMPLEMENTATION APPROACH

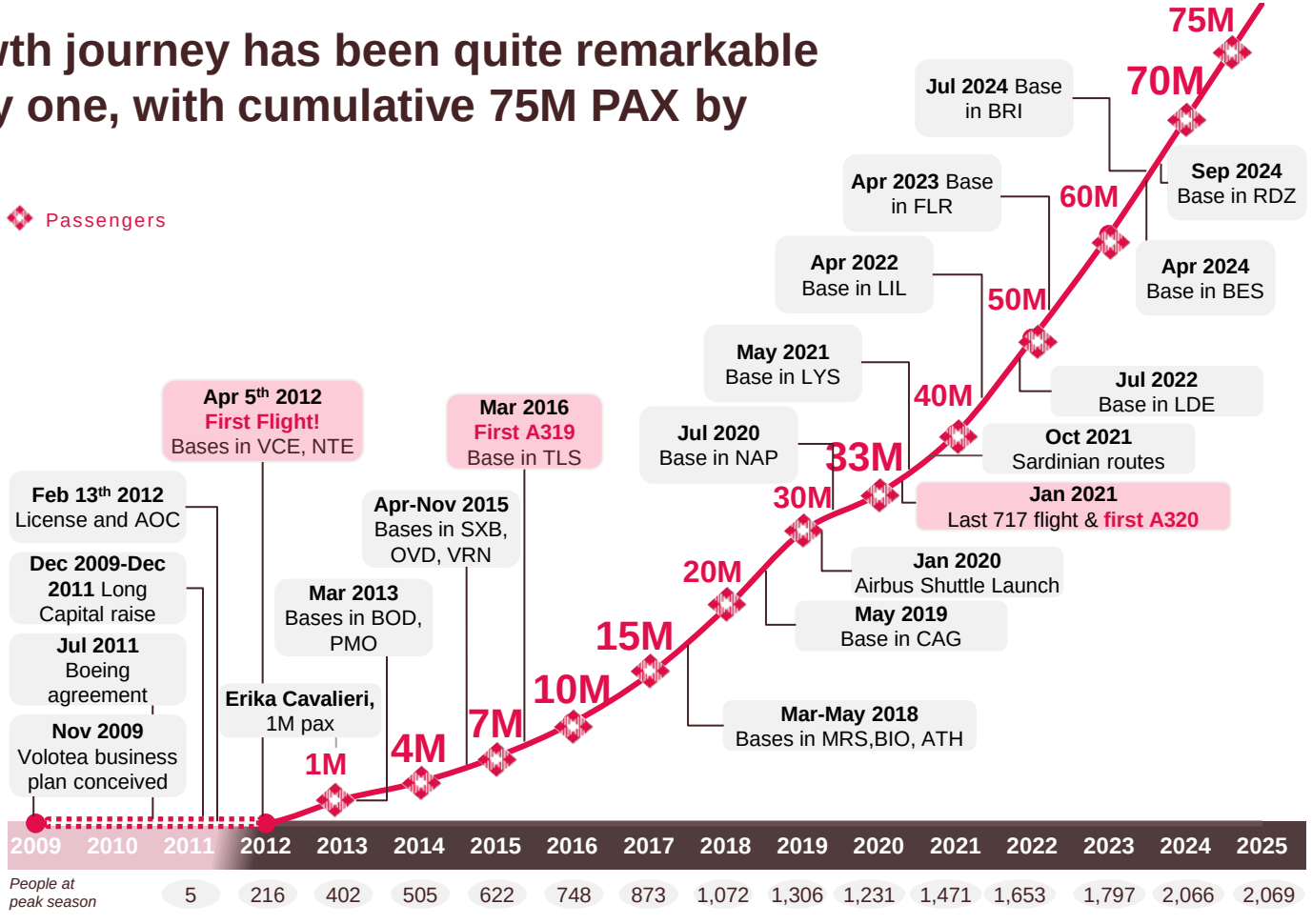
Nov 2025

VOLOTEA

Content

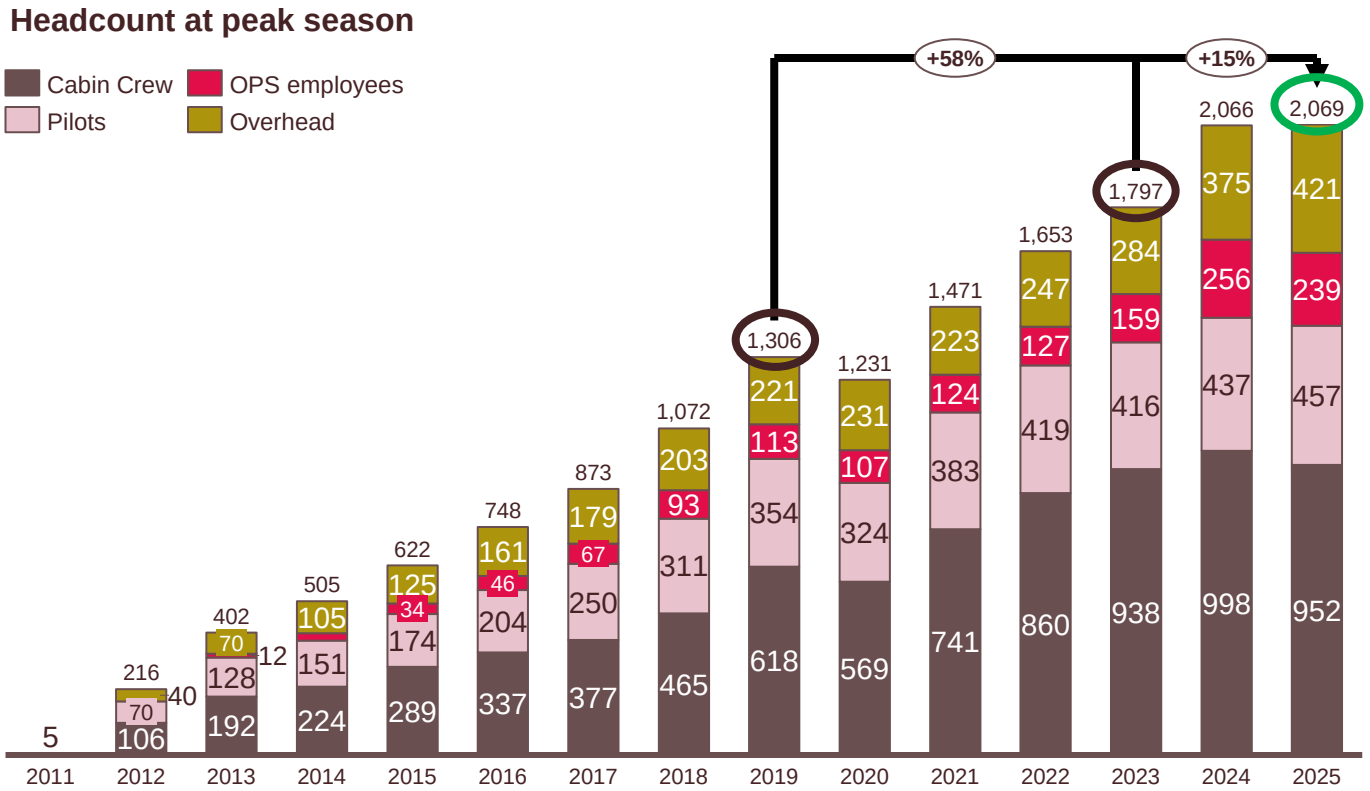
- VOE’s Background
- Part-IS: AESA’s Pilot Program
- Part-IS: Implementation Project
- Part-IS: Organizational structure of responsibilities
- Part-IS: Risk Management

Our growth journey has been quite remarkable since day one, with cumulative 75M PAX by mid 2025



Note: Years in the graph indicate end of year (e.g., 2024 corresponds to Dic. 24')

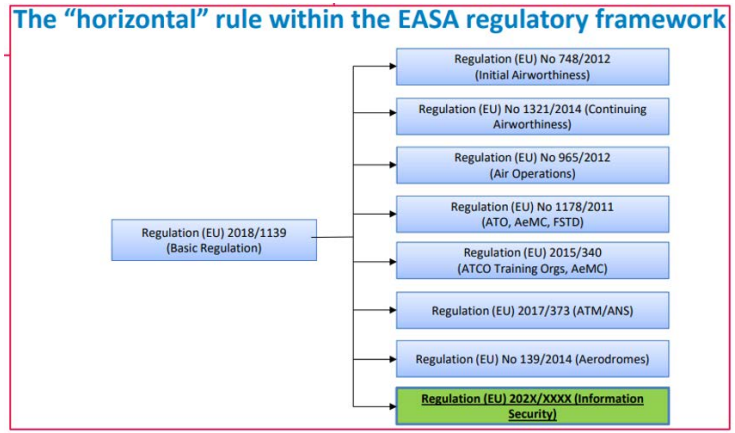
Starting with an initial group of five, Volotea team has grown rapidly, surpassing 2,000 employees since 2024



Our flight operation consists of 19 bases, resulting in 10 bases in France, 7 in Italy and 2 in Spain and expecting to launch some more in 2026 and 2027

Snapshot of VOE network

In 2019, the Cybersecurity team expanded its scope beyond the IT environment to also include the OT domain, namely our fleet and its operational ecosystem



Key milestones

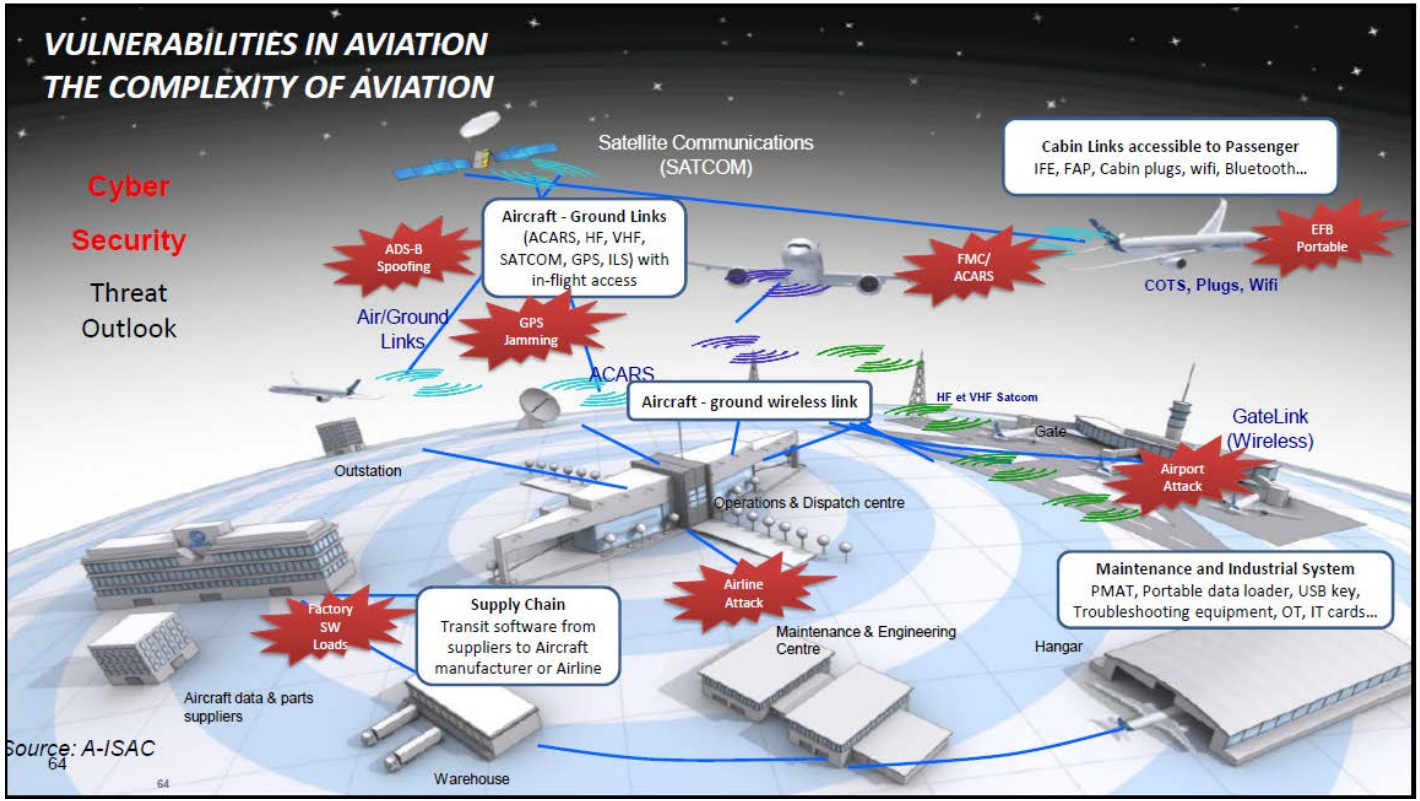
- Creation of a hybrid group to bridge Flight Operations areas (Safety, Maintenance, Crews, Engineering, etc.) and Cybersecurity.
- Integration of cybersecurity tasks into A/C daily basis.
- Engagement with leading communities focused on managing cybersecurity risks in aviation.

NATO's approach to cyber defence

Allies recognise that cyber-attacks could be as harmful to our societies as a conventional attack. As a result, cyber defence is recognised as part of NATO's core task of collective defence.

NATO declared cyberspace as a domain of operations – just like air, land and sea - at the Warsaw Summit in 2016. This enables NATO's military commanders to better protect missions and operations from cyber threats.

Aviation vulnerabilities, bridging the gap between IT and OT cybersecurity

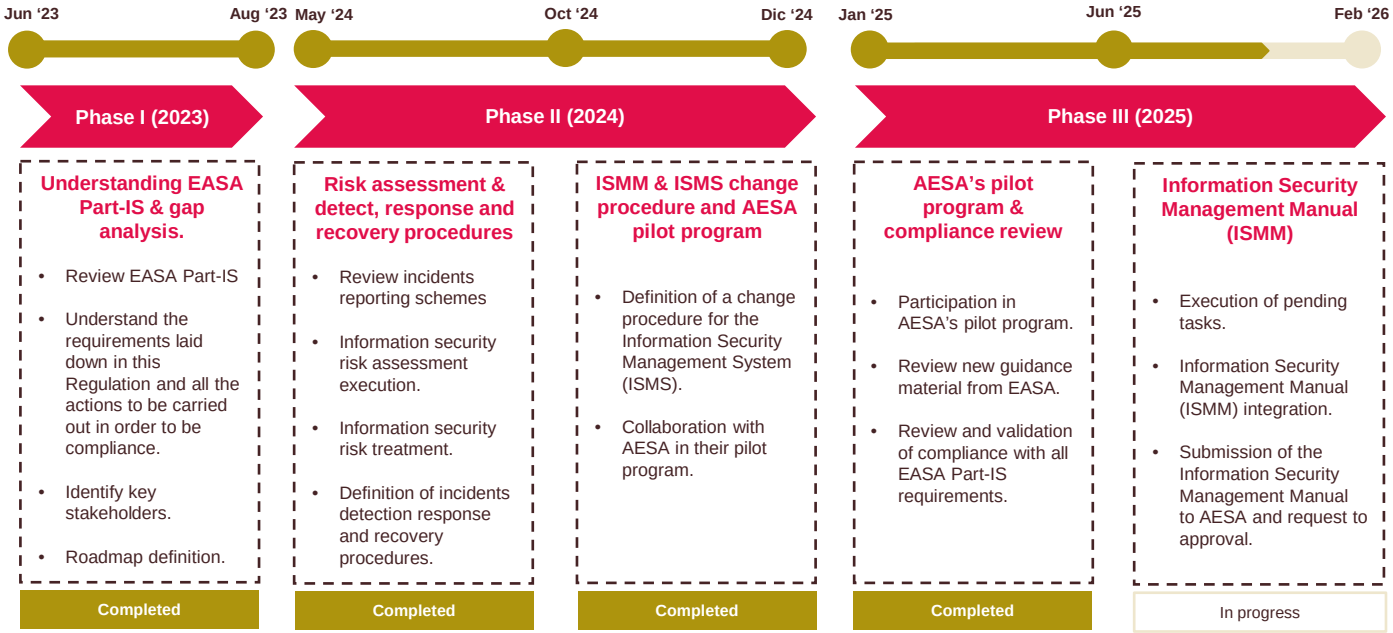


In-Flight cyber threats, understanding the risks to the aircraft in operation increased due to complexity of onboard systems

1. ACARS (Aircraft Communications & Reporting System)
2. ADS-B (Automatic Dependent Surveillance – Broadcast—out/in)
3. TCAS (Traffic Collision Avoidance System)
4. CPDLC (Controller Pilot Data Link Communication)
5. SATCOM (Satellite Communications):
6. IFE (In-Flight Entertainment)
7. EFB (Electronic Flight Bag)
8. Data Load

Our Part-IS implementation approach is divided into three phases, starting in 2023 with a review of regulatory requirements and concluding in 2025 with the submission of the ISMM to be approved by AESA

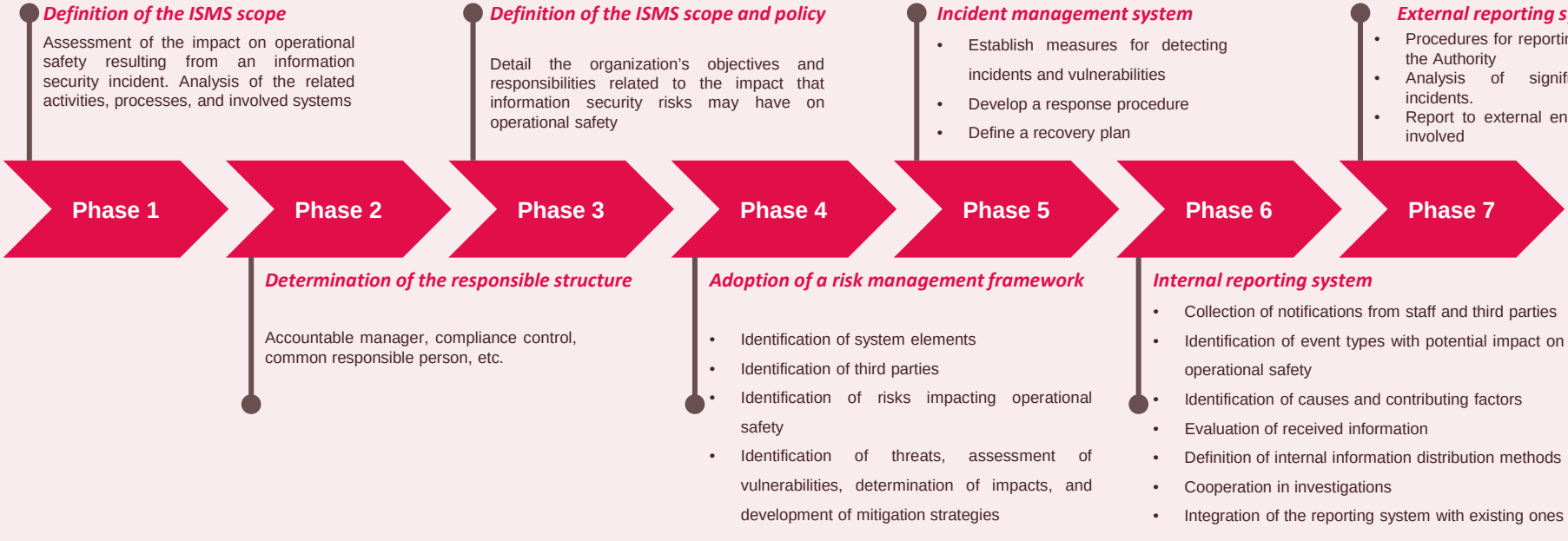
Project methodology timeline



Part-IS sets out the requirements to identify and manage information security risks with potential impact on aviation safety

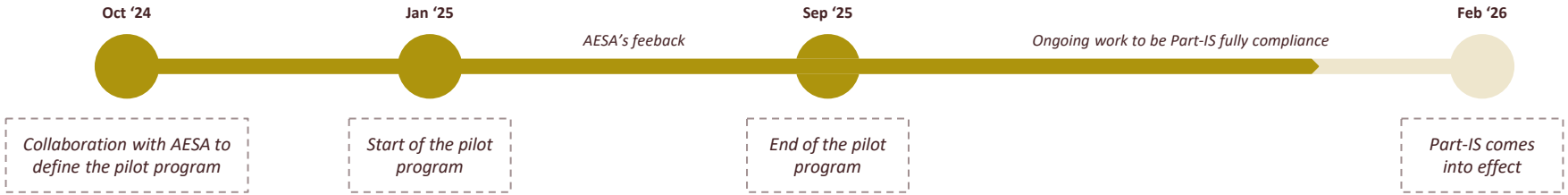
To comply with this regulation, the Safety and Cybersecurity departments must collaborate and build a bridge between them.

In Oct'24 VOE was proposed to be part of the AESA pilot program in relation to Part-IS. During 9 months, both entities followed a roadmap with key milestones to implement the Information Security Management System (ISMS) under EASA Part-IS Regulation



Collaboration was established with AESA through participation in its pilot program, which has now been completed and was followed to achieve Part-IS compliance based on a work plan defined by the authority

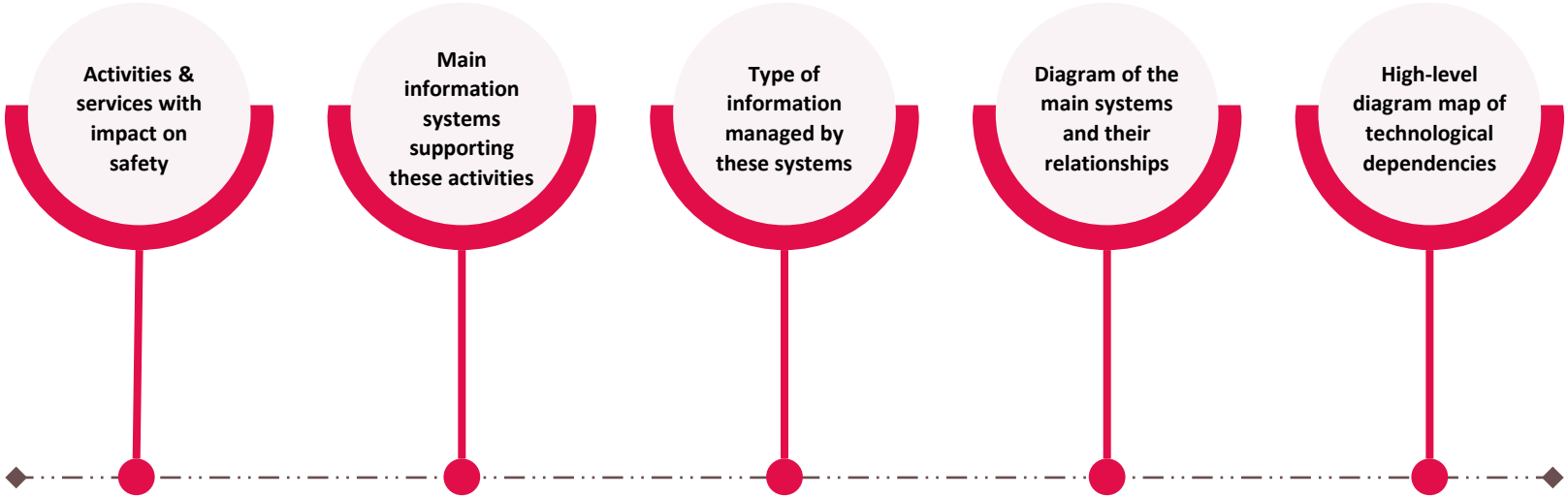
The main objective of participating in the AESA's Part-IS pilot program was to ensure that our approach to regulatory compliance was aligned with the expectations of the competent authority



Once the pilot program was completed, all **feedback** provided by AESA was used to **continue working towards compliance** with the regulation.

Phase	Task	Deadline	Status
I	Definition of the ISMS (Information Security Management System) scope	Jan '25	Reviewed with AESA
II	Determination of the responsible structure	Feb '25	Reviewed with AESA
III	Adoption of a risk management framework	Mar '25	Reviewed with AESA
IV	Establishment of an incident management system	Apr '25	Reviewed with AESA
V	Establishment of an internal reporting system	May '25	Reviewed with AESA
VI	Preparation of the ISMS Manual (Draft)	Sep '25	Reviewed with AESA

The scope of the ISMS must include all processes with potential impact on operational safety. To this end, all critical systems to safety, as well as their dependencies, must be identified



During the various phases of the Part-IS compliance project, several challenges have arisen and had to be addressed. The need for active collaboration between the Safety and Cybersecurity departments has been clearly identified

Main challenges identified

1) Review the scope of the asset inventory and risk assessment to include the operational environment, ensuring cybersecurity has visibility over safety-related risks.

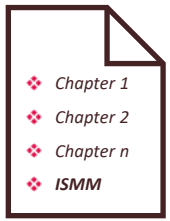
2) Increase and harmonize scope of current Information Security Management System (ISMS) to be aligned with the organization's Safety Management System (SMS).

Proposed Solution

1) Establishment of a **hybrid working group** *(Cybersecurity & Safety)* with the objective of identifying all **Safety-Relevant assets** within the organization.

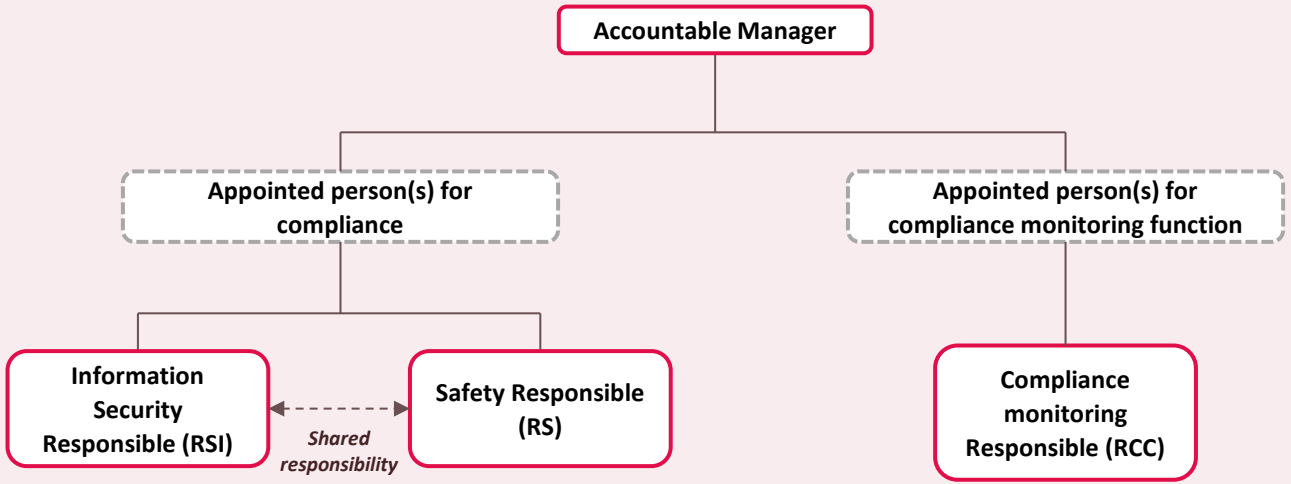
2) Leverage **synergies** between the SMS and the ISMM by **integrating the ISMM within the SMS** and referencing existing organizational procedures required by Part-IS.

Safety Management System



In accordance with the governance structure required by the regulation for Part-IS compliance, a set of roles and responsibilities has been determined within the organization

Part-IS proposed governance structure

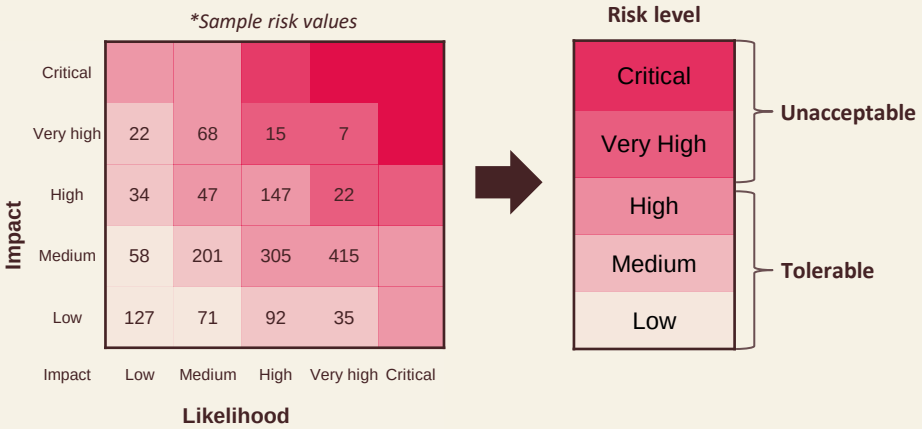


- The role of the **CRP** *(Common Responsible Person)* has **not** been considered **necessary** in the context of VOE.
- The **RSIAC** approved by **AESA SA-16** has been designated to fulfil the **RSI** role.
- A **shared responsibility model** has been established between the **RSI** and the **RS** regarding Part-IS compliance.

With the aim of identifying information security risks that could impact aviation safety, several adjustments were made to the risk management methodology

Cybersecurity risk assessment

The Safety-Relevant assets have been identified within the inventory that feeds the risk analysis process.



*Any risk exceeding the defined appetite must have an associated action plan. **Unacceptable risks** related to a **Safety-Relevant asset** shall be **notified** to the **Safety team**.*

Action Plan

*Any cybersecurity-related risk that has been escalated to the Safety team shall follow the standard **Safety risk management procedure.***

SIRA

(Safety Impact Risk Assessment)

*Once the impact on Safety has been assessed, the **hybrid working group** (Cybersecurity & Safety) shall determine an **action plan** to **mitigate** the **risk** to tolerable levels.*

THANK YOU

VOLOTEA