



# Cyber security trust framework

Ruben Flohr  
ATM Expert, SESAR JU

*10 November 2020*



Founding Members

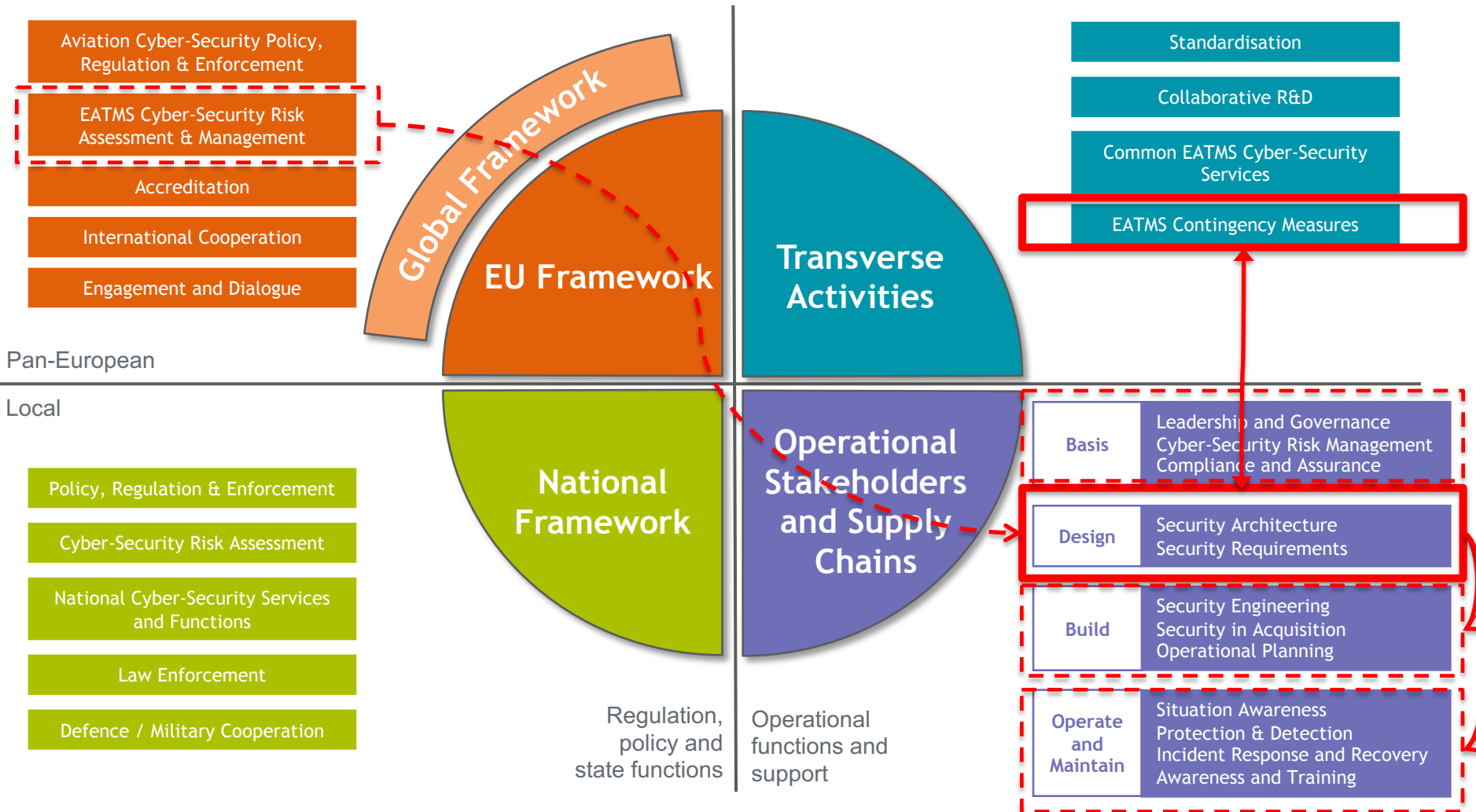


EUROPEAN UNION



EUROCONTROL

# Cyber study D2: European Target Framework

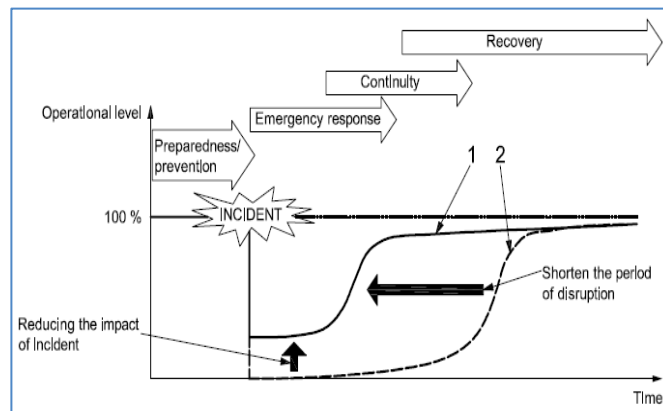


# The role of R&D in cyber resilience



Cyber resilient architecture

High level requirements for industrialization, deployment and operations



## Aspects of cyber-resilience

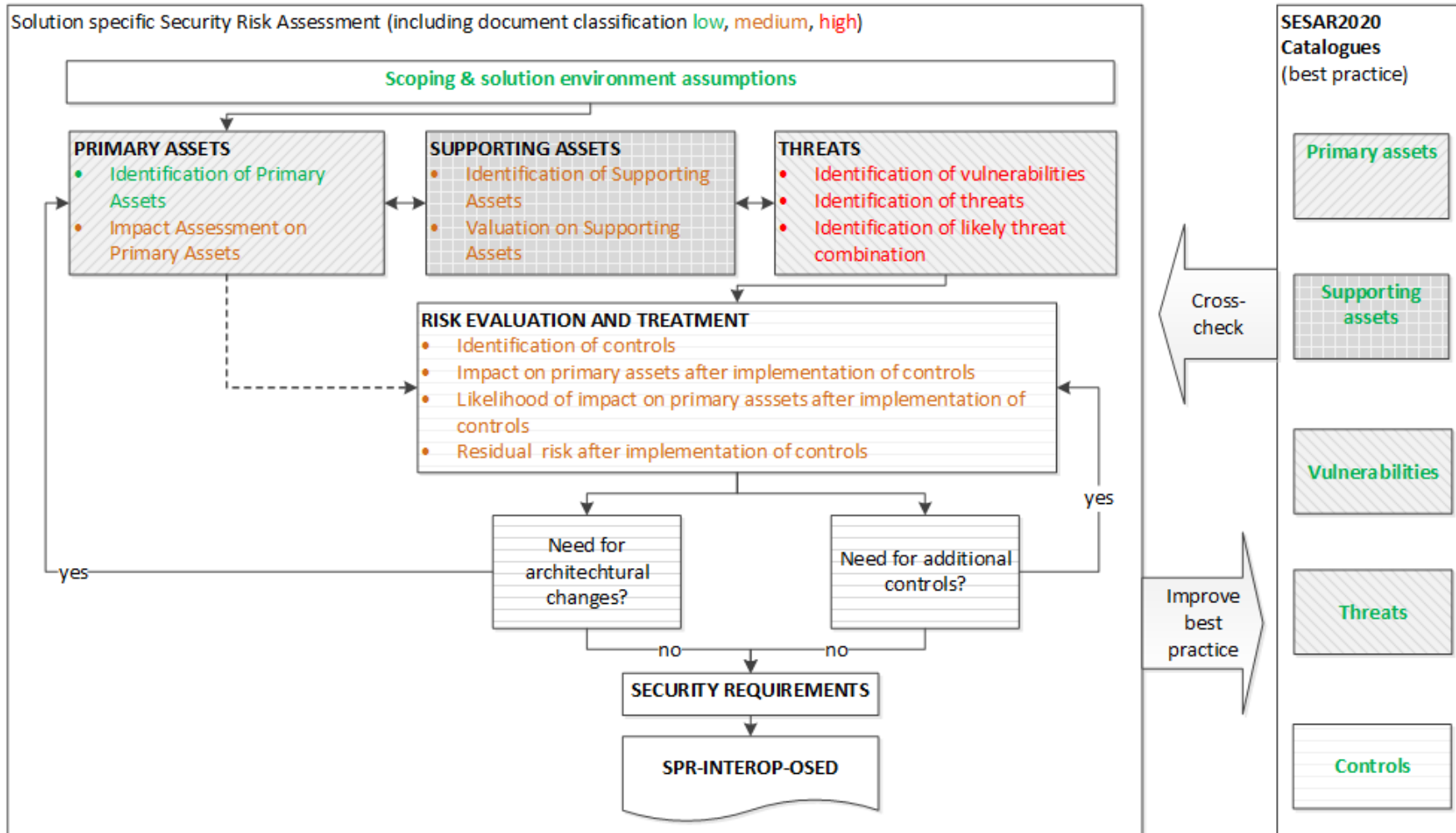
Foresight - prediction, anticipation  
 Robustness - ability to keep operating  
 Resourcefulness - control damage, mitigate it  
 Redundancy - substitutable  
 Rapid recovery  
 Adaptability - to changing environments

Identify  
 Protect  
 Detect  
 Respond  
 Recover

*Resilience is the ability to **prevent** disruptions, to **prepare** for and adapt to changing conditions and to **respond** and **recover** rapidly from disruptions to ensure the continuity of **services** at an acceptable performance level.*

# Security Risk Assessment Methodology

CYBER SECURITY OBJECTIVES (GIVEN)



# Clarified what to be done when

## 4.1 Checklist prioritized solutions

### Scoping & solution environment assumptions

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Scoping & solution environment assumptions	INITIALISE	Update	Update	Update

### Primary Asset identification and impact assessment

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Primary Assets	INITIALISE	Update	Update	Update
Impact Assessment on Primary Assets	INITIALISE	Update	Update	Update

### Supporting Asset identification and valuation

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Supporting Assets		INITIALISE	Update	Update
Valuation on Supporting Assets		INITIALISE	Update	Update

### Threats

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Vulnerabilities		INITIALISE	Update	Update
Identification of Threats		INITIALISE	Update	Update
Identification of Likely Threat combinations		INITIALISE	Update	Update

### Risk evaluation & treatment

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Controls		INITIALISE	Update	Update
Assets after implementation of Controls				
Likelihood of impact on Primary Assets after implementation of Controls		INITIALISE	Update	Update
Residual risk after implementation of controls		INITIALISE	Update	Update

### Security requirements

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Capturing controls as security requirements		INITIALISE	Update	Update

## 4.2 Checklist non-prioritized solutions

### Scoping & solution environment assumptions

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Scoping & solution environment assumptions	INITIALISE	Update	Update	Update

### Primary Asset identification and impact assessment

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Primary Assets	INITIALISE	Update	Update	Update
Impact assessment on Primary Assets	INITIALISE	Update	Update	Update

### Supporting Asset identification and valuation

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Supporting Assets		INITIALISE	Update	Update
Valuation on Supporting Assets		INITIALISE	Update	Update

### Threats

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Vulnerabilities		Optional	INITIALISE	Update
Identification of Threats		Optional	INITIALISE	Update
Identification of Likely Threat combinations		Optional	Optional	Optional

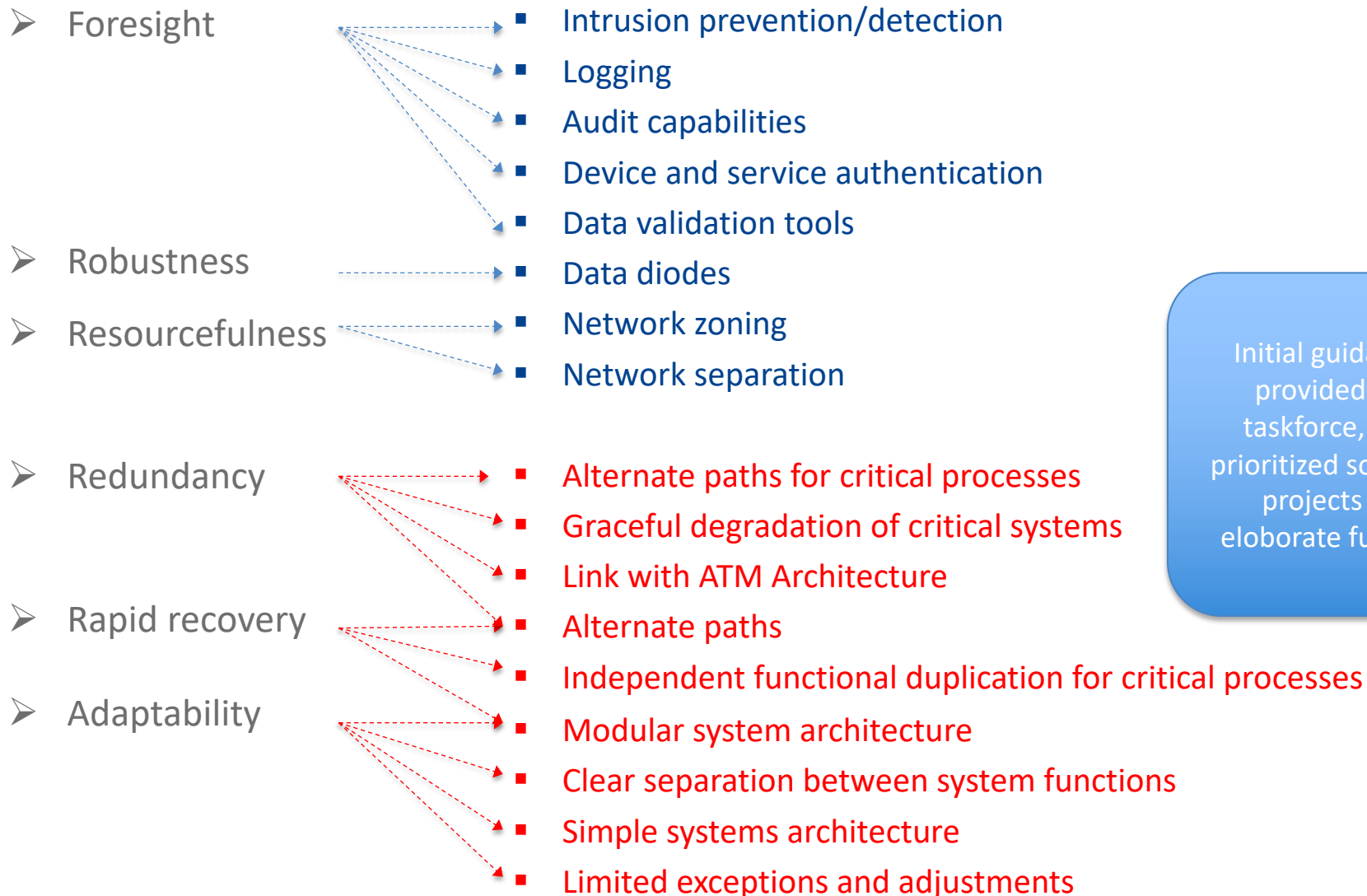
### Risk evaluation & treatment

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Identification of Controls		Optional	Optional	Optional
Impact on Primary Assets after implementation of Controls		Optional	Optional	Optional
Likelihood of impact on Primary Assets after implementation of Controls		Optional	Optional	Optional
Residual risk after implementation of controls		Optional	Optional	Optional

### Security requirements

	TRL2 (V1)	TRL4 (V2)	TRL 6 (V3)	VLD
Capturing controls as security requirements		Optional	Optional	Optional

# Cyber resilience controls



Initial guidance provided by taskforce, but prioritized solution projects to elaborate further

# 2018: SESAR issue on sharing security sensitive information



The security material developed by solution projects is sensitive material. Access to the solution's security risk assessments would provide hackers an easy entrance into aviation systems.

- A. From a legal perspective, management of this material has to comply with national regulation of all of our members. Potential non-compliance with any national regulations of any of our members may make the SJU or its employees liable in case of a security breach.
- B. From a legal perspective, management of this material has to comply with H2020 rules

## **Blocking information exchange of cyber security sensitive material**

- SESAR tools are not certified for exchanges of security critical material
- Requires many new personnel security clearances
- Liability in case of security breach of sensitive material

# 2019: The European Strategic Coordination Platform for Cybersecurity in Aviation (ESCP)

## Objective: Improve cyber resilience

<b>Operations continuity assurance is enabled with protections measures distributed along functional chains, which are appropriate to the level of risk.</b>	<b>Operational Systems can fail gracefully by ensuring continuity of essential functionalities.</b>
<b>Operational Systems adopt multi-layered protection measures that hinder the progress of an attack.</b>	<b>Aviation stakeholders understand the trans-organisational nature of the Aviation system and make use of connections to collaborate.</b>

## Objective: Self-strengthening aviation system

<b>Systems design practices are in place to avoid unintended use of functions exposed to users.</b>	<b>Systems design practices are in place to assess the risks of loss of security attributes and to implement protection measures, including adaptive solutions.</b>
<b>Assurance and scrutiny processes allow for the security effectiveness of systems during the whole lifecycle.</b>	<b>The level of protection against external causes is re-evaluated following a change in the original assumptions and, if necessary, restored.</b>



# 2020: ESCP on “Information sharing”



- Discuss which policies, legal basis and incentive scheme should be adopted to enable stakeholders' collaboration and sharing of sensitive information, respecting at the same time the security objectives of the EU Member States.
  - *Policies should encompass also collection, handling, marking, storing and disposal of such information.*
- Identify the needs of the different aviation stakeholders in terms of information sharing and which existing initiative and mean can be suitable.
- Discuss the possible cooperation and mutual support amongst stakeholders to improve resiliency in time of crisis.

# 2020: ESCP on “Information sharing”

<b>Aviation stakeholders understand the trans-organisational nature of Aviation system and make use of connections to collaborate</b>	
<b>S1.14</b>	Identify policies for the sharing and the handling of sensitive information that respect the security objectives of the European states;
<b>S1.15</b>	Develop the proper legal basis as well as the incentive for Organisations to enable them collecting, analysing and the disseminating cyber-incidents information in order to increase the base of available and relevant data to derive future mitigations.
<b>S1.16</b>	Build up a strong community of cybersecurity professionals in aviation to exchange good practices, information concerning new threats and vulnerabilities and ultimately offering mutual support for threat analysis, incident response and incident management.
<b>S1.17</b>	Create a portal, system, or means by which members of this community can collaborate and share information within a trust framework.
<b>S1.18</b>	Include military aviation stakeholders in the process, to ensure the required information sharing in escalating or crisis scenarios and to ensure early warning mechanisms and reduce reaction times.

# 2020: ICAO on cyber security



## **Secretariat Study Group on Cybersecurity (SSGC)**

- The forum to discuss all ICAO and related cybersecurity initiatives
- May be turned into an ICAO Cyber Panel, past the 40th ICAO Assembly.
- Critical, as it allows to globally export the ESCP Cyber Strategy.

## **ICAO INNOVA Project**

- Primarily a Trust Framework, applicable to any exchange of information
- Enables digital trust for the Internet technology-based Aeronautical Telecommunication Network (ATN)
- Builds upon operational needs of global aviation stakeholders

# Some questions

- What is more secure: old and obscure technologies or modern and open technologies?
- Should CNS be encrypted and how to secure existing non-encrypted CNS ?
- Technology is evolving faster & faster – how to ensure that our design is “future proof”?
- Avoiding tailor made approaches for aviation and opening up to new ideas from other critical infrastructures such as banking
- Is security so different from safety? Can we aim at a Safety and Security Management System?
- How to establish trust in a global environment?



ENGAGE cyber security – November 2020

---

Thank you very much  
for your attention!



Founding Members

