EASA
European Union Aviation Safety Agency

Workshop 1: “Cybersecurity from the global aviation perspective”

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

Cybersecurity risks are a global challenge

Elements driving the cybersecurity risks

Aviation is a "System of Systems", covering all aviation domains, and where products, services and organisations are increasingly interconnected.

Cybersecurity risks have no borders and are driven by the notion of malicious intent, where vulnerabilities are exploited and an accident is not a fortuitous event.

Cybersecurity risks evolve very quickly, which requires industry and authorities to do business differently.

The role of ICAO

The role of ICAO

- **In 2016, ICAO Assembly Resolution A39-19 instructed ICAO to develop a comprehensive cybersecurity work plan and governance structure;**

- **As a result, the SSGC (Secretariat Study Group for Cybersecurity) was established** under the authority of the Secretary General, being chaired by the Deputy Director for Aviation Security and Facilitation. **The SSGC is structured in four working groups:**
  - Working Group on Flight Safety (ANB lead)
  - Working Group on Air Navigation Systems (ANB lead)
  - Working Group on Airlines and Aerodromes (ATB lead)
  - Research Sub-Group on Legal Aspects (ATB/LEB lead)

The role of ICAO

- **Significant outcomes of the work of the SSGC:**
  - **Development of ICAO Cybersecurity Strategy**
    - Endorsed by ICAO 40th Assembly in October 2019
  - **Development of ICAO Cybersecurity Action Plan**
    - Presented to the SSGC for discussion and approval in December 2019.
    - Defines the cybersecurity programme for the next triennium.
    - Needs to be endorsed by the ICAO Council.

The ICAO Strategy: Main pillars

- **Cybersecurity Strategy – Main pillars**
  - International Cooperation
  - Governance
  - Effective Legislation and Regulation
  - Cybersecurity Policy
  - Information Sharing
  - Incident Management and Emergency Planning
  - Capacity Building, Training and Cybersecurity Culture

The ICAO Strategy: Main pillars

- **International cooperation:**
  - ICAO is the appropriate global forum to engage States in addressing cybersecurity in international civil aviation;
  - ICAO to facilitate and promote international events in the cybersecurity field.
- **Governance:**
  - States encouraged to support and build upon the ICAO Cybersecurity Strategy;
  - States to develop clear national governance and accountability for civil aviation cybersecurity;
  - States to include cybersecurity in their national civil aviation safety and security programmes.

The ICAO Strategy: Main pillars

- **Effective legislation and regulation:**
  - ICAO to provide States the basis for the development of appropriate legislation and regulation needed for the comprehensive implementation of the Cybersecurity Strategy;
  - ICAO to create, review and amend guidance material relating to the inclusion of cybersecurity aspects to safety and security.

- **Cybersecurity Policy:**
  - States to ensure that cybersecurity is a part of aviation security and safety systems and comprehensive risk management framework.

The ICAO Strategy: Main pillars

- **Information Sharing:**
  - ICAO to develop the Cybersecurity Repository and Point of Contact Network for sharing information on aspects such as vulnerabilities, threats, events and best practices.

- **Incident Management and Emergency Planning:**
  - States to amend existing contingency plans, include provisions for cybersecurity and conduct exercises to test cyber resilience.

The ICAO Strategy: Main pillars

- **Capacity Building, Training and Cybersecurity Culture:**
  - States to ensure that qualified personnel are hired, that there is increased cybersecurity awareness and training, and that cybersecurity innovation and research are promoted, along with cybersecurity culture – understanding the responsibility.

ICAO: Next steps

- → States to implement the Cybersecurity Strategy;
- → ICAO Council to endorse the Cybersecurity Strategy Action Plan;
- → ICAO to promote the Cybersecurity Strategy and the Action Plan;
- → States to develop their own action plan for the implementation of the Cybersecurity Strategy;
- → ICAO to start the implementation of the Action Plan and to monitor its implementation by States.

The creation of Regional Platforms and the experience of the European case

Background information on EASA involvement on cybersecurity

- EASA has been working on cybersecurity matters for a long time:
  - Initially, only for the certification of aircraft and engines (since 2003)
  - Later (after 2011), introducing certain cyber requirements for organisations involved in *Air Traffic Management, Air Navigation Services and Aerodrome operations*

- In May 2015, the European Commission tasked EASA to develop an Action Plan to:
  - Develop a coordinated defense against cyber threats
  - Minimize duplication and remove loopholes in regulation

As a result, EASA started working on a *"Comprehensive EU Cybersecurity Strategy for Aviation"* in coordination with EU Institutions and Agencies, States and stakeholders.

1. The importance of involving all the affected parties

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: *Aircraft/Engine manufacturers (ASD), Airlines (A4E, IATA, ERAA), Helicopter Operators (EHA), Aerodromes (ACI), Air Navigation Services (CANSO), Air Crew and maintenance personnel (ECA, ETF), Maintenance Organisations (EIMG), General Aviation (GAMA).*
- **Observers:**
  - ICAO (International Civil Aviation Organisation), FAA (US aviation authority), TCCA (Canada aviation authority), AIA (US manufacturers), AIAC (Canada manufacturers), NATO

The European Strategic Coordination Platform (ESCP)

- **The ESCP has been meeting regularly for more almost 3 years.**

- **The ESCP has been discussing, among other aspects:**
  - The development of an EU aviation cybersecurity strategy and action plan.
  - The approaches to take in order to coordinate this strategy at global level.
  - The development of common regulations for the management of cybersecurity risks.
  - The development of common methodologies for the risk assessments performed by different organisations.

2. The importance of developing a common EU cybersecurity strategy

The Strategy for Cybersecurity in Aviation

- **Developed by the European Strategic Coordination Platform (ESCP) and published on the EASA website on 10th September 2019**
- **According to this strategy, the future aviation systems needs to be:**
  - **A trustworthy and dependable environment,** where the different organisations can rely on the services and information provided by others
  - **A system-of-systems capable to adapt and to withstand new threats without significant disruptions,** following a systemic approach for current and legacy systems.
- **And the effort is focused on two aspects:**
  - **Making Aviation an evolutionary cyber-resilient system**, which, under attack, can maintain its essential functionalities.
  - **Making Aviation self-strengthening by adopting a “built-in security” approach** developed since the systems’ conception.
- **The strategy also contains objectives to achieve “cyber resiliency” and “built-in security”.**
- **The ESCP is working on the associated Implementation Plan**

3. The importance of global coordination

International Cooperation and Harmonization

ICAO SSGC (Secretariat Study Group on Cybersecurity)

- This is where all cybersecurity activities are coordinated at ICAO level.
- One of the activities has been the development of a global ICAO cyber strategy and action plan.
  - Members from EASA and from the ESCP have participated to ensure a coordinated approach between the global ICAO cyber strategy and the EU cyber strategy, as well as the associated action plans.

Other initiatives

- **FAA (ederal Aviation Administration):** Mainly on regulatory activities and standards.
- **Military Sector:** Since both civil and military share the same airspace.
- **Other EU Agencies:** Covering other transportation modes (ERA, EMSA).

4. The importance of developing an EU regulatory framework consistent with other EU cyber requirements

Common rules for the management of cybersecurity risks:

→ **Introducing common requirements for Information Security Management Systems and reporting of incidents.**

→ **Covering all aviation domains and interfaces, and applicable to organisations and authorities** *(aviation is a system-of systems).*

→ **Consistent with other EU requirements** such as NIS Directive 2016/1148 and Aviation Security Regulation 2015/1998 *(no gaps, loopholes or duplications).*

5. The importance of facilitating the coordination between the different authorities within each Member State

Coordination between authorities within the Member States

- **Essential because:**
  - **Cybersecurity is just at the interface between security and safety.**
  - In most cases, **there are different authorities within the Member States responsible for safety and security**:
    - National Aviation Authorities, Ministries, Cybersecurity Agencies, etc.
  - **There are different EU regulatory frameworks including cybersecurity requirements, with possible different authorities responsible for each one of them:**
    - Directive 2016/1148 (NIS Directive for essential services)
    - Regulation 2015/1998 (Aviation security)
    - Future EASA rules (currently under development)

  It is important to align regulatory requirements and inspection regimes.

6. The importance of promoting and facilitating the collaboration and information sharing between different parties, supported by adequate research initiatives

Collaboration and Information Sharing

ECCSA (European Centre for Cybersecurity in Aviation)

- **Objectives:**
  - Promote networking and information sharing among organisations and authorities, promoting a cybersecurity culture and trust environment.
  - Increase the understanding of risks and threats, and overall situational awareness.
- **Currently implemented with the support of CERT-EU (Computer Emergency Response Team of the European Union)**
- **Currently around 25 members.**

EASA
European Union Aviation Safety Agency

Questions

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union

Aviation Partnership Project Workshop on Cyber Security in Aviation

Workshop 2:

A Strategy for Cyber Security in Aviation

DR REBEKAH TANTI-DOUGALL

LEGAL CONSULTANT ON THE CYBER THREAT TO AVIATION

:

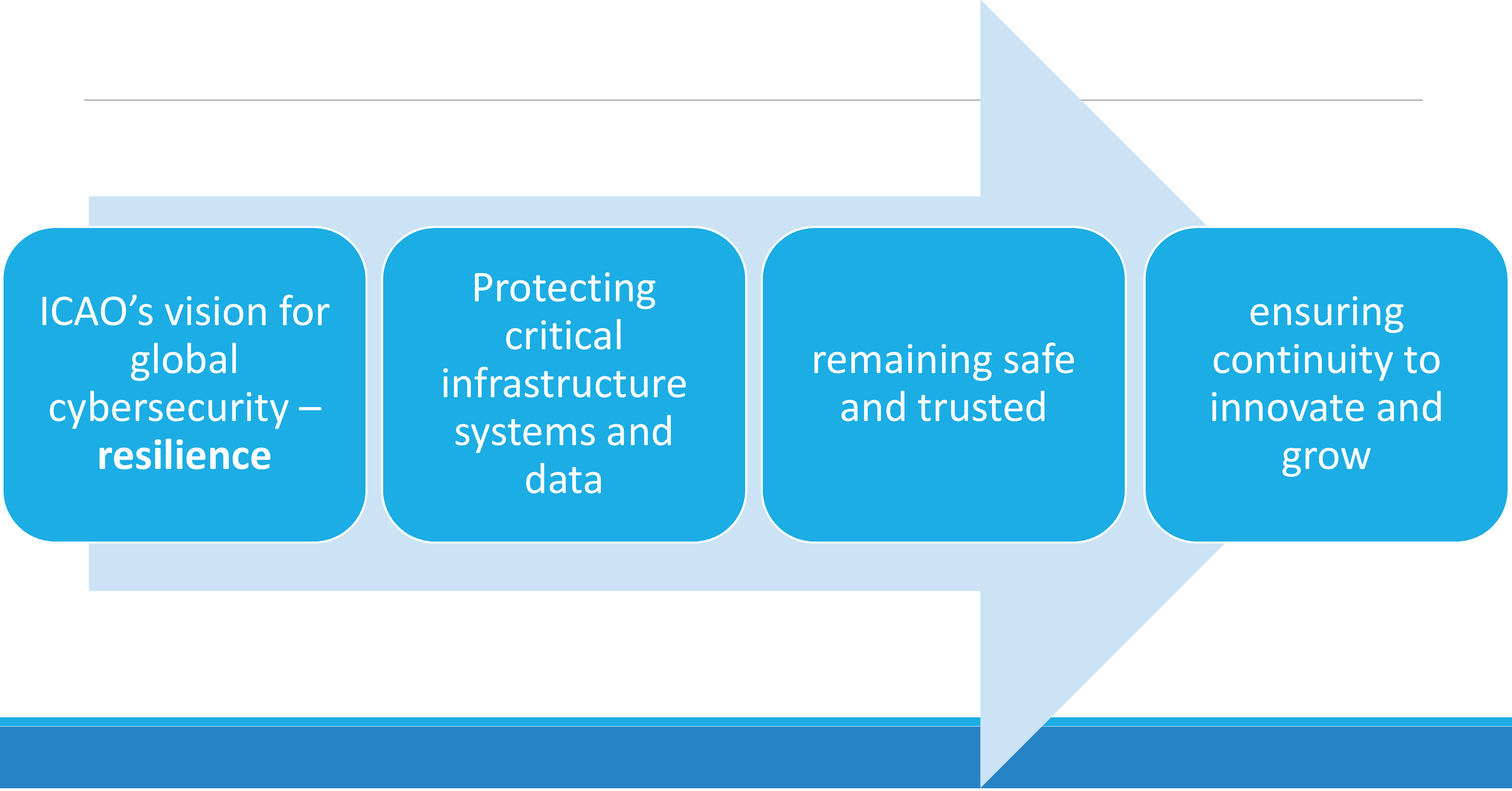
ICAO Secretariat Study Group on Cybersecurity [SSGC]

Member States, International Organisations and ICAO

4 Working Groups: Aerodromes and Airlines, Flight Safety, Air Navigation Systems as well as Legal

The strategy is the outcome of various discussions and meetings of the SSGC

The Strategy – what it seeks to achieve



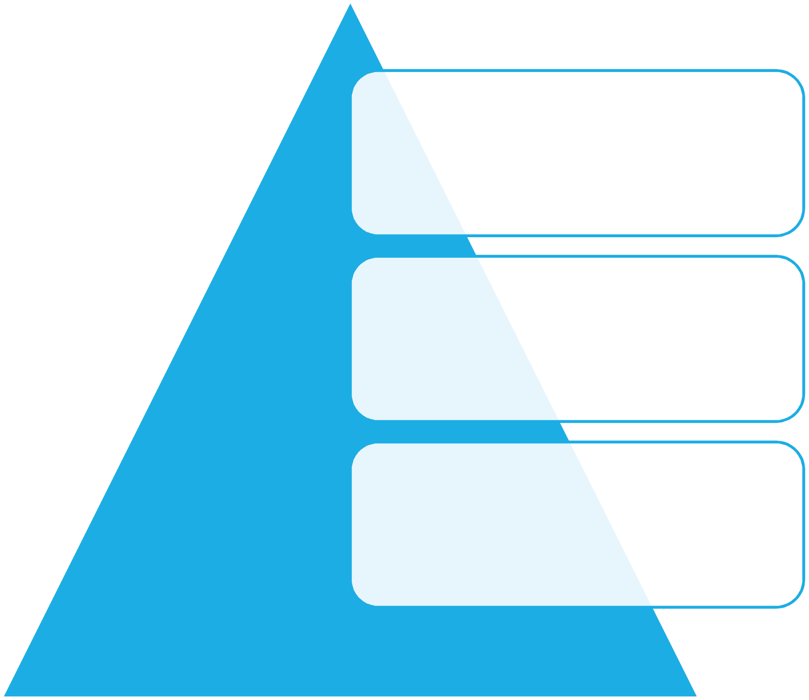
ICAO’s vision for global cybersecurity – **resilience**

Protecting critical infrastructure systems and data

remaining safe and trusted

ensuring continuity to innovate and grow

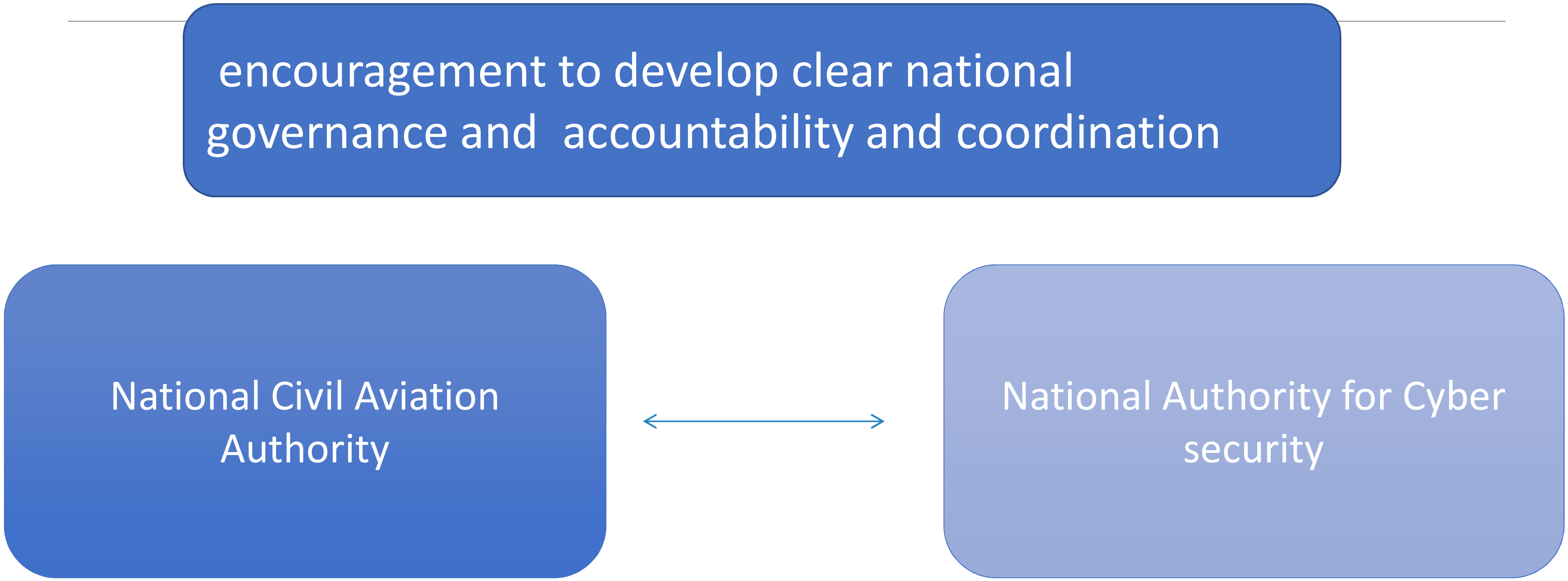
7 pillars in the strategy



International cooperation

- Both are borderless in nature.
- cooperation to ensure protection from cyber threats to safety and security.
- Harmonisation at national, regional and international

Governance



encouragement to develop clear national governance and accountability and coordination

National Civil Aviation Authority

National Authority for Cyber security

Cybersecurity policy

guidance material on the threats and risk assessments

Information sharing

- vulnerabilities,

- threats,

- events

- best practices

Through trusted relations

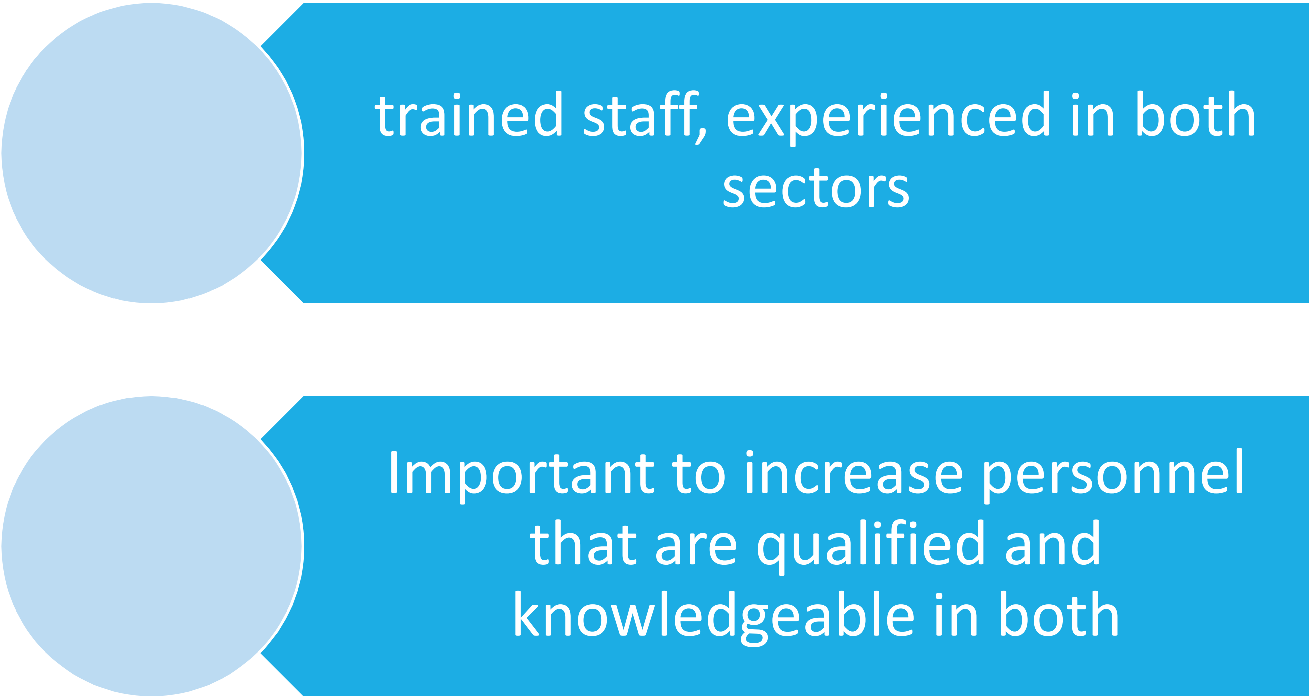
For early detection and to reduce impact of attacks

Incident management and emergency planning

Importance of having appropriate plans for the continuity during

and after cyber incidents.

Capacity Building, Training and cybersecurity Culture



trained staff, experienced in both sectors

Important to increase personnel that are qualified and knowledgeable in both

Legislation and Regulations

Legal Working Group

Legal Elements

International Law

Beijing

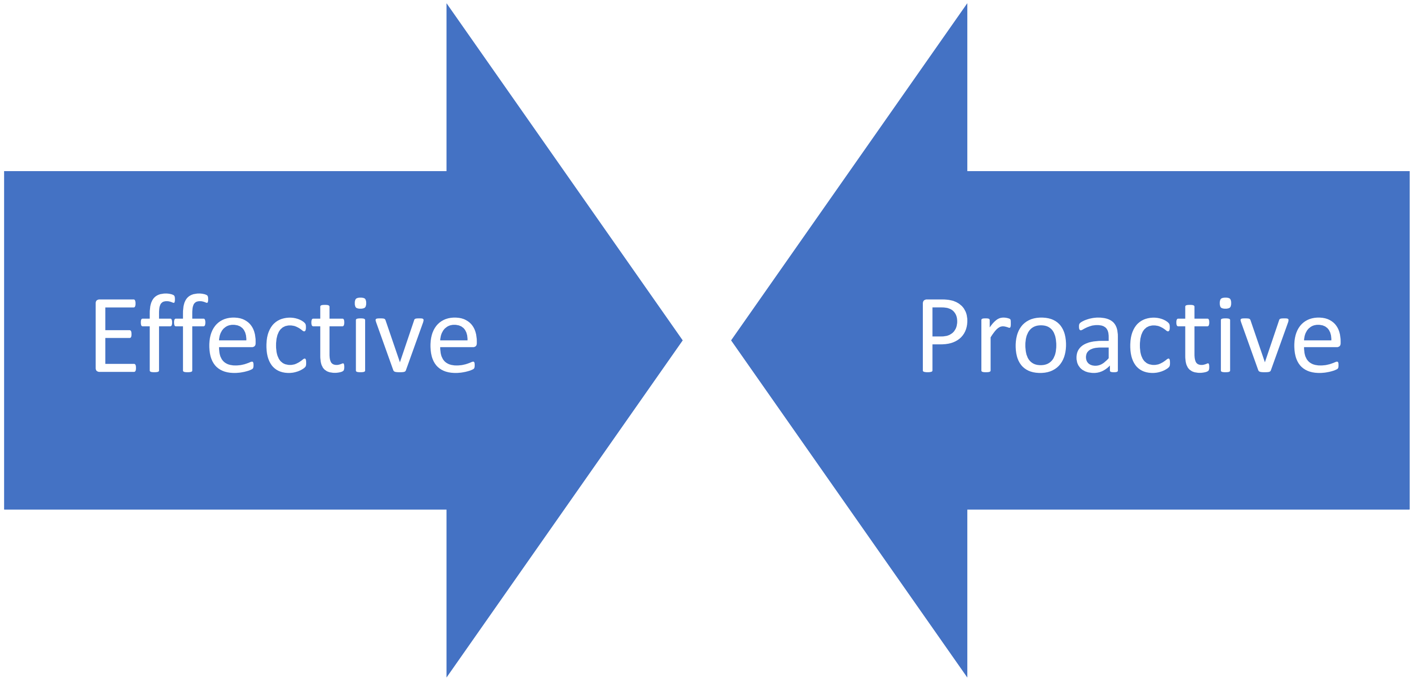
Lexicology

Appropriate National Law

Legal Aspects

- – Cross Border
  - Where was the offence committed?
- – Jurisdiction
- – Legal basis for Prosecution [legal provision]
- – Punishment
- – Awareness of the Judiciary

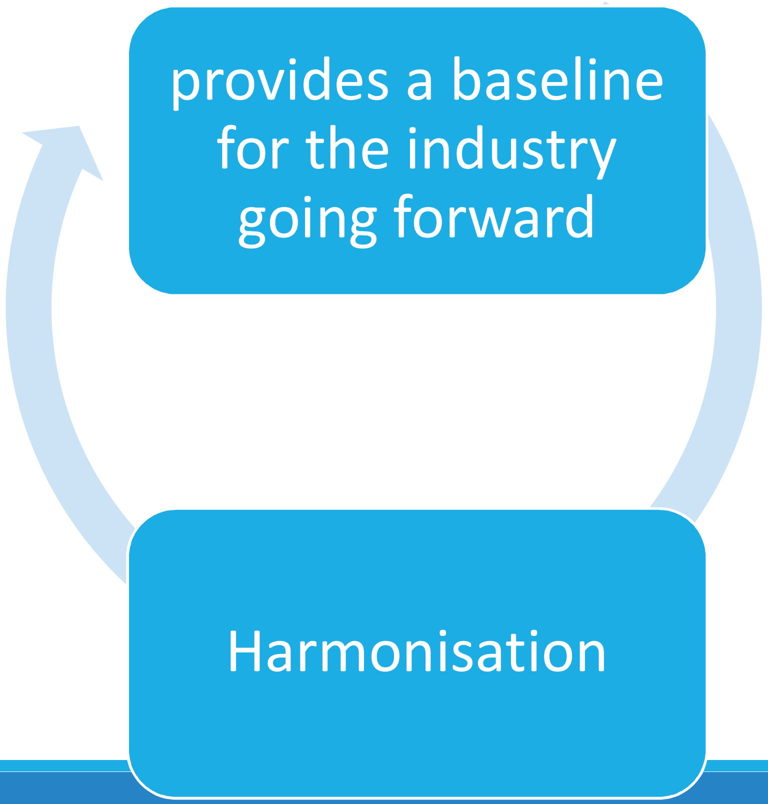
Legal Framework



Effective

Proactive

Conclusion - Strategy



provides a baseline for the industry going forward

Harmonisation

Thank you!

TRAFICOM
Finnish Transport and Communications Agency

Cybersecurity in Aviation

Katunayake Sri Lanka
5-7.2.2020

Workshop ONE: Cybersecurity From the Global Aviation Perspective

- Aviation is a global ecosystem, similar risks everywhere
- Local specialities
  - Environment, governance, culture etc.
- Limited resources and expertise
- ESCP & Finland

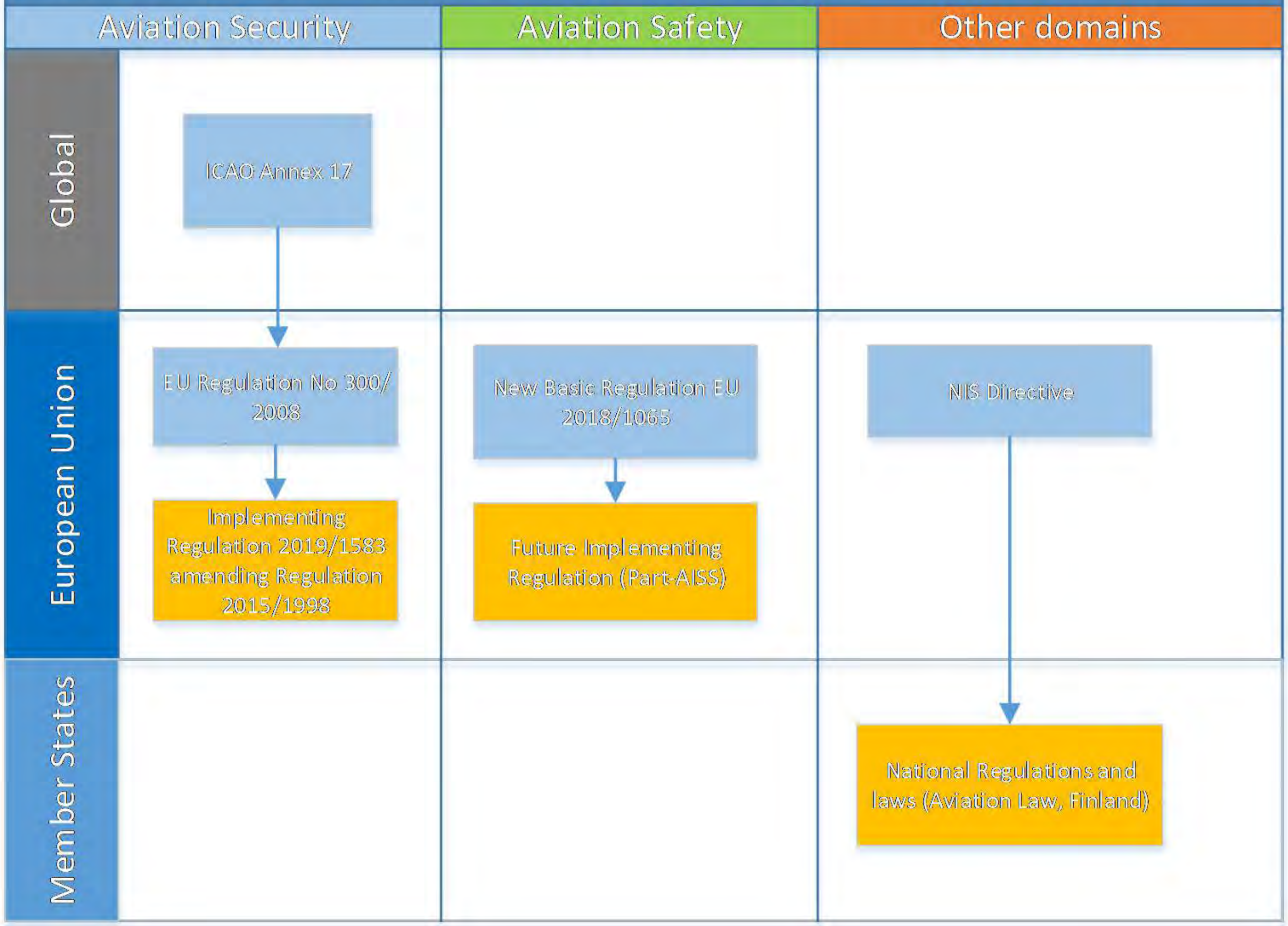
TRAFICOM

Workshop THREE: The Implementation Plan for the Cybersecurity Strategy

- Strategy & implementation plan as an asset
  - The Pilars as building blocks at regional and national level
- At national level:
  - policy
  - governance model
  - Risk management
  - Information sharing
  - Incident management
  - Capacity building, training and awareness

TRAFICOM

Cybersecurity in Aviation, High Level Legal Framework



Aviation Security

Aviation Safety

Other domains

Global

European Union

Member States

ICAO Annex 17

EU Regulation No 300/ 2008

Implementing Regulation 2019/1583 amending Regulation 2015/1998

New Basic Regulation EU 2018/1065

Future Implementing Regulation (Part-AISS)

NIS Directive

National Regulations and laws (Aviation Law, Finland)

TRAFICOM

Workshop FIVE: Information Security Management System (ISMS) and coordination with other Regulatory Frameworks

- Several cyber regulations
  - Cybersecurity for: aviation safety, aviation security, society
  - Information security management as a common thread
- CAA-FI is the Competent Authority for civil aviation cybersecurity in Finland
  - Interactive collaboration with
    - Ministry, agencies, authorities and organizations
  - Aim to leverage existing strong safety & security culture
    - Integration of management systems: SMS (Safety Management System, Security Management Systems and Information Security Management System)
  - Holistic approach over different aviation domains

Workshop SIX: Introduction to Risk Management Aspects

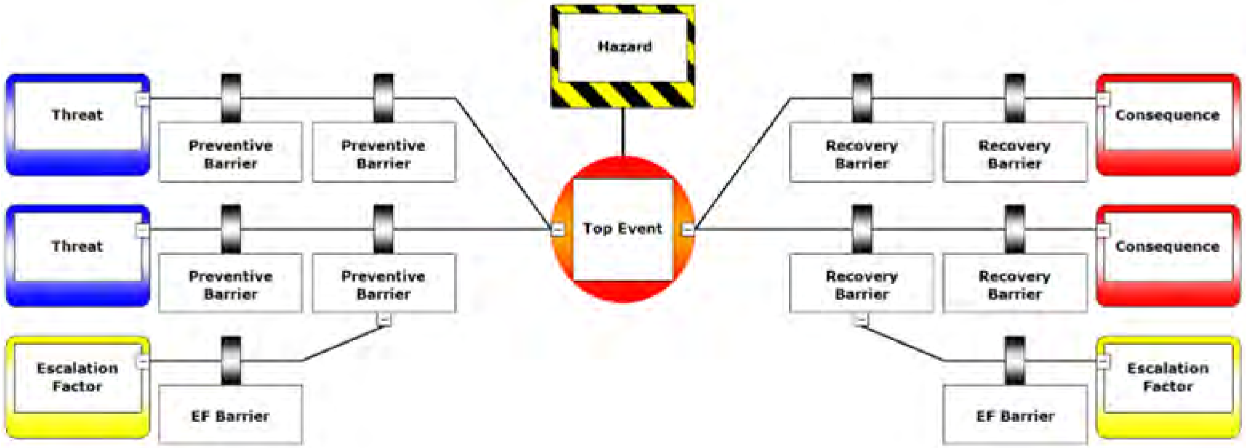
- Information security risk management in the safety context
  - Coordination between aviation security, safety and information security experts is a key

TRAFICOM

Workshop SIX: Introduction to Risk Management Aspects

– Different levels in risk management
Short case study

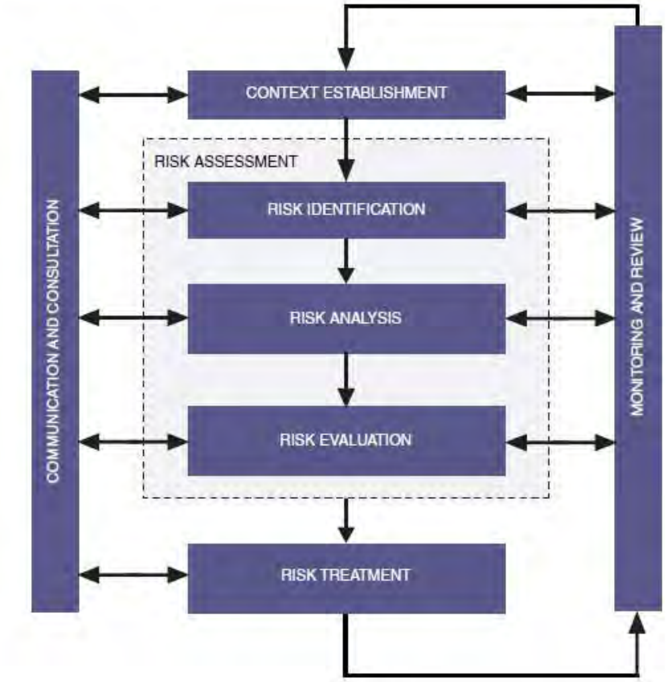
- National level
- All aviation domains
- Key strategic organization
- NCSC-FI
- No standards available



Workshop SIX: Introduction to Risk Management Aspects

– Different levels in risk management
  Short case study

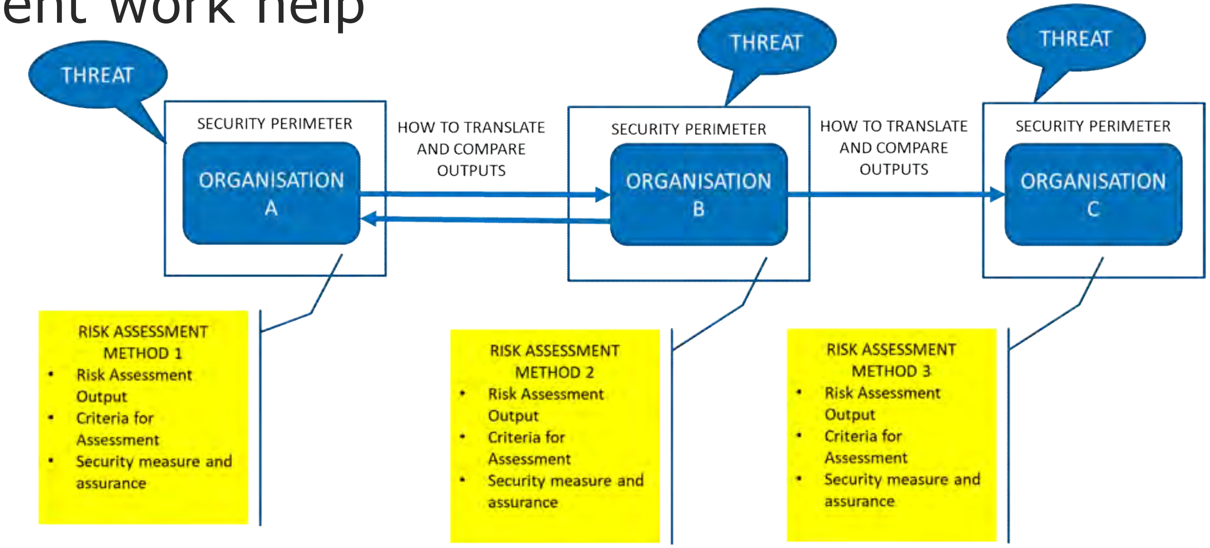
- Organizational level
  - Iaw standards



ISO 31000 / 27005

Workshop EIGHT: Introduction to the Sharing of Information

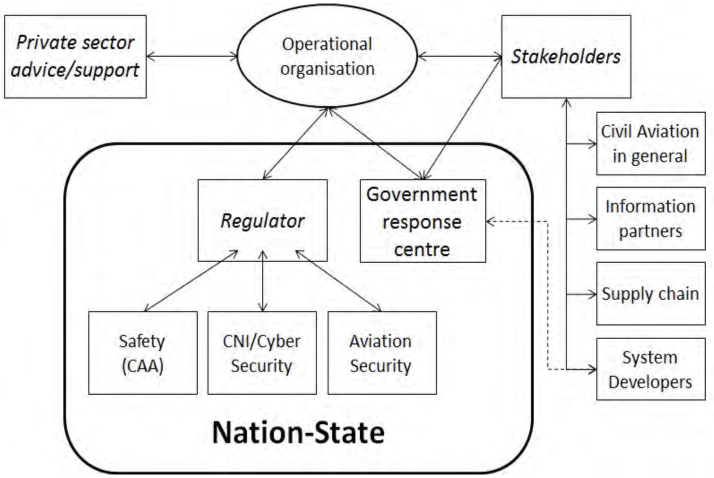
- Proactive: threat intelligence, vulnerability information
- National level risk management work help organizations to understand interdependencies



Picture: ED-201a?

Workshop EIGHT: Introduction to the Sharing of Information

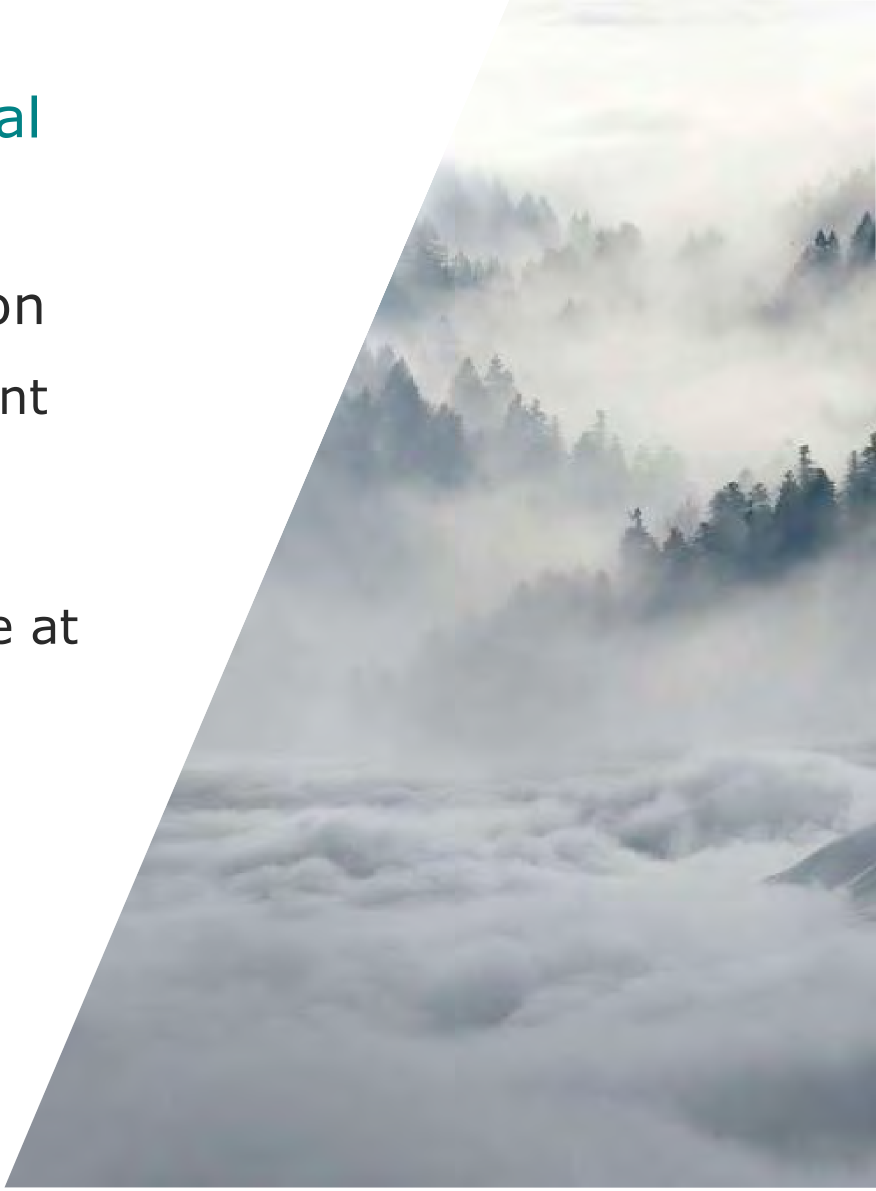
- Reactive: incident response information
  - Collaboration when something is not right
  - Information sharing mechanism
    - What, when, with whom and how to should information be shared



ECAC Cyber Study Group in Civil Aviation: Guidance material, Information sharing relationships from the **national** perspective

Workshop NINE: Sharing of Operational Information (SOC, CERT, CSC, ISAC)

- Reactive: Incident response information
  - Continuous monitoring and quick incident response
    - Detect, respond and recovery
  - How to make right information available at right time at right context?



TRAFICOM
Finnish Transport and Communications Agency

tomi.salmenpaa@traficom.fi
www.traficom.fi
@TraficomFinland

EASA
European Union Aviation Safety Agency

A Strategy for Cybersecurity in Aviation

Davide Martini
Senior Expert - Cybersecurity in Aviation

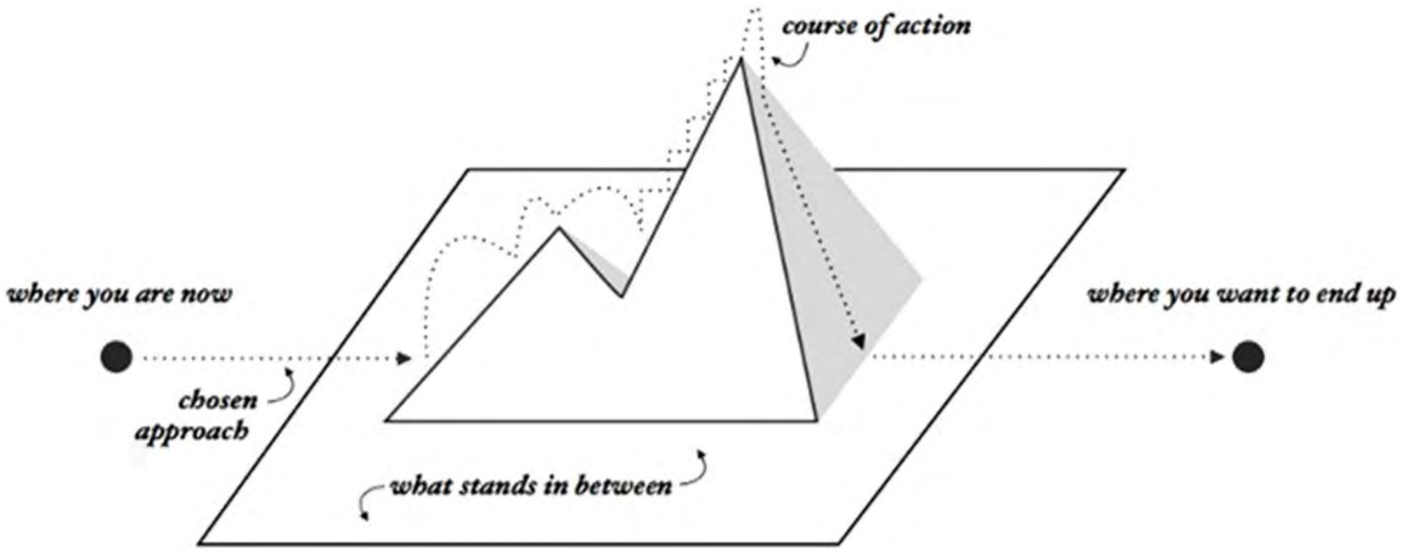
5th – 7th February 2020
Colombo – Sri Lanka

Your safety is our mission.

An Agency of the European Union

STRATEGY

the practice of figuring out the best way to get from here to there

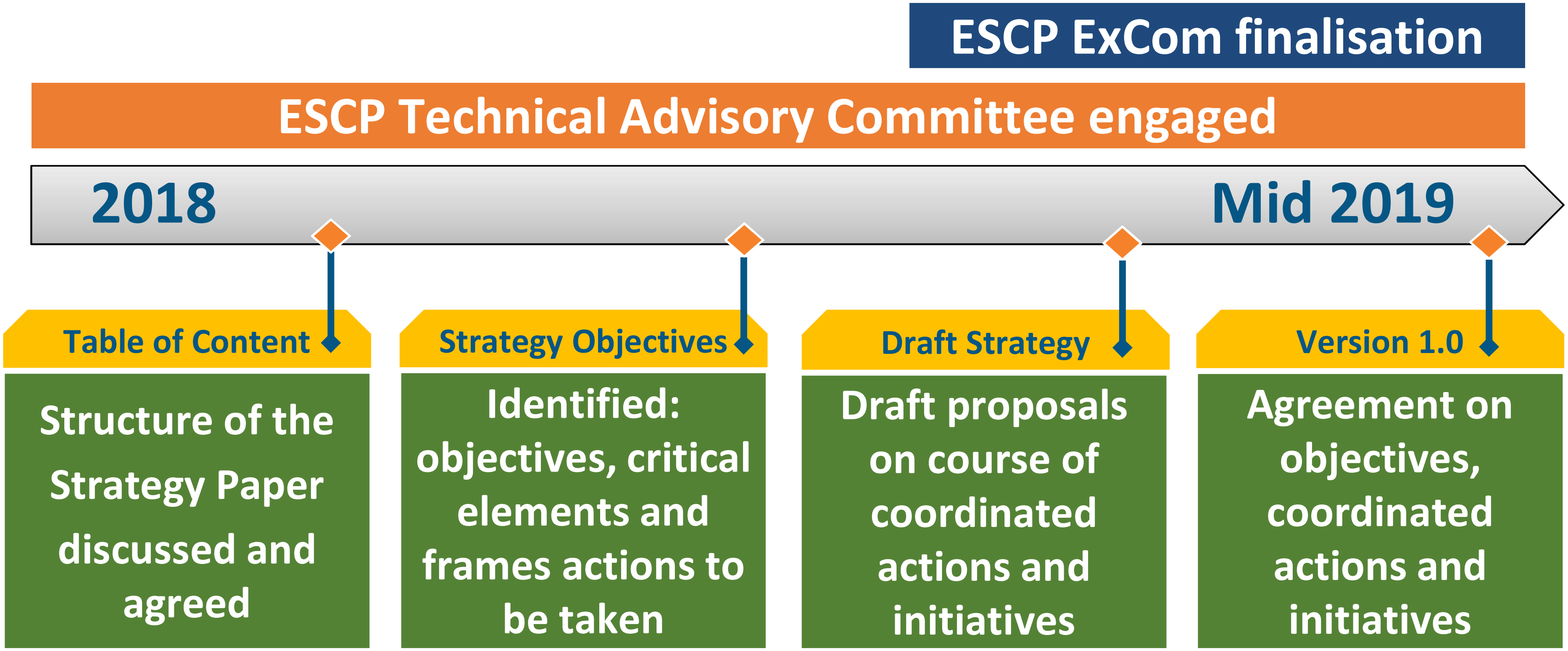


The European Strategic Coordination Platform (ESCP)

- **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 2.5 years

Work Plan



ESCP ExCom finalisation

ESCP Technical Advisory Committee engaged

2018

Mid 2019

Table of Content

Structure of the Strategy Paper discussed and agreed

Strategy Objectives

Identified: objectives, critical elements and frames actions to be taken

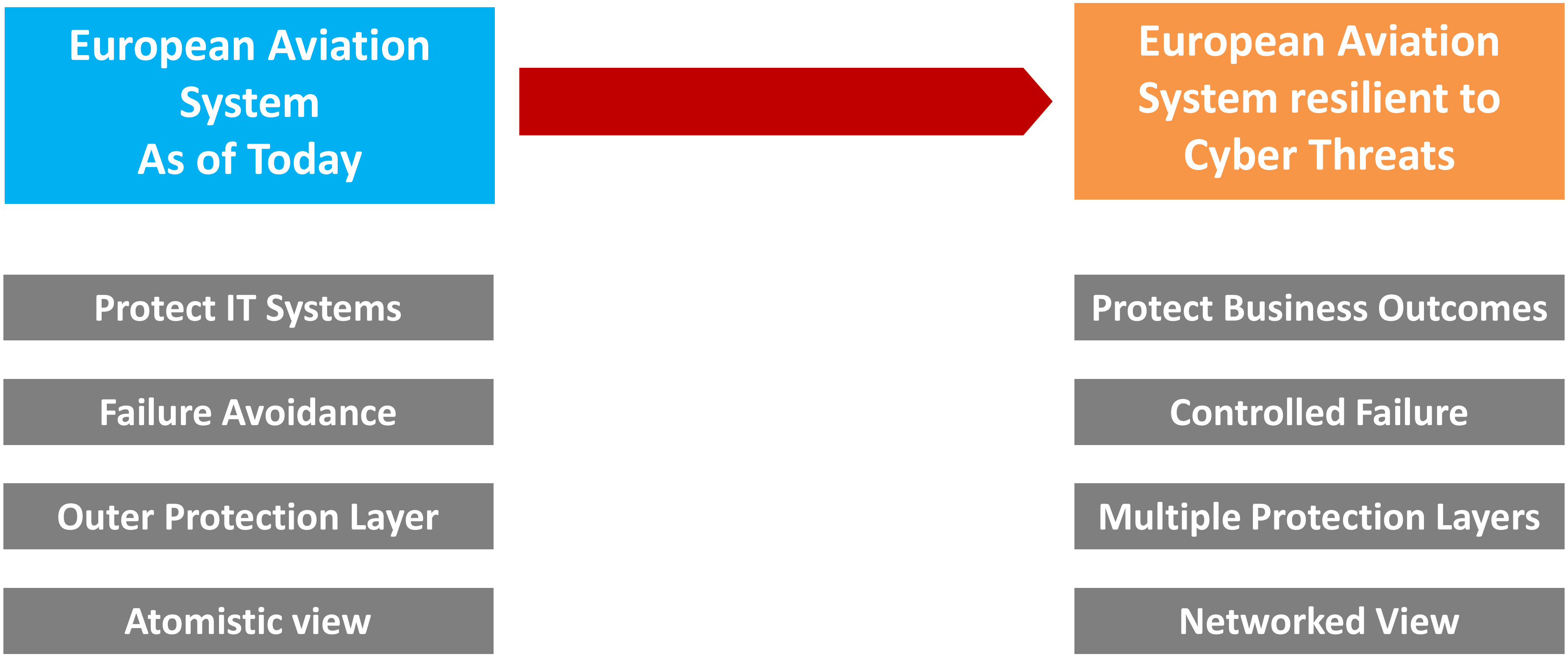
Draft Strategy

Draft proposals on course of coordinated actions and initiatives

Version 1.0

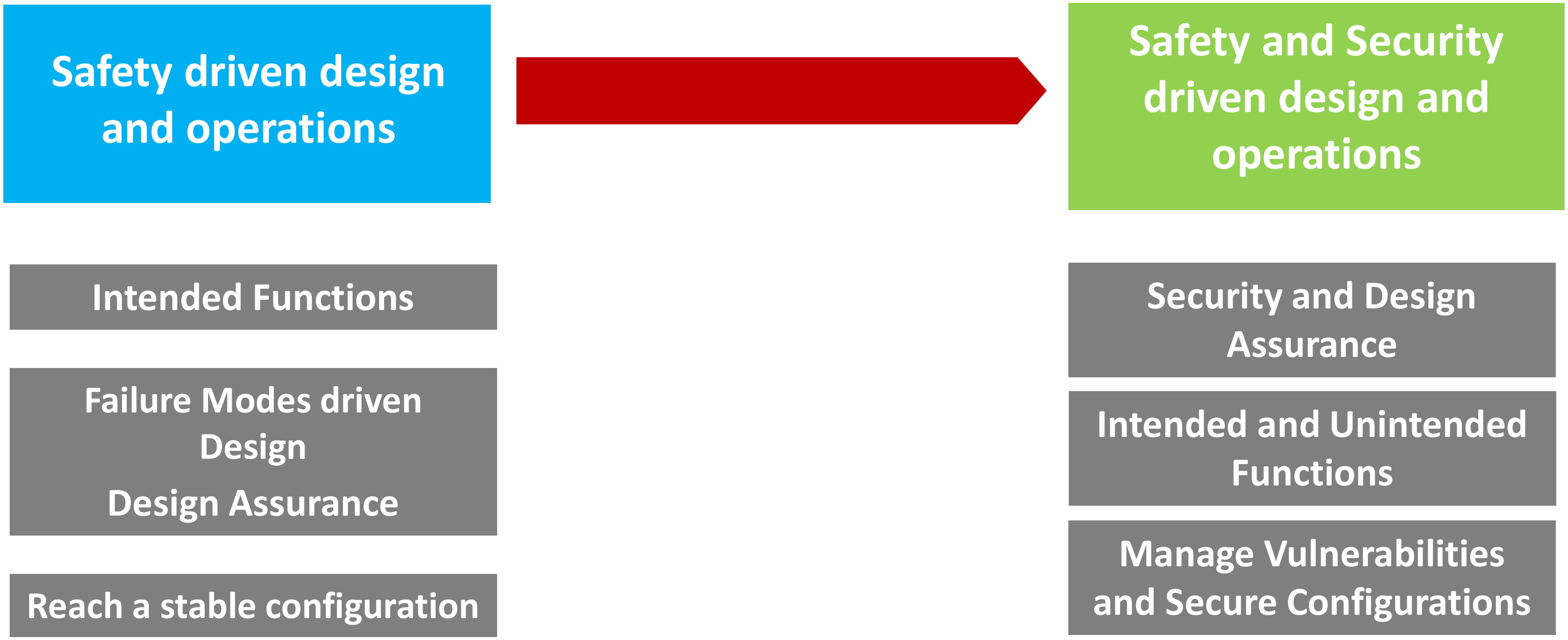
Agreement on objectives, coordinated actions and initiatives

Step 1 – Gap Analysis



European Aviation System As of Today	European Aviation System resilient to Cyber Threats
Protect IT Systems	Protect Business Outcomes
Failure Avoidance	Controlled Failure
Outer Protection Layer	Multiple Protection Layers
Atomistic view	Networked View

Step 1 – Gap Analysis



Safety driven design and operations

Safety and Security driven design and operations

Intended Functions

Failure Modes driven Design

Design Assurance

Reach a stable configuration

Security and Design Assurance

Intended and Unintended Functions

Manage Vulnerabilities and Secure Configurations

Step 2 – General Formulation

Where we want to be

The future aviation system will be a **trustworthy and dependable environment**, so that aviation stakeholders will be able to **rely on services and information provided by others** for the accomplishment of their operational objectives.

Step 2 – Formulation

Guiding Policy

We will focus resources and actions to introduce a **systemic approach to cybersecurity** in aviation of current and legacy systems to develop a **system-of-systems capable to adapt** and therefore, to **withstand new threats without significant disruptions**.

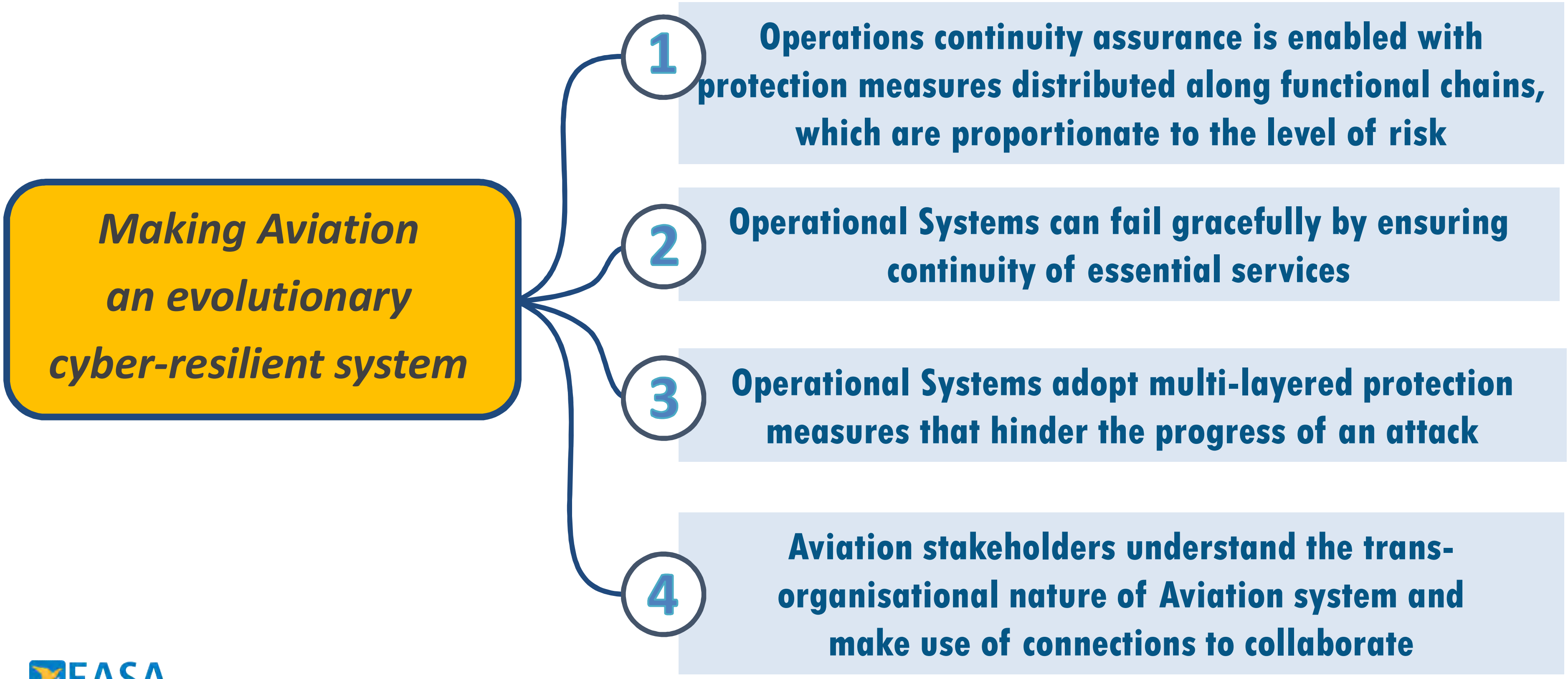
1st Direction

Making Aviation an evolutionary cyber-resilient system

2nd Direction

Making Aviation self-strengthening by adopting a "built-in security" approach

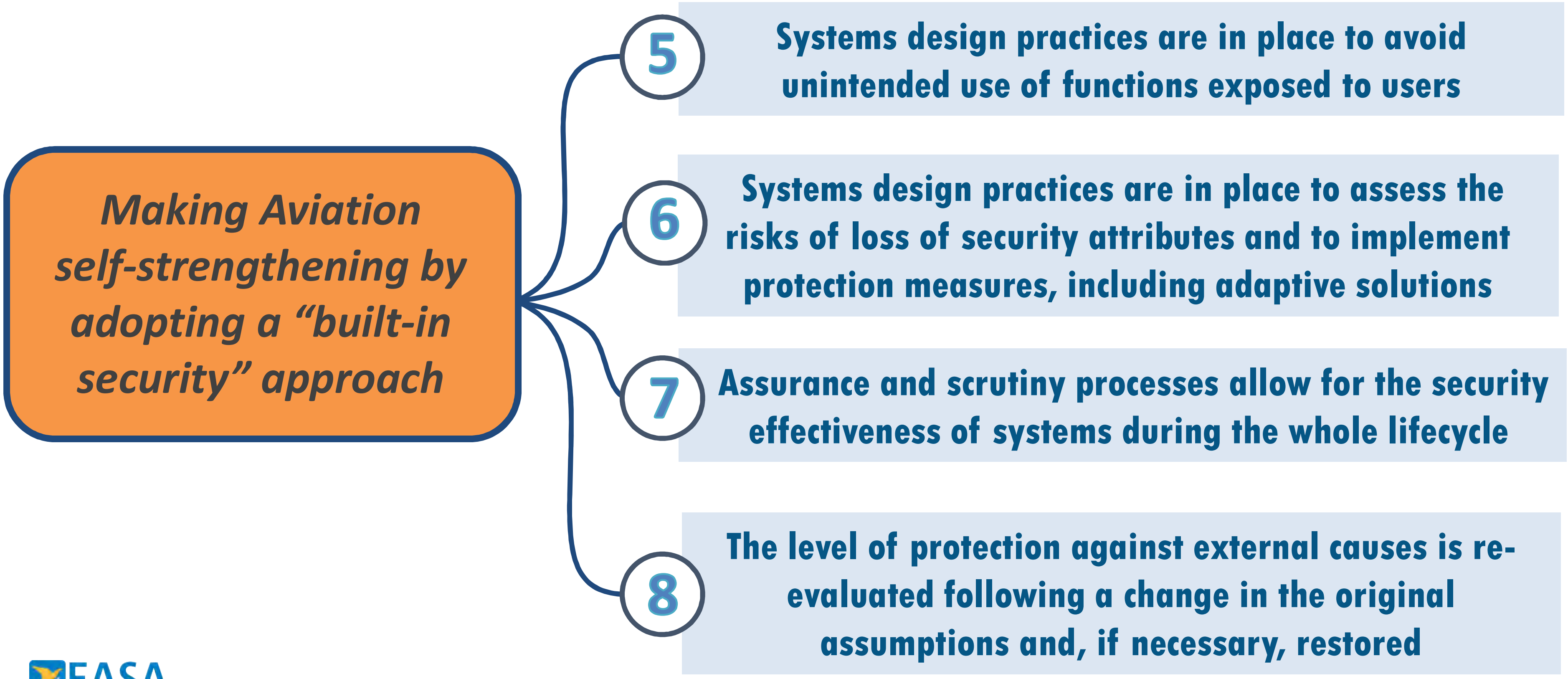
Step 3 – Detailed Formulation



Making Aviation an evolutionary cyber-resilient system

1. Operations continuity assurance is enabled with protection measures distributed along functional chains, which are proportionate to the level of risk
2. Operational Systems can fail gracefully by ensuring continuity of essential services
3. Operational Systems adopt multi-layered protection measures that hinder the progress of an attack
4. Aviation stakeholders understand the trans-organisational nature of Aviation system and make use of connections to collaborate

Step 3 – Detailed Formulation



Making Aviation self-strengthening by adopting a “built-in security” approach

5 Systems design practices are in place to avoid unintended use of functions exposed to users

6 Systems design practices are in place to assess the risks of loss of security attributes and to implement protection measures, including adaptive solutions

7 Assurance and scrutiny processes allow for the security effectiveness of systems during the whole lifecycle

8 The level of protection against external causes is re-evaluated following a change in the original assumptions and, if necessary, restored

ICAO Cybersecurity Strategy - Scope

- → to protect civil aviation and the travelling public from cybersecurity threats;
- → to maintain or improve the safety and security of the aviation system in preserving the continuity of air transport services;
- → to **coordinate cybersecurity measures among State authorities** to ensure effective and efficient management of cybersecurity risks.

ICAO Cybersecurity Strategy

→ Recognizes that **cybersecurity is a cross-cutting issue** that involves all domains of the aviation sector;

→ Provides States with a vision of the civil aviation sector as **resilient to cyber-attacks**, whilst **continuing to innovate and grow**.

Referenced documents

- ESCP Strategy

  https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20Strategy%20-%20First%20Issue%20-%2010%20September%202019.pdf

- ICAO Strategy / Resolution

  https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf

  https://www.icao.int/cybersecurity/Documents/A40-10.pdf

An Implementation Plan goes along

Captures actions and initiatives that need to be developed for a **strategy implementation**

EASA

European Union Aviation Safety Agency

Thank you for your attention!

Questions?

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union

Aviation Partnership Project Workshop on Cyber Security in Aviation

Workshop 2:

A Strategy for Cyber Security in Aviation

DR REBEKAH TANTI-DOUGALL

LEGAL CONSULTANT ON THE CYBER THREAT TO AVIATION

:

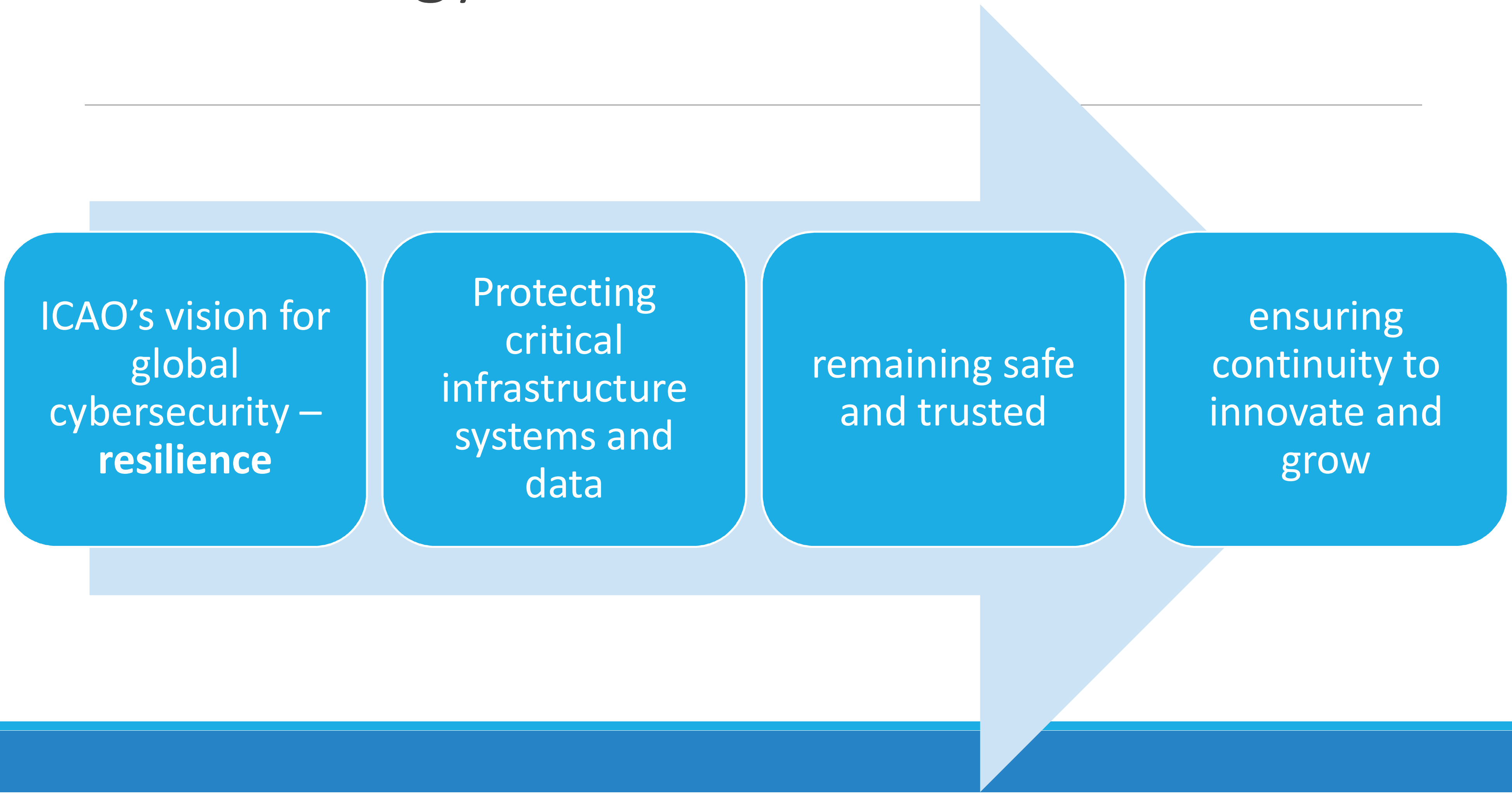
ICAO Secretariat Study Group on Cybersecurity [SSGC]

Member States, International Organisations and ICAO

4 Working Groups: Aerodromes and Airlines, Flight Safety, Air Navigation Systems as well as Legal

The strategy is the outcome of various discussions and meetings of the SSGC

The Strategy – what it seeks to achieve



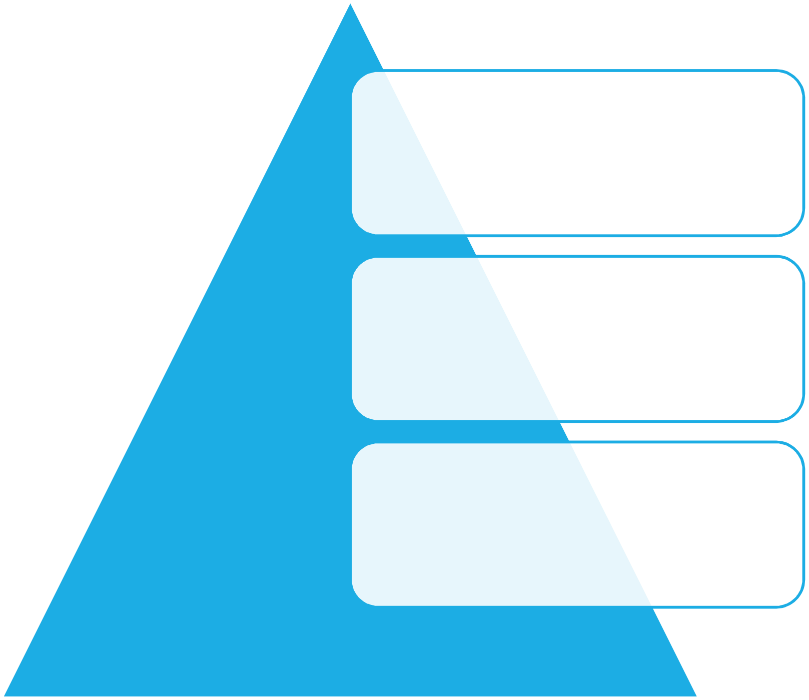
ICAO's vision for global cybersecurity – **resilience**

Protecting critical infrastructure systems and data

remaining safe and trusted

ensuring continuity to innovate and grow

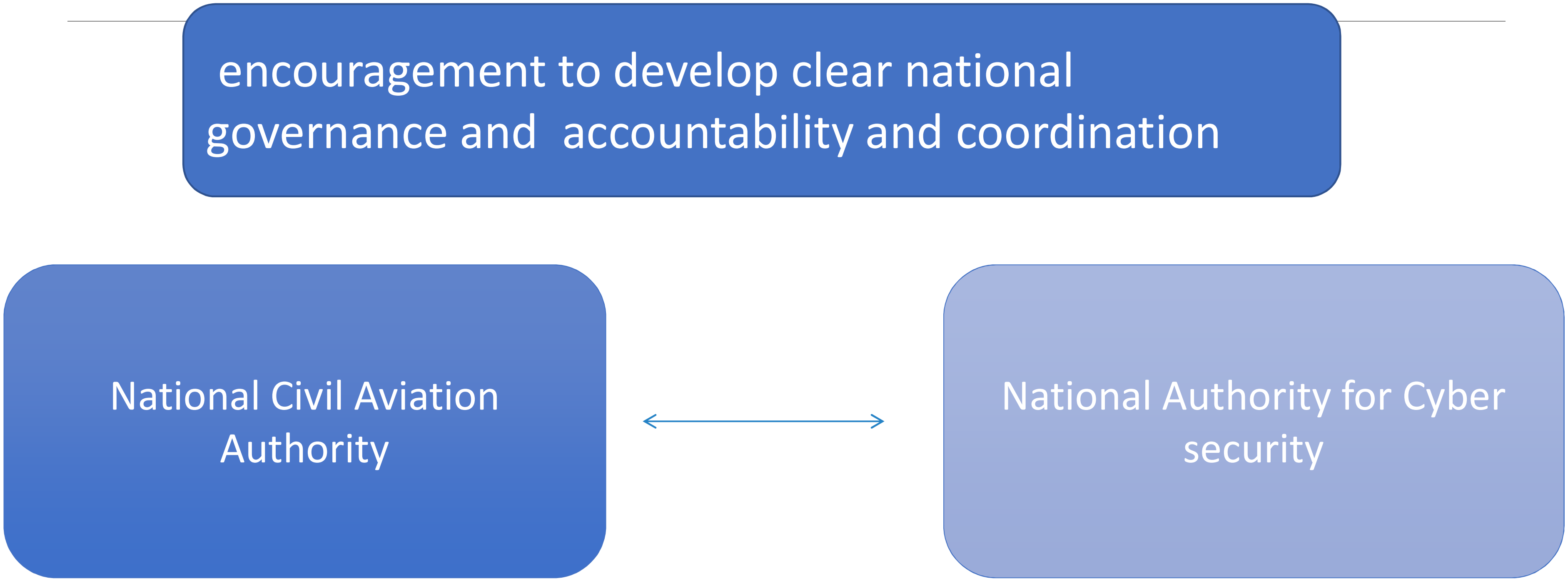
7 pillars in the strategy



International cooperation

- Both are borderless in nature.
- cooperation to ensure protection from cyber threats to safety and security.
- Harmonisation at national, regional and international

Governance



encouragement to develop clear national governance and accountability and coordination

National Civil Aviation Authority

National Authority for Cyber security

Cybersecurity policy

guidance material on the threats and risk assessments

Information sharing

- vulnerabilities,
- threats,
- events
- best practices

Through trusted relations

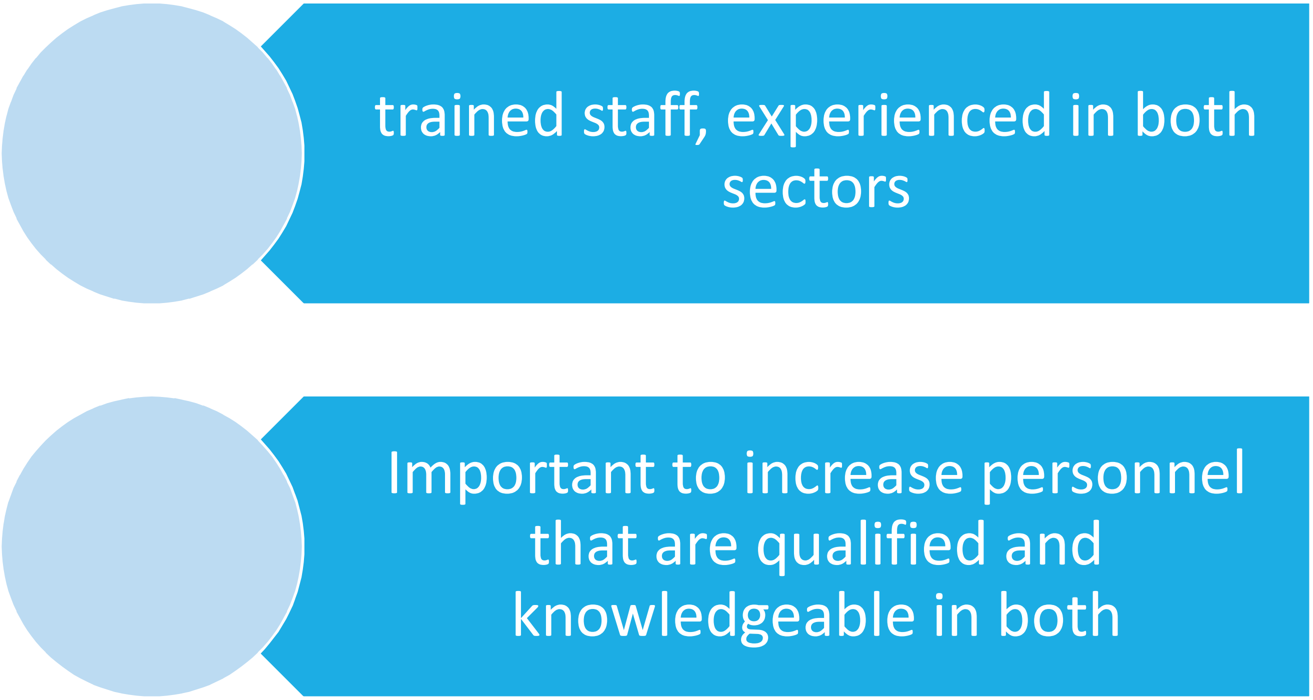
For early detection and to reduce impact of attacks

Incident management and emergency planning

Importance of having appropriate plans for the continuity during

and after cyber incidents.

Capacity Building, Training and cybersecurity Culture



trained staff, experienced in both sectors

Important to increase personnel that are qualified and knowledgeable in both

Legislation and Regulations

Legal Working Group

Legal Elements

International Law

Beijing

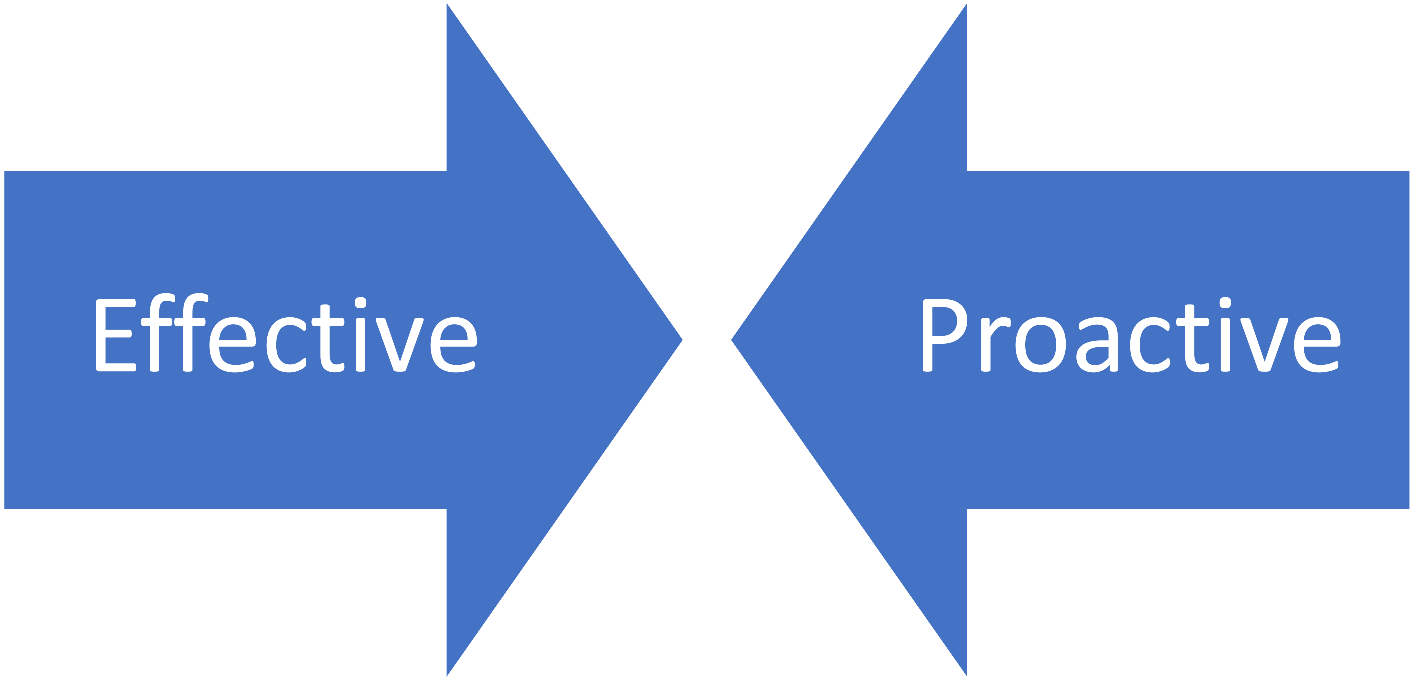
Lexicology

Appropriate National Law

Legal Aspects

- Cross Border
  - Where was the offence committed?
- Jurisdiction
- Legal basis for Prosecution [legal provision]
- Punishment
- Awareness of the Judiciary

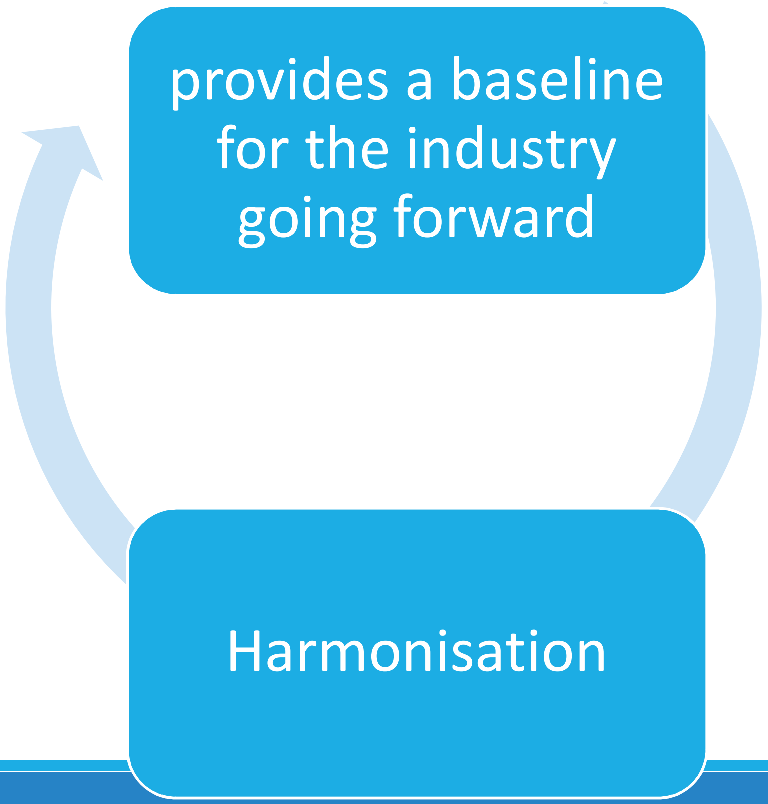
Legal Framework



Effective

Proactive

Conclusion - Strategy



provides a baseline for the industry going forward

Harmonisation

Thank you!

EASA

European Union Aviation Safety Agency

The Implementation Plan for the Cybersecurity Strategy

Davide Martini

Senior Expert - Cybersecurity in Aviation

5th – 7th February 2020

Colombo – Sri Lanka

Your safety is our mission.

An Agency of the European Union

Implementation Plan

Captures actions and initiatives that need to be developed for a **strategy implementation**

European Plan for Aviation Safety

Strategy for Cybersecurity in Aviation - Safety Prom. Task SPT.071

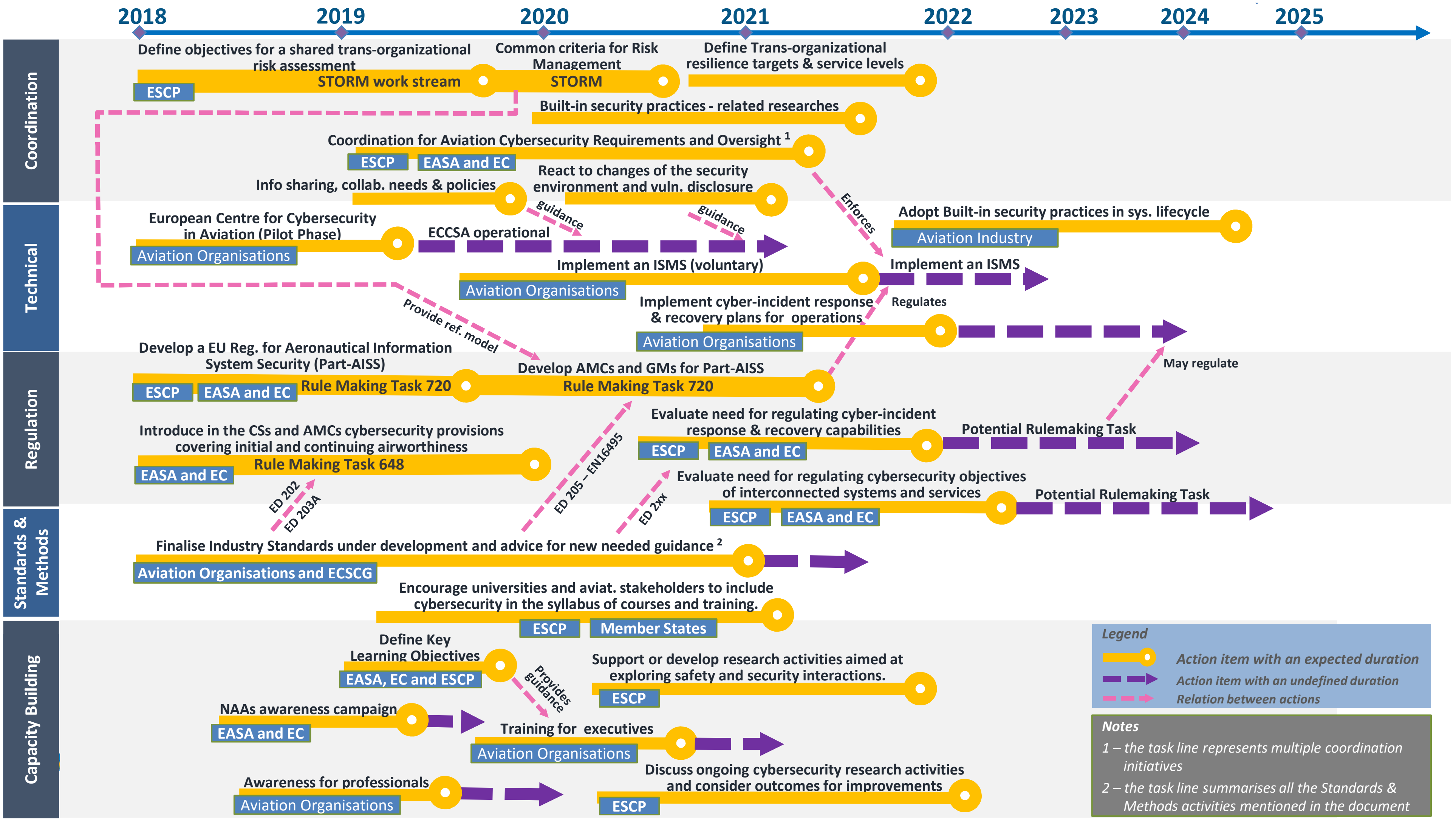
Objective

Define all the actions/activities required to reduce/mitigate the aviation cyber risks.

Elements of the implementation plan

The plan includes actions in the following areas:

Coordination	Capacity Building	Technical	Regulatory	Standards & Methods
7 actions	7 actions	4 actions	4 actions	2 actions



2018 2019 2020 2021 2022 2023 2024 2025

Coordination

Define objectives for a shared trans-organizational risk assessment – STORM work stream – ESCP

Common criteria for Risk Management – STORM

Define Trans-organizational resilience targets & service levels

Built-in security practices - related researches

Coordination for Aviation Cybersecurity Requirements and Oversight [1] – ESCP – EASA and EC

Info sharing, collab. needs & policies

React to changes of the security environment and vuln. disclosure

Technical

European Centre for Cybersecurity in Aviation (Pilot Phase) – Aviation Organisations

ECCSA operational

guidance

guidance

Enforces

Adopt Built-in security practices in sys. lifecycle – Aviation Industry

Implement an ISMS (voluntary) – Aviation Organisations

Implement an ISMS

Regulates

Implement cyber-incident response & recovery plans for operations – Aviation Organisations

Provide ref. model

May regulate

Regulation

Develop a EU Reg. for Aeronautical Information System Security (Part-AISS) – ESCP – EASA and EC – Rule Making Task 720

Develop AMCs and GMs for Part-AISS – Rule Making Task 720

Introduce in the CSs and AMCs cybersecurity provisions covering initial and continuing airworthiness – EASA and EC – Rule Making Task 648

Evaluate need for regulating cyber-incident response & recovery capabilities – ESCP – EASA and EC

Potential Rulemaking Task

Evaluate need for regulating cybersecurity objectives of interconnected systems and services – ESCP – EASA and EC

Potential Rulemaking Task

ED 202

ED 203A

ED 205 – EN16495

ED 2xx

Standards & Methods

Finalise Industry Standards under development and advice for new needed guidance [2] – Aviation Organisations and ECSCG

Capacity Building

Encourage universities and aviat. stakeholders to include cybersecurity in the syllabus of courses and training. – ESCP – Member States

Define Key Learning Objectives – EASA, EC and ESCP

Provides guidance

Support or develop research activities aimed at exploring safety and security interactions. – ESCP

NAAs awareness campaign – EASA and EC

Training for executives – Aviation Organisations

Awareness for professionals – Aviation Organisations

Discuss ongoing cybersecurity research activities and consider outcomes for improvements – ESCP

Legend

Action item with an expected duration

Action item with an undefined duration

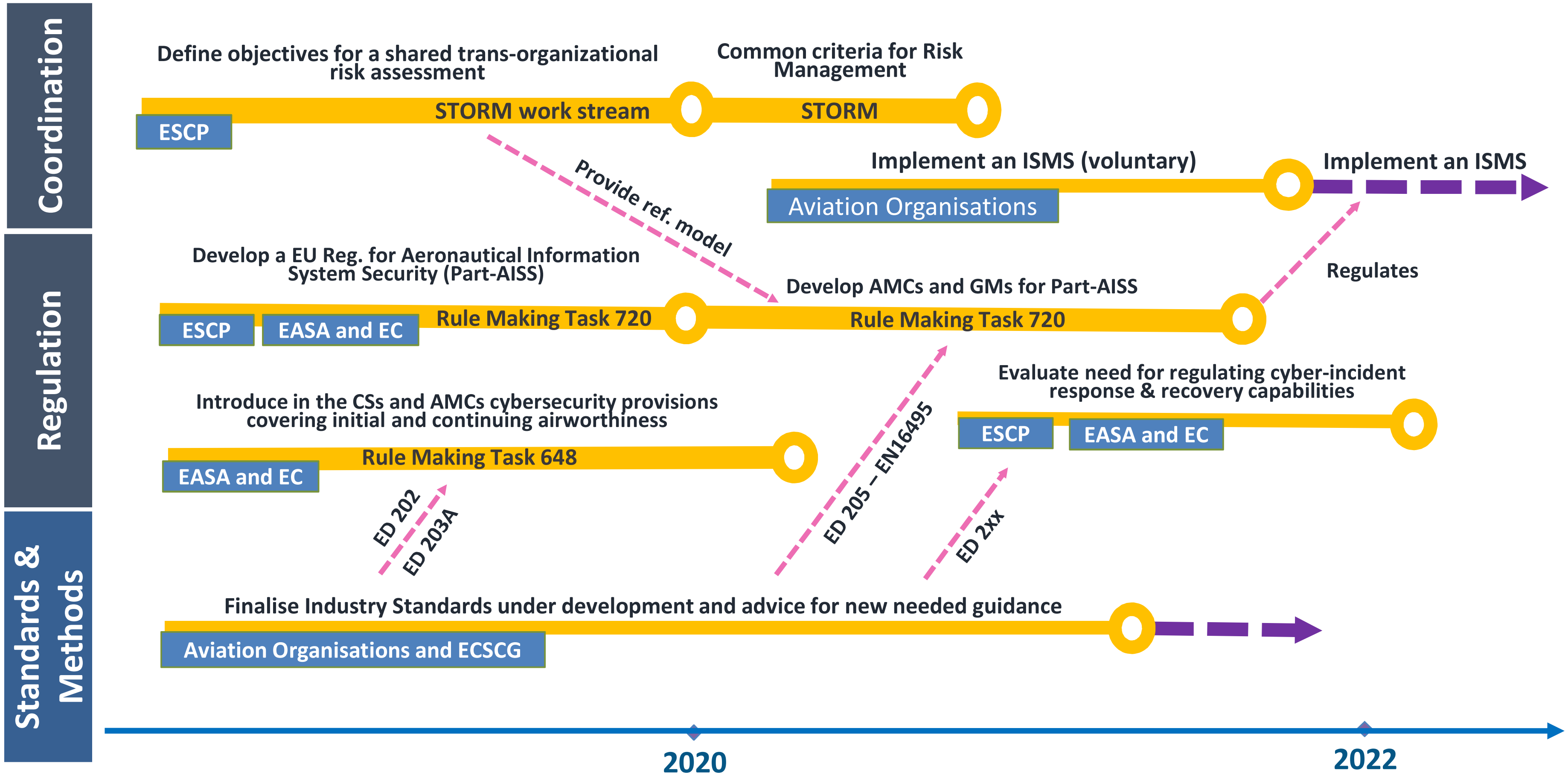
Relation between actions

Notes

1 – the task line represents multiple coordination initiatives

2 – the task line summarises all the Standards & Methods activities mentioned in the document

Detailed view at some cross-cutting activities



Coordination
Define objectives for a shared trans-organizational risk assessment
STORM work stream
ESCP
Common criteria for Risk Management
STORM
Provide ref. model
Implement an ISMS (voluntary)
Aviation Organisations
Implement an ISMS
Regulates
Regulation
Develop a EU Reg. for Aeronautical Information System Security (Part-AISS)
Rule Making Task 720
ESCP
EASA and EC
Develop AMCs and GMs for Part-AISS
Rule Making Task 720
Evaluate need for regulating cyber-incident response & recovery capabilities
ESCP
EASA and EC
Introduce in the CSs and AMCs cybersecurity provisions covering initial and continuing airworthiness
Rule Making Task 648
EASA and EC
ED 202
ED 203A
ED 205 – EN16495
ED 2xx
Standards & Methods
Finalise Industry Standards under development and advice for new needed guidance
Aviation Organisations and ECSCG
2020
2022

EASA
European Union Aviation Safety Agency

Thank you for your attention!

Questions?

easa.europa.eu/connect

f in 🐦 ◎ ▶ @

Your safety is our mission.

An Agency of the European Union

Aviation Partnership Project Workshop on Cyber Security in Aviation

Workshop 3: The implementation plan for the cybersecurity strategy

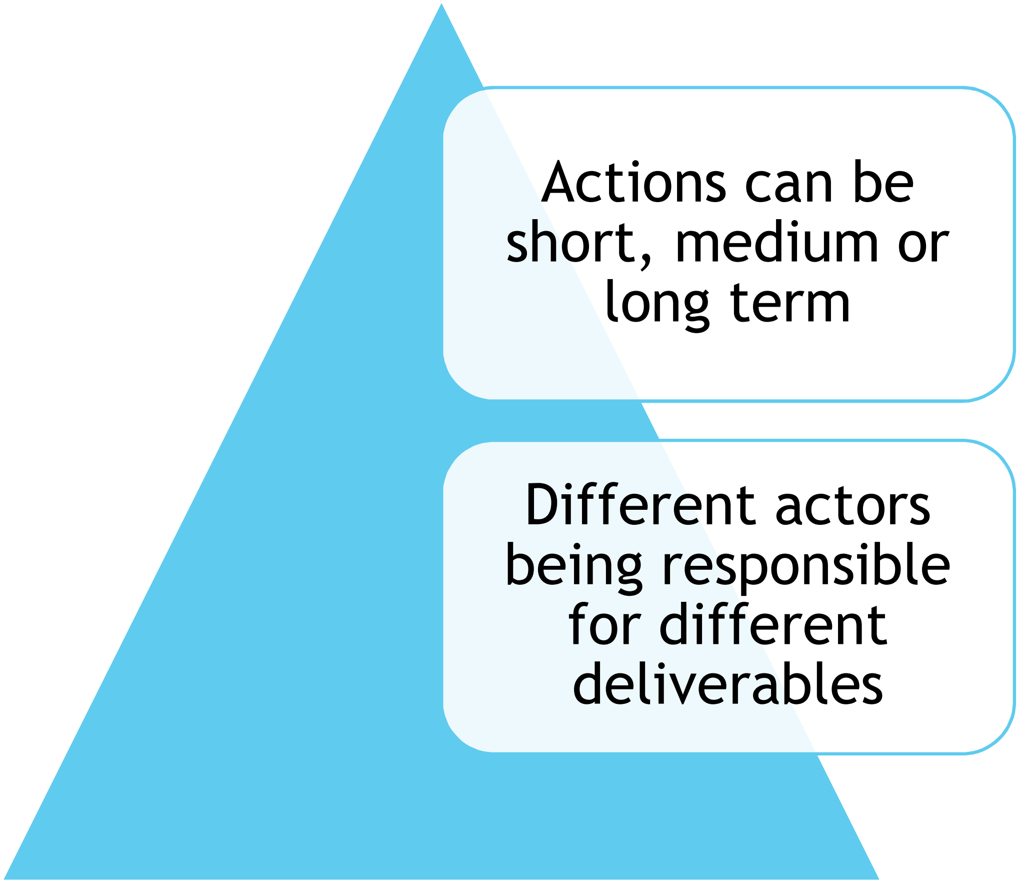
Dr Rebekah Tanti-Dougall
Legal Consultant on the Cyber Threat in Aviation

Cybersecurity Strategy Action Plan

Support for the adoption of the Strategy.

foundation for States, industry, and ICAO to work together

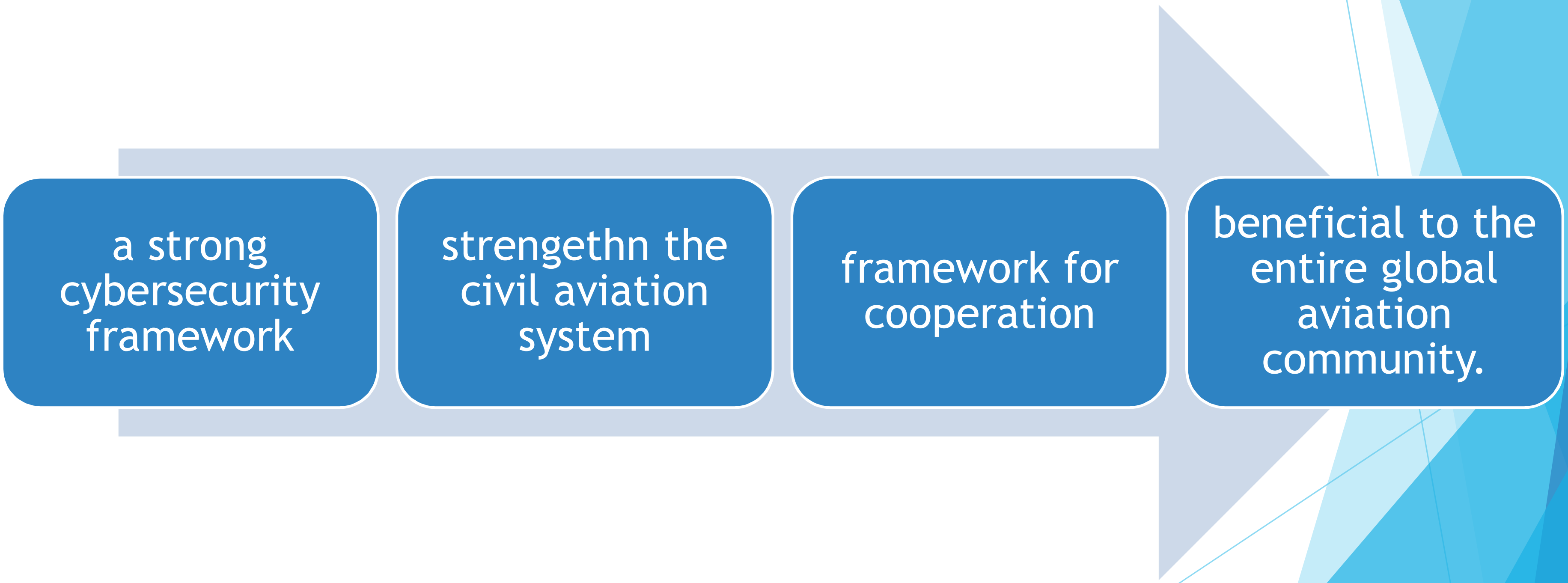
Based on principles and actions to achieve the objectives



Actions can be short, medium or long term

Different actors being responsible for different deliverables

Benefit of the action plan



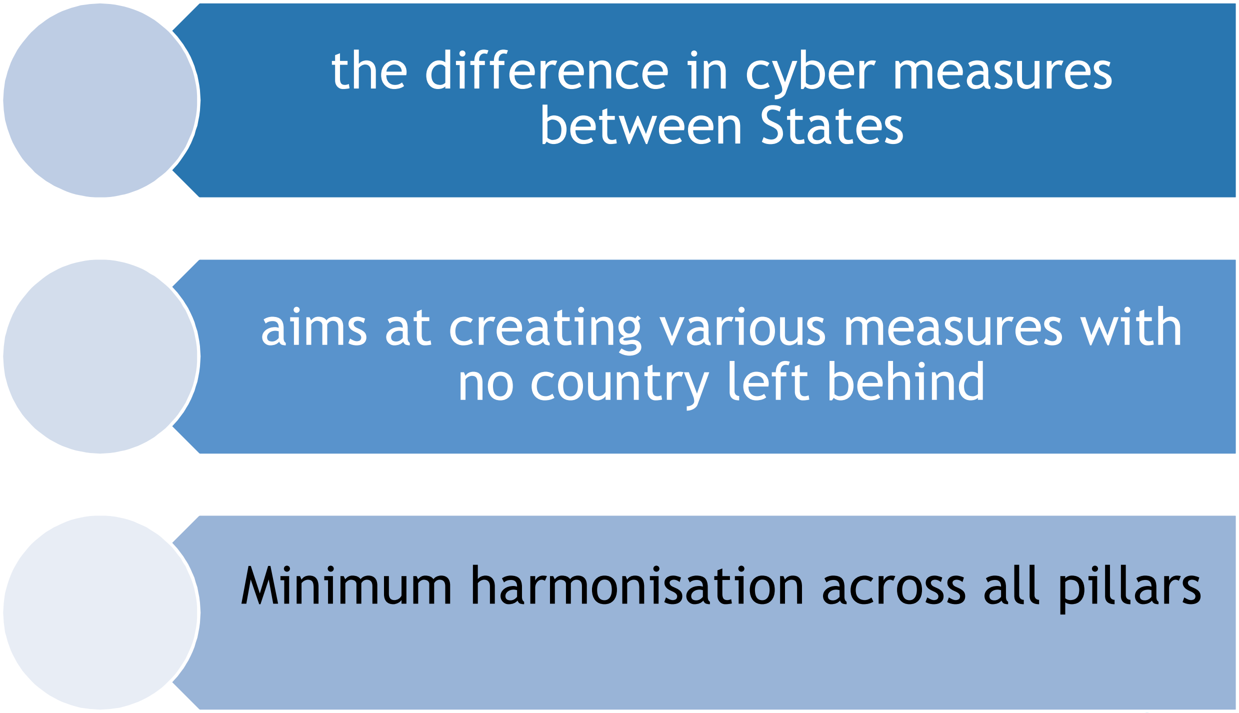
a strong cybersecurity framework

strengethn the civil aviation system

framework for cooperation

beneficial to the entire global aviation community.

The action plan takes into consideration



the difference in cyber measures between States

aims at creating various measures with no country left behind

Minimum harmonisation across all pillars

International cooperation

- Development of common terminology to allow all aviation stakeholders to understand each other.

ICAO

Short 2020

- Promotion of international and regional events for cybersecurity in civil aviation

ICAO

Long 2026

Governance and accountability

- States to put in place processes and identify specific cybersecurity in civil aviation responsibilities.

Member States

Short

- Ensure coordination between civil aviation authority and cyber security authority

Member States

Short

Cybersecurity policy

- Identify and evaluate cyber risks to civil aviation
- Develop some use cases for the highest cyber risks

ICAO States Industry

Short

- This will help the aviation community in identifying:

- Gaps in regulations
- raise awareness about those cyber risks
- new mitigation measures
- SARPS evolution

Incident management and emergency planning

Development of incident management and emergency planning

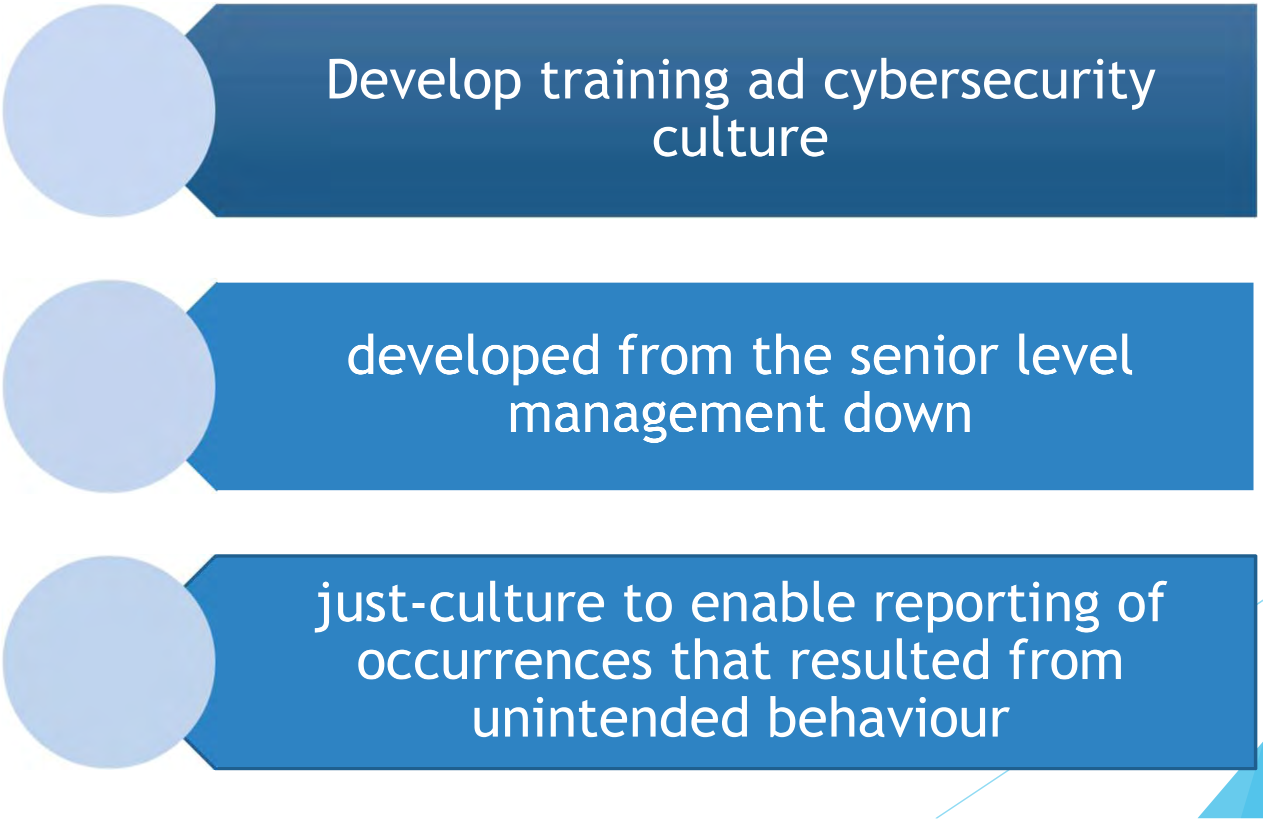
ICAO, States and industry

make use of existing contingency plans

- amend to include provisions for cyber security.

ICAO, States

Capacity building, training and cybersecurity culture and education



Develop training ad cybersecurity culture

developed from the senior level management down

just-culture to enable reporting of occurrences that resulted from unintended behaviour

Effective legislation and regulation

Review of existing ICAO Material [SARPs]	ICAO
Evaluation of national legal framework	States
review existing international instruments	ICAO
Ratification of Beijing instruments	States

Conclusion on Action Plan

It will bring together states, industry and other stakeholders

in a holistic and coordinated effort

to address cyber security challenges.

Through concrete actions

Thank you

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)

- **<u>They are not focused on the impact on aviation safety</u>**
  - **NIS Directive:** focus on preventing disruption of essential services (social and economic impact).
  - **Reg. 2015/1998:** focus on aviation security.
- **<u>They do not cover all aviation domains and stakeholders</u>**
  - **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

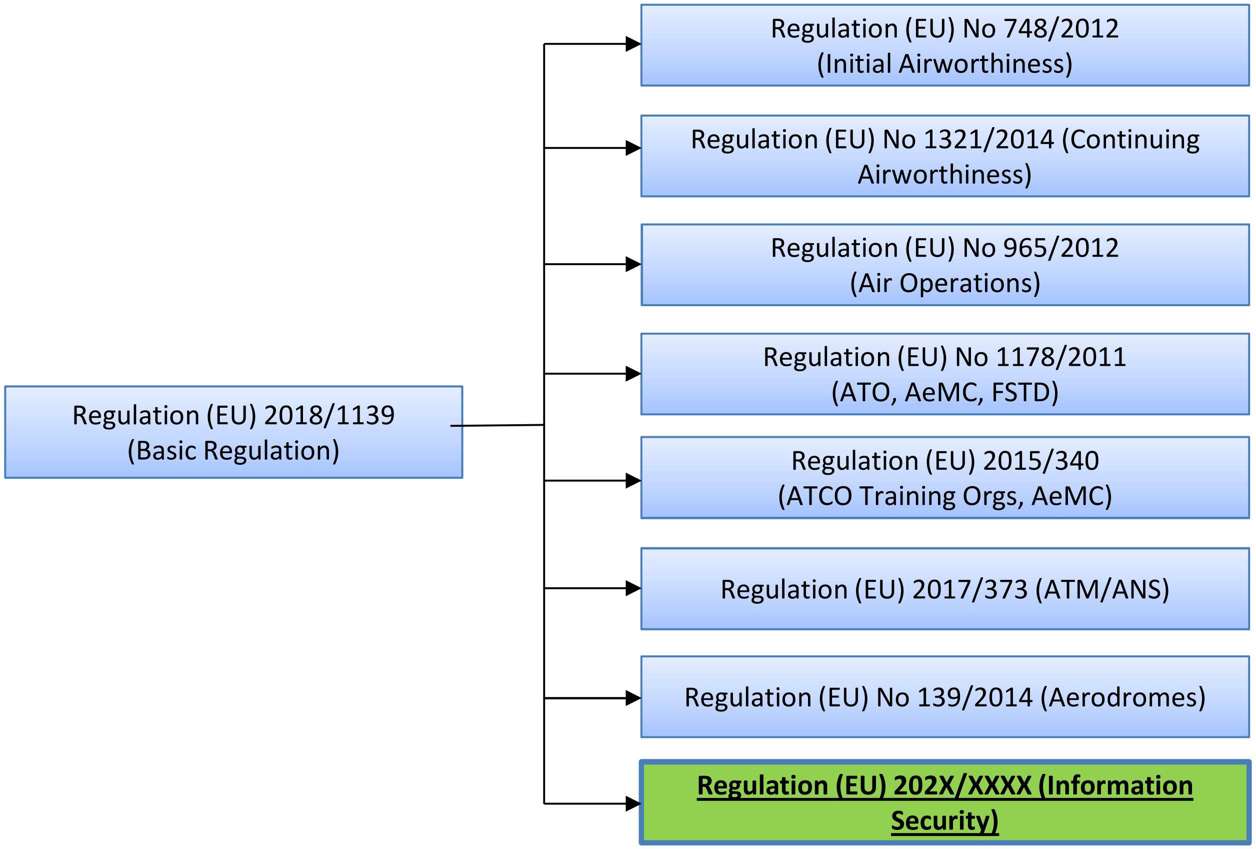
- Competent authorities.

- 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

Singapore Aviation Cybersecurity Framework and Structure

Regional Workshop on Cybersecurity In Aviation
5-7 Feb 2020

CAAS
Civil Aviation Authority of Singapore

Objective

To share about Singapore’s Aviation Cybersecurity Framework and Structure

Agenda

- Background
- Legislation, Policy and Compliance
- Education and Awareness

Background

Civil Aviation Authority of Singapore

CAAS Cybersecurity Branch

Cybersecurity Development Section

- Partner CAAS divisions and aviation sector to strengthen cybersecurity posture
- Drive cybersecurity projects to achieve security outcomes
- Conduct Education and awareness activities
- Enhance cybersecurity resiliency and readiness

Cybersecurity Regulation & Operations Section

- Develop cybersecurity strategies for the aviation sector
- Regulate aviation sector on cybersecurity
- Monitor sectoral cybersecurity readiness and Formulate Incident Response Plan
- Support incident management and SOC operations

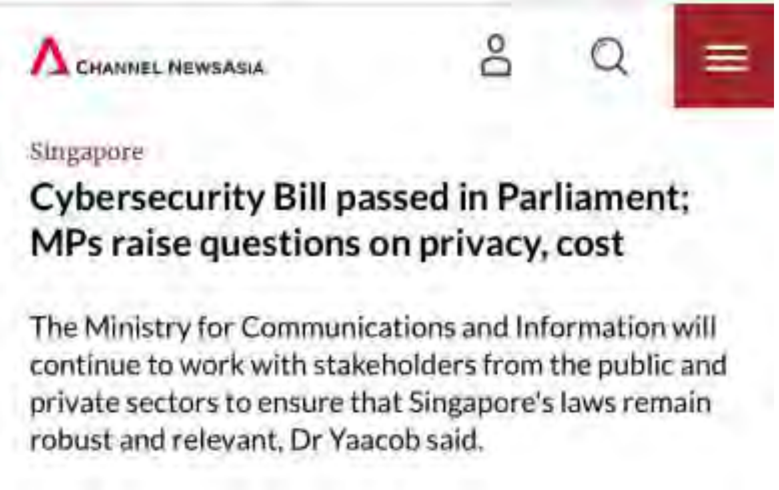
Legislation, Policy and Compliance

CAAS
Civil Aviation Authority of Singapore

Singapore’s Cybersecurity Act

- Cybersecurity Act was passed in parliament on 5 Feb 2018, came into force in 2nd half of 2018
- Law provides for the oversight & maintenance of cybersecurity
- Proactive approach for the protection of Critical Information Infrastructure (CII) to ensure continuous delivery of essential services
- Common framework for governing cybersecurity across all sectors
- Effective powers for incident response and investigation
- Powers vested in the Commissioner for Cybersecurity (CE of Cyber Security Agency – CSA)

New Bill proposed to beef up cyber security
It will take precedence over bank, privacy



Singapore

Cybersecurity Bill passed in Parliament; MPs raise questions on privacy, cost

The Ministry for Communications and Information will continue to work with stakeholders from the public and private sectors to ensure that Singapore's laws remain robust and relevant, Dr Yaacob said.

Cybersecurity Act 2018 – Key Features

1. Protection of Critical Information Infrastructure

- Essential services
- Designation of CIIs and their owners (CIIOs)
- Responsibilities of CIIOs in protecting their CIIs

2. Investigation of cybersecurity threats and incidents

- Powers to respond to cybersecurity threats and incidents

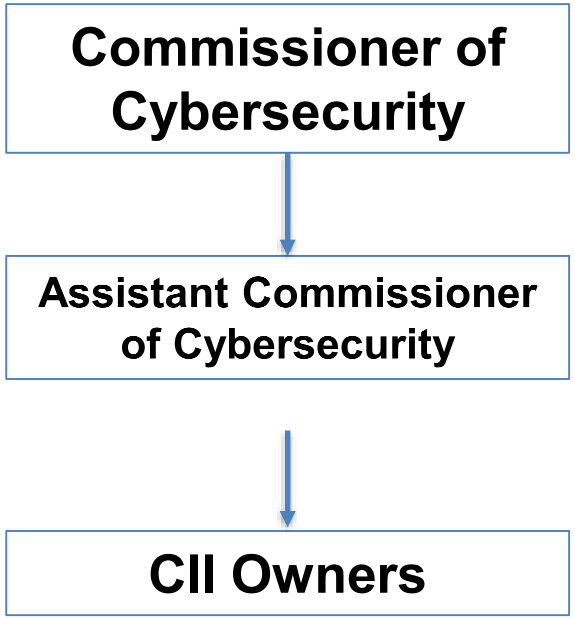
3. Information sharing

- Facilitate sharing of cybersecurity information with and by the Cyber Security Agency (CSA)

4. Licensing of cybersecurity service providers

- Penetration testing and managed security operations centre (SOC) services

CAAS is delegated regulatory powers to ensure compliance by CII owners under the Cybersecurity Act



Commissioner of Cybersecurity

Assistant Commissioner of Cybersecurity

CII Owners

The Cybersecurity Act sets out Essential Services in the aviation sector which cover the following areas:

- Air navigation services
- Airport passenger control and operations
- Airport baggage and cargo handling operations
- Aerodrome operations
- Flight operations of aircraft

Areas of compliance include risk management and information sharing such as audits, risk assessment and incident reporting

Security Directive on Cybersecurity

- Applicable to Singapore Air Operators with effect from 31 May 2019

- Air operators are to implement a Singapore Operator Cybersecurity Programme

- Extensive consultation carried out with air operators to take into account feasibility and implementation concerns

- Intended outcome
  - Strengthen cybersecurity and data security measures of important systems for aviation operations
  - Availability of systems as well as the confidentiality and integrity of data including customer information

Aviation Cybersecurity Committee (ACC) - Governance

- As cybersecurity issues can have implications across the aviation sector, it is essential to establish close coordination among key aviation stakeholders

- CAAS established a high-level forum to enhance cybersecurity collaboration, and development of strategies in the aviation sector
  - Comprises CE-level representatives from key aviation entities
  - ACC meeting is scheduled quarterly

Education and Awareness

CAAS

Civil Aviation Authority of Singapore

CAAS formed the Aviation Cybersecurity Community (ACSC) for engagement and information sharing

- Aviation Cybersecurity Community (ACSC) was established by CAAS in 2014:
  - Foster closer working relationships and develop greater synergy in cybersecurity efforts within the Aviation Sector
  - Facilitates information sharing
- CAAS organises cybersecurity seminars and workshops for the ACSC to create awareness and build capability, and enhance cyber resiliency

Aviation Cyber Security Community Workshop in 2019

- Training attended by about 100 participants from aviation community

- Focus on triage Standard Operating Procedure for first responders to assess whether an incident is cybersecurity related

- Establishes common understanding on incident notification and response protocols etc.

KPMG

Incident First Responder Training

June 2019

Thank you

Civil Aviation Authority of Singapore

EASA
European Union Aviation Safety Agency

Workshop 5: “Information Security Management System and coordination with other Regulatory Frameworks”

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:
      - 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.**

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 1: 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 2: 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 3: 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 initially selected in NPA 2019-07.</u>**

Option initially selected in NPA 2019-07

- **Option initially 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 initially selected in NPA 2019-07

- **Drawback:**
  - **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.

  - **Risk that in certain countries, the NIS Directive may have been implemented in a very relaxed manner.** The essential services would be complying with those relaxed requirements while the non-essential services would have to comply with the more strict requirements of the future EASA rules.

Option finally selected (after comments received to NPA 2019-07)

- **Option 2: 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.

  - **Mitigating measures:**
    - 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 the essential services to continue doing what they were doing (if considered robust enough).</u>
      - <u>This will also allow to use that material across all the EU Member States and for all stakeholders (not only for essential services)</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 has been recently 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.”*
- **Contains a provision that allows the replacement of those requirements by other equivalent EU requirements (the future EASA rules).**

Conclusions

Conclusions

- **The future EASA cybersecurity rule should serve as the standard for the management of cybersecurity risks and reporting of incidents for the full aviation domain.**

- **The requirements contained in the NIS Directive and the Aviation Security Regulation 2015/1998 would become superseded by the future EASA rules** (unless there are specific issues related to continuation of services and security which have not been properly addressed by the safety perspective of the future EASA rules)

- **The audits on the organisations should be performed in a consistent manner involving the different authorities of the country, without duplicating audits.**

- **The organisational structures in the Member States will need to be adapted to this new framework.**

EASA
European Union Aviation Safety Agency

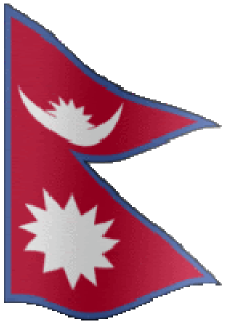
Questions

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union

Global Cyber Security and ICAO Strategy for Aviation Cyber Security



PRESENTED BY:
SANJEEV SINGH KATHAYAT
PRAMOD CHAUDHARY
PRADIN TAMRAKAR
NEPAL

Global Cybersecurity Threats

The major cyber security issues faced in Nepal are:

- Identity theft
- Spam email marketing
- Cyber bullying
- Child online protection
- Copyright issues
- Hacking
- Banking Fraud
- Phishing

Identity Theft

Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the U.S. Bureau of Justice Statistics (BJS), more than 1.1 million Americans are victimized by identity theft.

Hacking

Hacking involves the partial or complete acquisition of certain functions within a system, network, or website. It also aims to access to important data and information, breaching privacy. Most “hackers” attack corporate and government accounts. There are different types of hacking methods and procedures.

Scamming

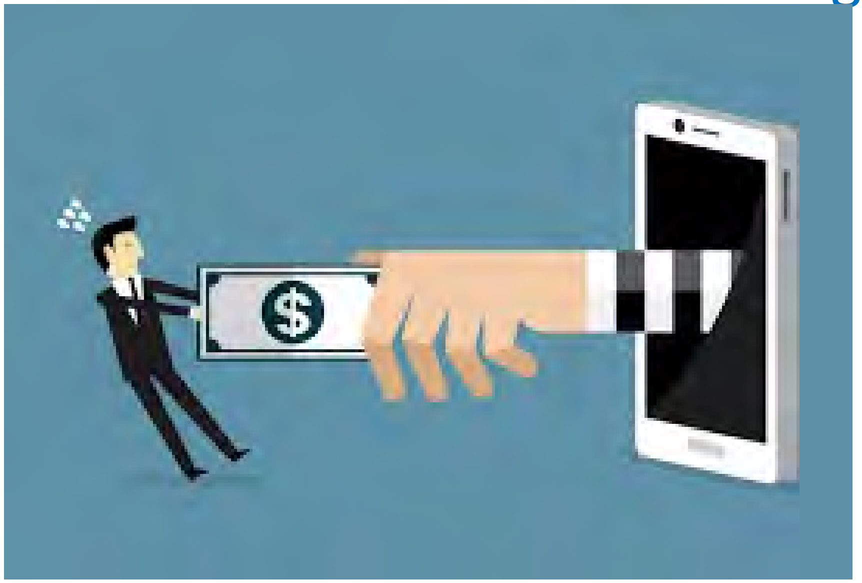
Scam happens in a variety of forms. In cyberspace, scamming can be done by offering computer repair, network troubleshooting, and IT support services, forcing users to shell out hundreds of money for cyber problems that do not even exist. Any illegal plans to make money falls to scamming.

Phishing

Phishers act like a legitimate company or organization. They use "email spoofing" to extract confidential information such as credit card numbers, social security number, passwords, etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

Fraud

Fraud is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure unlawful or unfair gain.

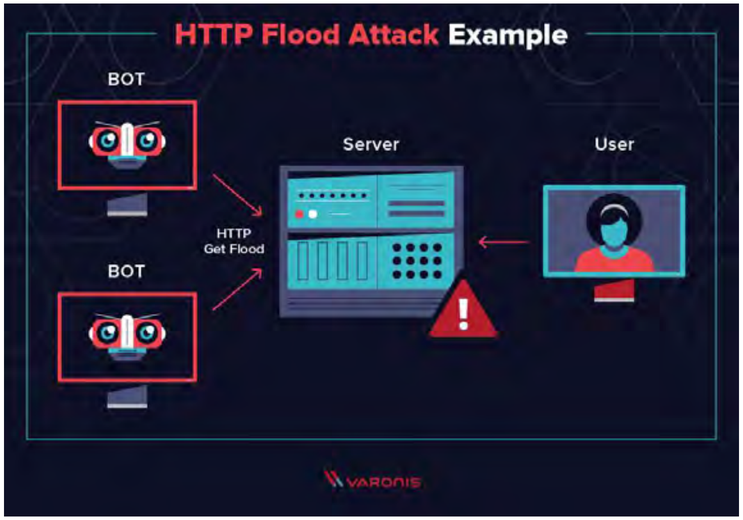


Ransomware

Ransomware is one of the most destructive malware-based attacks. It enters your computer network and encrypts files and information through public-key encryption. In 2016, over 638 million computer networks are affected by ransomware. In 2017, over $5 billion is lost due to global ransomware.

DDoS Attack

DDoS or the Distributed Denial of Service attack is one of the most popular methods of hacking. It temporarily or completely interrupts servers and networks that are successfully running. When the system is offline, they compromise certain functions to make the website unavailable for users. The main goal is for users to pay attention to the DDoS attack, giving hackers the chance to hack the system.

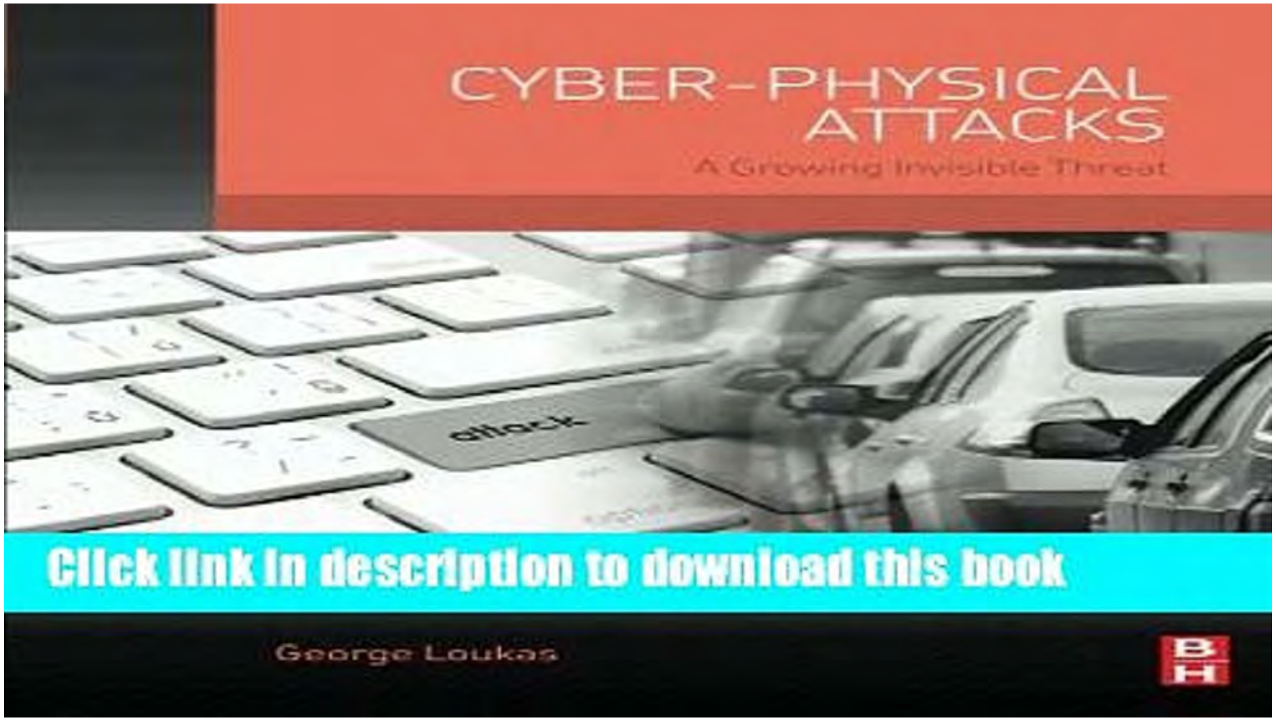


Cyberbullying

Cyberbullying is one of the most rampant crimes committed in the virtual world. It is a form of bullying carried over to the internet. On the other hand, global leaders are aware of this crime and pass laws and acts that prohibit the proliferation of cyberbullying.

Cyber-Physical Attacks

The ongoing threat of hacks targeting electrical grids, transportation systems like road, train and aviation , water treatment facilities, etc., represent a major vulnerability going forward.


CYBER-PHYSICAL
ATTACKS
A Growing Invisible Threat
attack
Click link in description to download this book
George Loukas
B
H

State-Sponsored Attacks

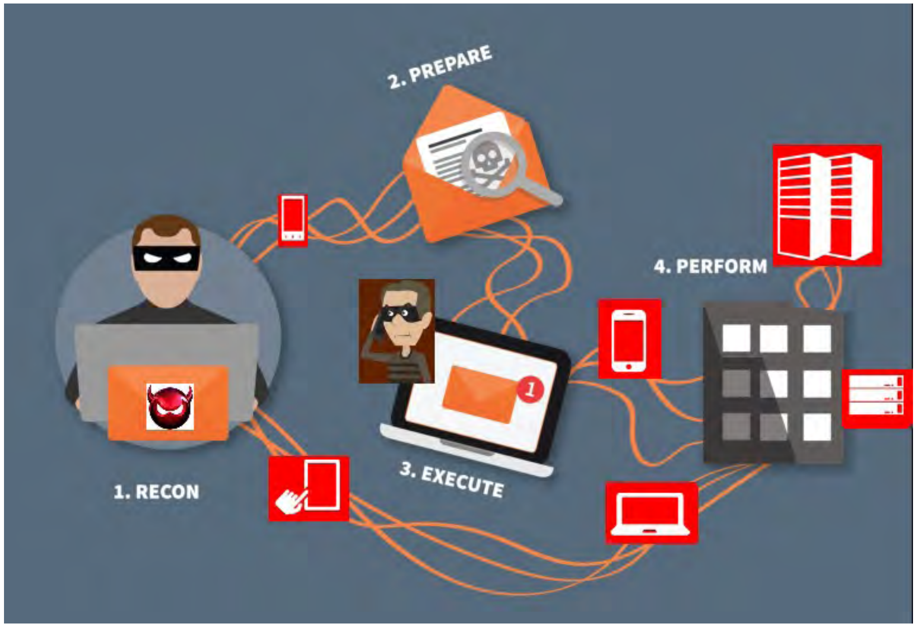
Beyond hackers looking to make a profit through stealing individual and corporate data, entire nation states are now using their cyber skills to infiltrate other governments and perform attacks on critical infrastructure

Computer Viruses

Most criminals take advantage of viruses to gain unauthorized access to systems and steal important data. Mostly, highly-skilled programs send viruses, malware, and Trojan, among others to infect and destroy computers, networks, and systems. Viruses can spread through removable devices and the internet.

Social Engineering

Social engineering is a method in which cybercriminals make a direct contact with you through phone calls, emails, or even in person. Basically, they will also act like a legitimate company as well. They will befriend you to earn your trust until you will provide your important information and personal data.



Software Piracy

The internet is filled with torrents and other programs that illegally duplicate original content, including songs, books, movies, albums, and software. This is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally reproduced.

The Major Cyber Security Issues in Nepal and Effort of Government of Nepal for Cyber Security

The popularity and availability of the internet are increasing day by day. By the end of 2016, about 48% of the world's population was using the internet. Today billions of people are connected to the internet via many devices to share information and make the world a small place. This global surge of the rise of the Internet hasn't left Nepal untouched.

In terms of the total number of internet users, Nepal ranks 73 in the world with about 5 million internet users. Currently, about 18% of the population of Nepal is using the internet but with the advancement in technology, the number of users growing by 12 to 15% each year.

With this huge increasing number of people sharing and transferring an enormous amount of data on the internet, a danger arises which does and should alarm every internet user. "Cybercrimes" are offenses that are committed against individuals or institutions to cause physical, mental or financial harm using telecommunication networks such as the internet. The number of cyber-

Reported Cyber Crime Cases

SN	Report Received	Jul 2016 to Jul 2017	Jul 2017 to Jul 2018	Jul 2018 to Jul 2019	Total
1	Central Investigation Bureau	96	131	135	362
2	Crime Division	1197	1482	1938	4617
3	Metro Police Range Kathmandu	25	81	136	242
	Total	1318	1694	2209	5221

Current Year Statistics Reported, only in Cyber Bureau (Jul 2019 to Dec 14, 2020)

Cases	Number
Facebook / Messenger	940
Viber	4
Whats App	0
IMO	2
YouTube	3
Twitter	2
Instagram	6
Web Site Hacking	0
Other	15
Total	972

Effort of Government of Nepal for Cyber Security

As modernization and development is deriving world to digitation, evolving in technology also fetching challenges in society. Numbers of cyber crime incident were reported as hacking, phishing, cyber bullying, cyber stalking, ATM hacking, ransomware, spam email, fraud, Social Engineering etc. To address the challenge Government of Nepal stepped toward Cyber Security as follows.

- **Law, Policy and Regulation Level**
- **Research & Coordination Level**
- **Law Enforcement & Awareness Level**

Law, Policy and Regulation Level

- Government of Nepal passed the bill of "Electronic Transaction Act - 2008".

- NTA (Nepal Telecommunication Authority) drafted Cyber Crime Policy & in pipeline process for Declaration.

- MCIT (Ministry for Communication & Information Technology) formed ITERT (Information Technology Emergency Response Team) headed by Director General of MCIT in 30 April 2019 to strengthen & reinforce the cyber policies.

Research & Coordination Level

Also formed CSMC (Cyber Security Monitoring Center) headed by Director of MCIT in 30 April 2019 which includes "Nepal Police, Cyber Bureau" as well, to analyze & investigate cyber threats in Nepal and to coordinate with MCIT & Nepal Police Cyber Bureau.

Law Enforcement & Awareness Level

1. Formed Cyber Bureau under Nepal Police headed by DIGP (Deputy Inspector General of Police) in 2019.
2. Formed Cyber Crime Unit under Metropolitan Police Crime Division, Nepal Police.
3. Formed Cyber Crime Unit Under Central Cyber Bureau (CIB), Nepal Police.
4. Lunching "Community Police Partnership Program" to aware Communities and Students (Class 1 to 12) about Cyber Security, Traffic, Human Trafficking, and Drugs awareness.
5. Establishment of Digital Forensic Investigation Units in various level.

Role of ICAO for Cyber Security for Civil Aviation

- Acknowledging the urgency and importance of protecting civil aviation's critical infrastructure, information and communication technology systems and data against cyber threats, ICAO is committed to developing a solid cyber security framework. The 40th Session of the ICAO Assembly adopted Assembly Resolution A40-10 – *Addressing Cyber security in Civil Aviation*.

- The resolution addresses cyber security through a horizontal, cross-cutting and functional approach, reaffirming the importance and urgency of protecting civil aviation's critical infrastructure systems and data against cyber threats and calls upon States to implement the ICAO Cyber security Strategy.

Strategy of ICAO

ICAO’s vision for global cyber security is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow. This can be achieved through:

- Member States recognizing their obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cyber security;
- Coordination of aviation cyber security among State authorities to ensure effective and efficient global management of cyber security risks, and
- All civil aviation stakeholders committing to further develop cyber resilience, protecting against cyber-attacks that might impact the safety, security and continuity of the air transport system.

The 56th Conference of Directors General of Civil Aviation of Asia and Pacific Regions

- The 56th Conference of Directors General of Civil Aviation of Asia and Pacific Regions was recently held in Kathmandu, Nepal from 19 to 23 August 2019. On this conference, IATA has presented the discussion Paper regarding the Aviation Cyber Security.

- It was mentioned that Global Aviation being one of the most complex and integrated systems of information and communications technology in the world it is a potential target for a large-scale cyber-attack and cyber threats to the civil aviation sector are real and their likelihood is increasing. Due to the increased digitization and connectivity as well as interdependent and global nature of the aviation sector, cyber security incidents could rapidly scale up and have impact internationally.

EASA
European Union Aviation Safety Agency

Workshop 7: “Risk Assessment and Management Principles and Identification of Functional Chains”

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

Key elements of the ISMS

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.

Shared Trans-Organisational Risk Management (STORM):

Identification of interfaces with other organisations and standardisation of risk assessments

Shared Trans-Organisational Risk Assessments

- An essential part of the discussions within the ESCP.

- Two Sub-Groups:
  - Sub-Group 1: Standardisation of Risk Assessments
  - Sub-Group 2: Identification of interfaces and functional chains

- The outcome will be used in order to develop:
  - Acceptable Means of Compliance (AMC) and Guidance Material (GM) to complement the future ISMS rules.
  - Industry Standards which will be referred to in the AMC/GM.

EUROCAE Standards

Organisation level

- ED-201 - **Aeronautical Information System Security Framework Guidance, 2015**
- ED-2xx - **Guidance on Security Event Management, 2020**

Product (Aircrafts/STCs)

- ED-202A/DO-326A - **Airworthiness Security Process Specification, 2014**
- ED-203A/DO-356 - **Airworthiness Security Methods and Considerations, 2018**
- ED-204/DO-355 - **Information Security Guidance For Continuing Airworthiness, 2014**

ATM/ANS

- ED205 - **Security Certification and Declaration of ATM ANS Ground Sys., 2020**

EUROCAE ED201 expected evolutions

ED-201 is under revision to provide compliancy support to future EASA regulation. **Sub-Group 1 of the ESCP is contributing to this work.**

ED-201A expected to be published by the end of 2020. Will include guidance on:

EXTERNAL AGREEMENTS

An External Agreement addresses the fundamental information security problems caused by using 3rd party products, linking networks and sharing data.

RECOMMENDED CLAUSES for External Agreements

External Agreements are documented expressions of trust comprising an **auditable set of clauses** (mutual agreements) to ensure that external dependencies on partners have adequate controls for safe and secure air transport operation.

Shared Trans-Organisational Risk Assessments

- → **Sub-Group 1: Standardisation of Risk Assessments**
  - → Development of material for the standardisation of risks assessments, including common terms and definitions and contractual provisions between interfacing organisations in order to be able to assess and compare their shared risks.
  - → This material will be used in AMC/GM material and Industry Standards (ED-201).
- → **Sub-Group 2: Identification of interfaces and functional chains**
  - → Identification of examples of chains of organisations and products/systems which are interconnected (end-to-end perspective). Risks are flowing along theses functional chains.
    - → A particular organisation could be in several functional chains.
  - → Development of maps (per aviation domain) showing examples of functional chains, in order to help organisations to identify their interfaces.
  - → This material will be used for the development of AMC/GM material

Next steps

- **March 2020: Table-Top Exercise in Madrid (Spain)**
  - Test the methodology developed by the Sub-Group 1 on a number of example organisations, in order to assess the risks coming from their interfacing organisations/systems in the corresponding functional chain (developed by Sub-Group 2).
  - This will include participation of members from ESCP STORM Sub-Groups 1 and 2.
  - It will help fine-tune the amendments to ED-201.
- **June 2020: Submission of ED-201 changes for formal consultation.**
- **End 2020: Adoption of amendments to ED-201.**

- **Expected end 2021 or beginning 2022: Once the future rule is adopted by the European Commission, adoption by EASA of the associated AMC/GM material, with reference to the applicable standards.**

EASA
European Union Aviation Safety Agency

Questions

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union

EASA
European Union Aviation Safety Agency

Introduction to the Sharing of Information

Davide Martini

Senior Expert - Cybersecurity in Aviation

5th – 7th February 2020

Colombo – Sri Lanka

Your safety is our mission.

An Agency of the European Union

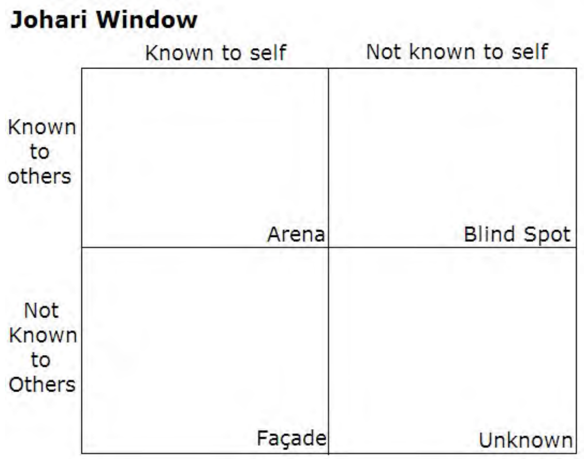
Why Sharing is so important in Cybersecurity

We may have some clue about the threat agents, vulnerabilities and exploits to perform a reasonable assessment as of today.

However, new threats may appear without notice and it is a fact that its practically impossible to know all the vulnerabilities of a system.

It is essential to be aware of the existence of elements of Knowledge that will emerge in the future and may change the risk picture.

The practical scheme is provided by the Johari Window that introduces the notion of "unknown unknowns".



Johari Window

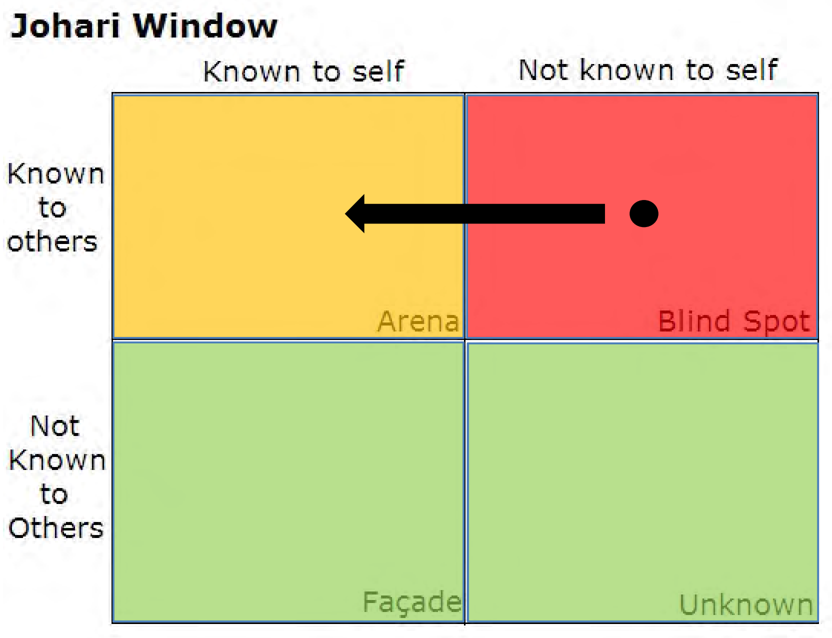
	Known to self	Not known to self
Known to others	Arena	Blind Spot
Not Known to Others	Façade	Unknown

Your (the defender) perspective

- The “Self” is your organisation

The “unknown unknown” is safe until it becomes know to a threat source than turns into a “blind spot” for you

If “others” with knowledge are “allies” there should be means in place to get to the Arena state



Johari Window

Known to self

Not known to self

Known to others

Not Known to Others

Arena

Blind Spot

Façade

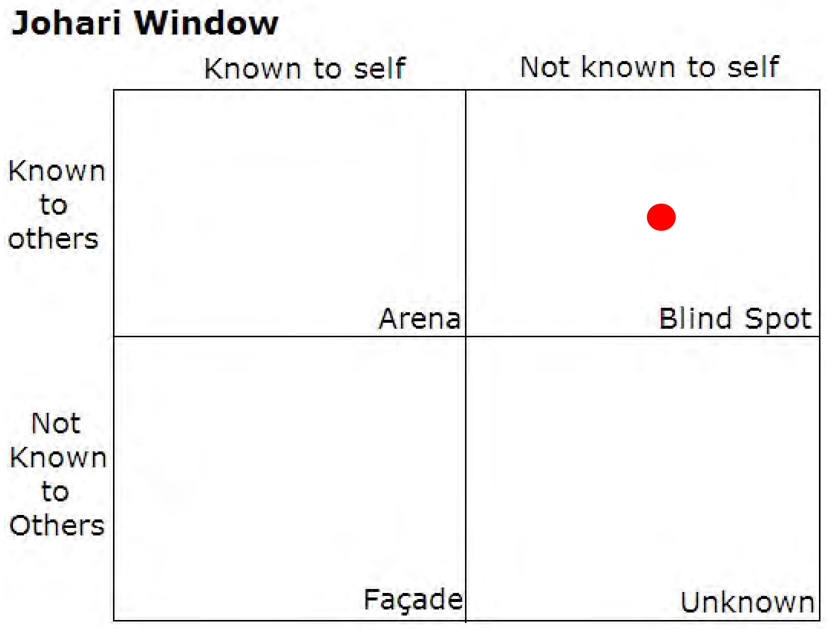
Unknown

The opponent perspective

What if “others” is a Threat Source?

The Blind Spot is a Zero Days quadrant

Vulnerabilities privately known, unpatched and exploitable!



Johari Window

	Known to self	Not known to self
Known to others	Arena	● Blind Spot
Not Known to Others	Façade	Unknown

How to maintain security – Reality Check

NIST - NVD

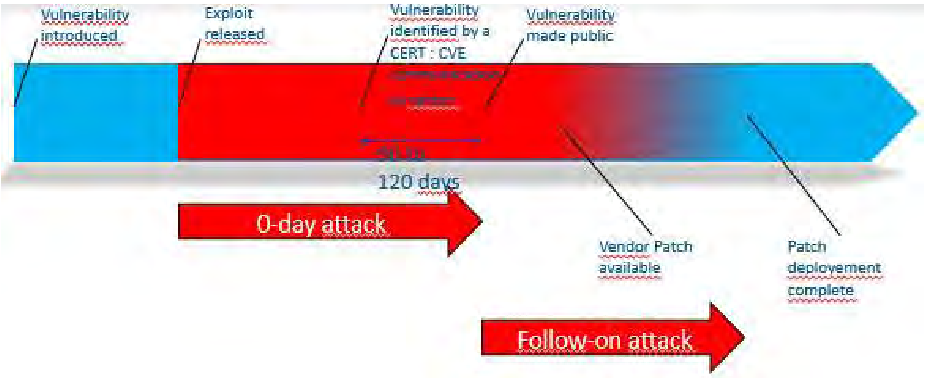
Common Vulnerabilities and Exposures is a list of entries for **publicly** known cybersecurity vulnerabilities.

Let’s have a look…

https://nvd.nist.gov

>100.000 entries ☹

Zero Day – Rand Corporation



7 years average ☹

ICAO Assembly Resolution 39-19

- Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as **sharing of information to help identify critical vulnerabilities that need to be addressed**;

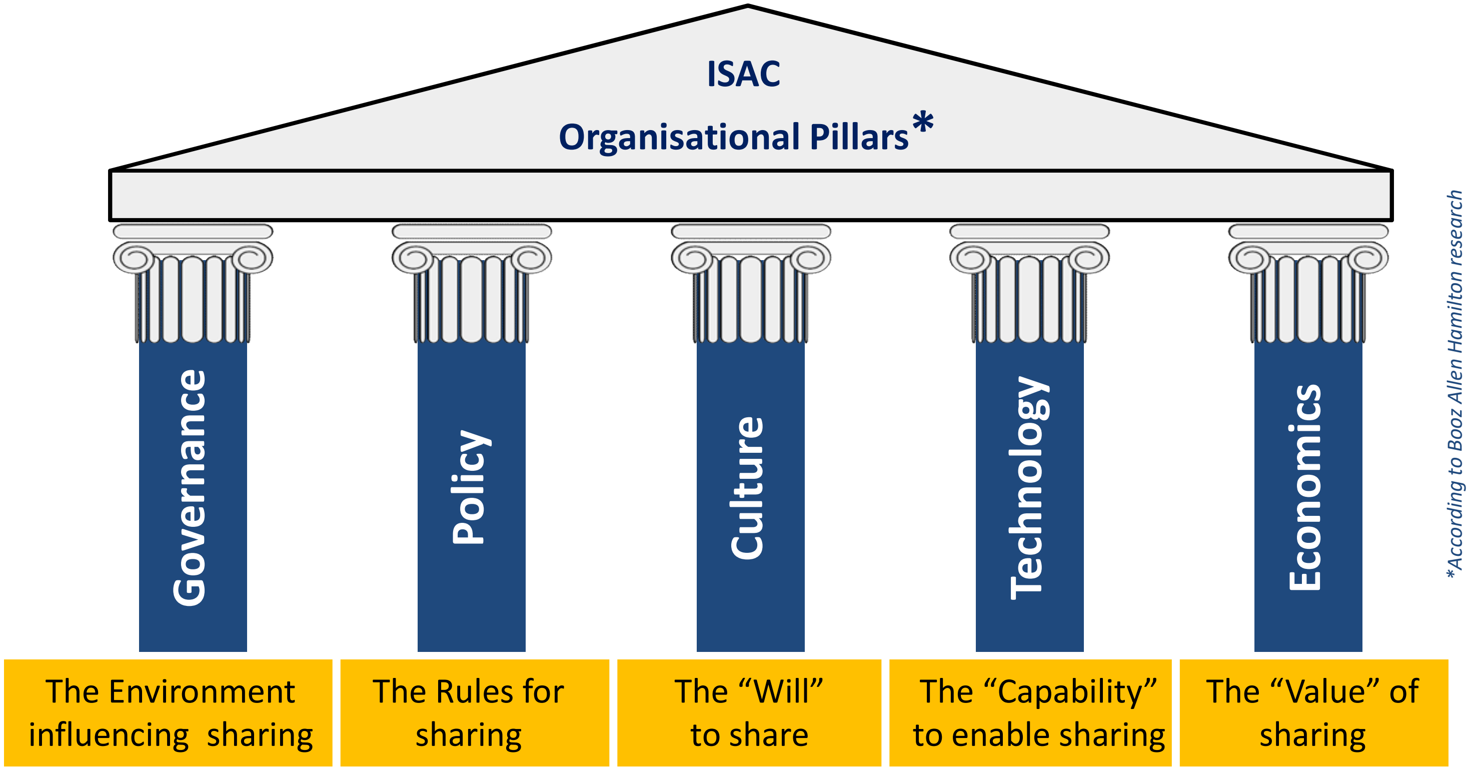
- Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts.

Main Sectorial Initiatives

Information Sharing and Analysis Centres (ISACs) and Computer Emergency Response Teams (CERTs)

- → Aviation ISAC (A-ISAC) – US Industry initiative, activities started in 2014, more than 70 members
- → European Centre for Cyber Security in Aviation (ECCSA) – EU cross cutting initiative supported by EASA, activities started in 2019, 26 members and growing
- → EATM- CERT –EUROCONTROL initiative aimed at to providing proactive cyber-security services, within EUROCONTROL, and, on a voluntary basis, to EUROCONTROL stakeholders

Organisational Pillars for Information Sharing



ISAC

Organisational Pillars*

Governance

Policy

Culture

Technology

Economics

The Environment influencing sharing

The Rules for sharing

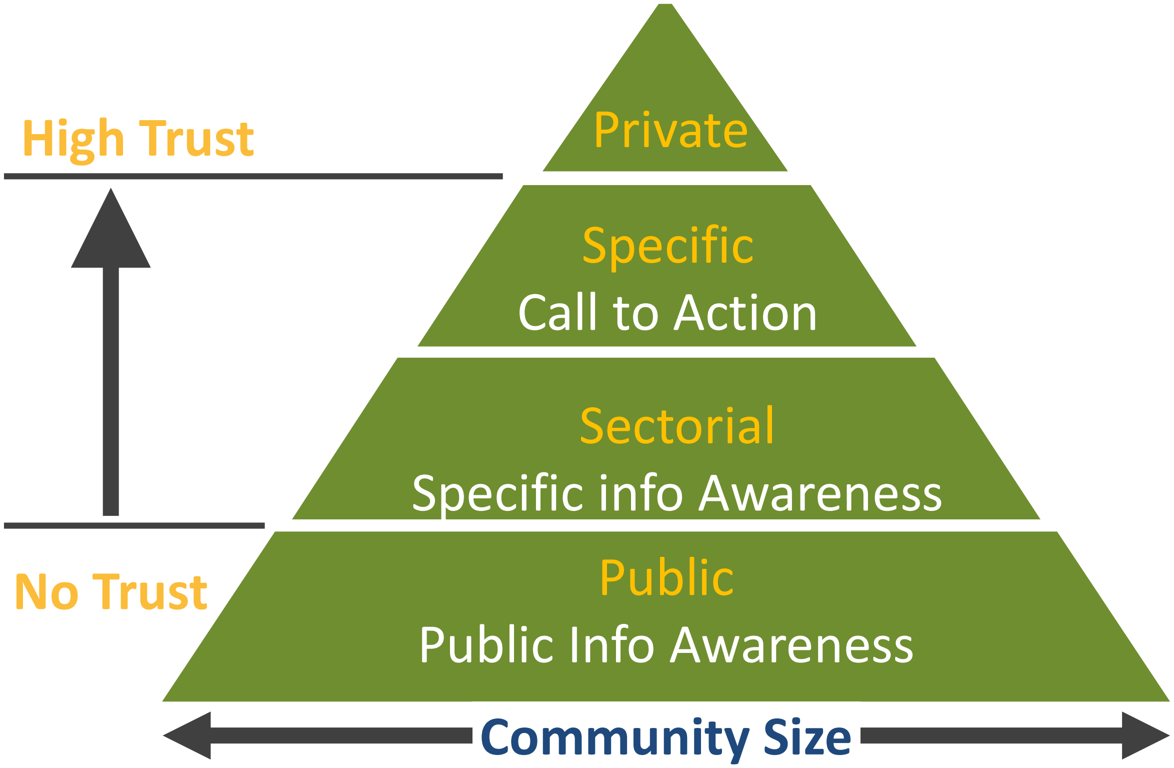
The "Will" to share

The "Capability" to enable sharing

The "Value" of sharing

**According to Booz Allen Hamilton research*

Info Sharing and Trust levels



High Trust

Private

Specific

Call to Action

Sectorial

Specific info Awareness

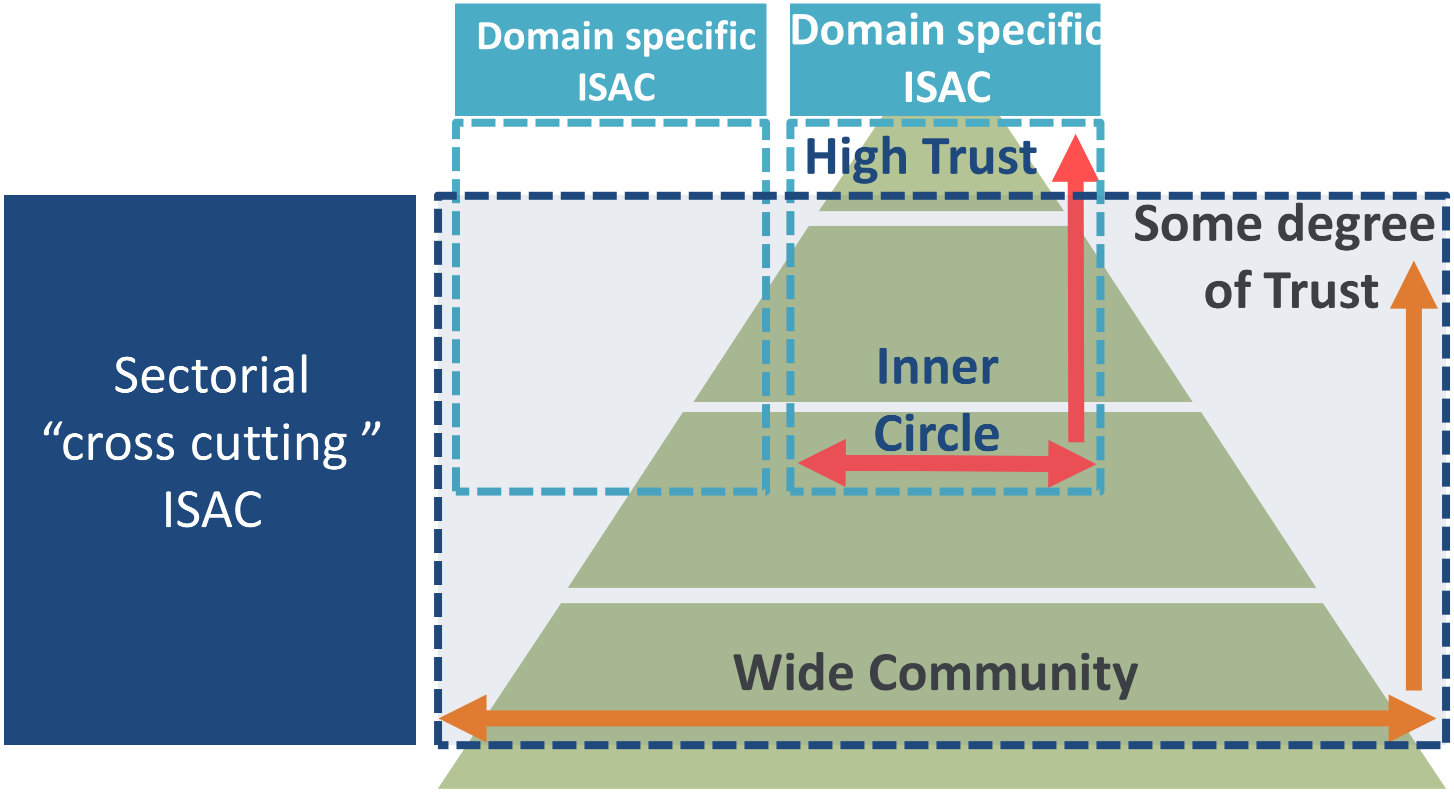
Public

Public Info Awareness

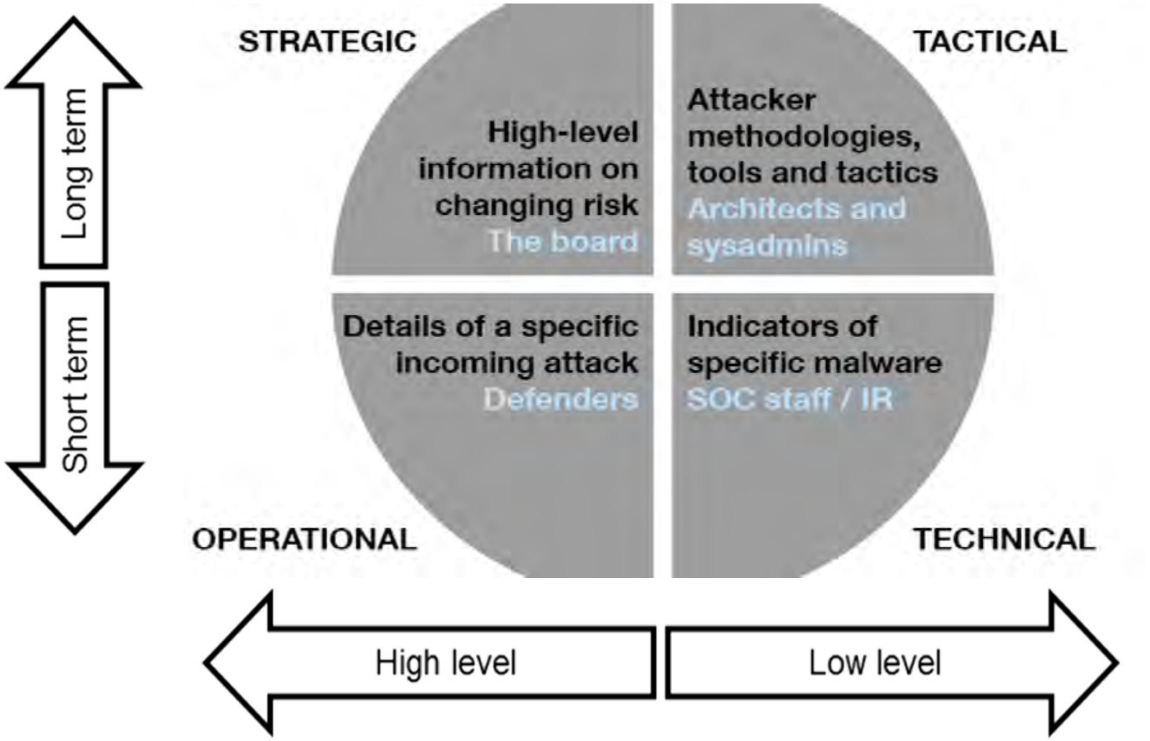
No Trust

Community Size

Cross cutting vs targeted initiatives



What to Share


Long term
Short term
STRATEGIC
TACTICAL
High-level information on changing risk
The board
Attacker methodologies, tools and tactics
Architects and sysadmins
Details of a specific incoming attack
Defenders
Indicators of specific malware
SOC staff / IR
OPERATIONAL
TECHNICAL
High level
Low level

EASA
European Union Aviation Safety Agency

Sharing of Operational Information

Davide Martini

Senior Expert - Cybersecurity in Aviation

5th – 7th February 2020

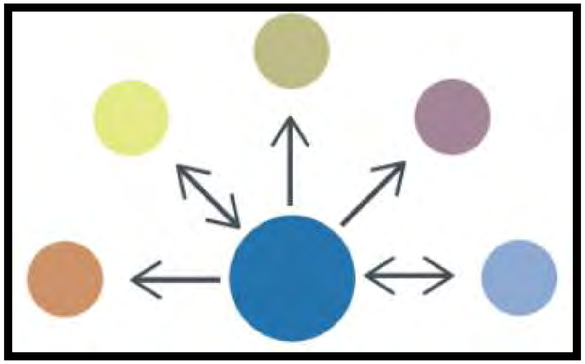
Colombo – Sri Lanka

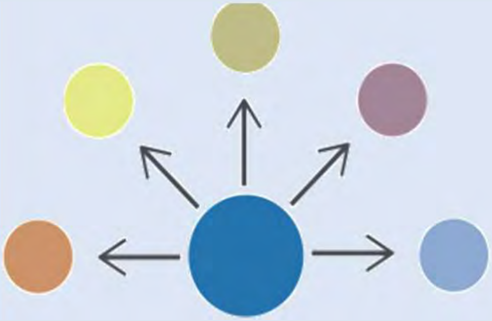
Your safety is our mission.

An Agency of the European Union

How - Information Sharing Models

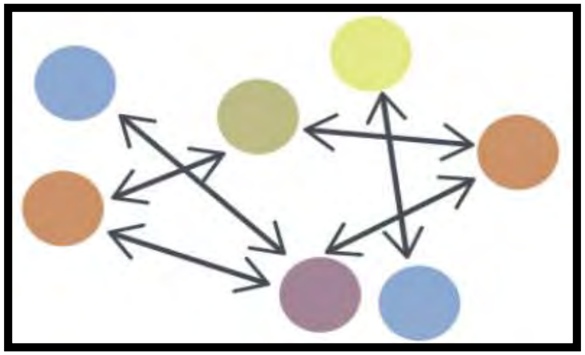
Hub and Spoke - one organization acts as a clearinghouse (the hub) for all sharing participants (the spokes). A spoke shares information with the hub, which then re-shares this information with all other spokes. The hub may perform analytics or filtering before re-sharing information. In this architecture, information may flow from spoke to hub and from hub to spoke.





Source/Subscriber - one organization acts as a single source of information for all subscribers. In this architecture, information flows from the source to a subscriber.

Peer to Peer - any number of organizations act as both producers and consumers of information. In this architecture, information flows from one peer to another peer.



How - Sensitive Information sharing Rules

Two main widely adopted rules:

→Traffic Light protocol

→Chatham House Rule

Traffic Light Protocol (TLP)

A way to ***commonly understand*** the exchange of (more or less) sensitive information among a group of organisations

A fundamental concept ***for the originator to signal*** how widely they want their information to be circulated beyond the immediate recipient.

What does the TLP NOT mean to be?

It is **NOT** a way to ***classify information*** according to sensitivity, based upon „harm to the organisation“!

It does NOT imply that those handling this information are „security cleared“

It does **NOT** prescribe a way ***to handle*** the information exchanged

EASA

The TLP Tags in Detail: TLP:RED

TLP:RED = Not for disclosure, restricted to participants only.

- Sources may use **TLP:RED** when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's *privacy, reputation, or operations* if misused.
- Recipients may not share **TLP:RED** information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
- In the context of a meeting, for example, **TLP:RED** information is limited to those present at the meeting.
- In most circumstances, **TLP:RED** should be exchanged verbally or in person.

(source: FIRST - Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:AMBER

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

- Sources may use **TLP:AMBER** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
- Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
- Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

(source: FIRST – Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:GREEN

TLP:GREEN = Limited disclosure, restricted to the community.

- Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
- Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
- Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.

(source: FIRST - Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:WHITE

TLP:WHITE = Disclosure is not limited.

- Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

(source: FIRST - Forum of Incident Response and Security Teams)

The Chatham House Rule

When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

The Missing Link - Attribution

→ Some legal frameworks restrict Sharing of full Information

- National Security Considerations

→ Organisations have contractual obligations

- Foreign National Customers
- State Customers

→ Trans-Organisational Information Sharing Facilities need to protect the interests of their constituencies

- Intellectual property, Privacy, Competitive Information

EASA
European Union Aviation Safety Agency

Thank you for your attention!

Questions?

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union

EASA

European Union Aviation Safety Agency

Introduction to the Sharing of Information

Davide Martini

Senior Expert - Cybersecurity in Aviation

5th – 7th February 2020

Colombo – Sri Lanka

Your safety is our mission.

An Agency of the European Union

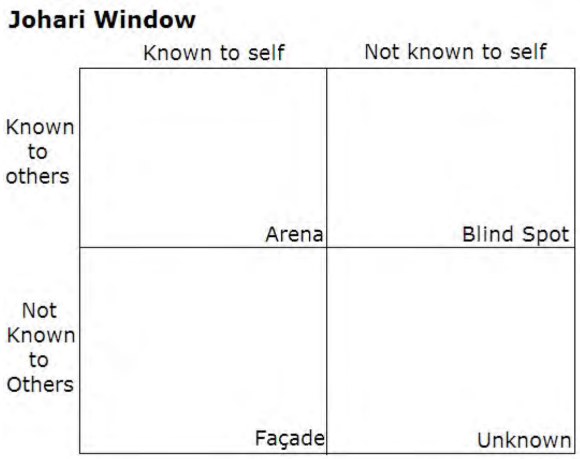
Why Sharing is so important in Cybersecurity

We may have some clue about the threat agents, vulnerabilities and exploits to perform a reasonable assessment as of today.

However, new threats may appear without notice and it is a fact that its practically impossible to know all the vulnerabilities of a system.

It is essential to be aware of the existence of elements of Knowledge that will emerge in the future and may change the risk picture.

The practical scheme is provided by the Johari Window that introduces the notion of "unknown unknowns".



Johari Window

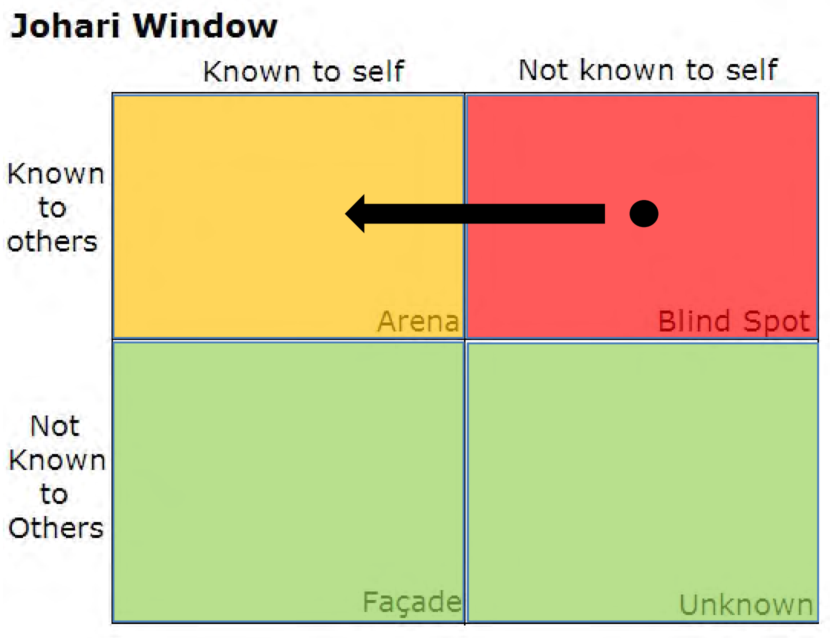
	Known to self	Not known to self
Known to others	Arena	Blind Spot
Not Known to Others	Façade	Unknown

Your (the defender) perspective

- The “Self” is your organisation

The “unknown unknown” is safe until it becomes know to a threat source than turns into a “blind spot” for you

If “others” with knowledge are “allies” there should be means in place to get to the Arena state

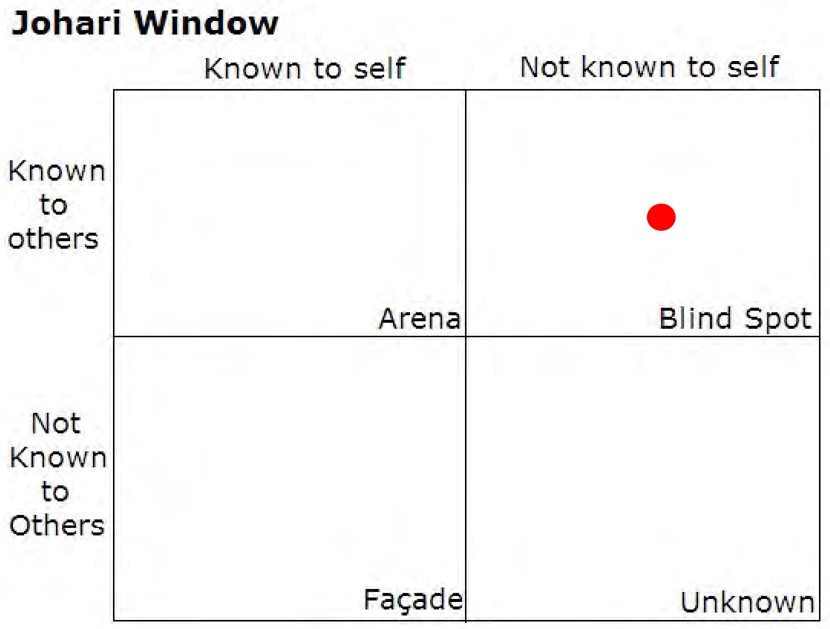


The opponent perspective

What if “others” is a Threat Source?

The Blind Spot is a Zero Days quadrant

Vulnerabilities privately known, unpatched and exploitable!



Johari Window

	Known to self	Not known to self
Known to others	Arena	● Blind Spot
Not Known to Others	Façade	Unknown

How to maintain security – Reality Check

NIST - NVD

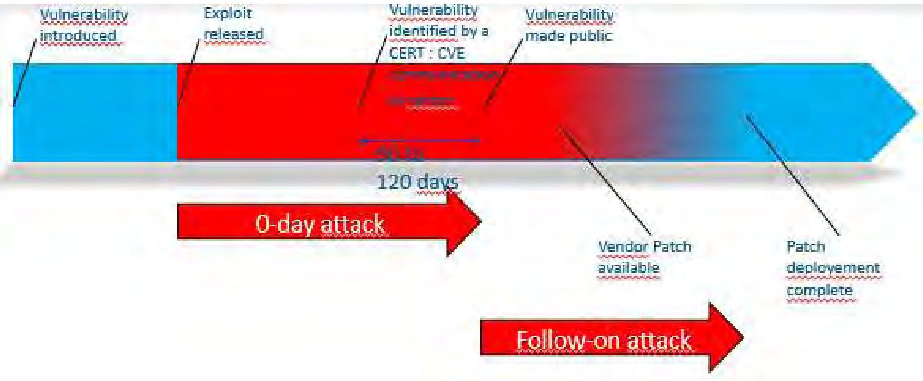
Common Vulnerabilities and Exposures is a list of entries for **<u>publicly</u>** known cybersecurity vulnerabilities.

Let’s have a look…

https://nvd.nist.gov

>100.000 entries ☹

Zero Day – Rand Corporation



7 years average ☹

ICAO Assembly Resolution 39-19

- Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as **sharing of information to help identify critical vulnerabilities that need to be addressed**;

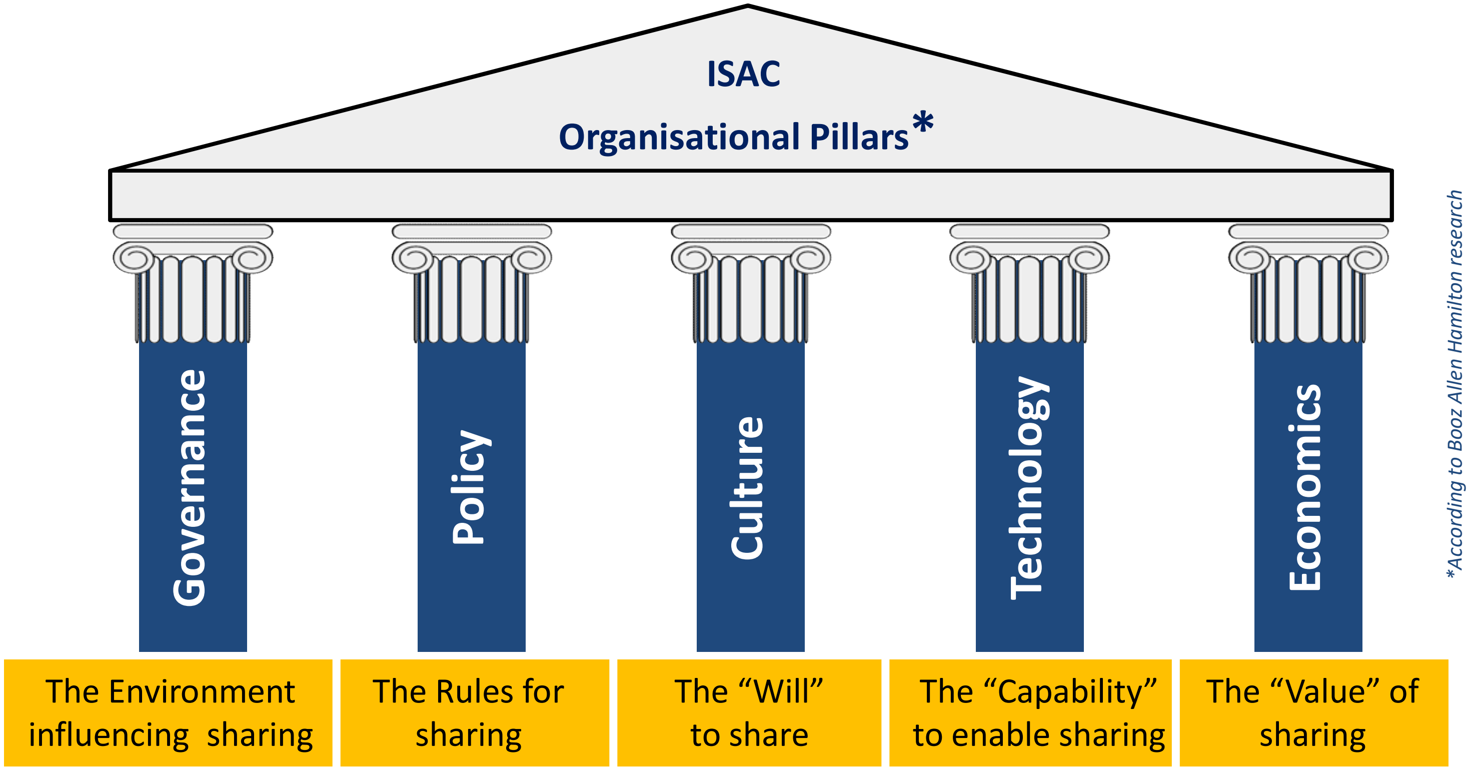
- Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts.

Main Sectorial Initiatives

Information Sharing and Analysis Centres (ISACs) and Computer Emergency Response Teams (CERTs)

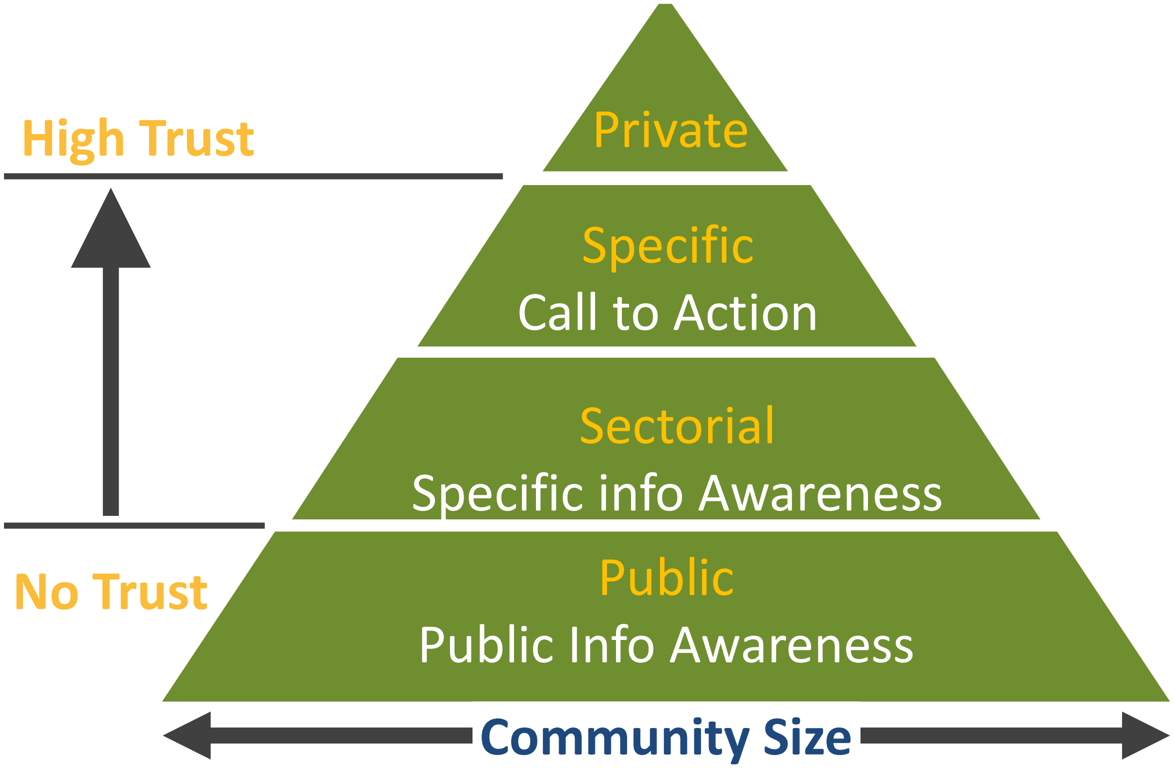
- → Aviation ISAC (A-ISAC) – US Industry initiative, activities started in 2014, more than 70 members
- → European Centre for Cyber Security in Aviation (ECCSA) – EU cross cutting initiative supported by EASA, activities started in 2019, 26 members and growing
- → EATM- CERT –EUROCONTROL initiative aimed at to providing proactive cyber-security services, within EUROCONTROL, and, on a voluntary basis, to EUROCONTROL stakeholders

Organisational Pillars for Information Sharing



*According to Booz Allen Hamilton research

Info Sharing and Trust levels


High Trust

No Trust

Private

Specific

Call to Action

Sectorial

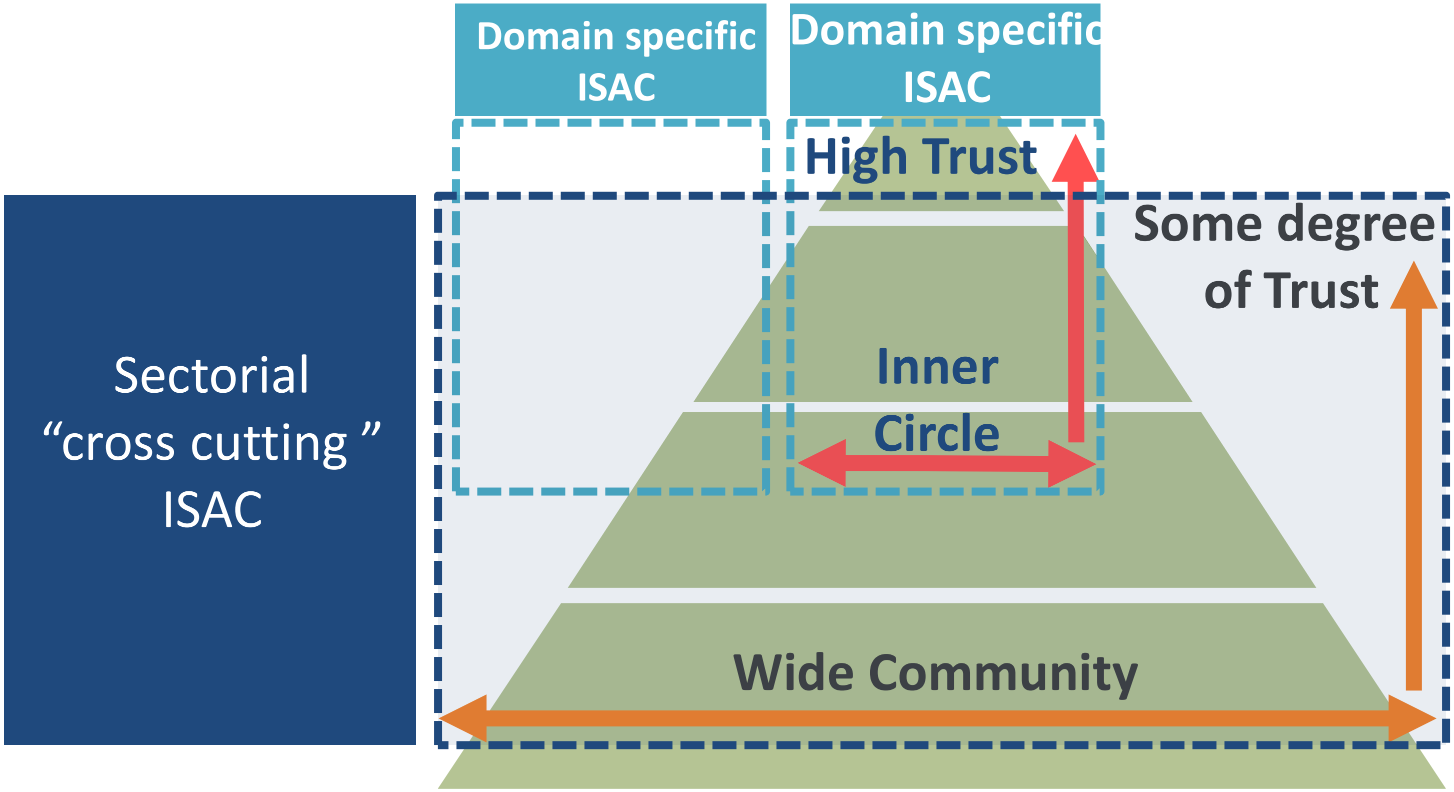
Specific info Awareness

Public

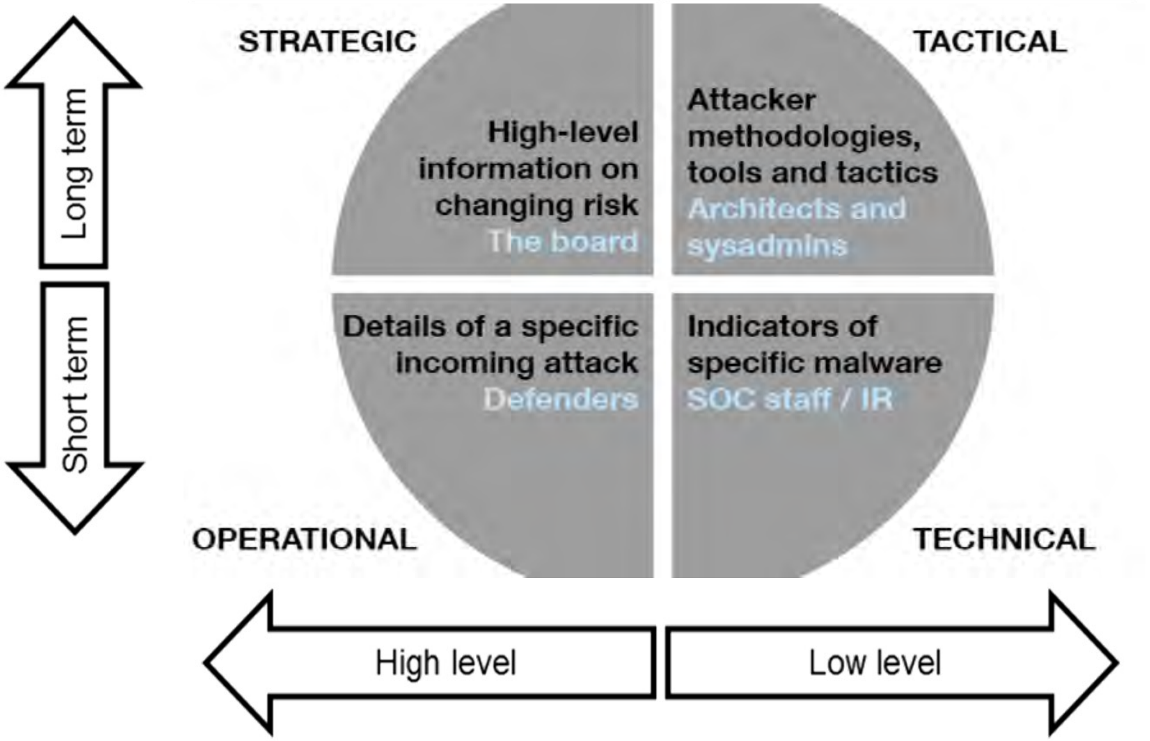
Public Info Awareness

Community Size

Cross cutting vs targeted initiatives



What to Share



Long term
Short term
STRATEGIC
TACTICAL
High-level information on changing risk
The board
Attacker methodologies, tools and tactics
Architects and sysadmins
Details of a specific incoming attack
Defenders
Indicators of specific malware
SOC staff / IR
OPERATIONAL
TECHNICAL
High level
Low level

EASA

European Union Aviation Safety Agency

Sharing of Operational Information

Davide Martini

Senior Expert - Cybersecurity in Aviation

5th – 7th February 2020

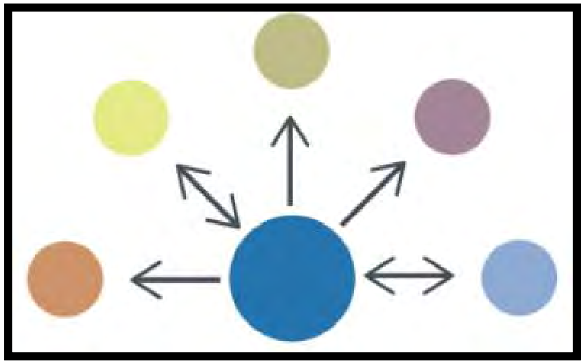
Colombo – Sri Lanka

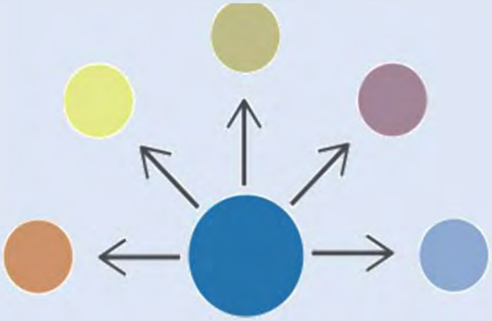
Your safety is our mission.

An Agency of the European Union

How - Information Sharing Models

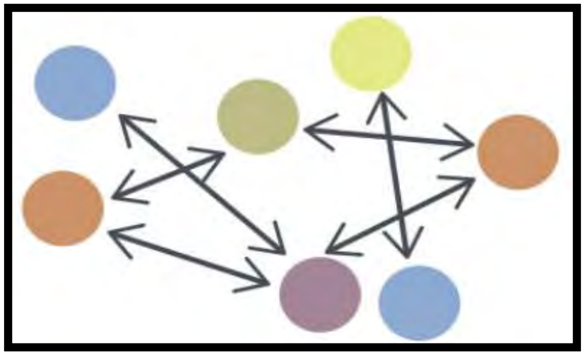
Hub and Spoke - one organization acts as a clearinghouse (the hub) for all sharing participants (the spokes). A spoke shares information with the hub, which then re-shares this information with all other spokes. The hub may perform analytics or filtering before re-sharing information. In this architecture, information may flow from spoke to hub and from hub to spoke.





Source/Subscriber - one organization acts as a single source of information for all subscribers. In this architecture, information flows from the source to a subscriber.

Peer to Peer - any number of organizations act as both producers and consumers of information. In this architecture, information flows from one peer to another peer.



How - Sensitive Information sharing Rules

Two main widely adopted rules:

→Traffic Light protocol

→Chatham House Rule

Traffic Light Protocol (TLP)

A way to ***commonly understand*** the exchange of (more or less) sensitive information among a group of organisations

A fundamental concept ***for the originator to signal*** how widely they want their information to be circulated beyond the immediate recipient.

What does the TLP NOT mean to be?

It is **NOT** a way to ***classify information*** according to sensitivity, based upon „harm to the organisation“!

It does NOT imply that those handling this information are „security cleared“

It does **NOT** prescribe a way ***to handle*** the information exchanged

EASA

The TLP Tags in Detail: TLP:RED

TLP:RED = Not for disclosure, restricted to participants only.

- Sources may use **TLP:RED** when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's *privacy, reputation, or operations* if misused.
- Recipients may not share **TLP:RED** information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
- In the context of a meeting, for example, **TLP:RED** information is limited to those present at the meeting.
- In most circumstances, **TLP:RED** should be exchanged verbally or in person.

(source: FIRST - Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:AMBER

TLP:AMBER = Limited disclosure, restricted to participants' organizations.

- Sources may use **TLP:AMBER** when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
- Recipients may only share **TLP:AMBER** information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.
- Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.

(source: FIRST – Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:GREEN

TLP:GREEN = Limited disclosure, restricted to the community.

- Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
- Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
- Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.

(source: FIRST - Forum of Incident Response and Security Teams)

The TLP Tags in Detail: TLP:WHITE

TLP:WHITE = Disclosure is not limited.

- Sources may use **TLP:WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
- Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

(source: FIRST - Forum of Incident Response and Security Teams)

The Chatham House Rule

When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed.

The Missing Link - Attribution

→ Some legal frameworks restrict Sharing of full Information

- National Security Considerations

→ Organisations have contractual obligations

- Foreign National Customers
- State Customers

→ Trans-Organisational Information Sharing Facilities need to protect the interests of their constituencies

- Intellectual property, Privacy, Competitive Information

EASA
European Union Aviation Safety Agency

Thank you for your attention!

Questions?

easa.europa.eu/connect

Your safety is our mission.

An Agency of the European Union