# High Level Cybersecurity Conference

## Airline perspective

Angeles Pozo, Assistant Director Security, Europe

Madrid, 4-5 March 2020

# IATA Aviation Cyber Security

**Challenge**

- Variety, complexity, scale of the impact of attacks
- Regulatory framework

**A threat-based, risk-managed and outcome-focused approach**

- with an integrated risk management system where SeMS and SMS are used jointly to manage cyber threats and risks

**Four Principles**

- **Cyber Security Culture**
- **Transparency and Trust**
- **Communication and Collaboration**
- **Workforce**

Challenges

# Avoid duplication of oversight activities

Current legal framework with different regulations applying simultaneously

- Ensure **clear guidance** is given to avoid duplications between Authorities.
- **Clarity** on the competent authority to do the oversight.
- Take advantage of all **commonalities** of different regulations.
- Guidance should be provided for **suppliers/contractors**

Challenges

# Consistency of incident reporting schemes

Internal and external reporting as an integral part of the cyber response

- **Guidance** should be given on what should be reported, who should be reporting, under what format and at what specific moment.
- **Vulnerabilities** vs. cyber security **occurrences**
- **Information sharing** as part of the reporting scheme which should involve all stakeholders.
- **Competent Authority** responsible to receive the occurrence report and legal basis

Challenges

# Availability of adequate competences

Ensure staff understands cyber risks and threats as well as roles and responsibilities

- Ensure to build an **aviation cyber security workforce** and **teach the current aviation personnel** how to recognize and manage cyber risks, leading to increased vigilance and resilience.
- Encourage the aviation industry to **instigate programs and inspire a new generation** of individuals and organizations
- Raise cyber security **awareness** and ensure **capacity building**
- Develop **cyber security training**

# Integrated cyber security approach

Threat-based, risk-managed and outcome-focused where Security Management System (SeMS) and Safety Management System (SMS) models can be applied to manage cyber threats and risks

- An **integrated risk management** approach to safety and security, which incorporates a pro-active assessment of vulnerabilities and threats to ensure information security risks are managed within acceptable levels.
- Guidance is needed to **integrate the requirement of Information Security Management Systems** with other management systems in place.
- Ensure **existing standards** used by industry are taken into account for complying purposes. GM will be needed in this area.

# THANK YOU