UK
Civil Aviation
Authority

# Airworthiness and Cyber Security Oversight

Nicky Keeley
Head of Cyber Security Oversight

# What is cyber security?

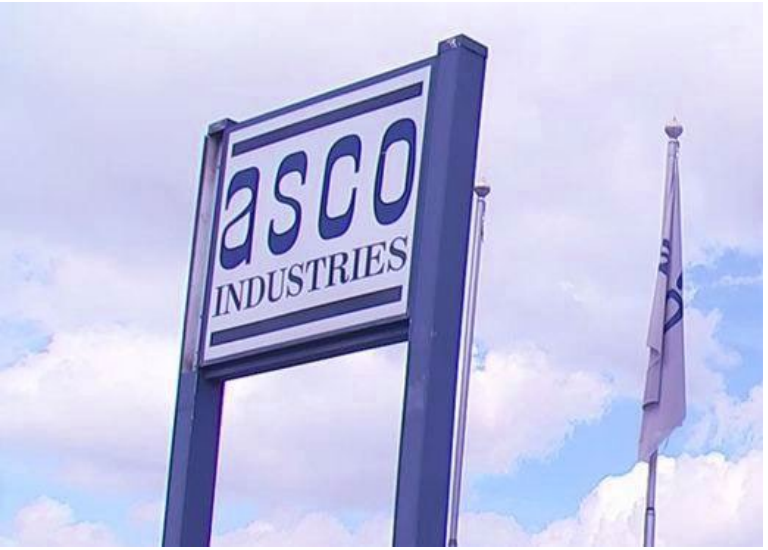
# Why is this relevant?

*Video on lateral movement removed due to size*

# Ransomware halts production for days at major airplane parts manufacturer

Nearly 1,000 employees sent home for the entire week, on paid leave.

By Catalin Cimpanu for Zero Day | June 12, 2019 -- 19:27 GMT (20:27 BST) | Topic: Security




BUSINESS NEWS SEPTEMBER 26, 2019 / 9:11 AM / 25 DAYS AGO

## Hackers tried to steal Airbus secrets via contractors - AFP

PARIS (Reuters) - A series of cyber attacks on Airbus in the past few months was conducted via the computer systems of its suppliers and security sources suspect a link to China, AFP news agency reported on Thursday.

National Cyber Security Centre

**Alert: Mass credential harvesting phishing campaign active in the UK**

The NCSC is investigating an automated, ongoing, widespread credential-harvesting phishing campaig...

NEWS • 18 OCTOBER 2019

AVIATION
DEF CON
VILLAGE

*To have a proportionate and effective approach to cyber security oversight that enables aviation to manage their cyber security risks without compromising aviation safety, security or resilience.*

# Our Vision

*To stay up-to-date and positively influence cyber security within aviation to support the UK's National Cyber Security Strategy.*

# Regulatory Landscape

UK Civil Aviation Authority

**REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**of 4 July 2018**

(12) The measures taken in accordance with this Regulation to regulate civil aviation in the Union, and the delegated and implementing acts adopted on the basis thereof, should correspond and be proportionate to the nature and risks associated with the different types of aircraft, operations and activities they address. Such measures should also, in as far as possible, be formulated in a manner which focuses on objectives to be achieved, while allowing different means of achieving those objectives, and should also foster a systemic approach to civil aviation, taking into account interdependencies between safety and other technical domains of aviation regulation, including cyber security. This should contribute to a more cost-efficient achievement of required safety levels and to the stimulation of technical and operational innovation. Use should be made of recognised industry standards and practices, where it has been found that they ensure compliance with the essential requirements set out in this Regulation.

## The Network and Information Systems Regulations 2018

**COMMISSION IMPLEMENTING REGULATION (EU) 2017/373**

**of 1 March 2017**

**ATM/ANS.OR.D.010 Security management**

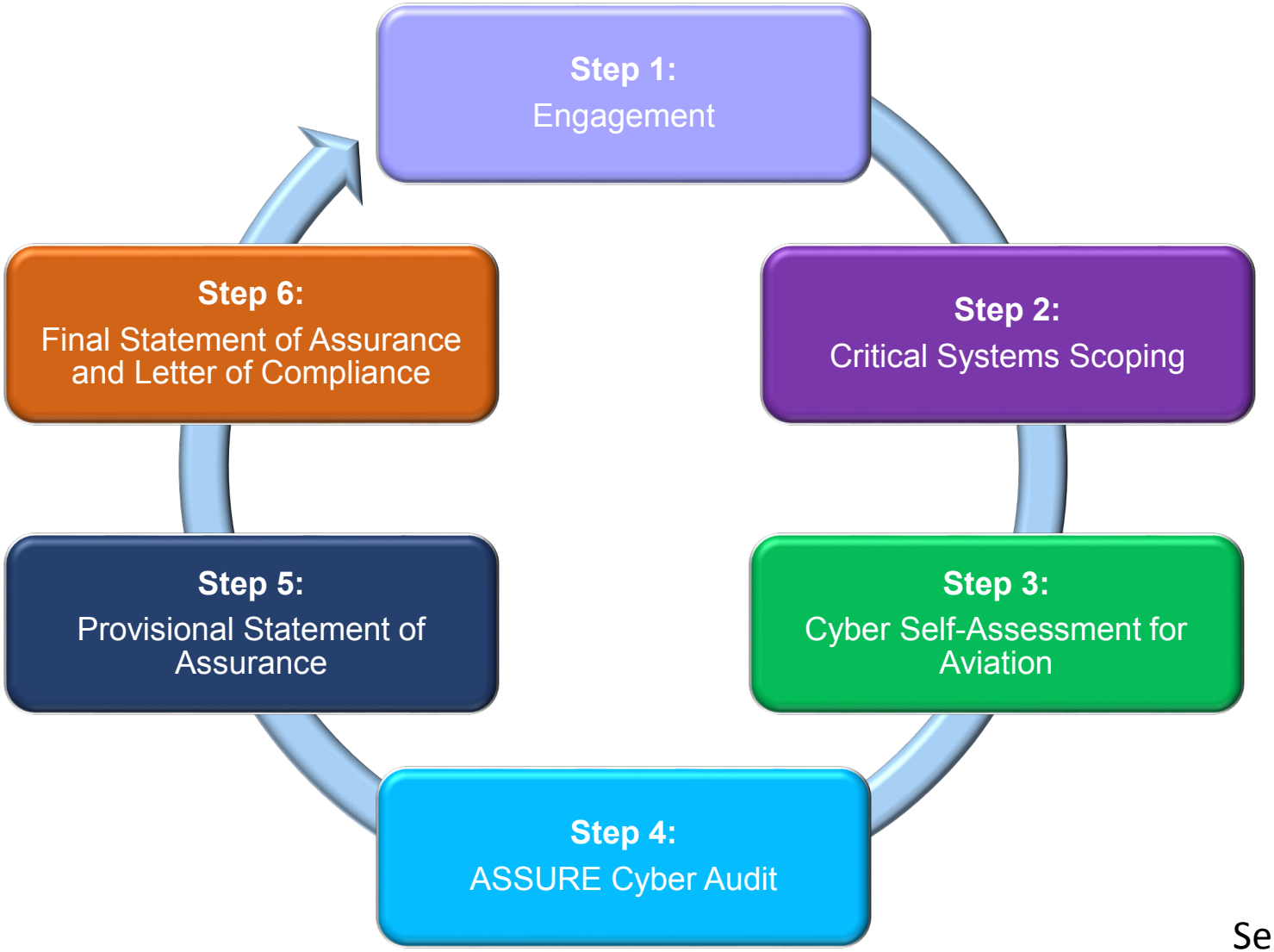
(d) Air navigation services and air traffic flow management providers and the Network Manager shall take the necessary measures to protect their systems, constituents in use and data and prevent compromising the network against information and cyber security threats which may have an unlawful interference with the provision of their service.

**COMMISSION IMPLEMENTING REGULATION (EU) 2019/1583**

**of 25 September 2019**

**amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures**

# Cyber Security Oversight Process




See CAP1753

# Critical System Scoping

- Think about your essential services– top down
- Keep an eye on what's critical to avoid scope creep
- Find your security boundaries
- Identify your critical suppliers
- Don't forget your operational technology!



UK Civil Aviation Authority

Department for Transport

National Cyber Security Centre
a part of GCHQ

UK Civil Aviation Authority

# CAF for Aviation

| Objectives | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A: Managing security risk** | | **B: Protecting against cyber attack** | | **C: Detecting cyber security incidents** | | **D: Minimising the impact of cyber security incidents** | |
| **Principles** | | | | | | | |
| A1: Governance | A2: Risk management | B1: Service protection policies and processes | B2: Identity and access control | C1: Security monitoring | C2: Proactive security event discovery | D1: Response and recovery planning | D2: Lessons learned |
| A3: Asset management | A4: Supply chain | B3: Data security | B4: System security | | | | |
| | | B5: Resilient networks and systems | B6: Staff awareness and training | | | | |

UK Civil Aviation Authority

ASSURE

CREST

ASSURE Cyber Suppliers

ASSURE Cyber Professionals

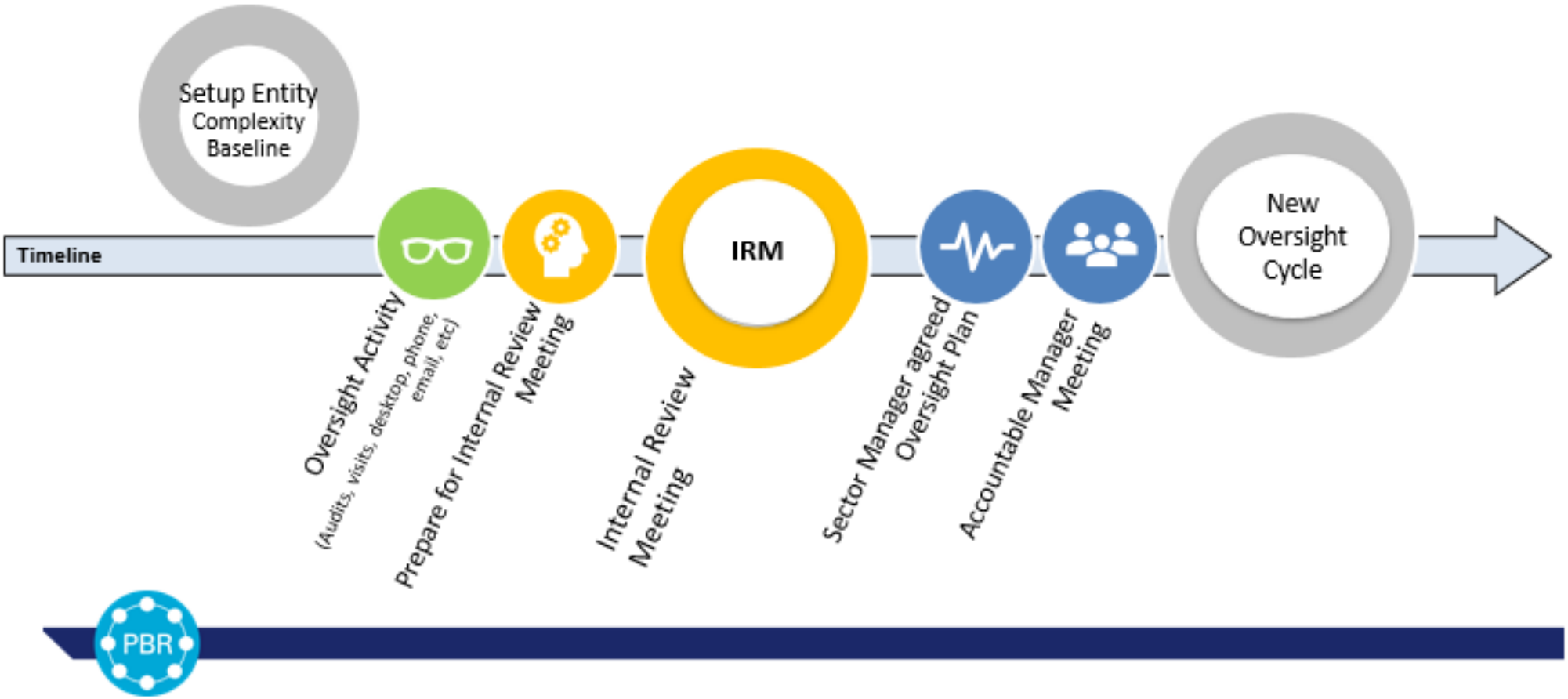
✓ ASSURE Cyber Audit

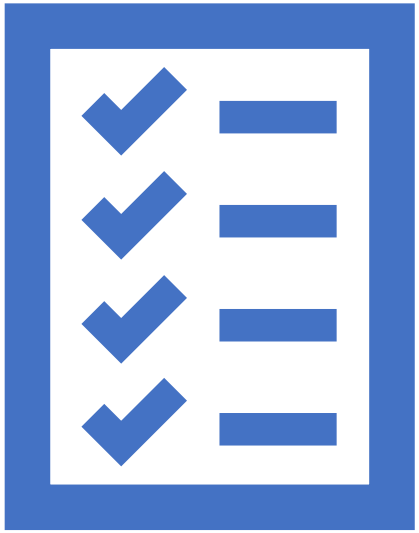
# Statement of Assurance

- Completed Critical Systems Scoping Templates
- Completed Critical system scoping diagrams
- ASSURE Audited CAF for Aviation for all in-scope systems
- ASSURE Audit Report
- Corrective Action Plan supporting documents

UK Civil Aviation Authority

# Performance Based Oversight





# Letter of Compliance

- Engagement with CAA
- Completion of critical system scoping activity
- Completion of Cyber Self-Assessment
- Procurement of ASSURE Cyber Audit where required
- Progress towards or maintenance of appropriate and proportionate cyber security controls in line with the agreed profile
- Notification of reportable incidents (if applicable)
- Notification of cyber security change
- Information requests


cyber@caa.co.uk