

The Cyber Security Oversight Process for Aviation

CAP 1753



Published by the Civil Aviation Authority, 2020

Civil Aviation Authority
Aviation House
Beehive Ring Road
Crawley
West Sussex
RH6 0YR

You can copy and use this text but please ensure you always use the most up to date version and use it in context so as not to be misleading and credit the CAA.

First published October 2019

Issue 2 – August 2020

Enquiries regarding the content of this publication should be addressed to: cyber@caa.co.uk

The latest version of this document is available in electronic format at: www.caa.co.uk/CAP1753

Contents

Contents	3
1. Introduction	4
2. Background	5
3. Purpose	6
4. Roles and Responsibility	7
Department for Transport	7
Civil Aviation Authority	7
National Cyber Security Centre	7
Accountable Manager	8
Cyber Security Responsible Manager	8
ASSURE Cyber Suppliers	8
ASSURE Cyber Professionals	8
5. Applicable Regulation	9
6. CAP1753 – Cyber Security Oversight Process for Aviation	10
Step 1 - Engagement	11
Step 2 - Critical System Scoping	11
Step 3 - Cyber Self-Assessment	12
Step 4 - ASSURE Cyber Audit	12
Step 5 - Provisional Statement of Assurance	14
Step 6 - Final Statement of Assurance and Certificate of Compliance	15
7. Frequency	16
8. Notification of Cyber Security Change	17
8.1. Notification of Change of Cyber Security Responsible Manager	17
Annex A: Information Handling	18
Annex B: The CAA's Regulatory Enforcement Approach (non-NIS)	19
Annex C: NIS Regulation	20
Annex D: DfT's Stepped Enforcement Approach for NIS	21
Annex E: Good Practice	22

1. Introduction

Cyber security risk profiles are dynamic, meaning attackers are always looking to exploit vulnerabilities and can quickly develop new ways of breaching cyber security. The aviation industry's progressively interconnected systems require the industry to maintain an up to date awareness of both direct and indirect cyber security threats. The changing threat landscape therefore, encourages a proactive approach to cyber security and in response means aviation organisations need dynamic protection.

Cyber security can be defined as:

“Cyber security refers to the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.”

UK National Cyber Security Strategy¹ - The Cyber Security Body of Knowledge (CyBOK)²

The Civil Aviation Authority's (CAA) cyber security oversight strategy must be reviewed regularly in order to keep pace with these ever-changing cyber security trends.

The vision for CAA Cyber Security Oversight is:

“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.

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

¹ <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>

² <https://www.cybok.org/knowledgebase/>

2. Background

The CAA's approach to cyber security oversight has been harmonised and consolidated to align with Better Regulation principles, this provides;

- **consistency** for aviation organisations;
- **reduced** duplication of oversight activity;
- assistance in **targeting** of cyber security regulatory activity; and
- improved **transparency**.

The CAA commit to, broad and collaborative engagement with industry and key stakeholders to continuously improve our cyber security oversight model.

Working closely with Department for Transport (DfT) and National Cyber Security Centre (NCSC) the CAA has developed the Cyber Assessment Framework (CAF) for Aviation³. Like the core CAF, the CAF for Aviation has been designed with scalability and consistency in mind. This allows it to be applied to aviation organisations of varying size and complexity whilst maintaining a consistent approach across different scopes including; safety, security, and resilience.



The CAA and the Council for Registered Ethical Security Testers (CREST)⁴, a not-for-profit accreditation and certification body, partnered to create an accreditation scheme (ASSURE). This service enables aviation organisations to procure accredited cyber security audit⁵ capabilities to audit their completed CAF for Aviation self-assessments⁶, where applicable.

³ The CAF for Aviation is an aviation specific adaptation of the core CAF v3 produced by NCSC

⁴ <https://crest-approved.org/index.html>

⁵ Step 4 – ASSURE Cyber Audit

⁶ Step 3 – Cyber Self-Assessment for Aviation

3. Purpose

CAP1753 outlines the CAA's approach to cyber security oversight, which includes:

- the CAF for Aviation;
- ASSURE Cyber Audit; and
- incorporation of cyber security oversight into existing CAA Performance Based Oversight processes.

The Cyber Security Oversight Process for Aviation involves six key steps:



Figure 1: Cyber Security Oversight Process for Aviation

4. Roles and Responsibility

The CAA has identified the following key roles pertinent to the Cyber Security Oversight Process for Aviation.

Department for Transport

DfT is responsible for setting the strategic direction of cyber security policy and regulation across transport, including Aviation. In relation to Network and Information Systems (NIS)⁷, where the Secretary of State for Transport is the co-competent authority, the Cyber Team in DfT will be responsible for NIS policy, identification thresholds, incident thresholds and enforcement.

Civil Aviation Authority

The UK's specialist aviation regulator is responsible for ensuring that the aviation industry meets the highest safety standards, that consumers have choice and, value for money, that they are protected and treated fairly when they fly, and that the aviation industry manages security risks effectively. The CAA holds responsibility for cyber security oversight for aviation and co-competent authority with Secretary of State for Transport under NIS, with responsibility for the implementation of NIS in aviation and post-incident investigation.

The CAA Cyber Security Oversight Team is responsible for all cyber security regulatory activity within any of the CAA regulatory domains (for example Continuing Airworthiness, Flight Operations, Aerodromes, Airspace, Air Traffic Management, and Aviation Security).

The team is also the first point of contact at the CAA for all questions and issues relating to the cyber security oversight process for aviation and can be contacted at cyber@caa.co.uk.

National Cyber Security Centre

As the UK's national technical authority for cyber security, the NCSC manages national cyber security incidents, provides an authoritative voice and centre of expertise on cyber security, and delivers tailored support and advice to departments, the Devolved Administrations, regulators, and businesses. While having no regulatory responsibilities, the NCSC is the Single Point of Contact (SPOC), and the Computer Security Incident Response Team (CSIRT) under NIS.

⁷ <http://www.legislation.gov.uk/ukxi/2018/506/made>

Accountable Manager

The Accountable Manager(s) is an individual or individuals designated by their aviation organisation as the person(s) responsible to the CAA in respect of the functions which are subject to regulation. It is expected that the role of Accountable Manager is held by an individual who has corporate authority for ensuring that all operational activities can be financed and carried out to the standard required by the CAA.

For cyber security accountability, individuals do not have to be the operational “Accountable Manager” registered with the CAA but instead can be an equivalent board member (e.g. Chief Information Security Officer, CIO, IT Director etc) dependent on the aviation organisation’s structure.

Cyber Security Responsible Manager

An individual who has been delegated responsibility for cyber security by the aviation organisation’s Accountable Manager, they may have responsibility for specific areas of their organisation (e.g. Head of Information Security, Safety Manager, Security Manager etc). The Cyber Security Responsible Manager ensures compliance with cyber security regulations and is responsible for the management of cyber security risk exposure.

As a Cyber Security Responsible Manager, you will be asked to demonstrate the appropriate competency for the post and to enable the sharing of threat information you will need to hold the relevant security clearance⁸.

ASSURE Cyber Suppliers

ASSURE Cyber Suppliers are third party “Qualified Entities” that are subject to rigorous and continuous accreditation processes in order to provide a cyber audit capability under the ASSURE Scheme. The ASSURE Cyber Supplier must adhere to the ASSURE Code of Conduct.

ASSURE Cyber Professionals

ASSURE Cyber Suppliers utilise ASSURE Cyber Professionals who hold appropriate professional certifications and are accredited to conduct ASSURE Cyber Audits. The accredited ASSURE Cyber Professionals must adhere to the ASSURE Code of Conduct.

ASSURE Cyber Professionals are accredited in one or more of the following three specialisms (all specialisms must be present for an ASSURE Cyber Audit):

- Cyber Audit & Risk Management;
- Technical Cyber Security Expert; and/or
- Industrial Control Systems/Operational Technology Expert.

⁸ Detail of the competency and vetting requirements can be found in the Cyber Security Responsible Manager Nomination Form.

5. Applicable Regulation

All aviation organisations that have regulatory cyber security obligations to comply with existing safety, security, and resilience requirements are deemed to be in scope of CAP1753. Following initial engagement⁹, each aviation organisation may be required to complete all or part of the of the steps detailed herein.

Existing regulations applicable to aviation organisations under CAP1753 include but are not limited to:

- EASA Basic Regulation and Implementing Rules;
- ICAO Standards and Recommended Practices (SARPs) and UK Air Navigation Order;
- Network and Information Systems (NIS) Regulation.

Note: This is an evolving area of regulation and the aviation organisation is responsible for staying abreast of regulatory requirements which may change from time to time.

The CAA recommend that regardless of the level of our regulatory involvement, aviation organisations should proactively apply appropriate and proportionate cyber security good practice¹⁰ into their operations.

⁹ Step 1 – Engagement

¹⁰ Annex E - Good Practice