UK Civil Aviation Authority

The Cyber Security Oversight Process for Aviation

CAP 1753

Published by the Civil Aviation Authority, 2024

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

First published October 2019
Issue 2 – August 2020
Issue 3 – April 2024

If you are already in possession of a Cyber Security Certificate of Compliance, you need take no further action in relation to this update, unless otherwise advised by the CAA.

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

1. Introduction

Recent reports indicate that cyber security threats remain a growing concern for many industries. Threat actors are continuously growing in capability as new products and tools become available and are relentlessly seeking to exploit vulnerabilities. The aviation industry's progressively interconnected systems and the ever-changing threat landscape requires the industry to remain vigilant to both direct and indirect cyber security threats.

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

2. Cyber Security Oversight

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

The CAA's approach to cyber security oversight has been updated to align with Better Regulation principles. It aims to provide:

- 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.

The CAA Cyber team has several Cyber Security Oversight Specialists who are available to offer support and guidance on all elements of the CAP1753 process. Aviation organisations will be assigned a specialist at Stage 1 – Engagement who will act as point of contact.

3. Objective and Scope

Aviation organisations will be notified of being in scope of the CAA Cyber Security Oversight Process for Aviation (CAP 1753) under applicable regulations. CAP 1753 is currently used to oversee the cyber security requirements in the following regulations:

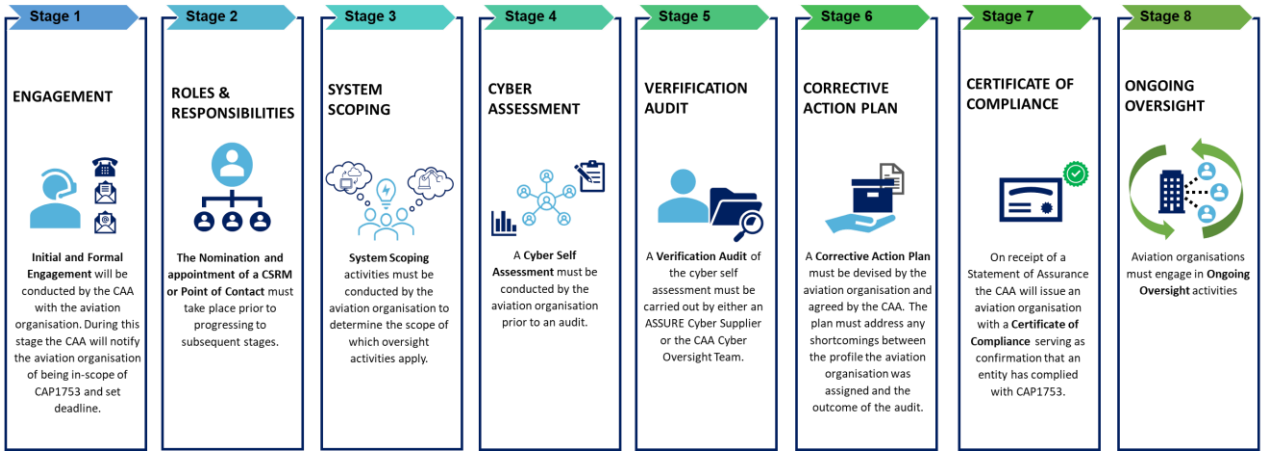
- Network and Information Systems (NIS) Regulations 2018
- National Aviation Security Programme (NASP)

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

4. Document Structure

The CAA is committed to ensuring CAP1753 remains an appropriate and proportionate model for the initial oversight of applicable cyber security regulatory requirements. Following engagement with the Cyber Security Industry Working Group (CSIWG) and key stakeholders, the CAA have revised the process to enable a more bespoke application across the different sub-sectors.

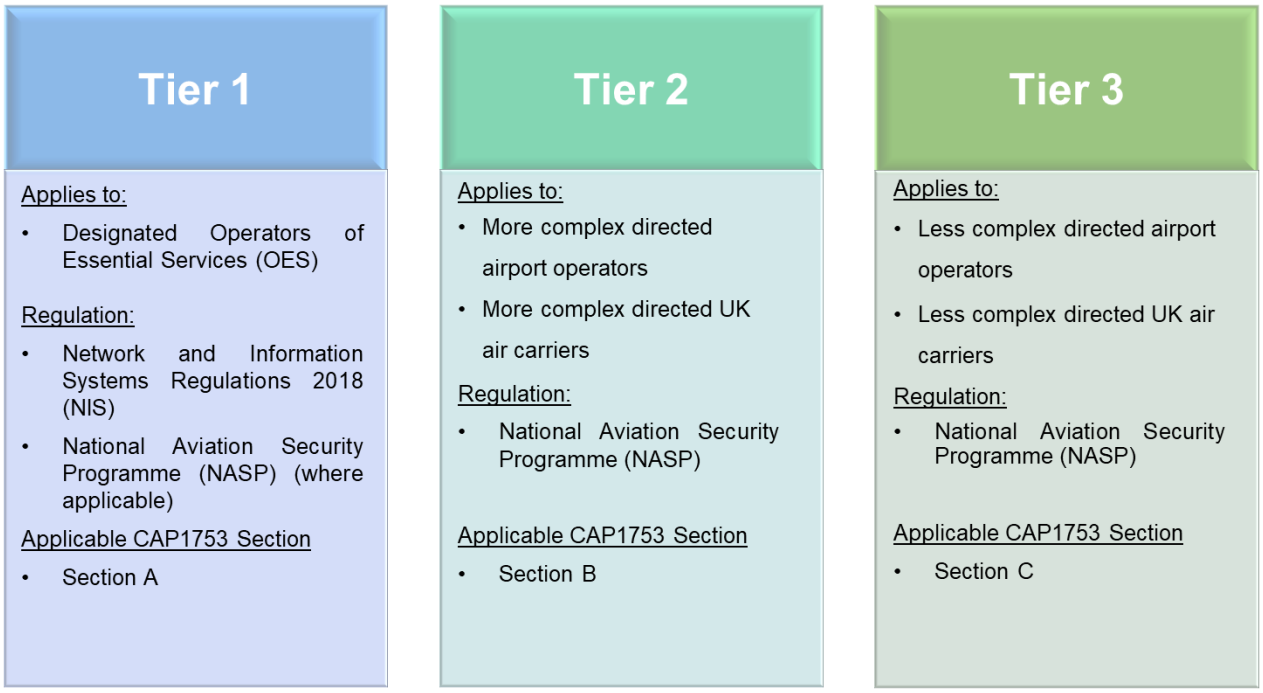
CAP1753 consists of three sections (A, B & C), which apply to the different tier of aviation organisation (e.g. a different size or type of aviation organisation). Each section contains requirements for progressing through the eight stages of CAP1753.



Please contact cyber@caa.co.uk should you have any questions about this process.

5. Profiles

Each aviation organisation will be assigned a profile at Stage 1 – Engagement. The CAA, in conjunction with the National Cyber Security Centre (NCSC), has developed a series of profiles that define the objectives aviation organisations are expected to meet. The three profiles are:



These profiles have been informed by sector and national assessments of risk, minimum regulatory requirements and the capabilities demonstrated by threat actors likely to target aviation organisations.

An aviation organisation's complexity is assessed using complexity matrices that are in standard widespread use within the CAA. A number of metrics are captured about an aviation organisation – the nature of its operation, and the size and scale of its operation, for example. These metrics are combined to form an overall measure of the aviation organisation's complexity.

6. Notification of Change

Aviation organisations in scope of CAP1753 must inform the CAA Cyber Security Oversight Team of changes to any of the elements below:

- Responsible persons;
- System scope;
- Cyber security controls that might affect the audit result for that particular indicator of good practice, contributing outcome, principle, or objective; or
- Corrective action plan, including any changes to the corrective actions themselves, or the implementation timescale.

This must be within 30 days of the change and accompanied by the relevant documents.

The CAA's Cyber Security Oversight team may, after assessment, determine that an audit is required.

7. Additional NASP requirements

Aviation organisations should note there are cyber security requirements within the National Aviation Security Programme, which are outside the scope of the 8 stages of cyber security oversight detailed in this document. Guidance on these additional requirements can be found in the FAQs accompanying the UK's Single Consolidated Direction.

These additional requirements will be assessed by either the CAA Aviation Security Compliance team or the CAA's Cyber Oversight team during routine compliance inspections and audits.

Section A – Tier 1 - Operators of Essential Services under the Network and Information Systems Regulations

Stage 1 – Engagement

- The CAA will issue a formal notification letter via email to the aviation organisation's Accountable Manager detailing the expectations for achieving compliance with CAP 1753.

Stage 2 – Nomination of Cyber Security Responsible Manager

- The aviation organisation's Accountable Manager must nominate a Cyber Security Responsible Manger to act as point of contact for cyber security matters.
- A CSRM Nomination Form must be completed and sent to cyber@caa.co.uk.

Stage 3 – System Scoping

- The aviation organisation shall conduct a scoping exercise, in accordance with CAP1849 - Cyber Security Critical Systems Scoping Guidance to determine which systems must be included in stages 4,5 and 6.
- Systems that must be included in the scope are those which a loss of confidentiality, integrity or availability could result in the inability to deliver the essential service or essential functions. It may include systems and services operated on behalf of the aviation organisation by third party suppliers.
- Once the aviation organisation has completed the systems scoping exercise, the completed scoping template (issued at Stage 1) shall be returned to the CAA's Cyber Security Oversight team before proceeding further. The Cyber Security Oversight team will review the scope and revert to the aviation organisation with comments, if required.

Stage 4 – Cyber Self-Assessment

- The Cyber Assessment Framework (CAF) for Aviation has been designed to provide an outcome-focused assessment against fourteen principles across four broad objectives.
- The aviation organisation must complete all required fields including references to evidence and details of any alternative methods of achieving the contributing outcomes, for each of its identified systems that are in scope of this process.
- Once completed, the CAF for Aviation shall be returned to the CAA via an encrypted USB flash drive (supplied by the CAA), or via other method(s) agreed between the CAA and the aviation organisation. The cyber team will assess the return to ensure it is ready to progress to the next stage.

Stage 5 – Verification Audit

- The aviation organisation shall submit to and procure an ASSURE cyber audit. Under exceptional circumstances, the CAA's Cyber Security Oversight team may undertake an audit instead of, or in addition to, an ASSURE cyber audit.
- The audit will be undertaken initially and subsequently at further intervals, as specified by the CAA. Any significant changes to the scope of systems and/or the corrective action plan may trigger an interim audit.
- Aviation organisations shall ensure that any relevant persons are available for the audit, and that any relevant information is readily provided.

Stage 6 – Corrective Action Plan

- The aviation organisation shall develop a corrective action plan to address any shortcomings between the assigned profile and the outcome of the audit.
- The corrective action plan must be detailed in the relevant part of the CAF for Aviation. Corrective action plans not received in this format may be rejected.
- The CAA's Cyber Security Oversight team will assess the corrective action plan and revert to the regulated entity within 60 days.
- Any change to the corrective action plan or timescales must be notified to the CAA's Cyber Security Oversight team within 30 days of the change.

Stage 7 – Certificate of Compliance

- Once the corrective action plan has been agreed, the aviation organisation must submit a signed Statement of Assurance declaration.
- The documents shall be submitted to cyber@caa.co.uk.
- On completion of Stages 1 – 7 the CAA will issue the aviation organisations with a Cyber Security Certificate of Compliance.

Stage 8 – Ongoing Oversight

- Until all corrective actions are completed, the aviation organisation shall present, in a format to be agreed by the CAA, quarterly updates regarding the progress against its corrective action plan to its assigned CAA Oversight Specialist.

- The CAA's Cyber Security Oversight team will monitor the progress of corrective actions. This activity may be announced or unannounced.

- The CAA's Cyber Security Oversight team may undertake additional audits at any time. This activity may be announced or unannounced.

Section B – Tier 2 - Directed UK Aerodromes and Directed UK Air Carriers

Stage 1 – Engagement

- The CAA will issue a formal notification letter via email to the aviation organisation's Accountable Manager and Security Manager detailing the expectations for achieving compliance with CAP 1753.

Stage 2 – Nomination of Cyber Key Roles

- The Accountable Manager is accountable for ensuring compliance with all applicable regulations.
- The Security Manager has responsibility for ensuring compliance with the NASP, including the cyber security requirements.
- The Security Manager may delegate responsibility for cyber security matters to a Cyber Security Responsible Manager (CSRM), who should be a suitably qualified or experienced individual within the aviation organisation.
- If the responsibility is delegated, the Security Manager shall ensure the delegation is detailed in the aviation organisation's security programme.
- A CSRM nomination form must be completed and sent to cyber@caa.co.uk.

Stage 3 – System Scoping

- The aviation organisation shall conduct a scoping exercise to determine which systems must be included in stages 4, 5, and 6.
- Systems that must be included in the scope are any that may affect the security of civil aviation operations. In particular, but not exclusively, that includes those systems used to help deliver a mandatory function under the NASP. The scope must include all systems and services operated on behalf of the aviation organisation by any third-party suppliers.
- To ensure the scope is accurate and includes all relevant systems CAP 1849 must be used as the basis for the scope. CAP 1849 defines mandatory functions, however is not exhaustive. Any technology-based system that is used to help deliver, support and/or impact the security of civil aviation operations must be included in the scope.
- The Cyber Oversight team will review the scope and revert to the aviation organisation with comments, if required.

Stage 4 – Cyber Self-Assessment

- The CAF for Aviation has been designed to provide an outcome-focused assessment against fourteen principles across four broad objectives.
- The aviation organisation must complete all required fields including references to evidence for each of its systems that are in scope of this process.
- Once completed, the CAF for Aviation shall be returned to cyber@caa.co.uk. The Cyber Security Oversight team will assess the return to ensure it is ready to progress to the next stage.

Stage 5 – Verification Audit

- The aviation organisation shall submit to and procure an ASSURE cyber audit. Under exceptional circumstances, the CAA's Cyber Oversight team may undertake an audit instead of, or additionally to, an ASSURE cyber audit.
- The audit will be undertaken initially and subsequently at further intervals, as specified by the CAA. Any significant changes to the scope of systems and/or the corrective action plan may trigger an interim audit.
- The aviation organisation shall ensure that any relevant persons are available for the audit, and that any relevant information is readily provided.

Stage 6 – Corrective Action Plan

- The aviation organisation shall develop a corrective action plan to address any shortcomings between the Tier 2 CAF profile and the outcome of the audit.
- The corrective action plan must be detailed in the relevant part of the CAF for Aviation. Corrective action plans not received in this format will be rejected.
- The CAA's Oversight Specialist will assess the corrective action plan and revert to the aviation organisation within 60 days.
- Any change to the corrective action plan or timescales must be notified to the CAA's Cyber Oversight team within 30 days of the change.

Stage 7 – Certificate of Compliance

- Once the corrective action plan has been agreed, the regulated entity will submit an updated and signed security programme that references the CAF for Aviation. The security programme must detail any procedures the aviation organisation has implemented to ensure the tool is reviewed at regular intervals.
- The documents shall be submitted to cyber@caa.co.uk.
- On completion of Stages 1 – 7, the CAA will issue the aviation organisation with a Cyber Security Certificate of Compliance.

Stage 8 – Ongoing Oversight

- Until all corrective actions are complete, the aviation organisation shall provide its Oversight Specialist with quarterly updates regarding the progress against its corrective action plan. Progress should be detailed on the original corrective action plan.
- The CAA's Cyber Oversight team will monitor the progress of corrective actions. This activity may be announced or unannounced.
- The CAA's Cyber Oversight team may undertake additional audits at any time. This activity may be announced or unannounced.

Section C – Tier 3 - Directed UK Aerodromes and Directed UK Air Carriers

Stage 1 – Engagement

- The CAA will issue a formal notification letter via email to the aviation organisation's Accountable Manager and Security Manager detailing the expectations for achieving compliance with CAP 1753.

Stage 2 – Nomination of Cyber Key Roles

- The Accountable Manager is accountable for ensuring compliance with all applicable regulations.
- The Security Manager has responsibility for ensuring compliance with the NASP, including the cyber security requirements.
- The Security Manager may delegate responsibility for cyber security matters to a Cyber Security Responsible Manager (CSRM), who should be a suitably qualified or experienced individual within the aviation organisation.
- If the responsibility is delegated, the Security Manager shall ensure the delegation is detailed in the aviation organisation's security programme.
- A CSRM nomination form must be completed and sent to cyber@caa.co.uk

Stage 3 – Systems Scoping

- The aviation organisation shall conduct a scoping exercise to determine which systems must be included in stages 4,5 and 6. Systems that must be included in the scope are any that may affect the security of civil aviation operations. In particular, but not exclusively, that includes those systems used to help deliver a mandatory function under the NASP. The scope may include systems and services operated on behalf of the aviation organisation by third party suppliers.
- To ensure the scope is accurate and includes all relevant systems CAP 1849 must be used as the basis for the scope. CAP 1849 defines mandatory functions, however is not exhaustive. Any technology-based system that is used to help deliver, support and/or impact the security of civil aviation operations must be included in the scope.
- The Cyber Oversight team will review the scope and revert to the aviation organisation with comments, if required.

Stage 4 – Cyber Assessment

- The Tier 3 Cyber Assessment Tool has been developed by the CAA and NCSC, and designed to provide a proportional, scalable, and consistent assessment of the cyber controls applied by the aviation organisation. It is controls-focussed rather than outcome-focused and is intended to be more suitable for smaller, less complex aviation organisations.
- If an aviation organisation wishes to complete the CAF for Aviation instead of the Tier 3 Cyber Assessment Tool, we will accommodate that.
- The aviation organisation will conduct an assessment of the systems it identified, by completing the Tier 3 tool or CAF for Aviation.
- The aviation organisation must complete all required fields including references to evidence for each of its systems that are in scope of this process.
- Once completed, the Tier 3 Cyber Assessment Tool or CAF for Aviation shall be returned to cyber@caa.co.uk. The cyber team will assess the return to ensure it is ready to progress to the next stage.

Stage 5 – Verification Audit

- The aviation organisation shall submit to a cyber audit undertaken by the CAA's Cyber Oversight team.
- This audit will be undertaken initially and subsequently at further intervals, as specified by the CAA. Any significant changes to the scope of the system and/or the corrective action plan may trigger an interim audit.
- The aviation organisation shall ensure that any relevant persons are available for the audit, and that any relevant information is readily provided.

Stage 6 – Corrective Action Plan

- The aviation organisation shall develop a corrective action plan to address any shortcomings between the Tier 3 profile and the outcome of the audit.
- The corrective action plan must be detailed in the relevant parts of the Tier 3 Cyber Assessment Tool. Corrective action plans not received in this format will be rejected.
- The CAA Oversight Specialist will assess the corrective action plan and revert to the regulated entity within 60 days.
- Any change to the corrective action plan or timescales must be notified to the CAA's Cyber Oversight team within 30 days of the change.

Stage 7 – Security Programme and Certificate of Compliance

- Once the corrective action plan has been agreed, the regulated entity will submit an updated and signed security programme that references the Cyber Assessment Tool. The security programme must detail any procedures the aviation organisation has implemented to ensure the tool is reviewed at regular intervals.
- The documents shall be submitted to cyber@caa.co.uk.
- On completion of Stages 1 – 7, the CAA will issue the aviation entity with a Cyber Security Certificate of Compliance.

Stage 8 – Ongoing Oversight

- Until all corrective actions are complete, the aviation organisation shall provide its Oversight Specialist with quarterly updates regarding the progress against its corrective action plan. Progress should be detailed on the original corrective action plan.
- The CAA's Cyber Oversight team will monitor the corrective actions. This activity may be announced or unannounced.
- The CAA's Cyber Oversight team may undertake additional audits at any time. This activity may be announced or unannounced.