UK Civil Aviation Authority

CAA Cyber Security Oversight Strategy 2024-26

CAP 2976

Published by the Civil Aviation Authority, 2024

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

First published 2024

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

Contents

Contents 3
1. Foreword 4
2. Purpose 5
3. Introduction 5
4. Scope 6
5. Roles 7
6. Regulatory Process 8
7. Cyber Oversight Process and CAP1753 10
8. Incident Response and Investigation 12
Appendix A. CAA Cyber Security Strategy on a page 13

1. Foreword

The UK's Aviation system is a vital part of Critical National Infrastructure and underpins the UK's connectivity, both domestically and internationally. System resilience and maintaining the very highest standards of safety and security performance are essential, given the backdrop of geo-political issues and the current national threat level in the UK[1].

Innovation and new technology provide both opportunities for improvement, but also present a complex set of challenges which require careful consideration and detailed risk assessment.

In this current environment there is a continued threat from hackers, ideologists and State actors who are developing their capabilities and targeting organisations for their own malevolent purposes; both public and private sector organisations must therefore continue to invest and continue to take preventative action.

A successful attack could result in a range of serious outcomes, which at the very least could amount to significant consumer disruption and financial terrorism.

With an industry that is so diverse, the challenge can often be about determining the level of security maturity required to proportionately address the risk that is posed. There is no doubt that the frameworks developed over recent years have helped progress the approach to such challenges, with information and knowledge sharing across the sector now materially helping improve the efficacy of the UK Aviation System barriers holistically.

Other key areas of focus have been supplier oversight and establishing crisis response plans to ensure robust recovery in the case of events.

Every organisation must play its part and the CAA, in line with our Mission of Protecting People and Enabling Aerospace, has a leading role in developing the capability and health of the UK Aviation System in order to minimise the threat posed by cyber crime.

Rob Bishton, CEO UK Civil Aviation Authority

[1] Threat Levels | MI5 - The Security Service

2. Purpose

To describe the role of CAA Cyber Security, providing clarity for industry to underpin our regulatory role in both security and safety requirements.

To ensure that appropriate urgency is taken with cyber security regulations to enable the UK aviation system to operate securely with resilience in an ever - changing cyber threat landscape.

Vision

An aviation & aerospace system that is resilient to Cyber Threats.

Mission

Ensure UK aviation & aerospace takes an effective approach in the management of cyber security risks in order to continuously improve safety, security and resilience outcomes for the UK aviation & aerospace system.

3. 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.

The CAA's cyber security oversight strategy must be reviewed regularly in order to keep pace with these ever-changing cyber security trends and to ensure that the roles of the National Cyber Security Centre (NCSC), industry and of the CAA are clear.

The industry must effectively protect Confidentiality, Integrity and Availability against various threats:

Figure 1, CIA and threats.

Examples of issue types are:

- **Confidentiality** – where a cyber related incident has resulted in unauthorised access to personal identifiable information (PII) or company data
- **Integrity** – where the safeguarding of the accuracy and completeness of safety and/or security critical information has been compromised, leading to unauthorised alteration of information
- **Availability** – where a cyber related incident has resulted in the inability to access a service, during circumstances such as a Distributed Denial of Service (DDoS) attack

4. Scope

All aviation organisations that have regulatory cyber security obligations to comply with existing safety, security, and resilience requirements may be in scope of CAA cyber security oversight.

Existing regulations applicable to aviation organisations CAA Cyber Security Oversight, 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) Regulations
- National Aviation Security Programme (NASP)

The CAA recommends that, regardless of the level of regulatory involvement, aviation organisations proactively apply appropriate and proportionate cyber security measures in their operations.

Protection needs to apply to all levels of the complex eco-system that makes up the UK's aviation system, including airports, air operators, air navigation service providers and suppliers and supply chain partners throughout the system.

The CAA Cyber Security Strategy must also be in alignment with the National Cyber Strategy 2022[2], the DfTs Cyber Security Strategic pillars of Understand, Build and Strengthen, and sets out to build the foundations detailed within a secure and resilient UK Aviation sector.

[2] Government Cyber Security Strategy 2022–2030 (publishing.service.gov.uk)

5. Roles

Aviation & Aerospace Entity

Organisations are accountable for assuring all aspects of their cyber security are maintained, including focusing on enhancing systems security, implementing robust network access controls, prioritising employee cyber security training and collaborating with industry to ensure robust resilience plans are in place to maintain operations.

Entities that are designated as Operators of Essential Service or Critical National Infrastructure are expected to exhibit positive indicators across all NCSC Cyber Assessment Framework[3] (CAF) objectives and evidence an enhanced cyber security posture.

Department for Transport

The Department for Transport (DfT) are responsible for setting the strategic direction of cyber security policy and regulation across transport, including Aviation. In relation to Networks and Information Systems (NIS)[4], 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.

Aside from regulation, DfT have a role working with the aviation sector to drive good cyber outcomes including a portfolio of strategic national projects to enhance safety & security and to improve the UK's infrastructure services.

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.

Civil Aviation Authority

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 and are also responsible for Cyber Security Oversight for organisations directed under the National Aviation Security Programme (NASP).

[3] NCSC CAF guidance - NCSC.GOV.UK

[4] The NIS Regulations 2018 - GOV.UK (www.gov.uk)

The CAA Cyber Security Oversight Team is responsible for all cyber security regulatory activity within any of the CAA regulatory domains and is the first point of contact at the CAA for all questions and issues relating to the cyber security oversight process for aviation.

6. Regulatory Process

Vision

An aviation & aerospace system that is resilient to Cyber Threats.

Mission

Ensure UK aviation & aerospace takes an effective approach in the management of cyber security risks in order to continuously improve safety, security and resilience outcomes for the UK aviation & aerospace system.

Behind the vision and mission are the following activities.

What we do

- **Deliver regulatory oversight** – we will work with Cyber Security Responsible Manager contacts to ensure effective management of corrective actions and that an effective cyber security regime is in place.

- **Lead on Cyber assurance of eco-system** – we will use our expertise to determine effective ways to provide assurance of aviation eco-system so that industry can effectively manage their supply chains.

- **Develop sector specific mitigation strategies** - we will use our industry expertise to identify common risk themes and mitigation approaches for industry to implement against the evolving threats.

- **Influence policy and regulation** – we will work with Government departments and international organisations to ensure effective & proportionate cyber security regulation in the UK and internationally.

- **Enforcement action for non-compliance** – where necessary we will use powers to ensure the appropriate security standards are met, recommending that DfT execute for NIS entities.

Why

- **Greater visibility of industry threats** – by achieving this we can effectively determine the industry threat profile.

- **To influence improved standards in UK aviation & aerospace** – bringing up cyber security standards across the UK aviation & aerospace system and protecting essential services.

- **Stronger support for UK aviation & aerospace** – providing the right support and intervention at the right time.

- **Collaborative approach to resilience** – to enable UK aviation to systematically defend as one and share lessons learned and best practice.

- **Protect critical national infrastructure (CNI)** – by ensuring security ambitions for increased resilience of the UK's CNI entities are met to keep the UK moving and open for business.

Industry role

- **Effective incident reporting** – by reporting the incidents that occur entities can help industry prepare and protect at system level and identify lessons learned to improve operational resilience.

- **Enhance cyber capabilities** – by identifying and then focusing on the right areas, entities can achieve the best technical and people capabilities & capabilities to protect against threats.

- **Manage organisation supply chain** – by mapping and assessing supply chains to ensure a clear understanding of the risks that exist within that eco-system.

- **Exercise resilience plans**– to maintain and exercise the resilience plans that are established through cyber maturity, improving plans with any lessons learned.

- **Collaborate on risk and threats** – to create a shared approach to system resilience, creating an industry that does not compete on cyber security.

The CAA Aviation & aerospace Cyber Security Oversight Strategy on a page is depicted in Appendix A.

7. Cyber Oversight Process and CAP1753

The CAA's Initial Oversight process is defined by CAP1753[5]. The CAA is committed to ensuring that CAP1753 remains an appropriate and proportionate model for the initial oversight of some of the cyber security regulatory requirements within aviation.

Following engagement with industry via the Cyber Security Industry Working Group (CSIWG) and key stakeholders, the CAA has revised the process to enable a more bespoke application across different sub-sectors. Consequently our CAP1753 oversight process has been amended to cater for different sizes or types of aviation organisation.

The CAP1753 process is based on the CAF and assesses four key objectives for Cyber Security:

Objective A - Managing security risk

Objective B - Protecting against cyber attack

Objective C - Detecting cyber security incidents

Objective D - Minimising the impact of cyber security incidents

Once organisations have completed the CAP1753 process and submitted a completed CAF to achieve a Certificate of Compliance, the CAA's Cyber Security Oversight specialists will work with the Cyber Security Responsible Manager to ensure focus continues in the area of Cyber Security and progression of identified corrective actions

The CAA Cyber Oversight Process and CAP1753 is depicted by figure 2.

[5] The Cyber Security Oversight Process for Aviation (caa.co.uk)

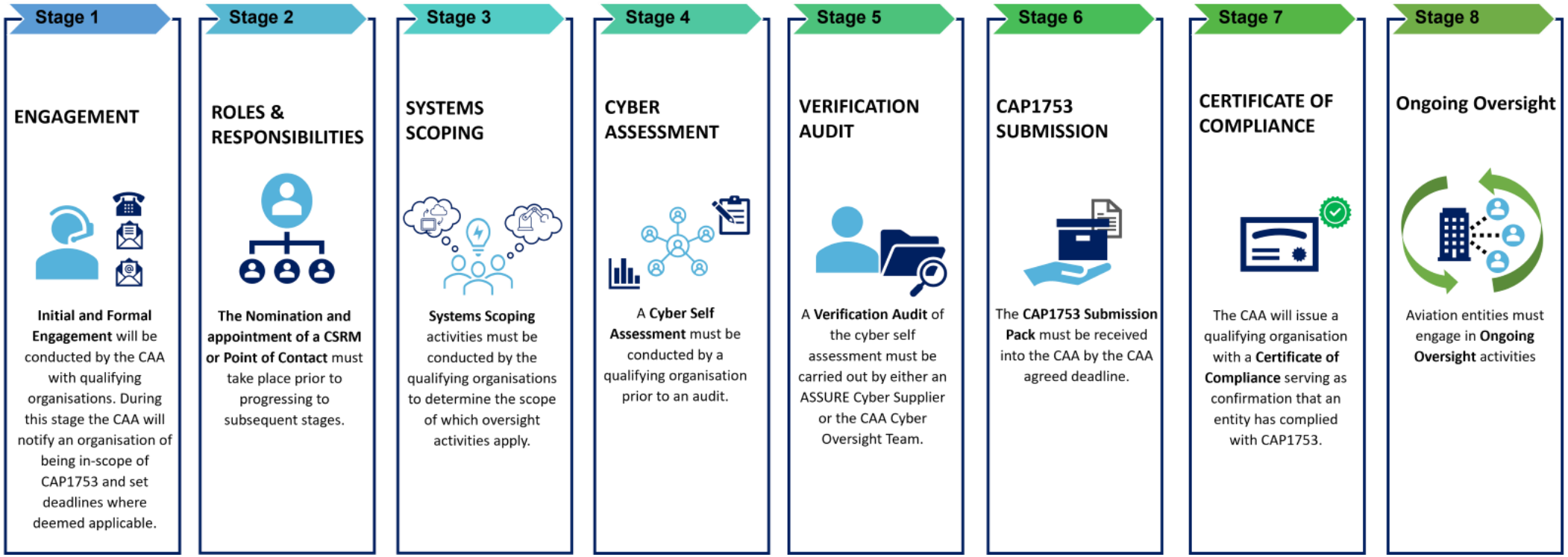

Figure 2, the CAA Oversight Process, CAP1753.

8. Incident Response and Investigation

The role of the CAA in an industry Cyber Security event:

- First and foremost, organisations should invoke their own Cyber Incident Response Plans and register the incident via the NCSC incident report service
- For Operators of Essential Service, reporting obligations as defined by the NIS regulation should be completed
- The Cyber Team will support these efforts by signposting agencies such as NCSC or DfT for reporting NIS incidents as a first port of call
- The Team will also be on hand for affected entities to raise any queries or request support for specific aspects of the event; essentially the team will support the organisation's own Cyber response plans and offer any advice or expertise as required
- The Cyber Team have established a Cyber Incident Panel (CIP) to address the difficulties in managing the flow of information and to ensure the relevant stakeholders have the most accurate and up to date information about future cyber incidents
- When convened, this group will perform a coordinative function to ensure consistent understanding of events, primarily this focuses on CAA capability teams
- This conduit role is critical to ensure that CAA colleagues may intervene and make the necessary regulatory interventions should there be any risks to safety or security
- In addition, the team will look to verify rumours and information received, and aim to share any information on the event, as appropriate, with other aviation entities
- This can be particularly valuable in circumstances where a compromise has occurred in an organisation that is part of the supply chain for UK Aviation, particularly where that organisation works with multiple aviation entities

Appendix A. CAA Cyber Security Strategy on a page

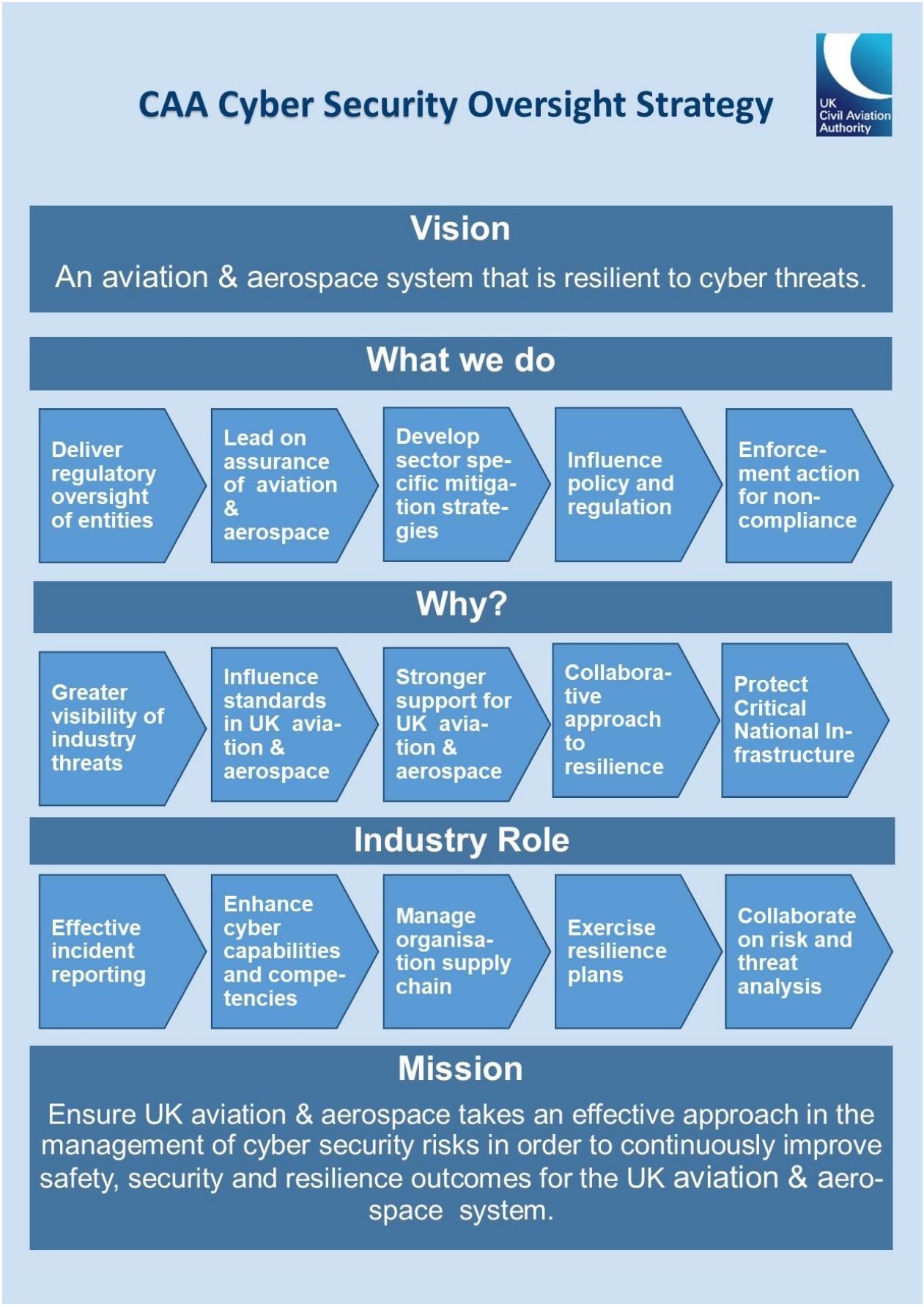

Figure 3, CAA Cyber Security Oversight Strategy on a page.