

Cyber Assessment Framework (CAF) for Aviation Guidance

CAP1850

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

Second publication – 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

Contents

Contents	3
1. Introduction	4
1.1. Supporting Documentation	4
2. Background	5
2.1. CAF for Aviation Overview	5
2.2. Important Notes	6
3. Completing the CAF for Aviation	7
3.1. Document Control	7
3.2. Summary (Aviation Organisation)	7
3.3. Summary (ASSURE Cyber Audit)	8
3.4. Audit Report – Appendix B	8
4. Assessment – System (1 – 25)	9
4.1. Indicators of Good Practice (IGP)	9
4.2. Alternative Methods	10
4.3. Self-Assessment Results	11
4.3.1. ASSURE Cyber Audit Assessment	12
4.4. Aviation Organisation Justification and Further Comments	13
4.4.1. ASSURE Supplier Justification and Further Comments	13
4.5. Aviation Organisation - Evidence Tracker	14
4.5.1. ASSURE Cyber Supplier – Evidence Tracker	14
5. Corrective Action Plan	15
5.1. Cyber Risk assessment	16
6. Statement of Assurance	17
6.1. Sharing Information Securely with the CAA	17
Annex B – Informative References and Example Evidence	18

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.

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.”

This document provides guidance on how to complete the Cyber Assessment Framework (CAF) for Aviation and Statement of Assurance.

1.1.Supporting Documentation

CAP1753 – Cyber Security Oversight Process for Aviation¹

CAP1849 – Cyber Security Critical System Scoping Guidance²

Cyber Security Critical System Scoping Template³

Cyber Assessment Framework (CAF) for Aviation³

¹ www.caa.co.uk/CAP1753

² www.caa.co.uk/CAP1849

³ <https://www.caa.co.uk/Commercial-industry/Cyber-security-oversight/Cyber-security-compliance/>

2. Background

Working closely with the Department for Transport (DfT) and the National Cyber Security Centre (NCSC) the CAA has developed the CAF for Aviation. The CAF for Aviation has been adapted from the NCSC core CAF v3.0 and designed specifically for aviation.

The NCSC core CAF v3.0⁴, and by association the CAA CAF for Aviation has been developed to meet the following set of requirements:

- Provide a suitable framework to assist in carrying out cyber resilience assessments;
- maintain the outcome-focused approach of the NCSC cyber security and resilience principles and discourage assessments being carried out as tick-box exercises;
- be compatible with the use of appropriate existing cyber security guidance and standards;
- enable the identification of effective cyber security and resilience improvement activities;
- be extensible to accommodate sector-specific elements as may be required;
- enable the setting of meaningful target security levels for organisations to achieve, possibly reflecting a regulator view of appropriate and proportionate security; and
- be as straightforward and cost-effective to apply as possible.

2.1. CAF for Aviation Overview

The CAF for Aviation has been designed to provide an outcome-focused assessment against fourteen Principles across four broad Objectives. The Principles are further broken down into thirty-nine Contributing Outcomes. Each outcome is associated with a set of Indicators of Good Practice (IGPs) which are broken down into the following three categories:

- The **'Achieved'** column of an IGP table defines the typical characteristics of an organisation fully achieving that outcome. It is intended that all the indicators would be present to support an assessment of 'Achieved';
- the **'Not Achieved'** column of an IGP table defines the typical characteristics of an organisation not achieving that outcome. It is intended that the presence of any one indicator would lead to an assessment of 'Not Achieved'; and
- when present, the **'Partially Achieved'** column of an IGP table defines the typical characteristics of an organisation partially achieving that outcome.

⁴ <https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework>

The result of applying the CAF for Aviation is thirty-nine individual assessments, each one derived from making a judgement on the extent to which a set of IGPs reflects the circumstances of the aviation organisation being assessed. The CAF for Aviation has been designed in such a way that a result in which all thirty-nine Contributing Outcomes were assessed as 'Achieved' would indicate a level of cyber security some way beyond the minimum 'basic cyber hygiene' level.

Assessment of Contributing Outcomes is primarily a matter of expert judgement and the IGP tables do not remove the requirement for the informed use of cyber security expertise and sector knowledge. The ASSURE Cyber Audit will be conducted against the completed CAF for Aviation. The CAA Cyber Security Oversight Team will use the outcome to consider an organisation's cyber security posture alongside the context of the sector and any additional relevant factors.

2.2. Important Notes

When completing the CAF for Aviation, aviation organisations should bear in mind the following:

- The CAF for Aviation is not intended to be exhaustive and is not in itself an indicator of compliance (see Step 6 of CAP1753).
- The CAF for Aviation is not intended to be inflexible, rule-based or applied as a checklist. The CAA appreciate that where an Indicator of Good Practice is not being met, an aviation organisation may be implementing alternative controls or methods which meet the Contributing Outcome.
- The CAA does not expect every aviation organisation to score 'Achieved' for each Contributing Outcome. The CAA will issue an aviation organisation with an expected profile (see Steps 1 and 3 of CAP1753).
- An aviation organisation is expected to produce suitable evidence (see Annex B – Informative References and Example Evidence) for the ASSURE Cyber Audit.

3. Completing the CAF for Aviation

The CAF for Aviation consists of several key tabs named:

- Document Control;
- Summary (Aviation Organisation);
- Summary (ASSURE Cyber Audit);
- Audit Report – Appendix B
- Corrective Action Plan
- Statement of Assurance data; and
- Assessment – System (1-25).

All tabs should be filled in by using the provided drop-down options (where applicable) and free text boxes by either the aviation organisation or ASSURE Cyber Professional.

3.1.Document Control

This tab contains information including; version number, background information and links to referenced guidance.

3.2.Summary (Aviation Organisation)

The “Summary (Aviation Organisation)” tab provides the aviation organisation with a summary view of their position against each of the Contributing Outcomes. Largely, this tab requires no input from the aviation organisation except to populate the “Organisation Information” table shown below.

Organisation Information	
Aviation Organisation:	
Cyber Security Responsible Manager:	
Number of Critical Systems:	1

Figure 2 – Summary (Aviation Organisation)

Note: All graphs and systems cells on the summary tab will auto populate throughout the completion of each “Assessment” tab.

3.3. Summary (ASSURE Cyber Audit)

The “Summary (ASSURE Cyber Audit)” tab provides a summary view of the ASSURE Cyber Supplier’s validated opinion of an aviation organisation’s position against each of the Contributing Outcomes, following the evidential audit. Largely, this tab requires no input from the ASSURE Cyber Supplier except to populate the “ASSURE Cyber Supplier Information” table shown below, however please note that the ‘Number of Critical Systems’ field will auto populate.

When completing the names of the ASSURE Cyber Professional’s this should include reference to their ASSURE specialism/s held.

ASSURE Cyber Supplier Information	
Selected ASSURE Cyber Supplier:	
ASSURE Cyber Professional:	
ASSURE Cyber Professional:	
ASSURE Cyber Professional:	
Number of Critical Systems:	1

Figure 3 – Summary (ASSURE Cyber Audit)

Note: All graphs and systems cells on the summary tab will auto populate throughout the completion of each “Assessment” tab.

3.4. Audit Report – Appendix B

This table can be used by the ASSURE Cyber Supplier to populate APPENDIX B of the ASSURE Cyber Audit report. There is no requirement for manual entry on this tab.

4. Assessment – System (1 – 25)

The assessment tabs should be used by an aviation organisation to complete a self-assessment against each of the Contributing Outcomes for each of the identified critical systems⁵.

Following this the ASSURE Cyber Supplier will complete the ASSURE Cyber Audit section against each of the Contributing Outcomes for each of the system assessment tabs.

The CAA has generated 25 separate system assessment tabs, if additional tabs are required please use a second CAF for Aviation workbook. Where some tabs are **not required please leave these blank**, if deleted the graphs will not populate accurately. The summary tab will simply show these as “not yet assessed”.

Note: Where Contributing Outcomes are generally “organisational” (e.g. A1. Board Direction) these must be completed in full on the first Assessment tab. Subsequent Assessment tabs should have the “result” indicated against the Contributing Outcome with a note in the Justification that the assessment is organisational and to refer to Assessment tab - System 1.

Note: Where it is found that multiple critical systems meet the same Contributing Outcomes and IGPs it is advised that they are grouped within the CAF for Aviation, in line with the Critical Systems Scoping Guidance and Template, to avoid duplicating the assessment.

4.1. Indicators of Good Practice (IGP)

Aviation organisations are required to use the IGPs to assess their essential functions and critical systems against each Contributing Outcome.

To indicate where IGPs are being met the aviation organisation is to mark the appropriate IGP with an X:

Guidance notes on determining the Contributing Outcome self-assessment result:				Aviation Organisation	
Achieved = All IGP statements in “Achieved” is true. Not Achieved = At least one of the “Not Achieved” IGP statements is true Partially Achieved = All of the “Partially Achieved” IGP statements are true				All below sections to be completed by the aviation organisation	
Please note that alternative methods for achieving a Contributing Outcome, not covered by the suggested IGPs, are acceptable. Evidence to support these methods must be considered by the ASSURE Cyber Professionals during the audit. Please document these methods in the alternative methods section.				Self - Assessment Result	IGP Selection (enter X to mark the applicable)
				Not yet assessed	Justification and Further Comments
Principle A1 - Governance: The organisation has appropriate management policies and processes in place to govern its approach to the security of critical systems.					
Contributing Outcome: A1.a Board Direction - You have effective organisational security management led at board level and articulated clearly in corresponding policies.					
Achieved					
A1.a.1: Your organisation's approach and policy relating to the security of critical systems are owned and managed at board level. These are communicated, in a meaningful way, to risk management decision-makers across the organisation.					
A1.a.2: Regular board discussions on the security of critical systems take place, based on timely and accurate information and informed by expert guidance.					
A1.a.3: There is a board-level individual who has overall accountability for the security of critical systems and drives regular discussion at board-level. <i>CAA comment:</i> For aviation this board level individual will be the Accountable Manager.					
A1.a.4: Direction set at board level is translated into effective organisational practices that direct and control the security of the critical systems supporting your essential functions.					

⁵ www.caa.co.uk/CAP1849