

Cyber Security Critical Systems Scoping Guidance

CAP 1849

Published by the Civil Aviation Authority, August 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 at: www.caa.co.uk/CAP1849

Contents

Contents	3
Introduction	4
Supporting Documentation	4
Background	5
Aviation Essential Service and Functions	6
Critical System Scoping Method	7
Identifying Criticality	9
Completing the Critical Systems Scoping Template	10
Critical Systems Grouping	10
Critical Supplier List	10
Diagramming	11
Notification of Cyber Security Change	12
Annex A: Aviation Functions and Sub-Functions	13
Annex B: Example Critical Systems Diagrams	16

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.”

Supporting Documentation

CAP1753 – Cyber Security Oversight Process for Aviation

Cyber Security Critical System Scoping Template

Cyber Assessment Framework (CAF) for Aviation

CAP1850 – Cyber Assessment Framework (CAF) for Aviation Guidance

Background

This guidance is intended to assist aviation organisations in the identification and documentation of their critical network and information systems¹.

Network and Information Systems are defined as:

- a) an electronic communications network within the meaning of section 32(1) of the Communications Act 2003;
- b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or
- c) digital data stored, processed, retrieved or transmitted by elements covered under paragraph (a) or (b) for the purposes of their operation, use, protection and maintenance.

It is important to clearly identify and document your critical network and information systems to aid in applying comprehensive, appropriate and proportionate cyber security measures. This guidance document aims to provide a methodology for critical system identification that can be applied consistently to aviation organisations of varying types and scale.

When considering the scope of critical systems, the CAA expect an aviation organisation to make an informed and competent consideration of reasonable and expected impacts. The CAA does not expect an aviation organisation to consider implausible scenarios or highly complex chains of events or failures—a reasonable worst-case scenario should be used.

An aviation organisation is ultimately responsible for their own risks and the identification and validation of their critical system scope. To ensure that the scope is accurate and includes critical systems that would reasonably be considered in scope, an aviation organisation must be able to demonstrate that a logical method was followed and included all stakeholders deemed relevant by the organisation (e.g. workshops with supporting documentation, board level discussions and decisions, business impact assessments, etc).

¹ The Network and Information Systems Regulations 2018, SI 2018/506, Schedule 2 section 4
<https://www.legislation.gov.uk/ukxi/2018/506/made>

Aviation Essential Service and Functions

The Department for Transport (DfT) has identified the following key essential services and essential functions within aviation:

- Safe, secure and timely movement of passengers via aircraft and aerodrome² facilities.

Provision of this essential service³ in the air transport sector is achieved through the ownership/management of aerodromes, provision of air traffic services (en-route as well as at an airport) and the running of an air carrier⁴.

To aid in the identification of an aviation organisation's critical systems associated with the delivery of this essential service, it is recommended to break the high-level essential service into the functions which enable it. These functions can similarly be broken down further into sub-functions and so forth.

A non-exhaustive list of functions and sub-functions has been provided in **Annex A: Aviation Functions and Sub-Functions**. This should not be used as a check-list, but instead is provided to enable consistency and to assist in the initial functional decomposition of the essential service.

It is important to note that responsibility for functions and sub-functions may be shared across organisations. Aviation organisations should identify both their responsibility and their dependency on functions or sub-functions to which other organisations have responsibility. This identification may highlight previously unknown connections or interdependencies between systems.

Organisations should ensure that where responsibility is shared, all responsible parties are aware of that responsibility and that reasonable and proportionate measures are taken to manage risk to the shared function or sub-function.

² "Aerodrome" has the same meaning as in the Civil Aviation Act 1982.

<https://www.legislation.gov.uk/ukpga/1982/16/contents>

³ Where provision of this service reaches defined thresholds an aviation organisation will be in scope of The Network and Information Systems Regulations 2018, SI 2018/506, Schedule 2 section 4.

<https://www.legislation.gov.uk/uksi/2018/506/made>

⁴ "Air carrier" has the same meaning as in Article 3(4) of Regulation (EC) No 300/2008 of the European Parliament and the Council on common rules in the field of civil aviation security and repealing Regulation EC No 2320/2202.

<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:097:0072:0084:EN:PDF>