UK Civil Aviation Authority

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

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 Aviation[1]

CAP1849 – Cyber Security Critical System Scoping Guidance[2]

Cyber Security Critical System Scoping Template[3]

Cyber Assessment Framework (CAF) for Aviation[3]

[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 v3.0[4], 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 again 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 Suplier:	
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 systems[5].

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".

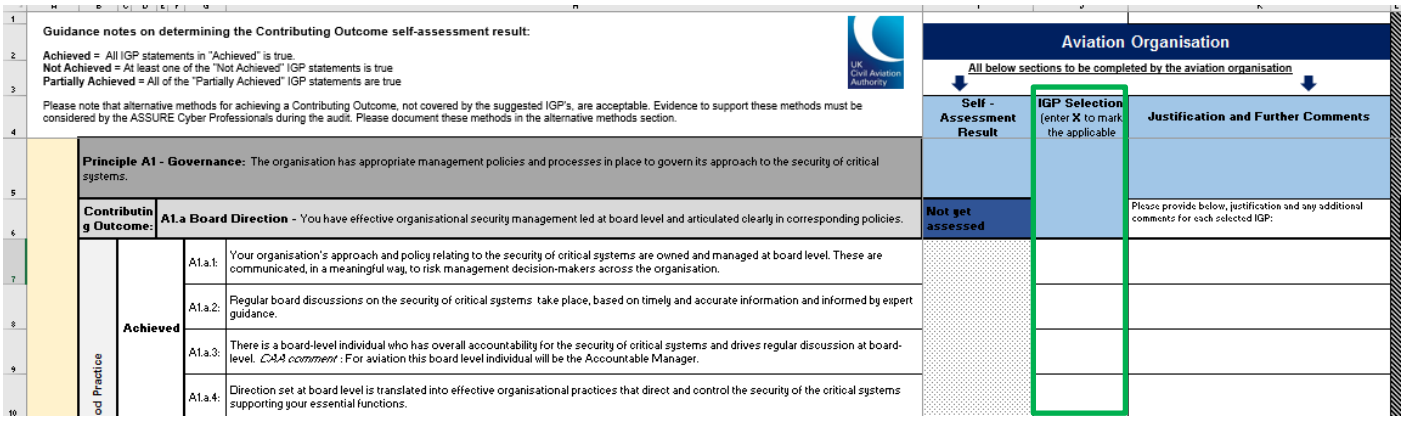
Note: Where Contributing Outcomes are generally "organisational" (e.g. A1. Board Direction) these must be completed in full on the first Assessment tab. Subsequent Assessment tabs should have the "result" indicated against the Contributing Outcome with a note in the Justification that the assessment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

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

Please note that alternative methods for achieving a Contributing Outcome, not covered by the suggested IGP's, 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.

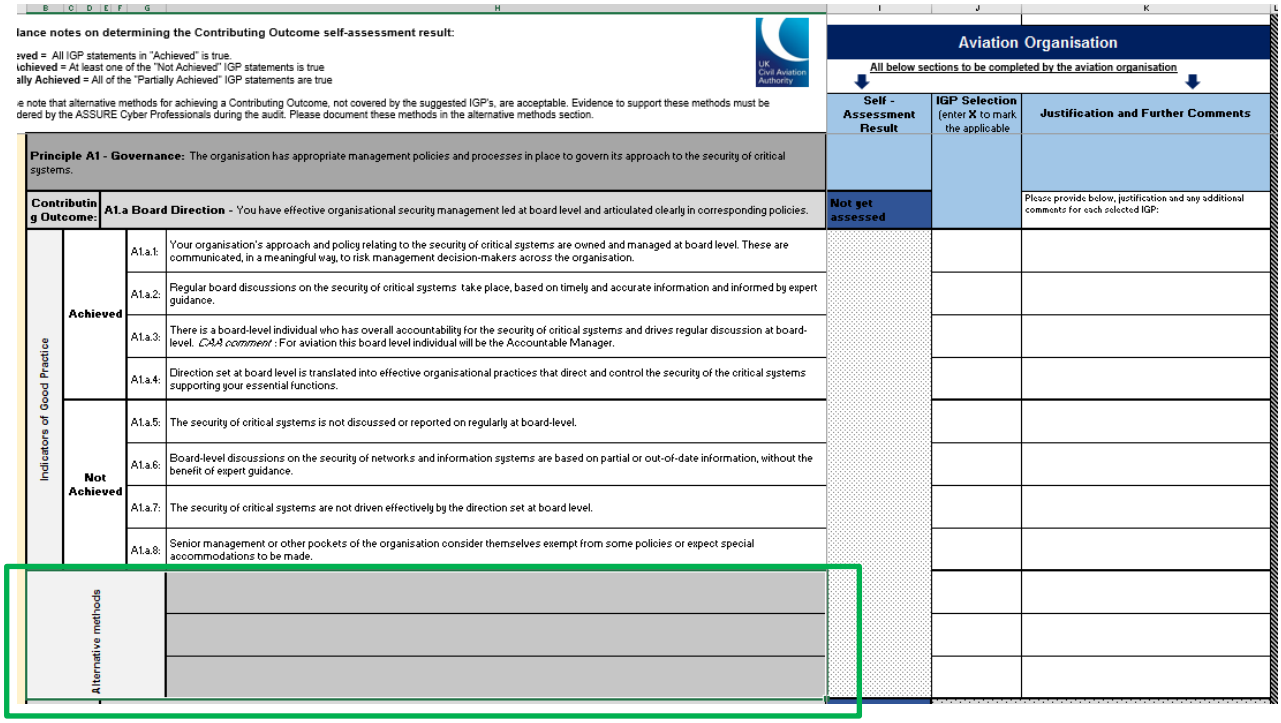
			Aviation Organisation All below sections to be completed by the aviation organisation		
			Self - Assessment Result	IGP Selection (enter X to mark the applicable	Justification and Further Comments
Principle A1 - Governance: The organisation has appropriate management policies and processes in place to 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.		**Not yet assessed**		Please provide below, justification and any additional comments for each selected IGP:
Good Practice	**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. *CAA comment*: 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

Note: In some cases, the Principle is the Contributing Outcome. This happens where there is only one Contributing Outcome. In these cases, the aviation organisation and ASSURE Cyber Professional should refer to the associated Principle.

4.2. Alternative Methods

In keeping with the spirit of the CAF for Aviation, the CAA understands that alternative methods (i.e. additional good practice and controls), which are not covered by the IGP's, but still meet the Contributing Outcome may be in place. These should be detailed within the "Alternative Methods" fields.



lance notes on determining the Contributing Outcome self-assessment result:

ved = All IGP statements in "Achieved" is true.
chieved = At least one of the "Not Achieved" IGP statements is true
ally Achieved = All of the "Partially Achieved" IGP statements are true

e note that alternative methods for achieving a Contributing Outcome, not covered by the suggested IGP's, are acceptable. Evidence to support these methods must be dered by the ASSURE Cyber Professionals during the audit. Please document these methods in the alternative methods section.

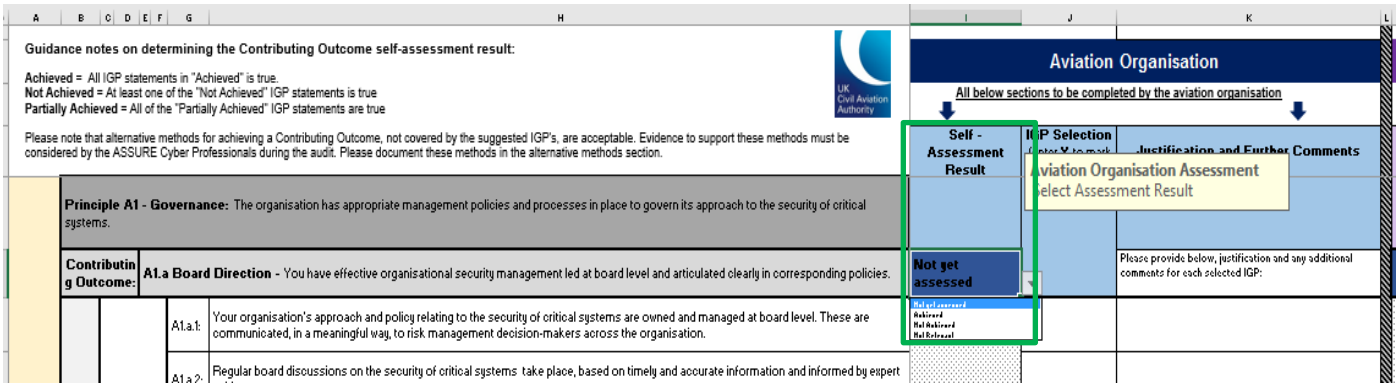
				Aviation Organisation All below sections to be completed by the aviation organisation		
				Self - Assessment Result	IGP Selection (enter X to mark the applicable	Justification and Further Comments
Principle A1 - Governance: The organisation has appropriate management policies and processes in place 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.			Not yet assessed		Please provide below, justification and any additional comments for each selected IGP:
Indicators of Good Practice	**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. *CAA comment*: 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.			
	Not Achieved	A1.a.5:	The security of critical systems is not discussed or reported on regularly at board-level.			
		A1.a.6:	Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance.			
		A1.a.7:	The security of critical systems are not driven effectively by the direction set at board level.			
		A1.a.8:	Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.			
Alternative methods						

Note: During the ASSURE Cyber Audit stage[6] the ASSURE Cyber Professional(s) **must** consider all additional good practice and controls detailed within this section when determining the aviation organisations position against the associated Contributing Outcome.

[6] www.caa.co.uk/CAP1753

4.3. Self-Assessment Results

Once IGPs have been selected against each Contributing Outcome, the aviation organisation must select an "Assessment" from the drop-down menu.



Selection of an Assessment status must be made in accordance with the following:

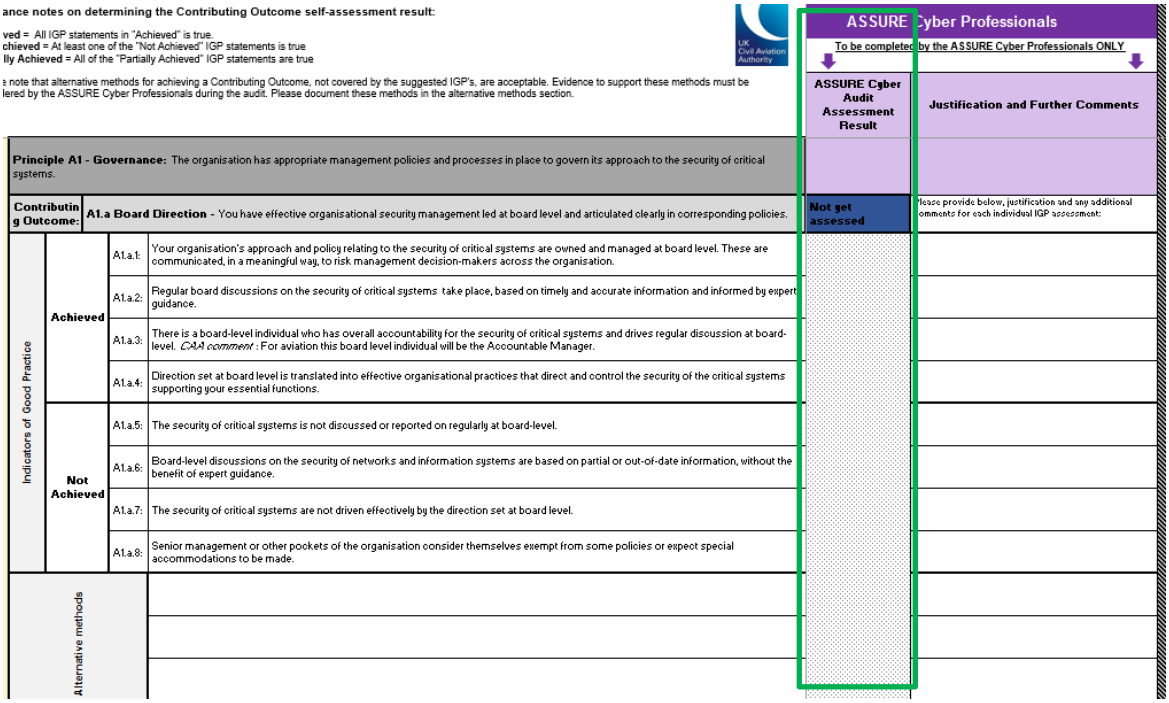
'Not Achieved'	**Should** be selected **even if only one** IGP statement in this column is applicable.
'Partially Achieved'	**Can only** be selected if **all** IGPs statements in this column are applicable, and **if no** 'Not Achieved' statements apply.
'Achieved'	**Can only** be selected if **all** IGP statements in this column are applicable, and **if no** 'Not Achieved' statements apply.

In certain circumstances, the following option may be chosen in place of those above:

- 'Not relevant' (justification **must** be provided where this is selected).

4.3.1. ASSURE Cyber Audit Assessment

The ASSURE Cyber Professional must, based on evidence, provide their own assessment status using the drop-down fields provided, for each Contributing Outcome. This must be based on **expert opinion** and validated through evidential audit. For further information on conducting an ASSURE Cyber Audit please refer to the relevant CAA ASSURE Implementation Guide[7].



ance notes on determining the Contributing Outcome self-assessment result:

ved = All IGP statements in "Achieved" is true.
chieved = At least one of the "Not Achieved" IGP statements is true
lly Achieved = All of the "Partially Achieved" IGP statements are true

note that alternative methods for achieving a Contributing Outcome, not covered by the suggested IGP's, are acceptable. Evidence to support these methods must be lered by the ASSURE Cyber Professionals during the audit. Please document these methods in the alternative methods section.

				ASSURE Cyber Professionals To be completed by the ASSURE Cyber Professionals ONLY	
				ASSURE Cyber Audit Assessment Result	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.		Not yet assessed	Please provide below, justification and any additional comments for each individual IGP assessment:
Indicators of Good Practice	**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. *CAA comment*: 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.		
	Not Achieved	A1.a.5:	The security of critical systems is not discussed or reported on regularly at board-level.		
		A1.a.6:	Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance.		
		A1.a.7:	The security of critical systems are not driven effectively by the direction set at board level.		
		A1.a.8:	Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.		
Alternative methods					

Selection of an Assessment status must be made in accordance with the following:

'Not Achieved'	**Should** be selected **even if only one** IGP statement in this column is applicable.
'Partially Achieved'	**Can only** be selected if **all** IGPs statements in this column are applicable, and **if no** 'Not Achieved' statements apply.
'Achieved'	**Can only** be selected if **all** IGP statements in this column are applicable, and **if no** 'Not Achieved' statements apply.

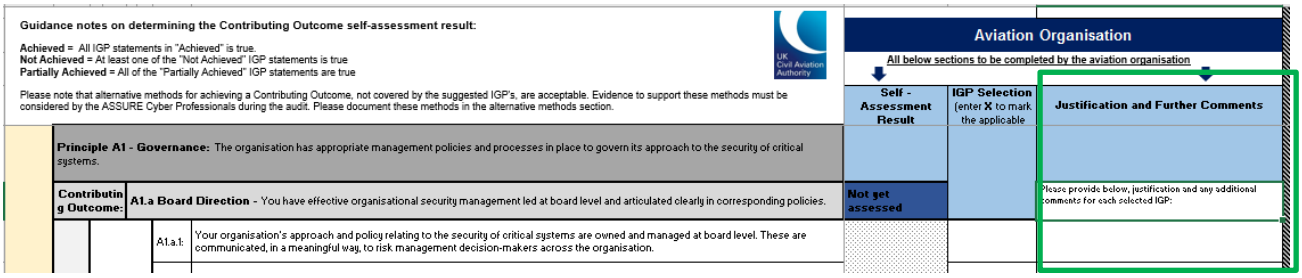
In certain circumstances, the following options may be chosen in place of those above:

- 'Not yet assessed' is the default status and must be replaced; or
- 'Not Audited' this status can only be used where there is no requirement for a Contributing Outcome to be audited. This is to be determined by an aviation organisation.

[7] https://www.caa.co.uk/Commercial-industry/Cyber-security-oversight/Cyber-security-compliance/

4.4. Aviation Organisation Justification and Further Comments

Following the selection of appropriate IGPs and/or Alternative Methods and the Assessment status, the aviation organisation must use the 'Justification and Further Comments' free flow text box to provide strong narrative evidence for the IGP's selected.



Guidance notes on determining the Contributing Outcome self-assessment result:

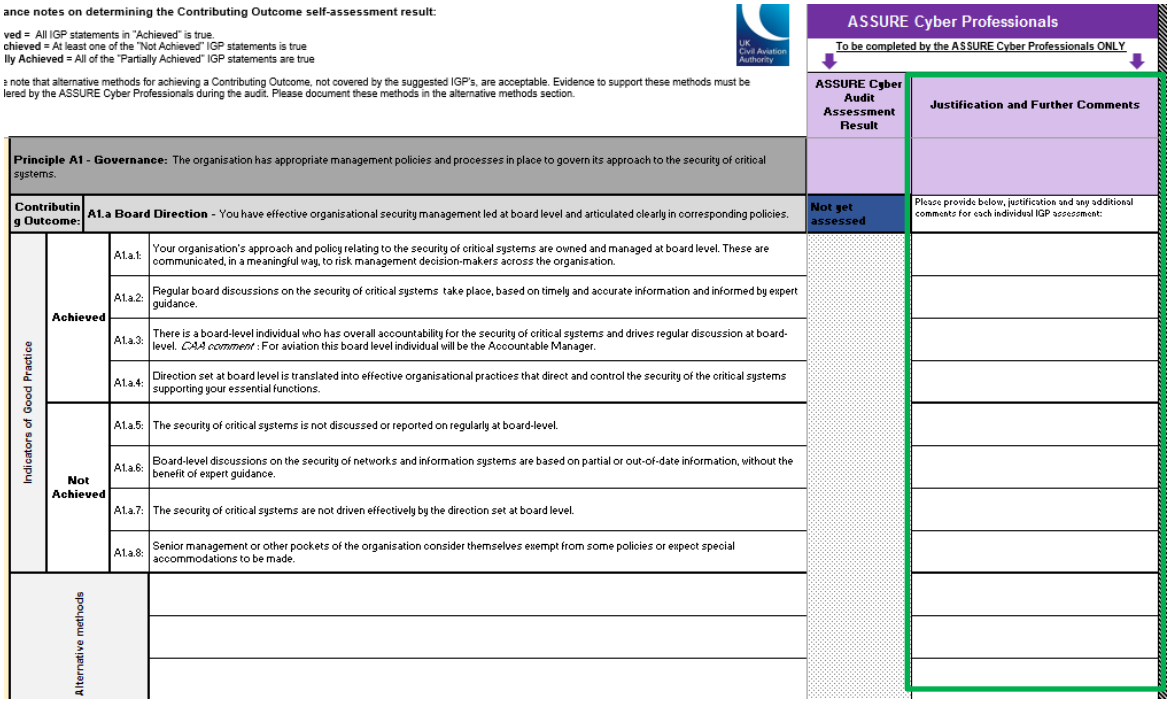
Achieved = All IGP statements in "Achieved" is true.
Not Achieved = At least one of the "Not Achieved" IGP statements is true
Partially Achieved = All of the "Partially Achieved" IGP statements are true

Please note that alternative methods for achieving a Contributing Outcome, not covered by the suggested IGP's, 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.

				Aviation Organisation All below sections to be completed by the aviation organisation		
				Self - Assessment Result	IGP Selection (enter X to mark the applicable	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.			Not yet assessed		Please provide below, justification and any additional comments for each selected IGP:
		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.			

4.4.1. ASSURE Supplier Justification and Further Comments

The ASSURE Cyber Professionals must use the 'Justification and Further Comments free flow text box to detail the validated good practice and controls, along with reference to the supporting evidence, which in their expert opinion enabled the Contributing Outcome to be met (strong narrative must be provided for all Alternative Methods audited).



ance notes on determining the Contributing Outcome self-assessment result:

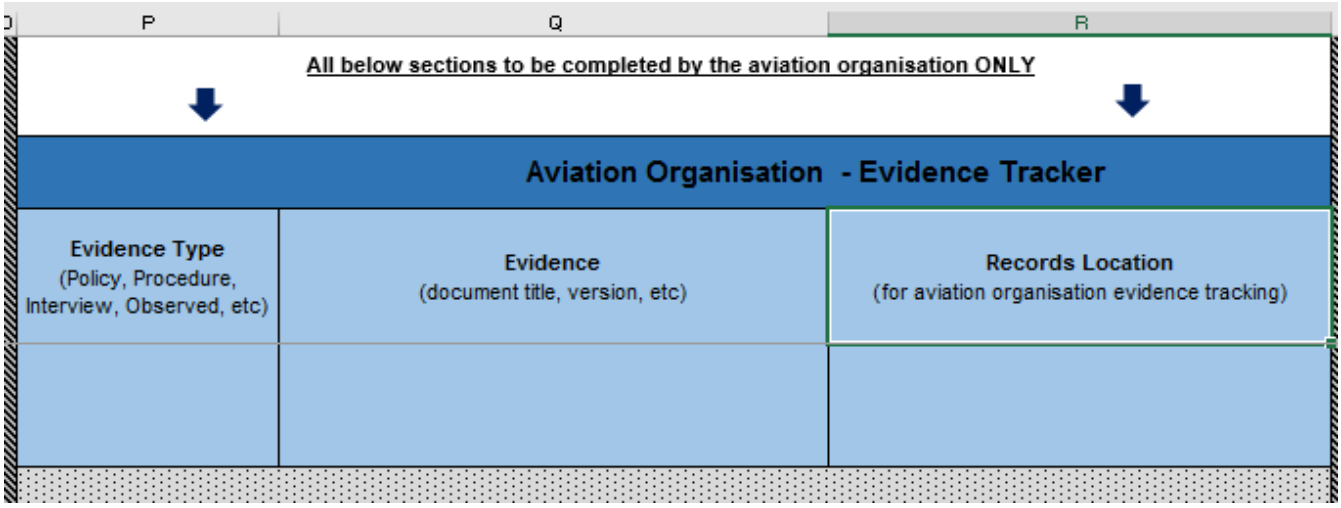
ved = All IGP statements in "Achieved" is true.
chieved = At least one of the "Not Achieved" IGP statements is true
lly Achieved = All of the "Partially Achieved" IGP statements are true

e note that alternative methods for achieving a Contributing Outcome, not covered by the suggested IGP's, are acceptable. Evidence to support these methods must be lered by the ASSURE Cyber Professionals during the audit. Please document these methods in the alternative methods section.

				ASSURE Cyber Professionals To be completed by the ASSURE Cyber Professionals ONLY	
				ASSURE Cyber Audit Assessment Result	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.			Not yet assessed	Please provide below, justification and any additional comments for each individual IGP assessment:
Indicators of Good Practice	**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. *CAA comment* : 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.		
	Not Achieved	A1.a.5:	The security of critical systems is not discussed or reported on regularly at board-level.		
		A1.a.6:	Board-level discussions on the security of networks and information systems are based on partial or out-of-date information, without the benefit of expert guidance.		
		A1.a.7:	The security of critical systems are not driven effectively by the direction set at board level.		
		A1.a.8:	Senior management or other pockets of the organisation consider themselves exempt from some policies or expect special accommodations to be made.		
Alternative methods					

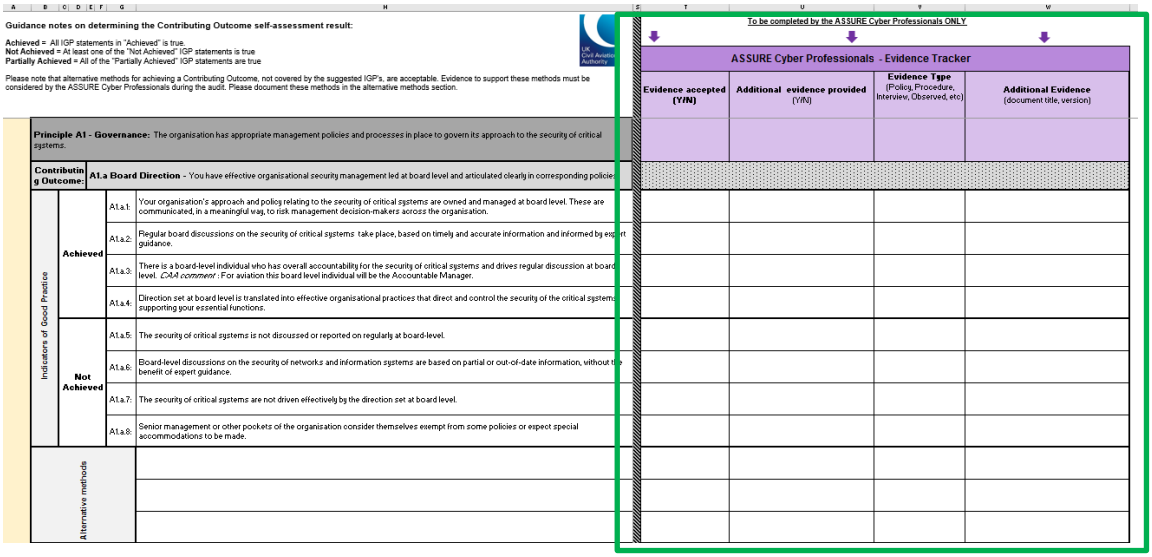
4.5. Aviation Organisation - Evidence Tracker

An evidence tracker has been provided within each of the “Assessment” tabs. This tracker should be used to document the evidence types, document tiles, versions and locations of stored evidence that support the selection IGP’s, specifically for achieved or partially achieved selections (to aid your ASSURE Cyber Audit).



4.5.1. ASSURE Cyber Supplier – Evidence Tracker

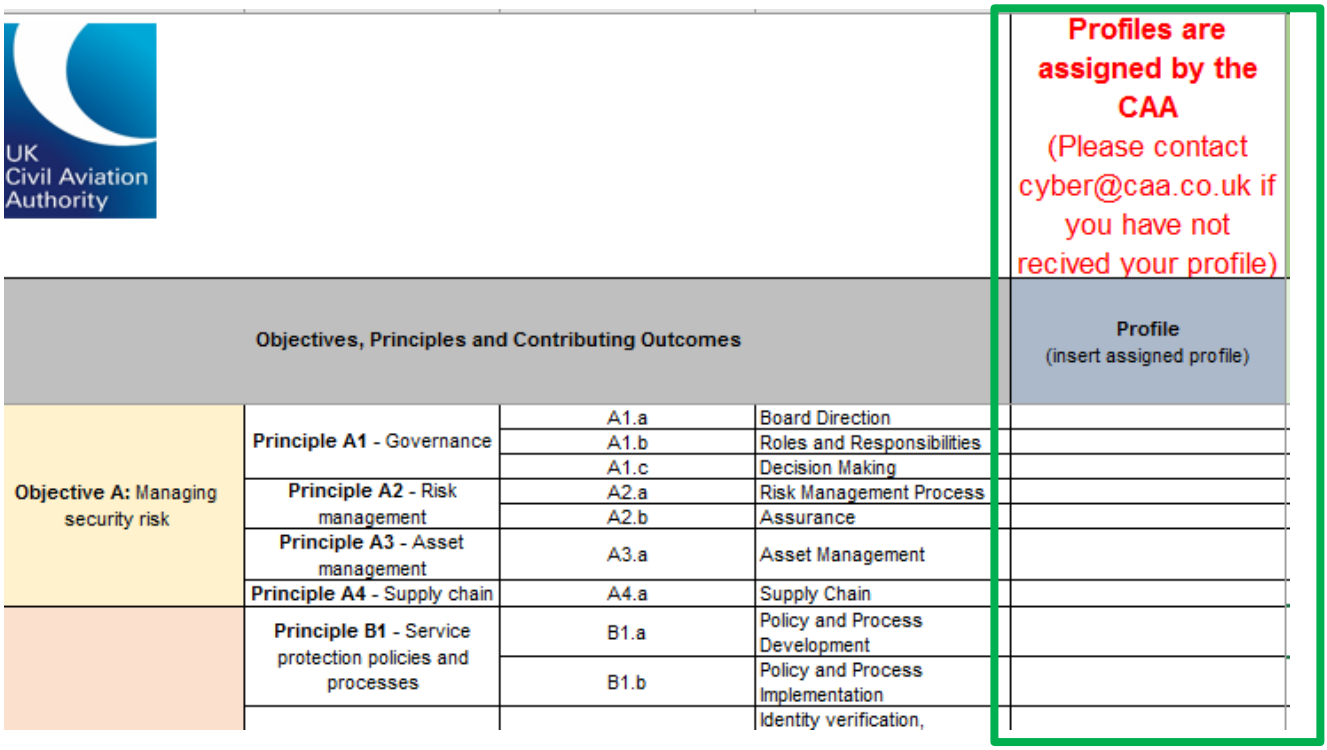
An ASSURE evidence tracker has been provided within each of the “Assessment” tabs. This tracker should be used to document whether the evidence submitted by the aviation organisation in support of the IGP’s and/or Alternative Methods is acceptable or not and where applicable, the details of additional evidence provided.



5. Corrective Action Plan

The 'Corrective Action Plan' tab enables an aviation organisation to assign remediation plans to the gaps identified between the ASSURE Cyber Audit Assessment and the assigned profile. An aviation organisation can start to develop the Corrective Action Plan and pull together information whilst performing the initial CAF for Aviation self-assessment. Plans should be updated following the ASSURE Cyber Audit, and where appropriate these can incorporate any suitable recommendations.

Aviation organisations must populate column E of the 'Corrective Action Plan' tab with the 'profile' assigned by the CAA during Step 1 – Engagement to populate the Statement of Assurance data tab.



UK Civil Aviation Authority

Profiles are assigned by the CAA
(Please contact cyber@caa.co.uk if you have not recived your profile)

Objectives, Principles and Contributing Outcomes				Profile (insert assigned profile)
Objective A: Managing security risk	**Principle A1** - Governance	A1.a	Board Direction	
		A1.b	Roles and Responsibilities	
		A1.c	Decision Making	
	Principle A2 - Risk management	A2.a	Risk Management Process	
		A2.b	Assurance	
	Principle A3 - Asset management	A3.a	Asset Management	
	Principle A4 - Supply chain	A4.a	Supply Chain	
	Principle B1 - Service protection policies and processes	B1.a	Policy and Process Development	
		B1.b	Policy and Process Implementation	
			Identity verification,	

Aviation organisations must also detail from Column AE to AJ in the 'Corrective Action Plan' tab for each Principle and associated Contributing Outcome the:

- Indicators of Good Practice(s) being addressed;
- risk assessment summary of inherent risk and current risk - inc details of existing mitigations;
- document name of attached evidence of planned actions (incl. resourcing, budgeting and ownership) actions (e.g. document name of project plan or risk remediation/mitigation plans);
- risk assessment summary of residual risk post plan implementation;

- start date (of planned remediation/mitigation work); and
- estimated completion date (of remediation/mitigation work).

Corrective Action Information					
IGPs being addressed	**Summary of inherent risk and current risk** (please include details of existing mitigations)	**Document name of attached evidence of planned actions** (this must include resourcing, budgeting and ownership)	**Summary of residual risk** (post plan implementation)	**Start date** (of planned actions)	**Estimated completion date**

In accordance with CAP1753 all documents detailed in 'Document Name of Evidence of Planned Action' must be sent securely to the CAA along with the aviation organisations provisional Statement of Assurance by the advised deadline.

5.1. Cyber Risk assessment

Aviation organisations should follow an effective cyber risk assessment methodology when conducting cyber risk assessments for the completion of their Corrective Action Plan.

- Inherent risk is an aviation organisation's calculated level of risk without any mitigations in place.
- Current risk is an aviation organisation's calculated current level of risk with mitigations in place (i.e. the current mitigations in place at the time of completing the CAF for Aviation).
- The residual risk is an aviation organisation's estimated level of risk once the corrective actions detailed in the corrective action plan, have been implemented.

There are many cyber risk assessment methodologies to choose from when conducting a risk assessment[8]. Aviation organisations are responsible for selecting a suitable cyber risk assessment methodology. The CAA recommend that the following areas are considered when conducting cyber risk assessments.

- Threats
- Vulnerabilities
- Impact (e.g. potential safety impacts)
- Likelihood
- Mitigations and existing controls

[8] https://www.cybok.org/media/downloads/Risk_Management__Governance_issue_1.0.pdf

6. Statement of Assurance

A Statement of Assurance serves as a commitment from an aviation organisation that it is complying with the Civil Aviation Authority's (CAA) Cyber Security Oversight Process (CAP1753) and that it is providing an accurate representation of the organisation's cyber risk posture and identified remediations.

The Statement of Assurance is divided into two sections; the ***provisional*** Statement of Assurance; and the ***final*** Statement of Assurance. Both *must* be completed by the aviation organisation and submitted to the Cyber Security Oversight Team for validation in line with the agreed milestones set out in the initial Engagement Letter.

The "Statement of Assurance data" tab in the CAF for Aviation requires no input from an aviation organisation and can be copied and pasted into your provisional Statement of Assurance.

6.1. Sharing Information Securely with the CAA

Any sensitive documentation including a completed CAF for Aviation, ASSURE Cyber Audit Report or Statements of Assurance with associated documentation **must not be submitted to the CAA via email**. The CAA will issue each aviation organisation with an AES256 hardware encrypted flash drive. Submissions will only be accepted using this flash drive and delivered either in person, by a representative of the aviation organisation, or by secure courier. Please refer to the CAA's Cyber Security Oversight Information Handling Instructions issued with your flash drive, please contact cyber@caa.co.uk for further assistance where required.

Annex B – Informative References and Example Evidence

Provided below are informative references and examples of evidence, these are not exhaustive and where alternate good practice or evidence is believed to meet a Contributing Outcome this should be detailed in the CAF for Aviation under “Alternative methods”.

Objective	Principle	Informative References	Example Evidence
Managing security risk	**A1 Governance:** The organisation has appropriate management policies and processes in place to govern its approach to the security of critical systems.	ISO/IEC 27001:2017 ISO/IEC 27002:2013 ISA/IEC 62443-2-1 NIST SP800-53 NIST SP800-82 EUROCAE ED-204	Details of employee’s roles, responsibilities, competencies, and appropriate security clearances Accountable Manager and Cyber Security Responsible Manager roles assigned Governance framework Cyber security policy documents Risk management approach Documented risk management decision Evidence of board meetings (e.g. agendas, minutes)
	A2 Risk management: The organisation takes appropriate steps to identify, assess and understand security risks to the critical systems supporting the operation of essential functions. This includes an overall	ISO/IEC 27005:2018 ISO/IEC 27001:2017 ISO/IEC 3100:2018 ISA/IEC 62443 1-1 ISA/IEC 62443 2-1 NIST SP800-30 NIST SP800-37 NIST SP800-39	Use of established methods or frameworks (e.g., ISO2700-X) Risk management approach Risk assessment review records conducted in line with risk governance Use of current threat and vulnerability information in risk assessment process Current risk-register with associated actions and improvement management plan (including risk ownership) Evidence of appropriate assurance activity

	organisational approach to risk management.	NIST SP800-82 EUROCAE ED202A, ED203A, ED204 & ED205 CyBOK Risk Management & Governance Knowledge Area	
	A3 Asset management: Everything required to deliver, maintain or support critical systems is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).	ISO/IEC 55001:2019 ISO/IEC27002: 2013 ISA 62443-1-1 NIST SP800-82 NIST SP800-53	Asset management policy Asset register and sample critical asset check through the lifecycle. To include IT and OT assets where applicable High-level network architecture diagrams Plans and road maps for hardware and software, including approach to patching and end of support dates
	A4 Supply chain: The organisation understands and manages security risks to critical systems supporting the operation of essential functions that arise as a result of dependencies on external suppliers. This	ISO/IEC 27002:2013 ISO/IEC 27036-2 ISO/IEC 27036-3 ISA/IEC 62443-2-1 NIST SP800-53 NIST SP800-37 EUROCAE ED201	List of critical suppliers maintained including their cyber security contacts and responsibilities Detail of cyber security requirements imposed on suppliers Overview of contractual agreements in place Reports of completed assessment and assurance of suppliers

	includes ensuring that appropriate measures are employed where third party services are used.		
Protecting against cyber-attack	**B1 Function protection policies and processes:** The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing critical systems and data that support operation of essential functions.	ISO/IEC 27001:2017 ISO/IEC 27002:2013 ISO/IEC 22301:2019 ISA/IEC 62443-1-1 NIST SP800-53 NIST SP800-82	Published and controlled policies, procedures, and work instructions etc HR procedures enabling appropriate security clearance of relevant staff Configuration records (e.g. for firewalls, etc.) Management of change records Management of change policies Validation test records Audit reports, review reports, and management of resulting actions

	B2 Identity and access control: The organisation understands, documents, and manages access to critical systems supporting the operation of essential functions. Users (or automated functions) that can access critical data or critical systems are appropriately verified, authenticated and authorised.	ISO/IEC 27001:2019 ISO/IEC 27002:2013 NIST SP800-53 NIST SP800-82 EUROCAE ED204 CyBOK Authentication, Authorisation and Accountability Knowledge Base	Appropriate authentication and authorisation approach defined within access control policies (including for physical, remote, and privileged access) Records of current authorised users / assets / accounts and the level of access / privilege assigned to each (noting data security and device management requirements) Records of access rights reviews Documented Joiners / Movers / Leavers process highlighting role-based access controls

	B3 Data security: Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause an adverse impact on critical systems. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the operation of critical systems. It also covers information that would assist an attacker, such as design details of critical systems.	ISO/IEC 27002:2013 ISA/IEC 62443-1-1 ISA/IEC 62443-2-1 ISA/IEC 62443-3-3 NIST SP800-53 NIST SP800-82 EUROCAE ED204 & ED205	Relevant procedures for identification and recording of sensitive data and assets containing this data and how this is protected, including for mobile device management, data minimisation, and remote wiping Detail on approach to encryption, including algorithms used, and key management Records of essential data, services, and connections identified and how these are protected where required and risk assessments supporting the level of protection applied Documented impact statements for data loss or alteration which are regularly reviewed, containing contingency plans where required Documented information management policies detailing retention and deletion

	B4 System security: Critical systems and technology critical for the operation of essential functions are protected from cyber attack. An organisational understanding of risk to the critical system informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.	ISO/IEC 27002:2013 ISA/IEC 62443-1-1 ISA/IEC 62443-2-1 ISA/IEC 62443-3-3 NIST SP800-53 NIST SP800-82 EUROCAE ED202A, ED203A, ED204 & ED205	Policy setting out design requirements for network architecture, segregation, and access Network designs support effective security monitoring and recovery Asset hardening procedures / instructions / templates Vulnerability / threat scanning and mitigation Patch management and asset configuration procedures Evidence of software whitelisting and identification of malware
	B5 Resilient Networks and Systems: The organisation builds resilience against cyber-attack and system failure into the design, implementation, operation and	ISO/IEC 27002:2013 ISO/IEC 27035-3 ISA/IEC 62443-1-1 NIST SP800-53 NIST SP800-82	Records of review of limitations, constraints and weaknesses with evidence of periodic review Documented Business Continuity and Disaster Recovery strategy with evidence of practices / tests being carried out Software/firmware/application/configuration libraries and safes

	management of critical systems.		
	B6 Staff Awareness and Training: Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of critical systems supporting the operation of essential functions.	NCSC 10 Steps: User Education and Awareness ISO/IEC 27001:2019 ISO/IEC 27002:2013 ISA/IEC 62443-2-1 NIST SP800-53 NIST SP800-82	Definition of competence requirements for defined roles and responsibilities in relation to essential services Cyber security awareness training and/or education programmes Competence management records Mechanisms for reporting of cyber security mechanism

Detecting cyber security events	**C1 Security monitoring:** The organisation monitors the security status of the network and systems supporting the operation of critical systems in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.	NCSC Introduction to logging for security purposes NCSC 10 Steps: Monitoring CREST – Cyber Security Monitoring Guide ISO/IEC 27002:2019 ISO/IEC 27002:2013 ISO/IEC 27035:1-3 ISA/IEC 62443-2-1 NIST SP 800-53 NIST SP800-82 NIST SP800-94	Procedures setting out security monitoring requirements including, incident resolution, malware signature/IoC requirements, and adequate resourcing Records of periodic monitoring (e.g. of security logs, virus detection logs, intrusion detection logs etc.) Analysis and interpretation of the threat intelligence and periodic monitoring records and management of resulting actions Logging data fidelity allows it to inform the protection function, and is itself adequately protected against unauthorised alteration, is correctly and securely correlated, and access to logs is attributable to unique users Evidence of threat intelligence feeds being available pertinent to the organisation and sharing taking place where necessary

	C2 Proactive security event discovery: The organisation detects, within critical systems, malicious activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard signature-based security prevent/detect solutions (or when standard solutions are not deployable).	ISO/IEC 27001:2019 ISO/IEC 27002:2013 ISO/IEC 27035-3 ISA/IEC 62443-2-1 NIST SP800-53	Procedures setting out security monitoring requirements including network baselining and malicious code detection Records of periodic monitoring feeding threat intelligence and monitoring processes (e.g. of security logs, virus detection logs, intrusion detection logs etc.) Analysis and interpretation of threat intelligence and network monitoring events, periodic monitoring records, and management of resulting actions Process detailing searching for threats or abnormalities within critical systems, and their documentation including relevant risk assessments

Minimising the impact of cyber security incidents	**D1 Response and recovery planning:** There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	NCSC 10 Steps: Incident Management ISO/IEC 27035 (all) ISO/IEC 22301:2019 ISO/IEC 27002:2013 NIST SP800-61 NIST SP800-53 NIST SP800-82 EUROCAE ED204	Up-to-date, approved, and comprehensive incident response plan detailing known and possible attacks and roles and responsibilities which covers the life-cycle of an incident Incident response exercise plans based on relevant threat intelligence and events, which are regularly reviewed and validated

	D2 Lessons learned: When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	NCSC 10 Steps: Incident Management ENISA Good Practice for Incident Management Guide ISO/IEC 27035:2-3 ISO/IEC 22301:2019 ISO/IEC 27001:2019 ISO/IEC 27002:2013 NIST SP800-61 NIST SP800-53	Evidence of comprehensive post-incident root cause analysis being conducted routinely which covers organisational policy as well as hardware/software issues/vulnerabilities Documented incident review policy detailing lessons learned requirements Evidence showing lessons learned feeding continual improvement