UK Civil Aviation Authority

ASSURE

CREST

ASSURE Scheme

CREST Implementation Guide

Contents

1.Introduction

1.1 Background

The UK Civil Aviation Authority (CAA) recognises its aviation cyber security regulatory oversight responsibilities under existing and emerging resilience, safety and security regulations. As a result, the CAA developed CAP 1753 *'The Cyber Security Oversight Process for Aviation'*, a proportionate, consistent and scalable six-step approach to cyber security oversight.

In partnership with CREST, the CAA have developed the 'ASSURE Scheme' a third-party cyber security audit model. This scheme enables aviation organisations, in-scope of CAP 1753, to procure ASSURE Cyber Audit capabilities from a pool of competent and skilled ASSURE Cyber Suppliers. The ASSURE Cyber Suppliers, on behalf of the CAA and as Qualified Entities, perform independent ASSURE Cyber Audits against the aviation organisation's Cyber Assessment Framework (CAF) for Aviation, as described in step four 'ASSURE Cyber Audit' of CAP 1753.

The ASSURE Scheme allows the CAA to maintain a smaller in-house team of Cyber Security Oversight Specialists who act as "senior decision makers", making informed judgements on oversight activity and, if necessary, remedial or enforcement measures.

1.2 Purpose

This Guide has been developed by the CAA's Cyber Security Oversight Team to provide an overview of the CAA's ASSURE Scheme, and guidance for new and existing ASSURE Cyber Suppliers on the ASSURE accreditation process. It also sets out the conditions for how ASSURE Cyber Suppliers and Professionals are expected to conduct ASSURE Cyber Audits.

CREST and the CAA's Cyber Security Oversight Team are available to answer any questions from prospective and existing ASSURE Cyber Suppliers, or aviation organisations. If you have any questions or feedback on this guide or the ASSURE Scheme, please contact assure@crest-approved.org or cyber@caa.co.uk.

1.3 Benefits

The ASSURE Scheme is a scalable and responsive model which provides aviation organisations with a level of assurance in their choice of audit supplier and a structure for how audits should be conducted.

The ASSURE Scheme utilises commercial suppliers, many of whom are well known to the aviation sector, bringing current knowledge and a wealth of experience to deliver independent validation.

Boards and owners of aviation organisations will value the independent assurance offered by a cyber security audit which provides an accurate representation of their organisation's cyber risk posture at a point in time. The ASSURE Cyber Audit Report will help organisations meet their regulatory requirements and communicate key cyber security issues to their Boards.

1.4 Legal Responsibility and Liability

The CAA ASSURE Scheme CREST Implementation Guide provides guidance to accredited ASSURE Cyber Suppliers on how to conduct an ASSURE Cyber Audit. Where ASSURE Cyber Audits are not conducted in accordance with this guidance, this may result in enforcement action being taken against an ASSURE accreditation – see paragraph 2.5.4 of the ASSURE Addendum (Annex B in this document) for further information. It is the ASSURE Cyber Supplier's responsibility to ensure they read, understand and conduct an ASSURE Cyber Audit in accordance with this guidance. The ASSURE Cyber Supplier is responsible for how they conduct an ASSURE Cyber Audit and ensuring they continue to satisfy the criteria to maintain their ASSURE accreditation.

The impartiality of the ASSURE Cyber Audit must be guaranteed; remuneration must not depend upon a "favourable" ASSURE Cyber Audit Report. The ASSURE Cyber Audit Report must be evidence based and maintain a high level of integrity.

All ASSURE Cyber Suppliers and ASSURE Cyber Professionals must observe professional secrecy with regard to all information acquired or reviewed when carrying out an ASSURE Cyber Audit on behalf of the CAA.

1.5 Document Set

The supplementary documents referred to in this guide include:

Title	Description	Location
ASSURE Addendum	Code of Conduct that must be signed in order for Cyber Suppliers to be accredited to conduct ASSURE Cyber Audits on behalf of the CAA.	Annex B
Cyber Assessment Framework (CAF) for Aviation	The CAF for Aviation is adapted from the NCSC's core CAF and has been designed specifically to meet the needs of the aviation industry. The CAF for Aviation *must* be completed by an aviation organisation in advance of the ASSURE Cyber Audit.	CAF for Aviation[1]

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

CAF for Aviation Guidance	Guidance produced by the CAA to assist in the completion of the CAF for Aviation, including informative cyber security references (or relevant standards) against each of the fourteen principles. It also includes examples of the types of evidence that the CAA would expect to support the CAF for Aviation self-assessment.	CAP 1850[2]
Critical System Scoping Guidance and Template	Guidance and template developed by the CAA to assist aviation organisations in the identification and documentation of in-scope critical systems.	CAP 1849[3] Scoping Template[4]
ASSURE Cyber Audit Report Template	Report template which can be used by ASSURE Cyber Suppliers to create their ASSURE Cyber Reports. The final completed report must be signed by the ASSURE-accredited Cyber Professionals as part of the ASSURE Cyber Audit (see section *5.7 ASSURE Cyber Audit Report and Template*).	Will be shared on request
Provisional Statement of Assurance	Aviation organisations are required to send a provisional Statement of Assurance to the CAA which must include, among other documents, the ASSURE Cyber Audit Report. More information can be found in CAP 1753[5].	A template will be shared with aviation organisations

[2] https://www.caa.co.uk/cap1850

[3] https://www.caa.co.uk/cap1849

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

[5] https://publicapps.caa.co.uk/cap1753

2. ASSURE Scheme

2.1 Model

The ASSURE Scheme involves five key stages as depicted in *Figure 1* below. Each stage is further described herein.

Figure 1: ASSURE Scheme stages

2.2 ASSURE Roles, Responsibilities and Definitions

The table below outlines the roles, responsibilities and definitions associated with the ASSURE Scheme.

Role	Description
Regulator (CAA)	The UK's specialist aviation regulator is responsible for ensuring that the aviation industry meets the highest safety standards, that consumers have choice and, value for money, that they are protected and treated fairly when they fly, and that the aviation industry manages security risks effectively. 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. The CAA Cyber Security Oversight Team is responsible for all cyber security regulatory activity within any of the CAA regulatory domains (for example Continuing Airworthiness, Flight Operations, Aerodromes, Airspace, Air Traffic Management, and Aviation Security).

Role	Description
	The Team is also the first point of contact at the CAA for all questions and issues relating to the cyber security oversight process for aviation and can be contacted at cyber@caa.co.uk.
Accountable Manager	The Accountable Manager(s) is an individual or individuals designated by their aviation organisation as the person(s) responsible to the CAA in respect of the functions which are subject to regulation. It is expected that the role of Accountable Manager is held by an individual who has corporate authority for ensuring that all operational activities can be financed and carried out to the standard required by the CAA. For cyber security accountability, individuals do not have to be the operational "Accountable Manager" registered with the CAA but instead can be an equivalent board member (e.g., Chief Information Security Officer, CIO, IT Director etc) dependent on the aviation organisation's structure.
Cyber Security Responsible Manager	An individual who has been delegated responsibility for cyber security by the aviation organisation's Accountable Manager, they may have responsibility for specific areas of their organisation (e.g., Head of Information Security, Safety Manager, Security Manager etc). The Cyber Security Responsible Manger ensures compliance with cyber security regulations and is responsible for the management of cyber security risk exposure. As a Cyber Security Responsible Manager, you will be asked to demonstrate the appropriate competency for the post and to enable the sharing of threat information you will need to hold the relevant security clearance[6].
Accreditation Body	An organisation capable of providing accreditation services and a platform to enable Cyber Suppliers and Cyber Professionals to be accredited to conduct ASSURE Cyber Audits in accordance with the Regulator's requirements.

[6] Detail of the competency and vetting requirements can be found in the Cyber Security Responsible Manager Nomination Form.

Role	Description
ASSURE Cyber Supplier	Third party "Qualified Entities" that are subject to a rigorous and continuous accreditation process, to provide a cyber audit capability under the ASSURE Scheme. The ASSURE Cyber Supplier must adhere to the CREST Code of Conduct and ASSURE Addendum.
ASSURE Cyber Professional	ASSURE Cyber Suppliers utilise ASSURE Cyber Professionals who hold appropriate professional certifications and are accredited to conduct ASSURE Cyber Audits. The accredited ASSURE Cyber Professionals must adhere to the CREST Code of Conduct, CREST Code of Ethics and ASSURE Addendum. ASSURE Cyber Professionals are accredited in one or more of the three specialisms detailed in section *5.1 Composition of the Audit Team* (all specialisms must be present for an ASSURE Cyber Audit).
ASSURE Cyber Audit	An ASSURE Cyber Audit is completed by the ASSURE Cyber Supplier utilising ASSURE Cyber Professionals. The purpose of the audit is to provide a validated opinion and associated commentary on the Contributing Outcomes self-assessed by an aviation organisation, in their CAF for Aviation. The audit is evidence-based, through observing processes in practice, sampling, conducting interviews and reviewing policies and other relevant documentation provided by the aviation organisation.
Qualified Entity	An ASSURE Cyber Supplier accredited by the UK Civil Aviation Authority in accordance with Article 69 and Annex VI of REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ("the EASA Basic Regulation), to carry out certain specified cyber security oversight tasks on the CAA's behalf under the EASA Basic Regulation and implementing regulations.

3. ASSURE Accreditation

3.1 ASSURE Accreditation

The ASSURE accreditation process provides a mechanism for interested parties to become accredited ASSURE Cyber Suppliers and ASSURE Cyber Professionals, following a series of in-depth checks performed by both CREST and the CAA.

To apply for ASSURE accreditation, a cyber supplier must meet the minimum requirements that include, but are not limited to:

- Professional Indemnity Insurance
- Management of the use of Contractors
- Quality policies and processes
- Information security policies and processes
- Staff vetting
- Complaint handling
- Data management & security
- Approved individuals that meet the ASSURE requirements (see 5.2)

3.2 ASSURE Addendum

In addition to the CREST Code of Conduct, prospective ASSURE Cyber Suppliers *must* sign the ASSURE Addendum which outlines a Code of Conduct for ASSURE Cyber Suppliers. The ASSURE Addendum will be provided during the application process and specifies the additional requirements which must be complied with to be eligible for, and to retain, ASSURE accreditation. Any amendments to the Addendum will also result in ASSURE Cyber Suppliers having to resign it to retain ASSURE accreditation. Please see *Annex B: ASSURE Addendum.*

ASSURE Cyber Suppliers will need to annually resign the ASSURE Addendum, provide details of any changes that affect their ASSURE accreditation and attest if no changes are detailed that the information provided in their application form is still accurate.

3.3 ASSURE Accreditation Process

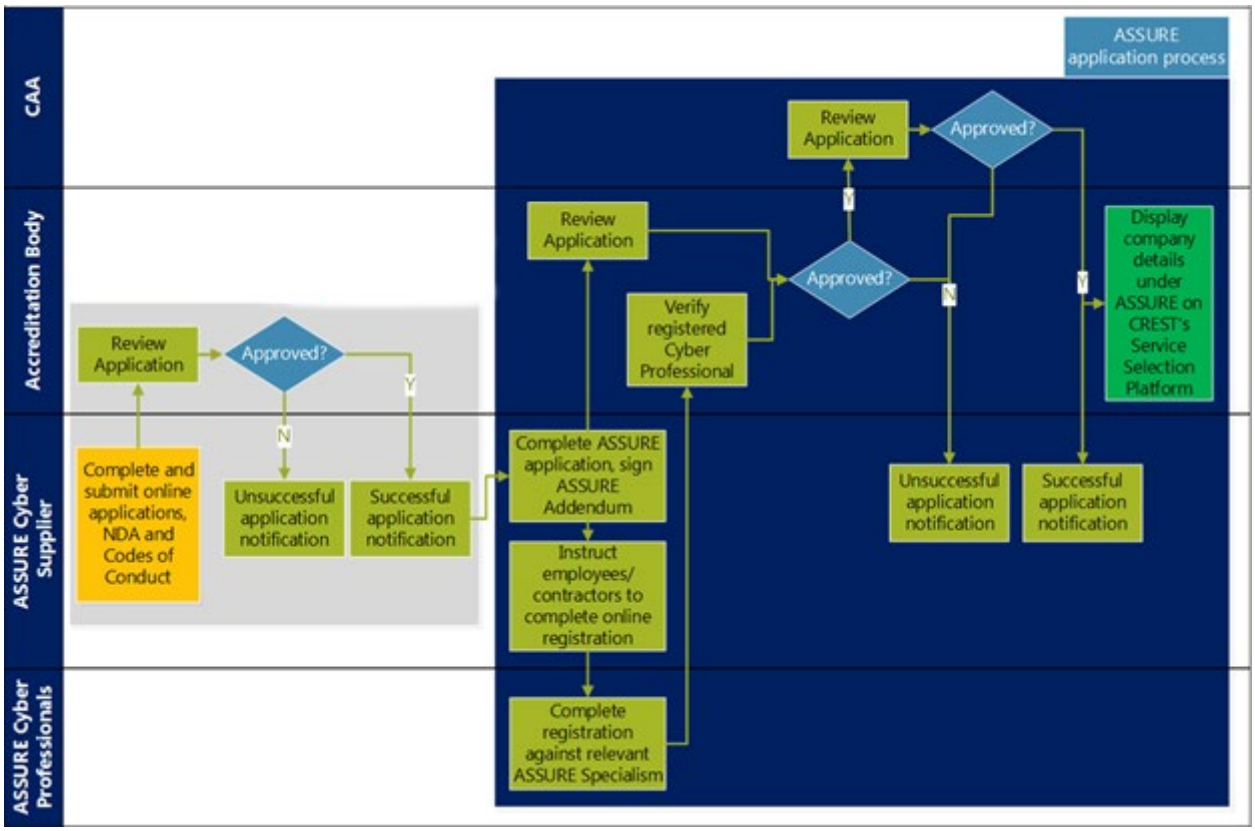

Figure 2: ASSURE accreditation process overview

Prospective ASSURE Cyber Suppliers are required to complete and submit an ASSURE Application Form, available via the CREST Membership Portal, to be reviewed by CREST and the CAA. The form requires all prospective ASSURE Cyber Suppliers to provide the following:

- Client references – two to three client references are required for the provision of cyber security services, either for aviation organisations or in similar client contexts comprising of both ICS and OT components. The CAA will contact these references as part of the application review.
- Demonstration of the organisation's audit capability – a demonstration of the audit capability must include; evidence of processes for managing the scope of the audit, communicating methods, managing risk and maintaining and improving auditor competence.
- Data retention, handling and disposal – details of procedures to ensure ASSURE Cyber Audit Reports and information gathered as part of the audit process will be securely protected at rest, in transit and through to disposal.
- Aggregation of information – details on how this will be managed where applicants plan to perform concurrent audits or hold information on more than one aviation organisation's ASSURE Cyber Audit. Further engagement with the CAA and NCSC *may* be required to ensure additional security measures are in place where;

- it is not possible for the ASSURE Cyber Supplier to maintain the report on client infrastructure; and
- not operationally feasible to hold multiple reports on a separate secure infrastructure.

- ASSURE Cyber Professionals - the ASSURE Cyber Supplier *must* register the names of all employees or contractors that qualify as ASSURE Cyber Professionals (as described below in section *5.1 Composition of the Audit Team*).

Where additional information is required to support an application CREST will contact the prospective ASSURE Cyber Supplier and ask for this to be supplied either through the CREST Membership portal or by email.

CREST will notify the prospective ASSURE Cyber Supplier, by email whether their application has been successful. If the Cyber Supplier is not successful CREST will provide details of where the application is deficient.

Note: It is the ASSURE Cyber Supplier's responsibility to notify CREST of any material changes that occur, which may affect their ASSURE accreditation. Where there is evidence that an ASSURE Cyber Supplier has provided deliberately false or misleading information or evidence, their ASSURE accreditation may be revoked.

4. Procurement

The approach taken to procure an ASSURE Cyber Audit, (e.g., single or competitive tender) is entirely at the discretion of the aviation organisation, provided the supplier selected is on the ASSURE Cyber Supplier register and has no conflict of interest.

Once accredited, the ASSURE Cyber Supplier and their contact details will be made available via the Service Selection Platform, under Regulator and Government Schemes (see Figure 3)[7]. For best results, use Chrome when visiting the Service Selection Platform.

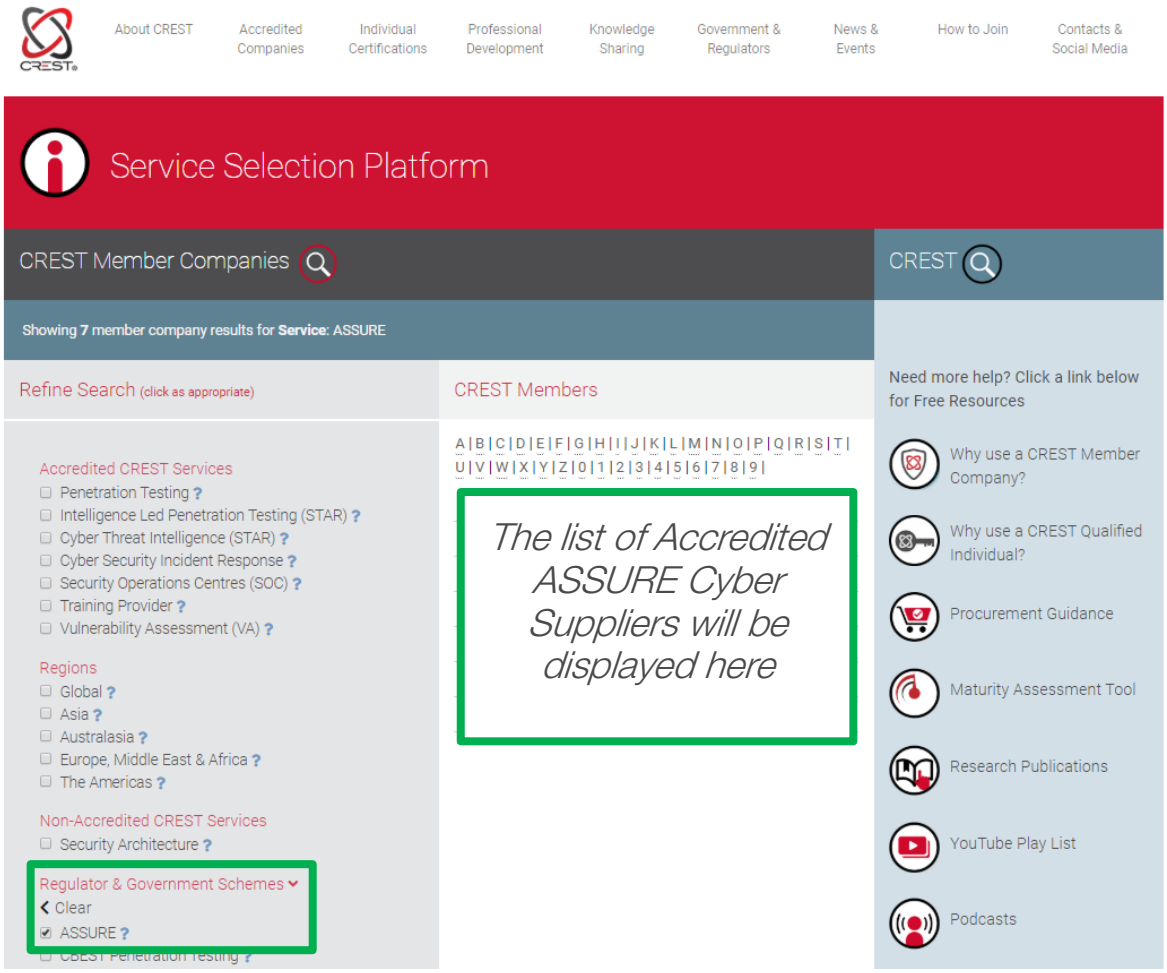

Figure 3: CREST's Service Selection Platform

Where the aviation organisation has additional requirements not specified in the ASSURE accreditation process (e.g. requires ASSURE Cyber Suppliers to hold government Security Clearance), these should be discussed directly with any prospective ASSURE Cyber Supplier during the procurement process. To ensure consistency and quality, the CAA may choose to attend any ASSURE Cyber Audit conducted by an ASSURE Cyber Supplier.

ASSURE Cyber Suppliers must inform the CAA of the dates, location and name of aviation organisation being audited when confirmed, by emailing cyber@caa.co.uk. This is a very important step and failure to inform the CAA before the audit is conducted may result inthe audit being invalidated.

[7] https://service-selection-platform.crest-approved.org/

An ASSURE Cyber Supplier must conduct the ASSURE Cyber Audit in line with the expectations and conditions (see section *5.8. ASSURE Cyber Audit Conditions*) set out in this Implementation Guide, as per section *1.4 Legal Responsibility and Liability*.

4.1 ASSURE Cyber Audit Scope

The critical systems and security boundaries detailed in the Critical Systems Scoping Documentation (see section *5.4 Critical Systems Scope and template*) will form the scope for the CAF for Aviation self-assessment and therefore the ASSURE Cyber Audit.

A suggested Statement of Work for an ASSURE Cyber Audit may consider the following:

- Number of **critical systems** in scope and any grouping.
- Number of **documents compiled as evidence** for the CAF for Aviation self-assessment by the aviation organisation, as these will need to be reviewed.
- Number of **people** in the aviation organisation who **provided evidence or contributed** to the CAF for Aviation self-assessment, as they may need to be interviewed.
- Number of **locations** that may need to be visited, whilst review of documents might in part be carried out remotely, it is likely most of the work will have to be on-site.
- Expectations around **hours required** to complete the audit and **period allocated** by the aviation organisation to ensure all relevant contacts can be interviewed.

In some cases, ASSURE Cyber Audits may be required in response to a change or with a more limited scope. In these cases, the scope will be agreed between the CAA and the aviation organisation, however the critical system scope and CAF for Aviation will still form the basis of the ASSURE Cyber Audit.

5. ASSURE Cyber Audit

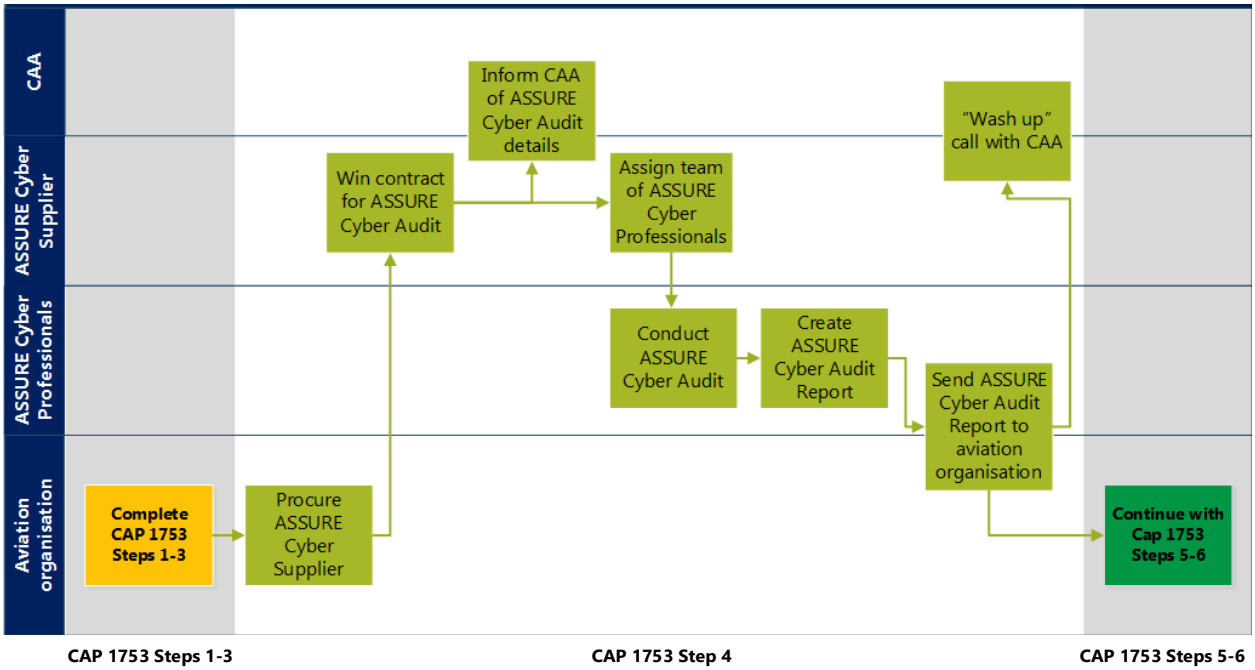

Figure 4: ASSURE Cyber Audit Process Overview, CAP 1753 Step 4 (See Annex A: Checklists for Cyber Suppliers)

5.1 Composition of the Audit Team

As part of an ASSURE application (see section *3.3 ASSURE Accreditation Process*), an ASSURE Cyber Supplier must register the names of all prospective ASSURE Cyber Professionals (employees and/or contractors) within their organisation. Registered individuals must qualify for one of the three ASSURE Specialisms (as shown in section *5.3 ASSURE Specialisms*) and to support this, must provide evidence of the associated qualifications.

All ASSURE Cyber Audit teams provided by an ASSURE Cyber Supplier, for a contracting aviation organisation, must collectively hold registrations across *all* three ASSURE Specialisms (e.g., if there are two ASSURE Cyber Professionals on the audit team, at least one of those individuals must hold, and be registered for two ASSURE Specialisms).

Note: It is possible for one ASSURE Cyber Professional to be registered for more than one specialism, however for resilience purposes, there is an expectation that an ASSURE Cyber Supplier registers more than one ASSURE Cyber Professional in total.

At the discretion of the ASSURE Cyber Supplier and the contracting aviation organisation, it is possible for non-ASSURE registered individuals to be deployed on an ASSURE Cyber Audit team alongside registered ASSURE Cyber Professionals. Unregistered individuals cannot sign off any ASSURE Cyber Audit deliverables.

5.2 ASSURE Specialisms

ASSURE Specialism	Required Qualifications
Cyber Audit & Risk Management	One of: • ISO27001 Lead Auditor • NCSC CCP - Security and Information Risk Advisor (SIRA) – Senior Practitioner • NCSC CCP – Cyber Security/IA Auditor – Senior Practitioner • ISACA - Certified Information Security Auditor (CISA)
Technical Cyber Security Expert	One of: • ISC2 - Certified Information Systems Security Professional (CISSP) • CREST Certified Penetration Tester • CREST Certified Infrastructure Tester • CREST Certified Web Applications Tester • CREST Certified Simulated Attack Specialist • CREST Certified Simulated Attack Manager • CREST Certified Intrusion Analyst • NCSC CCP - Cyber Security/IA Architect - Senior Practitioner • Cyber Scheme Team Leader (CSTL) • TigerScheme CHECK Team Leader (CTL/SST)
Industrial Control Systems/Operational Technology Expert	One of: • ISA99/IEC 62443 - Cyber Security Expert (2 or more certificates will be considered) • Information Assurance Certification Review Board - Certified ICS/SCADA Security Architect (CSSA) • SANS - Global Industrial Cyber Security Professional certification (GICSP) • ISA - Certified Automation Professional (CAP) OR: • Evidence of at least 5 years' experience with ICS/OT and responsibilities relating to cyber security e.g., performing security audits or penetration testing, aviation experience is preferable but not essential if experience in other relevant critical infrastructure sectors can be demonstrated. • Evidence of at least 5 years showing varied and deep knowledge of critical systems and ICS/OT in a security context such as from research or academia. CVs should be attached as part of the ASSURE application.

5.3 Supporting Audit Documentation

The ASSURE Cyber Audit team is expected to be familiar with the aviation organisation's critical systems scope and will be required to complete sections of the CAF for Aviation, both will be made available by the aviation organisation during the ASSURE Cyber Audit.

All critical systems lists and diagrams should be referred to when auditing the aviation organisation's CAF for Aviation self-assessment to ensure that it corresponds to the identified scope. If the provided responses/evidence do not support the systems identified within the critical systems scope, then this must be documented and challenged.

Please be aware that conditions apply to the ASSURE Cyber Audit in relation to the critical systems scope (see section *5.7 ASSURE Cyber Audit Conditions*). Checklists have been created to assist in the completion of an ASSURE Cyber Audit (see *Annex A*: *Checklists for ASSURE Cyber Suppliers*)

5.4 Critical Systems Scope and Template

The CAA developed the Cyber Security Critical System Scoping Guidance (CAP 1849) and template to assist aviation organisations in the identification and documentation of their network and information systems, that are critical to the provision of key essential services and functions. Aviation organisations can follow the Critical System Scoping Guidance, or use an alternative approach of their choice. The methodology used to identify critical systems will be agreed with the CAA prior to completion of the CAF for Aviation.

Aviation organisations are required to use the Critical Systems Scoping Template to document their critical systems, related information (e.g., a system description) and where they have grouped any systems. Aviation organisations are also required to produce diagrams showing the security boundary of the identified critical systems. Further information can be found in CAP 1849 Critical Systems Scoping Guidance.

The list of critical systems and associated diagrams (clearly identifying the security boundary) detailed in the Critical Systems Scoping Template, will form the scope for the CAF for Aviation self-assessment and therefore the ASSURE Cyber Audit. As such, at the beginning of any ASSURE Cyber Audit, the ASSURE Cyber Professionals should review the list of critical systems and diagrams provided by the aviation organisation to ensure the scope has been applied consistently.

The Critical System Scoping Guidance and template can be found on the CAA's website[8].

[8] https://publicapps.caa.co.uk/cap1849

5.5 CAF for Aviation

The ASSURE Cyber Supplier should refer to CAP 1850 'CAF for Aviation Guidance'[9] when providing their validated opinion against an aviation organisation's CAF for Aviation self-assessment.

The CAF for Aviation and corresponding CAF for Aviation Guidance is available via the CAA website[10], please pay particular attention to the relevant ASSURE columns and the Summary (ASSURE AUDIT) tab.

5.6 CAF for Aviation Evidence & Good Practice

The CAA has developed guidance on the appropriate forms of evidence at a principal level (CAP 1850- Annex B). This guidance should *not* be treated as a checklist and ASSURE Cyber Professionals will be expected to assess the detail and status of evidence at an IGP (Indicators of Good Practice) level. The examples provided are non-exhaustive and are only indicative of the type of evidence deemed appropriate by the CAA.

In some cases, an aviation organisation may provide evidence of alternate good practice which they believe meets a Contributing Outcome but is not detailed in the IGP list. The ASSURE Cyber Professional can use their expert judgement to accept the alternate evidence and must provide strong narrative evidence for this in the related CAF for Aviation ASSURE columns.

Timeliness of evidence, in relation to the nature and type of control they are associated with, must be considered by the ASSURE Cyber Professionals in deciding whether evidence supports a Contributing Outcome. Suggested guidance for this can be found in ISO27004 Annex B and NIST 800-55 Rev1 Appendix A.

Where evidence relates to Principle A4 Supply Chain, the correct permissions should be obtained to review supplier sensitive or specific information such as completed assurance reports or contracts. Where this is not possible, evidence of the process used should be reviewed, such as templates for supplier assessments, contracts and security requirements, as well as policies on how data shared with suppliers is secured and tracked.

During the ASSURE Cyber Audit, the ASSURE Cyber Professionals must complete the relevant ASSURE sections in the CAF for Aviation, and for each Contributing Outcome, select a response ('achieved', 'partially achieved' or 'not achieved') based on their **expert opinion**. In the related ASSURE columns, the ASSURE Cyber Professionals must detail the relevant observations, evidence, controls, guidance, standards or good practice that was evaluated to form their validated opinion.

---

[9] https://www.caa.co.uk/cap1850

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

5.7 ASSURE Cyber Audit Report and Template

The CAA have created an ASSURE Cyber Audit Report Template which can be obtained once an ASSURE Cyber Supplier is accredited. Where this hasn't been provided on accreditation, it can be obtained by emailing cyber@caa.co.uk. Template. The CAA is equally content for companies to use their own templates as long as it includes the same data points:

- Name of aviation organisation and ASSURE Cyber Supplier, accreditation number;
- report approval date and, date and duration of the audit;
- name of all ASSURE Cyber Professionals conducting the audit and their signatures;
- list of audit activities including evidence reviewed and interviews conducted;
- date of scheduled 'wash-up' call with the CAA;
- as per the template, all clauses on the Independent ASSURE Cyber Professionals' Report to the Civil Aviation Authority (CAA);
- Executive Summary;
- confirmation of whether the aviation organisation's CAF for Aviation encompasses the critical systems scope the organisation has defined through their critical systems scope template and diagrams;
- list of Contributing Outcomes that have been met through the aviation organisation providing alternative evidence and IGPs;
- summary of an aviation organisation's Contributing Outcomes and audit observations, highlighting any deviations from the self-assessment;
- summary table showing aviation organisation's self-assessment and ASSURE Audit assessment of Contributing Outcome achievement;
- and if applicable any Recommendations.

On completion of the ASSURE Cyber Audit the ASSURE Cyber Supplier must:

- Ensure the ASSURE sections of the CAF for Aviation are **completed**;
- ensure the ASSURE Cyber Audit Report is completed and **signed** by the ASSURE Cyber Professionals that conducted the ASSURE Cyber Audit;
- **agree** the final report with the aviation organisation before issuing;
- securely **issue** the ASSURE Cyber Audit Report to the associated aviation organisation following their instructions;
- **conduct** a 'wash-up' call with the CAA to provide a high-level summary and an opinion on how the ASSURE Cyber Audit went; and
- securely **dispose** of the ASSURE Cyber Audit Report and associated material, following relevant aviation organisation requirements or company policy.

Multiple ASSURE Cyber Audit Reports should not be stored unless approval has been given as part of your accreditation by the CAA. If you are unsure please contact the CAA at cyber@caa.co.uk.

Once the aviation organisation has received the completed ASSURE Cyber Audit Report, they will submit it to the CAA as part of the provisional Statement of Assurance, as detailed in CAP 1753.

5.8 ASSURE Cyber Audit Conditions

The ASSURE Cyber Audit is an independent validation of the aviation organisation's self-assessment conducted by the ASSURE Cyber Supplier. The results of the ASSURE Cyber Audit do not constitute any approval or decision by the ASSURE Cyber Supplier as to the aviation organisation's compliance or overall adequacy with applicable regulatory requirements in scope of the CAA's Cyber Security Oversight Process (see CAP 1753). Decisions relating to an entity's compliance with the regulatory requirements can only be made by the CAA as competent authority.

The ASSURE Cyber Audit must:

- Be **fact** based, **impartial** and conducted with the highest level of **integrity**;
- ensure **consistency** between the list of critical systems and the security boundary in the diagrams provided by the aviation organisation, with the scope used for the CAF for Aviation self-assessment, *any* discrepancies must be documented;
- be **evidence**-based by observing processes in practice, sampling, conducting interviews, and reviewing policies and other relevant documentation provided by the aviation organisation;
- include an **expert opinion** of 'achieved', 'partially achieved', 'not achieved' or 'not relevant' with associated commentary against each CAF for Aviation Contributing Outcome in the ASSURE columns;
- include, at the aviation organisation's discretion, **recommendations**, **mitigations**, **remediations** or **good practice**; and
- **adhere to the latest guidance** produced by CAA, not limited to but including, CAP 1753, CAP 1849 and CAP 1850.

The ASSURE Cyber Supplier and/or the ASSURE Cyber Professionals must not:

- Complete an ASSURE Cyber Audit where there is a **conflict of interest**;
- seek to **alter,** by increasing or decreasing, the critical systems scope as defined by the associated aviation organisation;
- perform any type of **testing** (e.g., penetration testing) during an ASSURE Cyber Audit, unless otherwise explicitly agreed by the aviation organisation;
- **amend** in any way an aviation organisation's completed parts of the CAF for Aviation self-assessment; or
- set **expectations** on levels of achievement for aviation organisations; or
  provide confirmation on whether an aviation organisation is complying with the Cyber Security Oversight Process or is compliant with any or all applicable aviation regulatory requirements.

5. Complaints

All complaints should be directed to CREST at assure@crest-approved.org who will inform the CAA. Together we will investigate a complaint in line with CREST Company Complaints Process and the ASSURE Addendum. All complaints will be investigated in a competent, diligent and impartial manner, resulting in a CREST Recommendation Report. Further details can be found in section *2.5 Complaints in Annex B.*

The CAA may take action including, but not limited to, the following:

i) Immediate provisional suspension of ASSURE accreditation pending investigation;
ii) Revocation of ASSURE accreditation following investigation;
iii) Where the CAA considers individual members of staff are not fit or competent to carry out ASSURE Cyber Audits on behalf of any ASSURE Cyber Supplier the CAA will indicate to ASSURE Providers that, in order to retain ASSURE accreditation, such members of staff are not permitted to undertake ASSURE Cyber Audits.

5.1 Dispute Resolution

Where there is a dispute regarding the findings or assessment of an ASSURE Cyber Audit, the aviation organisation and ASSURE Cyber Supplier should first try to resolve the dispute directly. If no resolution can be reached the aviation organisation or ASSURE Cyber Supplier should notify the CAA Cyber Security Oversight Team by emailing cyber@caa.co.uk. The CAA will then contact the relevant parties and review the dispute, requesting further detail where necessary, and come to a decision. The CAA will then communicate the rationale and decision to the aviation organisation and ASSURE Cyber Supplier.

Annex A: Checklists for ASSURE Cyber Suppliers

Accreditation

- ☐ As a potential ASSURE Cyber Supplier, you will need to complete the **ASSURE Application Form via the CREST membership portal**
- ☐ Sign up to the CREST Code of Conduct.
- ☐ Sign the **ASSURE Addendum** provided by CREST.
- ☐ Provide **two to three client references** to support the cyber security service you have detailed.
- ☐ Provide requested supporting documentation such as policies.
- ☐ Register **ASSURE Cyber Professionals** in all three specialisms and where applicable provide any required supporting documentation (e.g., CVs).

Once approved, Accredited ASSURE Cyber Suppliers will be provided by CREST with:

- ☐ CAA ASSURE accreditation number.
- ☐ CAA ASSURE logo and CAA ASSURE Branding Guidelines.

Before conducting an ASSURE Cyber Audit

- ☐ Read the **CAA's guidance**- https://www.caa.co.uk/Commercial-industry/Cyber-security-oversight/Cyber-security-compliance/
- ☐ Review this CAA ASSURE Scheme CREST **Implementation Guide**.
- ☐ If needed, request a copy of the **ASSURE Cyber Audit Report Template** from cyber@caa.co.uk.
- ☐ Email the CAA at cyber@caa.co.uk to **provide the dates and locations** of the ASSURE Cyber Audit, the name of the aviation organisation, and to book a **'wash-up' call** with the CAA.

ASSURE Cyber Audit

- ☐ Complete CAF for Aviation **ASSURE columns**, ensuring there is a strong narrative to support your response for each outcome, based on a set of observations, documentation and evidence as to whether the aviation organisation meets the Contributing Outcomes they have self-assessed.
- ☐ Ensure the CAF for Aviation **Summary (ASSURE Audit) tab** is complete.
- ☐ ASSURE Cyber Professionals to **complete and all sign** the ASSURE Cyber Audit Report either using the template or covering all the data points required (see section *5.7 ASSURE Cyber Audit Report and Template*).
- ☐ Provide the audited CAF for Aviation and the ASSURE Cyber Audit Report **securely** to the aviation organisation.

- Once the ASSURE Cyber Audit Report is complete and has been sent to the aviation organisation, conduct your **scheduled 'wash- 'up call** with the CAA.
- Communicate to the CAA any **feedback** that will improve the ASSURE Scheme.

CODE OF CONDUCT FOR ASSURE PROVIDERS

ADDENDUM TO CREST CODE OF CONDUCT

Document Reference	
Version Number	2.0
Status	Final
Issue Date	6th August 2020
Review Date	

CREST (International)
The Porter Building, 1 Brunel Way, Slough, Berkshire, SL1 1FQ
Tel: +44 (0)20 3058 3122 | www.crest-approved.org

Version History

Version	Date	Authors	Status
0.1	18/04/2019	Matthew Bristow	Initial Draft
1.0	06/06/2019	Matthew Bristow	Finalised following final review
2.0	05/08/2020	Sabrina Brookfield	Clarified Qualified Entity status.

Document Review

Reviewer	Position
President	CREST Executive
Chairman	CREST Executive
Head of Cyber Security Oversight	CAA Management

Table of Contents

1. INTRODUCTION

1.1 Purpose

1.1.1 This document is an Addendum to the CREST Code of Conduct and describes additional standards of practice required of CREST Accredited Providers in order to be accredited by the Civil Aviation Authority (CAA), and to maintain accreditation, as an ASSURE Cyber Supplier under the ASSURE Discipline for Aviation Cyber Security.

1.1.2 Becoming an accredited ASSURE Cyber Supplier means that the organisation will also be accredited as a Qualified Entity and when assessing entities under the European aviation safety framework, they will complete ASSURE Cyber Audits on behalf of the CAA as a Qualified Entity.

1.1.3 All revisions to this Addendum will be notified to ASSURE points of contact in CREST Member Companies.

1.2 Definitions

1.2.1 "ASSURE" means the discipline which is a mechanism for accrediting Cyber Suppliers to conduct Cyber Audits of aviation organisations on behalf of the Civil Aviation Authority.

1.2.2 "ASSURE Cyber Audit" means a Cyber Security Audit conducted by an ASSURE Accredited CREST Member for an aviation organisation.

1.2.3 "ASSURE Cyber Supplier", in the context of this Code of Conduct, means a CREST Member Company who has passed all the relevant requirements to become a CREST member and to be accredited under the ASSURE Discipline, has paid any fees associated with membership, has agreed to the CREST Code of Conduct and this ASSURE Addendum.

1.2.4 "ASSURE Cyber Professional" in the context of this Code of Conduct, means an ASSURE Cyber Supplier's member of staff who has been accredited in one or more of the three Specialisms required to perform ASSURE Cyber Audits.

1.2.5 "ASSURE Application Form" means the latest completed CREST Application Form for the ASSURE Discipline and associated reference material reviewed and agreed by CREST and the CAA. Any reports to the Member Company of minor compliance issues will also be considered as being part of the application.

1.2.6 "Aviation organisation" means Aerodromes, Airlines or Air Traffic Management Organisations employing an ASSURE Cyber Supplier to conduct an ASSURE Cyber Audit.

1.2.7 "Member of staff" means personnel employed directly by the ASSURE Cyber Supplier and any personnel engaged through a sub-contractor.

1.2.8 "Qualified Entity" means an ASSURE Cyber Supplier accredited by the UK Civil Aviation Authority in accordance with Article 69 and Annex VI of REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ("the EASA Basic Regulation) , to carry out certain specified cyber security oversight tasks on the CAA's behalf under the EASA Basic Regulation and implementing regulations.

1.3 Description

1.3.1 This document specifies additional standards of practice for ASSURE Cyber Suppliers. It does not replace the CREST Code of Conduct which must be signed and adhered to in parallel by ASSURE Cyber Suppliers.

1.3.2 ASSURE Cyber Suppliers will need to ensure that the policies and procedures described in the ASSURE Application Form have been implemented correctly.

1.3.3 There may be situations where there is a misunderstanding or dispute between an ASSURE Cyber Supplier and the aviation organisation, this document defines the amendments that apply to the standard CREST Complaints and Resolution Measures for this eventuality.

1.4 Scope

1.4.1 In Scope

i) The ASSURE Code of Conduct applies to ASSURE Cyber Suppliers engaged by aviation organisations to conduct ASSURE Cyber Audits.

1.4.2 Out of Scope

i) This ASSURE Code of Conduct applies only to companies who are, or are seeking to be accredited as, ASSURE Cyber Suppliers.

ii) This document does not apply to any services provided by CREST Member Companies other than ASSURE Cyber Audits.

1.5 Disclaimer

1.5.1 CREST and the CAA accept no responsibility for the accuracy or validity of assertions or claims made by CREST Member Companies in their ASSURE Application Form.

1.5.2 CREST and the CAA prescribes the method and rigor by which services should be conducted and does not underwrite the result of the services provided by ASSURE Cyber Suppliers.

1.5.3 Any reference to another organisation's website does not constitute a recommendation or endorsement of that organisation, site or its content by CREST or the CAA.

2. ASSURE Cyber Supplier REQUIREMENTS

2.1 ASSURE Accreditation

2.1.1 ASSURE Member Companies must demonstrate that they meet the requirements for ASSURE accreditation by completing the ASSURE Application Form, which will be reviewed by both CREST and the CAA as part of the accreditation process. With the final decision being made by the CAA. ASSURE Cyber Suppliers must ensure that all members of staff responsible for the management of or undertaking ASSURE Cyber Audits are made aware of the policies, procedures and obligations in the Company's completed ASSURE Application Form including but not limited to:

i) Ensuring that members of staff are aware of the additional ASSURE Data Handling Requirements;

ii) Ensuring that members of staff are aware of their responsibilities to the CAA, including full disclosure of information and the independent findings relating to ASSURE Cyber Audits, and ensuring compliance with any applicable laws.

iii) Ensuring that members of staff are aware of their responsibilities to notify the CAA in the event of a Conflict of Interest.

2.1.2 Members of staff that qualify for ASSURE Specialisms must be listed in the ASSURE Application Form. This form must be re-submitted for new members of staff.

2.2 ASSURE Cyber Audit

All ASSURE Cyber Supplier and ASSURE Cyber Professionals must conduct ASSURE Cyber Audits in accordance with the following:

2.2.1 The ASSURE Cyber Audit must be conducted in accordance with this Code of Conduct, including the Addendum, and the ASSURE Implementation Guide.

2.2.2 The ASSURE Cyber Audit must be based on the Cyber Assessment Framework (CAF) for Aviation and the ASSURE Cyber Audit Report template provided by the CAA.

2.2.3 ASSURE Cyber Audits must constitute an independent and objective evaluation of the client aviation organisation. ASSURE Cyber Professionals will not misrepresent, doctor or withhold information and findings relating to the ASSURE Cyber Audit from the CAA, whether at the request of the aviation organisation or otherwise.

2.2.4 The ASSURE Cyber Supplier will provide to the CAA, upon request, any information obtained from the client aviation organisation as part of the ASSURE Cyber Audit. Contracts between the aviation organisation and the ASSURE Cyber Supplier must not contain any provisions which seek to limit the CAA's access to information relating to the ASSURE Cyber Audit.

2.2.5 Subject to paragraph 2.2.4, ASSURE Cyber Suppliers and ASSURE Cyber Professionals must protect, from unauthorised disclosure, any confidential or commercially sensitive information acquired or reviewed when carrying out an ASSURE Cyber Audit on behalf of the CAA.

2.2.6 All ASSURE Specialisms must be represented in the team deployed to conduct ASSURE Cyber Audits. This means the team must be made up of professionals that between them hold CREST registrations for all ASSURE Specialisms (specified on the ASSURE Application Form).

2.2.7 The ASSURE Cyber Suppliers must participate in a 'wash-up' call with the CAA and be open and honest when responding to queries and challenges.

2.2.8 The results of the ASSURE Cyber Audit do not constitute any approval or decision by the ASSURE Cyber Supplier as to the aviation organisation's compliance or overall adequacy with applicable regulatory requirements in scope of the CAA's Cyber Security Oversight Process (see CAP 1753). Decisions relating to an entity's compliance with the regulatory requirements can only be made by the CAA as competent authority.

2.3 Conflict of Interest

Conflicts of interest must be handled as follows:

2.3.1 ASSURE Cyber Suppliers will seek to avoid any situation that may give rise to a conflict of interest between them, the aviation organisation or the CAA. Examples of potential conflicts of interest include but are not limited to:

i) An ASSURE Cyber Supplier having interests in products or services covered under the scope of an ASSURE Cyber Audit;

ii) An ASSURE Cyber Supplier conducting an ASSURE Cyber Audit for an aviation organisation for whom they have implemented or consulted on any of the Cyber elements covered in the scope of the Audit;

iii) Personal relationships between members of staff responsible for the management of or undertaking ASSURE Cyber Audits and staff within the aviation organisation.

2.3.2 ASSURE Cyber Suppliers must notify the CAA if they become aware of or suspect an actual or potential conflict of interest. Failure to notify will constitute a breach of this ASSURE Code of Conduct.

2.4 Data Handling

ASSURE Cyber Suppliers must comply with the following additional data handling standards:

2.4.1 The ASSURE Cyber Suppliers should ensure that it holds only the information pertaining to the aviation organisation's ASSURE Cyber Audit that is absolutely required. Where possible information should be accessed on the client aviation organisation's infrastructure.

2.4.2 Where more than one completed ASSURE Cyber Audit Report is held on the ASSURE Cyber Supplier's system, this constitutes an 'aggregation of information' to the extent that additional security controls are required. ASSURE Cyber Suppliers are first and foremost requested to avoid holding two completed ASSURE Cyber Audit Reports and related information at the same time and to ensure all members of staff are aware of and adhere to the data retention and disposal policies in place to ensure this.

2.4.3 Where it is considered operationally unfeasible for an ASSURE Cyber Supplier to avoid holding more than one completed ASSURE Cyber Audit on their infrastructure concurrently (see 2.4.2), the ASSURE Cyber Supplier must agree additional security measures with the CAA and/or NCSC as well as providing details of the infrastructure that will be used. ASSURE Cyber Suppliers must ensure that all members of staff are aware of and adhere to any additional security measures agreed.

2.4.4 The ASSURE Cyber Suppliers must notify the CAA in the event of non-compliance with these data handling requirements.

2.4.5 The ASSURE Cyber Supplier may be subject to Audit by CAA personnel to ensure compliance with these requirements.

2.5 Complaints

The Complaints process for ASSURE is aligned with the standard CREST Complaints and Resolution Measures outlined in the CREST Code of Conduct, with the following additions:

2.5.1 Where the complaint relates to the delivery of an ASSURE Cyber Audit, the CAA will be notified of the complaint and will participate, alongside the CREST President, in the review of the complaint; the review of the associated evidence gathered by CREST; and the Member Company's Response.

2.5.2 The CAA will participate, alongside the CREST President, in the production of the resultant Recommendation Report to the ASSURE Cyber Supplier and the Summary Report to the client aviation organisation.

2.5.3 If on considering an application for ASSURE accreditation the CAA is not satisfied that the applicant can or will comply with the requirements for ASSURE accreditation, the CAA may refuse the application.

2.5.4 If the CAA is not satisfied that the ASSURE Cyber Supplier is complying with the requirements for ASSURE accreditation, the CAA may take action including, but not limited to, the following:

iv) Immediate provisional suspension of ASSURE accreditation pending investigation;

v) Revocation of ASSURE accreditation following investigation;

vi) Where the CAA considers individual members of staff are not fit or competent to carry out ASSURE Cyber Audits on behalf of any ASSURE Cyber Supplier the CAA will indicate to ASSURE Providers that, in order to retain ASSURE accreditation, such members of staff are not permitted to undertake ASSURE Cyber Audits.

Where a Company applies for ASSURE accreditation and has previously held an ASSURE accreditation that was suspended or revoked, the CAA may take this into account in considering whether it can be satisfied of the entities' appropriateness to be re-accredited.

2.5.5 Where the complaint relates to an ASSURE Cyber Supplier but is not related to the delivery of an ASSURE Cyber Audit, the CAA will be party to information including the nature of the Complaint and the CREST Recommendation Report (redacted to avoid disclosure of details of the client). The CAA will consider whether any further action is required including that set out at 2.5.4.

3 SIGNATURES

3.1 Your signature below indicates your acceptance of these terms.

	CREST		**COMPANY**
Signature:		Signature:	
Print Name:		Print Name:	
Title:		Title:	
Date:		Date:	

CREST and the CAA reserve the right to update the Codes of Conduct Addendum and require ASSURE Cyber Suppliers to re-sign as a condition of their continued accreditation.