Table of Contents

[1. Introduction 2](#_Toc74558837)

[2. Cyber Audit Service and Contact Details 2](#_Toc74558838)

[3. ASSURE References 2](#_Toc74558839)

[4. Conducting Cyber Audits 5](#_Toc74558840)

[5. Data Handling 8](#_Toc74558841)

[6. Cyber Professional Registration 10](#_Toc74558842)

[7. Signatures 12](#_Toc74558843)

## 1. Introduction

**The ASSURE Scheme is a mechanism for accredited Cyber Suppliers to conduct Cyber Audits of Aviation Organisations on behalf of the Civil Aviation Authority. Before completing this form, you should have read and understood the ASSURE Supplier requirements including the CAA ASSURE scheme IASME Consortium implementation guide.**  
  
**Any questions relating to the ASSURE Scheme and Aviation Cyber Security Oversight should be sent to** [**info@iasme.co.uk**](mailto:assure@iasme.co.uk)

## 2. Cyber Audit Service and Contact Details

|  |  |
| --- | --- |
| **Main contact name:** |  |
| **Trading address of the organisation as listed at Company house:**  **(Must be U.K. based organisation)** |  |
| **Contact telephone number:** |  |
| **Contact Email:** |  |
| **Web link for cyber audit services:** |  |
| **Service description overview:**  **The IASME website is a regular source of information for potential customers. The information provided below should detail your organisation’s Cyber Audit services.** |  |

## 3. ASSURE References

**This section is for providing references that demonstrate your organisation’s capability to deliver ASSURE Cyber Audits. Please Note Aviation Industry experience is desirable but not essential if you can demonstrate having delivered services in similar contexts comprising IT and OT components.**

|  |
| --- |
| **3** **(i). Does your organisation have a track record of delivering Cyber Audit, Consultancy and/or testing services to the Aviation Industry?** |

* Yes
* No

|  |
| --- |
| **3** **(ii). For how many years have you been delivering these services to the Aviation Industry?** |

* < 3
* 3-5
* 5-10
* <10

|  |
| --- |
| **3** **(iii). Does your organisation have a track record of delivering Cyber Audit, Consultancy and/or testing servers in environments comprising both IT and OT components?** |

* Yes
* No

|  |
| --- |
| **3** **(iv). For how many years have you been delivering these services?** |

* < 3
* 3-5
* 5-10
* <10

|  |
| --- |
| **3** **(v). Please provide details of up to three client references for whom you have provided the Cyber Security Services above, please also provide details of the services provided. Supporting documentation may be uploaded.** |

|  |  |
| --- | --- |
| **Reference No. 1** | |
| **Organisation:** |  |
| **Contact name:** |  |
| **Address:** |  |
| **Contact title:** |  |
| **Contact telephone number:** |  |
| **Contact Email:** |  |
| **Services provided:** |  |
| **Date:** |  |
| **Any other notes:** |  |

|  |  |
| --- | --- |
| **Reference No. 2** | |
| **Organisation:** |  |
| **Contact name:** |  |
| **Address:** |  |
| **Contact title:** |  |
| **Contact telephone number:** |  |
| **Contact Email:** |  |
| **Services provided** |  |
| **Date:** |  |
| **Any other notes:** |  |

|  |  |
| --- | --- |
| **Reference No. 3** | |
| **Organisation:** |  |
| **Contact name:** |  |
| **Address:** |  |
| **Contact title:** |  |
| **Contact telephone number:** |  |
| **Contact Email:** |  |
| **Services provided** |  |
| **Date:** |  |
| **Any other notes:** |  |

## 4. Conducting Cyber Audits

|  |
| --- |
| **4** **(i). Does your organisation commit to conducting ASSURE Cyber audits in accordance with the standards, procedures and templates outlined in the CAA ASSURE scheme IASME Consortium implementation guide?** |

* Yes
* No

|  |  |
| --- | --- |
| 4 (ii). Please provide details as to how you will ensure employees or contractors are suitably trained on the ASSURE standards, procedures, and the required deliverables as part of their induction or prior to their deployment on ASSURE Cyber Audits. | |
|  | |
| **Supporting document evidence provided?** | * Yes * No |

|  |  |
| --- | --- |
| 4 (iii). Can your organisation commit to resourcing ASSURE Cyber Audits such that all ASSURE Specialisms are represented in the Audit Team? This means the team must be made up of professionals that between them hold qualification for all ASSURE Specialisms (See 6. Cyber Professionals). | * Yes * No |
| **4 (iv). Please describe how your resourcing model supports this (incl. caveats)** | |
|  | |
| **Supporting document evidence provided?** | * Yes * No |

|  |  |
| --- | --- |
| 4 (v). Please confirm that ASSURE Cyber Audit Reports produced by your Organisation will be signed by the registered ASSURE Cyber Professionals that conducted the Audit. | |
| **Confirmation?** | * Yes * No |

|  |  |
| --- | --- |
| 4 (vi). Please confirm that your organisation understands its obligations to the CAA under the ASSURE scheme. In so far as ASSURE Cyber Audit reports must constitute an independent and objective evaluation of the Client Aviation Organisation. ASSURE Member Companies must not misrepresent, doctor, or withhold information and findings relating to the Cyber Audit from the CAA, whether at the request of the Aviation Organisation or otherwise. | |
| **Confirmation?** | * Yes * No |

|  |
| --- |
| 4 (vii). Please describe how your internal governance, quality assurance and escalation routes will enforce this. |
|  |

|  |  |
| --- | --- |
| 4 (viii). Please confirm that employees or contractors deployed in Cyber Audits will be available to participate in a “wash-up call” with the CAA. | |
| **Confirmation?** | * Yes * No |

|  |  |
| --- | --- |
| 4 (ix). The results of the Cyber Audit do not constitute any judgement by your organisation as to the Aviation Organisation’s compliance with the CAA’s Cyber Oversight Regulation or the overall adequacy of their Cyber Security from a legal and regulatory standpoint. This judgement can only be made by the CAA. Please confirm you acknowledge and understand this. | |
| **Confirmation?** | * Yes * No |

|  |
| --- |
| 4 (x). Please describe your process for agreeing the scope of the audit with the client and how this agreement will be documented and recorded. |
|  |

|  |
| --- |
| 4 (xi). Please describe how you will communicate and keep the client informed throughout the audit on progress and findings. |
|  |

|  |
| --- |
| 4 (xii). Please describe your process for managing the risks that may prevent an individual audit from being completed or achieving its objectives. |
|  |

|  |
| --- |
| 4 (xiii). Please describe your process for maintaining and improving auditor competence |
|  |

## 5. Data Handling

|  |  |
| --- | --- |
| 5 (i). Please confirm your organisation will hold only the information pertaining to the Aviation Organisation’s Cyber Audit that is absolutely required. | |
| **Confirmation?** | * Yes * No |
| **5 (ii). Where information must be held off client infrastructure, please specify how you will store this?** |  |

|  |
| --- |
| 5 (iii). Please specify how you will transmit this data. |
|  |

|  |  |
| --- | --- |
| 5 (iv). Please provide a copy of your data retention and disposal policy for client information. | |
| **Supporting document evidence provided?** | * Yes * No |

|  |  |
| --- | --- |
| 5 (v). Where more than one completed ASSURE Cyber Audit Report is held on your organisation’s system this constitutes and “aggregation of information “to the extent that additional controls are required. Is it operationally feasible for you to ensure two completed audits are not stored on your infrastructure at the same time? | * Yes * No |
| **5 (vi). If yes,** please provide details of the measures your organisation will take to ensure this? | |
|  | |
| **Supporting document evidence provided?** | * Yes * No |
| **5 (vi). If no,** please provide contact details of the person within your organisation authorised to discuss you security infrastructure and additional controls with a representative from the CAA and/or NCSC: | |
| **Contact name:** |  |
| **Contact telephone number:** |  |
| **Contact Email:** |  |

## 6. Cyber Professional Registration

**There are currently three Cyber Specialisms under the ASSURE Framework. All of which must be represented on any ASSURE Cyber Audit. It is possible for one individual to be registered for more than one Specialism but there is an expectation there will be more than one name listed for reconciliation purposes. The table below lists the qualification requirements for a Cyber Professional to be registered under each Specialism.**  
  
**For the initial wave of Cyber Audits the CAA will provide personnel as part of Cyber Audit teams to provide Aviation Sector expertise. However, this is likely to become a specialism for which your staff can be accredited in future.**

|  |  |
| --- | --- |
| **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 Infrastructure Tester * Certified CREST Intrusion Analyst * Cyber Scheme Team Leader (CSTL) * TigerScheme CHECK Team Leader (CTL/SST) * NCSC CCP - Cyber Security/IA Architect - Senior Practitioner |
| **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. |

|  |  |
| --- | --- |
| Complete for **Cyber Audit & Risk Management** cyber professional/s: | |
| **Name/s** |  |
| **Qualification/s (Incl. Ref)** |  |
| **Other Qualifying Factors** |  |
| **\*Supporting Document Submitted** | * Yes * No |

|  |  |
| --- | --- |
| Complete for **Technical Cyber Security Expert** cyber professional/s: | |
| **Name/s** |  |
| **Qualification/s (Incl. Ref)** |  |
| **Other Qualifying Factors** |  |
| **\*Supporting Document Submitted** | * Yes * No |

|  |  |
| --- | --- |
| Complete for **Industrial Control Systems/Operational Technology Expert** cyber professional/s: | |
| **Name/s** |  |
| **Qualification/s (Incl. Ref)** |  |
| **Other Qualifying Factors (Industrial ControlSystem/Operational Technology Expert only)** |  |
| **\*Supporting Document Submitted (Industrial Control System/Operational Technology Expert only)** | * Yes * No |

## 7. Signatures

**This form must be signed by a Director/Partner/Proprietor of the applicant’s business. By signing, you agree that your organisation and contact details provided in this form, will be listed on the IASME website if your application is successful.**

* Please check this box to confirm this statement.

**Sign below or upload electronic signature here:**

|  |  |
| --- | --- |
| **Name:** |  |
| **Position held:** |  |
| **Date:** |  |