Department for
Science, Innovation
& Technology

Office for Digital
Identities & Attributes

UK DIGITAL IDENTITY AND ATTRIBUTES

TRUST FRAMEWORK CERTIFICATION SCHEME

CONFORMITY ASSESSMENT BODY PERSONNEL SKILLS AND COMPETENCIES

VERSION 1.7

TABLE OF CONTENTS

1 VERSION HISTORY

Version	Date	Pages	Changes	Author
0.1	November 2023	All	From previous version of Document previously title 11 – Framework Auditor Competencies as issued by DCMS.	DSIT
1.1	November 2023	All	Updates as per review document and actions requested by UKAS. Additional extended content added by DSIT.	DSIT
1.2	March 2024	All	Updates to reflect actions issued by UKAS in the February review.	DSIT
1.3	April 2024	All	Updates to reflect outstanding actions from UKAS post March review.	DSIT
1.4	Sept 2024	All	Document name change. References to ‘Assessor’ replaced with ‘Auditor’.	DSIT
1.5	Oct 2024	All	Document format amended. Change of terminology from certification body to conformity assessment body.	DSIT
1.6	April 2025	p13	Addition specific to supplementary codes and specific and relevant standards as defined in the supplementary codes.	DSIT
1.7	May 2025	P11-12	Addition of word ‘review’ in two sections	DSIT

2 AUDITOR COMPETENCIES

2.1 REQUIREMENTS FOR AUDITORS

1 To assess a **SERVICE PROVIDER**'s compliance with the **UK DIGITAL IDENTITY AND ATTRIBUTES TRUST FRAMEWORK** (UK DIATF) to:

1.1 Provide impartial assessment and reports covering security investigations, information risk management and investment decisions to improve an organisation's information risk management,

1.2 Provide an independent opinion on whether cyber security/IA control objectives are being met within an organisation,

1.3 Identify a **SERVICE PROVIDER**'s systemic trends and weaknesses in security, and

1.4 Report and recommend responses to evaluation findings.

2.2 KEY SKILLS AND EXPERIENCE

1 It is recognised that **CONFORMITY ASSESSMENT BODIES** are likely to put audit teams together based on differing skills.

1.1 Specialist knowledge of Audit methodologies

1.2 Preferably ISACA/Certified Information Systems Auditor (CISA) or equivalent

2 One of the following:

2.1 ISO 27001 Lead Auditor

2.2 ISO 27701 Lead Auditor

2.3 ISO 22301 Lead Auditor

2.4 PCI/DSS Lead auditor

2.5 ISO9001 Lead Auditor

3 In addition, the **AUDITOR** acting as Team Leader on a particular certification should have participated in at least three complete **UK DIGITAL IDENTITY AND ATTRIBUTES TRUST FRAMEWORK** certifications.

4 *Note: Initially,* **CONFORMITY ASSESSMENT BODIES** *may be unable to identify individuals who fulfil the requirements relating to previous experience of UKDIATF* **EVALUATIONS***. In this instance the* **CONFORMITY ASSESSMENT BODY** *should be able to provide recorded evidence that justifies the use of its chosen* **AUDITORS** *and lead* **AUDITORS** *based on other, relevant experience.*

5 Nice to have:

5.1 Member of Institute of Internal Auditors

5.2 Certified Information Security Management System (ISMS) Lead or Principal Auditor by International Register of Certificated Auditors (IRCA)

6 Other skills required:

6.1 GPG 44 Strong knowledge to the extent that valid judgments on the scoring and level of confidence can be validated including the ability to determine the quality and protection offered by the Authentication method(s) provided by the **SERVICE** if applicable

6.2 GPG 45 Strong knowledge to the extent that valid judgments on the scoring and level of confidence can be validated

6.3 Ability to effectively assess whether presented evidence results in the correct scores being assigned in accordance with the Identity Profiles document

6.4 Knowledge of eIDAS

6.5 Knowledge of Digital Wallets/Personal Data Stores or other user-facing devices, software or apps that allow a user to collect, store, view, manage or share identity and/or attribute information and reuse it in multiple scenarios over time - if applicable to the **SERVICE**

6.6 Knowledge of different industry regulations such as Anti Money Laundering Regulations

6.7 In depth knowledge of UK GDPR and DPA 2018

6.8 Knowledge of vertical/horizontal auditing techniques

2.3 COMPETENCIES IN AUDIT TECHNIQUES

1 Capable of undertaking evaluations to verify compliance against identity, credential and attribute standards and profiles, security policies, standards, legal and regulatory requirements

2 Can verify that a **SERVICE PROVIDER**'s information processes meet the security criteria (requirements or policy, standards and procedures)

3 Uses **EVALUATION** processes and techniques to verify on-going conformance to security requirements

4 Is competent in conducting security compliance **EVALUATIONS** in accordance with an appropriate methodology and/or standard

5 Can demonstrate ability to conduct complex **EVALUATIONS** (e.g. involving multiple stakeholders, testing compliance against novel requirements or objectives.)

6 Is familiar with legal and regulatory requirements that could affect a **SERVICE PROVIDER**'s security policies

7 Is competent in performing **EVALUATIONS** that ensure security policies comply with all personal data protection laws and regulations relevant to the entity

8 Is competent in performing **EVALUATIONS** that ensure security policies support compliance with governance practices

2.4 COMPETENCIES IN RISK ANALYSIS AND RISK MANAGEMENT METHODS

1 Demonstrates in depth knowledge of information risk management methodologies such as:

1.1 ISO 27005 - Information Security Risk Management

1.2 ISO 31000 – Risk Management; Principles & Guidelines

1.3 A Risk Management Standard from The Institute of Risk Management

2.5 COMPETENCIES IN EVALUATION TECHNIQUES THAT ASSESS RISK

1 Competent in **EVALUATION** techniques that assess risks such as:

1.1 Threats & threat actors

1.2 Vulnerabilities

1.3 Privacy

1.4 Aggregation

1.5 Information assets and risk to asset values

2 Can identify assets that require protection

3 Can identify and assess relevant threats to the assets

4 Can identify exploitable vulnerabilities

5 Can assess the level of threat posed by potential threat agents

6 Has the competency to produce an Information Security risk assessment

7 Can report on the business impact of risk realisation

8 Can assess:

8.1 Risk appetite

8.2 Risk tolerance

8.3 Business risk

2.6 COMPETENCIES FOR ASSESSMENT OF SECURE SYSTEMS

1 Can evaluate Security Architectures and Patterns

2 Can evaluate Secure Development processes

3 Can evaluate lifecycle activities

4 Can evaluate and assess management responsibilities

5 Can assess business requirements

6 Is competent in evaluating architectural frameworks such as:

6.1 The Open Group Architecture Framework (TOGAF)

6.2 Zachman

7 Must understand and be capable of conducting **EVALUATIONS** that assess a range of core security technologies, including:

7.1 Access control models

7.2 Public and private encryption

7.3 Cryptographic methods

7.4 Authentication techniques

7.5 Biometric technologies

7.6 Intrusion detection techniques and how to apply them

7.7 Common design patterns for mitigating against information risks

8 Must understand and be capable of conducting **EVALUATIONS** that assess:

8.1 The implementation of secure systems, products and components using an appropriate methodology

8.2 The implementation of secure development standards and practices

8.3 The selection and implementation of appropriate test strategies to demonstrate security requirements are met

8.4 The implementation of appropriate processes for transfer of a service/system to operational/live use

8.5 Appropriate secure change- and fault-management processes

8.6 That a developed **SERVICE** meets its security criteria (requirements and/or policy, standards and procedures)

9 Must be able to conduct **EVALUATIONS** and:

9.1 Analyse scans and reports for signs of anomalous security issues, vulnerabilities and determining corrective action where necessary.

9.2 Analyse the processes that maintain the required level of security of a **SERVICE** through its lifecycle.

9.3 Assess a formal security assessment.

9.4 Assess methodologies for assessing the correct implementation of mitigation measures.

9.5 Assessing the level of assurance provided by a security mechanism, system or product in accordance with one or more recognised methodologies and standards.

9.6 Assessing whether a process is “fit for purpose” and meets the security requirements.

2.7 COMPETENCIES FOR ASSESSMENT OF SECURITY TESTING

1 Must be able to conduct an **EVALUATION** that assesses Security Testing:

1.1 Assess testing processes for vulnerabilities, highlighting those that are not addressed by security policies, standards and procedures and advising on corrective measures.

1.2 Assess recognised testing methodologies, tools and techniques and advise on corrective measures.

1.3 Assess the robustness of a system, product or technology against attack and advise on safeguards and corrective measures.

1.4 Assess commonly accepted governance practices and standards when testing in an operational environment.

3 OTHER TEAM MEMBER COMPETENCIES

3.1 CONFORMITY ASSESSMENT BODY PERSONNEL

1 In addition to the requirements of ISO 17065, a **CONFORMITY ASSESSMENT BODY SHALL** ensure that its personnel undertaking certification **CONFORMITY ASSESSMENT** tasks:

1.1 has relevant and appropriate knowledge about and experience in applying data protection legislation including appropriate technical and organisational measures as relevant

1.2 has relevant and appropriate knowledge about and experience in applying Digital Identity assessments including appropriate technical and organisational measures as relevant

1.3 demonstrate that they maintain relevant, specific knowledge in technical and evaluation skills through continuous professional development

2 In other areas of the certification team:

2.1 Certification team individuals providing technical expertise must have obtained a qualification in a relevant area of technical expertise or have significant relevant professional experience in that field.

2.2 Certification team individuals providing legal expertise must have obtained a degree level (or equivalent) qualification in law and have significant professional experience in data protection law.

2.3 Certification team individuals responsible for **EVALUATIONS** must demonstrate relevant and recent professional experience and knowledge in technical data protection, and experience in comparable procedures (e.g. certifications/evaluations) and appropriate professional qualifications where relevant.

2.4 Certification team individuals responsible for certification **REVIEWS** and **DECISIONS** must collectively have significant professional experience in identifying and implementing Digital Identity solutions and associated information security measures, or access to someone with that expertise, and an appropriate professional/degree level qualification.

3 The **CONFORMITY ASSESSMENT BODY** must be able to define and explain to DSIT and UKAS which professional experience requirements are appropriate to the scope of the **CONFORMITY ASSESSMENTS** undertaken.

4 The **CONFORMITY ASSESSMENT BODY SHALL** ensure that the persons or committees that make the certification reviews and/or decisions **SHALL,** collectively, have the same key skills as the certification team that carried out the certification evaluation.

5 Any other **CONFORMITY ASSESSMENT BODY** staff involved in the administration of UKDIATF **SHOULD** have appropriate knowledge of **CERTIFICATION SCHEME** Requirements and CAB Personnel Skills and Competencies documents.

3.2 COMPETENCIES AND PREREQUISITES FOR AUDITING

1 The **CONFORMITY ASSESSMENT BODY** personnel performing **EVALUATIONS** as described above **SHALL** have the following specific competencies and knowledge, and fulfil the following requirements:

2 Requirements:

2.1 formal academic qualifications or professional training or extensive experience indicating general capability to carry out **EVALUATIONS** based on the knowledge given below; and

2.2 at least four years full time practical workplace experience in information technology, of which at least two years have been in a role or function relating to relevant digital identity services, information security (including risk assessment/management), network security and physical security.

3 Knowledge of:

3.1 **EVALUATION** principles, practices and techniques in the field of trust-service provider (TSP) **EVALUATIONS** gained in a training course of at least five days;

3.2 the issues related to various areas of trust services, information security including risk assessment/management, network security and physical security;

3.3 the specified applicable standards referenced in the **UK DIGITAL IDENTITY AND ATTRIBUTES TRUST FRAMEWORK**, publicly available specifications and regulatory requirements for TSPs and other relevant publicly available specifications including standards for IT product evaluation;

3.4 the specified applicable standards referenced in any **SUPPLEMENTARY CODES** which they are conducting **EVALUATIONS** relating to; and

3.5 the **CONFORMITY ASSESSMENT BODY**'s processes.

4 Competences:

4.1 note-taking, report-writing, presentation, and interviewing skills; and

4.2 personal attributes: objective, mature, discerning, analytical, persistent and realistic.

5 The **CONFORMITY ASSESSMENT BODY** personnel performing evaluations **SHALL** maintain competence on the basis of appropriate education, training or experience. All relevant experience **SHALL** be current and prior to assuming responsibility for performing as an **AUDITOR**, the candidate shall have gained experience in the entire process of TSP **EVALUATION**. This experience **SHALL** have been gained by participating under supervision of lead **AUDITORS** in a minimum of four TSP **EVALUATIONS** for a total of at least 20 days, including documentation review, on-site **EVALUATION** and **EVALUATION** reporting.