Department for Science, Innovation & Technology

Office for Digital Identities & Attributes

Conformity Assessment Body principles and code of ethics

UK digital verification services trust framework certification scheme

Version 1.8

Table of contents

1.1.14

1 Version history

Version	Date	Pages	Changes	Author
1	2021	All	First Draft	DSIT
1.1	2022	All	Updates	DSIT
1.2	November 2023	All	Substantial changes to add further requirements	DSIT
1.3	September 2024	All	Change document title Update document references Change references to “certification bodies” and replace with “conformity assessment bodies”, and “assessors” with “auditors” Add clarification on prohibitions and restrictions	DSIT
1.4	April 2025	All	Aligned with new template for the scheme documents.	DSIT
1.5	May 2025	All	Grammatical updates	DSIT
1.6	June 2025	p16	1.1.3 section vi, reference added to Companies House	DSIT
1.7	March 2026	All	Updated to the new template and aligned the document with the TF v1.0	DSIT

2 Related documents

2.1 Principles

2.1.1 These principles should be read in combination with the following documents:

2.1.1 a Certification scheme requirements for Conformity Assessment Bodies,v1.11.

2.1.1 b CAB personnel skills and competencies requirements v1.8

2.2 Terms and definitions

2.2.1 All **bold** terms are defined terms as per the Certification scheme requirements for Conformity assessment bodies v1.11

3 Introduction

3.1 Purpose

3.1.1 The **UK digital verification services trust framework certification scheme** (hereafter referred to as **the trust framework**) expects all independent **auditors** and **Conformity Assessment Bodies (CABs)** engaged with both **the trust framework** and the providers to adhere to a set of principles and a code of ethics.

3.1.2 The Code of Ethics described in this document constitutes a definitive statement regarding the principles which should guide the work, requirements and the professional obligations expected of auditors and where applicable **CABs** employing **auditors**.

3.1.3 Where it relates to **CABs** providing **auditors** to t**he trust framework certification scheme** the **CAB shall** follow this code of ethics and ensure these are communicated and followed by the **auditors** it provides.

3.1.4 In keeping with auditing standards and principles of auditing the conduct of **auditors shall** always demonstrate integrity and in all circumstances **auditors** and **CABs should** avoid any actions that **may** call their professional conduct into question. The quality and validity of audits and evaluations must always be maintained and is open to assessment by DSIT's assurance function as described.

3.1.5 **Auditors** and **CABs** are required to complete quarterly reports for DSIT's Governing Body detailing what certifications have been started and completed, how many audits have been completed and the outcomes. This report must also provide information on planned audits and evaluations.

3.1.6 **Auditors** and certification **shall** follow the Certification Procedures as described in the relevant documents. Any deviations from these procedures must be justified.

3.1.7 **CABs shall not** offer clients any additional scope, use case or additional scheme, or supplementary code that is not approved by DSIT.

3.1.8 **CABs shall not** behave in any way that brings t**he trust framework certification scheme** into disrepute. Any evidence of such behaviour will be passed to UKAS to deal with and if found conclusive, UKAS and DSIT will consider withdrawal of both **approved** status and **accreditation** status.

3.1.9 **CABs shall not** discuss with any client or potential client another **CAB** in such a way that their credibility is called into question. Any evidence of such behaviour will be passed to UKAS to deal with and if found conclusive, UKAS and DSIT will consider withdrawal of both **approved** status and **accreditation** status.

3.2 Principle 1 – Integrity

3.2.1 **Auditors** and **CABs shall** undertake their work with integrity, honesty, diligence, and responsibility.

3.2.2 **Auditors** and **CABs shall** not knowingly be a party to any illegal activity or engage in acts that are discreditable to the profession of auditing or to DSIT, **the trust framework certification scheme** or its providers and members.

3.2.3 **Auditors** and **CABs shall** observe applicable laws and make disclosures expected by the law and the profession.

3.2.4 **Auditors** and **CABs shall** respect the legitimate, ethical, legal and operational mission of **the trust framework certification scheme**.

3.2.5 **Auditors** and **CABs shall** maintain high standards of behaviour while carrying out audits and evaluations and related work and in their relationships with the staff of audited entities.

3.2.6 **Auditors** and **CABs shall** maintain the principles of independence and objectivity.

3.2.7 **Auditors** and **CABs shall** maintain irreproachable standards of professional conduct.

3.2.8 **Auditors** and **CABs shall** apply honesty in carrying out audits and evaluations and in handling the resources of the provider and **the trust framework certification scheme**.

3.3 Principle 2 – Independence

3.3.1 **Auditors** and **CABs shall** maintain Independence from the audited entity and from any other outside interest groups.

3.3.2 **Auditors** and **CABs shall** behave in a way that in no way diminishes their independence.

3.3.3 **Auditors** and **CABs shall** avoid all relationships with managers and staff in the audited entity and other interested parties.

3.3.4 **Auditors** and **CABs shall** avoid all situations that may influence, compromise or threaten their ability to be seen to be acting independently.

3.3.5 **Auditors should** not use their official position for private purposes and **should** avoid relationships which involve the risk of corruption or which **may** raise doubts about their objectivity and independence. **CABs** employing **auditors** on behalf of t**he trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.3.6 **Auditors shall** not diminish their independence for personal or external interests. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.3.7 **Auditors shall** avoid external pressure or influence that can diminish their independence.

3.4 Principle 3 – Objectivity

3.4.1 **Auditors shall** be objective in dealing with all items and issues involved in the audit. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.4.2 **Auditors shall not** accept anything that may impair or can be used to suggest their professional judgement has been impaired. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.4.3 **Auditors shall not** hold prejudices concerning the audited entity or its employees and **shall** remain objective in their dealings with these.

3.4.4 **Auditors shall** remain objective in all work conducted.

3.4.5 **Auditors shall** ensure all reports produced for **the trust framework certification scheme**

are accurate and objective. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.4.6 **Auditors shall** provide recommendations, opinions and actions in reports that are based exclusively on evidence obtained and assembled in accordance with auditing standards. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.4.7 **Auditors can** make use of information prepared by previous audits and internal audits provided by the audited entity and other **auditors** but must treat these with objectivity. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.5 Principle 4 - Impartiality

3.5.1 **Auditors shall** maintain impartiality when taking any previously collected information into account. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.6 Principle 5 – Conflicts of interest

3.6.1 **Auditors** and **CABs** that provide advice or services to other entities **shall** alert **the trust framework certification scheme** if there is likelihood that this could lead to a conflict of interest.

3.6.2 **Auditors** and **CABs shall not** have any management responsibility or professional connection with the audited entity behind the audit function.

3.6.3 **Auditors shall** maintain their independence and refuse gifts or gratuities offered by the audited entity. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.6.4 **Auditors shall not** divulge information which would provide unfair or unreasonable advantage to other individuals or entities. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.6.5 **Auditors shall not** use information they have gained from one entity to have a negative impact on any other entity. **CABs** employing **auditors** on behalf of **the trust framework**

certification scheme will ensure compliance with this principle with regular checks.

3.6.6 **Auditors shall not** use information obtained whilst conducting their auditing work as a means of securing personal benefit for themselves or for others. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.6.7 **CABs can** carry out the following duties without them being considered as consultancy or necessarily creating a conflict of interest. However, all potential conflicts of interests should be dealt with in accordance with ISO/IEC 17065:2012 section 4.2:

3.6.7.a (i) conformity assessment – including information meetings, planning meetings, examination of documents, auditing (not internal auditing) and follow up of non-conformities;

3.6.7.a (ii) arranging and participating as a lecturer in training courses, provided that where these courses relate to evaluation of services, quality assurance, management systems or auditing they should confine themselves to the provision of generic information and advice that is freely available in the public domain, i.e. they should not provide company specific advice that contravenes the definition of consultancy given by ISO/IEC 17065:2012 section 3.2c;

3.6.7.a (iii) making available or publishing on request information on the basis for the **CAB**'s interpretation of the requirements of the assessment standards;

3.6.7.a (iv) activities prior to **audit** aimed solely at determining readiness for **assessment**; but such activities should not result in the provision of recommendations or advice that would constitute consultancy and the **CAB** should be able to confirm that such activities do not contravene these provisions and that they are not used to justify a reduction in the eventual **assessment** duration;

3.6.7.a (v) performing second and third party **audits** according to other standards or regulations than those being part of the scope of accreditation against the **trust framework certification scheme**;

3.6.7.a (vi) adding value during **assessments** and surveillance visits, e.g., by identifying opportunities for improvement, as they

become evident, during the **audit** without recommending specific solutions;

3.6.7.a (vii) explaining associated theories, methodologies, techniques or tools;

3.6.7.a (viii) sharing non-confidential information on related best practices.

3.7 Principle 6 - Confidentiality

3.7.1 **Auditors shall not** disclose information obtained in the auditing process to third parties via any means beyond the purposes of meeting the **CAB**'s or **trust framework certification scheme's** statutory or other identified responsibilities where this is part of the **trust framework certification scheme's** normal procedures or in accordance with relevant laws. **CABs** employing auditors on behalf of the **trust framework certification scheme** will ensure compliance with this principle with regular checks.

3.8 Principle 7 – Maintaining competency

3.8.1 **Auditors shall** only engage with providers and services for which they have the necessary knowledge, skills and experience. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this requirement by carrying out regular assessments of auditor's skills and competencies.

3.8.2 **Auditors shall not** undertake audits or work that they are not competent to perform. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this requirement by regularly checking the quality of audits undertaken.

3.8.3 **Auditors** and **CABs shall** always conduct themselves in a competent and professional manner. **Auditors** and **CABs should** do nothing that brings **the trust framework certification scheme** reputation into disrepute. Nor **shall** they do anything either through verbal or written communication that brings DSIT into disrepute.

3.8.4 **Auditors shall** maintain a high professional standard when carrying out **audits** that enable them to perform their duties competently and with independence, objectivity and impartiality. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks on the quality of audits undertaken.

3.8.5 **Auditors shall** exercise due professional care in conducting and supervising the audit and in preparing related

reports. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks on the quality of audits undertaken.

3.8.6 **Auditors shall** use methods and practices of the highest possible quality in their audits. In the conduct of the audit and the issue of reports, **auditors** have a duty to adhere to the principles and accepted auditing standards. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks on the quality of audits undertaken.

3.8.7 **Auditors shall** know and follow applicable auditing, identity management and security management standards, policies, procedures and practices. **CABs** employing auditors on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular assessment of auditor's skills and competencies and regular checks on the quality of audits undertaken.

3.8.8 **Auditors shall** possess a good understanding of the legal and regulatory and institutional principles and standards governing the operations of the audited entity. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular checks on the quality of audits undertaken.

3.9 Principle 8 – Professional development

3.9.1 **Auditors shall** accept a continuous obligation to update and improve the skills required to conduct their professional responsibilities. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this principle with regular assessments on the auditor's skills and competencies and regular checks on the quality of audits undertaken.

3.9.2 **Auditors shall** continually improve their proficiency and the effectiveness and quality of their services. **CABs** employing **auditors** on behalf of **the trust framework certification scheme** will ensure compliance with this requirement by carrying out regular assessments of **auditor**'s skills and competencies. This requires **auditors** to keep up to date with changes to standards, regulations and practices relevant to identity management and security.

4 Requirements to maintain the principles

4.1 Outline of requirements

4.1.1 The following outlines the requirements that **shall** maintain the principles:

1.1.14

1. Leadership and governance	
1.1. General requirements	Criteria
1.1.1 Legal and contractual matters	i. The lead roles and responsibilities of the Conformity Assessment Body and any advisory structures shall be defined and documented.
	ii. The Conformity Assessment Body shall ensure that there is a documented agreement between the various parties that make a contribution to the digital identity service that is the focus of certification.
	iii. The Conformity Assessment Body shall ensure that the agreement is reviewed at least annually to ensure its effectiveness.
	iv. The Conformity Assessment Body shall have an agreed set of principles that it operates to, these should be in keeping with principles DSIT have documented. Note: The principles should, as a minimum meet compliance with those above.
	v. Members of the Conformity Assessment Body and its boards shall be assisted in fulfilling their responsibilities through clear terms of reference, which include roles, membership and lines of reporting.
	vi. The Conformity Assessment Body shall define its governance structure and how its management structure interacts with it.
	vii. The Conformity Assessment Body shall have a clear vision statement for all its activities that provide the basis for operational planning and direction.
	viii. There shall be documented agreements with professional societies and service user groups defining how they recognise and support the trust framework certification scheme, how they are involved in the governance, development and delivery of the trust framework certifications scheme and how they promote participation.
	ix. Conformity Assessment Bodies shall be represented on relevant committees and advisory/working groups as required by DSIT.

1.1.14

	x. The Conformity Assessment Body shall be a stand-alone legal entity, or part of a legal entity, and document its governance arrangements and responsibilities. Note: A legal entity is any structure that has legal standing in the eyes of law. The provider organisation can enter into agreements or contracts, assume obligations, incur and pay debts, sue and be sued in its own right, and to be held responsible for its actions.

	xi. The Conformity assessment body shall have clear policies and agreements for any contracted work related to the delivery of the trust framework certification scheme. Note: A provider may have a number of contracted activities or none. These relate directly to the provision of certification activities and may apply to assessors who are contracted to support the trust framework certifications scheme operated by DSIT . They may also apply to external contractors providing professional and technical expertise to the delivery of the trust framework certifications scheme (for example, trainers) and where assessments might be carried out on behalf of the Conformity Assessment Body by another organisation.
	xii. The Conformity Assessment Body shall ensure the competence and effectiveness of any external organisations or individuals that are contracted provide services to the Conformity Assessment Body through monitoring and reviews.
1.1.2 Management of impartiality	i. The Conformity Assessment Body shall seek to operate impartially so that its certification activities are not adversely influenced. The Conformity Assessment Body shall have formal rules for the appointment and operation of any committees that are involved in the certification process. Such committees shall be free from any commercial, financial and other pressures that might influence decisions. The Conformity Assessment Body shall retain authority to appoint and withdraw members of such committees.
	ii. Staff shall have information and training on the Conformity Assessment Body's specific policies related to individual the trust framework certification schemes. Note: All relevant documentation relating to the trust framework certification scheme shall be made available to these people.
	iii. Staff shall have the information and training to assist them in fulfilling their role.

1.1.14

	iv. The effectiveness of the governance of the scheme delivery shall be evaluated using indicators and other measures of performance. These shall Be made available to DSIT's assurance function on request.

	v. The Conformity Assessment Body shall have policies in place in order to ensure effective and efficient delivery of its trust framework certification scheme. As a minimum the following policies shall be included: Impartiality: to ensure that all decisions are independent and objective. There shall be clear arrangements in place to ensure impartiality in all its activities and avoidance of any conflicts of interest. Code of conduct: the set of rules outlining the responsibilities of, or proper practices for, all staff, contractors, members of committees and assessors to operate to. Complaints: there shall be a documented process with timescales in place to support client organisations, auditors and stakeholders. Appeals: there shall be a clear process in place related to certification decisions. Serious personal and professional issues: to clarify and manage issues about individuals including reporting advice and arrangements to professional organisations.
1.1.3 Liability and financing	i. The Conformity Assessment Body shall have documented arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations.
	ii. The Conformity Assessment Body shall make the required performance level to support its activities clear to any external contractors. Note: Examples may include tools, systems and IT services and human resource administration.
	iii. There shall be documented agreements and monitoring arrangements with all key suppliers. Note: A key supplier is an independent company or body contracted to provide services e.g. an IT provider or training company.
	iv. The Conformity Assessment Body shall have the financial stability and resources required for its operations. Any change or risk to financial stability shall be made known to DSIT's Governance function.
	v. The Conformity Assessment Body shall state clearly the costs to participate in a scheme and this shall be periodically reviewed and transparent to all scheme participants and stakeholders.

1.1.14

	vi. The financial accounts of the Conformity Assessment Body shall be transparent and available. Note: The Conformity Assessment Body shall publish a summary of annual financial accounts. This shall be done via maintaining Companies House record or equivalent in other countries.
	vii. The Conformity Assessment Body shall have processes for financial planning and budgeting, and policies for delegation of financial responsibility.
	viii. There shall be internal and independent systems of financial and asset control that protect the Conformity Assessment Body/'s assets.
	ix. Financial systems shall be well managed including monitoring, tracking and review systems. Note: The Conformity Assessment Body should have clear, documented procedures for budget control and auditing, clear lines of responsibility and accountability and robust processes to support all procedures.
1.1.4 Non-discriminatory conditions	i. Non-discrimination: the procedures under which the Conformity Assessment Body operates, and the administration of them, shall be non-discriminatory. Procedures shall not be used to impede or inhibit access by applicants.
1.1.5 Confidentiality	i. The Conformity Assessment Body shall have policies in place in order to ensure effective and efficient delivery of the trust framework certification scheme including: – Confidentiality: to manage all information obtained or created during the performance of certification activities
1.2 Structural requirements	Criteria
1.2.1 Risk Management	i. The Conformity Assessment Body shall have a risk management framework that is used to identify and manage all known risks and learn from unexpected events.
	ii. The Conformity Assessment Body shall identify all potential risks for its operations including those specific to the trust framework certification scheme. Note: Risks might include but are not limited to: reputation, engagement in the scheme, impartiality, financial, human resources, IT systems, environmental, quality assurance, and operation of the scheme.
	iii. The Conformity Assessment Body shall consult with stakeholders; lay representatives, staff members, contract staff to ensure that recorded risks are relevant and comprehensive.
	iv. The Conformity Assessment Body shall establish processes to mitigate the identified risks and define metrics to monitor the known risks.

1.1.14

	v. The Conformity Assessment Body shall review the risks on a regular basis to determine whether the processes to mitigate risk have been effective and, if not, design and implement new processes to reduce risk.

2. Operational delivery	
2.1 Resource requirements	Criteria
2.1.1 Conformity Assessment Body personnel	i. The human resource strategy of the Conformity Assessment Body shall reflect the requirements of the strategic and operational plans.
	ii. All employment policies and procedures shall be developed in accordance with local law and legislation and cover all aspects from recruitment to end of service.
	iii. The Conformity Assessment Body shall have policies and systems in place to ensure it has sufficient competent staff with the mix of skills to enable delivery of the trust framework certification scheme.
	iv. The Conformity Assessment Body shall have a description of its staff, and the responsibilities of both its staff and the wider team. Note: The wider team includes but is not exclusive to: contractors, professionals providing specialist advice and auditors.
	v. Peer assessors shall be appointed to represent the requirements of the digital service and the delivery of the scheme.
	vi. Auditors shall have documented roles, competencies and agreements.
	vii. Resources who are experts by experience may participate as full members of audit teams.
	viii. The Conformity Assessment Body shall have policies and systems in place to meet the induction requirements of staff, including any additional service specific education and training.
	ix. The Conformity Assessment Body shall have policies and systems in place to ensure the workforce, including auditors, are properly trained and competent.
	x. A training needs analysis shall support all new staff that support the trust framework certification scheme.

1.1.14

	xi. New auditors shall have a structured training plan and shall be evaluated for their competence in the role.

	xii. The Conformity Assessment Body shall have an effective appraisal system for all staff.
	xiii. All training programmes shall be evaluated to ensure that they are achieving agreed learning outcomes.
	xiv. There shall be on-going development of staff skills. Auditors shall be supported to update skills and knowledge proportionate to the needs of the scheme. Note: Auditors may have annual or as-needed face to face refresher training, remote updates or a combination of both. They shall maintain the competencies as detailed in CAB Personnel Skills and Competency Requirements -
	xv. The Conformity Assessment Body shall seek and evaluate feedback from services and auditors to inform the performance of auditors and staff.
2.2 Process requirements	Criteria
2.2.1 UKDVSTF CSs	i. The UKDVSTF CS is developed in response to a defined industry need.
	ii. The Conformity Assessment Body shall consult with key stakeholders to ensure that their delivery and operation of the trust framework certification scheme is viable and supported.
	iii. The Conformity Assessment Body shall consider the digital identity service that is the focus of a trust framework certification scheme from the perspective of service users and other stakeholders such as relying parties.
	iv. The Conformity Assessment Body shall keep an up to date register of clients and their certification status.

	v. The Conformity Assessment Body shall have an operating plan that reflects the overall future of their delivery and operation of the trust framework certification scheme and the resources required to achieve this.
	vi. When the Conformity Assessment Body is a defined part of a legal entity, the operational structure shall include the line of authority and the relationship to other parts of the same legal entity.
	vii. The Conformity Assessment Body shall define its management and Board structure, making it clear who the personnel are and their responsibilities. Note: This should include responsibility for the following: – Development of policies relating to the operation of the Conformity Assessment Body/certification body Risk management.
2.2.2 Client application and management	i. Requirements shall be documented and publicised.
	ii. The Conformity Assessment Body shall ensure that all applicants for certification are aware of and understand the entry criteria before agreeing their entry to the trust framework certification scheme. If necessary a pre-assessment form may be completed or if a client has undertaken a Readiness Assessment with DSIT the client may choose to submit the findings. DSIT will not share this information with a Conformity Assessment Body without the agreement of the potential client. Note: Applicants should provide as a minimum details of their organisation and the scope of their digital service on application.
	iii. The Conformity Assessment Body shall actively promote the trust framework certification scheme to digital identity services to encourage participation.
	iv. The Conformity Assessment Body shall offer the trust framework certification scheme to the full range of digital identity services managed by private and public sector providers.
	v. The Conformity Assessment Body staff shall have an agreed mission statement that defines the etiquette and values of the Conformity Assessment Body and is made clear to all clients.

	vi. The Conformity Assessment Body shall have a database of all participating digital identity services that

1.1.14

	includes their status, certification date, surveillance date and monitoring and assessment dates.
	vii. Services being assessed shall be provided with relevant information about the trust framework certification scheme.
	viii. The Conformity Assessment Body shall have an individual agreement with each digital identity service. Note: The agreement with each service should include: Mechanisms for addressing serious concerns about service user security, potential abuse of or other serious matters relating to service user care identified during the course of assessment of a digital identity service. Mechanisms for the client to inform the Conformity Assessment Body in a timely way, of changes that may affect its ability to conform with the trust framework certification scheme certification requirements, including: Legal, commercial, organisational status or ownership Changes to the digital identity service, its structure and delivery Major changes to the quality and safety of the digital identity service Major changes to the leadership of the digital identity service and personnel
	ix. There shall be defined resources available to assist a digital identity service to achieve the standards.
2.2.3 Certification standards	i. The Conformity Assessment Body shall ensure that its trust framework certification scheme(s) operate to agreed standards for provision of a digital identity service. The standards and other performance measures shall be based on DSIT requirements, national guidance, guidelines developed by professional associations, current research evidence, consensus agreements and/or recommendations from other digital identity fora.
	ii. The scope and purpose of the standards and underpinning criteria shall be clear in terms of: The type of digital identity service and roles to which they apply
	iii. The Conformity Assessment Body shall provide information and education to staff and auditors of standards to support effective assessments.
	iv. The standards and criteria to certify a digital identity service shall be made available in a format that is accessible to key stakeholders and service users.

	v. The need for new or revised underpinning criteria and other performance measures shall be established by seeking the views of DSIT.

2.2.4 UKDVSTF CS service audit and audit team	i. The Conformity Assessment Body shall actively plan the audit in collaboration with the service involved.
	ii. The Conformity Assessment Body shall communicate all audit information to the digital identity service, including special requirements, auditors in training and observers.
	iii. There shall be an effective mechanism for avoiding conflicts of interest when peer assessors are selected to undertake a review of a digital service.
	iv. The Conformity Assessment Body shall ensure that the digital identity service has an opportunity to raise any conflicts of interest it has identified.
	v. The Conformity Assessment Body shall ensure that all pre documentation and preparation materials are communicated to the digital identity service through authorised individuals.
	vi. The Conformity Assessment Body shall ensure that all information is provided ahead of the site audit for the audit team to review.
	vii. The Conformity Assessment Body shall support audits through an IT system or manual systems to support evidence review, feedback, communication and production of a Certification Feedback Report.
	viii. The Conformity Assessment Body shall agree a timetable with the digital identity service for completion of evidence preparation, review and virtual meetings and attendance on site.
	ix. The Conformity Assessment Body shall make it clear who from the digital identity service is required for attendance on the day of a virtual meeting or a site visit.
	x. For onsite or virtual audits, all auditors shall have clear means of identifying who they are, including photographic ID. Auditors must make sure the client has confidence that they are the legitimate representative of the Conformity Assessment Body.
	xi. The Conformity Assessment Body shall ensure security policies for those attending a site visit are complied with.
	xii. The Conformity Assessment Body shall ensure that a clear and consistent verbal feedback process to the digital identity service on the day of the virtual audit or site visit is followed.
	xiii. There shall be a methodology for consistently determining the achievement of a standard.
	xiv. Audits shall be conducted by auditors and digital identity services to a structured timeline from application to the Certification award.

1.1.14

	xv. There shall be methods of data collection and sample sizes to support valid audits for quality indicators, service user outcome measures, service user satisfaction scales and collected as part of the audit process.
	xvi. The audit shall be conducted using agreed guidelines and audit tools.
	xvii. The level of performance expected shall match or exceed that expected by DSIT.

	xviii. The Conformity Assessment Body shall have a clear policy to determine the circumstances where security or data protection issues such as suspected breaches in a digital identity service may need escalation.
	xix. The Conformity Assessment Body shall ensure that there is two way, on-going communication with digital identity services regarding outstanding actions for certification.
	xx. The planning of the audit shall be transparent and timely.
	xxi. The audit team shall be selected to provide a balance of skills and experience to match the needs of the participating digital identity service. See CAB Personnel Skills and Competency Requirements.
	xxii. The Conformity Assessment Body shall make all guidelines for audits available to all auditors who will audit the digital identity service.
	xxiii. The Conformity Assessment Body shall ensure that regular checks are conducted of audit activity including timescales to ensure compliance with audit protocols.
2.2.5 Certification decision and reporting	i. The Conformity Assessment Body shall have a clear policy and procedures to determine the outcome of an audit. Note: The policy should state who is responsible for determining the outcome of the audit including the audit team's responsibility and what is expected during the audit.
	ii. The certificate shall include the period/date for review so that any external organisations will be aware not only of the date of issue, but when a formal review is due.
	iii. The Conformity Assessment Body shall ensure that the certification award follows an agreed format.
	iv. The Conformity Assessment Body shall have agreed rules about the uses of certificates, logos and references to the trust framework certification scheme.

	v. The Conformity Assessment Body shall have a clear policy to determine the circumstances where a digital identity service may be suspended or withdrawn from the trust framework certification scheme resulting in the loss of certification. Note: The certification decision policy should state the changes in circumstances a digital identity service needs to advise the Conformity Assessment Body about and the associated timescales.
	vi. The Conformity Assessment Body shall have a clear and consistent process to feedback information about the audit to the digital identity service. The policy for recommendations of certification and the achievement of key actions and recommendations shall be communicated to the digital identity service.
	vii. The Conformity Assessment Body shall ensure that the results of the audit are documented in a Certification Feedback Report that may be independently quality assured and that there are clear timescales for the communication of the report.
	viii. The Conformity Assessment Body shall require digital identity services to develop and submit an action plan to address any weaknesses identified by the audit.
	ix. The Conformity Assessment Body shall have a policy and process on how the final results of a certification audit are displayed and communicated. Note: Outcomes may result in 'key actions' such as non-conformities graded as major and minor (to comply with) or recommendations for improvement (not mandatory).

2.2.6 Surveillance	i. The Conformity Assessment Body shall have a documented policy and process for surveillance of certified digital identity services, including agreement of areas monitored and security parameters. This should follow the requirements as stipulated in the document – Certification Scheme Requirements for Conformity Assessment Bodies. Note: Trust framework certification scheme expects surveillance audits to be scheduled +/- 30 days from original certification date.
	ii. The Conformity Assessment Body shall require digital identity services to develop and submit an action plan to address any weaknesses identified by the audit.
	iii. There shall be agreed timescales for review and rectification of areas of non-compliance by the digital

1.1.14

	identity service. For major non conformities this shall be no longer than 30 days.
2.2.7 Records	i. The Conformity Assessment Body shall ensure effective management of all information, which defines and describes the types of information generated, collected, used and delivered as part of its certification activities.
	ii. The Conformity Assessment Body shall have clear policies and systems to support information management to ensure accuracy, integrity, confidentiality, reliability, timeliness, security and retention. Note: The compliance evidence for digital identity services should be retained for the duration of the digital identity service certification cycle e.g. two years
	iii. The information collected and held shall meet all statutory and professional requirements including compliance with UK DPA and GDPR. Note: The following are examples of information for digital service trust framework certification scheme(s): The digital identity service to be certified and the general features of the client, including its name and the address of its physical location(s) General information concerning the digital identity service, relevant to the field of certification for which the application is made, such as its activities, its human and technical resources, and its functions and relationship in a larger corporation, if any All other information needed in accordance with the relevant certification requirements, such as information for initial evaluation including identity data and surveillance activities. The Conformity Assessment Body shall operate clear processes for information requests related to digital identity services and their audit outcomes Information applications/tools/programmes shall have ongoing maintenance and development to ensure integrity and reliability All quality improvement and training resources provided for auditors shall be maintained and reflect up to date practice Staff shall be trained on how to run operational systems correctly and shall be aware of information management policies

3. Assessment management	
3.1 Management system requirements	Criteria
3.1.1 General management system	i. There shall be a document management system with mechanisms in place to ensure that all policies and procedures are up to date and reviewed.

1.1.14

	ii. The Conformity Assessment Body shall have an agreed framework for improving the quality and performance of its services.
	iii. The Conformity Assessment Body shall have internal systems to monitor, review and act on: Performance against accepted standards (including timeliness of planning and delivery of peer assessment visits and of delivery of the Certification Feedback Report); Performance on defined indicators and other relevant measures; Compliance with policies, procedures and guidelines; Progress against the quality improvement plan. Results of the above shall be reported and communicated to staff.
	iv. The Conformity Assessment Body staff participating in the trust framework certification scheme shall be surveyed formally at least once per year about their perceptions of the trust framework certification scheme and for areas to be improved.
	v. The Conformity Assessment Body shall actively seek and evaluate feedback after each audit and act promptly upon any improvements required.
	vi. The evaluation of the performance of the Conformity Assessment Body shall include a defined approach to measure the impact of the trust framework certification scheme in bringing about improvements in the quality of digital identity and attributes provided by participating services.
	vii. Identified staff, auditors, advisors and contractors shall participate actively in audits and analysis about the effectiveness of the Conformity Assessment Body in bringing about improvements in digital identity services.
	viii. Improvement activities and projects shall be planned and documented to enable continuous improvement to processes and services using a defined improvement model.
	ix. The quality improvement framework shall be regularly evaluated and the results reported by management to the governing group.
	x. The Conformity Assessment Body shall make known to DSIT the results of all the accreditation assessments it undergoes, including indicators and other measures of its performance.

Required Evidence	Criterion	Suggested evidence
Legal and contractual matters	1.1.1 i	An organogram or equivalent documenting the roles and responsibilities of the Conformity Assessment Body and any advisory structures. A supporting description of how the roles

		function and relate to the scheme.
	1.1.1 ii	Documented agreement process/document/contracts between parties that are the focus of certification.
	1.1.1 iii	A description of the annual review process for any DSIT schemes and supporting meeting output notes and any actions.
	1.1.1 iv	A summary of the documented Conformity Assessment Body principles and values that it operates to.
	1.1.1 v	Actively support the development and delivery of the trust framework certification scheme including terms of reference and membership of the relevant WG.
	1.1.1 vii	Written vision statement for the Conformity Assessment Body or evidence to support activities that provide the basis for operational planning.
	1.1.1 viii	Documented agreements with professional societies and service user groups defining support, involvement and promotion of the trust framework certification scheme.
	1.1.1 xi	Statement on legal status of the provider organisation. Provide a description of the type of entity it is.
	1.1.1 xii	Policy for outsourcing contract work and whom the provider outsources to and a description of the process for monitoring this.
	1.1.1 xiii	A description of the process for service level agreements and monitoring review process with external organisations or individuals that provide services to the trust framework certification scheme.
Management of impartiality	1.1.2 i	Impartiality and conflict of interest policy.
	1.1.2 ii	Copies of standards pertaining to the trust framework certification scheme, code of

1.1.14

		conduct, confidentiality policy, impartiality policy.
	1.1.2 iii	The communications and training plan to support staff.
	1.1.2 iv	Summary of indicators used to evaluate governance performance.
	1.1.2 v	Impartiality policy, statement on consultancy, code of conduct, conflict of interest policy, complaints policy, appeals policy.
Liability and financing	1.1.3 i	A copy of the provider's liability insurance cover or alternative arrangements.
	1.1.3 ii	Examples of external contracts, performance levels required and review arrangements.
	1.1.3 iv	Budget planning and approval process, financial summary reports or annual reports.
	1.1.3 v	Trust framework certification scheme costs and a summary of what the service gets for this payment fee.
	1.1.3 vi	Budget tracking systems, financial audit, and financial reports.
	1.1.3 vii	Documented policies for financial responsibility and processes for financial planning, budgeting.
	1.1.3 viii	Process for internal and independent systems of financial and asset control.
Non-discriminatory conditions	1.1.4 i	Non-discriminatory procedures and application processes.
Confidentiality	1.1.5 i	Confidentiality procedures and application processes.
Risk management	1.2.1 i	Risk management strategy and process, minutes of meetings to support reviews of risks and supporting policies.
	1.2.1 ii	Risk plan including those specific to the trust framework certification scheme including mitigation strategies.
	1.2.1 iv	Sample meeting minutes that show monitoring, review and actions taken to reduce risk
Conformity Assessment Body personnel	2.1.1 i	The human resource strategy for the Conformity Assessment Body/.

1.1.14

	2.1.1 ii	Employment policies and procedures to support the operational delivery of the trust framework certification scheme.
	2.1.1 iii	The establishment and skill mix for the Conformity Assessment Body to deliver the trust framework certification scheme.
	2.1.1 iv	Role descriptions for all auditor roles including other representatives.
	2.1.1 v	Application process and pack for all auditors.
	2.1.1 vi	auditor contract, competencies and agreements.
	2.1.1 vii	Documented process for how lay auditors participate in the audit process.
	2.1.1 viii	Induction programmes for staff, including service specific education and training.
	2.1.1 ix	Training pathways including competency assessments and evaluations of these for auditors and other staff.
	2.1.1 x	Training needs analysis examples for new staff that support the trust framework certification scheme.
	2.1.1 xi	A structured training pathway for new auditors and a process for evaluation of their competence in the role.
	2.1.1 xii	A description of appraisal system for all staff. A summary/matrix of staff appraisals.

	2.1.1 xiii	Evaluation for training programmes and examples of results.
	2.1.1 xiv	Systems and process for on-going development of staff and auditor skills and knowledge.
	2.1.1 xv	Feedback from services and auditors relating to the performance of auditors and staff.
UKDVSTF CSs	2.2.1 i	Operational plan, minutes of meetings with stakeholders.
	2.2.1 iii	List of schemes operating and descriptions of scheme and their objectives.
	2.2.1 iv	Register of clients and their certification status for schemes.
	2.2.1 v	The operating plan for the trust framework certification scheme.

1.1.14

	2.2.1 vii	Organogram and description of governance and management.
Client application and management	2.2.2 i	Publicly available information about the trust framework certification scheme requirements.
	2.2.2 ii	Policy and process for application and suitability.
	2.2.2 iii	Marketing and communications plan for the trust framework certification scheme.
	2.2.2 iii	The range and type of services participating in the trust framework certification scheme.
	2.2.2 v	Team etiquette and values policy.
	2.2.2 vii	Summary of information or pack provided to applicants about the trust framework certification scheme.
	2.2.2 vii	Relevant information about the trust framework certification scheme for the services being audited.
	2.2.2 viii	Copies of agreements for digital identity services participating in the trust framework certification scheme.
	2.2.2 ix	Escalation policy and process for addressing serious concerns about users of the digital identity service, security, fraud and suspicion of breaches.
	2.2.2 x	Policy and process for the client to inform the Conformity Assessment Body of changes that may affect its ability to conform with the trust framework certification scheme certification requirements.
Certification standards	2.2.3 i	The process for developing the standards, underpinning criteria and evidence requirements.
	2.2.3 ii	Copies of up to date standards and requirements for the trust framework certification scheme(s).
	2.2.3 iii	Processes to provide education and information to staff and auditors of standards to support effective audits.
	2.2.3 iv	The systems and processes for services to access the standards and criteria for audit.
	2.2.3 v	Methodology for review and update of the standards.
	2.2.3 vi	Evidence of feedback on standards, this includes feedback from digital services, professional and patient groups.
	2.2.3 vii	Examples of where user outcomes are included in the standards used for individual schemes.

UKDVSTF CS assessment and assessment team	2.2.4 i	Policies and process for planning audits in collaboration with the digital identity service involved.
	2.2.4 ii	The policy and processes for communicating the full audit process to the digital identity service.
	2.2.4 iii	Conflicts of interest policy and process.
	2.2.4 vii	Process for review of service evidence ahead of the virtual or site audit.
	2.2.4 viii	Audit timetable examples and process for agreeing it with a service with the digital identity service.
	2.2.4 ix	Policy for auditor identification, security and etiquette on site audits.
	2.2.4 xii	The process for verbal feedback to the digital identity service and how this is monitored for consistency.
	2.2.4 xiii	Methodology for determining the achievement of a standard.
	2.2.4 xiv	Process for checks of audit activity including timescales to ensure compliance with audit protocols.
	2.2.4 xv	Description of methods of data analysis and outcomes to support assessments.
	2.2.4 xvi	Auditor guidelines/handbook for audits.
	2.2.4 xix	The communication processes with service and auditors regarding outstanding actions for certification.
	2.2.4 xxii	Selection process for audit teams.
	2.2.4 xxiii	Process for checks of audit activity including timescales to ensure compliance with audit protocols.
Certification decision and reporting	2.2.5 i	Policy and procedures to determine the outcome of an audit.
	2.2.5 ii	Examples of certificates including process for management and review.
	2.2.5 iv	Policy for use of certificates, logos and references to the trust framework certification scheme.
	2.2.5 v	Policy for suspension or withdrawal from the trust framework certification scheme resulting in the loss of certification.
	2.2.5 vi	Policy and processes for certification decisions and examples, performance level for achievement of standards.
	2.2.5 vii	Quality assurance of reports policy and process.
	2.2.5 viii	Policy and processes for ingoing submission of actions plans and the review process to achieve certification.

Surveillance	2.2.6 i	Policy and description of processes for all surveillance activities including timescales

Records	2.2.7i	Effective management of all information, which defines and describes the types of information generated, collected, used and delivered as part of the trust framework certification scheme activities.
	2.2.7ii	Clear policies and systems to support information management to ensure accuracy, integrity, confidentiality, reliability, timeliness, security and retention.
	2.2.7iii	The information collected meets all statutory and professional requirements.
General management system	3.1.1 i	Description of quality management approaches to the trust framework certification scheme, evidence of reviews and feedback to staff.
	3.1.1 ii	Strategy and plans for improving the quality and performance of its services.
	3.1.1 iii	Internal monitoring, review and audit systems to determine performance and quality of services provided. Evidence of feedback to staff.
	3.1.1 iv	Feedback surveys from Conformity Assessment Body staff and digital services participating in the trust framework certification scheme and for areas to be improved.
	3.1.1 v	Methodology and summary of digital identity service with action plans for any improvements required.
	3.1.1 vii	Research involvement, effectiveness of scheme reports.
	3.1.1 viii	Summary of improvement activities projects and reviews to support improvements in the scheme.
	3.1.1 x	The policy and description of the process to make public the results of all the audits.