

ACCS 1:2026

Conformity Assessment Requirements for ISO/IEC 27566-1 – Age Assurance Systems – Part 1: Framework

Technical requirements for the certification of age assurance systems and components under the Age Check Certification Scheme

This is a publicly available specification created by the Age Check Certification Scheme Ltd. It is subject to the intellectual property rights of the Scheme and may not be copied, used in a retrieval system or utilised without the express consent of the Scheme, save that it may be mentioned by name as a reference document with appropriate attribution and a link to the document itself.

© Age Check Certification Scheme Ltd 2026

All rights reserved.



Contents

Introduction	6
1. Scope	7
1.1 Purpose and Application.....	7
1.2 Scope Boundaries.....	7
2. Normative References.....	9
2.1 Normative references.....	9
2.2 Bibliography	9
3. Terms and Definitions	11
3.1 Interpretation.....	11
3.2 Terms defined in normative documents	11
3.3 Objects of Certification.....	12
3.4 Technical and Process Concepts	12
4. Target of Evaluation	15
4.1 General	15
4.2 Age Assurance Providers	15
4.3 Relying Parties.....	16
4.4 Intermediaries.....	16
4.5 Declaration of Threats and Attack Vectors.....	16
4.6 Definition of Boundaries.....	16
4.7 Contexts of Use	17
4.8 Data Dependencies, Assumptions and Exclusions.....	18
5. Classification Accuracy Levels	19
5.1 Purpose	19
5.2 Classification Accuracy Levels.....	19
5.3 Classification Accuracy Requirements.....	19
5.4 Test Sample Integrity Requirements.....	21
5.5 Successive Validation and Multi-Method Systems	24
5.6 Demographic Fairness and Outcome Error Parity	24
5.7 Date of Birth Requirements.....	24
5.8 Jurisdictional Requirements	25



6.	Practice Statements	26
6.1	General Requirements.....	26
6.2	Content of Practice Statements	26
6.3	Basis for Assessment	27
6.4	Updates and Maintenance	27
6.5	Structured Submission	28
6.6	Practice Statement Review.....	28
6.7	Configuration Management	28
6.8	Change Control, Documentation and Record Keeping	28
7.	Stage One Evaluation	29
7.1	Purpose of Stage One Evaluation.....	29
7.2	Stage One Audit Plan.....	30
7.3	Testing Plan.....	30
7.4	Privacy Documentation	31
7.5	Risk Management and Attack Vectors	31
7.6	Monitoring and Continuous Improvement	31
7.7	Stage One Audit Report	32
8.	Testing Requirements	33
8.1	Purpose and Testing Framework	33
8.2	Competence of Test Analysts	36
8.3	Development of Test Plans.....	36
8.4	Test Coverage.....	37
8.5	Sample Size and Demographic Requirements.....	38
8.6	Classification Accuracy Levels.....	39
8.7	Jurisdictional Requirements	39
8.8	Statistical Assurance Framework	39
8.9	Data Integrity and Anti-Gaming Controls	42
8.10	Recognition of External Testing	43
8.11	Execution of Testing	43
8.12	Test Report - Content and Records	44
8.13	Submission, Review and Publication.....	45
9.	Stage Two Evaluation	46
9.1	Purpose of Stage Two Evaluation.....	46
9.2	Stage Two Audit Plan.....	46
9.3	Age Assurance Method Register.....	46

9.4	Age Assurance Methods Assessment (ISO/IEC 27566-1 Clause 4)	47
9.5	Functional Characteristics (ISO/IEC 27566-1 Clause 5)	48
9.6	Performance Characteristics (ISO/IEC 27566-1 Clause 6)	48
9.7	Privacy Characteristics (ISO/IEC 27566-1 Clause 7)	51
9.8	Security Characteristics (ISO/IEC 27566-1 Clause 8)	52
9.9	Acceptability Characteristics (ISO/IEC 27566-1 Clause 9)	52
9.10	Practice Statement Assessment and Finalisation	52
9.11	Draft Certification Scope and Schedule	53
9.12	Auditor's Recommendation and Handover	55
10.	Evaluation Review, Certification Decision and Post-Certification	56
10.1	Purpose of Evaluation Review	56
10.2	Evaluation Review	56
10.3	Certification Decision	56
10.4	Certificate of Conformity and Schedule of Certification - Issuance	57
10.5	Practice Statement Issuance	57
10.6	Regulatory Notifications	57
11.	Surveillance, Recertification and Ongoing Certification Obligations..	59
11.1	Purpose and Governing Framework	59
11.2	Changes Relevant to Continued Certification	59
11.3	Surveillance Audit Scope and Planning	59
11.4	Continuous Monitoring	60
11.5	Surveillance Outcome	61
11.6	Recertification Requirements	61
11.7	Practice Statement Maintenance During the Certification Period	62
12.	Extension of Scope	63
12.1	General	63
12.2	What Constitutes an Extension of Scope	63
12.3	Retesting Requirements	63
12.4	Practice Statement and Registry	65
Annex A -	Calculation of Audit and Testing Effort (normative)	66
A.1	Purpose and Scope	66
A.2	Structure of Effort	66
A.3	Preparation and Scoping	67
A.4	Stage One — Policy and Governance Assessment	67
A.5	Stage Two — Component Effort	68

A.6	Stage Two — Context of Use Effort.....	69
A.7	Testing Effort.....	71
A.8	Independent Review of Certification Evidence and Certification Decision	78
A.9	Surveillance and Recertification	78
A.10	Changes and Extensions to Certification	78
A.11	Scheme Levy.....	79
A.12	Documentation and Record.....	79

Annex B - Practice Statement Template (informative)..... 80

B.1	Purpose	80
B.2	Private Practice Statement - Content.....	80
B.3	Public Practice Statement - Contents.....	83

Annex C - Model Certification Documents (normative)..... 85

C.1	Purpose	85
C.2	Model Certificate of Conformity.....	85
C.3	Model Schedule of Certification	86
C.4	Model Public Practice Statement Front Sheet.....	87

Annex D - Mapping of ISO/IEC 27566-1 Requirements to the ACCS 1

Evaluation Process (informative)..... 89

D.1	Method and Maintenance	89
D.2	ISO/IEC 27566-1 "Shall" Requirements → ACCS1:2026 Sections	89
D.3	Testing and Indicators - Cross-Standard Mapping.....	97
D.4	Certificates, Schedules and Transparency	97
D.5	Use of the Mapping	98

Annex E – Competency and Learning Resources (informative)..... 99

E.1	Purpose	99
E.2	Status of the Competency and Learning Resources	99
E.3	Maintenance of Competency and Learning Resources.....	100



Introduction

This document sets out the technical conformity assessment requirements applicable to age assurance systems and components certified under the Age Check Certification Scheme (ACCS). It is the scheme-specific technical counterpart to ACCS 0, which governs the general operation of the scheme, the requirements for Participating Conformity Assessment Bodies (CABs) and the certification process framework.

Age assurance systems utilise one or more methods (age verification, age estimation, age inference or successive validation) to produce an age assurance result. This document establishes the requirements for demonstrating, evaluating and documenting conformity of those systems and components with ISO/IEC 27566-1:2025. It specifies requirements for practice statements, testing methodology, Stage One and Stage Two evaluation, evaluation review, certification documentation, surveillance and recertification and any extension of scope.

Certification under this document forms part of the ACCS Type 6 product certification scheme, as described in ISO/IEC 17067, and is undertaken by Conformity Assessment Bodies in accordance with ISO/IEC 17065 and ACCS 0:2026. Certification may apply to complete age assurance systems or to individual components - for example binding modules, liveness detection components or orchestration layers - where those components are presented separately for certification.

Previous Editions

ACCS 1:2026 supersedes ACCS 1:2025 in its entirety. References to requirements in previous editions of ACCS 1 do not apply to certification under this edition unless expressly stated otherwise.

ISO/IEC 27566 series

ISO/IEC 27566-1:2025 is the principal technical standard for certification under this document. Other parts of the ISO/IEC 27566 series may be incorporated into the scheme through future revisions of ACCS 1 where relevant.



1. Scope

1.1 Purpose and Application

- 1.1.1 This document specifies the technical conformity assessment requirements for the certification of age assurance systems and components under the Age Check Certification Scheme (ACCS). It applies to Certification Clients seeking certification to ISO/IEC 27566-1:2025 - Age Assurance Systems - Part 1: Framework.
- 1.1.2 This document applies to the certification of:
- a) complete age assurance systems operated by Age Assurance Providers, Intermediaries or Relying Parties
 - b) individual components within age assurance systems - including age verification components, age estimation components, age inference components, binding mechanisms, liveness detection components, successive validation systems and orchestration layers - where those components are presented separately for certification
- 1.1.3 This document applies to the following categories of Certification Client:
- a) **Age Assurance Providers** - entities responsible for providing age assurance results to relying parties, either directly or via application programming interfaces or intermediaries
 - b) **Relying Parties** - entities that depend upon an age assurance result to make an age-related eligibility decision
 - c) **Intermediaries** - entities that facilitate interactions between individuals, providers and relying parties, or that provide supporting infrastructure for the exchange of age assurance results

NOTE: The requirements applicable to each category of Certification Client differ in certain respects, as specified in Sections 4.2 to 4.4 and throughout this document.

1.2 Scope Boundaries

- 1.2.1 This document applies to the age assurance target of evaluation as defined and recorded in the Practice Statement. Certification under this scheme applies only to the defined scope and does not extend to:
- a) the information society service, platform, website or venue in which the age assurance system is deployed, except to the extent that a Relying Party is itself the Certification Client
 - b) content moderation policies, age-related eligibility rules or commercial terms of the Certification Client or any Relying Party
 - c) the legal compliance of the Certification Client's organisation as a whole
 - d) systems, components or functions outside the declared scope boundaries, contexts of use or jurisdictions recorded in the Schedule of Certification

- 
- 1.2.2 The general scheme requirements applicable to certifications issued under this scheme - including requirements for Participating CABs, the certification process, surveillance, recertification, complaints, appeals and the scheme levy - are set out in ACCS 0:2026. This document is to be read together with ACCS 0:2026. Where this document is silent on a matter of process or governance, ACCS 0:2026 applies.

NOTE 1: This document does not independently certify conformity with data protection legislation, including UK GDPR or equivalent national frameworks. Where privacy characteristics are assessed under this scheme, the assessment confirms conformity with the privacy requirements of ISO/IEC 27566-1 - it is not a legal compliance determination.

*NOTE 2: This scheme is designed for global application. Where regulatory frameworks in specific jurisdictions impose requirements additional to or differing from those in ISO/IEC 27566-1, those requirements are addressed as jurisdictional requirements under **Sections 5.8 and 8.7**, as applicable, and recorded as local indicators in the Practice Statement.*

2. Normative References

2.1 Normative references

- 2.1.1 The following documents are normative to this document. For dated references, only the edition cited applies. For undated references, the latest edition (including any amendments) applies.

Reference	Title
ISO/IEC 27566-1:2025	Information security, cybersecurity and privacy protection - Age assurance systems - Part 1: Framework
ACCS 0	Age Check Certification Scheme - General Scheme Rules (undated - current edition)

2.2 Bibliography

- 2.2.1 The following documents are not normative to this document but are referenced in its provisions or provide relevant guidance or methodology for Participating CABs, Authorised Test Laboratories and Certification Clients.

Reference	Title	Relevance
IEEE 2089.1:2024 (as amended March 2026)	Online Age Verification Systems	Source material informing the ACCS classification accuracy framework in Section 5
ISO/IEC/IEEE 29119 series	Systems and software engineering - Software testing	Expected methodology for test design, planning and reporting under Section 7.4 and 8. Auditors should confirm alignment with this series or document the equivalent approach used
ISO/IEC 25000 series	Systems and software Quality Requirements and Evaluation (SQuaRE)	Product quality characteristics framework informing relevant functionality, performance and acceptability assessment criteria in Section 9
ISO/IEC 30107 series	Biometric presentation attack detection	Applicable to liveness detection and binding evaluation where relevant to the target of evaluation
ISO/IEC 19795-1:2021	Biometric performance testing and	Applicable to the testing of biometric-based age estimation



Reference	Title	Relevance
	reporting - Part 1: Principles and framework	or verification where relevant to the target of evaluation
ISO/IEC 42001:2023	Artificial intelligence management systems	Applicable where AI-driven estimation is within the certified scope
ISO/IEC TR 24027:2021	Bias in AI systems and AI-aided decision-making	Applicable to demographic fairness assessment, particularly in relation to the outcome error parity requirements of Section 5.6
ISO/IEC 29115:2013	Entity authentication assurance framework	Applicable to binding assurance results to individuals. Note: identity assurance frameworks may be applicable in some jurisdictions
ISO/IEC 24760 series	Identity management framework	Applicable to interoperability and secure exchange of age assurance results between providers, intermediaries and relying parties
ISO/IEC 27701:2025	Privacy information management systems - Requirements and guidance	Relevant supporting evidence for privacy assessment under Section 9.7 and recognition of external evidence under Section 8.10
ISO/IEC 27001	Information security management systems	Relevant to management system baseline assessment and to the audit effort reduction provisions of Annex A
ISO 10007:2017	Quality management - Guidelines for configuration management	Basis for configuration management requirements under Section 6.7

Note on exhaustiveness: This bibliography is not exhaustive. Other international standards, national standards or regulatory guidance documents may be identified and applied where relevant to a specific target of evaluation, its context of use or its applicable jurisdictions. Auditors and Authorised Test Laboratories should identify and apply the appropriate standards when designing test plans and conducting evaluations, having regard to the role, context of use and potential attack vectors relevant to the target of evaluation.



3. Terms and Definitions

3.1 Interpretation

3.1.1 In this document and in all ACCS implementing procedures:

- **"shall"** indicates a requirement
- **"should"** indicates a recommendation
- **"may"** indicates a permission
- **"can"** indicates a possibility or a capability

GUIDANCE NOTES are shown in italic text. They are intended to assist the reader in understanding provisions and do not add to or reduce requirements.

3.1.2 The interpretation and application of these verbal forms in conformity assessment activities shall be in accordance with ACCS-P07 – Interpretation and Application of Requirements. In particular, the use of “should” shall not be interpreted as meaning that a provision is automatically optional or may be disregarded. Its applicability and the manner in which it is addressed shall be evaluated having regard to the Target of Evaluation and its relevant context of use.

3.1.3 When citing ACCS documents, the convention is: document reference, comma, section number, for example ACCS 0, 4.3.

3.1.4 The terms in the following documents may be used for interpretation of terms in this document:

- **ISO/IEC 2382** (current edition) - *Information technology - Vocabulary* - which provides the foundational vocabulary for information technology concepts used in this document, including terms relating to systems, components, software, data and processing.
- **ISO/IEC 27000** (current edition) - *Information security management systems - Overview and vocabulary* - applies to information security and privacy concepts used in this document and is not repeated here.

3.2 Terms defined in normative documents

3.2.1 The terms and definitions established in the following normative documents apply to this document and are not repeated here:

- **ISO/IEC 27566-1:2025** — the terms and definitions in Clause 3 apply.
- **ACCS 0** — the terms and definitions established in Section 3 apply.



3.3 Objects of Certification

3.3.1 target of evaluation

defined age assurance system, subsystem or component presented for certification under this scheme, with explicit scope boundaries, contexts of use and version or deployment references.

NOTE 1: Certification can apply to a complete age assurance system or to an individual component - for example a binding module, liveness detection function, identity document scanning module or orchestration service - provided the component can be defined with sufficient boundary precision to enable repeatable evaluation.

NOTE 2: The target of evaluation is identified in the Certification Agreement and further defined in accordance with Section 4.

3.3.2 context of use

declared operating environment for a target of evaluation, comprising the sector or sectors of operation, the channel or channels of operation, the intended use type and the jurisdiction or jurisdictions of deployment

NOTE 1: ISO/IEC 27566-1:2025, 5.6 addresses context in use as a functional characteristic but does not define it as a term. This definition provides the specific dimensions required for certification scoping under this scheme.

NOTE 2: A single target of evaluation can be certified for multiple contexts of use. Where multiple contexts apply, each context is separately declared under Section 4.7 and audit effort is calculated accordingly under Annex A.

3.3.3 age gate

numeric age threshold against which an age assurance result is evaluated for the purpose of determining age-related eligibility

NOTE 1: An age gate can represent a minimum age threshold or a maximum age threshold.

NOTE 2: A target of evaluation can be certified for more than one age gate. Each age gate is separately identified in the Age Assurance Method Register where applicable.

3.4 Technical and Process Concepts

3.4.1 private practice statement

comprehensive practice statement maintained by the Certification Client that describes the practices, procedures and controls employed in relation to the target of evaluation and contains the information and evidence necessary to support conformity assessment

NOTE 1: The Private Practice Statement is the primary documentary basis for Stage One evaluation and is made available to the Participating CAB and, where applicable, the Authorised Test Laboratory. It is not intended for public disclosure.



NOTE 2: The Private Practice Statement contains the detailed information necessary to support evaluation, including information that may be commercially sensitive, security-sensitive or otherwise inappropriate for public disclosure.

NOTE 3: Requirements for the preparation, content and maintenance of the Private Practice Statement are set out in Section 6.

SOURCE: ISO/IEC 27566-1:2025, 3.1.14, modified — the scheme-specific term distinguishes the comprehensive practice statement used for conformity assessment from the Public Practice Statement.

3.4.2 **public practice statement**

publicly available practice statement that provides information about the certified target of evaluation and its practices, procedures and controls at a level appropriate for public disclosure

NOTE 1: The Public Practice Statement provides transparency about the certified system or component without requiring disclosure of information that is commercially sensitive, security-sensitive or otherwise inappropriate for public disclosure.

NOTE 2: The Public Practice Statement is derived from information represented in the Private Practice Statement but is a separate controlled document. It does not replace the Private Practice Statement for the purposes of conformity assessment.

NOTE 3: Requirements for the preparation, content, publication and maintenance of the Public Practice Statement are set out in Section 6.

SOURCE: ISO/IEC 27566-1:2025, 3.1.14, modified — the scheme-specific term distinguishes the publicly available practice statement from the Private Practice Statement used for conformity assessment.

3.4.3 **classification accuracy level**

scheme classification assigned to the demonstrated classification accuracy of an age assurance method at a specified age gate

NOTE 1: The classification accuracy levels used under this scheme are Basic, Effective, Highly Effective and Strict.

NOTE 2: The requirements applicable to each classification accuracy level are specified in Section 5.

3.4.4 **deployment mode**

manner in which an age assurance result is intended to be used following completion of an age assurance process

NOTE 1: Deployment modes under this scheme are single-use, reusable or both.

NOTE 2: In a single-use deployment, the age assurance result is intended for use in relation to the transaction, interaction or eligibility decision for which it was produced. In a reusable deployment, the result or an age-related assertion derived from it is capable of being used for subsequent transactions, interactions or eligibility decisions without repeating the original age assurance process.



3.4.5 **continuous monitoring**

ongoing review of the operational performance of a certified target of evaluation throughout the certification period, to detect changes in classification accuracy, outcome error parity, security, privacy or acceptability that may affect continued conformity.

NOTE: Continuous monitoring supplements but does not replace scheduled surveillance audits. Requirements for continuous monitoring are set out in Section 11.4.

3.4.6 **Age Assurance Method Register**

structured record established by the Lead Auditor at the opening of Stage Two evaluation, recording each discrete permutation of age assurance method, age gate and claimed classification accuracy level, and carrying the Lead Auditor's conformity determinations for each entry

NOTE 1: The Age Assurance Method Register provides the basis for determining the age assurance methods and configurations recorded in the final Practice Statement.

NOTE 2: The structure of the register and the process for completing it are set out in Section 9.3.



4. Target of Evaluation

4.1 General

- 4.1.1 The target of evaluation shall be defined with sufficient precision to enable repeatable evaluation and to establish the boundaries within which certification applies.
- 4.1.2 The target of evaluation shall identify the system or component presented for certification, the role of the Certification Client, its applicable boundaries and contexts of use and any other characteristics necessary to determine the applicable certification requirements and evaluation activities.

NOTE: The Target of Evaluation can comprise a complete age assurance system or an individually identifiable component of an age assurance system.

4.2 Age Assurance Providers

- 4.2.1 Where the Certification Client is an age assurance provider, the target of evaluation shall identify:
- a) the name, including deployment or version reference, of the target of evaluation
 - b) the operating parameters, including:
 - a. any process limitations
 - b. prerequisites for operation
 - c. tethering or connectivity requirements
 - d. technological dependencies
 - e. performance throttling or exclusions applied to outputs
 - f. whether the system operates online, offline or both
 - g. the goods, content, services, venues or spaces for which it is designed
 - h. the jurisdictions in which it is intended to operate (which may be global)
 - i. whether age assurance results are intended for single-use or reusable contexts
 - c) a technical architecture diagram showing the high-level interaction between the target of evaluation and relevant parties (the individual, intermediaries, relying parties)
 - d) where applicable, identification of the international standards to be applied for testing and analysis of the component (e.g. ISO/IEC/IEEE 29119 for test methodology, ISO/IEC 25000 for quality attributes, ISO/IEC 30107 for presentation attack detection)



4.3 Relying Parties

- 4.3.1 Where the Certification Client is a relying party, the target of evaluation shall identify:
- a) the relevant organisational footprint of the Relying Party, including where the target of evaluation is deployed
 - b) the goods, content, services, venues or spaces in which the system or component is deployed
 - c) the age-related eligibility requirements established by the relying party (e.g. age limits or age bands)
 - d) the jurisdictions in which the relying party operates (which may be global)
 - e) any other relevant specifications, performance requirements, regulatory obligations or practical requirements specified by the relying party

4.4 Intermediaries

- 4.4.1 Where the Certification Client is an intermediary, the target of evaluation shall identify:
- a) the name, including deployment or version reference, of the component or function under analysis
 - b) the function performed by the intermediary, including its relationships and responsibilities toward providers, relying parties, individuals or other parties
 - c) the process limitations, technological requirements or other parameters applicable to the component or function under analysis
 - d) the jurisdictions in which the component or function operates (which may be global)

4.5 Declaration of Threats and Attack Vectors

- 4.5.1 Known or reasonably anticipated attack vectors relevant to the Target of Evaluation shall be identified and recorded, including, where applicable, presentation attacks, injection attacks, synthetic media attacks and iterative probing (“hill-climb”) attacks.

4.6 Definition of Boundaries

- 4.6.1 The Certification Client shall define the boundaries of the target of evaluation with sufficient precision to enable repeatable evaluation. The boundary definition includes, as applicable:
- a) a high-level architecture diagram identifying:
 - a. the target of evaluation
 - b. the interfaces with other systems, components or intermediaries
 - c. the flow of data and results between parties (individuals, intermediaries, relying parties)

- d. any dependencies on external systems or services
- b) documentary identification of:
 - a. the name of the system or component
 - b. the version, issue or deployment reference
 - c. the date of release or deployment
 - d. the jurisdictions and contexts of use covered by this certification
- c) a statement of scope boundaries, which should specify:
 - a. what functions, processes or methods are included in the certification
 - b. what functions, processes or methods are explicitly excluded from certification
 - c. any assumptions, prerequisites or conditions necessary for operation within the certified scope
- d) where relevant, reference to the applicable international standards or normative specifications against which each component within the boundary will be analysed.
- e) The certified scope shall reflect those boundaries as verified during Stage Two evaluation and shall be documented in accordance with Sections 9.11 and 10.4.

4.7 Contexts of Use

- 4.7.1 The contexts of use applicable to the target of evaluation shall be declared in accordance with Section 3.3.2

The declaration shall identify, as applicable:

- a) Sector(s) in which the system or component operates (for example: retail and convenience, licensed hospitality, gambling, regulated entertainment/social media and content, body modification or other)
- b) Channel(s) of operation (offline, online or both)
- c) Intended use of age assurance results (single-use or reusable)
- d) Jurisdiction(s) of deployment, including:
 - a. specific countries
 - b. regional groupings (such as EU, US, APAC)
 - c. global application

- 4.7.2 Where multiple contexts of use apply, the Participating CAB should determine whether testing, analysis and audit effort must be applied separately or in combination, considering sectoral requirements, jurisdictional regulations and risk of harm.

GUIDANCE NOTE: The Scheme Owner provides reference templates to support the scoping and initial call process – ACCS-T02 – Initial Call and Scoping Report - available through the ACCS document portal and listed in ACCS 0, Annex A. Use of the reference template is not mandatory, but any equivalent document used by the Participating CAB must contain all the elements required by Sections 4.1 to 4.8.



4.8 Data Dependencies, Assumptions and Exclusions

Data Dependencies

- 4.8.1 The Certification Client shall declare all data sources utilised by the target of evaluation. For each data source, the Certification Client should identify:
- a) whether it is an authoritative source (e.g. government-issued identity document, verified digital credential or accredited register)
 - b) whether it is a non-authoritative or secondary source (e.g. credit reference, mobile network operator, social signals or self-asserted information)
 - c) any conditions, contractual arrangements or trust frameworks that govern the use of the data
 - d) any dependencies on third-party services for access to or validation of the data
- 4.8.2 The declaration of data dependencies should form part of the scoping documentation and be reviewed at surveillance and recertification audits.

Assumptions and Exclusions

- 4.8.3 The Certification Client shall declare any assumptions that underpin the correct operation of the target of evaluation. Such assumptions may include, but are not limited to:
- a) environmental conditions (e.g. lighting levels, network connectivity, device capabilities)
 - b) demographic coverage (e.g. minimum dataset size or population representativeness)
 - c) operational practices (e.g. requirement for human oversight or fallback procedures)
- 4.8.4 The Certification Client shall declare any exclusions from the scope of certification, such as:
- a) explicit age groups for which the system or component is not intended (e.g. under 13s)
 - b) contexts of use not supported (e.g. offline use only, not suitable for mobile deployment)
 - c) functions or methods excluded from the certified boundary



5. Classification Accuracy Levels

5.1 Purpose

5.1.1 This section establishes the performance classification framework for the target of evaluation certified under this scheme. The framework defines the minimum classification accuracy thresholds, demographic parity requirements and measurement parameters that underpin the four classification accuracy levels used throughout this scheme.

5.1.2 The classification framework is informed by the performance levels described in IEEE 2089.1:2024, Annex A as amended in March 2025. For the purposes of certification under this scheme, four classification accuracy levels are used: Basic, Effective, Highly Effective and Strict. Self-asserted age does not provide a classification accuracy level for certification under this scheme.

NOTE 1: The ACCS classification accuracy level names differ from the corresponding accuracy levels in IEEE 2089.1:2024, Annex A. ACCS “Effective” corresponds to the IEEE “Standard” accuracy level and ACCS “Highly Effective” corresponds to the IEEE “Enhanced” accuracy level. This correspondence relates to the applicable accuracy thresholds and does not constitute certification to an IEEE 2089.1 level of age assurance.

NOTE 2: The thresholds specified are normative requirements of this scheme. Amendment of the source material from which they were derived does not alter these requirements unless ACCS 1 is formally revised in accordance with ACCS 0, Section 13.

5.2 Classification Accuracy Levels

5.2.1 The four classification accuracy levels used under this scheme are:

- a) **Basic** - suitable for lower-risk applications
- b) **Effective** - suitable for moderate-risk applications
- c) **Highly Effective** - suitable for high-risk applications
- d) **Strict** - suitable for very high-risk applications

5.2.2 The classification accuracy levels achieved by a target of evaluation is determined by the lowest level achieved across all applicable performance dimensions. A system or component may achieve a higher level on some dimensions; the certified indicator is that of the lowest dimension achieved.

5.3 Classification Accuracy Requirements

5.3.1 Each age assurance method presented for certification shall demonstrate classification accuracy at or above the minimum threshold for the classification accuracy level claimed.

- 5.3.2 The primary measure of accuracy under this scheme is adapted from the underage detection rate in IEEE 2089.1, Annex A, Table A.2 as amended in March 2026 - the proportion of users below the declared age threshold correctly identified and excluded by the system. This is assessed alongside the false positive rate (incorrect rejection of users above the threshold) and the failure to acquire rate.
- 5.3.3 The minimum requirements for each indicator of effectiveness are set out in Table 1.

Table 1 – ACCS Classification Accuracy Framework

Indicator of Effectiveness	Underage Detection Rate (min)	False Positive - Adult Rejection (max)	Failure to Acquire (max)	Outcome Error Parity (max)
Strict	99%	1%	1%	1%
Highly Effective	95%	3%	1%	1%
Effective	90%	5%	1%	1%
Basic	50–90%	10%	1%	1%

Source: Performance thresholds draw on IEEE 2089.1:2024, Annex A, Table A.2 as amended in March 2026. The thresholds in this table are normative requirements of this scheme.

NOTE 1: Underage detection rate refers to the proportion of users below the declared age threshold correctly identified relative to that threshold.

NOTE 2: False positive (adult rejection) refers to users above the threshold incorrectly classified as underage and refused access.

NOTE 3: Failure to acquire (including liveness-related failures) is reported separately from classification accuracy and is not included in classification accuracy calculations. See Section 8.11 for test report content requirements.

NOTE 4: These thresholds apply to classification outcomes and exclude transactions that fail to complete. The distinction between failure to acquire and misclassification is documented in the test report in accordance with Section 8.11.

NOTE 5: Outcome error parity may be specified independently of the overall accuracy level.

NOTE 6: Where systems apply a higher operational threshold (a "challenge age"), accuracy should be assessed against that threshold for routing purposes. Overall system accuracy should be assessed based on the final determination relative to the regulatory age threshold. Where appropriate, systems should report both routing performance at the operational threshold and final classification performance at the regulatory threshold.

NOTE 7: Some methods, including certain age estimation techniques, may not achieve higher accuracy levels as standalone approaches and may require combination with additional methods to meet those levels.

- e) otherwise makes direct testing at the sample size required to establish statistical confidence impracticable

5.4.4 The use of analysis by proxy shall be justified and documented in the test plan. The justification should identify the limitation affecting direct testing, the alternative evidence to be relied upon, the methodology by which that evidence will be analysed, and any resulting limitations on the conclusions that may be drawn.

5.4.5 Analysis by proxy may include one or more of the following approaches, individually or in combination:

- a) Independent analysis of internally generated test evidence - Where the provider has conducted testing using datasets, Participatings, simulations or operational information that cannot practicably be reproduced independently at equivalent scale, the conformity assessment may include an independent analysis of that testing. The analysis should consider, as applicable:
 - i. the design and suitability of the test methodology
 - ii. the provenance, composition and relevance of the test data or population
 - iii. the conditions and configurations under which testing was performed
 - iv. the controls applied to establish ground truth
 - v. the statistical methodology and treatment of uncertainty
 - vi. the completeness and integrity of test records
 - vii. whether the reported conclusions are supported by the underlying results
 - viii. the potential for selection, methodological or reporting bias
- b) Analysis of decision logic and inference methodology - Where an age assurance result is derived from behaviour, profiling, accumulated information, rules, algorithms, policy decisions or other inference processes that cannot reasonably be assessed through conventional point-in-time population testing, the analysis may examine the logic and evidential basis by which the age-related inference is produced. The analysis should consider whether:
 - i. the characteristics or behaviours relied upon have an objectively supportable relationship with the age-related inference being made
 - ii. the rules, weightings, thresholds or policy decisions applied to those characteristics are reasonable and supported by evidence
 - iii. contrary or ambiguous indicators are appropriately treated
 - iv. the accumulation of information over time is sufficient to support the inference claimed
 - v. the methodology avoids assumptions or proxies that could produce materially unreliable or discriminatory outcomes
 - vi. uncertainty is appropriately recognised in the resulting age assurance outcome



- vii. the resulting inference remains consistent with the indicators of effectiveness claimed in the practice statement
- c) Aggregate population and outcome analysis - Where sufficiently large volumes of operational results are available, the distribution of age assurance outcomes may be compared with reliable external population, demographic or other reference data relevant to the declared context of use. The analysis should consider whether the distribution of outcomes produced by the system is reasonably consistent with the expected characteristics of the relevant population and should investigate material or unexplained divergence.

For example, where a system identifies a materially greater proportion of a population as belonging to a particular age or age group than could reasonably be expected from reliable population data for the relevant context, this may provide evidence of systematic error, calibration issues or inappropriate inference.

Aggregate population analysis can take account of differences between the actual user population and the general population, including selection effects, service demographics, geography, sector, channel and other factors capable of explaining an observed difference. Population comparison should therefore be used as corroborative evidence and should not, without further justification, be treated as a direct measure of individual classification accuracy.

- 5.4.6 Analysis by proxy should not be used solely because it is less costly, quicker or more convenient than direct testing. Where direct testing is reasonably practicable and necessary to establish conformity with an applicable requirement or claimed indicator of effectiveness, appropriate direct testing should be undertaken.
- 5.4.7 Wherever practicable, conclusions derived through analysis by proxy should be supported through triangulation of evidence, combining two or more sources such as direct testing, independently sampled provider testing, analysis of decision logic, operational monitoring, aggregate population analysis, external testing or other competent evidence.
- 5.4.8 The test report shall identify:
 - a) which conclusions are supported by direct testing and which rely wholly or partly upon analysis by proxy
 - b) the methodology and evidence used
 - c) the reason direct testing was not reasonably practicable
 - d) the extent of any independent sampling, replication or corroboration undertaken
 - e) assumptions and limitations affecting the analysis
 - f) any restriction that those limitations place upon the indicators of effectiveness or claims of conformity that may be reported



NOTE 1: Testing should consider performance for users close to the age threshold. Higher error rates are commonly observed near the threshold boundary and, where observed, should be documented separately in the test report.

NOTE 2: Analysis by proxy does not reduce the level of confidence required to support a certification decision. It provides an alternative means of obtaining objective evidence where conventional direct testing cannot reasonably provide that evidence. The strength of any conclusion should reflect the quality, independence, relevance and combination of the evidence available.

5.5 Successive Validation and Multi-Method Systems

- 5.5.1 Where a target of evaluation uses successive validation or multiple age assurance methods, classification accuracy shall be determined for each separately identifiable method or configuration for which a classification accuracy claim is made.
- 5.5.2 A classification accuracy claim for a combined or successive validation process shall be supported by evidence demonstrating the performance of that process as configured and deployed.
- 5.5.3 Where a system includes components or steps outside the control of the Certification Client, the scope of the system under assessment shall be clearly defined in the scope definition under Section 4.
- 5.5.4 Individual components may be assessed separately and will each carry their own component classification accuracy level in the Practice Statement.

5.6 Demographic Fairness and Outcome Error Parity

- 5.6.1 Outcome error parity shall be assessed for all systems and components under analysis.
- 5.6.2 Where material disparities in classification accuracy exist between demographic groups - including groups defined by gender, skin tone, age band, accessibility needs or environmental conditions - these should be declared in the Stage Two audit report and considered in determining the indicators of effectiveness.

5.7 Date of Birth Requirements

- 5.7.1 This scheme does not require the use or retention of a specific date of birth as a default. Where a regulatory authority or relying party requires the use of a specific date of birth as part of the age assurance process - for example in certain online gambling jurisdictions - this requirement may be applied within any indicator level. Such a requirement should be:
 - a) identified in the scope definition under Section 4

- 
- b) declared in the practice statement
 - c) recorded on the Practice Statement as a jurisdictional condition

NOTE: The use of a specific date of birth in the process does not of itself affect the indicator of effectiveness achieved.

5.8 Jurisdictional Requirements

- 5.8.1 Where national regulators or statutory instruments specify minimum classification accuracy thresholds that exceed those in Table 1, those thresholds shall apply in addition to the requirements of this section for certifications within the relevant jurisdiction. Local or jurisdictional indicators shall be reported alongside the scheme indicators in the Practice Statement.



6. Practice Statements

6.1 General Requirements

- 6.1.1 All Certification Clients seeking certification shall prepare a Private Practice Statement and a Public Practice Statement in accordance with ISO/IEC 27566-1, Clause 10 and this section.
- 6.1.2 The Private Practice Statement shall represent the Certification Client's formal claim of conformity and serve as the primary basis for assessment under this scheme.
- 6.1.3 Practice statements under this scheme exist in two forms:
- a) a **Private Practice Statement**, containing the information necessary to support conformity assessment; and
 - b) a **Public Practice Statement**, containing the information appropriate for public disclosure.
- 6.1.4 The Public Practice Statement shall contain the information specified in Annex B for public disclosure. Information that is commercially sensitive, security-sensitive or otherwise inappropriate for public disclosure may be omitted from the Public Practice Statement provided that it is included, where required, in the Private Practice Statement.

NOTE: Detailed information concerning mechanisms used to detect, prevent or mitigate attack vectors should not be included in the Public Practice Statement where disclosure could compromise the security or effectiveness of those mechanisms.

6.2 Content of Practice Statements

Core Content Requirements

- 6.2.1 The practice statement shall, at a minimum, contain the elements required by ISO/IEC 27566-1, Clause 10, which differ according to whether the Certification Client is an age assurance provider, a relying party or an intermediary. Those elements are not repeated here - see ISO/IEC 27566-1, Clauses 10.2, 10.3 and 10.4 respectively.
- 6.2.2 Where applicable, the practice statement may identify the relevant international standards applied for testing or analysis of the target of evaluation.



Additional Content Requirements

- 6.2.3 In addition to the applicable requirements of ISO/IEC 27566-1, the Private Practice Statement shall contain the information necessary to define and support evaluation of the target of evaluation, including, as applicable:
- a) the identified needs of relying parties that the system or component is intended to meet
 - b) the sources of data used, distinguishing authoritative sources from non-authoritative or secondary sources and the management of those dependencies
 - c) how the system or component ensures the correct handling of date information
 - d) the functional characteristics of the system or component, including suitability, completeness, correctness and appropriateness
 - e) the claimed indicator of effectiveness (Basic, Effective, Highly Effective or Strict) for each component or for the system as a whole
 - f) any publicly available specifications with which the Certification Client asserts conformity
 - g) performance efficiency claims, including intended time, throughput, resource utilisation and capacity parameter
- 6.2.4 The Public Practice Statement shall contain the information specified in Annex B and sufficient information to describe the certified Target of Evaluation, its contexts of use, applicable classification accuracy levels, material limitations or conditions and the basis of certification.

6.3 Basis for Assessment

- 6.3.1 Statements made in the initial draft Private Practice Statement constitute claims to be evaluated and do not, by themselves, demonstrate conformity.
- 6.3.2 The assessment shall determine whether the claims made in the practice statement are:
- a) supported by objective evidence from testing, analysis and audit
 - b) consistent with the scope boundaries and contexts of use declared under Section 4
 - c) aligned with the normative references and scheme requirements

6.4 Updates and Maintenance

- 6.4.1 The Practice Statements submitted for certification shall reflect the target of evaluation as presented for assessment and shall be updated where necessary to reflect changes identified during evaluation.

- 
- 6.4.2 The requirements for maintenance of Practice Statements following certification are set out in ACCS 0, Section 7.4 and Section 11.7 of this document

6.5 Structured Submission

- 6.5.1 Practice Statements should follow the structure provided in Annex B or an equivalent structure that enables the applicable requirements and supporting evidence to be readily identified and evaluated.

6.6 Practice Statement Review

- 6.6.1 The Lead Auditor shall review the Private Practice Statement to determine whether:
- a) the applicable requirements of ISO/IEC 27566-1, Clause 10 are addressed
 - b) the Target of Evaluation and applicable contexts of use are adequately described
 - c) the claims made are sufficiently clear to support evaluation and test planning
 - d) the supporting evidence necessary for Stage One evaluation has been identified or provided
- 6.6.2 Omissions or ambiguities that prevent effective evaluation should be resolved before completion of Stage One.

6.7 Configuration Management

- 6.7.1 Where the target of evaluation permits variable configuration, the Private Practice Statement shall describe the available configuration settings and the information necessary to evaluate conformity with ISO/IEC 27566-1, 5.5.
- 6.7.2 The Practice Statement should identify configuration settings that can materially affect functionality, performance, privacy, security or acceptability.

6.8 Change Control, Documentation and Record Keeping

- 6.8.1 The Private and Public Practice Statement shall include a version reference and date of issue.
- 6.8.2 The Certification Client shall identify the authority responsible for approving and maintaining its Practice Statements.



7. Stage One Evaluation

7.1 Purpose of Stage One Evaluation

7.1.1 The Stage One evaluation establishes whether the Certification Applicant has provided sufficient documented information and objective evidence to enable Stage Two evaluation to proceed effectively.

7.1.2 Stage One includes review of the Private Practice Statement, the definition of the Target of Evaluation, applicable classification accuracy claims, relevant supporting documentation and the proposed testing approach.

NOTE: Stage One does not determine conformity with ISO/IEC 27566-1. Documentary claims and evidence identified at Stage One are evaluated for conformity through the applicable Stage Two activities.

7.1.3 For the purposes of this scheme, the Lead Auditor shall have demonstrable knowledge of:

- a) the requirements of ISO/IEC 27566-1:2025 and the performance framework for age assurance systems
- b) age assurance system evaluation generally, sufficient to direct the audit team, assess the adequacy of technical evidence and make independent conformity determinations under Section 9.6

7.1.4 The audit team as a whole shall collectively cover the following areas of technical competence:

- a) software and systems testing methodology, with reference to at least one of ISO/IEC/IEEE 29119, ISO/IEC 19795 or ISO/IEC 30107 as applicable to the system under analysis
- b) data protection and privacy requirements applicable to age assurance systems, including the privacy characteristics of ISO/IEC 27566-1:2025 Clause 7
- c) the security threat landscape for age assurance systems, including the attack vectors identified in Section 4.5

NOTE: Where the Lead Auditor does not personally hold competence in one or more of the areas in Section 7.1.3, the audit team should include a technical expert with the requisite competence. The identity, organisation, competence and proposed scope of work of any such expert should be declared in the Stage One audit plan (ACCS-T03) in accordance with Section 7.3.1. The Participating CAB retains full responsibility for all technical expert outputs.

7.1.5 The competency and learning resources identified in Annex E provide informative guidance for CABs, ATLs, auditors, technical assessors and other competent personnel on the interpretation and application of individual clauses and subject areas of ISO/IEC 27566-1. They may be used to support competency development, audit and test planning, auditor enquiry,



identification and consideration of objective evidence and the exercise of professional judgement.

7.2 Stage One Audit Plan

7.2.1 The Stage One audit plan prepared in accordance with ACCS 0 shall identify, as applicable:

- a) the Target of Evaluation and applicable version or deployment reference
- b) the contexts of use for which certification is sought
- c) the age assurance methods within scope
- d) the classification accuracy levels claimed
- e) applicable jurisdictional requirements
- f) the ISO/IEC 27566-1 and ACCS 1 subject matter to be addressed during Stage One.

7.3 Testing Plan

7.3.1 The testing plan shall be prepared and approved by the Participating CAB before the Stage One audit report is completed.

7.3.2 The testing plan shall be prepared by the Participating CAB or by the Authorised Test Laboratory engaged in accordance with ACCS 0 and ACCS-P02.

7.3.3 The testing plan shall include:

- a) identification of the person or ATL responsible for testing and confirmation that the applicable competence and impartiality requirements have been met
- b) the private practice statement version reference on which the testing plan is based
- c) acceptance criteria for each of the five core characteristics, mapped to the classification accuracy claims in the practice statement, mapped to the test specification identified under Section 8
- d) a normative requirements coverage mapping confirming that the test methods selected collectively cover all applicable ACCS1 and ISO/IEC 27566-1 requirements within the agreed scope
- e) attack vector testing approach, identifying the attack vectors relevant to the system and the planned testing approach for each
- f) any national or jurisdictional requirements applicable to the test programme and how they will be addressed
- g) the testing schedule, deliverables, staffing and subcontracting arrangements.

7.3.4 Where testing is subcontracted, the Participating CAB retains full responsibility for all subcontracted outputs and shall confirm that the



subcontractor is subject to equivalent impartiality and competence requirements.

- 7.3.5 Testing activities conducted under this scheme - whether by the Participating CAB itself or by an Authorised Test Laboratory - are conducted solely as part of the conformity assessment cycle. They do not constitute a standalone testing service and test results are not issued as standalone laboratory reports.

NOTE: The Scheme Owner provides a reference template for the testing plan – ACCS-T04 - available through the ACCS document portal and listed in ACCS 0, Annex A.

7.4 Privacy Documentation

- 7.4.1 The Stage One evaluation should confirm that the Private Practice Statement and supporting documentation contain sufficient information to enable the privacy characteristics applicable to the Target of Evaluation to be evaluated at Stage Two, including, where applicable:
- a) the categories and sources of personal data processed
 - b) the purposes and flows of personal data relevant to the Target of Evaluation
 - c) retention and deletion arrangements
 - d) applicable privacy controls and data-subject mechanisms
 - e) relevant independent certifications or assessments relied upon as supporting evidence.

7.5 Risk Management and Attack Vectors

- 7.5.1 The Stage One evaluation should confirm that the Certification Client has supplied documentation demonstrating:
- a) risks relevant to the Target of Evaluation, including reasonably foreseeable misuse and harms
 - b) the risk-based rationale supporting declared assumptions, dependencies and exclusions under Section 4.8
 - c) relevant attack vectors identified under Section 4.5 and the controls or mitigations intended to address them

7.6 Monitoring and Continuous Improvement

- 7.6.1 The Stage One evaluation should confirm that the Certification Applicant has provided documentation describing the arrangements used to monitor the continuing performance and effectiveness of the Target of Evaluation, including processes for internal review and improvement where applicable.



7.7 Stage One Audit Report

- 7.7.1 The audit report prepared in accordance with ACCS 0 shall additionally record:
- a) the Target of Evaluation, applicable version or deployment reference and contexts of use
 - b) the age assurance methods and classification accuracy levels claimed
 - c) the status of documentary review against the five core characteristics of functionality, performance, privacy, security and acceptability
 - d) the outcome of the testing plan review
 - e) any ACCS 1-specific matters that must be addressed at Stage Two
- 7.7.2 Stage One is subject to the Stage One Quality Assurance Review requirements in ACCS 0, Section 6.15

8. Testing Requirements

8.1 Purpose and Testing Framework

8.1.1 Testing under this scheme provides objective evidence to support Stage Two evaluation of the Target of Evaluation against the applicable requirements of ISO/IEC 27566-1 and this document.

8.1.2 Testing and technical evidence evaluation operate through two complementary approaches:

- a) **Track A — direct testing:** testing conducted by the Participating CAB or an Authorised Test Laboratory using appropriate test methods, datasets, tools, simulations or proxy methods
- b) **Track B — external evidence evaluation:** review of relevant evidence supplied by the Certification Applicant, including operational performance data, user experience studies, accessibility assessments and other testing or evaluation evidence

8.1.3 The testing plan shall identify the requirements addressed through each approach and the evidence relied upon

8.1.4 The five core characteristics of ISO/IEC 27566-1 - functionality, performance, privacy, security and acceptability - are mapped to the ISO/IEC 25010:2023 product quality model and to the testing types and levels in ISO/IEC/IEEE 29119-1:2022 as follows:

ISO/IEC 27566-1 characteristic	ISO/IEC 25010:2023 quality characteristics	ISO/IEC/IEEE 29119-1 testing types	Notes
Functionality (Clause 5)	Functional suitability - completeness, correctness, appropriateness	Functional testing; system testing; acceptance testing	Covers age assurance method operation, binding, result delivery and configuration management
Performance (Clause 6)	Performance efficiency - time behaviour, resource utilisation, capacity; Reliability - fault	Performance testing; stress testing; load testing; capacity testing;	Includes classification accuracy, underage detection rate, false positive rate



ISO/IEC 27566-1 characteristic	ISO/IEC 25010:2023 quality characteristics	ISO/IEC/IEEE 29119-1 testing types	Notes
	tolerance, availability	reliability testing	and outcome error parity
Privacy (Clause 7)	Security - confidentiality, accountability; Interaction capability - user error protection	Security testing; functional testing of privacy controls	Covers data minimisation, data disposal, audit log generation and consent mechanisms - measurable privacy characteristics assessed in laboratory; policy compliance assessed at audit
Security (Clause 8)	Security - integrity, non- repudiation, authenticity, resistance; Reliability - fault tolerance	Security testing; penetration testing; reliability testing; fail- safe testing	Covers replay and forwarding protection, biometric presentation attack detection, spoofing and counterfeiting resistance, contra- indicator handling and fail-safe behaviour
Acceptability (Clause 9)	Interaction capability - appropriateness, recognisability, operability, user error protection, user engagement, inclusivity,	Accessibility testing; usability testing; functional testing	Outcome error parity by demographic assessed through stratified performance testing; user

ISO/IEC 27566-1 characteristic	ISO/IEC 25010:2023 quality characteristics	ISO/IEC/IEEE 29119-1 testing types	Notes
	accessibility; Safety - operational constraint		experience evidence reviewed from Certification Client- supplied testing

8.1.5 The testing levels applicable under this scheme are:

- a) **Component testing** - where the scope of certification covers an individual age assurance component (e.g. a facial age estimation module, a liveness detection function or a document verification service), testing shall be conducted at component level against the characteristics applicable to that component
- b) **System testing** - where the scope of certification covers a complete age assurance system, testing shall be conducted at system level against all five core characteristics
- c) **Acceptance testing** - the test report (Reference 08) and its conclusions constitute the evidence base for the Stage Two acceptance determination by the Participating CAB. Testing under this scheme is not product acceptance testing in the commercial sense; it is conformity assessment testing

8.1.6 The primary test design techniques applicable under this scheme are:

- a) **Specification-based techniques** - used for functional, performance and acceptability testing, including equivalence partitioning (age bands, demographic groups), boundary value analysis (ages near the declared threshold), decision table testing (access grant/deny logic) and requirements-based testing (mapping claims in the practice statement to test conditions)
- b) **Experience-based techniques** - used for security and attack vector testing, including error guessing and exploratory testing for novel attack patterns not covered by pre-defined test cases
- c) **Statistical methods** - used for performance and outcome error parity testing, including confidence interval analysis, non-inferiority testing and stratified analysis across demographic groups, in accordance with Section 8.8



8.2 Competence of Test Analysts

8.2.1 Test Analysts conducting testing under this scheme shall have demonstrated competence appropriate to the testing activities assigned to them, including:

- a) knowledge of ISO/IEC 27566-1 and the applicable requirements of this document
- b) competence in the test methods and technologies applicable to the Target of Evaluation
- c) competence in statistical methods where classification accuracy, outcome error parity or other statistical claims are evaluated
- d) where applicable, competence in biometric performance testing, presentation attack testing, security testing, usability or accessibility evaluation.

8.2.2 General competence, impartiality and authorisation requirements for Test Analysts and Authorised Test Laboratories are governed by ACCS 0 and ACCS-P02.

8.3 Development of Test Plans

8.3.1 The testing plan shall translate the applicable requirements, claims and acceptance criteria for the Target of Evaluation into a test programme capable of producing sufficient objective evidence for Stage Two evaluation. The Participating CAB should ensure that each test plan:

- a) specifies the scope and objectives of testing, consistent with the scope of the target of evaluation defined under Section 4
- b) identifies the components, functions or characteristics to be tested and any explicitly excluded
- c) maps each declared claim in the practice statement to a corresponding test or analysis, with acceptance criteria linked to the claimed indicator of effectiveness
- d) confirms coverage of all applicable normative requirements of this scheme and ISO/IEC 27566-1 within the agreed scope, identifying any requirements addressed at audit rather than through laboratory testing and the rationale for each
- e) records the pre-declared statistical framework in accordance with Section 8.8 before testing commences
- f) specifies entry and exit criteria appropriate to the scope of testing, and defines test completion criteria
- g) records of any national or jurisdictional requirements applied to the test programme and how they have been addressed, in accordance with Section 8.7

- 
- 8.3.2 Test plans shall be reviewed and approved by the Participating CAB before Stage Two testing proceeds, in accordance with Section 7.3 and the Stage One QA Review in ACCS 0, 6.15.

8.4 Test Coverage

- 8.4.1 Functional and performance testing can be designed using ISO/IEC/IEEE 29119 test design techniques, selected in accordance with the nature of the target of evaluation.

- 8.4.2 Test coverage should include, at a minimum:
- a) functional suitability - completeness, correctness and appropriateness of the age assurance function
 - b) classification accuracy - assessed against the declared age threshold in accordance with Section 5.3, using the underage detection rate as the primary metric
 - c) performance efficiency - response time, throughput and scalability, including under simulated load conditions
 - d) resistance to relevant attack vectors - presentation attacks, injection attacks, deepfake and synthetic media attacks, replay attacks and iterative probing attacks, as applicable to the target of evaluation
 - e) measurable privacy characteristics as declared in the practice statement - including data minimisation, data disposal procedures and audit log generation - assessed by technical testing against ISO/IEC 27566-1 Clause 7. Privacy policy compliance is assessed at Stage Two audit, not through laboratory testing
 - f) security and acceptability characteristics, as declared in the practice statement and assessed against ISO/IEC 27566-1 Clauses 8 and 9 respectively, including outcome error parity measured by demographic subgroup (false positive and false negative rates by age band, gender and skin tone)
 - g) user experience and acceptability - assessed by review of Certification Client-supplied UX testing evidence, accessibility assessments and user research, conducted against criteria specified in the testing plan. Where the Certification Client has not supplied adequate UX testing evidence, the Lead Auditor may raise this as a nonconformity at Stage One

NOTE: Where biometric accuracy testing is conducted using static datasets - for example still photography or pre-recorded video - liveness detection may be disabled for that test, provided this is declared in the testing plan and reflected in the scope limitations on the Schedule of Certification. This approach is consistent with ISO/IEC 19795 test methodology for biometric component evaluation. Testing of liveness detection itself is conducted as a separate test activity using PAD test sets in accordance with ISO/IEC 30107-3.

8.5 Sample Size and Demographic Requirements

Sampling methodology

- 8.5.1 For Basic level claims, simple random sampling is permitted.
- 8.5.2 For Effective, Highly Effective and Strict level claims, stratified random sampling by demographic subgroup may be applied. Test datasets should include subjects across declared strata. Datasets may be:
- a) vendor-supplied, subject to the data integrity controls in Section 8.9
 - b) independently sourced benchmark datasets with documented provenance and ground truth labelling
 - c) a combination of the above
- 8.5.3 Where vendor-supplied datasets are used, the Participating CAB or Authorised Test Laboratory shall apply the anti-gaming controls in Section 8.9 before any analysis is conducted.
- 8.5.4 The minimum number of subjects per stratum should be specified in the test plan before testing commences. Where a stratum falls below its declared minimum, the Test Analyst shall notify the Participating CAB before testing proceeds. The Participating CAB may determine whether to proceed with a reduced sample, limit the scope of certification, apply analysis by proxy (see Section 5.4) or require additional recruitment.

Stratified floor requirements

- 8.5.5 The following minimum per-stratum floors apply. National or jurisdictional requirements may supersede these floors where they are more stringent:

Indicator	Total minimum	Per key stratum minimum	Demographic requirements	Underage detection rate (min) - see Section 5, Table 1
Basic	≥60	≥10	No stratification required	50–90%
Effective	≥150	≥25	At least one demographic group	90%
Highly Effective	≥400	≥50	≥3 skin tone groups and ≥2 genders	95%
Strict	≥1,000	≥100	≥3 skin tones, ≥2 genders and ≥2 device types	99%

NOTE: These are minimum floors for laboratory testing using controlled datasets. Where a Certification Client can supply credible operational data demonstrating sustained performance in production across the relevant strata, the Participating CAB may accept this as supplementary evidence under Section 8.8.3, subject to documented data quality controls.

NOTE: The underage detection rate thresholds in the final column are normative requirements from Section 5, Table 1, reproduced here for ease of reference. In the event of any conflict, Section 5 prevails.

- 8.5.6 The sampling and recruitment process should be documented in the test plan, including the recruitment source, eligibility criteria, stratum allocation method and how stratum counts were verified before testing commenced.
- 8.5.7 Key strata should reflect the declared contexts of use and known risk factors including age bands, gender, skin tone, accessibility needs and device or channel type.
- 8.5.8 Test populations should include variation in age, gender, skin tone, accessibility needs and environmental conditions, unless exclusions are justified and declared under Section 4.8.3 – 4.8.4.

8.6 Classification Accuracy Levels

- 8.6.1 Classification accuracy shall be determined for each age assurance method, configuration or combined process for which a classification accuracy level is claimed, in accordance with Section 5.
- 8.6.2 Where different methods or configurations achieve different classification accuracy levels, the test report shall record the level demonstrated for each

8.7 Jurisdictional Requirements

- 8.7.1 Where jurisdictional requirements identified under Section 5.8 require additional or modified testing, those requirements shall be incorporated into the testing plan and evaluated using appropriate acceptance criteria.

8.8 Statistical Assurance Framework

Pre-registration

- 8.8.1 Before testing commences, the test plan shall pre-register all of the following, where applicable to the test methodology adopted:
 - a) primary endpoints and performance thresholds
 - b) non-inferiority or equivalence margins (Δ) where applicable
 - c) stopping rules, including any interim looks and early stopping conditions for success or futility

- 
- d) the analysis method - confidence interval (frequentist) or credible interval (Bayesian) - and for Bayesian approaches, the declared priors
 - e) alpha level or coverage probability
 - f) stratification plan and stratum minimum floors in accordance with Section 8.5.5
 - g) approach to handling missing data, incomplete samples or test transactions that fail to complete, and any protocol deviations

8.8.2 Pre-registration constitutes the boundary of confirmatory analysis. Any analysis conducted outside pre-declared parameters should be treated as exploratory and should not be used as the primary basis for a certification determination.

Acceptance rules

- 8.8.3 Performance claims shall be evaluated against the classification accuracy levels in Section 5.3 using the following approach:
- a) **Non-inferiority:** A claim at a given indicator level is accepted if the one-sided lower confidence bound (or credible interval lower bound) for the underage detection rate meets or exceeds the threshold for that level
 - b) **Sequential or adaptive designs:** Where group-sequential or sequential probability ratio test (SPRT) designs are used, early stopping for success is permitted where the interim lower bound meets or exceeds the threshold plus the pre-declared margin (δ). Testing continues to the next declared interim look if the interim result is inconclusive
 - c) **Demographic fairness:** Per-stratum lower bounds should be reported for all key strata. Where any stratum lower bound falls below the applicable local or jurisdictional minimum, the Participating CAB should determine, having regard to the Test Analyst's findings, whether a mitigation plan, additional testing or a scope limitation is required
 - d) **Operational corroboration at recertification:** Where automated continuous monitoring (Section 11.4) demonstrates sustained performance at or above the certified threshold, with documented statistical process controls (e.g. CUSUM), a reduced confirmatory sample may be accepted at recertification. The basis for the reduction should be documented in the test plan and reviewed at the Evaluation Review

Risk-based sample allocation

- 8.8.4 Where risk-based sampling is used, the test plan should set minimum per-stratum floors in accordance with Section 8.5.5. Where risk-based sampling is used, the test plan should identify higher-risk strata and the rationale for any additional sample allocation to those strata - including younger age cohorts close to the declared threshold, accessibility groups and under-represented skin tone categories.

- 
- 8.8.5 Where external evidence (Section 8.10) or operational monitoring data is used to reduce new sampling requirements, the test plan should document:
- a) data lineage and provenance of the external or operational data
 - b) quality controls applied to that data
 - c) the statistical method used for integration - for example meta-analytic priors or propensity weighting

Integrity of analysis by proxy

- 8.8.6 Where analysis by proxy is used in accordance with Section 5.4, the statistical assurance framework should take account of the nature, strength and limitations of the proxy evidence. The use of analysis by proxy does not, of itself, reduce the level of assurance required to support the applicable indicator of effectiveness or certification determination.
- 8.8.7 The Test Analyst should determine the evidential weight that may reasonably be attributed to proxy evidence, taking into account:
- a) the independence and competence of the party responsible for generating the underlying evidence
 - b) the provenance, quality, completeness and representativeness of the underlying data
 - c) the extent to which the conditions, population, configuration and context represented by the evidence correspond to the certified scope
 - d) the extent of independent review, sampling, replication or validation undertaken
 - e) the strength of the objective evidence supporting any assumptions, decision logic or inference methodology
 - f) the relevance and comparability of any external population or aggregate data used
 - g) the degree of uncertainty associated with extrapolating from the proxy evidence to the claimed performance of the system or component
- 8.8.8 Where proxy evidence is combined with direct testing, operational monitoring or other evidence, the method used to combine or triangulate those sources should be defined in the test plan. The methodology should avoid double-counting evidence derived from the same underlying data, population, model or test activity and should identify any material dependencies between evidence sources.
- 8.8.9 Proxy evidence may be used to corroborate a performance determination, support a reduction in the amount of new direct testing required, or provide evidence in respect of characteristics that cannot reasonably be established through conventional population testing. Any reduction in direct sample size should be justified by the strength and relevance of the additional evidence and documented in the test plan.

- 
- 8.8.10 Where the analysis by proxy does not itself provide a statistically representative measure of individual system performance, it should not be treated as though it produces an equivalent confidence or credible interval. In particular, analysis of algorithmic logic, policy rules or aggregate population outcomes should not, without an appropriate statistical basis, be converted into a numerical classification accuracy or confidence level.
- 8.8.11 Where such evidence is relied upon, the Test Analyst should distinguish between:
- a) statistical evidence of performance, derived from observations capable of supporting a quantified performance estimate
 - b) corroborative evidence, supporting or challenging the plausibility and consistency of the observed performance
 - c) analytical evidence, supporting a determination that the underlying logic, assumptions or inference being made is objectively reasonable
- 8.8.12 Where different forms of evidence produce materially inconsistent conclusions, the inconsistency should be investigated and resolved before the evidence is relied upon for certification. The most favourable result should not be selected solely because it supports the claimed indicator of effectiveness.
- 8.8.13 The statistical assurance reported should reflect the combined strength of the evidence actually available. Where the limitations of analysis by proxy prevent the applicable statistical threshold from being demonstrated, the Evaluation Review should determine whether additional evidence or testing is required or whether the resulting certification scope, indicator of effectiveness or conformity statement should be limited accordingly.

8.9 Data Integrity and Anti-Gaming Controls

- 8.9.1 Testing used to support certification shall be designed and conducted so as to minimise the risk that prior knowledge, sample selection, configuration changes, repeated testing or selective reporting could materially bias the result.
- 8.9.2 The following controls apply to all test programmes:
- a) Where vendor-supplied datasets are used, data should be locked and split into design and confirmatory sets before any analysis is conducted. The confirmatory set should not be used for any exploratory analysis. This requirement applies where vendor-supplied or pre-collected datasets are used. It does not apply to live system testing conducted via direct API or interface interaction.
 - b) Interim data should not be examined outside pre-declared interim looks. Any deviation from pre-declared looks should be recorded as a protocol deviation and assessed for its impact on the validity of results.

- 
- c) Full traceability should be maintained throughout the test programme, including dataset version references, random number seeds where applicable, code versions, software environment and any deviations from the test plan.
 - d) Sufficient traceability information should be recorded to allow the test methodology and results to be independently verified and, where technically feasible, reproduced.

8.10 Recognition of External Testing

- 8.10.1 External test results may be used as objective evidence where the Participating CAB determines that they are relevant, sufficiently current and technically suitable for the Target of Evaluation and the certification requirements concerned.
- 8.10.2 In determining the weight to be given to external testing in accordance with ACCS 0, Section 6.13, the Participating CAB should consider:
 - a) competence and independence of the testing body
 - b) accreditation status and scope, where applicable
 - c) test methodology and acceptance criteria
 - d) sample composition and statistical validity
 - e) version and configuration tested
 - f) contexts of use and jurisdictions covered
 - g) age and continuing relevance of the evidence
 - h) availability of sufficient underlying records to verify the conclusions.
- 8.10.3 Where external testing has been conducted by a laboratory or CAB accredited by a GAC member body within the scope of that accreditation, substantial weight shall be given to those results. Where testing was conducted outside accreditation scope or by a non-accredited body, the Participating CAB shall determine whether additional confirmatory testing is required. In either case, reference to the external test results and the weight assigned shall be recorded in the test report.

8.11 Execution of Testing

- 8.11.1 Testing shall be conducted in accordance with the approved testing plan as reviewed and approved at Stage One.
- 8.11.2 The Test Analyst or Authorised Test Laboratory shall document all deviations from the approved testing plan during execution, including the reason for each deviation and its assessed impact on result validity. Deviations shall be reported in the test report in accordance with ACCS-T08 and Section 8.12.1(a).

- 
- 8.11.3 Testing shall be conducted in a manner that is systematic and consistent, with sufficient records to allow an independent reviewer to verify the approach taken and the validity of results.
- 8.11.4 Test data, test environments and configuration settings shall be controlled, documented and retained for audit throughout the testing programme and for a minimum period consistent with the retention requirements in ACCS 0, Section 10.

8.12 Test Report - Content and Records

- 8.12.1 Testing activities shall be documented in a test report. The test report shall:
- confirm that testing was conducted in accordance with the approved testing plan, identifying any deviations and their assessed impact on result validity
 - record test results for each of the five core characteristics - functionality, performance, privacy, security and acceptability - with pass or fail determination against the acceptance criteria specified in the test plan
 - record the review of Certification Client-supplied user experience testing evidence, including the methodology, Participating demographics, key findings and the ATL's assessment of its adequacy and credibility for the purposes of the acceptability characteristic determination
 - record all defects and nonconformances identified across all test domains, classified by severity (Critical, High, Medium, Low or Informational), domain, relevant requirement reference and remediation status
 - where applicable to the Target of Evaluation, the completion rate for each age assurance method evaluated, including the basis used to determine initiation and successful completion
 - provide a consolidated statistical analysis summary including total test cases executed, overall pass rate, defects by severity, number of open unresolved defects, confidence intervals for key metrics, the statistical methodology applied, and any assumptions or limitations
 - state the indicator of effectiveness achieved for each component and for the system as a whole
 - state any conditions, caveats or scope limitations on the overall conclusion, including exclusions declared under Section 4.8.3 – 4.8.4
 - include recommendations for Stage Two audit consideration, including any areas requiring further examination
- 8.12.2 The test report shall be retained by the Participating CAB and made available for the Evaluation Review.

NOTE: The scheme recognises that maintaining a standing pool of live human test subjects - particularly children - is not operationally feasible for a commercial Authorised Test

-



9. Stage Two Evaluation

9.1 Purpose of Stage Two Evaluation

- 9.1.1 Stage Two is the substantive technical evaluation of the Target of Evaluation against the applicable requirements of ISO/IEC 27566-1:2025 and this document.
- 9.1.2 Stage Two builds upon the documentary review completed at Stage One and evaluates, through objective evidence, whether the applicable certification requirements are fulfilled.
- 9.1.3 Stage Two is conducted in accordance with ACCS 0, Section 6.16. Findings, nonconformities and their resolution are governed by ACCS 0.
- 9.1.4 The Stage Two evaluation has five aims:
- a) to assess conformity against each of the five core characteristics of ISO/IEC 27566-1 - functionality, performance, privacy, security and acceptability
 - b) to translate the ATL's technical test report findings into the Lead Auditor's independent conformity determinations, expressed in the scheme's conformity categories
 - c) to confirm, for each age assurance method and age gate claimed, the indicator of effectiveness that is supported by objective evidence and that will be stated in the Practice Statement
 - d) to agree the final private practice statement and public practice statement with the Certification Client, incorporating any amendments required by Stage One findings or test report outcomes
 - e) to produce the draft Certificate of Conformity, Schedule of Certification and Public Practice Statement front sheet, ready for handover to the Evaluation Review

9.2 Stage Two Audit Plan

- 9.2.1 Stage Two shall be conducted in accordance with the confirmed Stage Two audit plan. The plan shall have been agreed with the Certification Client before Stage Two commences and shall have been confirmed as adequate at the Stage One QA Review.

9.3 Age Assurance Method Register

- 9.3.1 At the opening of Stage Two, the Lead Auditor shall establish an Age Assurance Method Register containing a separate entry for each discrete permutation of age assurance method, age gate and claimed classification accuracy level.

- 
- 9.3.2 Each row in the register shall record:
- a) the method type - age verification, age estimation or age inference
 - b) the specific age assurance method
 - c) the age gate - the numeric age threshold only
 - d) the classification accuracy level claimed for that method at that age gate - Basic, Effective, Highly Effective or Strict
 - e) the deployment mode - single-use, reusable or both
- 9.3.3 Two further determinations can be completed within the register during the course of Stage Two, and not before the relevant assessment section is complete:
- a) **After Section 9.6 (Performance Characteristics):** whether the claimed classification accuracy level for each row is supported by objective evidence from the test report - Yes or No
 - b) **After Section 9.10 (Private Practice Statement Assessment):** whether each row is accurately and consistently reflected in the final private practice statement - Yes or No
- 9.3.4 The completed register, with both determinations made, is the primary source document for the final certified Public and Private Practice Statements. Only entries for which both determinations under 9.3.3 are affirmative can be included within the certified scope and recorded in the final certification documentation.
- 9.4 **Age Assurance Methods Assessment (ISO/IEC 27566-1 Clause 4)**
- 9.4.1 The Stage Two evaluation shall assess conformity for each method type declared in the Age Assurance Method Register against the applicable requirements of ISO/IEC 27566-1 Clause 4.
- 9.4.2 For **age verification** methods, the assessment shall confirm that:
- a) identity documents used are genuine (ISO/IEC 27566-1, 4.3.2(a))
 - b) the document is associated with the correct individual (ISO/IEC 27566-1, 4.3.2(b))
 - c) the document is not expired (ISO/IEC 27566-1, 4.3.2(c))
 - d) the document has not been revoked or suspended at the time of use (ISO/IEC 27566-1, 4.3.2(d))
- 9.4.3 For **age estimation** methods, the assessment shall confirm that:
- a) the method does not process more personal data than is necessary (ISO/IEC 27566-1, 4.3.3(a))
 - b) the method is designed to minimise misclassification risk at the stated age threshold (ISO/IEC 27566-1, 4.3.3(b))



- c) the method meets the performance requirements for the claimed classification accuracy level (ISO/IEC 27566-1, 4.3.3(c))

- 9.4.4 For **age inference** methods, the assessment shall confirm that:
- a) only adequate, relevant and necessary data sources are used (ISO/IEC 27566-1, 4.3.4(a))
 - b) the data sources and signals used are disclosed (ISO/IEC 27566-1, 4.3.4(b))
 - c) the method meets the performance requirements for the claimed classification accuracy level (ISO/IEC 27566-1, 4.3.4(c))

- 9.4.5 Where the system employs **successive validation** - using more than one method in sequence (ISO/IEC 27566-1, 4.3.5) - conformity shall be assessed for each method independently and for the combined system.

9.5 Functional Characteristics (ISO/IEC 27566-1 Clause 5)

- 9.5.1 The Stage Two evaluation shall assess conformity against the functional characteristic requirements of ISO/IEC 27566-1 Clause 5, including:
- a) data acquisition for age assurance components (ISO/IEC 27566-1, 5.2), including correct date interpretation and date format handling
 - b) binding of the age assurance result to the correct individual (ISO/IEC 27566-1, 5.3), including anti-circumvention measures
 - c) age assurance data processing (ISO/IEC 27566-1, 5.4)
 - d) configuration management (ISO/IEC 27566-1, 5.5), including relying-party dashboard safeguards and the impact of configuration settings on performance, privacy, security and acceptability characteristics
 - e) context in use (ISO/IEC 27566-1, 5.6) and delivery of the age assurance result (ISO/IEC 27566-1, 5.7), including secure delivery and protection of the integrity and confidentiality of the result
- 9.5.2 The assessment of functional characteristics draws primarily on documentary evidence and the Lead Auditor's direct examination of the system, supplemented by the test report where functional testing has been conducted by the ATL.

9.6 Performance Characteristics (ISO/IEC 27566-1 Clause 6)

Test Report Review

- 9.6.1 The Lead Auditor shall assess the test report against the approved testing plan, applicable acceptance criteria and the performance claims recorded in the Age Assurance Method Register.

- 
- 9.6.2 Any material gap, anomaly or deficiency in the test evidence shall be resolved, or its effect on the scope and conformity determination established, before the applicable performance assessment is concluded.

Translation of ATL Findings into Lead Auditor Determinations

- 9.6.3 The test report contains the ATL's technical findings. The Lead Auditor's role is to assess those findings as an auditor and translate them into conformity determinations expressed in the scheme's conformity categories. This translation is not automatic - it involves professional judgement. The following principles govern it:
- a) A technical result in the test report that meets or exceeds the threshold for the claimed classification accuracy level does not automatically produce a conformity determination of "Conforms" - the Lead Auditor must also be satisfied that the testing methodology was appropriate, the sample was adequate, and there are no other material concerns about the result.
 - b) A technical result that falls below the threshold for the claimed level but meets the threshold for a lower level does not constitute a nonconformity - it is a scope adjustment. The Lead Auditor shall record the level actually supported by evidence in the Age Assurance Method Register and propose a scope limitation accordingly.
 - c) Where the test report contains a qualification, caveat or limitation on a result, the Lead Auditor should assess its materiality and determine whether it affects the conformity determination or the scope limitation on the Schedule of Certification.
 - d) Where the Lead Auditor's conformity determination differs from the ATL's conclusion, the Lead Auditor shall record the reason for the difference in the Stage Two audit report.

Performance Effectiveness (ISO/IEC 27566-1, 6.1)

- 9.6.4 The Stage Two evaluation shall assess conformity against each of the performance effectiveness requirements of ISO/IEC 27566-1, 6.1, with reference to the test report. The assessment shall address:
- a) whether the system correctly grants access to individuals who have been positively identified as age-eligible (ISO/IEC 27566-1, 6.1(a))
 - b) whether the system does not rely solely on self-asserted age (ISO/IEC 27566-1, 6.1(b))
 - c) whether the system provides a low and consistent spread of errors across different demographics - outcome error parity - taking into account the sensitivity of the context and the risk of exposing children to harm (ISO/IEC 27566-1, 6.1(c))
 - d) whether the age assurance result relates to the individual in question - correct binding (ISO/IEC 27566-1, 6.1(d))
 - e) whether data is managed in accordance with the privacy characteristics of Clause 7 (ISO/IEC 27566-1, 6.1(f))

- 
- f) whether the system is established in a way that is amenable to independent testing (ISO/IEC 27566-1, 6.1(g))
 - g) whether the system operates in accordance with applicable law in the deployment jurisdictions (ISO/IEC 27566-1, 6.1(h))

Indicators of Effectiveness (ISO/IEC 27566-1, 6.2)

9.6.5

The indicators of effectiveness are the scheme's principal mechanism for expressing the level of confidence that can be placed in an age assurance system's performance. The Lead Auditor shall assess each of the following indicators for each applicable method and configuration, with reference to the test report. Where an indicator does not apply to the method type under assessment, this shall be recorded with the reason.

- a) **False Rejection Rate (FRR)** (ISO/IEC 27566-1, 6.2.1) - the proportion of eligible individuals incorrectly denied access. A high FRR indicates over-restriction. The Lead Auditor shall confirm that the test report states the FRR for each applicable method and configuration and assess whether the reported FRR is acceptable in the context of use.
- b) **False Acceptance Rate (FAR)** (ISO/IEC 27566-1, 6.2.2) - the proportion of ineligible individuals, including children, incorrectly granted access. A high FAR represents a child protection failure. The Lead Auditor shall confirm that the test report states the FAR for each applicable method and configuration and assess whether the reported FAR is acceptable given the child protection context.
- c) **Age Estimation Accuracy** (ISO/IEC 27566-1, 6.2.3) - applicable to facial, voice and other biometric estimation methods. Expressed as mean absolute error (MAE) or equivalent metric. The Lead Auditor shall confirm that the test report states the age estimation accuracy for each applicable method and assess whether it is adequate for the context of use.
- d) **Classification Accuracy** (ISO/IEC 27566-1, 6.2.4) - the overall proportion of correct age-eligibility decisions across all individuals tested. This is the primary headline metric for certification purposes. The Lead Auditor shall confirm that the test report states the overall classification accuracy for each method and configuration tested, and shall determine whether the reported accuracy meets the threshold for the claimed level in accordance with Section 5, Table 1.
- e) **Presentation Attack Detection Performance** (ISO/IEC 27566-1, 6.2.5) - applicable to biometric and document-based methods. The Lead Auditor shall confirm that the test report addresses PAD performance for each applicable method and assess whether it is adequate for the context of use.
- f) **Calibration Error** (ISO/IEC 27566-1, 6.2.6) - the degree to which the system's confidence scores correspond to true likelihoods. The Lead Auditor shall confirm that the test report addresses calibration where applicable and assess whether the reported calibration is adequate.

- 
- g) **Completion rate** - the measurement and reporting of completion rate in accordance with ISO/IEC 27566-1:2025, 6.2.5, including the basis used to determine initiation and successful completion. Where completion rate is not measured or reported, the rationale shall be recorded.

Performance Metrics (ISO/IEC 27566-1, 6.3)

- 9.6.6 The Stage Two evaluation shall confirm that:
- a) classification accuracy level has been determined for each configuration of the system and is stated in the practice statement (ISO/IEC 27566-1, 6.3)
 - b) the system has evaluated and reported its scalability, including how performance characteristics change as the scale of operation changes (ISO/IEC 27566-1, 6.3)
 - c) the system is designed and operated in a manner that is capable of being independently tested (ISO/IEC 27566-1, 6.3)

Completion of Age Assurance Method Register - Performance Column

- 9.6.7 Following completion of Sections 9.6.1 to 9.6.6, the Lead Auditor shall complete the performance evidence column of the Age Assurance Method Register, recording for each row whether the claimed classification accuracy level is supported by objective evidence from the test report.

9.7 Privacy Characteristics (ISO/IEC 27566-1 Clause 7)

- 9.7.1 The Stage Two evaluation shall assess conformity against the privacy characteristics requirements of ISO/IEC 27566-1 Clause 7. The assessment draws on both the technical test report (for measurable privacy characteristics) and documentary evidence (for privacy by design, data subject rights and policy compliance). The Lead Auditor shall assess:

- a) privacy by design and default (ISO/IEC 27566-1, 7.2)
- b) data minimisation (ISO/IEC 27566-1, 7.3), including collection limitations, disclosure restrictions and access controls
- c) purpose limitation (ISO/IEC 27566-1, 7.3.4)
- d) user awareness (ISO/IEC 27566-1, 7.5) - the information provided to users about the age assurance process
- e) audit logs (ISO/IEC 27566-1, 7.6) - integrity protection and retention of access logs

- 9.7.2 Privacy policy compliance is assessed at Stage Two by documentary review. Measurable privacy characteristics - including data minimisation verification, data disposal and audit log generation - are evidenced by the test report.

GUIDANCE NOTE: Evaluation under this subsection determines conformity with ISO/IEC 27566-1 privacy characteristics and does not constitute a determination of compliance with applicable data protection law.

9.8 Security Characteristics (ISO/IEC 27566-1 Clause 8)

- 9.8.1 The Stage Two evaluation shall assess conformity against the security characteristics requirements of ISO/IEC 27566-1 Clause 8, including:
- a) general security requirements (ISO/IEC 27566-1, 8.1)
 - b) replay, forwarding and reuse protection (ISO/IEC 27566-1, 8.2)
 - c) resistance to attack (ISO/IEC 27566-1, 8.3) - including biometric presentation attacks, spoofing, counterfeiting and deepfake resistance
 - d) contra-indicators (ISO/IEC 27566-1, 8.4)
 - e) fail-safe behaviour (ISO/IEC 27566-1, 8.5) - default denial on system failure, cessation of data collection on component failure and logged remediation

9.9 Acceptability Characteristics (ISO/IEC 27566-1 Clause 9)

- 9.9.1 The Stage Two evaluation shall assess conformity against the acceptability characteristics requirements of ISO/IEC 27566-1 Clause 9, including:
- a) general acceptability (ISO/IEC 27566-1, 9.1)
 - b) inclusivity (ISO/IEC 27566-1, 9.2) - including accommodations for users unable to complete the standard age assurance process and outcome error parity across demographic groups
 - c) user engagement and assistance (ISO/IEC 27566-1, 9.3) - including the clarity and comprehensibility of information provided to users
 - d) complaint handling (ISO/IEC 27566-1, 9.4) - including written agreement between the age assurance provider and relying party on complaint handling responsibility
- 9.9.2 The acceptability assessment draws on outcome error parity data from the test report and on Certification Client-supplied UX testing evidence reviewed under Section 8.4.2(g). Where adequate UX evidence has not been supplied, this shall be recorded as a nonconformity.

9.10 Practice Statement Assessment and Finalisation

- 9.10.1 The Lead Auditor shall review the final Private Practice Statement against the evidence and findings obtained during evaluation before completion of Stage Two.
- 9.10.2 The review shall confirm that the Private Practice Statement:
- a) accurately describes the Target of Evaluation and its boundaries
 - b) identifies the applicable contexts of use
 - c) accurately records the age assurance methods and configurations evaluated
 - d) accurately records the classification accuracy levels demonstrated

- 
- e) reflects material assumptions, dependencies, exclusions and limitations identified during evaluation
 - f) does not contain claims of certified conformity that are unsupported by the Stage Two evidence

9.10.3 The Lead Auditor shall review the Public Practice Statement for consistency with the Private Practice Statement and the certified scope, having regard to the public disclosure requirements in Section 6.

Private Practice Statement

9.10.4 The Lead Auditor shall confirm the final content of the private practice statement with the Certification Client. The private practice statement shall:

- a) contain full technical detail including configuration settings, performance data and any commercially sensitive information provided to the Participating CAB under the Certification Agreement
- b) be version-controlled and approved by the Certification Client
- c) be retained in the certification record and referenced on the Schedule of Certification

Public Summary Practice Statement

9.10.5 The Lead Auditor shall agree the final content of the public practice statement with the Certification Client. The public practice statement shall:

- a) be derived from the private practice statement but contain only information suitable for public disclosure
- b) include at a minimum: the Certification Client's identity, the system or component certified, the age assurance method or methods deployed, the indicator of effectiveness achieved at each age gate and the jurisdictions of operation
- c) not include commercially sensitive configuration details or information that would compromise security by disclosure of attack vector mitigations
- d) be submitted to the Scheme Owner for publication on the ACCS public registry following the Evaluation Reviewer's certification decision, in accordance with ACCS 0, Section 7.3

9.10.6 Following completion of Sections 9.10.1 to 9.10.5, the Lead Auditor shall complete the practice statement column of the Age Assurance Method Register, recording for each row whether the entry is accurately and consistently reflected in the final practice statement.

9.11 Draft Certification Scope and Schedule

9.11.1 During Stage Two, the Lead Auditor shall prepare draft certification documentation for handover to the Evaluation Review. The certification documents will not be issued until the Evaluation Reviewer has made the



certification decision. The drafts prepared by the Lead Auditor are the input to that decision and shall be accurate and complete at the point of handover.

Certificate of Conformity

- 9.11.2 The draft Certificate of Conformity shall record:
- a) the full legal name and registered address of the Certification Client
 - b) the name of the product, system or process being certified - the Target of Evaluation
 - c) the proposed certificate reference number
 - d) the proposed Schedule of Certification reference number
 - e) the proposed date of issue and valid-until date (proposed issue date plus three years)
 - f) the name of the proposed Certification Decision Maker

Schedule of Certification

- 9.11.3 The Schedule of Certification is a document setting out the scope of certification and identifying and cross-referencing the applicable certified Practice Statement and other relevant certification documents and includes:
- a) the Schedule reference number and cross-reference to the Certificate of Conformity
 - b) the Target of Evaluation - name, version, deployment reference and release date
 - c) the Certification Client's role - age assurance provider, relying party or intermediary
 - d) material limitations, assumptions or exclusions affecting the certified scope
 - e) the title, version and date of the private practice statement

Public Practice Statement Front Sheet

- 9.11.4 The Lead Auditor should prepare a draft front sheet for the public practice statement. The front sheet should record:
- a) the Certification Client's name
 - b) the public summary practice statement title, version and date
 - c) the proposed date of certification - corresponding to the proposed date of issue on the Certificate of Conformity, subject to Evaluation Reviewer confirmation
- 9.11.5 The completed front sheet shall be appended to the public practice statement and submitted to the Scheme Owner registry following the Evaluation Reviewer's certification decision.

Cross-Document Consistency Check

- 9.11.6 Before handover for evaluation review, the Lead Auditor should confirm that the Certification Client name, address, proposed reference numbers, proposed dates and Target of Evaluation description are consistent across all three draft documents, and that the practice statement references on the Schedule correspond to the approved versions recorded in Sections 9.10.4 and 9.10.5.
- 9.11.7 The Lead Auditor should also confirm that the audit report contains references to all material records examined - including logs, configuration management records, monitoring data, complaint handling records and external certifications relied upon in accordance with Section 8.10 - sufficient to allow the Evaluation Reviewer to trace each conformity determination to its evidence base.
- 9.11.8 The Stage Two audit report includes standardised indicators of effectiveness reporting table for each certified component and for the system as a whole. The table records:
- a) component or system name and version
 - b) indicator of effectiveness achieved
 - c) classification accuracy achieved, with confidence interval lower bound
 - d) FRR, FAR and where applicable MAE, with confidence bounds
 - e) sample size and demographic coverage
 - f) applicable contexts of use and jurisdictions
 - g) any local or jurisdiction-specific indicators applied
 - h) limitations, assumptions and scope exclusions

9.12 Auditor's Recommendation and Handover

- 9.12.1 On completion of the Stage Two evaluation, the Lead Auditor shall prepare the Stage Two audit report and certification recommendation in accordance with ACCS 0.
- 9.12.2 The Stage Two evaluation record shall additionally include:
- a) the completed Age Assurance Method Register
 - b) the final test report and the Lead Auditor's assessment of it
 - c) the final Private and Public Practice Statements
 - d) the proposed certified scope and Schedule information
 - e) any technical limitations, conditions or unresolved matters relevant to the Evaluation Review or certification decision.



10. Evaluation Review, Certification Decision and Post-Certification

10.1 Purpose of Evaluation Review

- 10.1.1 Evaluation Review and the Certification Decision are conducted in accordance with ACCS 0, Sections 6.18 and 6.19.
- 10.1.2 This section specifies the additional matters applicable to Evaluation Review and certification documentation for certification under ACCS 1.

10.2 Evaluation Review

- 10.2.1 In addition to the requirements of ACCS 0, 6.18, the Evaluation Reviewer shall confirm that:
- a) the Target of Evaluation and its boundaries are consistently identified throughout the evaluation record
 - b) the applicable contexts of use and jurisdictional requirements have been addressed
 - c) each age assurance method and configuration included within the proposed certified scope is supported by the completed Age Assurance Method Register
 - d) each classification accuracy level included within the proposed certified scope is supported by appropriate test evidence
 - e) applicable outcome error parity requirements have been evaluated
 - f) the final Private Practice Statement accurately reflects the Target of Evaluation and the evidence obtained during evaluation
 - g) the Public Practice Statement is consistent with the certified scope and the Private Practice Statement
 - h) material assumptions, dependencies, limitations and exclusions identified during evaluation are appropriately reflected in the proposed Schedule of Certification
 - i) the proposed certified scope is supported by the evaluation evidence
- 10.2.2 The outcome of the ACCS 1-specific review shall be recorded as part of the Evaluation Review record required by ACCS 0.

10.3 Certification Decision

- 10.3.1 The certification decision shall be made in accordance with ACCS 0, Section 6.19.
- 10.3.2 A positive certification decision under this scheme applies only to the Target of Evaluation, contexts of use, methods, configurations, classification



accuracy levels and other characteristics supported by the completed evaluation record and identified within the certified scope.

10.4 Certificate of Conformity and Schedule of Certification - Issuance

10.4.1 The Certification documentation shall be issued in accordance with ACCS 0, Section 7 and the model documentation in Annex C.

10.4.2 For certification under this scheme, the Schedule of Certification shall identify or cross-reference, as applicable:

- a) the Target of Evaluation and applicable version or configuration
- b) the role or roles of the Certification Client
- c) the certified age assurance methods and applicable age gates
- d) the classification accuracy levels demonstrated
- e) the certified contexts of use
- f) applicable jurisdictional indicators
- g) material conditions, limitations or exclusions affecting the certified scope
- h) the applicable certified Practice Statement

10.5 Practice Statement Issuance

10.5.1 The version of the Private Practice Statement accepted at completion of the evaluation shall be identified as part of the certification record.

10.5.2 The Public Practice Statement shall be reviewed by the Participating CAB to confirm that it accurately represents the certified scope and is consistent with the Private Practice Statement.

10.5.3 The approved Public Practice Statement shall be identified by version reference and date and published in accordance with ACCS 0, Section 7.4.

10.5.4 Subsequent amendment of either Practice Statement during the certification period is governed by ACCS 0 and Section 11.7 of this document.

10.5.5 The Public Practice Statement applicable to certification under this scheme shall be made available through the ACCS Public Registry in accordance with ACCS 0, Section 7.5.

10.6 Regulatory Notifications

10.6.1 Where applicable law, regulatory requirements or an arrangement recognised by the Scheme Owner requires notification of certification to a



supervisory or regulatory body, the Participating CAB shall make or facilitate that notification in accordance with the applicable requirements.

NOTE: Certification under this scheme does not, by itself, constitute regulatory approval or authorisation.



11. Surveillance, Recertification and Ongoing Certification Obligations

11.1 Purpose and Governing Framework

11.1.1 Certification under this scheme is subject to the surveillance, certification monitoring and recertification requirements of ACCS 0, Section 6.20.

11.1.2 This section specifies the additional technical requirements applicable to ongoing certification of Targets of Evaluation certified under ACCS 1.

11.1.3 The certification period under this scheme shall not exceed three years.

11.2 Changes Relevant to Continued Certification

11.2.1 The following changes shall be notified and assessed as changes potentially affecting certification in accordance with ACCS 0, Section 8:

- a) addition, removal or substitution of an age assurance method within the Target of Evaluation
- b) addition or change of an age gate
- c) a model update, algorithm change, retraining or other material modification capable of affecting classification accuracy or outcome error parity
- d) a configuration change capable of materially affecting functionality, performance, privacy, security or acceptability
- e) a change to a certified context of use or jurisdiction that introduces new or changed certification requirements
- f) a material security incident, personal data breach or identified attack vector affecting the Target of Evaluation
- g) regulatory action or investigation materially relevant to the Target of Evaluation
- h) any other change capable of affecting the continuing validity of the certified scope or supporting evidence

11.3 Surveillance Audit Scope and Planning

11.3.1 In addition to the requirements of ACCS 0, surveillance planning under this scheme should take into account:

- a) changes to the Target of Evaluation, its boundaries, configurations and contexts of use
- b) the continuing accuracy of the Private and Public Practice Statements
- c) operational and continuous monitoring data generated since the previous evaluation

- 
- d) trends in classification accuracy, outcome error parity, failure rates and other relevant performance measures
 - e) changes in known or reasonably anticipated attack vectors, vulnerabilities and security incidents
 - f) complaints or other evidence relevant to continued conformity
 - g) new or changed jurisdictional requirements applicable to the certified scope.

11.3.2 Retesting is not required as a routine element of every surveillance activity. The Participating CAB shall determine whether retesting is necessary having regard to whether the evidence supporting certification remains current and applicable.

11.3.3 Retesting should normally be required where:

- a) a material change could affect a previously demonstrated technical characteristic or classification accuracy level
- b) monitoring data indicates a material or statistically significant deterioration in performance
- c) a security incident, newly identified attack vector or vulnerability raises credible doubt about previously evaluated security characteristics
- d) a new or changed jurisdictional requirement requires additional technical evaluation
- e) other objective evidence raises credible doubt about the continuing validity of the certification evidence

11.3.4 Where retesting is required, it shall be planned in accordance with Section 8 and proportionate to the change, concern or evidence giving rise to the requirement.

11.3.5 Each audit-based surveillance evaluation shall include:

- a) confirmation that the certified Target of Evaluation remains within the certified scope
- b) review of material changes notified or identified since the previous evaluation
- c) confirmation that the Private Practice Statement remains current and that the Public Practice Statement remains consistent with it
- d) review of monitoring results, incidents and complaints relevant to continued conformity
- e) review of configuration changes capable of affecting the certified characteristics

11.4 Continuous Monitoring

11.4.1 Where continuous or automated monitoring is used to support ongoing certification, the monitoring arrangements should be appropriate to the characteristics and operation of the Target of Evaluation and capable of



identifying material deviation from the conditions under which certification was granted.

- 11.4.2 Monitoring can include, as applicable:
- a) classification accuracy and related performance measures
 - b) outcome error parity
 - c) failure-to-acquire or failure-to-complete rates
 - d) changes in configuration or deployed version
 - e) security events, attacks and identified vulnerabilities
 - f) privacy incidents
 - g) complaints and operational anomalies
 - h) other measures relevant to the continuing validity of certification
- 11.4.3 Monitoring thresholds and escalation criteria should be established having regard to the certified classification accuracy level, statistical uncertainty, normal operational variation and the potential effect of a deviation on continued conformity.
- 11.4.4 A monitoring alert does not, by itself, constitute a nonconformity. Where monitoring identifies a material deviation or other concern, the Participating CAB shall investigate and determine the appropriate action in accordance with ACCS 0.

11.5 Surveillance Outcome

- 11.5.1 Surveillance reporting, evaluation review and post-surveillance certification are conducted in accordance with ACCS 0.
- 11.5.2 Where surveillance identifies a change to the certified Target of Evaluation, classification accuracy level, contexts of use, limitations or other information forming part of the certified scope, the certification documentation and Practice Statements shall be updated as applicable.

11.6 Recertification Requirements

- 11.6.1 Recertification shall reassess the full certified scope, with the nature and extent of evaluation activities determined in accordance with ACCS 0 and this section having regard to the continuing validity of existing certification evidence.
- 11.6.2 The Participating CAB shall determine the extent of retesting required at recertification by assessing whether the existing test evidence remains current, representative and applicable to the Target of Evaluation.
- 11.6.3 Full or substantial retesting should normally be required where:



- a) a material change has occurred to an age assurance method, age gate, model, algorithm or configuration relevant to the previous test evidence
- b) monitoring or surveillance results indicate material deterioration or instability
- c) changes in relevant attack vectors or vulnerabilities call previous security testing into question
- d) the contexts of use have materially changed
- e) new jurisdictional requirements require additional technical testing
- f) the age, methodology, provenance or continuing representativeness of the previous test evidence is insufficient to support a new certification decision

11.6.4 Existing test evidence and continuous monitoring data may be relied upon where the Participating CAB determines that they remain sufficiently current, representative and reliable to support recertification.

11.7 Practice Statement Maintenance During the Certification Period

11.7.1 The Certification Client shall maintain the Private Practice Statement so that it continues to accurately describe the certified Target of Evaluation throughout the certification period.

11.7.2 A change that would make information in the Private Practice Statement materially inaccurate, incomplete or misleading shall be notified to the Participating CAB in accordance with ACCS 0.

11.7.3 The Participating CAB shall determine whether the change:

- a) can be accommodated as an administrative amendment
- b) requires evaluation as a change affecting certification
- c) constitutes an extension of scope
- d) requires reassessment of the existing certified scope

11.7.4 Where an approved change affects information contained in the Public Practice Statement, the Public Practice Statement shall be updated so that it remains consistent with the certified scope and the current Private Practice Statement.



12. Extension of Scope

12.1 General

- 12.1.1 Extensions of scope are governed by ACCS 0, Section 6.21. This section specifies the additional technical requirements applicable to extension of scope under ACCS 1.

12.2 What Constitutes an Extension of Scope

- 12.2.1 For or certification under this scheme, an extension of scope includes, as applicable:
- a) addition of an age assurance method not included within the existing certified scope
 - b) addition of an age gate for an existing certified method
 - c) a claim to a higher classification accuracy level for an existing certified method, age gate or configuration
 - d) addition of a context of use not covered by the existing certification where additional evaluation is required
 - e) addition of a jurisdiction where new or different certification requirements apply
 - f) addition of a Certification Client role not included within the existing certified scope
 - g) addition of another product, component, configuration or deployment that materially extends the existing Target of Evaluation
- 12.2.2 A proposed change that does not require extension of the certified scope can be treated as an administrative amendment in accordance with ACCS 0. Where there is uncertainty, the Participating CAB shall determine the appropriate pathway having regard to whether additional evaluation is required to support the changed certification claim.

12.3 Retesting Requirements

- 12.3.1 The Participating CAB shall determine the evaluation activities required for the proposed extension having regard to the nature of the extension, the continuing applicability of existing certification evidence and the requirements of ACCS 0, Section 6.21.
- 12.3.2 The types of change set out in Table 2 are examples of changes that can constitute an extension of scope under this scheme. The Participating CAB shall determine whether a proposed change requires an extension of scope having regard to the existing certified scope, the nature and significance of the proposed change, and whether additional evaluation is required to support the resulting certification claim. The table identifies the principal

evaluation focus for each type of extension; the specific evaluation activities required shall be determined in accordance with Section 12.3.

Table 2: Extension of Scope Evaluation Requirements

Proposed extension	Minimum evaluation focus
New age assurance method	Applicable ISO/IEC 27566-1 requirements for the new method; interaction with the existing Target of Evaluation; applicable classification accuracy and other technical evidence
New age gate	Performance at the new threshold, including classification accuracy and outcome error parity; any consequential functional, privacy, security or acceptability effects
Higher classification accuracy level	Evidence demonstrating the applicable threshold in Section 5 for the relevant method, age gate and configuration
New context of use	Context-specific effects on functionality, performance, privacy, security and acceptability
New jurisdiction	Additional jurisdictional requirements under Section 5.8 and any consequential technical evaluation or testing
New Certification Client role	Applicable ISO/IEC 27566-1 requirements for the new role, including the applicable Practice Statement requirements
New product/component/configuration	Differences from the existing certified Target of Evaluation and any requirements or previous evidence affected by those differences

- 12.3.3 Testing under Section 8 shall be undertaken where the existing objective evidence is insufficient to demonstrate conformity of the proposed extended scope.
- 12.3.4 Where existing test evidence is relied upon, the Participating CAB shall determine its applicability to the proposed extension in accordance with Section 8.10.



Annex A - Calculation of Audit and Testing Effort (normative)

A.1 Purpose and Scope

- A.1.1 This annex specifies the scheme-specific factors and minimum effort requirements used to determine the audit and testing effort applicable to initial certification, surveillance, recertification and extension of scope under ACCS 1.
- A.1.2 Audit and testing effort shall be calculated in accordance with ACCS 0, ACCS-P04 and this annex. ACCS-P04 governs the common calculation process, administrative arrangements and Scheme Levy; this annex specifies the technical effort factors applicable to certification under ACCS 1.
- A.1.3 The calculated effort shall be sufficient to enable the Participating CAB and, where applicable, the Authorised Test Laboratory to complete the required evaluation activities and obtain sufficient objective evidence to support the certification process.

NOTE: The Scheme Owner provides an online calculation tool to assist Participating CABs with their calculation of audit effort.

- A.1.4 The calculation takes account of the nature, scale and complexity of the Target of Evaluation, the role or roles of the Certification Applicant, certification boundaries, age assurance methods and configurations, contexts of use, jurisdictions, classification accuracy levels claimed, required testing activities and the extent to which recognised prior conformity assessment evidence can be relied upon.

A.2 Structure of Effort

- A.2.1 Certification effort comprises:
- a) **CAB effort** — effort required for scoping, documentary evaluation, Stage One, Stage Two evaluation, Evaluation Review and other certification activities undertaken by the Participating CAB
 - b) **ATL effort** — effort required for testing and technical analysis undertaken by an Authorised Test Laboratory
- A.2.2 CAB and ATL effort shall be calculated and recorded separately.
- A.2.3 Total certification effort is:

Total Certification Effort = CAB Effort + ATL Effort

- A.2.4 The calculation should not assume that every activity applies to every applicant. Activities should be included where they are relevant to the Certification Client's role, certification boundary, system or components under analysis, contexts of use and certification claims.
- A.2.5 The CAB should maintain a record of the calculation showing the activities included, applicable values or factors, recognised prior certification and any adjustment made to the calculated effort.

A.3 Preparation and Scoping

- A.3.1 Preparation establishes the certification boundary and provides the information necessary to determine the subsequent assessment and testing effort. It shall include, as applicable:
- identification of the role or roles undertaken by the applicant as an Age Assurance Provider, Intermediary or Relying Party
 - identification of the system and components under analysis
 - establishment of the certification boundary and technical architecture
 - initial assessment of the Practice Statement
 - identification of the indicators of effectiveness sought for each relevant component
 - preparation of the Stage One assessment plan
- A.3.2 The following effort shall be allocated:

Preparation activity	Audit effort
Identification and scoping of the system or components under analysis, including agreed technical architecture and certification boundary	0.5 days
Initial Practice Statement assessment — Intermediary	0.25 days
Initial Practice Statement assessment — Age Assurance Provider or Relying Party	0.5 days
Review of desired indicators of effectiveness — Basic	0.5 days
Review of desired indicators of effectiveness — Effective	0.75 days
Review of desired indicators of effectiveness — Highly Effective	1.0 day
Review of desired indicators of effectiveness — Strict	1.25 days

A.4 Stage One — Policy and Governance Assessment

- A.4.1 Stage One assesses the applicant and the policies, governance arrangements and controls that apply across the system or components within the certification boundary. Stage One shall establish whether the applicant is sufficiently prepared for Stage Two and shall inform the detailed Stage Two assessment and testing plan.

A.4.2 The following effort shall be allocated, where applicable:

Stage One activity	Audit effort
Applicant/Product Owner assessment, including legal entity, sanctions and regulatory checks, declarations and relevant adverse history	0.5 days
Document and policy assessment against the five core characteristics of functionality, performance, privacy, security and acceptability	2.0 days
Assessment of external sources of data and handling of date information	0.5 days
Configuration management — internally controlled configuration only	0.5 days
Configuration management — external configuration permitted	1.0 day
Configuration management — both internal and external configuration	1.5 days

A.4.3 Assessment of external sources of data shall only be included where such sources are used by the system or component.

A.4.4 Stage One shall conclude with planning for Stage Two, taking account of the components identified, indicators of effectiveness sought, required testing, contexts of use, jurisdictions and any prior accredited certification proposed to be relied upon.

A.5 Stage Two — Component Effort

A.5.1 Stage Two component effort shall be determined by identifying each principal component included within the certification boundary and the indicator of effectiveness sought for that component.

A.5.2 Principal components may include:

- Age Assurance Methods** — including age verification, age estimation and age inference;
- Process Methods** — including binding and successive validation; and
- Delivery Methods** — including the delivery of results, reuse and replay.

A.5.3 An effort value shall be allocated to each principal component according to the indicator of effectiveness sought:

Indicator of effectiveness	Effort per principal component
Basic	0.4 days
Effective	0.5 days
Highly Effective	0.6 days

Strict	0.7 days
--------	----------

Different components within the same certification scope may be assessed against different indicators of effectiveness.

Applicant role

- A.5.4 The total component effort shall be adjusted according to the role undertaken by the applicant within the relevant certification scope:

Applicant role	Factor
Intermediary only	× 0.75
Age Assurance Provider only	× 1.00
Relying Party only	× 1.20
Multiple roles	× 1.50

Where the applicant undertakes different roles in different contexts, the CAB shall apply the factor relevant to the scope being assessed rather than automatically applying the highest factor to unrelated activities.

Prior accredited certification

- A.5.5 Where a component is subject to current accredited certification or other accredited conformity assessment that is relevant to the same component, characteristics and context of use, the CAB may recognise that evidence in calculating the remaining assessment effort.
- A.5.6 Where accepted, a prior certification factor of ×0.2 shall apply to the component effort that would otherwise be required.
- A.5.7 Prior certification shall not be recognised solely because a certificate exists. The CAB shall establish its validity, scope, accreditation status, applicability to the component and relevance to the contexts of use and requirements being assessed.

A.6 Stage Two — Context of Use Effort

- A.6.1 In addition to component effort, Stage Two shall include effort appropriate to the contexts in which the certified system or components are intended to be used.
- A.6.2 The context calculation shall take account of:
- sector
 - channel
 - whether the age assurance result is single-use or reusable
 - geographic and jurisdictional scope

Context score

- A.6.3 Each declared context of use shall be assigned the applicable sector value:

Sector	Weighting Value
Retail and Convenience	0.5
Licensed Hospitality	0.5
Body Modification	0.5
Gambling	0.75
Other (Including use at Ports & Borders)	0.75
Regulated Entertainment, Social Media and Content	1.0

- A.6.4 The applicable channel factor shall then be applied:

Channel	Factor
Offline	×1
Online	×2
Both	×3

- A.6.5 The applicable use factor shall then be applied:

Use	Factor
Single use	×1
Reusable	×2

- A.6.6 The context score shall be calculated as:

Context Score = total applicable sector value × channel factor × use factor

- A.6.7 The resulting effort shall be:

Context score	Stage Two context effort
0.5–5.0	1 day
5.1–15.0	2 days
15.1+	3 days

Jurisdictional scope

- A.6.8 Additional effort shall be allocated to assessment of the jurisdictional scope of certification:

Jurisdictional scope	Additional effort
Each country for which no additional local requirements apply	0.2 days
Each country for which additional local requirements apply	0.5 days
Regional block	2.0 days



Global scope

3.0 days

- A.6.9 The jurisdictional options are alternative means of representing geographic scope and shall not be cumulatively applied where the broader option already encompasses the narrower scope. Where Supplemental Scheme Rules apply, the effort necessary to assess those requirements shall be included within the jurisdictional calculation or separately increased where their complexity requires it.

A.7 Testing Effort

- A.7.1 Where testing or technical analysis is required, ATL effort shall be calculated separately from CAB audit effort. The testing effort shall be sufficient to develop the test plan, execute the required test or analysis programme and prepare the test report in accordance with Section 8.

- A.7.2 ATL effort shall be determined having regard to:
- a) the number and type of components requiring testing or analysis
 - b) the indicators of effectiveness sought
 - c) the test approach selected
 - d) required sample sizes and statistical assurance
 - e) demographic or other stratification requirements
 - f) the number of configurations, thresholds or operating conditions requiring assessment
 - g) specialist testing requirements
 - h) the extent to which analysis by proxy is required
 - i) the availability and suitability of existing test evidence or operational data
 - j) the extent of replication, corroboration or independent analysis required

- A.7.3 ATL effort shall therefore not be reduced below the level necessary to execute the test programme specified in the approved test plan solely by application of a predetermined audit-day calculation.

Principles of Calculation for Testing Effort

- A.7.4 The ATL shall determine the effort required in four stages:
- a) calculate the Core Complexity Score;
 - b) convert the score into Core ATL Effort;
 - c) apply any applicable Scale Adjustment or additional specialist effort; and
 - d) apply any justified recognition of reusable existing test evidence.

A.7.5 The calculation may be expressed as:

$$\text{ATL Effort} = \text{Core ATL Effort} + \text{Scale Adjustment} + \text{Additional Specialist Effort} - \text{Recognised Reusable Test Effort}$$

A.7.6 The ATL shall retain sufficient information to demonstrate how each element of the calculation was determined.

A.7.7 The calculation provides the normally expected minimum effort. The ATL may increase the calculated effort where the approved test plan demonstrates that further effort is necessary because of technical complexity, scale, risk, novel methodology or other factors not adequately reflected within the standard matrix.

Core Complexity Score

A.7.8 The Core Complexity Score shall be determined by assessing the test programme against the following six factors:

Factor	Minimum score	Maximum score
A. Test or analysis complexity	1	4
B. Statistical and sample complexity	1	4
C. Stratification and fairness analysis	0	3
D. Configurations and thresholds	0	3
E. Specialist technical testing	0	3
F. Analysis by proxy or existing evidence complexity	0	3

Factor A — Test or Analysis Complexity

This factor reflects the inherent complexity of designing and conducting the test or analysis activity.

Score	Criteria
1	Single straightforward test method using an established test procedure, readily obtainable ground truth and limited test conditions
2	Multiple test conditions, moderate procedural complexity or more than one material test variable
3	Complex interaction, binding, successive validation, reusable results, longitudinal behaviour, multiple linked components or significant interdependency between test activities
4	Novel or highly complex methodology requiring bespoke test design, simulation, specialist analysis, substantial methodological validation or extensive technical judgement

Factor B — Statistical and Sample Complexity

This factor reflects the statistical design and analytical effort required to establish the level of assurance specified in the test plan.

Score	Criteria
1	Small or non-statistical sample, functional or qualitative analysis, or limited confirmatory testing
2	Conventional statistical sample with a single principal endpoint and straightforward confidence or credible interval analysis
3	Large sample and/or multiple endpoints, thresholds, comparisons or material statistical sub-analysis
4	Complex statistical design including sequential or adaptive testing, equivalence or non-inferiority analysis, Bayesian methods, extensive near-threshold analysis, substantial operational datasets or other advanced statistical methodology

Factor C — Stratification and Fairness Analysis

This factor reflects the additional effort arising from demographic, accessibility, fairness or other required sub-group analysis.

Score	Criteria
0	No material stratification required
1	Limited stratification across a small number of relevant groups
2	Multiple demographic, accessibility or performance strata requiring separate analysis
3	Extensive stratification, minimum stratum floors, intersectional analysis, significant under-represented populations or substantial fairness analysis

Factor D — Configurations and Thresholds

This factor reflects additional test effort arising from the number of configurations, thresholds, operating modes or materially different implementations included within the test programme.

Score	Criteria
0	Single material configuration and single threshold
1	Limited additional configurations, thresholds or operating conditions
2	Multiple configurations, thresholds or operating modes requiring separate analysis
3	Extensive configurable system, numerous thresholds or materially different deployments requiring substantial separate testing or analysis

Factor E — Specialist Technical Testing

This factor reflects specialist test activities additional to conventional performance assessment.

Score	Criteria
0	No specialist testing beyond the normal performance test programme
1	One additional specialist test area
2	Multiple specialist test areas
3	Extensive or technically complex specialist testing programme

Specialist testing may include, where relevant to the test plan:

- a) presentation attack detection or liveness
- b) injection attack resistance
- c) replay or reuse testing
- d) circumvention and evasion testing
- e) binding
- f) successive validation
- g) security testing
- h) accessibility testing
- i) other specialist tests necessary to evaluate the applicable characteristics or indicators of effectiveness

Where a specialist activity requires substantial additional effort beyond that reasonably represented by the score, additional specialist effort may be assigned under Section A.7.15.

Factor F — Analysis by Proxy and Existing Evidence Complexity

This factor reflects the analytical effort required where evidence other than conventional direct population testing forms a material part of the test programme.

Score	Criteria
0	Conventional direct testing with no material reliance upon proxy analysis or external evidence
1	Existing evidence requiring straightforward validation and limited independent sampling
2	Significant independent analysis of internally generated testing, decision logic, inference methodology, operational evidence or aggregate population data
3	Complex proxy methodology involving multiple evidence sources, substantial independent sampling or replication, methodological review or triangulation

Analysis by proxy shall not automatically result in a reduction in ATL effort.

Where direct test execution is reduced but additional independent analysis, methodological assessment or triangulation is required, the resulting analytical effort shall be reflected within this factor.

Conversion of Complexity Score to Core ATL Effort

- A.7.9 The scores determined under Section A.7.8 shall be added together to produce the Core Complexity Score. The corresponding minimum Core ATL Effort shall be determined using the following table:

Core Complexity Score	Test planning	Execution / analysis	Reporting	Minimum Core ATL Effort
2–4	0.5 day	0.5 day	0.5 day	1.5 days
5–7	0.5 day	1.0 day	0.5 day	2.0 days
8–10	0.75 day	1.5 days	0.75 day	3.0 days
11–13	1.0 day	2.5 days	1.0 day	4.5 days
14–16	1.5 days	4.0 days	1.0 day	6.5 days
17 or more	Individually calculated	Individually calculated	Individually calculated	Technical justification required

- A.7.10 The allocation between planning, execution or analysis, and reporting may be adjusted where the nature of the test programme requires it, provided that the total calculated effort is not reduced without justification.
- A.7.11 Where the Core Complexity Score is 17 or greater, the ATL shall prepare a documented technical justification setting out the expected effort for each material element of the test programme.

Scale Adjustment

- A.7.12 The Core Complexity Score reflects the complexity of the test programme but does not necessarily account for the operational effort associated with very large numbers of test transactions or individual assessments.
- A.7.13 Where sample volume materially increases ATL execution, data handling or analytical effort, the following adjustment should normally be applied:

Number of direct test transactions or individual assessments	Additional ATL effort
Up to 500	Included in Core ATL Effort
501–1,000	+0.5 day
1,001–2,500	+1.0 day
2,501–5,000	+1.5 days
5,001–10,000	+2.0 days



More than 10,000	Individually calculated
------------------	-------------------------

- A.7.14 The Scale Adjustment shall not be applied mechanically where the number of transactions does not materially increase ATL effort.

EXAMPLE: where large volumes of automated test transactions can be executed, processed and analysed without corresponding manual intervention, the ATL may reduce or omit the scale adjustment. The rationale shall be recorded. Conversely, where a smaller sample requires significant manual recruitment, supervision, ground-truth verification, specialist equipment or individual assessment, additional effort may be justified notwithstanding the nominal sample size.

Additional Specialist Effort

- A.7.15 Where a specialist test activity requires effort materially beyond that represented within Factor E, the ATL may allocate additional specialist effort. This may include, for example:
- extensive presentation attack testing involving multiple artefact classes
 - bespoke injection or circumvention testing
 - complex security or penetration testing
 - substantial accessibility assessment
 - specialist demographic recruitment
 - longitudinal testing
 - extensive human-subject testing
 - simulation or synthetic test environment development
 - other technically complex activities specified within the approved test plan

- A.7.16 Additional specialist effort shall be separately identified and justified.

Recognition of Existing Test and Conformity Assessment Evidence

- A.7.17 Existing evidence may be recognised where it demonstrably reduces the amount of new test activity necessary to establish conformity. Recognition shall apply only to the part of the test programme for which the evidence is current, competent, relevant and applicable.

- A.7.18 The following maximum recognition levels may normally be applied:

Existing evidence	Maximum recognition of affected test activity
Directly applicable accredited testing covering the same component, configuration, performance claim and relevant context	Up to 80%
Competent independent testing that is relevant but not accredited or not fully applicable to the certification scope	Up to 50%

Applicant's own controlled testing capable of independent validation, sampling or replication	Up to 40%
Operational monitoring data suitable for statistical or analytical corroboration	Case-specific
Unsupported manufacturer, supplier or vendor performance claims	0%

- A.7.19 The recognition percentage shall apply only to the affected test execution or analysis effort and shall not automatically reduce:
- test-plan development
 - assessment of the suitability and provenance of the evidence
 - independent validation or sampling required by the ATL
 - statistical analysis that remains necessary
 - reporting
 - any specialist test activity not covered by the existing evidence

Treatment of Analysis by Proxy

- A.7.20 Where analysis by proxy is used in accordance with Section 8 and the Statistical Assurance Framework, the ATL shall distinguish between reductions in direct test execution and additional analytical work required to establish sufficient confidence in the evidence.
- A.7.21 Analysis by proxy may therefore:
- reduce the amount of direct Participating or transaction testing required
 - leave overall ATL effort materially unchanged
 - increase ATL effort where substantial methodological review, independent sampling, replication or triangulation is required
- A.7.22 The ATL shall not apply an automatic discount solely because analysis by proxy is used.
- A.7.23 Where internally generated test evidence is relied upon, effort shall be allocated for review of the underlying methodology, test population or dataset, ground truth, test conditions, configuration, statistical methodology, controls and conclusions, together with such independent sampling or replication as is specified in the test plan.
- A.7.24 Where decision logic or inference methodology is analysed, sufficient effort shall be allocated to assess the objective evidential basis for the relationship between the characteristics observed and the age-related inference produced.
- A.7.25 Where aggregate population or operational evidence is used, sufficient effort shall be allocated to establish the suitability of the comparator

population, analyse material divergence and consider relevant selection, demographic, geographic, sector or channel effects.

A.8 Independent Review of Certification Evidence and Certification Decision

- A.8.1 Effort shall be allocated for independent review of the resulting certification evidence.

Activity	Effort
Scientific or technical review of testing and analysis	0.25 days
Independent Review of Certification Evidence	1.0 day
Certification Decision	Included
Entry onto the certification registry	Included
Enrolment into Scheme monitoring services	Included

- A.8.2 The review effort specified above represents the normal minimum. Additional review effort may be required where the certification scope, technical evidence, test methodology, findings or complexity of the certification determination requires further independent review.

A.9 Surveillance and Recertification

- A.9.1 Annual surveillance effort shall normally be calculated as **one-third of the initial certification effort**, adjusted where necessary to reflect changes to the certified system, components, configurations, contexts of use, jurisdictions, applicable requirements, monitoring results and previous audit findings.
- A.9.2 Recertification shall normally be undertaken every three years. Recertification effort shall normally be calculated as **two-thirds of the initial certification effort**, subject to review of changes occurring during the certification cycle and the extent to which existing certification evidence remains valid.

A.10 Changes and Extensions to Certification

- A.10.1 Where an applicant seeks to add or update a component, context of use, jurisdiction, configuration or classification accuracy level during the certification cycle, the CAB shall recalculate only those elements of effort affected by the proposed change.
- A.10.2 Existing assessment and test evidence may continue to be relied upon where the CAB determines that it remains current, relevant and applicable to the revised certification scope.



A.11 Scheme Levy

- A.11.1 The Scheme Levy applicable to the calculated effort is determined in accordance with ACCS 0 and ACCS-P04.

A.12 Documentation and Record

- A.12.1 The Participating CAB shall maintain a record of the effort calculation showing:
- a) the certification scope on which the calculation is based
 - b) CAB effort by applicable activity
 - c) ATL effort and the applicable complexity calculation
 - d) adjustments applied and their justification
 - e) prior conformity assessment or testing evidence relied upon to reduce effort
 - f) total CAB and ATL days
 - g) any subsequent revision to the calculation
- A.12.2 The effort calculation shall be reviewed where information obtained during scoping, Stage One or subsequent evaluation materially changes the assumptions on which the calculation was based.
- A.12.3 The effort calculation shall be reviewed at surveillance and recertification planning. Where the scope has changed since initial certification, the calculation can be updated accordingly.

GUIDANCE: Worked examples demonstrating the application of the audit and testing effort calculation methodology set out in this Annex are provided in ACCS-P04 — Scheme Levy and Audit Effort Calculation. These examples illustrate the calculation of CAB and ATL effort for different applicant roles, systems and components, contexts of use, testing approaches and circumstances involving prior conformity assessment evidence. The examples are informative and are intended to support consistent application of this Annex by Participating CABs and ATLs. They do not replace the requirements of this Annex, and the effort for each certification should be calculated according to the actual scope and circumstances of the application.



Annex B - Practice Statement Template (informative)

B.1 Purpose

- B.1.1 This annex provides a structured template for the Private and Public Practice Statements required under Section 6 and ISO/IEC 27566-1, Clause 10. Certification Clients are not required to use the structure or format of this annex, provided that the Practice Statements contain the applicable required information and enable that information to be readily identified and evaluated.
- B.1.2 Practice Statements under this scheme comprise:
- a) the **Private Practice Statement**, containing the information necessary to support conformity assessment, including information that is commercially sensitive, security-sensitive or otherwise inappropriate for public disclosure
 - b) the **Public Practice Statement**, containing the information required for public disclosure under this scheme and providing an accurate public description of the certified Target of Evaluation and certified scope.
- B.1.3 The Private Practice Statement provides the principal documentary basis for evaluation and is developed and updated as necessary during Stage One and Stage Two. Before certification, the Public Practice Statement shall be reviewed against the final Private Practice Statement and the evaluation evidence to confirm that it accurately represents the certified scope. Information can be omitted from the Public Practice Statement where disclosure would be commercially sensitive, security-sensitive or otherwise inappropriate, but the Public Practice Statement shall not contradict, obscure or overstate the information relevant to the certified scope.
- B.1.4 Certification Clients may use the ACCS Practice Statement Tool (online) to generate structured outputs aligned with this annex. Use of the tool is not mandatory.

B.2 Private Practice Statement - Content

- B.2.1 The Private Practice Statement shall contain the following information, as applicable to the Target of Evaluation and the role or roles performed by the Certification Client:

1. Administrative Information

- Certification Client legal name
- Registered address and jurisdiction

- Trading name, where applicable
- Certification contact
- Certification Client role or roles
- Practice Statement version and date
- Version history
- Approving authority and approval date

2. Target of Evaluation

- Name and description of the Target of Evaluation
- Version, release or deployment reference
- Purpose and intended use
- Role or roles performed by the Certification Client
- Functions included within the Target of Evaluation
- Architecture and principal components
- Boundaries and interfaces
- Third-party components and dependencies
- Contexts of use
- Applicable jurisdictions
- Material assumptions and exclusions

3. Age Assurance Methods and Claims

- Age assurance method or methods
- Method type, including age verification, age estimation, age inference or successive validation, as applicable
- Age gate or age gates
- Deployment mode
- Applicable configurations
- Classification accuracy level claimed for each applicable method, age gate and configuration
- Successive validation, fallback or alternative methods, where applicable
- Date-of-birth capability, where claimed

4. Functional Characteristics

- Data acquisition
- Binding
- Processing
- Configuration management
- Operation within the declared contexts of use
- Delivery of the age assurance result
- Supporting evidence and controlled documentation

5. Data Dependencies, Assumptions and Exclusions

- Data and evidence sources
- External services and dependencies
- Third-party systems or components
- Assumptions on which operation or performance depends
- Known limitations

- Exclusions from the Target of Evaluation
- Conditions necessary for operation within the certified scope

6. Performance Characteristics

- Classification accuracy
- Classification accuracy levels claimed
- Applicable age gates and configurations
- Outcome error parity
- Failure-to-acquire or failure-to-complete characteristics, where applicable
- Relevant uncertainty and limitations
- Operational performance monitoring arrangements

7. Privacy Characteristics

- Categories of personal data processed
- Purposes of processing
- Data sources and flows
- Data minimisation arrangements
- Retention and deletion
- Access controls
- Onward use and disclosure
- Mechanisms relevant to data-subject rights
- Audit logging
- Applicable privacy framework and supporting evidence

8. Security Characteristics and Attack Vectors

- Security architecture and controls
- Relevant known or reasonably anticipated attack vectors
- Threat assessment and risk treatment
- Replay, forwarding and reuse controls, where applicable
- Presentation attack, spoofing and counterfeiting controls, where applicable
- Fail-safe behaviour
- Security testing and supporting evidence
- Vulnerability and incident management arrangements
- Material security assumptions or limitations

9. Acceptability Characteristics

- Accessibility
- Inclusivity and accommodations
- Age-appropriate operation and information
- User information and transparency
- Alternative or fallback arrangements
- Complaints, challenge and redress arrangements
- Other measures relevant to acceptability within the declared contexts of use



10. Monitoring and Continuing Conformity

- Characteristics and performance measures subject to monitoring
- Monitoring methods and frequency
- Thresholds and escalation criteria, where applicable
- Configuration and version monitoring
- Security and privacy incident monitoring
- Change-control arrangements
- Internal review and improvement arrangements
- Arrangements for maintaining the continuing accuracy of the Practice Statement

11. Audit, Certification and Review

- Arrangements for audit, independent assessment and review
- Relevant external certification, accredited testing or other conformity assessment evidence relied upon
- Material results or limitations required to be recorded under ISO/IEC 27566-1, Clause 10

B.3 Public Practice Statement - Contents

- B.3.1 The Public Practice Statement shall provide sufficient information for users, relying parties, regulators and other interested parties to understand the nature and scope of the certified age assurance system without disclosing information that would materially compromise security, facilitate circumvention or disclose legitimately confidential information.
- B.3.2 Information contained in the Public Practice Statement shall be consistent with the Private Practice Statement and the certified scope. Omission of information from the public version shall not result in a materially misleading description of the certification.
- B.3.3 The public summary should contain all of the following elements, where relevant to the system or component under evaluation.

1. Cover Information *(populated from the Public Practice Statement front sheet)*

- Certification Client name
- Date certified

2. System Description

- Name and version of the certified system or component
- Plain-language description of what the system does and how it is used
- Certification Client's role - Age Assurance Provider, Relying Party or Intermediary



3. Certified Age Assurance Methods

For each entry in the Age Assurance Method Register

- Method type and specific method
- Age gate
- Indicator of effectiveness achieved
- Classification accuracy achieved (*expressed as a percentage - not the statistical interval*)
- Deployment mode
- Jurisdiction(s) covered

4. Contexts of Use

- Sector(s) of deployment
- Channel(s) - online, in-person or both
- Any scope limitations or exclusions applicable to public disclosure

5. Privacy Summary

- High-level statement of what personal data is processed and for what purpose
- How users are informed
- How users can exercise rights or make complaints

6. Complaint Handling

- How users can raise a complaint about the age assurance process
- Contact details or reference to the Certification Client's published complaints procedure

B.3.4 The public summary should not be drafted until the private practice statement is finalised. Attempting to draft both in parallel before performance testing is complete frequently results in inconsistencies between the two documents.

Annex C - Model Certification Documents (normative)

C.1 Purpose

C.1.1 This annex provides model formats for certification documentation issued under ACCS 1. The requirements governing the issue, content, control and publication of certification documentation are specified in ACCS 0 and Section 10 of this document.

C.1.2 The model formats illustrate how the certified scope and associated Practice Statement can be presented. Conformity with the visual format of this annex is not required, provided that the applicable certification information is clearly and unambiguously stated.

C.2 Model Certificate of Conformity

Certificate of Conformity

*This is to certify that the [Name of product, system, process]
provided by [Name of Client]
of [Address of client]*

*Has been assessed and found to meet the requirements of ACCS
1:2026 Conformity Assessment Requirements for ISO/IEC 27566-1 –Age
Assurance Systems – Part 1: Framework*

*Technical requirements for the certification of age assurance systems and
components under the Age Check Certification Scheme*

*This Certificate is valid only when read together with the accompanying
Schedule of Certification (Insert number)*

Certificate Reference	
Client Name	
Date Issued	[DD/MM/YYYY]
Valid Until	[DD/MM/YYYY]

A QR code may be placed on the Certificate to allow for Verification

*Signature of the person (or other defined authorisation) of the person(s) of
the certification body assigned such responsibility*

Name

Position



[ACCS CERTIFICATION MARK]

Participating CAB Name, Address and Logo

C.3 Model Schedule of Certification

Schedule of Certification

ACCS 1:2026; ISO/IEC 27566-1:2025

Reference Number:

Issue Date:

This is a Schedule of Certification independently assessed by competent and qualified audit professionals to demonstrate that [Insert the name of the product, system or process] provided by [NAME OF CLIENT], meet the relevant requirements of ACCS 1:2026 Conformity Assessment Requirements for ISO/IEC 27566-1 –Age Assurance Systems – Part 1: Framework Technical requirements for the certification of age assurance systems and components under the Age Check Certification Scheme for the Scope outlined.

The Schedule is only valid when presented alongside Certificate of Conformity [Certificate Number] issued to [Name of Client and address]

SCOPE OF CERTIFICATION:

- Target of evaluation (Name, version, deployment reference release date]
- Limitations
- Full Practice Statement [Title, Version and date]

Conformity Assessment:

The Checks of Conformity independently assessed by competent and qualified audit professionals demonstrate, through sampling that [NAME OF CLIENT], as an [Role] meets the requirements as outlined in Practice Statement [Title, Version and date]

A certified copy of the full Practice Statement that has been assessed is available to view on the ACCS Registry. This Public Practice Statement provides information about the certified service while protecting information that is not publicly available.

Monitoring and Surveillance:



Date of Certification:
Certificate Valid Until:
Surveillance Audit 1 Due: [Annual ± 30 days]
Surveillance Audit 2 Due: [Annual ± 30 days]
Recertification due date: [3 years from issue]

Limitations of certification:

This certification applies only to the target of evaluation as defined above.
Any modifications outside the declared boundaries, contexts of use or configurations **are not** certified.

Certification does not extend to relying party operations, data controllers or external systems not declared in scope

Simple Explainer

Participating CABs may provide explanatory text or a simple explainer to aid understanding of the certification documentation.

C.4 Model Public Practice Statement Front Sheet

NAME OF CLIENT – Public Practice Statement

About this Public Practice Statement

This Public Practice Statement provides a certified, informative summary of the Practice Statement identified by title, version and date

The full Practice Statement and the underlying product, process or service has been assessed by the ACCS Certification Scheme and has met the applicable requirements of ACCS 1:2026 Conformity Assessment Requirements for ISO/IEC 27566-1 –Age Assurance Systems – Part 1: Framework Technical requirements for the certification of age assurance systems and components under the Age Check Certification Scheme in accordance with scope of certification set out on their certificate and schedule.

The full Practice Statement contains sensitive, confidential or security-related information and is therefore not published. This public version provides information about the certified service while protecting information that should not be made publicly available.

For further information about the service, including enquiries about aspects of its operation that are not covered in this public summary, please contact the certified organisation directly.



Name of Client	
Public Practice Statement Title	
Public Practice Statement Version	
Public Practice Statement Date	
Date Certified	

Participating CAB Name, Address and Logo



Annex D - Mapping of ISO/IEC 27566-1 Requirements to the ACCS 1 Evaluation Process (informative)

D.1 Method and Maintenance

- D.1.1 This annex provides a mapping between the requirements of ISO/IEC 27566-1:2025 and the evaluation activities specified in ACCS 1. It is intended to support consistent evaluation, audit planning, traceability and completeness checking by Conformity Assessment Bodies.
- D.1.2 The mapping is provided as an aid to application of the scheme and does not reproduce, replace, modify or interpret the requirements of ISO/IEC 27566-1. Certification shall be determined against the requirements of the normative standard and the applicable requirements of ACCS 1 and ACCS 0.
- D.1.3 Where there is any inconsistency between this annex and a normative requirement of ISO/IEC 27566-1, ACCS 1 or ACCS 0, the applicable normative requirement takes precedence.
- D.1.4 The Scheme Owner should review and update this mapping following amendments to ISO/IEC 27566-1 or material revisions to the evaluation requirements or clause numbering of ACCS 1.

D.2 ISO/IEC 27566-1 "Shall" Requirements → ACCS1:2026 Sections

- D.2.1 The following table identifies the principal points within ACCS 1 at which conformity with the applicable requirements of ISO/IEC 27566-1 is evaluated. The requirement subjects are provided for navigation and traceability only and do not replace or modify the requirements of ISO/IEC 27566-1:

ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
4.3.2 a)	Age verification — genuineness of identity document	8.4; 9.4	Practice Statement; method documentation; document-validation evidence; test evidence where applicable



ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
4.3.2 b)	Age verification — association of identity document with correct individual	8.4; 9.4; 9.5	Practice Statement; binding arrangements; method documentation; test evidence
4.3.2 c)	Age verification — identity document expiry	8.4; 9.4	Method documentation; validation controls; test evidence where applicable
4.3.2 d)	Age verification — identity document revocation or suspension	8.4; 9.4	Method documentation; source/issuer arrangements; validation controls; test evidence where applicable
5.2	Correct interpretation of date information	8.4; 9.5	Functional specification; date-processing controls; functional test evidence
5.3	Binding of age assurance result to correct individual	4.2–4.4; 8.4; 9.5	Practice Statement; architecture; binding methodology; functional/security test evidence
5.3	Prevention of use of another individual's age assurance result	4.5; 8.4; 9.5; 9.8	Binding controls; threat assessment; attack testing; functional/security evidence
5.5	Communication of standard configuration settings by provider to relying party	6.7; 9.5	Private Practice Statement; configuration documentation; provider/relying-party arrangements
5.6	Documentation of contexts of use	4.7; 6; 9.5; Annex B	Target of Evaluation; Private and Public Practice Statements; Stage Two evidence
5.7	Secure delivery of age assurance result	4.6; 8.4; 9.5; 9.8	Architecture; interfaces; delivery controls; security assessment/test evidence
6.1	Effective age-related eligibility decision — true	5.2–5.3; 8.6; 9.6	Testing plan; test report; classification accuracy results; Method Register



ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
	positive/true negative outcomes		
6.1	Self-asserted age treated as ineffective for age-related eligibility decisions	5.1–5.3; 9.4; 9.6	Method Register; Practice Statement; certification scope determination
6.1	Outcome error parity across demographics	5.6; 8.5; 8.6; 8.8; 9.6	Sample design; demographic analysis; test report; statistical assessment
6.1	Correct binding as a characteristic of effective operation	5.3; 8.4; 9.5; 9.6	Binding evidence; test report; Stage Two assessment
6.1	Functional characteristics as a condition of effective operation	8.4; 9.5; 9.6	Functional evidence; test report where applicable; Stage Two assessment
6.1	Privacy characteristics as a condition of effective operation	9.6; 9.7	Privacy evidence; Practice Statement; Stage Two assessment
6.1	Security characteristics as a condition of effective operation	9.6; 9.8	Security evidence; threat assessment; test evidence
6.1	Acceptability characteristics as a condition of effective operation	9.6; 9.9	Acceptability evidence; accessibility/usability evidence; Practice Statement
6.3	Classification accuracy determined for each configuration	5.3; 5.5; 8.6; 9.3; 9.6	Testing plan; configuration records; test report; Method Register
6.3	Classification accuracy recorded and regularly reviewed	5.3; 6; 9.6; 11.3; 11.6	Test report; Practice Statement; continuous monitoring records
6.3	Classification accuracy stated in Practice Statements	5.3; 6; 9.10; Annex B	Private and Public Practice Statements; Method Register



ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
6.3	Scalability evaluated and reported	8.3–8.4; 8.11; 9.6	Testing plan; scalability/load evidence; test report
6.3	Age assurance system is testable	6.3; 7.3; 8.3–8.4; 9.6	Practice Statement; testing plan; access to Target of Evaluation; test evidence
7.3	Personal data minimisation	6; 9.7	Practice Statement; data-flow documentation; privacy assessment; objective evidence
7.3	Acquisition of data limited to creation of age assurance result	6; 9.7	Practice Statement; data-flow records; processing controls
7.3	Prevention of onward use without explicit user consent	6; 9.7	Privacy controls; Practice Statement; technical/organisational evidence
7.3	Access controls for personal data	6; 9.7	Access-control documentation; technical evidence; audit records
7.3	Deletion of personal data following establishment of age assurance result and minimisation of retained data	6; 9.7	Retention/deletion policy; technical controls; Practice Statement; evidence of implementation
7.6	Relying-party audit log of access granted	6; 9.7	Logging specification; audit logs/sample records; Practice Statement
7.6	Integrity protection and declared retention of audit logs	6; 9.7; Annex B	Logging controls; retention policy; Practice Statement; technical evidence
7.6	Prohibited biometric/identity-document content in audit logs	6; 9.7	Logging specification; sample logs; privacy assessment



ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
8.2	Protection against unplanned reuse of age assurance results	4.5; 8.4; 9.8	Architecture; threat assessment; security controls; test evidence
8.2	Replay protection for age-related cryptographic digital proofs	4.5; 8.4; 9.8	Protocol specification; cryptographic/security evidence; test evidence
8.2	Protection against unplanned forwarding of age assurance results	4.5; 8.4; 9.8	Architecture; result-delivery controls; threat assessment; security testing
8.2	Relying party determines appropriate duration where an age assurance result is memorised	6; 9.8	Practice Statement; relying-party policy; configuration/retention controls
8.3	Age assurance system designed and managed to resist attack	4.5; 7.5; 8.4; 9.8	Threat assessment; security architecture; risk treatment; security test evidence
8.3	Protection against biometric presentation attacks	4.5; 8.4; 9.8	PAD testing where applicable; threat assessment; security evidence
8.3	Protection against spoofing attacks	4.5; 8.4; 9.8	Threat assessment; attack testing; security controls
8.3	Protection against counterfeiting attacks	4.5; 8.4; 9.8	Threat assessment; attack testing; document/credential validation evidence
8.3	Competence of persons or systems undertaking document validation	8.2; 9.8	Competence evidence; validation-system evidence; training/qualification records where applicable
8.5	Fail-safe operation	8.4; 9.5; 9.8	Failure-mode documentation; functional/security test evidence; Practice Statement



ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
8.5	Denial of access as default age-related eligibility decision following relevant system failure or malfunction	8.4; 9.5; 9.8	Failure-mode testing; configuration evidence; system behaviour records
9.4	Means for individuals to register complaints	6; 9.9	Practice Statement; complaint procedure; user-facing information
9.4	Relying party responsibility for interaction with provider in complaint handling	6; 9.9	Complaint procedure; contractual/operational arrangements
9.4	Written agreement between provider and relying party allocating complaint-handling responsibility	6; 9.9	Contract, service agreement or other documented allocation of responsibility
10.2 a)	Provider Practice Statement — required age-related eligibility outcome and source of requirement	6; 9.10; Annex B	Private Practice Statement; Public Practice Statement
10.2 b)	Provider Practice Statement — components, data sources, credential types and methods	4; 6; 9.3; 9.10; Annex B	Practice Statements; Target of Evaluation; Method Register
10.2 c)	Provider Practice Statement — indicators of effectiveness achieved	5; 6; 9.6; 9.10; Annex B	Test report; Method Register; Practice Statements
10.2 d)	Provider Practice Statement — binding	6; 9.5; 9.10; Annex B	Practice Statements; binding evidence



ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
10.2 e)	Provider Practice Statement — prevention of collaborative attacks	4.5; 6; 9.8; 9.10; Annex B	Private Practice Statement; threat/security evidence
10.2 f)	Provider Practice Statement — privacy approach	6; 9.7; 9.10; Annex B	Private and Public Practice Statements; privacy evidence
10.2 g)	Provider Practice Statement — functionality appropriate to capacity and age of users	6; 9.5; 9.9; 9.10; Annex B	Practice Statements; functional/acceptability evidence
10.2 h)	Provider Practice Statement — security characteristics	6; 9.8; 9.10; Annex B	Private Practice Statement; appropriate public disclosure; security evidence
10.2 i)	Provider Practice Statement — accessible, inclusive and understandable implementation without undue restriction of access	6; 9.9; 9.10; Annex B	Practice Statements; accessibility, inclusivity and user-information evidence
10.2 j)	Provider Practice Statement — audit, certification and review	6; 9.10; 10; 11.6; Annex B	Final Practice Statements; certification records; continuing certification arrangements
10.3 a)	Relying Party Practice Statement — age-related eligibility criteria	4.3; 6; 9.10; Annex B	Target of Evaluation; Practice Statements
10.3 b)	Relying Party Practice Statement — providers and intermediaries used	4.3; 6; 9.10; Annex B	Architecture; Practice Statements; provider/intermediary references
10.3 c)	Relying Party Practice Statement — source of age-	4.3; 5.8; 6; 9.10; Annex B	Practice Statement; policy/regulatory source information



ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
	related eligibility requirements		
10.3 d)	Relying Party Practice Statement — methods, issuers/intermediaries, fallback and configuration	4; 6; 9.3; 9.10; Annex B	Practice Statements; Method Register; configuration evidence
10.3 e)	Relying Party Practice Statement — privacy, security and acceptability approach	6; 9.7–9.10; Annex B	Practice Statements; privacy/security/acceptability evidence
10.3 f)	Relying Party Practice Statement — functionality appropriate to capacity and age of users	6; 9.5; 9.9; 9.10; Annex B	Practice Statements; functional and acceptability evidence
10.3 g)	Relying Party Practice Statement — accessible, inclusive and understandable implementation without undue restriction	6; 9.9; 9.10; Annex B	Practice Statements; accessibility/inclusivity evidence; user information
10.3 h)	Relying Party Practice Statement — redress	6; 9.9; 9.10; Annex B	Practice Statement; complaints/redress procedure
10.3 i)	Relying Party Practice Statement — audit, certification and review	6; 9.10; 10; 11.6; Annex B	Final Practice Statements; certification and review records
10.4 a)	Intermediary Practice Statement — role and direct/independent impact on age assurance characteristics	4.4; 6; 9.10; Annex B	Target of Evaluation; architecture; Private and Public Practice Statements



ISO/IEC 27566-1 reference	Requirement subject	Principal ACCS 1 evaluation point	Supporting evidence / evaluation activity
10.4 b)	Intermediary Practice Statement — providers or relying parties supported	4.4; 6; 9.10; Annex B	Practice Statements; architecture; cross-referenced provider/relying-party information
10.4 c)	Intermediary Practice Statement — audit, certification and review	6; 9.10; 10; 11.6; Annex B	Final Practice Statements; certification and review records

D.3 Testing and Indicators - Cross-Standard Mapping

Evaluation matter	ACCS 1 requirement	Principal evidence
Testing plan	7.3; 8.3	Approved testing plan
Test coverage	8.4	Requirement/evidence mapping
Sample integrity	8.5	Sample design and demographic data
Classification accuracy	5.3; 8.6	Test report
Outcome error parity	5.6; 8.6	Test report
Jurisdictional requirements	5.8; 8.7	Jurisdiction-specific evidence
Statistical assurance	8.8	Pre-specified statistical design and analysis
Anti-gaming	8.9	Test controls and execution records
External testing	8.10	External evidence assessment
Reporting	8.12	Final test report
Certification claim	9.3; 9.6; 9.10	Method Register and Practice Statement

D.4 Certificates, Schedules and Transparency

Document	Function	Principal technical information
Certificate of Conformity	Records certification decision and identifies client, standard and scheme	High-level certification identification



Document	Function	Principal technical information
Schedule of Certification	Defines certified Target of Evaluation and identifies controlling Public Practice Statement	Target/version; role; Practice Statement reference; limitations/exclusions where applicable
Public Practice Statement	Detailed public description of certified scope	Methods; age gates; classification accuracy levels; configurations; contexts; jurisdictions; limitations and conditions
Private Practice Statement	Comprehensive technical description supporting certification	Full applicable ISO Clause 10 and ACCS 1 information
Method Register	Certification evidence/control record	Method-by-method technical claims and determinations
Test Report	Technical evidence	Testing, statistical results, uncertainty, performance and limitations

D.5 Use of the Mapping

- D.5.1 The mapping in this annex can be used by Lead Auditors, Test Analysts and Evaluation Reviewers to support audit planning, evidence traceability and completeness checking. It does not replace the requirement to evaluate the Target of Evaluation against all applicable requirements of ISO/IEC 27566-1 and this scheme.
- D.5.2 The applicability of individual requirements depends upon the Target of Evaluation, the role or roles performed by the Certification Client, the age assurance methods deployed, and the certified contexts of use. A requirement shall not be treated as inapplicable solely because no corresponding row or evidence item is identified in this annex.
- D.5.3 Where evaluation evidence demonstrates conformity with more than one requirement, the same evidence can be cross-referenced to each applicable requirement provided that its relevance and sufficiency are established.



Annex E – Competency and Learning Resources (informative)

E.1 Purpose

- E.1.1 The Scheme Owner maintains competency and learning resources to support the consistent interpretation and application of ISO/IEC 27566-1 in conformity assessment activities undertaken under this scheme.
- E.1.2 The resources are intended for use by Conformity Assessment Bodies, Authorised Test Laboratories, Lead Auditors, Test Analysts, Evaluation Reviewers and other personnel involved in evaluation activities under ACCS 1.
- E.1.3 The resources can be used to support competence development, audit and test planning, consideration of objective evidence, professional judgement and consistency of evaluation.

E.2 Status of the Competency and Learning Resources

- E.2.1 The competency and learning resources are informative. They do not create, amend, replace or extend any requirement of ISO/IEC 27566-1, ACCS 0 or ACCS 1 and shall not be treated as additional certification criteria.
- E.2.2 Where there is any inconsistency between a competency or learning resource and a normative requirement, the applicable normative requirement takes precedence.
- E.2.3 The resources provide guidance relevant to particular clauses, requirements, recommendations or subject areas within ISO/IEC 27566-1. They can include explanatory material, suggested auditor enquiries, examples of objective evidence, matters for professional judgement, indicators of potential conformity or nonconformity and model wording.
- E.2.4 The resources are intended to promote consistency without constraining professional judgement. Their application should be proportionate to the Target of Evaluation, its complexity, the Certification Client's role or roles, contexts of use and applicable certification scope.
- E.2.5 Examples of documents, evidence or evaluation approaches contained in a resource do not require the Certification Client to use or produce that particular form of evidence where conformity can be objectively demonstrated by other appropriate means



E.3 Maintenance of Competency and Learning Resources

- E.3.1 The Scheme Owner maintains the competency and learning resources as controlled supporting material and can revise, replace, withdraw or supplement individual resources without amendment of ACCS 1, provided that such changes do not create or modify certification requirements.
- E.3.2 The current set of competency and learning resources is maintained in the ACCS document portal. Each resource is identified by an ACCS-L reference and the relevant ISO/IEC 27566-1 clause or subject area.
- E.3.3 Conformity Assessment Bodies and Authorised Test Laboratories should ensure that personnel have access to the current resources relevant to the evaluation activities they are assigned to undertake.