DRAFT International Standard

ISO/IEC DIS 27566-3

Information security, cybersecurity and privacy protection – Age assurance systems —

Part 3: Approaches to analysis or comparison

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2026-09-11

Voting terminates on:
2026-12-04

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document has not been edited by the ISO Central Secretariat.

Reference number
ISO/IEC DIS 27566-3:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**
3.1 Analytical activity terms 1
3.2 Actors and parties in analysis 2
3.3 Technical analytical terms 3

4 Abbreviated terms **5**

5 Approaches to analysis or comparison **5**
5.1 Reasons for conducting analysis or comparison 5
5.2 Types of analysis 7
5.3 Implementation of an analysis process 7
5.3.1 General 7
5.3.2 Analysis initiation and resourcing 8
5.3.3 System identification and scoping 8
5.3.4 Review of declared characteristics and practice statements 9
5.3.5 Analysis planning 10
5.3.6 Execution and data collection 11
5.3.7 Synthesis and interpretation 12
5.4 Supporting analysis activities and application of results 12

6 Indicators of effectiveness **13**
6.1 Introduction to indicators of effectiveness 13
6.2 Key indicators of effectiveness 14
6.2.1 Accuracy effectiveness 14
6.2.2 Binding effectiveness 16
6.2.3 Privacy-preserving effectiveness 16
6.3 Functional Effectiveness 17
6.3.1 General 17
6.3.2 Result consistency 17
6.3.3 Decision consistency under variable inputs 17
6.3.4 Intent alignment / purpose conformity 17
6.4 Performance effectiveness 17
6.4.1 General 17
6.4.2 Processing time 18
6.4.3 System availability 18
6.4.4 Output stability 18
6.4.5 Latency under load 18
6.4.6 Scalability and concurrency 18
6.4.7 Resource efficiency 18
6.4.8 Performance under configuration variability 18
6.5 Privacy effectiveness 19
6.5.1 General 19
6.5.2 Data minimization 19
6.5.3 Data retention control 19
6.5.4 Transparency and user control 19
6.5.5 Purpose limitation 19
6.6 Security effectiveness 19
6.6.1 General 19
6.6.2 Binding robustness under adversarial conditions 20
6.6.3 Presentation attack resistance 20
6.6.4 Tamper resistance and integrity protection 20
6.6.5 Adversarial input or model poisoning resilience 20

© ISO/IEC 2026 – All rights reserved

6.6.6 Secure assertion and transmission 20
6.7 Acceptability effectiveness 20
6.7.1 General 20
6.7.2 User accessibility and equity 21
6.7.3 Demographic fairness (age, gender, skin tone) 21
6.7.4 Accessibility for users with disabilities 21
6.7.5 User dropout or rejection rate 21
6.7.6 Interface clarity and comprehensibility 21
6.7.7 Complaints handling and recourse 21

7 Analysis considerations 22
7.1 Analysis considerations applicable to all age assurance methods 22
7.1.1 Selection of test methods based on system type 22
7.1.2 System configuration, deployment context and environmental variability 23
7.1.3 User experience and acceptability factors 23
7.1.4 Selection of test methods based on system type 24
7.2 Analysis considerations only applicable to age estimation methods 25
7.2.1 Demographic distribution of test samples 25
7.2.2 Testing around age threshold values 25
7.2.3 Sample size expectations 25
7.2.4 Sampling approach 25
7.2.5 Sampling design and statistical power 26

8 Characteristics and measurements for age assurance components 26
8.1 Overview 26
8.2 Application of indicators to components 26
8.3 Age assurance provider perspective 27
8.4 Relying party perspective 28

9 Reporting of analysis results 28
9.1 General 28
9.2 Core reports and explanatory reports 29
9.3 Structure of analysis reports 30
9.4 Reporting by indicator of effectiveness 31
9.5 Reporting about fairness, accessibility and inclusiveness 32
9.6 Reporting limitations 33
9.7 Supporting annexes or artefacts 33
9.8 Comparisons of results between instances of analyses 34

Annex A (Informative) **Document authenticity 35**

Annex B (Informative) **Illustrative age assurance deployment models 37**

Annex C (Informative) **Measurement of the classification accuracy for classification models using facial analysis 49**

Annex D Sample breakdowns, liveness detection and biometric presentation attack detection for facial age estimation methods 54

Annex E (Informative) **Example analysis report 57**

Bibliography 60

© ISO/IEC 2026 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO should not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see https://www.iso.org/foreword-supplementary-information.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, Subcommittee SC 27 - Information security, cybersecurity and privacy protection.

A list of all parts of ISO/IEC 27566 can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© ISO/IEC 2026 – All rights reserved

Introduction

Age assurance is a set of methods that enables a relying party to make age-related eligibility decisions with varying degrees of certainty, depending on the use case and the desired levels of efficiency. As the deployment of age assurance systems grows across digital and physical domains, there is an increasing need for structured and transparent ways to analyse or compare the characteristics and performance of these systems and their components.

This document provides guidance for analysing and comparing age assurance systems and components that use age verification, age estimation or age inference methods. These may be based on identity credentials, biometric techniques, behavioural signals or other data-driven approaches. Analysis may focus on full systems or discrete components, depending on the context of use and level of abstraction.

This document is intended for analysts, system providers, implementers and oversight bodies involved in the conduct or the review of age assurance analysis.

The approach defined in this document builds upon the concepts and principles introduced in ISO/IEC 27566-1 (Age Assurance Systems – Framework), particularly the core characteristics of functionality, performance, privacy, security and acceptability. It enables structured analysis of a “system under analysis” or “component under analysis” through comparison against these characteristics, either in isolation or relative to other systems.

The guidance herein supports a wide range of analysis activities, including:

— analysis of a system or component to determine how it operates under specific conditions or contexts;

— comparison of similar or different systems to inform design decisions or procurement choices;

— assessment of specific characteristics relevant to a particular policy or operational requirement;

— support for audit, validation or public transparency efforts.

Recognising that age assurance methods differ significantly in their mechanisms and contexts of use; this document allows for flexibility in analytical methodology. For instance, age verification using digital credentials may require assessment of document authenticity and credential binding, while biometric age estimation may necessitate statistical testing for accuracy, bias and demographic fairness. Contextual factors (such as whether the system is used for online access, entry to a venue or interaction with a vending machine) can also influence the relevant analysis criteria.

Analysis planning may draw upon existing international standards such as ISO/IEC 29155 (benchmarking framework),[1]ISO/IEC 25010 Systems and software engineering — Systems and software Quality Requirements and Analysis (SQuaRE),[2] Product quality model, ISO/IEC 25040 (product quality),[3] ISO/IEC 29119 (software testing), and ISO/IEC 30107 (biometric presentation attack),[4] as applicable.

The document provides a consistent basis for analysis or comparison of age assurance systems, helping to clarify system characteristics, inform stakeholder decision-making and support the development of a trustworthy and effective marketplace for age assurance solutions.

This document does not:

— establish policy decisions, such as age thresholds or mandatory characteristics

— address financial or commercial models

— define or determine conformity or certification outcomes

© ISO/IEC 2026 – All rights reserved

Information security, cybersecurity and privacy protection – Age assurance systems —

Part 3:
Approaches to analysis or comparison

1 Scope

This document establishes considerations for analysing, comparing or differentiating the characteristics of age assurance systems or components.

The document includes metrics, elements and indicators of effectiveness for age assurance systems or components.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27566-1, *Information security, cybersecurity and privacy protection — Age assurance systems — Part 1: Framework*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27566-1 apply, together with the following.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 Analytical activity terms

3.1.1
analysis
structured process of examining or comparing an age assurance system or component to assess how it meets declared characteristics, functional claims or indicators of effectiveness

3.1.2
analysis plan
document describing the scope, methods, tools and indicators to be used in an analysis

3.1.3
system under analysis
age assurance system being subjected to analysis or comparison

Note 1 to entry: This includes a full end-to-end system of a provider or multiple parties.

© ISO/IEC 2026 – All rights reserved

3.1.4
component under analysis
component of an age assurance system being subjected to analysis or comparison

3.1.5
comparison
structured process of examining two or more age assurance systems or components to identify similarities or differences against defined characteristics, functional claims or indicators of effectiveness

3.1.6
comparative analysis
analysis involving two or more systems or components tested under consistent conditions to compare performance, effectiveness or suitability

3.1.7
contextual analysis
analysis of a single system or component within its intended deployment setting and user environment

3.1.8
replicated analysis
analysis that examines system or component characteristics across different points in time or lifecycle stages

3.1.9
exploratory testing
experience-based testing in which the tester spontaneously designs and executes tests based on the tester's existing relevant knowledge, prior exploration of the test item (including the results of previous tests), and heuristic "rules of thumb" regarding common software behaviours and types of failure

Note 1 to entry: Exploratory testing hunts for hidden properties (including hidden behaviours) that, while quite possibly benign by themselves, could interfere with other properties of the software under test, and so constitute a risk that the software will fail.

[SOURCE: ISO/IEC TR 29119-11:2020, 3.1.32[12]]

3.1.10
benchmarking
activity of comparing two or more components under analysis to each other or against a set of benchmarks to measure or rate characteristics.

Note 1 to entry: In the context of this document, age assurance components and age assurance methods are the objects of comparison.

3.1.11
core report
document for providing a description of the process and outcome of analytical activity.

Note 1 to entry: Two kinds of core reports (executive summary and detailed report) are often produced for reporting results of an instance of activity.

[SOURCE: ISO/IEC 29155-1:2017, 3.10 with the term" benchmarking " changed into the term " analysed"[14]]

3.2 Actors and parties in analysis

3.2.1
analyst
person or organization skilled and trained to measure or estimate the effectiveness, efficiency, utility or relevance of a service or facility

Note 1 to entry: An analyst may be internal or external to the system provider but should be independent from system development.

© ISO/IEC 2026 – All rights reserved

3.3 Technical analytical terms

3.3.1
testable element
discrete function or feature of a system or component under analysis that can be independently measured, observed or validated

3.3.2
processing time
time required for an age assurance component or system to complete its operation and to provide a result either to another age assurance component, the user or a relying party

3.3.3
system availability
proportion of time a system is fully operational and accessible for use, functional and responsive over a defined period

3.3.4
latency under load
time delay experienced when multiple users access a system concurrently

3.3.5
scalability
capability of a product to handle growing or shrinking workloads or to adapt its capacity to handle variability

[SOURCE: ISO/IEC 25010, 3.8.2[5]]

3.3.6
data minimization
practice of processing only personal data necessary in relation to the purposes for which they are processed by a component

3.3.7
tamper resistance
ability of a system or component to resist unauthorised modification or manipulation

3.3.8
presentation attack
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Note 1 to entry: An attack presentation can be a single attempt, a multi-attempt transaction, or another type of interaction with a subsystem.

[SOURCE: ISO/IEC 30107-3:2023, 3.1.1[16]]

3.3.9
adversarial input
input intentionally designed to mislead or exploit a component or system’s behaviour decision logic that makes the system fail or affects model behaviour

3.3.10
model poisoning
manipulation of AI model's training dataset to introduce vulnerabilities, backdoors or biases with the intent to modify the model's behaviour to obtain incorrect or unintended decisions

3.3.11
accessibility
usability of a product, service, environment or facility by people with the widest range of capabilities

Note 1 to entry: The concept of accessibility addresses the full range of user capabilities and is not limited to users who are formally recognized as having a disability.

© ISO/IEC 2026 – All rights reserved

Note 2 to entry: The usability-orientated concept of accessibility aims to achieve levels of effectiveness, efficiency and satisfaction that are as high as possible considering the specified context of use, while paying particular attention to the full range of capabilities within the user population.

[SOURCE: ISO 9241-171.3.2[1]]

3.3.12
user interface
set of all the components of an interactive system that provide information and controls for the user to accomplish specific tasks with the interactive system

3.3.13
classification model
machine learning model whose expected output for a given input is one or more classes

[SOURCE: ISO/IEC 23053:2022, 3.1.1[4]]

3.3.14
regression model
machine learning model whose expected output for a given input is a continuous variable

[SOURCE: ISO/IEC 23053:2022, 3.1.2[4]]

3.3.15
ecosystem
infrastructure and services based on a network of organizations and stakeholders

Note 1 to entry: Organizations can include public bodies.

[SOURCE: ISO/IEC TS 27570:2021,[9] 3.8 and ISO/IEC 27400:2022, 3.8[8]]

3.3.16
effectiveness
measure of the degree to which given characteristics are achieved

3.3.17
machine learning
ML
process of optimizing model parameters through computational techniques, such that the model's behaviour reflects the data or experience

[SOURCE: ISO/IEC 22989:2022, 3.4.5[3]]

3.3.18
metric
verifiable measure that captures performance in terms of how something is being done relative to a standard, allows and encourages comparison, supports business strategy

[SOURCE: ISO TS 18864:2017, 3.20[2]]

3.3.19
unlinkability
ability to ensure that an individual can make multiple uses of resources or services without others being able to link these uses together

© ISO/IEC 2026 – All rights reserved