TECHNICAL REPORT

ISO/IEC TR 29119-13

First edition
2022-11

Software and systems engineering — Software testing —

Part 13:
Using the ISO/IEC/IEEE 29119 series in the testing of biometric systems

Reference number
ISO/IEC TR 29119-13:2022(E)

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, definitions and abbreviated terms **1**
3.1 Terms and definitions 1
3.2 Abbreviated terms 7

4 Introduction to biometrics **9**
4.1 Biometrics overview 9
4.2 Standardization and biometrics 9
4.2.1 Introduction to standardization of biometrics 9
4.2.2 ISO/IEC JTC 1/SC 37 (biometrics) 9
4.2.3 ISO/IEC JTC 1/SC 37/WG 5 (biometrics and testing) 10

5 Introduction to software testing **10**
5.1 Software testing in context 10
5.2 Static and dynamic testing 10
5.3 Systematic software testing 10
5.4 Purpose of testing 11
5.5 Standardization and software testing 11
5.5.1 Testing standards prior to the ISO/IEC/IEEE 29119 series 11
5.5.2 The ISO/IEC/IEEE 29119 series 11
5.5.3 ISO/IEC JTC 1/SC 7/WG 26 (software testing) 12
5.6 Risk-based testing 12
5.6.1 Risk-based testing at the core of software testing 12
5.6.2 Risk categories 13

6 Software testing of biometric systems and subsystems **13**
6.1 Traditional evaluation of biometric systems 13
6.1.1 General 13
6.1.2 Evaluation levels for biometric systems 13
6.1.3 Performance measures for biometric systems 17
6.2 Scope of testing for biometric systems 18
6.2.1 General 18
6.2.2 Biometric enrolment and recognition 18
6.2.3 Biometric components and supporting components 18
6.2.4 Biometric subsystem as part of a larger system 18
6.2.5 Static and dynamic testing of the biometric system 19
6.2.6 Testing all quality characteristics or limited to biometric performance 19
6.3 Documentation for testing biometric systems 19
6.4 Standards for testing biometric systems 19

Annex A (informative) **Brief introduction to biometric systems** **20**

Annex B (informative) **Standards related to the testing of biometric systems** **26**

Annex C (informative) **Generic risks in biometric systems** **32**

Annex D (informative) **Test documentation mappings for biometric systems** **77**

Annex E (informative) **Mapping from ISO/IEC 19795-1 to the ISO/IEC/IEEE 29119 series** **97**

Annex F (informative) **Mapping from ISO/IEC 19795-2 to the ISO/IEC/IEEE 29119 series** **150**

Annex G (informative) **Mapping from ISO/IEC 19795-4 to the ISO/IEC/IEEE 29119 series** **194**

Annex H (informative) **Mapping from ISO/IEC 19795-6 to the ISO/IEC/IEEE 29119 series** **226**

Annex I (informative) **Mapping from ISO/IEC 19795-7 to the ISO/IEC/IEEE 29119 series** **236**

Annex J (informative) **Mapping from ISO/IEC TS 19795-9 to the ISO/IEC/IEEE 29119 series** **247**
Annex K (informative) **Mapping from ISO/IEC 29109-1 to the ISO/IEC/IEEE 29119 series** **261**
Bibliography **272**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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 document 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 or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall 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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

A list of all parts in the ISO/IEC/IEEE 29119 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

Introduction

This document provides an overview of the topics of biometric systems and software testing and their standardization. It describes how to apply the ISO/IEC/IEEE 29119 series of software testing standards to the testing of both pure biometric systems and more extensive systems that include biometric subsystems.

It includes information on the creation of a risk-based test strategy that addresses the full range of quality characteristics for a system (i.e. not restricted or focused solely on those quality characteristics covered by biometric technical performance testing).

This document includes mappings between the documentation requirements of:

— ISO/IEC 19795-1

— ISO/IEC 19795-2

— ISO/IEC 19795-6

and the software test documentation defined by ISO/IEC/IEEE 29119-3.

It provides mappings between the ISO/IEC/IEEE 29119 series and the following standards defining the testing of biometric systems:

— ISO/IEC 19795-1

— ISO/IEC 19795-2

— ISO/IEC 19795-4

— ISO/IEC 19795-6

— ISO/IEC 19795-7

— ISO/IEC TS 19795-9

— ISO/IEC 29109-1

The standards covering the evaluation and testing of biometric systems (e.g. the ISO/IEC 19795 series) are written from the perspective of an expert in biometric systems, are focused on technical biometric performance testing (i.e. error rates and throughput rates) based on dynamic testing and do not explicitly use a risk-based approach to the testing, as required by the ISO/IEC/IEEE 29119 series of software testing standards.

This document has been created to provide support to software testers who are inexperienced in testing biometric systems. It lists the most relevant biometric standards for software testers of biometric systems. It provides information on performing systematic software testing (static and dynamic) of biometric systems using a risk-based approach in conformance with the ISO/IEC/IEEE 29119 series of software testing standards. The mappings also show how conformance with the most popular biometric testing standards maps to the requirements of the ISO/IEC/IEEE 29119 series. This document also provides useful information for biometrics experts, who want to test a complete biometric system using a risk-based approach in conformance with the ISO/IEC/IEEE 29119 series of software testing standards.

As a Technical Report, this document contains data of a different kind from that normally published as an International Standard or Technical Specification, such as data on the “state of the art”.

Software and systems engineering — Software testing —

Part 13: Using the ISO/IEC/IEEE 29119 series in the testing of biometric systems

1 Scope

This document:

— gives information for software testers for the systematic, risk-based testing of biometric systems and larger systems which include biometric subsystems;

— establishes the importance of both biometric standards and software testing standards and provides overviews of both areas and their standardization;

— specifies the most important biometric standards for software testers of biometric systems;

— provides information for software testers who wish to conform to both the relevant biometrics standards and the ISO/IEC/IEEE 29119 series of software testing standards by providing mappings between the two sets of standards;

— is not limited to the testing of the technical performance of biometric systems in terms of error rates and throughput rates, but instead covers the testing of the full range of relevant quality characteristics, such as reliability, availability, maintainability, security, conformance, usability, human factors, and privacy regulation compliance;

— gives information on applying a risk-based testing approach to the testing of biometric systems that covers the full range of product and project risks;

— provides testers with an example set of product and project risks associated with biometric systems along with suggestions on how these risks can be treated as part of a risk-based approach to the testing;

— includes mappings between the documentation requirements of ISO/IEC 19795-1, ISO/IEC 19795-2 and ISO/IEC 19795-6 and the software test documentation defined by ISO/IEC/IEEE 29119-3.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology 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/

3.1.1
biometric characteristic
biological and behavioural characteristic of an individual from which distinguishing, repeatable *biometric features* (3.1.3) can be extracted for the purpose of *biometric recognition* (3.1.6)

EXAMPLE Galton ridge structure, face topography, facial skin texture, hand topography, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, handwritten signature dynamics, etc.

[SOURCE: ISO/IEC 2382-37:2022, 37.01.02, modified — The deprecated term has been removed.]

3.1.2
biometric data
biometric sample (3.1.9) or aggregation of biometric samples at any stage of processing

EXAMPLE *Biometric reference* (3.1.7), *biometric probe* (3.1.5), *biometric feature* (3.1.3) or biometric property.

Note 1 to entry: Biometric data need not be attributable to a specific individual, e.g. Universal Background Models.

[SOURCE: ISO/IEC 2382-37:2022, 37.03.06]

3.1.3
biometric feature
number or label extracted from *biometric samples* (3.1.9) and used for *comparison* (3.1.14)

[SOURCE: ISO/IEC 2382-37:2022, 37.03.11, modified — Notes to entry have been removed.]

3.1.4
biometric identification
process of searching against a biometric enrolment database to find and return the *biometric reference* (3.1.7) identifier(s) attributable to a single individual

[SOURCE: ISO/IEC 2382-37:2022, 37.08.02, modified — Note 1 to entry has been removed.]

3.1.5
biometric probe
biometric query
biometric sample (3.1.9) or *biometric feature* (3.1.3) set input to an algorithm for biometric *comparison* (3.1.14) to a *biometric reference(s)* (3.1.7)

Note 1 to entry: In some comparisons, a biometric reference can be used as the subject of the comparison with other biometric references or incoming biometric samples used as the objects of the comparisons. For example, in a duplicate enrolment check, a biometric reference will be used as the subject for comparisons against all other biometric references in the database.

Note 2 to entry: Typically in a biometric comparison process, incoming biometric samples serve as the subject of comparisons against objects stored as biometric references in a database.

[SOURCE: ISO/IEC 2382-37:2022, 37.03.14, modified — "biometric query" has been changed from a preferred term to an admitted term.]

3.1.6
biometric recognition
biometrics
automated recognition of individuals based on their biological and behavioural characteristics

Note 1 to entry: Biometric recognition encompasses *biometric verification* (3.1.12) and *biometric identification* (3.1.4).

Note 2 to entry: Automated recognition implies that a machine-based system is used for the recognition either for the full process or assisted by a human being.

[SOURCE: ISO/IEC 2382-37:2022, 37.01.03, modified — The original notes 1, 2, 5 and 6 to entry have been removed; notes 3 and 4 to entry have been renumbered as notes 1 and 2 to entry.]

3.1.7
biometric reference
one or more stored *biometric samples* (3.1.9), *biometric templates* (3.1.11) or biometric models attributed to a *biometric data* (3.1.2) subject and used as the object of biometric *comparison* (3.1.14)

EXAMPLE Face image stored digitally on a passport, fingerprint minutiae template on a National ID card or Gaussian Mixture Model for speaker recognition, in a database.

Note 1 to entry: A biometric reference may be created with implicit or explicit use of auxiliary data, such as Universal Background Models.

Note 2 to entry: The subject/object labelling in a comparison can be arbitrary. In some comparisons, a biometric reference can potentially be used as the subject of the comparison with other biometric references or incoming samples and input to an biometric algorithm for comparison. For example, in a duplicate enrolment check a biometric reference will be used as the subject for comparison against all other biometric references in the database.

[SOURCE: ISO/IEC 2382-37:2022, 37.03.16]

3.1.8
biometric reference adaptation
automatic incremental updating of a *biometric reference* (3.1.7)

Note 1 to entry: Biometric reference adaptation can be used to improve performance (e.g. adapting the reference to take account of variability of an individual's *biometric characteristics* (3.1.1) and to mitigate performance degradation (e.g. due to changes in biometric characteristics over time).

[SOURCE: ISO/IEC 2382-37:2022, 37.05.05]

3.1.9
biometric sample
analogue or digital representation of *biometric characteristics* (3.1.1) prior to *biometric feature* (3.1.3) extraction

EXAMPLE A record containing the image of a finger is a biometric sample.

[SOURCE: ISO/IEC 2382-37:2022, 37.03.21]

3.1.10
biometric system
system for the purpose of the *biometric recognition* (3.1.6) of individuals based on their behavioural and biological characteristics

[SOURCE: ISO/IEC 2382-37:2022, 37.02.03, modified — Note 1 to entry has been removed.]

3.1.11
biometric template
reference biometric feature set
set of stored *biometric features* (3.1.3) comparable directly to a *biometric probe* (3.1.5)

EXAMPLE A record containing a set of finger minutiae is a biometric template.

Note 1 to entry: A *biometric reference* (3.1.7) consisting of an image, or other *captured biometric sample* (3.1.13), in its original, enhanced or compressed form, is not a biometric template.

Note 2 to entry: The biometric features are not considered to be a biometric template unless they are stored for reference.

[SOURCE: ISO/IEC 2382-37:2022, 37.03.22, modified — "reference biometric feature set" has been changed from a preferred term to an admitted term.]

3.1.12
biometric verification
DEPRECATED: authentication
process of confirming a biometric claim through *comparison* (3.1.14)

[SOURCE: ISO/IEC 2382-37:2022, 37.08.03, modified — Notes to entry have been removed; the deprecated term has been added.]

3.1.13
captured biometric sample
DEPRECATED: raw biometric sample
biometric sample (3.1.9) resulting from a biometric capture process

[SOURCE: ISO/IEC 2382-37:2022, 37.03.25]

3.1.14
comparison
DEPRECATED: match
DEPRECATED: matching
estimation, calculation or measurement of similarity or dissimilarity between *biometric probe(s)* (3.1.5) and *biometric reference(s)* (3.1.7)

[SOURCE: ISO/IEC 2382-37:2022, 37.05.07]

3.1.15
decision policy
one or more rules used to determine whether a biometric *comparison* (3.1.14) results in a positive or negative match

Note 1 to entry: The decision policy often includes a threshold above which a comparison score is considered a match.

3.1.16
detection error trade-off
DET
relationship between false-negative and false-positive errors of a binary classification system as the discrimination threshold varies

Note 1 to entry: The DET may be represented as a DET table or a DET plot.

Note 2 to entry: The receiver operating characteristic (ROC) curve was used in the previous edition of this document. The ROC is unified with the DET.

[SOURCE: ISO/IEC 19795-1:2021, 3.28]

3.1.17
failure to acquire
FTA
failure to accept for subsequent *comparison* (3.1.14) the *biometric sample* (3.1.9) of the *biometric characteristic* (3.1.1) of interest output from the biometric capture process

Note 1 to entry: Acceptance of the output of a biometric capture process for subsequent comparison will depend on policy.

Note 2 to entry: Possible causes of failure to acquire include *failure to capture* (3.1.19), failure to extract, poor biometric sample quality, algorithmic deficiencies and biometric characteristics outside the range of the system.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.03]

3.1.18
failure-to-acquire rate
FTAR
proportion of a specified set of biometric acquisition processes that were *failures to acquire* (3.1.17)

Note 1 to entry: The results of the biometric acquisition processes may be *biometric probes* (3.1.5) or *biometric references* (3.1.7).

Note 2 to entry: The experimenter specifies which biometric probe (or biometric reference) acquisitions are in the set, as well as the criteria for deeming a biometric acquisition process has failed.

Note 3 to entry: The proportion is the number of processes that failed divided by the total number of biometric acquisition processes within the specified set.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.04]

3.1.19
failure to capture
FTC
failure of the biometric capture process to produce a *captured biometric sample* (3.1.13) of the *biometric characteristic* (3.1.1) of interest

Note 1 to entry: The decision as to whether or not a biometric sample has been captured depends on system policy. For example, one system can use a low-quality fingerprint whereas another can declare it a failure to capture.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.05]

3.1.20
failure to enrol
FTE
failure to create and store a biometric enrolment data record for an eligible biometric capture subject in accordance with a biometric enrolment policy

Note 1 to entry: Not enrolling someone ineligible to enrol is not a failure to enrol.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.06]

3.1.21
failure-to-enrol rate
FTER
proportion of a specified set of biometric enrolment transactions that resulted in a *failure to enrol* (3.1.20)

Note 1 to entry: Basing the denominator on the number of biometric enrolment transactions can result in a higher value than basing it on the number of biometric capture subjects.

Note 2 to entry: If the FTER is to measure solely transactions that fail to complete due to quality of the submitted *biometric data* (3.1.2), the denominator should not include transactions that fail due to non-biometric reasons (i.e. lack of eligibility due to age or citizenship).

[SOURCE: ISO/IEC 2382-37:2022, 37.09.07]

3.1.22
false accept rate
FAR
proportion of verification transactions with false biometric claims erroneously accepted

[SOURCE: ISO/IEC 19795-1:2021, 3.21]

3.1.23
false match
comparison (3.1.14) decision of a match for a *biometric probe* (3.1.5) and a *biometric reference* (3.1.7) that are from different biometric capture subjects

Note 1 to entry: It is recognized that this definition considers the false match at the subject level only, and not at the *biometric characteristic* (3.1.1) level. Sometimes a comparison can be made between a biometric probe and a biometric reference from different biometric characteristics of a single biometric capture subject. In some of these cases, for example, when comparing Galton ridges of different fingers of the same *biometric data* (3.1.2) subject, a comparison decision of match can be considered to be an error. In other cases, for example when comparing a mispronounced pass-phrase in text-dependent speaker recognition, a comparison decision of match can be considered to be correct.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.08]

3.1.24
false match rate
FMR
proportion of the completed biometric non-mated *comparison* (3.1.14) trials that result in a *false match* (3.1.23)

Note 1 to entry: The value computed for the false match rate depends on thresholds, and other parameters of the comparison process, and the protocol defining the biometric non-mated comparison trials.

Note 2 to entry: Comparisons between the following require proper consideration (see ISO/IEC 19795-1):

— identical twins;

— different, but related *biometric characteristics* (3.1.1) from the same individual, such as left and right-hand topography.

Note 3 to entry: "Completed" refers to the computational processes required to make a comparison decision, i.e. failures to decide are excluded.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.09]

3.1.25
false-negative identification rate
FNIR
FNIR(N, R, T)
proportion of a specified set of *identification transactions* (3.1.30) by capture subjects enrolled in the system for which the subject's correct reference identifier is not among those returned

Note 1 to entry: The false-negative identification rate can be expressed as a function of N, the number of enrolees, and of parameters of the identification process where only candidates up to rank R, and with a candidate score greater than threshold T are returned to the candidate list.

[SOURCE: ISO/IEC 19795-1:2021, 3.22, modified — "FNIR(N, R, T)" has been changed from a preferred term to an admitted term.]

3.1.26
false non-match
comparison (3.1.14) decision of non-match for a *biometric probe* (3.1.5) and a *biometric reference* (3.1.7) that are from the same biometric capture subject and of the same *biometric characteristic* (3.1.1)

Note 1 to entry: There can need to be consideration on how much non-conformance to system policy on the part of the biometric capture subject is tolerated before the biometric probe and the biometric reference are deemed to be of different biometric characteristics.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.10]

3.1.27
false non-match rate
FNMR
proportion of the completed biometric mated *comparison* (3.1.14) trials that result in a *false non-match* (3.1.26)

Note 1 to entry: The value computed for the false non-match rate will depend on thresholds, and other parameters of the comparison process, and the protocol defining the biometric mated comparison trials.

Note 2 to entry: "Completed" refers to the computational processes required to make a comparison decision, i.e. failures to decide are excluded.

[SOURCE: ISO/IEC 2382-37:2022, 37.09.11]

3.1.28
false-positive identification rate
FPIR
FPIR(*N*, *T*)
proportion of *identification transactions* (3.1.30) by capture subjects not enrolled in the system, where an identifier is returned

Note 1 to entry: The false-positive identification rate can be expressed as a function of parameters of the identification process for returning matched reference identifiers including comparison score threshold (*T*), and the number of enrolees in the system (*N*).

[SOURCE: ISO/IEC 19795-1:2021, 3.23, modified — "FPIR(*N*, *T*)" has been changed from a preferred term to an admitted term; the original notes 1 and 2 to entry have been replaced by a new note 1 to entry.]

3.1.29
false reject rate
FRR
proportion of verification transactions with true biometric claims erroneously rejected

[SOURCE: ISO/IEC 19795-1:2021, 3.20]

3.1.30
identification transaction
sequence of one or more capture attempts and biometric searches to find and return the *biometric reference* (3.1.7) identifier(s) attributable to a single individual

[SOURCE: ISO/IEC 19795-1:2021, 3.10]

3.1.31
multi-modal biometric system
biometric system (3.1.10) based on multiple *biometric characteristics* (3.1.1)

3.1.32
throughput rate
number of subjects that can be processed by a *biometric system* (3.1.10) per unit time

Note 1 to entry: The throughput rate is dependent on both the system characteristics and those of the subjects.

3.2 Abbreviated terms

API	application programming interface
BIT	built-in test
BDIR	biometric data interchange record

CPU	central processing unit
CMC	cumulative match characteristic
DAC	digital-to-analogue converter
DET	detection error trade-off
EQ	equal
FAR	false accept rate
FAS	failure at source
FIF	fusion information format
FTA	failure to acquire
FTAR	failure-to-acquire rate
FTC	failure to capture
FTE	failure to enrol
FTER	failure-to-enrol rate
FMR	false match rate
FNIR	false-negative identification rate
FNMR	false non-match rate
FPIR	false-positive identification rate
FRR	false reject rate
GDPR	General Data Protection Regulation
GFAR	generalized false accept rate
GFRR	generalized false reject rate
GT	greater than
GTE	greater than or equal
HTER	half total error rate
IBDR	input biometric data record
ICAO	International Civil Aviation Organization
IEEE	Institute of Electrical and Electronics Engineers
INC	incremental
LT	less than
LTE	less than or equal
MO	member of

MRP	machine-readable passport
NEQ	not-equal
OS	operating system
RACI	responsible, accountable, consulted, and informed
RAM	random access memory
RBT	risk-based testing
ROC	receiver operating characteristic
ROM	read-only memory

4 Introduction to biometrics

4.1 Biometrics overview

Biometric systems are used to recognize people based on their physiological and/or behavioural characteristics. A key benefit is that the user does not have to carry a token of their identity (e.g. an identity card), which can be lost or stolen, or remember one or more passwords, as their identity can be recognized from their in-built traits. Example biometric characteristics used by biometric systems include, among others: fingerprints, faces, hands, retinas, and voices.

Biometric systems and biometric subsystems within larger systems are becoming more prevalent and critical to people's daily lives. These systems are used to recognize people in a range of contexts, such as border management, voter authentication, law enforcement, and access to a variety of entities (e.g. computer systems, personal devices, and physical areas, such as buildings and entertainment events).

Annex A provides a brief introduction to biometrics for those new to the field (e.g. testers who have been asked to test their first biometric system or system including a biometric subsystem).

4.2 Standardization and biometrics

4.2.1 Introduction to standardization of biometrics

Standardization aims to promote innovation, help improve system quality, and ensure user safety, while creating a fair and open industry ecosystem. Biometric standardization occurs at various levels, including:

— international standards organizations;

— regional standards organizations;

— national standards;

— other standards organizations.

Under Joint Technical Committee 1 (JTC 1) of ISO and IEC, Subcommittee 37 (SC 37) is specifically responsible for biometrics standards, although biometric systems are also covered by other ISO/IEC committees and groups, such as SC 17 (Cards and security devices for personal identification) and SC 27 (Information security, cybersecurity and privacy protection).

4.2.2 ISO/IEC JTC 1/SC 37 (biometrics)

ISO/IEC JTC 1/SC 37 covers the standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic

human biometric standards include common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.

4.2.3 ISO/IEC JTC 1/SC 37/WG 5 (biometrics and testing)

ISO/IEC JTC 1/SC 37 Working Group 5 (WG 5) covers the standardization of biometric testing and reporting.

Annex B provides descriptions of standards related to the testing of biometric systems.

5 Introduction to software testing

5.1 Software testing in context

Software testing has been a fundamental part of software development since well before life cycle models were defined, with references to a separate software testing activity being made as early as 1954.[46] Today, estimates for the proportion of life cycle costs spent on testing vary from below 20 % up to 80 % for safety-critical systems.

Software testing is a form of quality control, which, together with quality assurance comprise quality management. Verification and validation are both quality control concepts supported by software testing; verification focuses on the conformance of a test item with specifications, specified requirements, or other documents, while validation focuses on the value of the test item in respect to the intended use by the stakeholders.

5.2 Static and dynamic testing

Software testing can take two forms; static and dynamic.

Static testing is evaluation of a test item where no execution of the code takes place and can be performed manually (e.g. reviews) or by using tools (e.g. static analysis). Reviews, as defined in ISO/IEC 20246, range in formality and include inspections, technical reviews, walkthroughs, and informal reviews. Static analysis involves the use of tools to detect anomalies in code or documents without execution (e.g. a compiler, a cyclomatic complexity analyser, or a security analyser for code).

Dynamic testing involves executing code and running test cases and can be performed manually or using test tools. The test cases are generated using test design techniques, as defined in ISO/IEC/IEEE 29119-4 and can be black-box (based on a specification), white-box (based on the source code) or some mix of the two (grey-box). The requirement to create test cases tends to make the cost of dynamic testing far higher than static analysis.

5.3 Systematic software testing

To prove that a specific test item meets all requirements under all given circumstances, then all possible combinations of input values in all possible states would need to be dynamically tested. This activity is referred to as “exhaustive testing”, but, in practice, test items tend to be complex enough that the application of exhaustive testing is not possible. For this reason, in practice, software testing derives test suites by sampling from the (extremely large) set of possible input combinations and states. Choosing the subset of possible tests that are most likely to uncover issues of interest is one of the most demanding tasks of a tester but is helped by the use of test case design techniques, which provide a systematic means of deriving this subset.

5.4 Purpose of testing

Testing usually serves more than one purpose. Typical purposes include, but are not restricted to, the following.

— Detecting defects - this allows for their subsequent removal thus increasing software quality.

— Gathering information on the test item - testing generates information. This information can serve different purposes, such as:

  — developers can use the information to remove defects, increase the code quality or learn to create better code in the future;

  — testers can use the information to create better test cases;

  — managers can use the information to assess the project situation.

— Creating confidence and taking decisions - by providing evidence that the test item performs correctly under specific circumstances, the stakeholders' confidence that the test item will perform correctly operationally increases. With sufficient confidence, stakeholders can decide to release the test item.

Testing can be performed for some or all of these purposes, and additional purposes not listed also exist; these purposes are identified and agreed as a starting point to any testing activity.

5.5 Standardization and software testing

5.5.1 Testing standards prior to the ISO/IEC/IEEE 29119 series

Until 2013, several software testing standards were available. For instance, BS 7925-2 covered the dynamic testing of software components, while IEEE 829 covered test documentation. However, only a small part of software testing was covered by standards (e.g. test management was not covered) and some of the standards overlapped in their coverage of the topic, often providing conflicting guidance.

5.5.2 The ISO/IEC/IEEE 29119 series

In 2007 the proposal for a new set of standards on software testing was approved by ISO, to be based on existing IEEE and BSI standards (e.g. IEEE 829, BS 7925-1 and BS 7925-2). The ISO/IEC/IEEE 29119 series is intended to support testing in a wide variety of application domains, for varying levels of criticality and in any life cycle; thus, the standards are generic and can be applied to:

— the full range of quality characteristics, both functional and non-functional;

— all industrial domains;

— safety critical and non-safety critical systems;

— exploratory and scripted testing;

— any life cycle model, including traditional (e.g. waterfall, V-model) and agile (e.g. Scrum, Kanban, hybrid);

— automated testing.

The underlying model used as the basis for the ISO/IEC/IEEE 29119 series is shown in Figure 1, with the test processes at the core. The test documentation is produced by executing the test processes; thus, the test documentation describes the outputs of the test processes. The requirement to use techniques to design the test cases is specified by the test processes in ISO/IEC/IEEE 29119-2, while the different test design techniques are defined separately in ISO/IEC/IEEE 29119-4. The overall concepts used by the other parts are defined in ISO/IEC/IEEE 29119-1.

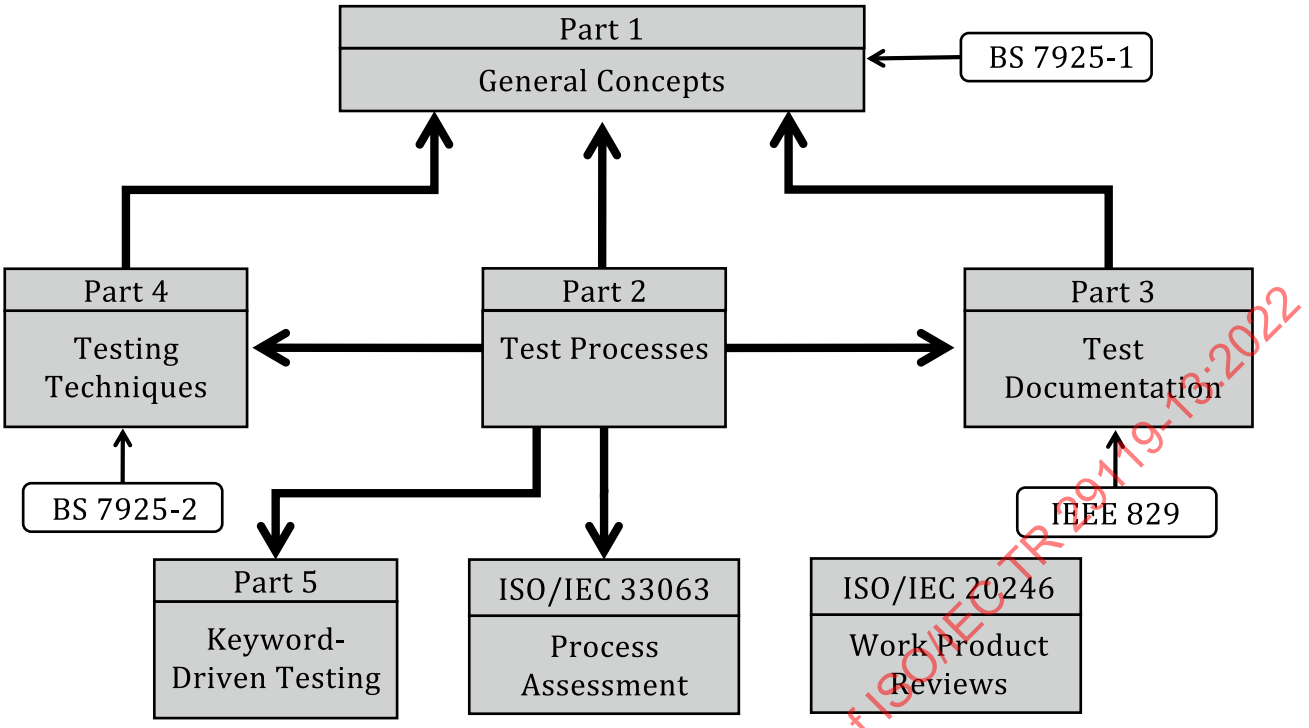

Figure 1 — ISO/IEC/IEEE 29119 software testing standards

Soon after work on the first four parts of the ISO/IEC/IEEE 29119 series started, ISO/IEC 33063 on test process assessment (assessing against the test processes defined in ISO/IEC/IEEE 29119-2) was created by a separate proposal and this was followed by the development of ISO/IEC/IEEE 29119-5 on keyword-driven testing. The first three parts were initially published in 2013, ISO/IEC/IEEE 29119-4 in 2015 and ISO/IEC/IEEE 29119-5 was published in 2016. A separate standard on reviews (ISO/IEC 20246) was subsequently developed to complement the dynamic testing covered by the other standards and was published in February 2017. Updated second editions of ISO/IEC/IEEE 29119-2, ISO/IEC/IEEE 29119-3 and ISO/IEC/IEEE 29119-4 were published in 2021.

5.5.3 ISO/IEC JTC 1/SC 7/WG 26 (software testing)

The ISO/IEC/IEEE 29119 series was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 7, Software and systems engineering, in cooperation with the Software and Systems Engineering Standards Committee of the IEEE Computer Society, under the Partner Standards Development Organization cooperation agreement between ISO and IEEE. WG 26 was set up in 2007 to develop the standards.

5.6 Risk-based testing

5.6.1 Risk-based testing at the core of software testing

Risk-based testing (RBT) is a core concept in the ISO/IEC/IEEE 29119 series, which expect risks to be used as the prime driver for determining the content of the test strategy.

The process for managing risks by testing (RBT) is similar to most other risk management processes. Initially potential risks are identified, sometimes using checklists based on quality characteristics, such as those defined in ISO/IEC 25010. Next, they are analysed to determine the potential impact (severity) they would have (on a delivered product or the project) if they were to occur. The likelihood of each risk is determined, which can be based on factors such as requirement quality, staff capabilities, system complexity and historical information. A risk exposure level is then established, based on combining the impact and likelihood of each risk. Risks can then be prioritized accordingly, and treatments decided,

if appropriate (or possible) – always remembering that a treatment for one risk can be the cause of, or increase exposure to, another risk.

Annex C provides a set of risks applicable to biometric systems in general (i.e. not specific to any particular biometric characteristic). It also provides example software testing actions that can be used to treat these risks, which would be included in the test strategy (and test plan) for the testing of a biometric system.

5.6.2 Risk categories

Risks can be categorized as either product or project risks.

Product risks are concerned with the deliverable product (in this case the biometric system) and include possible losses or harm to users or other stakeholders due to the product not performing as required.

Project risks are concerned with how the product is developed and include the threat that developers, testers, and other project members lack the necessary skills or time to perform their required activities, or that the product will be delivered late or over budget.

6 Software testing of biometric systems and subsystems

6.1 Traditional evaluation of biometric systems

6.1.1 General

The testing of biometric systems is distinctive in two principal areas; in the levels of evaluation and in the performance measures. Readers new to biometrics can read Annex A, which provides a brief introduction to biometric systems, before this clause.

6.1.2 Evaluation levels for biometric systems

6.1.2.1 Overview

There are three widely used evaluation levels for biometric systems, technology evaluation, scenario evaluation and operational evaluation. These three evaluation levels are shown in relation to the test levels typically used when performing software testing using a V lifecycle model in Figure 2. Technology evaluation is performed at the component test level, while scenario evaluation is performed at the integration and system test levels. Operational evaluation includes both operational trials and performance monitoring, and so covers both the acceptance test level and maintenance testing, which is performed on operational systems.

For technology evaluation the test environment typically involves no system hardware, with all tests being run on development/test machines. In scenario evaluation the real sensors are used, and the rest of the biometric system is kept as closely representative of the operational environment as possible. Operational evaluation is normally performed in the operational environment itself.

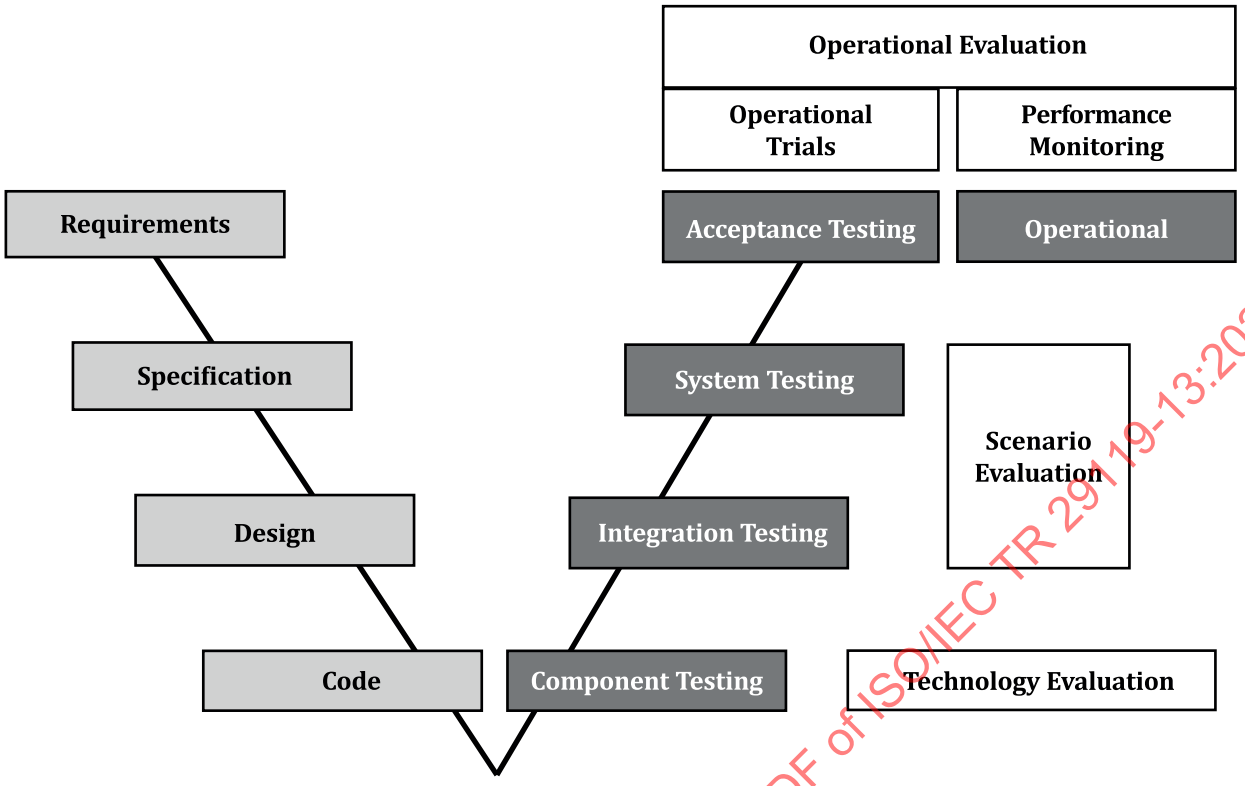

Figure 2 — Evaluation levels across the software lifecycle

6.1.2.2 Technology evaluation

Technology evaluation is concerned with the evaluation and comparison of biometric components when presented with the same input data in the same test environment. A technology evaluation is ideally reproducible and does not use real sensors to provide the input data; instead, a set of biometric samples, often known as a corpus, is used instead. As the performance of biometric systems is heavily dependent on the test data and test environment, the results of a technology evaluation are qualified with details of these two factors.

Figure 3 provides a logical view of technology evaluation and the different biometric system components that are tested as part of it. The elements shown in grey (e.g. enrolment biometric sample corpus) are part of the test environment and are not part of the deliverable system.

Tests performed as part of technology evaluation generate biometric performance measures, which can be divided into two areas.

The first area is concerned with the ability of components to gather information into a format that can be used by the biometric system from biometric samples (which would come from sensors in the finished system but are replaced here with drivers that present sensor input data to the system that are read from databases). This allows biometric performance measures in the form of failure to enrol rate (specific to enrolment of a subject on the system), failure to acquire rate and failure to capture rate (these latter two measures can be associated with creating a biometric probe for comparison with stored biometric references or the creation of a biometric reference for storage in the biometric enrolment database) to be calculated.

The second area provides biometric performance measures on the ability of the tested components to recognize if a captured biometric probe adequately matches a reference in the system's biometric enrolment database. At this point the decision policy is applied that can, for instance, specify that multiple attempts are allowed. This area provides measures for verification or identification (e.g. false match rate, false non-match rate) and is dependent on the first area providing suitable inputs.

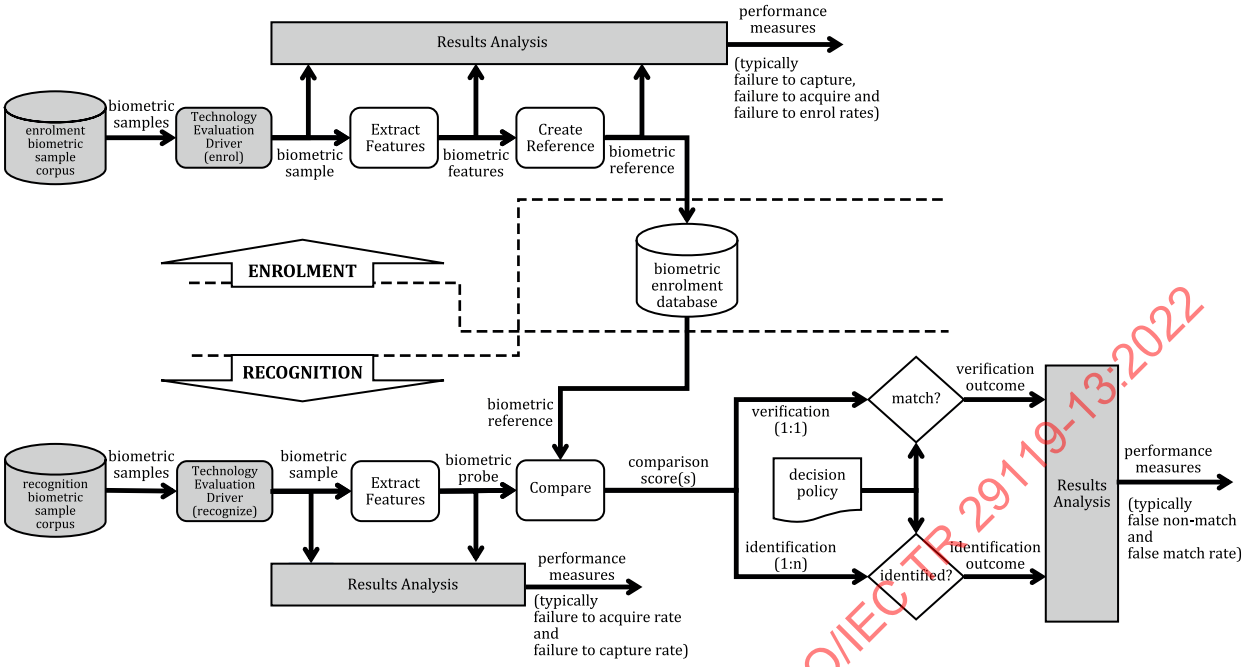

Figure 3 — Technology evaluation of biometric systems

6.1.2.3 Scenario evaluation

Scenario evaluation is concerned with the evaluation of a complete biometric system in a test environment that is representative of the actual operational environment using the same sensors as the proposed operational system. As a scenario evaluation involves real people providing inputs via real sensors, the results are less reproducible than for a technology evaluation.

Figure 4 provides a logical view of scenario evaluation. Compared to technology evaluation, the drivers are now replaced by actual sensors, which means the biometric characteristics (e.g. facial features, fingerprints) are now provided by real test subjects rather than being read from a database. Similar biometric performance measures are generated as for technology evaluation, except that now it is also possible to provide a measure of the throughput rate of the system (e.g. number of test subjects handled by the system per hour).

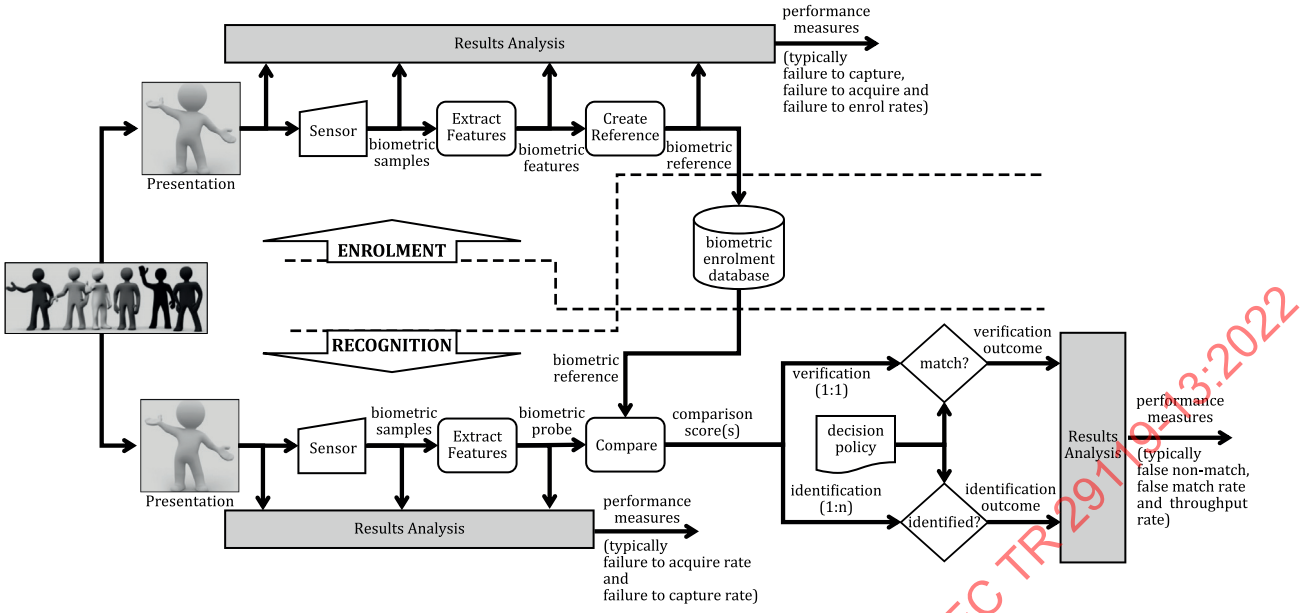

Figure 4 — Scenario evaluation of biometric systems

6.1.2.4 Operational evaluation

Operational evaluation is concerned with the performance of a biometric system in its target operational environment. Operational evaluation is normally performed with real subjects (e.g. actual passengers passing through an airport), which means that reproducibility is typically extremely low (lower than for scenario evaluation). It can also sometimes be difficult to know when the system is providing the correct results (e.g. if the system permits access to a building for many subjects, then determining if each of those subjects are supposed to be allowed access or not can often be impossible).

Figure 5 provides a logical view of scenario evaluation. For an operational biometric system, lack of access to intermediate measures (e.g. determining if a failure to generate a biometric probe was due to failure to capture a suitable sample or a failure to extract the features) can make the generation of some biometric performance measures more difficult than for scenario evaluation. In Figure 5, it is assumed that failure to capture/enrol can be determined from the feedback given to the test subjects. Although it is relatively easy to measure the throughput rate of the system, the generation of accurate figures for false match and false non-match rates can be far more difficult.

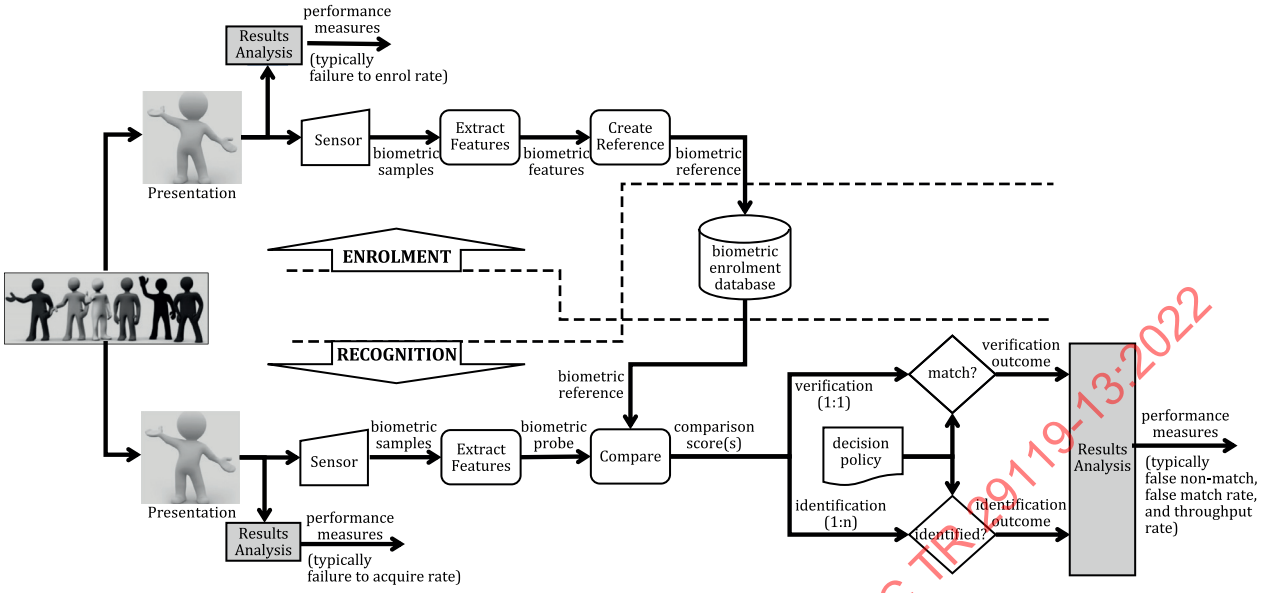

Figure 5 — Operational evaluation of biometric systems

The evaluation and testing of biometric systems can be challenging. It is often the case that test results from development (e.g. scenario evaluation) are not representative of those found in real world operation.

6.1.3 Performance measures for biometric systems

Biometric systems can be measured using various performance measures.

NOTE 'Performance measures' for biometric systems are not directly related to non-functional performance testing or the performance efficiency quality characteristic defined in ISO/IEC 25010. They are, instead, a mix of functional and non-functional measures of the effectiveness of a biometric system.

The following are some of the most common biometric performance measures (as described in ISO/IEC 19795-1).

— Failure to acquire (FTA) rate. The proportion of times the biometric system fails to create a biometric reference (for enrolment) or biometric probe (for recognition). A failure to acquire can be due to a failure to capture a biometric sample or due to an extracted biometric sample being of inadequate quality. Capture is the first part of acquisition, and so the failure to acquire rate cannot be lower than the failure to capture rate.

— Failure to capture (FTC) rate. The proportion of times the biometric system fails to capture a biometric sample presented by an individual. For example, the fingerprint reader was not able to gather enough information from the finger presented to the device. Failure to capture is strongly associated with the sensors used to capture biometrics samples and can be measured for both enrolment and recognition.

— Failure to enrol (FTE) rate. The proportion of times the biometric system fails to acquire a valid individual's biometric reference and store it in the enrolment database. This measure is based on the proportion of unsuccessful transactions rather than the number of individuals who attempt to enrol, as it is possible the biometric system will allow a single individual multiple attempts to enrol.

— False non-match rate (FNMR). The proportion of times the biometric system does not match an individual's acquired biometric probe to their valid stored reference (e.g. when a system refuses access to someone who meets the requirements to be let in).

— False match rate (FMR). The proportion of times the biometric system matches an individual's biometric probe to an unrelated set of biometric data (e.g. when a system allows access to someone who does not meet the requirements to be let in).

— Throughput rate. The number of subjects that can be processed by the system over a period of time (e.g. a biometric system controlling access to a sports event with a requirement to achieve a throughput of at least 1 000 spectators per minute).

Only one of these 'performance' measures relates to a non-functional system requirement/characteristic (throughput rate) as defined in ISO/IEC 25010. In practice, several other non-functional system quality characteristics will also need to be evaluated and a risk-based approach to the testing is the most effective approach to identifying the most relevant characteristics to measure and test (see 5.6).

When a biometric system is being tuned, the correct balance between the false non-match rate and false match rate needs to be achieved - this depends on the context of the system. For instance, a biometric system controlling access to a highly secure area would have an extremely low false match rate, and, to achieve this, a higher false non-match rate is then accepted.

6.2 Scope of testing for biometric systems

6.2.1 General

The potential scope of software testing for biometric systems can be considered from several viewpoints.

6.2.2 Biometric enrolment and recognition

Logically, biometric systems comprise two parts; enrolment and recognition, as shown in Figure A.1. For some projects only one of the two parts will be in scope. For instance, a biometric access system for a sports venue that uses national identity cards as the source of the biometric reference will not include enrolment functions (but it is possible that the quality of enrolled references is of interest).

If just one of the two parts is being tested, then the test environment will need to include the other part in some way to support integration testing of the two parts. This can be by using an operational version, if it is available, or, if the other part is not available, then it will need to be simulated for testing.

6.2.3 Biometric components and supporting components

The core software components of a biometric system support feature extraction and matching, however a typical biometric system also requires software components to support implementation of the user interface, the database, and communications, among other components, as shown in Figure A.3.

If the scope of the biometric system testing encompasses all the software components in the larger biometric system (e.g. all the software components shown in Figure A.3), then the acceptance criteria will need to include more than those biometric performance metrics described in 6.1.3.

6.2.4 Biometric subsystem as part of a larger system

A biometric system can be part of a larger system, such as a banking app, as shown in Figure A.4.

Where the biometric system is a subsystem of a larger system then, in addition to the testing of the biometric subsystem and the other subsystems in isolation, system integration testing to ensure interoperability between the biometric subsystem and other subsystems will also need to be performed. Subsequently, the complete system will need to be tested for the most important quality characteristics (determined using a risk-based approach) and then, the complete system will undergo acceptance testing.

6.2.5 Static and dynamic testing of the biometric system

Full testing of a biometric system would include both static testing (e.g. reviews and static analysis) and dynamic testing (i.e. executing code).

According to ISO/IEC/IEEE 29119-1, testing comprises both static testing and dynamic testing – and a test strategy that conforms to ISO/IEC/IEEE 29119-3 would include both static and dynamic testing.

6.2.6 Testing all quality characteristics or limited to biometric performance

Testing performed in conformance with ISO/IEC/IEEE 29119-2 and ISO/IEC/IEEE 29119-3 is expected to manage risks across all relevant quality characteristics (e.g. including those listed in ISO/IEC 25010), which far exceeds the scope of the biometric performance metrics specified in ISO/IEC 19795-1.

If the testing is to consider all relevant quality characteristics, then acceptance criteria for each relevant quality characteristics are agreed by stakeholders, and a risk-based approach used to prioritise the management of the risks by testing, resulting in a test strategy that is not solely focused on biometric performance metrics, such as those described in 6.1.3.

6.3 Documentation for testing biometric systems

Software testers who are required to perform their testing in accordance with both biometric standards and the ISO/IEC/IEEE 29119 series of software testing standards will find that there are two sets of documentation requirements that they need to meet. As these two sets of requirements were developed without collaboration between the developers of these standards then satisfying the requirements of both sets of standards can be challenging.

To support testers in such a situation, Annex D provides four sets of test documentation requirements for biometric testing (general, technology evaluation, scenario evaluation, and operational evaluation) and maps these to the test documentation defined in ISO/IEC/IEEE 29119-3.

6.4 Standards for testing biometric systems

ISO/IEC JTC 1/SC 37/WG 5 have developed numerous standards applicable to the testing of biometric systems, several of which will be useful to a software tester required to test such a system. There are also several biometric standards that, while not being directly related to software testing, are also likely to be useful to software testers, such as standards defining biometric data interchange formats and APIs for biometric systems. Annex B provides descriptions of some of these biometric standards that are most likely to be of use to a software tester.

Software testers who are required to perform their testing in accordance with both biometric standards and the ISO/IEC/IEEE 29119 series of software testing standards can perform their testing more effectively if they know how the biometric testing/evaluation standards relate to the software testing standards. To support such activities, mappings are provided in this document from the following biometrics testing and evaluation standards to ISO/IEC/IEEE 29119-2 and ISO/IEC/IEEE 29119-3:

— ISO/IEC 19795-1 (see Annex E)

— ISO/IEC 19795-2 (see Annex F)

— ISO/IEC 19795-4 (see Annex G)

— ISO/IEC 19795-6 (see Annex H)

— ISO/IEC 19795-7 (see Annex I)

— ISO/IEC TS 19795-9 (see Annex J)

— ISO/IEC 29109-1 (see Annex K)

Annex A
(informative)

Brief introduction to biometric systems

A.1 General

'Biometric' is compound term formed from the terms bio (meaning life) and metric (meaning measurement) – resulting in an adjective pertaining to the use of a person's physical or behavioural traits for the purpose of measurement. Biometric systems are generally considered to be those used for the purposes of recognition.

Biometric recognition encompasses:

— biometric verification; this is where the biometric system determines if the person matches a previously stored record of their biometric data; thus, it is performing a one-to-one match as it works with just one person and one set of biometric data;

— biometric identification; this is where the biometric system identifies which record in a database of stored biometric data matches the person; thus, it is performing a one-to-many match as it works with one person and many sets of biometric data.

For either verification or identification of a person to be performed, the biometric system first needs the person's biometric reference, which captures their individual features, to be stored in a biometric enrolment database (see A.2.1).

A.2 Generic biometric system

A.2.1 Structure of a biometric system

A high-level view of the components that make up a generic biometric system is shown in Figure A.1. Logically, there are two parts; the enrolment part and the recognition part, which both share use of the biometric enrolment database. In the enrolment part the person's biometric characteristics are captured and their biometric reference is stored. The template is often stored in a database, but it is also often stored on a portable repository, such as a passport (see A.2.2 for more details). In the recognition part the person provides a biometric probe that is then compared with one or more stored references (comparison with one template for verification and comparison with multiple templates for identification).

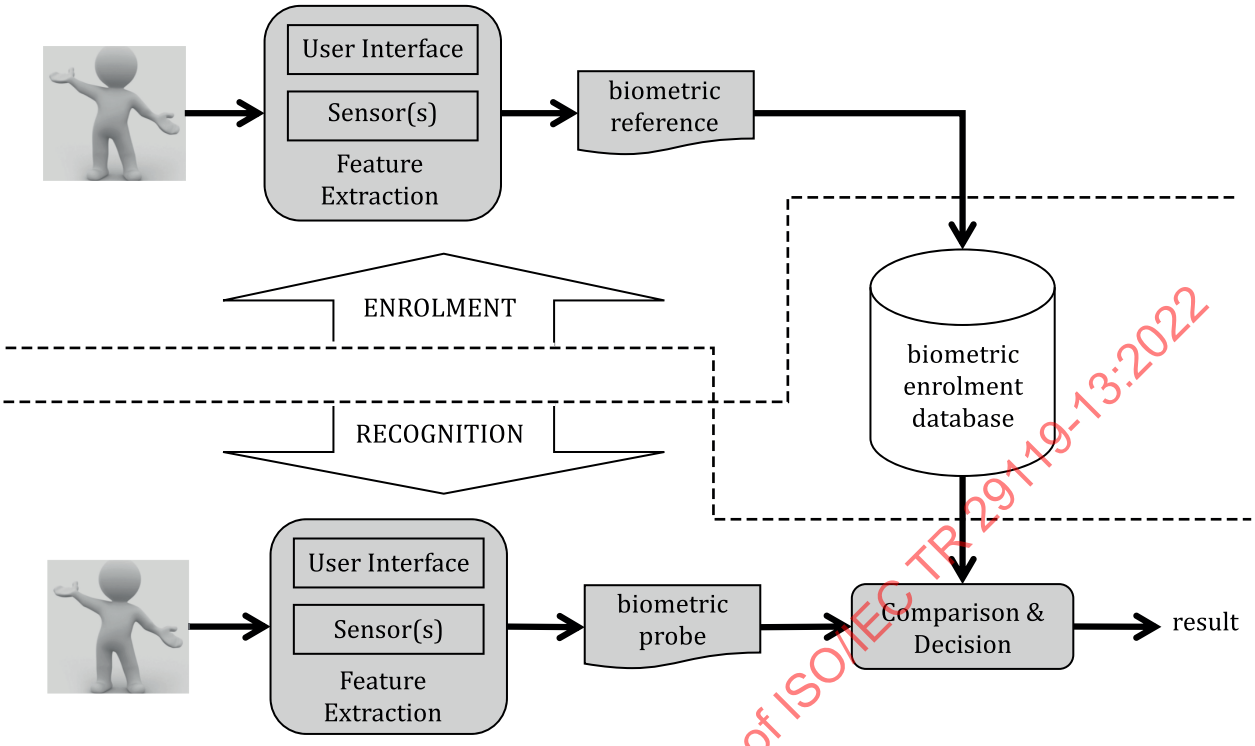

Figure A.1 — Generic biometric components – high level

When feature extraction is performed, normally the system will initially evaluate the quality of the extracted biometric sample to determine if it is good enough to be used by the system. If it is not good enough the system will often try again, because, for instance, on a second attempt the person presents the characteristic in a way that makes it easier to extract the required features at the required quality level.

When the system attempts to match an extracted sample, it is highly unlikely that a perfect match will be achieved, and the system typically generates a comparison score for the match. The system implementers or administrators can often set the threshold which the system uses to decide if the match score is considered adequate to confirm a match.

Figure A.2 provides a more detailed view of the components that make up a generic biometric system. In this figure, the capture of the biometric sample and the extraction of the biometric features/probe are shown explicitly, and the decision-making is shown in more detail. The subject presents biometric characteristics (e.g. fingerprints) to a biometric sensor, which captures a biometric sample. If there are sufficient details in this sample, relevant biometric features are extracted and, in the case of enrolment, these are used to create a biometric reference, which is stored in a database. For recognition, the extracted features form a biometric probe, which is compared against the contents of the database. The system can perform either verification (a one-to-one comparison), where the probe is compared with one stored reference (i.e. verifying that the subject is who they say they are), or identification (a one-to-many comparison), where the probe is compared against all of the stored references (e.g. to determine if the subject is on a watch list). For either identification or verification, a comparison score is generated, and a decision policy is used to decide if the probe and template match closely enough to be flagged as a probable match; the difference is that for identification multiple matches can be flagged.

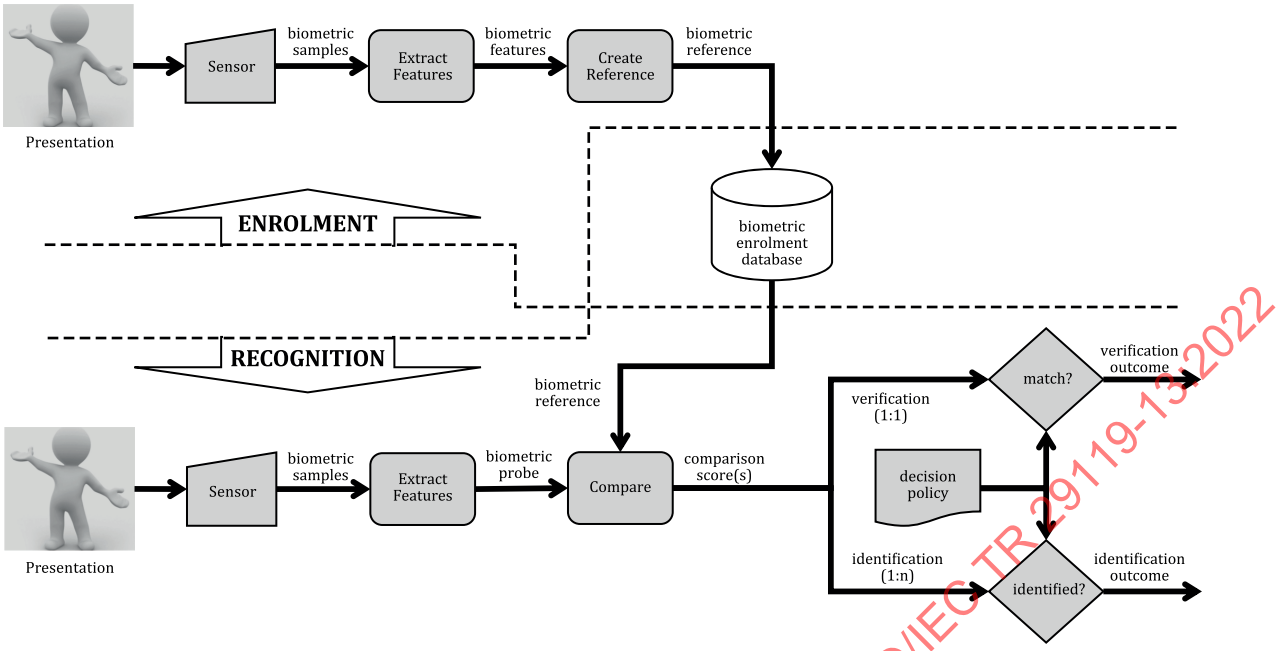

Figure A.2 — Generic biometric components - detailed

In practice, the biometric components in Figure A.1 and Figure A.2 cannot work in isolation. Biometric systems typically also need to provide a user interface and to manage communication with other systems; Figure A.3 shows a biometric subsystem (itself comprised of the components in Figure A.2) as part of a larger system, interacting with a user interface, sensors, external interfaces (e.g. for communication with other systems), and a database through several software components.

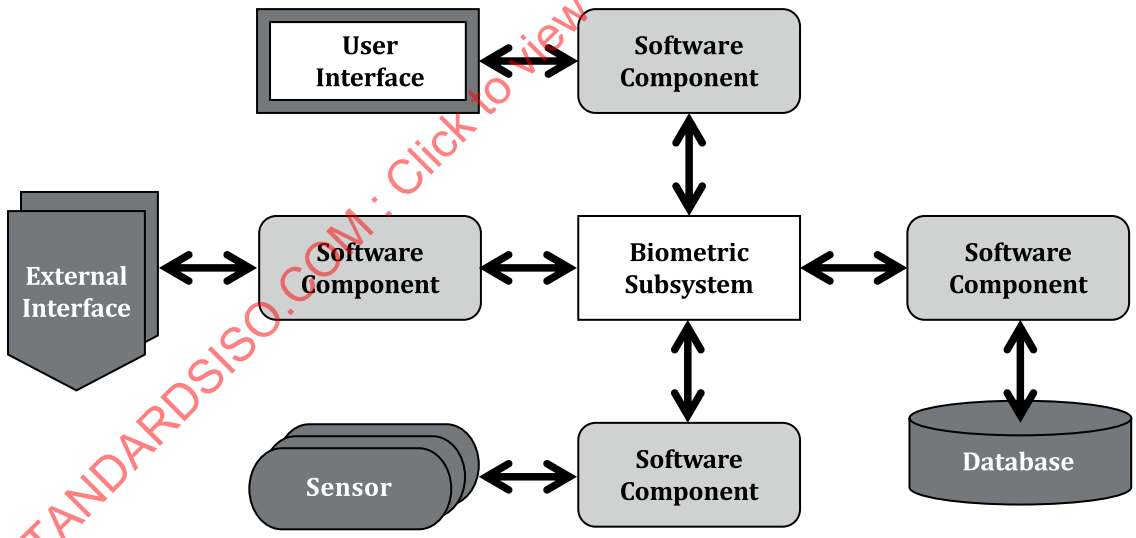

Figure A.3 — Generic biometric system

Biometric systems often form parts of larger systems, where they are more correctly known as biometric subsystems. For instance, Figure A.4 shows a biometric subsystem as part of a banking application. Many smartphones and laptops also include biometric subsystems (e.g. using fingerprint or facial recognition).

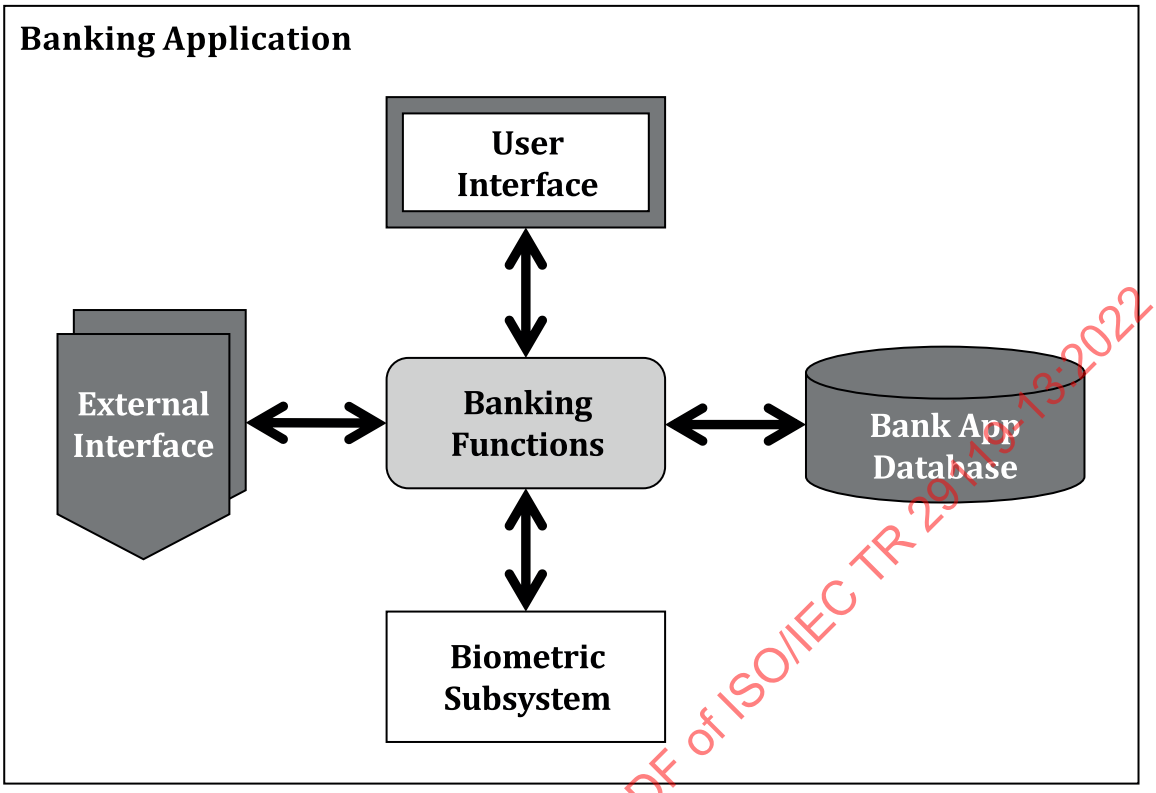

Figure A.4 — Example banking application with biometric subsystem

A.2.2 Biometric enrolment database

A.2.2.1 General

The biometric reference can be stored in several ways that are not obvious from Figure A.1 and Figure A.2, but there are typically four options.

A.2.2.2 Central server

The references are stored centrally, often in a database. If the central server is not secure, there is a danger that all the references will be stolen or illegally accessed. Also, the references need to be communicated over a network so that they can be used for comparison, opening up another potential vulnerability if the communication is compromised (although communication of biometric references would normally be encrypted).

A.2.2.3 Workstations

The references are stored on individual workstations. This means they are only available at the location of the workstation, however, by distributing the system's biometric references across several workstations, there is no one target for malicious attacks and references are less likely to be communicated across a network. However, managing security across multiple workstations can be more open to mistakes than managing security on a single central server.

A.2.2.4 Smart sensors

The references are stored on an individual sensor. As with workstations, the references are only available at a single location, but getting access to biometric references on a smart sensor can be faster than accessing a central server. A disadvantage is that the small size and portability of smart sensor

devices can make them vulnerable to being physically stolen, however physical and/or logical template protection measures can be used to protect the references.

A.2.2.5 Portable tokens

The references are stored on a portable device, such as a smartcard with an in-built chip, on which the biometric reference is held. For instance, an ePassport typically holds a biometric reference on an in-built chip. References stored in this manner can be stolen, but normally only individually, and the holder of the portable token has responsibility for its security. Physical and/or logical template protection measures can also be used to protect the references. Biometric reference data stored in this way does not need to be communicated over a network, however each time the reference is used a reference reading device is required.

A.3 Typical biometric applications

Biometric recognition is used in a wide variety of application domains, including:

— access control/security;

— event entry control;

— payment management;

— personalization (e.g. of advertising);

— demographics;

— staff management (e.g. timekeeping).

A.4 Biometric characteristics

A.4.1 Introduction to biometric characteristics

Biometric systems use one or more biometric characteristics to perform recognition – these can be physiological or behavioural and some multi-modal systems use both. Biometric systems can be single modality and use just one biometric characteristic (e.g. only fingerprints) or can be multi-modal and use more than one biometric characteristic.

A.4.2 Biometric characteristics – physiological

Physiological biometric characteristics are based on physical attributes of the human body. Physiological biometric characteristics include:

— retinas;

— fingerprints;

— hand geometry;

— iris;

— faces;

— DNA;

— footprints;

— ear shape;

— sweat pores;

— vein patterns;

— fingernail bed;

— skin luminescence;

— facial thermography;

— body odour.

A.4.3 Biometric characteristics – behavioural

Behavioural biometric characteristics are based on actions performed by a person. Behavioural biometric characteristics include:

— keyboard dynamics;

— voice recognition;

— signature/handwriting dynamics;

— walking gait;

— foot dynamics;

— hand grip;

— brain wave pattern.

A.4.4 Biometric characteristics – attributes

According to ISO/IEC TR 24741, a biometric characteristic should be:

— distinctive: different across all people;

— repeatable: similar across time for each person, over an extended period (several years);

— accessible: easily presented to a sensor (e.g. face to a camera or fingerprint to a scanner);

— universal: observable on all people;

— acceptable: people are prepared to use the biometric characteristic in the given application.

In practice, no biometric characteristic displays all these characteristics. For instance, fingerprints, the most widely used biometric characteristic, is not universal because, for instance, it is not observable on people who have lost fingers, or those who work in manual professions where fingerprints become unreadable (e.g. bricklayers). For this reason, some biometric systems are multi-modal and use multiple characteristics.

Annex B
(informative)

Standards related to the testing of biometric systems

B.1 General

This annex provides a list of biometric standards applicable to the testing of biometric systems, several of which will be useful to a software tester required to test such a system. Although this annex lists some of the most widely used standards for testing biometric systems, it is not a comprehensive list of every standard applicable to the testing of biometric systems and testers are encouraged to identify any other relevant standards, especially those that are mode-specific (e.g. standards that are specific to a particular biometric characteristic, such as fingerprints).

These standards (including technical specifications and technical reports) have been grouped into two subclauses; one subclause that contains standards directly related to testing and evaluating biometric systems, and the following subclause that contains standards on biometrics that are sometimes used to support testing (e.g. defining biometric APIs). Unless otherwise stated, each of the listed standards was developed by the ISO/IEC biometrics subcommittee (SC 37).

B.2 Standards directly covering biometrics and testing

B.2.1 The ISO/IEC 19795 series - Biometrics performance testing and reporting

B.2.1.1 ISO/IEC 19795-1 - Principles and framework

ISO/IEC 19795-1 (newly published in 2021) provides generic guidance on the testing of biometric systems, independent of which biometric characteristics are being used and which of the three biometric evaluation levels for biometric systems are being used.

It defines the fundamental performance metrics (error rates and throughput rates) for biometric systems. It also specifies how biometric systems are tested, covering test planning, test execution, and test reporting.

See Annex E for a detailed overview of ISO/IEC 19795-1.

B.2.1.2 ISO/IEC 19795-2 - Testing methodologies for technology and scenario evaluation (including amendment that expands coverage to multi-modal biometric implementations)

See Annex F for a detailed overview of ISO/IEC 19795-2.

B.2.1.3 ISO/IEC TR 19795-3 - Biometric performance testing and reporting - Modality-specific testing

ISO/IEC TR 19795-3 (unchanged since 2007) is a technical report that provides guidance on the interpretation of the generic guidance on testing provided in ISO/IEC 19795-1 for different biometric modalities (e.g. fingerprints, face images, iris images). It is concerned with how factors related to the subjects (e.g. facial expressions) and the operational environment (e.g. lighting) change by modality and how they can be considered during the testing of biometric systems.

B.2.1.4 ISO/IEC 19795-4 - Biometric performance testing and reporting - Interoperability performance testing

See Annex G for a detailed overview of ISO/IEC 19795-4.

B.2.1.5 ISO/IEC 19795-5 - Biometric performance testing and reporting - Access control scenario and grading scheme

ISO/IEC 19795-5 (published in 2011) provides a framework for the biometric performance testing of biometric systems used as general-purpose access control applications. It specifically covers the definition of requirements for such systems and their test environments. It also defines a grading system for the biometric performance of the tested systems based on a minimum 90 % confidence level.

B.2.1.6 ISO/IEC 19795-6 - Testing methodologies for operational evaluation

See Annex H for a detailed overview of ISO/IEC 19795-6.

B.2.1.7 ISO/IEC 19795-7 - Testing of on-card biometric comparison algorithms

See Annex I for a detailed overview of ISO/IEC 19795-7.

B.2.1.8 ISO/IEC TS 19795-9 - Testing on mobile devices

See Annex J for a detailed overview of ISO/IEC TS 19795-9.

NOTE There is no part 8 in the ISO/IEC 19795 series.

B.2.2 ISO/IEC 21472 - Scenario evaluation methodology for user interaction influence in biometric system performance

ISO/IEC 21472 defines a methodology for testing and reporting how different user interaction factors influence the performance of biometric systems when performing a scenario-level evaluation. Factors considered include the position and condition of the capture system, attributes of the users of the system, and how users interact with the system. ISO/IEC 21472 does not cover usability testing of biometric systems.

ISO/IEC 21472 is referenced by ISO/IEC TS 19795-9, which covers biometric testing on mobile devices (see Annex I for more details).

B.2.3 The ISO/IEC 29109 series - Conformance testing methodology for biometric data interchange formats defined in the ISO/IEC 19794 series

See Annex K for a detailed overview of ISO/IEC 29109-1.

ISO/IEC 29109-2 to ISO/IEC 29109-10 cover specific approaches to conformance testing for different biometric modalities.

B.2.4 ISO/IEC 29120-1 - Machine readable test data for biometric testing and reporting - Part 1: Test reports

ISO/IEC 29120-1, published in 2015, specifies a format for machine readable test documentation. It is intended to support communication of test results and the certification status of biometric systems tested in conformance with the ISO/IEC 19795 series. It specifies machine-readable test report formats recording test results for both technology and scenario evaluation levels.

ISO/IEC 29120-1 does not appear to be referenced from other biometric standards; however it is informatively referenced from ISO/IEC 24761 (a security standard), which defines data structures for checking the validity of test results for biometric systems at remote sites.

B.2.5 ISO/IEC 29197 - Evaluation methodology for environmental influence in biometric system performance

ISO/IEC 29197, published in 2015, provides a methodology for analysing how environmental conditions (e.g. temperature, humidity, illumination, and noise) influence the performance of biometric systems. The methodology considers the biometric system as a whole, and so is pertinent for either scenario or operational level biometric evaluations (see 6.1.2).

ISO/IEC 29197describes a methodology which specifies evaluations that are special cases of the generic scenario evaluations defined in ISO/IEC 19795-2 and the operational evaluations defined in ISO/IEC 19795-6.

B.2.6 ISO/IEC 30136 - Performance testing of biometric template protection schemes

ISO/IEC 30136, published in 2018, is for testing the efficacy of the protection scheme for biometric systems which incorporate biometric template protection. Biometric template protection schemes derive data from an individual's biometric template and only use that derived data for subsequent comparison. The derived data cannot be used to reverse-engineer the biometric template, and so if the biometric system (and the derived data) is compromised, the individual's biometric template data cannot be accessed and reused (perhaps in other biometric systems).

ISO/IEC 30136 specifies metrics for evaluating template protection-based biometric verification and identification systems by evaluating the accuracy, secrecy, and privacy of the biometric template protection system.

B.2.7 ISO/IEC TR 29198 - Characterization and measurement of difficulty for fingerprint databases for technology evaluation

ISO/IEC TR 29198, a technical report published in 2013, provides guidance on predicting the level of difficulty of a fingerprint dataset, based on factors such as relative sample quality, relative rotation, deformation, and overlap between impressions. This guidance can be used for characterizing and measuring the relative difficulty levels of fingerprint datasets used in technology evaluation, especially when comparing biometric systems and components.

B.2.8 ISO/IEC 19792 - Security evaluation of biometrics

ISO/IEC 19792, published in 2009 by the ISO/IEC information security subcommittee (SC 27), covers the security evaluation of biometric systems. It provides generic requirements for the evaluation rather than being focused on a particular certification scheme and is focused on the biometric components of the evaluated system.

ISO/IEC 19792 references ISO/IEC 19795-1.

B.2.9 The ISO/IEC 19989 series - Criteria and methodology for security evaluation of biometric systems

The ISO/IEC 19989 series are developed by the ISO/IEC information security subcommittee (SC 27).

ISO/IEC 19989-1: This framework standard, published in 2020, focuses on the evaluation of biometric recognition and presentation attack detection based on the ISO/IEC 15408 series that provide evaluation criteria for IT security.

ISO/IEC 19989-2 and ISO/IEC 19989-3: These standards, published in 2020, provide detailed recommendations for biometric recognition performance in ISO/IEC 19989-2 and for presentation attack detection in ISO/IEC 19989-3.

ISO/IEC 19792 covers a similar area to the ISO/IEC 19989 series; however, it does not specify the concrete criteria and methodology that are needed for security evaluation based on the ISO/IEC 15408 series.

B.2.10 The ISO/IEC 15408 series - Evaluation criteria for IT security - Parts 1 to 5

The ISO/IEC 15408 series, developed by the ISO/IEC information security subcommittee (SC 27), provides a common set of requirements for the security functionality and for assurance measures applied to all forms of IT products during a security evaluation.

B.2.11 The ISO/IEC 30107 series — Biometric presentation attack detection

The ISO/IEC 30107 series provides recommendations on automated presentation attack detection for biometric systems. ISO/IEC 30107-3, published in 2017, focuses on testing and reporting, while ISO/IEC 30107-4, published in 2020, focuses on the testing of mobile devices.

B.3 Standards supporting biometrics and testing

B.3.1 ISO/IEC TR 24741 - Biometrics — Overview and application

ISO/IEC TR 24741, a technical report published in 2018, replaces the first edition published in 2007. It provides a background to the field of biometrics. It covers the history of biometrics, the architecture of a generic biometric system, the different biometric technologies (e.g. fingerprints, faces), and different application areas for biometrics.

B.3.2 ISO/IEC 2382-37 - Biometrics vocabulary

ISO/IEC 2382-37 provides definitions of the most commonly used terms in biometrics.

B.3.3 The ISO/IEC 19784 series - Biometric application programming interface

ISO/IEC 19784-1, published in 2018, specifies an architectural model which enables components of a biometric system to be provided by different vendors, and to communicate through application programming interfaces (APIs).

ISO/IEC 19784-2, published in 2007, specifies the interface to a function for a biometric archive (database).

ISO/IEC 19784-4, published in 2011, specifies the interface to allow systems to interface to biometric sensors.

NOTE There are only three parts in the ISO/IEC 19784 series.

B.3.4 The ISO/IEC 19794 series - Biometric data interchange formats

ISO/IEC 19794-1, published in 2011, describes requirements for defining biometric data interchange formats in general and covers the definition of content common to all biometric types. Each of the remaining parts of the ISO/IEC 19794 series covers a distinct biometric type.

ISO/IEC 19794-2 to ISO/IEC 19794-15 define data formats for different biometric types (e.g. ISO/IEC 19794-2 covers finger minutiae, ISO/IEC 19794-5 covers face image data and ISO/IEC 19794-6 covers iris image data).

NOTE The ISO/IEC 19794 series are being superseded by the ISO/IEC 39794 series.

B.3.5 The ISO/IEC 39794 series – Extensible biometric data interchange formats

Limitations encountered with the ISO/IEC 19794 series, largely due to advances in technology, have led to the development of what are considered to be more future-proof standards for biometric data interchange formats. To aid the future-proofing, these standards define extensible data interchange formats. The intention is for the new ISO/IEC 39794 series to supersede the ISO/IEC 19794 series.

ISO/IEC 39794-1 (Framework), ISO/IEC 39794-4 (Finger image data), and ISO/IEC 39794-5 (Face image data) were already published by 2020, while the remaining parts were still under development.

B.3.6 The ISO/IEC 24713 series - Biometric profiles for interoperability and data interchange

ISO/IEC 24713-1, published in 2008, provides an overview of biometric systems and biometric profiles (for specific application areas) to support interoperability and data interchange between biometrics systems.

ISO/IEC 24713-2 and ISO/IEC 24713-3, published in 2008 and 2009 respectively, cover physical access control for employees at airports and biometric-based verification and identification of seafarers.

B.3.7 ISO/IEC TR 29196 - Guidance for biometric enrolment

ISO/IEC TR 29196, a technical report published in 2018, provides a set of principles to guide the development of a generic biometric enrolment policy and the deployment of the corresponding service. It is limited to mandatory, attended enrolment at fixed locations.

B.3.8 ISO/IEC TR 30117 - Guide to on-card biometric comparison standards and applications

ISO/IEC TR 30117, a technical report published in 2014, provides a guide to the numerous standards and technical reports applicable when developing on-card biometric systems, relating them to the kind of application being developed.

B.3.9 The ISO/IEC 30137 series - Use of biometrics in video surveillance systems

The recent ISO/IEC 30137 series (so far just parts 1 and 4) provides guidance on the use of biometrics using video surveillance systems, and procedures for establishing ground truth and annotating video data for testing.

NOTE ISO/IEC 30137-2, a standard on performance testing and reporting for biometric video surveillance systems, was not published as the project was deleted.

B.3.10 The ISO/IEC 17839 series - Biometric System-on-Card

The ISO/IEC 17839 series covers requirements for the development of biometric systems on cards. Unlike ISO/IEC 19795-7, these standards are not limited to the comparison algorithm, but cover a complete biometric system (biometric acquisition, data processing, storage, comparison, and decision).

ISO/IEC 17839-1, published in 2014, covers the core requirements.

ISO/IEC 17839-2, published in 2015, covers the physical characteristics.

ISO/IEC 17839-3, published in 2016, covers the logical information interchange mechanism.

B.3.11 ISO/IEC 24761 - Authentication context for biometrics

ISO/IEC 24761, published in 2019 by the ISO/IEC information security subcommittee (SC 27), defines a mechanism for checking that a biometric verification process executed at a remote site is trustworthy.

B.3.12 The ISO/IEC 15408 series - Evaluation criteria for IT security

The ISO/IEC 15408 series, published by the ISO/IEC information security subcommittee (SC 27), provides a common set of requirements for the security functionality and for assurance measures applied to all forms of IT products during a security evaluation.

B.3.13 ISO/IEC TR 30125 - Biometrics used with mobile devices

ISO/IEC TR 30125, a technical report published in 2016, covers the use of biometrics for making secure transactions from mobile devices.

B.3.14 ISO/IEC TR 29156 - Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics

ISO/IEC TR 29156, a technical report published in 2015, covers the specification of biometric performance targets considering both usability and security. It considers the effect on the overall system of the use of additional non-biometric authentication approaches, such as passwords and physical tokens. It also uses the trade-off between usability and security when selecting passwords (i.e. long passwords provide higher security but are difficult to remember and so provide decreased usability) as a reference for making similar decisions about biometric systems.

It is informatively referenced from ISO/IEC 19989-2 (security evaluation of biometric systems), which uses it in the context of selecting FAR values.

B.3.15 ISO/IEC TR 29195 - Traveller processes for biometric recognition in automated border control systems

ISO/IEC TR 29195, a technical report published in 2015, recommends best practices for automated border control systems, which can be manned or fully automated. It is based on the use of ePassports (or similar) and provides guidance at two levels; generic guidance for all biometric modalities and specific guidance for specific modalities and technologies.

ISO/IEC TR 29195 does not appear to be referenced from other standards.

B.3.16 ISO/IEC 7501-1 - Machine readable travel documents — Part 1: Machine readable passport

ISO/IEC 7501-1, published in 2008, was prepared by the International Civil Aviation Organization (as ICAO Doc 9303, Part 1, sixth edition) and fast-tracked to become an ISO/IEC standard.

ISO/IEC 7501-1 specifies the format for a machine-readable passport (MRP), where holder details are presented in both visual and machine-readable formats. It also specifies the format of the electronic versions of such passports (ePassports), which include additional biometric data.

Annex C
(informative)

Generic risks in biometric systems

C.1 Introduction to generic risks for biometric systems

Testing in conformance with ISO/IEC/IEEE 29119-2 (on test processes) and ISO/IEC/IEEE 29119-3 (on test documentation) requires the use of risk-based testing (RBT). RBT requires the identification, assessment, and treatment of risks, where appropriate.

This annex provides checklists of potential risks for biometric systems, along with typical treatments that can be implemented by software testing. Other treatments are possible and more effective in some situations and the list of risks is not intended to be exhaustive. The treatments by software testing would form the basis of a conformant software test strategy that would be part of the test plan. The selection of treatments for implementation depends on the situation, and on the risk exposure assigned to the risk.

NOTE Some of the suggested risks and/or treatments are not the responsibility of the software testing function in an organization. In such cases, the relevant stakeholders are responsible for these risks and/or treatments.

The tester of a biometric system will need to 'tailor' the checklists based on the biometric characteristics (e.g. fingerprints, facial features, voice) being used by the biometric system they are testing.

The risks are broken into two main categories; project risks and product risks, as described in 5.6.2.

The project risks are covered in C.2 and the product risks are covered in C.3.

C.2 Biometric system project risks and treatments

C.2.1 General

The biometric system project risks have been divided into several sub-categories for ease of documentation. Other categorisations are equally valid.

C.2.2 Generic biometric system project risks

The biometric system project risks and treatments covered in this clause are described in Table C.1 and are listed in the following order:

— Project management risks

— Product-related project risks

— Customer risks

— Security and privacy risks

— External risks

— Requirements risks

— Development risks

— Testing risks – Organizational-related risks

— Testing risks – Development-related risks
— Testing risks – Test team-related risks
— Testing risks – Environment/Tools-related risks
— Testing risks – Acceptance-related risks
— Testing risks – Representativeness risks – template
— Testing risks – Representativeness risks - test subjects
— Testing risks – Representativeness risks – biometric processes

Table C.1 — Generic biometric system project risks and possible treatments

Generic biometric system project risks	Possible treatments by software testing
Project management risks	
It is possible the project manager is missing or lacking in expertise	If there is no project manager, appoint a test manager to take responsibility for both project management and test management.
It is possible the project manager is unfamiliar with biometric systems	Appoint a test manager who is familiar with biometric systems.
It is possible the project manager underestimates the resources required for adequate testing of a biometric system	Agree risks and minimum levels of treatment by testing to include in the test strategy. Provide test plans with clear estimates to perform the activities described in the test strategy. Highlight the risks with the project manager that are not treated if inadequate resources are provided for testing – and record this information.
It is possible the project goals and objectives are not clearly stated	Review the relevant project document (e.g. project initiation document) to ensure the project goals and objectives are clearly stated and feasible.
It is possible the project is following a life cycle they are not familiar with (e.g. agile, DevOps)	Ensure the test manager is familiar with the project life cycle and that the test team includes some team members who have experience of it.
It is possible the project schedule is not clearly specified	Review the project schedule (or equivalent) for clarity.
It is possible the project schedule is optimistic (rather than realistic)	Review the project schedule (or equivalent) and decide whether the required testing can be performed within this schedule (this is determined from a knowledge of the perceived risks).
It is possible the project schedule omits some necessary testing activities	Review the project schedule (or equivalent) to ensure the full set of necessary testing activities (these are determined from a knowledge of the perceived risks) are included.
It is possible re-estimation based on project slips does not consider the project's history (e.g. these slips recur)	Review updated project estimates to ensure they take account of previous events in the project, especially in the area of software testing.
It is possible the change control procedures for the software/system are lacking/missing/poorly implemented	Review the change control procedures for the project to confirm that they are adequately documented and complete. Perform audits to check that the change control procedures are correctly applied.
It is possible contracts with 3rd-parties do not match project schedules	Review project inputs from third-party suppliers to ensure that the required testing fits within the overall project schedule.
Product-related project risks	
It is possible the project is to replace an existing biometric system	Testers make themselves aware of the deficiencies in the replaced biometric system to use as a basis for generating test cases. Testers make themselves aware of existing system characteristics as these can be used as minimal benchmarks for the new biometric system.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
It is possible the project is to update to an existing biometric system	Testers make themselves aware of the deficiencies in the current biometric system to use as a basis for generating test cases. Testers make themselves aware of existing system characteristics as these can be used as minimal benchmarks for the updated biometric system.
It is possible the project is a new development (rather than an update to an existing biometric system)	Review the required quality characteristics and confirm the requirements in this area are understood, testable, and clearly documented.
It is possible the technology to be implemented is new and/or complex	Testers identify those parts of the system that are new/complex and focus relatively more testing in these areas.
It is possible the biometric system will be implemented on multiple platforms	Test environments capable of simulating each platform are obtained for testing.
It is possible the biometric system will interface with multiple other systems	System integration testing is performed for the biometric system and the other systems it communicates with.
It is possible the biometric system will be implemented with biometric data stored on workstations	If the biometric data is stored on a workstation, then readers are required to allow the template to be read from the token/smartcard each time authentication takes place. This typically increases the cost of the biometric system as workstations are required at each authentication location. A test method, corresponding test suite and test environment for testing each workstation can be developed.
It is possible the biometric system will be implemented with biometric data stored on tokens or smartcards	If the biometric data is stored on a token/smartcard, then readers are required to allow the template to be read from the token/smartcard each time authentication takes place. This typically increases the cost of the biometric system as token/smartcard readers are required at each authentication location. A test method, corresponding test suite and test environment for testing each individual token/smartcard reader can be developed.
Customer risks	
It is possible the customer will frequently change their stated needs	Ensure contingency is included in the test plan to cope with the possibility of changes to planned testing due to changes in the customer requirements.
It is possible unrealistic performance metrics are set by the customer	Review the performance metrics set by the customer and confirm their testability.
It is possible customers overrate the effectiveness of the system	Ensure that reports on the effectiveness of the system based on test results that are visible to the customer are clearly stated in a form understandable by the customer.
It is possible the time taken to review planned testing by the customer and users is longer than expected	Ensure contingency is included in the time assigned for test planning to cope with the possibility of delays in receiving feedback from customers and users.
It is possible the customer is unaware of the importance of testing	Be ready to explain the importance of testing biometric systems from the perspective of a customer, focusing on the risks of putting an insufficiently tested biometric system into production.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
It is possible project stakeholders have a lack of familiarity with the customer organization	Prefer using testers with familiarity with the customer organization (all other things being equal).
It is possible decision making by the customer is slow	Ensure contingency is included in the test plan to cope with the possibility of testing being delayed due to waiting for customers to make decisions.
It is possible the customer representative (or domain experts) with authority to make decisions are not clearly identified	Identify those stakeholders with the authority to make decisions about the software testing as early as possible.
It is possible the project schedule is not agreed with the customer	Include the customer as an approval authority for the test plan.
It is possible the delivery date is brought forward by the customer for commercial reasons	Explicitly use a risk-based approach to the testing in the test plan, so that any cuts to the planned testing can be clearly understood in terms of increased risks to the customer.
Security and privacy risks	
It is possible processes for managing biometric data used during development and testing do not meet regulatory requirements (e.g. GDPR)	Identify any regulatory requirements that apply to the test data used for testing the biometric system. Ensure the planned management of test data meets all identified regulatory requirements and the test data are managed correctly.
It is possible the permitted uses of biometric data (e.g. only for access control, not for tracking work times) are unclear	Ensure all biometric data used for testing is being used within the relevant regulations (e.g. all test subjects who provide biometric data have agreed to this).
It is possible data on test subjects are destroyed and so test subjects are reused resulting in biased test results	Ensure that records of test subjects who take part in testing are retained long enough to prevent unexpected multiple use of the same test subjects.
It is possible privacy standards change during the course of the project	Maintain awareness of the current privacy standards that apply to the biometric system.
It is possible system designers act maliciously	Review the architecture and design of the biometric system using a relevant security checklist, ideally focused on biometric systems design.
It is possible system programmers act maliciously	Review the code of the biometric system using a relevant security checklist, ideally focused on biometric systems coding.
It is possible system operators act maliciously	Review the operator processes for the biometric system using a relevant security checklist, ideally focused on biometric systems operations.
External risks	
It is possible third-party suppliers fail to fulfil their contracts	Include contingency in the test plan to cope with the possibility that planned testing of third-party software can be delayed or changed.
It is possible relevant standards are missing or unstable	Identify any new standards that are likely to become relevant and any relevant standards that are likely to change where these can affect the planned testing and include contingency in the test plan to cope with these possibilities.
It is possible government regulations change unexpectedly	Identify any areas where government regulations in the area of biometrics are likely to change and include contingency in the test plan to cope with this possibility.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
Requirements risks	
It is possible requirements for the expected template quality are missing or unclear	Review the template quality requirements to confirm they match those expected by the developers of the biometric system.
It is possible specifications for third-party subsystems are missing or lacking	Attempt to replace or supplement the specifications with knowledge about how the third-party subsystems are expected to behave. Use testing techniques that are more appropriate for when detailed specifications are not available, such as exploratory testing.
It is possible requirements specifications do not specify all the required functions/features	Attempt to replace or supplement the specifications with knowledge about how the system is expected to behave. Use testing techniques that are more appropriate for when detailed specifications are not available, such as exploratory testing.
It is possible acceptance criteria are not clearly specified	Work with the relevant stakeholders, such as the customer and users, to agree a clear set of acceptance criteria.
It is possible non-functional requirements are not described in sufficient detail, if at all	Attempt to replace or supplement the specifications with knowledge about how the system is expected to behave. This can be by asking relevant stakeholders for these non-functional requirements, or it can be by getting the customer to agree to proposed non-functional requirements based on similar systems. Use testing techniques that are more appropriate for when detailed specifications are not available, such as exploratory testing.
It is possible the requirements scope changes (typically increases)	Ensure contingency is included in the test plan to cope with the possibility of changes to planned testing due to an increase in the scope of system requirements.
Development risks	
It is possible the use of machine learning to train the biometric system introduces specific challenges for the testing	Consider using the guidelines for testing AI-based systems (of which machine learning is an example) described in ISO/IEC TR 29119-11.
It is possible the costs to build the initial system are too high	Clearly cost the testing in the test plan on a feature-by-feature basis, so that if any changes in project scope are suggested to save money, valid estimates can be provided for the resultant change in testing costs. Explicitly use a risk-based approach to the testing in the test plan, so that any cuts to the planned testing can be clearly understood in terms of increased risks to the customer.
It is possible system maintenance costs are too high	Create a maintenance test plan to cover the testing necessary after the biometric system is released into production that includes estimates of testing costs for each of the different testing types and the risks the tests are treating. In this way, any initiative to save overall system maintenance costs can be informed of the risks of cutting back on specific types of testing.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
It is possible the system delivery date is not met	Explicitly use a risk-based approach to the testing in the test plan, so that any cuts to the planned testing to bring forward the delivery date can be clearly understood in terms of increased risks to the customer.
It is possible some components contribute more to the overall technical performance than others	Explicitly use a risk-based approach to the testing, so that those components that are considered more important in the event they are not working can be assigned a higher level of risk and so tested more rigorously.
It is possible development standards are missing, lacking in quality or poorly implemented	Consider whether the quality of the developed code is likely to be affected by the implementation of development standards and, if so, assign higher probability to the likelihood of failure of developed code than if the development standards were considered stable and well-implemented.
It is possible hardware is not available to support integration testing	Consider using a simulator for the missing hardware during integration testing. Depending on the commonality of the hardware, a commercial simulator can be acquired, or a simulator can be developed for this project.
It is possible the system design is not fully consistent with the specified requirements	Review the architecture and designs for consistency with the requirements.
It is possible design quality is lower than expected	Review the architecture and designs ahead of code implementation. Checklists focused on software system design quality are often used to support this.
It is possible the quality of the delivered code is low, so requiring more fixing than planned	Perform code reviews, before accepting code into builds for testing. Code checklists for specific programming languages are often used to support this.
It is possible the quality of third-party components is lower than expected	Assign an initial higher likelihood of failure to third-party components so that they are tested more rigorously than otherwise. If test results do not indicate that third-party components are lower quality than expected, re-evaluate their likelihood of failure.
It is possible the delivery of 3rd-party components is later than expected	Include contingency in the test schedule in the test plan to allow for the late delivery of third-party components. Where this is not possible, consider using simulators for components that are delivered late – or consider sourcing these components from other suppliers or developing them internally.
It is possible third-party software is not fully accessible (e.g. for white-box testing)	Where white-box testing is not possible, consider replacing it with rigorous black-box testing that will provide a similar level of confidence in the software. If black-box testing to a suitable level is not possible, consider suggesting that the third-party software is replaced. Alternatively, request the supplier of the third-party software to provide evidence that it has been tested to a suitable level of confidence.
It is possible the quality of defect reports (e.g. from testers, users, etc.) make it difficult for developers to reproduce defects	Ensure the defect management system requires all relevant fields to be completed. Make examples of good defect reports available and provide training in defect reporting, if necessary.
It is possible version control tools are missing or lacking quality	Use industry standard version control tools (high quality open-source tools are available in this area).

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
It is possible developers are slow to implement defect fixes	Assign all defects with a priority so that developers are aware of which fixes need to be made first. Ensure sufficient developer resources are assigned to defect fixing when it needs to run concurrently with new development.
Testing risks – Organizational-related risks	
It is possible the test organization is poorly defined	Define a formal structure for the testing within the organization.
It is possible the organizational test practices are missing, lacking in quality or poorly implemented	Define organizational test practices and manage their implementation.
It is possible the testers assigned to the biometric project are assigned to multiple projects and with unclear priorities	Ideally assign testers to work on one project at a time. Where this is not possible (e.g. due to their specialist knowledge being needed on multiple projects), clearly define the expected proportion of time to be spent on each project and agree the relative priorities of the projects.
It is possible testers do not have access to the project risk register	Provide testers with access to the risk register (or equivalent). Where this is not possible directly, arrange with the project manager to allow testers access to the project risk information.
It is possible the test manager's relationship with the project manager needs improvement	Align the test plan with the project plan, where possible. When alignment is not possible (e.g. due to insufficient time allocated for testing), provide options for reducing the amount of testing, supported by a clear explanation of how such reductions increase risks.
It is possible the estimates for testing are inaccurate	Use a mix of metrics-based and expert-based estimation to derive the initial estimates for the testing of the biometric system. Include the requirement in the test plan to gather metrics on resources spent and to analyse how closely estimates match resources used. This allows estimates to be improved as the project progresses and treatments employed earlier if estimates are seen to be wrong.
It is possible frequent maintenance testing is not planned or not implemented	Use a risk-based approach to identify the requirements for maintenance testing (testing after the biometric system has been released to production) and clearly document the planned testing in a maintenance test plan.
It is possible testers do not communicate the state of testing to other stakeholders in a satisfactory manner	Base the form and content of test reports on the user of the report. Do not include unnecessary details and present the needed information as clearly and concisely as possible.
It is possible the infrastructure to support the testers is not available	Ensure support infrastructure for testers (e.g. computers, offices, desks) is available as soon as testers start work on the project.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
Testing risks – Development-related risks	
It is possible developers are not willing to provide technology support to the testers	Employ testers who are familiar with biometric technology. Liaise closely with the development manager and developers to build a rapport that encourages knowledge sharing (e.g. support developers with unit testing).
It is possible developers do not deliver software/systems for testing as planned	Agree with the developers when test items are to be made available for testing. Share test schedules, which show when testing of developer-provided test items is planned to occur. Include contingency in the test schedule in the test plan in case developers deliver test items later than planned. Where this is not possible, consider using simulators for components that are delivered late – or consider sourcing these components from third-party suppliers.
It is possible the test manager's relationship with the development manager needs improvement	Provide constructive feedback on the development plan. Align the test plan with the development plan, where possible, and otherwise liaise to come to an agreement. Agree expectations on the defect reporting, fixing, and re-testing process between testers and developers.
It is possible the quality of the delivered code is low, so requiring more re-testing than planned	Provide guidance on unit testing to developers, to assist them in improving the quality of delivered code. Include code reviews to identify defects as early as possible. Ensure test cases are well-documented and saved so that they are easily retrievable and reusable during re-testing. Include contingency in the test plan to allow more test cycles (test-fix-retest), if necessary.
It is possible testers are not allocated to review requirements and design specifications	Strongly advocate that testers are included in the reviews of early lifecycle artefacts, such as requirements and design specifications. Explain that testers will provide an independent perspective and direct input on testability.
It is possible the complexity of the system design makes fault detection excessively expensive	Explain the balance between design complexity and testability (and testing costs) early in the life cycle (e.g. as part of design reviews), where this is relevant.
It is possible some components are more error-prone than others	Include measurement and analysis of defect metrics in the test plan so that error-prone components can be identified and their risk level increased due to a raised likelihood of failure.
Testing risks – Test team-related risks	
It is possible the test lead/manager is missing or lacking experience	Appoint a test manager/lead with sufficient test management experience.
It is possible the test lead/manager has little or no experience in biometrics	Appoint a test manager/lead with experience working on the testing of biometric systems or provide them with support from senior testers with this experience.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
It is possible the organization do not have suitable testers available	Employ testers with suitable skills and experience, either on a permanent or contract basis.
It is possible the testers do not have access to experts in biometrics	Encourage testers to talk to the system designers and users of the biometric system, to gain insight into how the system is expected to work (and previous systems worked). Provide testers with the opportunity to learn more about biometrics, such as through training, attending conferences, or, as a minimum, support them by providing time for self-learning in this area.
It is possible the assigned testers are inexperienced in biometrics	Employ testers with suitable skills and experience in biometrics, either on a permanent or contract basis to replace or supplement the assigned (inexperienced) testers. Train assigned testers in the area of biometrics.
It is possible that training on biometrics is not available for testers	Provide testers with the opportunity to learn more about biometrics through attending conferences and support them by providing time for self-learning in this area.
It is possible there is insufficient time to train testers in biometrics	Employ new testers with experience in biometrics, either on a permanent or contract basis.
It is possible the assigned testers are inexperienced in testing	Employ experienced testers, either on a permanent or contract basis to replace or supplement the assigned (inexperienced) testers.
It is possible the assigned testers become ill, or unavailable for some other reason	Include contingency in the test plan in the area of resourcing testers, so that there are still sufficient testers if some become unavailable part way through the project. Encourage testers to work together (such as in pairs) so that experienced testers share their knowledge with less experienced colleagues.
Testing risks – Environment/Tools-related risks	
It is possible the assigned testers are inexperienced in using the test tools	Employ testers with suitable skills and experience in test automation, either on a permanent or contract basis to replace or supplement the assigned (inexperienced) testers. Train assigned testers in the area of test automation.
It is possible the test tools were not selected based purely on technical merit	Determine the suitability of the selected test tools and identify any gaps in test tool coverage.
It is possible the test tools will not be available on time	Include test tool acquisition as an early activity in the test plan. Use a risk-based approach to ensure the most important test tools are available.
It is possible the test tools are ineffective	Monitor the effectiveness of the test tools being used on the project and be prepared to acquire new test tools to replace any that are found to be ineffective or where new tools would provide a significant improvement.
It is possible the test environments are not ready on time	Include test environment requirements definition and set-up as an early activity in the test plan.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
It is possible the testers do not have ready access to representative test environments (including back-up and disaster recovery sites)	Where representative test environments are not available investigate the possibility of scaling test results from less representative environments or using simulators to make the test environments more representative. Liaise with operations staff to determine the availability of using operational environments for testing where using a test environment close to the operational environment is important.
It is possible the testers are not responsible for managing the test environments	Where test environments are managed separately, form a close relationship with those setting up and maintaining the test environments. Ensure that test environment requirements are provided as early as possible and in sufficient detail.
It is possible that hardware is not available for system integration testing	Include contingency in the test schedule in the test plan to allow for the late delivery of hardware. Where this is not possible, consider using simulators for hardware components that are delivered late – or consider sourcing these components from other suppliers.
It is possible the sensor types/makes used for testing do not match the operational system sensor types/makes	Include contingency in the test schedule in the test plan to allow for additional testing of the sensors once the system is moved to the operational environment. Review the differences between the sensors used in the test environment and the sensors in the operational environment to identify any differences which are likely to need addressing. Consider building simulators of the sensors to be used in the operational system to support the testing, where the differences between sensors available for testing and the sensors in the operational environment differ significantly.
It is possible the high cleanliness of sensors used for testing does not match the relatively poor operational system sensor cleanliness	Run tests with sensors that have been artificially dirtied to make their level of dirtiness similar to that of sensors used in operational biometric systems.
It is possible the new sensors used for testing do not match the ages of operational system sensors after the system has been operational for some time	Identify how sensor performance deteriorates over time and consider building simulators of older sensors to support the testing, where the differences in performance between new and old sensors is considered to be significant. Alternatively, source old sensors of the correct make and type for inclusion as part of the test environment.
It is possible the number and positioning of sensors used for testing do not match the operational system number and positioning	Design a test strategy where the results of the testing performed on the test environment can be used to infer the performance in the different, operational environment. Consider building a test environment that more closely matches the operational environment, using simulators for missing sensors, where needed.
Testing risks – Acceptance-related risks	
It is possible there is no clarity on who approves acceptance tests	Identify those stakeholders, such as customers or their representatives, responsible for approving acceptance tests. Liaise closely with these stakeholders when preparing the acceptance tests.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
It is possible that feedback from acceptance testing results in major rework	As far as possible, schedule tests that have the potential to shed light on problems that result in the need for major rework as early as possible in the life cycle.
It is possible customers/users do not make themselves available to support acceptance testing	Liaise closely with those stakeholders responsible for supporting acceptance testing to encourage them to take part in acceptance tests. Where there is doubt over their availability, consider asking the project manager to persuade them to attend, consider identifying other suitable stakeholders, and add contingency to the test schedule to allow more times to be made available.
Testing risks – Representativeness risks - template	
It is possible that a profile representing the range of template qualities that are used operationally (e.g. the range of qualities of face templates in passports or the range of qualities of fingerprints stored in mobile phones) is not available	It is sometimes necessary to derive the profile of template qualities by analysing a statistically significant sample of templates that are being used operationally. Where the users consider these to be private, this can be more of a challenge.
It is possible the quality of templates used for testing do not match operational template quality	The quality of the templates used for testing will ideally be based on a known profile of template qualities for the type of system being tested.
It is possible the ages of templates used for testing do not match operational template ages	The ages of the templates used for testing are based on a known profile of template ages for the type of system being tested (e.g. most adult passports are valid for 10 years and so testing of biometric systems based on passports will ideally use a range of passport ages between 0 and 10 years).
Testing risks – Representativeness risks - test subjects	
It is possible the profile of users of the operational system is not available	Knowledgeable stakeholders (e.g. customer) are used to derive a profile of expected users of the biometric system. Where the biometric system is replacing an existing system, then it is possible to derive the profile from transaction data and logs held by the existing system. If the system is similar to another biometric system, then it is possible to derive the profile from observation of users of the other system.
It is possible the test subjects used for testing do not match the people expected to use the system (e.g. number, age, physically, intelligence, race, gender, etc.)	A profile of the typical users of the biometric system are used to generate the test subjects for the testing of the system. For instance, a biometric system used to control access toa sports venue includes subjects of different ages, both genders, different races, etc.
It is possible the testers do not know how the biometric system will be used operationally	The testers talk to knowledgeable stakeholders (e.g. customer) and analyse available documentation on the new system to determine how it is likely to be used. Where these conversations and documentation do not completely satisfactorily answer the question, observation of other similar systems can provide insights into the expected use of the new system.
It is possible the test subjects behave differently to the people expected to use the system (e.g. more relaxed, more familiar with system, not so sleepy with jetlag)	Tests that can be affected by the test subjects' behaviour are performed using test subjects that are expected to behave as closely as possible to the operational subjects of the biometric system. For instance, it would not be appropriate to test for throughput with test subjects who had used the biometric system several times earlier in the day when the biometric system is only expected to be used by real subjects once per year on average.

Table C.1 *(continued)*

Generic biometric system project risks	Possible treatments by software testing
It is possible there are insufficient test subjects to provide statistically significant results from the testing	The number of test subjects used for testing will affect how accurately the performance of the biometric system is measured. ISO/IEC 19795-1 provides guidance on the number of test subjects to be used for testing.
Testing risks – Representativeness risks – biometric processes	
It is possible the enrolment process used for testing is not the same as that used operationally	The testers talk to knowledgeable stakeholders (e.g. customer, existing operators) and analyse available documentation on the new system to determine how enrolment is likely to be performed. Where these conversations and documentation do not completely satisfactorily answer the question, observation of other similar systems can provide insights into the expected use of the new system. Ideally the enrolment process used for testing will match the expected enrolment process for the operational biometric system as closely as possible.
It is possible the recognition process used for testing is not the same as that used operationally	The testers talk to knowledgeable stakeholders (e.g. customer, existing operators) and analyse available documentation on the new system to determine how recognition is likely to be performed. Where these conversations and documentation do not completely satisfactorily answer the question, observation of other similar systems can provide insights into the expected use of the new system. Ideally the recognition process used for testing will match the expected recognition process for the operational biometric system as closely as possible.

C.3 Biometric system product risks and treatments

C.3.1 General

The biometric system product risks are divided into several sub-categories for ease of documentation. The quality characteristics from ISO/IEC 25010 have been used to create several of the categories, and performance metrics, standards, and operational risk categories have also been identified. Other categorisations are equally valid.

Risks can be adversarial (e.g. from hackers) or non-adversarial (mistakes, system failures, natural disasters). The adversarial risks are most likely to be listed under security risks.

C.3.2 Generic biometric system product risks

The biometric system product risks and treatments covered in this clause are described in Table C.2 and are listed in the following order:

— Functionality – sensor risks

— Functionality - feature extraction risks

— Functionality - repository risks

— Functionality - matcher risks

— Functionality - network risks

— Functionality - performance metrics risks

— Usability risks – documentation

— Usability risks - appropriateness recognizability risks

— Usability risks - learnability risks

— Usability risks - operability risks

— Usability risks - user error protection risks

— Usability risks - user interface aesthetics risks

— Usability risks - accessibility risks

— Portability risks

— Reliability risks

— Maintainability risks

— Compatibility risks

— Performance efficiency risks

— Standards-related risks

— Security risks – attack vulnerabilities

— Security risks – vulnerabilities (accidental)

— Security risks – system access

— Security risks – sensors

— Privacy risks

— Operational risks – training
— Operational risks – support
— Operational risks - incidents/defects
— Operational risks – sensors
— Operational risks – enrolment
— Operational risks – recognition
— Operational risks – operation
— Operational risks – recovery
— Operational risks - install/update

Table C.2 — Generic biometric system product risks and possible treatments

Generic biometric system product risks	Possible treatments by software testing
Functionality – sensor risks	
It is possible the sensor interface does not meet the specification	Perform interoperability testing based on the specified interface standard for the sensor. Typically set up a test device using the specified interface protocol and check that it communicates correctly with the sensor. This will require checking that command and reply messages are correctly communicated and match the specified protocol.
It is possible the transformation from analogue input to a digital representation causes a loss in feature detail that makes differentiating between subjects difficult	This level of testing is typically outside the scope of biometric system testing but can be performed using a back-to-back testing approach with a corresponding (and more accurate) digital-to-analogue converter (DAC).
It is possible sensors are sensitive to small changes in the operational environment	The required sensor accuracy is specified and can be measured through testing against more accurate test equipment. Where changes in the operational environment occur (e.g. temperature or lighting changes) it can be necessary to recalibrate sensors and then test that the resultant accuracy is within defined and expected tolerances.
It is possible non-genuine sensors are installed as part of the system	Audit of actual sensors, or sales invoices for the sensors.
It is possible there is insufficient sensor storage space to store the gathered sensor data	Performance testing at maximum specified load for those sensors that store data.
It is possible the system accepts duplicate sample data from sensors (when ideal data will contain no duplicates in practice)	One way of spoofing biometric systems is to present recorded subject samples to the system. One means of detecting this is for the system to compare new samples with previously presented samples and reject any that are identical as this suggests they are not from a real subject (in practice, for most sensors each sample is different, even when collected from the same subject). When this mechanism of rejecting identical samples is implemented in a biometric system, ideally test cases do not include identical samples that can be rejected by the system.
It is possible the chosen sensors are prone to getting dirty (e.g. due to residual characteristics)	Testing of sensors at various levels of 'dirtiness' are performed to determine the effect on the performance of the biometric system. The results of these tests are used to inform the required frequency of cleaning of operational sensors. Testing (through reviews or dynamic checking) of the procedures for maintaining sensors is performed to ensure the procedures include the necessary level of sensor cleaning. Tests of sensors in the operational biometric system are also performed to ensure the procedures for the cleaning of sensors are being followed.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
Functionality - feature extraction risks	
It is possible the system requires several samples to be presented to provide sufficient information for a single feature (e.g. side of finger, front of finger, etc.)	Testing uses a boundary value approach and test that the specified feature information can be captured using the minimum number of attempts at presenting samples and also check that it is not possible to exceed the maximum number of attempts at presenting samples. Usability testing can be used to ensure subjects are provided with sufficient guidance on how to present multiple samples by the biometric system.
It is possible that feature extraction results in a template from which it is possible to reverse-engineer the raw biometric for the subject	Ideally feature extraction is one-way so that raw biometric data cannot be reconstructed from the extracted feature, so patterns in the template will not be traceable to the raw data. Negative testing based on attempting to reverse engineer the raw biometric from templates is performed.
It is possible there is insufficient system memory to store the required sample data	A form of performance testing, focused on memory usage, is used to ensure that sufficient memory is available to store a full set of samples for feature extraction. This can be particularly relevant when multiple samples are collected to derive the information for a single feature.
It is possible there is insufficient system storage space to store the required feature data	A form of performance testing, focused on memory usage, is used to ensure that sufficient memory is available to store a full set of feature data before it is passed to the matcher algorithm. This can be particularly relevant for a multi-modal biometric system, where multiple features are used.
It is possible signal noise causes a loss in feature detail that makes differentiating between subjects difficult	Noise can be generated in several ways, such as poor contact between the subject and the sensor, heat generated by the biometric system, and static electricity. The signal noise is filtered, so testing of the noise filter can be performed with different noise levels.
It is possible the detail required in templates is set too low	This can occur when the template standards were set some time previously and have not been updated, or new versions of standards have not been adopted. Review of the minimum template specification will identify if this is a design problem.
It is possible enrolled templates are of too low quality	This can occur when a 3rd party is responsible for the enrolment of templates. Where enrolled templates are below the minimum specification this will be identified by the system and can be tested using a form of boundary value analysis based around the minimum specification of the template.
Functionality - repository risks	
It is possible biometric template data is not stored for long enough for some uses	Where there are privacy concerns, template ageing, or memory concerns the biometric system is set up to delete templates from the biometric repository after a period of disuse. Boundary value analysis around the boundary of the upper limit for storing a template without using it can be performed.
It is possible biometric feature (non-template) data is not stored for long enough for some uses	In the event of network outages, it can be necessary for extracted features to be stored temporarily until the network resumes so that the features can be stored as a template in the repository. The need for the system to work under such conditions can be specified as part of interoperability, availability, or fault tolerance. Testing this scenario can be performed using fault injection testing, where the network failure was injected as the fault.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible there is insufficient storage space in the enrolment database	Performance (capacity) testing can be used to determine if the specified biometrics enrolment database is large enough to hold the maximum expected number of biometric templates. Stress testing can be used to determine the maximum number of references that can be stored.
It is possible biometric data is stored on a workstation	If biometric data is stored on a workstation, it means the template must be read from the workstation each time authentication takes place and, typically, in multiple locations. Each of the workstations can need to be tested to ensure any sensor, feature extraction or security risks are treated.
It is possible biometric data is stored on a token or smartcard	If biometric data is stored on a token/smartcard, it means the template must be read from the token/smartcard each time authentication takes place and, typically, in multiple locations. Each of the workstations can need to be tested to ensure any sensor, feature extraction or security risks are treated.
Functionality - matcher risks	
It is possible a poor choice of matching algorithm adversely affects system performance	Typically tested along with the decision algorithm to determine if biometric performance metrics (e.g. false match, false non-match) are achieved.
Functionality - network risks	
It is possible network bandwidth issues cause overall system performance to degrade	Performance testing based on specified operational profiles can be performed, initially with the specified network bandwidth and then with compromised levels of bandwidth to determine the effect on performance (e.g. response times and throughput rates).
It is possible encryption and decryption cause a loss in template integrity	Encryption and decryption can be tested together as one function is the reverse of the other. Random messages can be encrypted and then decrypted, and the only effort is in comparing that the decrypted message is the same as the random encrypted message. Note that this will not ensure that the encrypted message is secure – that is covered as a security risk. Several standards cover the requirements and testing of cryptographic modules: — ISO/IEC 19790 defines the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems — ISO/IEC 24759 specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790. — ISO/IEC TS 20540 provides recommendations and checklists which can be used to support the specification and operational testing of cryptographic modules in their operational environment within an organization's security system.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible compression and decompression cause a loss in template integrity	Compression and decompression can be tested together as one function is the reverse of the other. Random messages can be compressed and then decompressed, and the only effort is in checking that the decompressed message is the same as the random compressed message.
Functionality - performance metrics risks	
It is possible performance requirements are not met - false match rate, false non-match rate, etc.	ISO/IEC 19795-2 can be used to inform this testing.
It is possible performance requirements are not achieved due to a reliance on using a single feature	ISO/IEC 19795-2 can be used to inform this testing.
It is possible the selected feature is too similar in different subjects to meet the performance requirements for the system	ISO/IEC 19795-2 can be used to inform this testing.
It is possible performance requirements are not achieved if subjects' features change too much (e.g. due to age)	ISO/IEC 19795-2 can be used to inform this testing. Use boundary value analysis to test the system with subjects at the specified limits of feature change (e.g. using passports that have a biometric image that is 12 years old – assuming that a 2-year-old image was used to register a passport with a 10-year life).
It is possible signal noise (e.g. due to lighting, background noise) was not considered when predicting expected performance	ISO/IEC 19795-2 can be used to inform this testing. Use boundary value analysis to test the performance at the specified limits of signal noise (e.g. at maximum and minimum lighting, or maximum and minimum temperatures). Use pairwise testing to test combinations of these boundary values unless there are so few that all combinations can be tested.
It is possible achieved performance degrades over time due to hardware deterioration	ISO/IEC 19795-2 can be used to inform this testing. Use boundary value analysis to test the performance at the specified limits of hardware deterioration (e.g. with video camera lens obscured by the maximum amount). Where two or more hardware components can both cause deterioration (e.g. camera and lighting), use pairwise testing to test combinations of these boundary values, unless there are so few that all combinations can be tested.
It is possible achieved performance degrades over time due to a change in the expected subject profiles	ISO/IEC 19795-2 can be used to inform this testing. Use boundary value analysis on the specified expected subject profiles to identify maximum changes in these profiles (e.g. using a facial recognition system that was initially implemented for a Scandinavian country in a black African scenario).

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
Usability risks - documentation	
It is possible user documentation (e.g. installation guides, user guides, user manuals, read-me files, and online help) is unavailable or of poor quality	Perform usability testing to determine whether learnability and operability of the biometrics system documentation meets user needs. ISO/IEC/IEEE 26513 can be used to inform this testing. It suggests using the following evaluation criteria: — accuracy of content; — topic coverage; — safety (provision of critical information to protect against hazards or defects); — legal, statutory, and regulatory requirements for those regions where the product is offered; — documentation's structure, format, and style compared to plans, requirements, and established standards; — suitability for translation and localization; — overall readiness of the documentation for release. In addition, ISO 9241-11 defines usability as “the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use” - these are also worthwhile considering as evaluation criteria for user documentation. Use a risk-based approach to identify those system features that are most important (used the most and/or most likely to have an adverse effect if they fail) and test the relevant parts of the documentation more rigorously. Use reviews early in the life cycle, at a minimum to ensure the user documentation aligns with the organization’s documentation style guide. During system testing use dynamic testing, ideally with real users, or, at least, representative users. Use equivalence partitioning to identify the different expected user groups for the system. Use a scenario testing approach to test the documentation supporting the most important end-to-end scenarios.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
Usability risks - appropriateness recognizability risks	
It is possible subjects are not motivated to use the biometric system	In many situations, subjects have no choice on using a biometric system (e.g. border control, access to employee premises), however for some systems the subjects get to choose (e.g. biometric access to laptop or tablet). Usability testing, perhaps in the form of a questionnaire or survey, can be useful in testing whether users can recognize the appropriateness of the biometric system in meeting their needs.
It is possible the amount of change compared with the previous system causes resistance to its use by some subjects	Testing usability, in the form of learnability and operability, can be useful for determining the degree to which a changed system is likely to cause subjects to resist using it. For instance, measuring how much effort is required to learn the changes and how much easier the updated biometric system is to use. Perform user profiling to ensure representative users are identified for the testing.
Usability risks - learnability risks	
It is possible subjects are unfamiliar with the user interface	Testing usability, in the form of learnability and operability, can be useful for determining the ease with which subjects will be able to gain familiarity with the user interface. Where user interface guidelines are specified (e.g. the user interface is expected to follow Windows, iOS, or Android user interface guidelines), then review the user interface against the specified guidelines.
It is possible subjects take several uses to become familiar with the biometric system	Testing usability, in the form of learnability and operability, can be useful for determining the ease with which subjects will be able to gain familiarity with the user interface. Perform user profiling to take account of the likely frequency of use of the biometric system and ensure representative users are identified for the testing. For instance, users of a border control biometric system sometimes only use it once per year (so do not use the same 'testers' every time you test the usability of the system), while a user of a travel access system for commuters can use it 10 times a week, on average.
It is possible subjects are not aware of the best way to present features to the system	Testing usability, in the area of learnability and user error, can be useful for determining the ease with which users will learn how to best present their features to the system (e.g. not smiling and wearing a hat and sunglasses when presenting at a facial recognition system). Perform user profiling to take account of the likely frequency of use of the biometric system and ensure representative users are identified for the testing.
It is possible subjects' presentation of features change as they become more familiar with the system	Testing usability, in the area of learnability and user error, can be useful for determining the ease with which users will learn how to best present their features to the system (e.g. not smiling and wearing a hat and sunglasses when presenting at a facial recognition system). Perform user profiling to take account of the likely frequency of use of the biometric system and ensure representative users are identified for the testing.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible subjects and/or operators are not trained to use the biometric system	Testing usability, in the area of learnability, can be useful for determining the ease with which users will learn how to use the biometric system. Perform user profiling to ensure users who are tired or impaired are identified for the testing (e.g. with different levels of familiarity with similar IT systems).
It is possible subjects are unclear on how the system results are used	Review user documentation to ensure that users are made aware on how the system results will be used.
Usability risks - operability risks	
It is possible tired or impaired subjects find it difficult to use the biometric system	Testing usability, in the area of operability, can be useful for determining the ease with which tired or impaired users can use the system. Some subjects sometimes have had long flights and need to use a biometric border control system or can be accessing an entertainment venue with biometric access control after drinking alcoholic drinks. Perform user profiling to ensure representative users are identified for the testing and, if necessary, prepare them for the testing to ensure they are tired and/or impaired.
It is possible users have to actively interact with the biometric system	Testing usability, in the area of operability, can be useful for determining the ease with which users can actively interact with the system. Usability testing, perhaps in the form of a questionnaire or survey, can be useful in testing whether users are persuaded that actively interacting with the biometric system is in their best interest.
It is possible the user interface makes it difficult for subjects to interact with the system	Testing usability, in the area of operability, can be useful for determining the ease with which users can actively interact with the system. Identify and test the different scenarios that can make interacting with the system difficult (e.g. air passengers carrying bags when using a fingerprint system or having to present a passport containing their biometric template at the border control).
It is possible users are not able to configure the system interfaces for different screen sizes and resolutions	Testing usability, in the area of operability, can be useful for determining the ease with which users can work with the range of different screens sizes and resolutions. Review the user interface to check that it complies with any relevant user interface guidelines. Perform user profiling to ensure representative users are identified for the testing (e.g. with different eyesight and hand co-ordination capabilities).
It is possible users are not provided with the opportunity for customizing their user experience	Testing usability, in the area of operability, can be useful for determining the ease with which users can use the biometric system. Perform user profiling to ensure representative users are identified for the testing (e.g. with different capabilities and levels of familiarity with similar systems).

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the system requires users to follow inefficient workflows when interacting with the system	Testing usability, in the area of operability, can be useful for determining the efficiency of the workflows followed when using the biometric system. Perform user profiling to ensure representative users are identified for the testing (e.g. with different capabilities and levels of familiarity with this and similar systems).
It is possible subjects find the system lacks support for their native language and culture	Perform localization testing. This testing is often focused on usability testing the user interface and following a localization checklist, where available. This is applicable when globalized applications are localized for a particular region or when an application successful in one region is used in a different region.
It is possible the user interface is not designed for the full range of possible users	Testing usability, in the area of operability, accessibility and user interface aesthetics, can be useful for determining the ease with which different users can use the biometric system. Perform user profiling to ensure representative users are identified for the testing (e.g. with different ages, capabilities, and levels of familiarity with similar systems). The following standard for biometric systems is applicable for the treatment of usability and accessibility risks: — ISO/IEC TR 29194 provides guidance for biometric system design and procurement to handle the range of accessibility and usability issues
It is possible the menu structure of the system lacks clarity	Testing usability, in the area of operability, can be useful for determining the efficiency of the workflows followed when using the biometric system. A form of state transition testing, based on assigning screens as states, can be useful to check the ease of use and correctness of the menu structure. Perform user profiling to ensure representative users are identified for the testing (e.g. with different capabilities and levels of familiarity with this and similar systems).
It is possible subjects find the user interface is confusing	Testing usability, in the areas of operability and error protection, can be useful for determining the ease with which users can use the user interface. Perform user profiling to ensure representative users are identified for the testing (e.g. with different capabilities and levels of familiarity with this and similar systems).
It is possible subjects find they can only opt out of using the biometric system with severe penalties	Testing usability, in the area of learnability and operability, can be useful for determining the efficiency of the alternative (manual) biometric process. A form of end-to-end scenario testing of the alternative process and a check for characteristics, such as ease of use and length of time to complete the alternative process can be useful.
Usability risks - user error protection risks	
It is possible the system does not provide suitable feedback to users	Testing usability, in the area of error protection, can be useful for determining the level of useful feedback to users provided by the system. Perform user profiling to ensure representative users are identified for the testing (e.g. with different capabilities and levels of familiarity with this and similar systems).

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible users are requested to present the same biometric feature multiple times before a successful enrolment or recognition	Testing usability, in the area of error protection, can be useful for checking that users are provided with suitable feedback on presenting biometric features. Fault injection testing can be used to present inadequate biometric samples to the system (to ensure the biometric system correctly identifies inadequate biometric samples).
Usability risks - user interface aesthetics risks	
It is possible users find the user interface unappealing	Testing usability, in the area of user interface aesthetics, can be useful for determining how much the users like the user interface. User surveys and questionnaires can be useful in this testing. Perform user profiling to ensure representative users are identified for the testing (e.g. with different capabilities and levels of familiarity with this and similar systems).
It is possible subjects worry about the hygiene/health risks associated with touching the sensors	User surveys and questionnaires can be useful in determining if subjects feel discomfort with touching the sensors. Only applicable to those biometric systems where the subjects need to touch the sensor (e.g. for fingerprints, hand geometry).
It is possible users find the sensors intrusive	User surveys and questionnaires can be useful in determining if subjects feel that the sensors are intrusive. Only applicable to those biometric systems where the subjects need to get close to the sensor (e.g. for retinal scans requiring the eye to be within one centimetre of the sensor).
Usability risks - accessibility risks	
It is possible users with disabilities find difficulty using the system	Testing usability, in the area of accessibility, can be useful for determining how easily disabled users can use the system. Both software and hardware aspects are considered (e.g. user interface suitability for users with poor eyesight, and height of sensors for users in wheelchairs). Perform user profiling to ensure representative users are identified for the testing (e.g. those with a variety of different disabilities). The following standard for biometric systems is applicable for treatment of accessibility risks: — ISO/IEC TR 29194 provides guidance for biometric system design and procurement to handle the range of accessibility and usability issues

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible subjects with unusual attributes (e.g. tall/short or fat) find difficulty presenting features	Testing usability, in the area of accessibility, can be useful for determining how easily subjects with unusual attributes can use the system. More typically tested by considering hardware aspects (e.g. whether barriers are wide enough for fat subjects, or cameras can be moved for tall subjects). The following standard for biometric systems is applicable for treatment of accessibility risks: — ISO/IEC TR 29194 provides guidance for biometric system design and procurement to handle the range of accessibility and usability issues
It is possible subjects with missing or damaged features (e.g. missing fingers or abraded fingerprints) are not able to use the system	Testing usability, in the area of accessibility, can be useful for determining how easily subjects with missing or damaged features can use the system. Fault injection testing can be used to present inadequate biometric samples to the system (to ensure the biometric system correctly identifies inadequate biometric samples). Testing also checks how the biometric system handles the situation when the system cannot capture valid samples from the subjects. The following standard for biometric systems is applicable for treatment of accessibility risks: — ISO/IEC TR 29194 provides guidance for biometric system design and procurement to handle the range of accessibility and usability issues

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
Portability risks	
It is possible the time taken to install the system exceeds the maximum time specified	Installability testing can be used to check the time needed to install the system. Where there are multiple install parameters (e.g. target device, perform reboot, language choice), a pairwise approach can be used to test installation parameter combinations. Coverage of error conditions raised during installation can be decided based on a risk-based approach (probability/impact), while a form of fault injection can be used to simulate the error conditions.
It is possible the system design allows different sensors, interfaces, internal components, and other peripheral devices to be used	Both compatibility (co-existence) and portability (replaceability) testing can be applicable. When components are replaced (e.g. due to technology improvement, new standards coming into force, or components failing), portability testing can be used to check the replaceability of components and that the system works correctly with the replaced component. When there are choices for different components (e.g. the fingerprint sensor can be sourced from several different suppliers), configuration testing can be performed to check for co-existence and interoperability problems with different combinations of components. Where there are multiple options a combination of a risk-based approach (e.g. testing with the most popular components) and a pairwise approach (to reduce tested component combinations) can be useful.
It is possible the design allows the system to be adapted to be hosted on the various hardware devices (h/w configurations)	Adaptability testing can be used to check that the system can be adequately hosted on different hardware configurations. Where combinations of hardware devices can be configured together, a pairwise approach can be used to test the most popular combinations.
Reliability risks	
It is possible the system's levels of reliability and availability do not meet those required	Levels of reliability and availability are closely related. Reliability is typically measured as the mean time between system failures (or mean time to failure, which is typically used when the object being measured is not repairable), while availability is typically measured as the percentage of time a system is available (or not available) for use in a given period (both normally while the system is being used based on a specified operational profile). A third characteristic, maintainability, can also be relevant, as the time taken to repair a system after a failure (caused by lack of reliability) will directly affect the measure of availability. Together these three characteristics are often referred to as the RAM characteristics. Testing for both reliability and availability requires test inputs matching the specified operational profile to be prepared and a representative test environment to be set up. Testing systems with high levels of specified reliability and availability can take a long time. Often reliability growth model needs to be developed to measure reliability (and availability) for systems that have not been released, after which they can be measured from operational use.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible that after a catastrophic failure (e.g. the server room is flooded) system operation cannot be resumed within the required time schedule	Disaster recovery testing is used to determine the ease with which it is possible to recover the biometric system to operational use after a catastrophic failure. This often requires testing the ease of transferring operation of the system to a backup site, and then testing the transfer back to the main site after it has been repaired. Disaster recovery testing is typically based on the disaster recovery plan, and, for critical systems, can be performed without previously informing the involved stakeholders (often including senior officials). Measures suitable for disaster recovery testing include recovery time objectives, such as the maximum time to recover to the backup site, and the time to recover to the main site, and recovery point objectives, which define the maximum amount of data that can be lost.
It is possible there is no back-up system available in the event of a system failure or data corruption	Failover/recovery testing is a form of disaster recovery testing that is limited to moving to a back-up system in the event of failure, without transfer to a different backup site. Measures suitable for failover/recovery testing include recovery time objectives, such as the maximum time to recover to the backup system, and recovery point objectives, which define the maximum amount of data that can be lost.
It is possible system data, such as template enrolments, have been lost due to a system failure	Back-up/recovery testing is a form of disaster/recovery testing that is limited to restoring from back-up memory in the event of failure, without transfer to a different operating site or back-up system. Measures suitable for back-up/recovery testing include recovery point objectives, which define the maximum amount of data that can be lost.
It is possible the time taken to re-boot after a system failure is longer than specified	Testing the time to reboot a system after failure is normally considered to be a form of recovery testing.
It is possible the time taken to restore from a back-up is longer than specified	Testing the time to restore data from a backup system after failure is normally considered to be a form of recovery testing.
It is possible the inclusion of new technology makes the system unreliable	Where the system has high reliability requirements, the risk associated with using new technology can be high. This can require the system design to include fault tolerance, so that the system can continue to function in the event of individual component failures. Fault injection testing is often appropriate to test that the fault tolerance mechanism works in practice.
Maintainability risks	
It is possible the level of testability is too low	Low levels of testability mean that it can be more difficult to identify and identify defects in the system. Many of the factors that contribute to low testability are introduced early in the lifecycle, such as poor requirements, design with information hiding, and poorly structured, uncommented code. Thus, inclusion of testers in the review of early life cycle artefacts is a major contribution to identifying unacceptable levels of testability.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the time taken to make updates exceeds the time planned	System modifiability is a measure of the ease with which a system can be changed, and it is typically measured as part of maintainability testing. It is possible to measure the time taken to make generic, expected changes, such as the time to replace a broken sensor with a new one with some accuracy. However, with many software-intensive systems, updates to software are often unpredictable, as they are performed in response to unexpected failures. The corresponding fixes will vary in the impact they have on the system and the effort required to make the change, test it and, subsequently, perform regression testing.
It is possible the system is difficult to update if new biometric template formats are used	System modifiability is a measure of the ease with which a system can be changed, and it is typically measured as part of maintainability testing. If the designers were aware there was a possibility that new biometric template formats would be used in the future, ideally they will have designed the system to easily accommodate this change. Similarly, if this is a known risk, testing the ease of changing the system, including subsequently testing the change and performing regression testing will typically be relatively easy to measure. Testing of this change will normally include function testing of the biometric performance metrics to ensure the change to the template format has not adversely affected the functional performance of the system (e.g. an increase in false non-match rates).
It is possible biometric template data is reused in a context other than the one for which it was originally created	Performing functional biometric performance testing can be used to determine if the reused template data achieves a suitable level of accuracy (in case the level of fidelity of the template data was lower than expected for the system).
Compatibility risks	
It is possible the biometric system software is sharing some computers with other apps	Compatibility testing to check for potential co-existence problems is performed. Co-existence problems tend to occur when multiple applications share the same resources and conflicts over this usage occur. Generically, the types of shared resources are likely to include memory (e.g. virtual, cache, RAM, ROM), CPU cycles and communication channels. For instance, reuse of registry keys is likely to be checked as part of co-existence testing of applications on a machine running Windows.
It is possible the system interacts with other systems (e.g. built by third parties)	When there are risks associated with multiple systems exchanging and using information, interoperability testing is performed. Interoperability testing is often performed at system interfaces and is typically based on testing that functionality can be performed correctly when it is necessary to interact with another system. If the biometric system's template repository can be updated by multiple template enrolment systems, the testing would need to ensure that all such systems can update the repository, and that the stored templates were in the correct format. ISO/IEC 19795-4 can be used to inform this testing. ISO/IEC 19795-4 includes procedures for establishing an interoperable set of implementations, defines procedures for testing interoperability with previously established sets of implementations, and gives testing procedures for the measurement of interoperable performance.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the system fails to perform properly when other systems it communicates with change	When other systems change, it is normally necessary to perform interoperability testing to check that the system can still communicate with the new systems and use the communicated information. Interoperability testing ideally will have already been performed with the previous system, and, unless there has been a deliberate change in the communication, the interoperability tests previously used can be re-run as a form of regression testing. ISO/IEC 19795-4 can be used to inform this testing. ISO/IEC 19795-4 includes procedures for establishing an interoperable set of implementations, defines procedures for testing interoperability with previously established sets of implementations, and gives testing procedures for the measurement of interoperable performance.
It is possible the large number of links to other systems causes interoperability issues	Testing links to other systems is part of interoperability testing. In the event that there are many links to other systems (e.g. many smart sensors in the biometric system) then equivalence partitioning can be used to group similar classes of systems and so reduce the testing needed to cover all links (e.g. just test links to one camera sensor if many of the same type are used as part of the biometric system). ISO/IEC 19795-4 can be used to inform this testing. ISO/IEC 19795-4 includes procedures for establishing an interoperable set of implementations, defines procedures for testing interoperability with previously established sets of implementations, and gives testing procedures for the measurement of interoperable performance.
Performance efficiency risks	
It is possible response times are too long (e.g. at peak expected load)	Performance testing of response times at various specified loads is carried out. A risk-based approach would suggest starting with the peak expected load. If performance issues are identified, resource monitoring (e.g. of used CPU capacity, used network bandwidth, and used memory) can provide guidance on where the system needs improvement. Performance testing to ascertain response times will be carried out on those end-to-end test scenarios identified as highest risk. Where necessary, response times will be checked for the more critical individual components of the biometric system.
It is possible system memory constraints are exceeded	Performance testing for memory use at various specified loads is carried out. A risk-based approach would suggest starting with the peak expected load. If performance issues are identified, resource monitoring (e.g. of used CPU capacity, used network bandwidth, and used memory) can provide guidance on where the system needs improvement. Performance testing to ascertain memory use is carried out on those end-to-end test scenarios identified as highest risk. Where necessary, memory use will be checked for the more critical individual components of the biometric system.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible system bandwidth constraints are exceeded	Performance testing for network bandwidth use at various specified loads is carried out. A risk-based approach would suggest starting with the peak expected load. If performance issues are identified, resource monitoring (e.g. of used CPU capacity, used network bandwidth, and used memory) can provide guidance on where the system needs improvement. Performance testing to ascertain network bandwidth use is carried out on those end-to-end test scenarios identified as highest risk. Where necessary, network bandwidth use is checked for the more critical individual components of the biometric system.
Standards-related risks	
It is possible the system does not comply with existing standards	Standards can be organizational, contractual, or regulatory. Reviews and checklists are often the most appropriate way of checking compliance with standards. In some situations, there test suites are available to test compliance with standard communication protocols for mass-produced system components, such as sensors.
It is possible the system does not comply with future standards	Standards can be organizational, contractual, or regulatory. It is difficult to predict how future standards will affect compliance of the biometric system. Assuming that they will require updates to be made to the system, it would be possible to test for system modifiability – and so measure the ease with which a system can be changed. This is typically measured as part of maintainability testing. System modifiability can be tested by measuring the ease of making changes to the system (the changes used can be based on expected future standardization) or by reviewing the system for maintainability using a suitable checklist.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
Security risks – attack vulnerabilities	
It is possible the system does not comply with security standards for biometric systems	Security standards for biometric systems can be grouped into two classes. Those that are specifically applicable to biometric systems and those that apply to systems in general. Biometric-specific: — ISO/IEC 19792 covers the biometric-specific aspects and principles to be considered during the security evaluation of a biometric system. — ISO/IEC 24745 provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. — The ISO/IEC 30107 series addresses the problems of presentation attack detection to biometric systems. ISO/IEC 30107-3 focuses on 'Testing and reporting', while ISO/IEC 30107-4 provides a 'Profile for testing of mobile devices'. — ISO 19092 describes the security framework for using biometrics for authentication of individuals in financial services. Generic: — The ISO/IEC 15408 series is meant to be used as the basis for evaluation of security properties of IT products. — ISO/IEC 18045 defines the minimum actions to be performed by an evaluator in order to conduct an evaluation based on the relevant criteria and evidence defined in the ISO/IEC 15408 series. It is a companion document to ISO/IEC 15408 series. These standards, or a subset of them, can be used for many of the risks listed here as security or privacy risks.
It is possible transaction data (e.g. who has gained access via use of the biometric system) can be hacked	Knowledge of who has used a biometric system can be useful to some external parties and can constitute a violation of privacy for those who have used the biometric system to gain access (e.g. to a private clinic). Security testing can be performed to determine the ease with which these records can be accessed by those who are not authorised to do so.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible a denial of service attack forces the backup system to be used	A denial-of-service attack typically attempts to overload a system with requests for services. For a biometric system, this can take the form of many requests for authentication being requested at the same time. This would be most likely to overload the matcher or decision components but can also overload feature extraction and accessing the template repository, or the internal network. Where there is a known flaw in the system, denial of service attacks will often target this flaw. Testing for denial of service of the system is often carried out in the form of a penetration test. If enough resources are devoted to the attack then it will succeed in overwhelming the biometric system. However, conducting such an attack will allow system vulnerabilities to be identified and a decision can then be made as to whether it is worthwhile addressing them. If performing such a test on an operational system it is likely to cause performance issues. In the event of a successful denial of service attack, then it is often necessary to fall back to using a backup system, which can be manual. Part of the testing for a denial-of-service attack will be on the backup system and consider its accuracy and security as denial-of-service attacks are often performed to force the use of an inferior and more easily spoofed or attacked backup system.
It is possible a trusted individual attacks the system (an insider attack)	A high proportion of security breaches are due to insider threat actors, with Verizon reporting that 34 % of all breaches were from this source, with some industries more prone to this form of attack than others. Insider attacks are the most likely form of security attack to go unreported. One form of insider attack that is specific to biometric systems is where an insider gains access to a protected resource (e.g. money in a bank account) and then uses the argument that the account was accessed because the biometric system flagged the access as valid, when it was not, using the fact that biometric systems are not 100 % accurate as the false positive rate is never zero. Individuals who attack systems are most likely to resort to an attack when they are under stress (e.g. financial or personal difficulties), and so a key preventive measure is for managers and human resource staff to be trained to identify individuals in such situations. One way that testing can play a part here is by review of the management and HR training and checking that there are records showing that such threats are actually addressed on an ongoing basis. Another way is checking that the levels of privileges assigned to different administrators and cross-checking between administrators have been properly implemented.
It is possible a trusted individual uses poor passwords or other security measures	Individuals can cause security vulnerabilities through poor use of passwords, but administrators often cause larger problems, such as by misconfiguring cloud storage databases, so providing easy access to sensitive information. The main treatment for this risk is security training, which needs to be taken at all levels in the organization. Higher management often miss out on this training but are often in a position to make the biggest mistakes. From a testing perspective, the main check is on the availability and take-up of regular security training.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible software is compromised by system developers (or 3rd-party) providers	See previous risk on 'It is possible a trusted individual attacks the system (an insider attack)' Where the trusted individual is a system developer then the form of attack can include unauthorised code, that can perform functions that breach the security of the system. Identification of such unauthorised code can be accomplished using both static analysis and code reviews.
It is possible the enrolment process can be subverted	If the enrolment process is subverted, then the enrolment data in the template repository cannot be trusted. Possible inappropriate enrolment data, such as enrolling fingerprints from two different individuals under the same name, can be used by an attacker to obtain incorrect recognition by the system. This is most likely to occur when the enrolment process is not properly monitored, or when the person responsible for managing the enrolment process helps to subvert the enrolment. Testing or reviewing of the enrolment process can detect the possibility of such misuse of the biometric system.
It is possible stored templates (e.g. fingerprint in phone memory or main repository database for a large biometric system) are corrupted to force a fall-back to be used	A security attack can deliberately target stored references to force the biometric system to use a fall-back, which is likely to be less secure. Two forms of testing are normally considered. First, testing how easy it is to corrupt stored templates, and second, testing that the fall-back (template or process) is just as secure as using the primary template.
It is possible data is intercepted during transmission between system components and used to replay the authentication	For an attacker to replay an authentication request on a biometric system, they must first intercept either the sample captured from a sensor or the extracted features, and subsequently inject the sample or feature into the system to gain unauthorised authentication. This is a form of man-in-the-middle attack. One approach to biometric system design to prevent replay attacks is for the biometric system components to use a 'challenge/response' approach to communication between components, whereby the receiving component (e.g. the feature extractor) requests the sending component (e.g. sensor) to include a randomly-generated token in the captured sample so that the receiving component knows the sample was received from the sending component and not injected into the channel between them. This form of attack can also be targeted at changing the score that is passed from the 'matcher' component to the ''decision' component. Checking the design and implementation of such security features can be done through design and code reviews and tested using a form of fault injection testing. Encryption of communicated data will also be part of the biometric system design. See the risk 'It is possible the encryption/decryption of communicated data is missing, lacking quality or poorly implemented' for more information on treatment of this risk.
It is possible false data is injected during transmission between system components	This is one half of a replay attack (i.e. there is no interception as the injected data is created rather than stolen). Treatment is the same as for the replay attack (i.e. checking the design/implementation of a suitable 'challenge/response' approach).

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the 'decision' component of the biometric system is compromised to allow comparisons to be marked as matching when they are not	This can be achieved by modification of the code in the 'decision' component or overriding the threshold value used to determine the minimum required level of matching if this is provided as an input. Code protection tools providing various levels of protection are available. Review of the design and code can be used to ensure a suitable level of protection is implemented in the biometric system.
It is possible the enrolment database is attacked	Templates can be deleted from the repository as part of a denial-of-service attack (see the 'It is possible a denial of service attack forces the backup system to be used' risk). If reference data is stolen from the database, it can be used as part of a later man-in-the-middle attack (see the 'It is possible data is intercepted during transmission between system components and used to replay the authentication' risk). If template data is directly associated with a clear subject identifier an attacker can change the identifier and/or template data. Encryption of the data held in the repository can be used to prevent this (see the 'It is possible the encryption/decryption of communicated data is missing, lacking quality or poorly implemented' risk).
It is possible the biometric system is implemented with biometric template data stored on workstations	The additional risk associated with storing biometric data on workstations would be that security policies are not properly implemented on workstations. Testing and auditing of the processes to ensure that security policies are implemented on the workstation can be performed.
It is possible individual system components are attacked	This can be achieved by modification of the code in the attacked components. Code protection tools providing various levels of protection are available. Review of the design and code can be used to ensure a suitable level of protection is implemented in the biometric system.
It is possible the encryption keys used for data transmission within the biometric system are stolen	Encryption keys cannot be stored on the biometric system as they can be identified by hackers who have already gained access to the system. Review of operational processes for encryption key management will determine that encryption keys are securely stored separate from the biometric system.
It is possible the system is the subject of a brute force attack	In this scenario an attacker presents many raw samples to the biometric system in the hope that one of the samples matches an entry in the template repository. In practice, an effective approach would be to intercept the output of the biometric sensor and feed millions of raw images (obtained from the web, for example) into the matcher. Testing that the biometric system meets its targets for specified biometric performance measures will provide confidence that the system will not be prone to brute force attacks succeeding more than expected.
It is possible a presentation attack uses an artefact to mimic a biometric source	Presentation attacks differ depending on the modalities used in the biometric system, such as fingerprints, walking gait, face, voice, etc. The ISO/IEC 30107 series addresses the problems of presentation attack detection to biometric systems. ISO/IEC 30107-3 focuses on 'Testing and reporting', while ISO/IEC 30107-4 provides a 'Profile for testing of mobile devices'.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the biometric source is stolen to use it to gain access (e.g. cut off finger)	Opportunities to steal an example of biometric source differs depending on the modalities used in the biometric system, such as fingerprints, handprints, etc. The ISO/IEC 30107 series addresses the problems of presentation attack detection to biometric systems. ISO/IEC 30107-3 focuses on 'Testing and reporting', while ISO/IEC 30107-4 provides a 'Profile for testing of mobile devices'.
Security risks – vulnerabilities (accidental)	
It is possible the security plan for the biometric system is missing/lacking/not being implemented/not being reviewed adequately	A security plan defines the operating procedures related to software, system, and operational security of the biometric system and is aligned with the security policy. Operators and managers will ideally be familiar with the security plan. Security plans can be reviewed and audited against.
It is possible raw biometric data is stored in the biometric system	A biometric system does not store raw sample data, as this can be stolen and reused in other systems the subject is enrolled in. Testing for this can be done by review of the biometric system design.
It is possible biometric feature and template data is stored in the matcher component of the biometric system	The matcher component does not retain copies of the biometric feature or template data after it has performed its 'match' as this can be stolen and used in a replay attack. Testing for this can be done by review of the biometric system design.
It is possible platform security configuration settings are not adequate	The security plan requires a risk-based approach to security is implemented. This includes consideration of platform security configuration settings. Audits against the security plan identify if the settings are inadequate.
It is possible security patches are not installed within necessary timescales	The security plan requires a risk-based approach to security is implemented. This includes consideration of frequent checking for, and implementation of, security updates. Audits against the security plan identify if this is not being done.
It is possible the process for handling security breaches is missing, lacking quality or inadequately implemented	The security plan defines the procedures for handling security breaches. Audits against the security plan identify if this is not being done.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the encryption/decryption of communicated data is missing, lacking quality or poorly implemented	The design specification for the biometric system defines the requirements for encryption and decryption in the system. Several standards cover the requirements and testing of cryptographic modules: — ISO/IEC 19790 defines the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems — ISO/IEC 24759 specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790. — ISO/IEC TS 20540 provides recommendations and checklists which can be used to support the specification and operational testing of cryptographic modules in their operational environment within an organization's security system.
Security risks – system access	
It is possible the rules for who is allowed access to the biometrics system are missing/lacking/not enforced	The security plan requires a risk-based approach to security is implemented. This includes specifying rules for who is allowed access to the various component parts of the biometrics system. Audits against the security plan identify if this is not being done.
It is possible that access to the system provided for testing was not rescinded when testing was completed	The security plan requires a risk-based approach to security is implemented. This will ideally include the specification of rules for when testers are allowed access to the various component parts of the biometrics system and the rules for when such access is rescinded. Audits against the security plan identify if this is not being done.
It is possible that the physical access to where the biometric system is housed is not adequately controlled	The security plan requires a risk-based approach to security is implemented. This includes specifying rules for who is allowed physical access to the biometric system. Audits against the security plan will identify if this is not being done.
It is possible access logs for the biometric system are not reviewed on a regular basis	The security plan requires a risk-based approach to security is implemented. This includes specifying schedules for reviewing access logs for the biometric system (e.g. to check that only authorised personnel accessed the system). Audits against the security plan will identify if this is not being done.
It is possible the rules for accessing the biometrics system are less strict than those implemented by the system itself	The security plan requires a risk-based approach to security is implemented. This includes specifying rules for who is allowed access to the biometric system. Ideally these rules will not be less strict than those for the system/facility the biometric system provides access to. If the biometric system has weaker security, then this makes the biometric system itself the weak point in the overall system of systems. Audits against the security plan will identify if this is not being done.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
Security risks – sensors	
It is possible a sensor can be replaced by a fake sensor	A fake sensor can be used to gather biometric samples without the knowledge of the owners of the biometric system. The security plan requires that a risk-based approach to security is implemented. This will include specifying procedures for the monitoring and safeguarding of sensors. Audits against the security plan will identify if this is not being done.
It is possible that data can be intercepted during transmission between the sensor and the rest of the biometric system and used to extract biometric data	Loss of raw sample data can have a significant impact, especially if it is associated with a particular subject, as if stolen it can be reused in other systems the subject is enrolled in (or used in other systems). The system design of the biometric system will ideally ensure separation of the subject personal details and their sample data, so requiring an attacker to intercept multiple messages on multiple channels. Testing for this can be done by review of the biometric system design. Ideally encryption of communicated data will also be part of the biometric system design. See the risk 'It is possible the encryption/decryption of communicated data is missing, lacking quality or poorly implemented' for more information on treatment of this risk.
It is possible the biometric system is implemented with biometric data stored on sensors	The additional risk associated with storing biometric data on sensors would be that the sensors can be physically stolen due to their small size. Testing and auditing of the processes to ensure that sensors are physically secured (to prevent them being stolen) can be performed.
It is possible sensors are deliberately damaged to force fallback procedures to be used	The security plan requires a risk-based approach to security is implemented. This will include specifying procedures for the monitoring and safeguarding of sensors. Audits against the security plan will identify if this is not being done. If a sensor is damaged, then ideally the biometric system will identify the failure and provide suitable reporting. This can be tested using a form of fault injection testing. In the event of a sensor being rendered inoperative, it is often necessary to fall back to using a backup system, which can be manual. Part of the testing for such a situation will be on the backup system and consider its accuracy as such attacks are often performed to force the use of an inferior and more easily spoofed backup system. Alternatively, for larger biometric systems, it is possible to simply re-route subjects to an alternative sensor. Part of the testing for such a situation will be on the ease with which subjects are re-routed, and possibly measuring the throughput rate now there are less sensors available.
It is possible sensors are not certified by the relevant body	For some situations, the biometric system requires compliance and the sensors to be certified. Audits can be used to check the certification of sensors.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
Privacy risks	
It is possible that the relevant privacy standard for biometric systems was not used	The following security standard for biometric systems can be applicable for treatment of privacy risks: — ISO/IEC 24745 provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer.
It is possible litigation occurs due to leaked data	Customers need to be aware of the financial and reputational dangers of leaking subjects' biometric data, especially raw biometrics which can be used in other biometric systems. Reviews of the system design and penetration testing can both be used to improve confidence in the ability of the biometric system to keep subject data secure.
It is possible that biometric data is used for other than the originally agreed purpose	Function creep with biometric systems, where the original functionality is extended to new areas, is a common privacy issue with users of biometrics systems. Care must be taken to ensure that function creep does not cause any permissions granted by the subjects of the biometric system to be exceeded. In Europe, the EU General Data Protection Regulation (GDPR) requires organisations to collect biometric data only for 'specified, explicit and legitimate purposes' and cannot subsequently process this data 'in a manner that is incompatible with those purposes.' Review or audit of the permissions to ensure they are still in scope will be undertaken whenever any additional functions are added, or biometric data is reused in another system.
It is possible biometric data is stored for longer than is necessary	Review or audit of the permissions granted by the subjects of the biometric system will be undertaken whenever biometric data is held for more than the minimum required for the system to fulfil its function.
It is possible personal data regulatory requirements (e.g. GDPR) are not complied with	Review or audit of biometric systems will be undertaken to ensure that the system complies with the relevant personal data privacy regulations. For instance, in Europe, the EU General Data Protection Regulation (GDPR) requires organisations to collect biometric data responsibly and keep it secure. In the US, several states (e.g. New York, California, Washington, Illinois, and Texas) have privacy laws that cover the use of biometric data. Testing against these laws and regulations will change depending on where the system is used. However, a biometric system (and its operational processes) in Europe that complies with GDPR would need to be tested to ensure that subjects provided explicit consent and have the right to be forgotten. Administrators would also have to report data breaches within 72 hours of discovery. Fines for organizations not protecting data under GDPR can reach up to 4 % of annual worldwide turnover, so making the risk of non-compliance extremely high.
It is possible the process for a subject to request that their data is removed from the system is missing/lacking/not adequately implemented	Review and/or audit of the operational processes supporting the biometric system check that subjects can request that their data is removed from the biometric system (e.g. under the GDPR 'right to be forgotten').
It is possible the process for removing subject data is missing/lacking/not implemented adequately	Review and/or audit of the operational processes supporting the biometric system check that subject data can be removed from the biometric system (e.g. under the GDPR 'right to be forgotten').

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible subjects are unaware that their biometric data are being collected (i.e. systems are used covertly)	Unless consent is given, the storage and processing of biometric data is not allowed under data protection rules, such as EU GDPR. However, government agencies are often exempt from these rules, provided their actions are proportional to the potential threat (e.g. looking for terrorists on a watch list). Review and/or audit of the operational processes supporting the biometric system check that consent is obtained before biometric data is stored and processed.
It is possible subjects are unhappy that they are forced to provide biometric data	Some subjects of biometric systems do not want to provide biometric data (e.g. due to associations of fingerprinting with crime). This means they are unlikely to opt in to using the biometric system (if its use is optional). Usability testing, perhaps in the form of a questionnaire or survey, can be useful in testing whether users can recognize the appropriateness of the biometric system in meeting their needs.
It is possible information leakage occurs due to sensors picking up extraneous inputs (e.g. from microphones on cameras)	Biometric systems will ideally be restricted to gathering the data needed for the system to perform its primary function, and consent is unlikely to have been given for the system to gather extraneous data, such as overheard conversations. Interoperability testing of the communication channels from the sensors can identify if extraneous data were being gathered by the biometric system.
Operational risks - training	
It is possible the training of tech support for the biometric system is missing/lacking/poorly implemented	Review the relevant documentation to confirm that training of technical support staff is available. Survey technical support staff to determine the quality and effectiveness of training for them in their use of the biometric system.
It is possible training for operators on their role with the biometric system is missing/lacking/poorly implemented NOTE: Operators assist subjects and prevent spoofing	Review the relevant documentation to confirm that training of operators is available. Survey operators to determine the quality and effectiveness of training for them in their use of the biometric system.
It is possible training for helpdesk staff on the biometric system is missing/lacking/poorly implemented	Review the relevant documentation to confirm that training of helpdesk staff is available. Survey helpdesk staff to determine the quality and effectiveness of training for them in their use of the biometric system.
Operational risks - support	
It is possible helpdesk support is missing/lacking	Perform walkthroughs and /or scenario testing of potential helpdesk scenarios using representative helpdesk staff. Select the scenarios based on risk (e.g. likelihood of scenario occurring and impact if mishandled).
It is possible the complaints procedure for subjects is missing/lacking/not managed adequately	Perform walkthroughs and/or scenario testing to cover the complete lifecycle of a complaint, from its submission to it being closed. Complaints and the representative stakeholder submitting it will be selected using risk by selecting the most common complaints and the stakeholders who would make them, and the biggest potential impact if the complaint was not handled suitably.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible subjects feel that their concerns about the system are not taken seriously (e.g. concerns are ignored)	Review the publicly available information available on the biometrics system to ensure typical concerns are addressed in a manner suited to typical subjects and that this information is easily available.
It is possible support for subjects requiring temporary verification by the biometric system is missing/lacking/poorly implemented	Perform walkthroughs and/or scenario testing of the situation where a potential subject requires temporary verification by the biometric system.
It is possible the volume of user litigation due to false positives and false negatives is high	Review the basis for the selected levels of false positives and false negatives for the system and perform functional testing to ensure the selected levels are being achieved in operation.
It is possible the system is not internationalized/localized for the current country/region	Perform internationalization or localization testing, as appropriate.
Operational risks - incidents/defects	
It is possible operators do not know how to report incidents	Review the relevant documentation to confirm that operator training includes incident reporting. Survey operators to determine the quality and effectiveness of training for them in incident reporting for the biometric system. Perform walkthroughs and/or scenario testing of incident reporting by operators using representative operators.
It is possible the incident management process for the biometrics system is lacking/missing/badly implemented	Review the relevant documentation to confirm that incident management for the biometric system is adequately documented and follows a suitable process.
It is possible it is unclear who has responsibility for handling incidents	Review the relevant documentation to confirm that incident management for the biometric system is adequately documented and that responsibilities are clearly defined, e.g. in a RACI (responsible, accountable, consulted, and informed) matrix.
It is possible the defect management process for faults found in the biometrics system during testing is lacking/missing/badly implemented	Review the relevant documentation to confirm that defect management for the biometric system is adequately documented and follows a suitable process.
It is possible the defect management tool is inadequate	Review the defect management tool and consider how well it supports the agreed defect management process. If the level of support is inadequate, suggest to the project manager that a more suitable and effective tool is acquired.
It is possible defect analysis does not detect common errors until it is too late to fix them	Ensure that the defect management process includes the performance of root cause analysis early in the life cycle. Confirm that root cause analysis results are shared among the relevant stakeholders (and, ideally, acted on).

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
Operational risks - sensors	
It is possible the sensor was not adequately calibrated on installation	Review the installation instructions to confirm that the calibration of the sensors is adequately documented. Perform walkthroughs and/or scenario testing of the installation of sensors in the biometric system. Perform functional testing of the sensors after installation to determine that they have been adequately calibrated.
It is possible the sensor was not re-calibrated at the required regular intervals or when the operational environment changes, once operational	Review the operational maintenance documentation to confirm that recalibration instructions for the sensors are adequately documented. Perform walkthroughs and/or scenario testing of the recalibration of sensors in the biometric system. Perform functional testing of the operational sensors to determine that they are adequately calibrated.
It is possible that sensor cleanliness causes sample data to be compromised	Review the operational maintenance documentation to confirm that cleaning instructions for the sensors are adequately documented. Perform walkthroughs and/or scenario testing of the cleaning of sensors in the biometric system. Perform functional testing of the operational sensors to determine that they are adequately cleaned (note that different features will be presented to ensure residual characteristics are not being interpreted as a new subject's biometric features).
Operational risks - enrolment	
It is possible the enrolment process is not fully defined/communicated/understood by operators	Review the operators' enrolment documentation to confirm that enrolment instructions for new subjects are adequately documented. Perform walkthroughs and/or scenario testing of the enrolment process in the biometric system using representative operators. Perform functional testing to check that newly enrolled subjects are recognized by the biometric system.
It is possible the enrolment process is not fully defined/communicated/understood by subjects	Perform walkthroughs and/or scenario testing of the enrolment process in the biometric system using representative subjects. Perform functional testing to check that newly enrolled subjects are recognized by the biometric system.
It is possible the process for how enrolment failure is handled is missing/lacking/poorly implemented	Review the operators' enrolment documentation to confirm that instructions for failed enrolments are adequately documented and the process is valid. Perform walkthroughs and/or scenario testing of a failed enrolment in the biometric system using representative operators and subjects (this can be simply achieved by mismatching the subject and the template). Perform functional testing to check that the subject with the failed enrolment is not recognized by the biometric system.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the process for checking the true identity of those enrolling is missing/lacking/poorly implemented (e.g. it does not require sufficient checks)	Review the operators' enrolment documentation to confirm that instructions for checking the true identity of an enrolling subject are adequately documented and the process is valid. Perform walkthroughs and/or scenario testing of the checking the true identity of an enrolling subject using representative operators and subjects.
It is possible the process for updating template data (e.g. re-enrolment with new face images) is lacking/missing/not implemented adequately	Review the operators' enrolment documentation to confirm that instructions for re-enrolments are adequately documented and the process is valid. Perform walkthroughs and/or scenario testing of a re-enrolment in the biometric system using representative operators and subjects (this can be simply achieved by mismatching the subject and the template). Perform functional testing to check that the re-enrolled subject is recognized by the biometric system.
It is possible performance requirements are not achieved if new templates are not enrolled frequently enough	Review the operational documentation to confirm that the processes for re-enrolment are adequately documented and that the maximum time between enrolments is not too long. Perform functional testing with templates around the maximum time between enrolments to check that performance requirements are met by the biometric system with 'old' templates.
It is possible the process for removing an enrolled person from the system is lacking/missing/not implemented adequately	Review the operators' enrolment documentation to confirm that instructions for removal of subjects are adequately documented and the process is valid. Perform walkthroughs and/or scenario testing of removal of a subject from the biometric system using representative operators. Perform functional testing to check that removed subjects are no longer recognized by the biometric system.
Operational risks - recognition	
It is possible the recognition process is not defined/communicated/understood by subjects	Review the publicly available information available on the biometrics system to ensure it covers typical use cases of the biometric system by typical subjects and that this information is easily available. Perform walkthroughs and/or scenario testing of typical use cases of the biometric system using representative subjects.
It is possible the recognition process is not defined/communicated/understood by operators	Review the operators' recognition documentation to confirm that instructions for operating the biometric system are adequately documented. Perform walkthroughs and/or scenario testing of the recognition process in the biometric system using representative subjects and operators. Perform functional testing to check that enrolled subjects are recognized by the biometric system and subjects who are not enrolled are not recognized by the system.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the process for handling a false-negative result (e.g. subject incorrectly being refused access) is missing/lacking/poorly implemented	Review the operators' recognition documentation to confirm that instructions for handling of a false negative result provided from the biometric system are adequately documented. Perform walkthroughs and/or scenario testing of the process for handling of a false negative result from the biometric system using representative subjects and operators.
It is possible the process for handling a verification of a true-negative result (e.g. subject correctly being refused access) is missing/lacking/poorly implemented	Review the operators' recognition documentation to confirm that instructions for handling of a true negative result provided from the biometric system are adequately documented. Perform walkthroughs and/or scenario testing of the process for handling of a true negative result from the biometric system using representative subjects and operators.
It is possible the number of templates used as the basis for identification increases to a level that impacts time-based performance of the biometric system	Perform non-functional performance testing to determine that required response times and processing times are achieved by the biometric system.
Operational risks - operation	
It is possible transaction logs for the enrolment and recognition systems are not recorded	Review the relevant support documentation to confirm that instructions for recording transaction logs are adequately documented. Perform walkthroughs and/or scenario testing of the process for recording transaction logs using representative support staff. Perform audits to check that transaction logs are available for the required periods (not too short a time that information is not available for analysis when needed and not too long that privacy regulations are not met).
It is possible transaction logs are not analyzed to identify unusual use of the system	Review the relevant support documentation to confirm that instructions for analyzing transaction logs are adequately documented. Perform walkthroughs and/or scenario testing of the process for analyzing transaction logs using representative support staff. Perform audits to check that any required analysis of transaction logs has been carried out and the results recorded.
It is possible the process for the regular testing of performance (e.g. accuracy) is lacking/missing/not implemented adequately	Review the relevant support documentation to confirm that instructions for regularly testing the performance of the biometric system are adequately documented. Perform walkthroughs and/or scenario testing of the process for performing performance tests using representative support staff. Check that these tests are representative of the system status at the time (e.g. number of enrolled templates). Perform audits to check that required performance tests have been carried out and the results recorded at the required intervals.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the process of regularly monitoring system throughput is lacking/missing/not implemented adequately	Review the relevant support documentation to confirm that instructions for regularly measuring the number of subjects using the biometric system are adequately documented. Perform audits to check that throughput for the biometric system is measured and the results recorded at the required intervals.
It is possible the process of regularly monitoring system response times is lacking/missing/not implemented adequately	Review the relevant support documentation to confirm that instructions for regularly measuring the response and processing times for the biometric system are adequately documented. Perform audits to check that response and processing times for the biometric system are measured and the results recorded at the required intervals.
It is possible that use of the biometric system is not adequately supervised	Review the relevant management documentation to confirm that instructions for regularly checking the operation and support of the biometric system are adequately documented. Perform walkthroughs and/or scenario testing of the process for supervising use of the biometric system using representative management, operator, and support staff.
It is possible the operational environment of the biometric system is not adequately controlled	Review the relevant operational management documentation to confirm that instructions for control of the operational environment of the biometric system are adequately documented and the process is valid. Survey relevant stakeholders (e.g. operators, support staff) to determine whether the operational environment is adequately managed in practice.
It is possible there are insufficient human operators to support operation of the system	Review the relevant operational management documentation to confirm that instructions for resourcing operation of the biometric system are adequately documented and the required levels are valid. Survey relevant stakeholders (e.g. managers, operators) to determine whether the operational environment is adequately resourced in practice.
Operational risks - recovery	
It is possible the process for managing backups (in case there is a system failure requiring recovery) is missing/lacking/poorly implemented	Review the relevant support documentation to confirm that instructions for making backups of the biometric system data (e.g. transaction data, templates) are adequately documented. Perform audits to check that required backups have been made and stored at the required intervals.
It is possible the processes for handling a system (or subsystem) failure are missing/lacking/poorly implemented	Review the relevant support documentation to confirm that instructions for recovering the biometric system after a system or subsystem failure are adequately documented. Perform recoverability tests, such as walkthroughs and/or scenario testing of the process for recovering the biometric system after a system or subsystem failure using representative support staff. Check that these tests are representative of the system status at the time (e.g. number of recorded transaction and enrolled templates). Recoverability tests typically include failover testing, which are tests of the ability of the system to switch to a backup (failover) system (also called disaster recovery testing) and backup and restore testing (more appropriate if there is not a failover system available as a backup. Perform audits to check that required recoverability tests have been carried out and the results recorded at the required intervals.

Table C.2 *(continued)*

Generic biometric system product risks	Possible treatments by software testing
It is possible the disaster recovery process is missing/lacking/poorly understood	Review the disaster recovery documentation to confirm that instructions for recovering the biometric system after a system or subsystem failure are adequately documented. Ensure responsibilities (e.g. who is responsible for performing testing of the recovered system) are clearly defined. Perform recoverability tests, such as walkthroughs and/or scenario testing of the process for recovering the biometric system after a system or subsystem failure using representative support staff. Check that these tests are representative of the system status at the time (e.g. number of recorded transaction and enrolled templates). Recoverability tests for such a situation include failover testing, which are tests of the ability of the system to switch to a backup (failover) system and also called disaster recovery testing. Perform audits to check that required disaster recovery tests have been carried out and the results recorded at the required intervals.
It is possible the backup/disaster recovery system is not tested to the same level of rigour as the main system (e.g. accuracy, security)	Perform the same tests (e.g. for performance, response times, throughput, security) on the backup system as were performed on the main system (when the systems are not identical).
Operational risks - install/update	
It is possible updates to the biometric system have not been performed in a timely manner	Review the relevant support documentation to confirm that instructions for regularly checking for and performing updates to the biometric system are adequately documented. Perform audits to check that required updates have been carried out within recommended times.
It is possible the processes for installing (and uninstalling) the system are missing/lacking/inadequately applied	Review the installation documentation to confirm that instructions for installing the biometric system are adequately documented. Perform installability tests, such as walkthroughs and/or scenario testing of the process for installing the system on different hardware, middleware, and software configurations. Installability tests can cover both installation and deinstallation of the system.
It is possible the processes for performing updates to the biometrics systems are missing/lacking/inadequately applied	Review the relevant documentation to confirm that instructions for updating the biometric system are adequately documented. Perform installability tests, such as walkthroughs and/or scenario testing of the process for different update types (e.g. hardware, middleware, and software updates). Ensure these installability tests include smoke tests to ensure there has been no regression of the system due to the updates.
It is possible system update testing is not given access to the real environment	Perform installability tests for different update types (e.g. hardware, middleware, and software updates) on the operational environment or a representative test environment.
It is possible that updates to the biometric system have not been authorised / tested / approved	Review the relevant documentation to confirm that instructions for updating the biometric system include suitable coverage of the authorisation, testing, and approval of updates and that these are adequately documented. Perform audits to check that updates to the biometric system are authorized, tested, and approved before being applied to the operational system.

Annex D
(informative)

Test documentation mappings for biometric systems

D.1 General

This annex provides mappings between the software test documentation requirements defined by ISO/IEC/IEEE 29119-3 and the documentation requirements of:

— ISO/IEC 19795-1

— ISO/IEC 19795-2

— ISO/IEC 19795-6

D.2 Test documentation mappings

D.2.1 Overview

ISO/IEC 19795-1 covers generic biometric testing, while ISO/IEC 19795-2 covers technology and scenario evaluation and ISO/IEC 19795-6 covers operational evaluation. Each of these standards defines documentation requirements for the testing of biometric systems. The test documentation requirements from ISO/IEC 19795-1 are general and apply to all three forms of biometric evaluation, while the other two standards provide test documentation requirements which are specific to each of the three forms of biometric evaluation.

A tester who is required to perform and document testing for a particular biometric evaluation level will normally be required to create test documentation in accordance with two biometric test standards; the requirements that apply to all biometric testing defined in ISO/IEC 19795-1 and the requirements for the specific evaluation level, which are defined in ISO/IEC 19795-2 and ISO/IEC 19795-6. The four mapping tables in this clause show each of these four sets of biometric test documentation requirements.

Testers who are also required to document their testing in accordance with ISO/IEC/IEEE 29119-3 can use the mapping tables to see which clauses in in the software testing documentation standard map to the biometric test documentation requirements.

D.2.2 Mapping of ISO/IEC 19795-1:2021 documentation to ISO/IEC/IEEE 29119-3:2021 documentation

Table D.1 shows the mapping from test documentation requirements in ISO/IEC 19795-1:2021 to subclauses in ISO/IEC/IEEE 29119-3:2021, along with a brief description of the required test documentation.

Table D.1 — General test documentation mapping from ISO/IEC 19795-1:2021 to ISO/IEC/IEEE 29119-3:2021

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-1:2021 Required/Recommended/Optional test documentation (required unless stated)	
Reporting - General		
Test plan/ Context of testing (7.2.2)	12.1 The system(s) tested	Including details of: — algorithms evaluated; — biometric sensors; — user interface; — supporting hardware.
	12.1 Type of evaluation	— In the case of technology evaluation: details of the test corpus used. — In the case of scenario evaluation: details of the test scenario. — In the case of operational evaluation: details of the operational application.
Test plan/ Test strategy (7.2.7)	12.1 Size of evaluation	— Number of test subjects; — Number of instances (fingers, hands or eyes etc.) enrolled by each test subject; — Number of visits made by test subject; — Number of transactions per test subject (or test subject instance) at each visit;
	12.1 Test crew	— Demographics of the test crew (age, gender, etc.); — The manner in which the test crew was assembled, to include exclusions, volunteers etc., as well as the degree to which the test crew mirrored the target population. — The level of training, instruction, familiarization, and habituation of test crew in the use of the system.
	12.1 (referencing 8.3.2.1, 8.4.2, and C.2.6) Test environment	Enrolment and recognition environmental conditions
		Environmental influences including: — background — lighting level, direction or reflections — weather
	12.1 (referencing 7.3.7) Time separation between enrolment and recognition transactions	The time between the enrolment and recognition transactions (allows the effects of 'template ageing' to be considered). Typically measured in weeks, months or years.
	12.1 Quality and decision thresholds used during data collection	The thresholds used, and those recommended for the target application (if different).

Table D.1 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-1:2021 Required/Recommended/Optional test documentation (required unless stated)	
	12.1 (referencing 7.3 and Annex C) Control of factors potentially affecting performance	Population demographics, including: — age; — ethnic origin; — gender; — occupation.
		Application information, including: — time of day; — subject familiarity; — subject motivation.
		Capture subject anatomy, including: — beards and moustaches; — baldness; — disability, disease or illness; — eyelashes; — fingernail growth; — fingerprint condition; — iris colour intensity; — skin tone.
		Capture subject behaviour, including: — dialect, accent and native language; — expression, intonation and volume; — facial expressions; — language alphabet; — misspoken or misread phrases; — movement; — pose and positioning; — prior activity; — stress, tension, mood or distractions.

Table D.1 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-1:2021 Required/Recommended/Optional test documentation (required unless stated)	
		Capture subject appearance, including: — bandages or band-aids; — clothing; — contact lenses; — cosmetics; — glasses, sunglasses; — false fingernails; — hair style and colour; — rings; — tattoos.
		Sensor and hardware, including: — dirt smears (e.g. residual prints); — focus; — sensor quality; — sensor variations; — sensor wear; — sensor replacement; — transmission channel.
		User interface, including: — feedback; — instruction; — supervision.
	12.1 Test procedures	— E.g., policies for determining enrolment failures. — Details of any abnormal cases occurring during testing that are excluded from performance analysis.
Test completion report/ Summary of testing performed (7.4.2)	12.1 Estimated uncertainties (optional)	Estimated uncertainty in performance results, and method of estimation. See 8.11 and Annex B
Test completion report/ Deviations from planned testing (7.4.3)	12.1 Deviation from guidelines (optional)	Deviations from the guidelines of ISO/IEC 19795-1 “should” be explained. Sometimes it will be necessary to compromise one aspect to achieve another; for example, randomising the order of using fingers on a fingerprint device can lead to user confusion and a higher number of labelling errors

Table D.1 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-1:2021 Required/Recommended/Optional test documentation (required unless stated)	
Test plan/ Test strategy (7.2.7)	12.2 Single number summary statistics	Ideally single number summary statistics (e.g. Equal Error Rate (EER), Half Total Error Rate (HTER), Area under the ROC) "should" not be used. When used, report the method of derivation.
Reporting – Enrolment Performance		
Test plan/ Test strategy (7.2.7)	12.3 (referencing 9.2.1) Failure to enrol rate (FTER)	FTER Enrolment policy, including: — sample quality threshold for enrolment; — decision threshold to confirm the enrolment is usable; — the number of attempts or time allowed for enrolment in an enrolment transaction.
	12.3 (referencing 9.2.2) Enrolment transaction duration (optional)	Average (mean or median) transaction duration. Cumulative distribution function of enrolment transaction times (e.g. plotting FTE(duration) against duration) showing both successful and failed enrolments. — used for comparison of systems, where thresholds for time allowed or sample quality are not set the same for all systems.
	12.3 (referencing 9.10.2 a) Enrolment transaction computational workload (optional)	Each enrolment transaction is measured over: — generation of a biometric enrolment data record; — duplicate enrolment check (which corresponds to an identification search against existing enrolment references), if implemented; — storage in the reference database. Transaction computational workload includes: — transaction time; — memory usage; — optionally CPU usage, and network and disk activity.
Reporting - Acquisition Performance		
Test plan/ Test strategy (7.2.7)	12.4 (referencing 9.3.1) Failure-to-acquire rate (FTAR)	FTAR plus thresholds for sample quality. Either duration for sample acquisition or allowed number of presentations
	12.4 (referencing 9.3.2) Acquisition duration (optional)	Average (mean or median) transaction duration. Cumulative distribution as a function of acquisition duration (e.g. plotting FTAR(duration) against duration) — used for comparison of systems, where thresholds for sample quality and allowed duration for sample acquisition are not set the same for all systems.

Table D.1 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-1:2021 Required/Recommended/Optional test documentation (required unless stated)	
Reporting – 1:1 Comparison Performance		
Test plan/ Test strategy (7.2.7)	12.5 (referencing 9.4.1 and 9.4.2) False match rate (FMR) and False non-match rate (FNMR)	FMR FNMR plus threshold Otherwise, FMR and corresponding FNMR "shall" be reported over the range of decision thresholds tested. — A DET plot is recommended in the case of multiple operating points.
	12.5 Failure to enrol rate (FTER)	FTER Enrolment policy — sample quality threshold for enrolment — decision threshold to confirm the enrolment is usable — the number of attempts or time allowed for enrolment in an enrolment transaction OR a statement that FTER is unknown.
	12.5 Failure-to-acquire rate (FTAR)	FTAR plus thresholds for sample quality Either duration for sample acquisition or allowed number of presentations OR a statement that FTAR is unknown.
	12.5 Computational workload of biometric comparison (optional)	Computational workload (e.g. CPU operations, memory used)
Test completion report/ Summary of testing performed (7.4.2)	8.4.2 Collection conditions (recommended)	If the presentation and channel effects are allowed to vary randomly across test subjects the experimenter "should" report on any correlation in these effects between enrolment and comparison sessions.

Table D.1 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-1:2021 Required/Recommended/Optional test documentation (required unless stated)	
Reporting - Verification System Performance		
Test plan/ Test strategy (7.2.7)	12.6 (referencing 9.5.2 and 9.5.3) False accept rate (FAR) and False reject rate (FRR)	FAR plus: — decision policy — matching decision threshold — threshold for sample quality — allowed duration or allowed number of presentations FRR plus: — decision policy — matching decision threshold — threshold for sample quality Otherwise, FAR and corresponding FRR "shall" be reported over the range of decision thresholds tested. A DET plot is recommended in the case of multiple operating points.
	12.6 Failure to enrol rate (FTER)	FTER Enrolment policy — sample quality threshold for enrolment — decision threshold to confirm the enrolment is usable — the number of attempts or time allowed for enrolment in an enrolment transaction OR a statement that FTER is unknown.
	12.6 Failure-to-acquire rate (FTAR)	FTAR plus thresholds for sample quality Either duration for sample acquisition or allowed number of presentations OR a statement that FTAR is unknown.
	12.6 (referencing 9.5.4) Verification transaction duration (optional)	Average (mean or median) transaction duration. Cumulative distribution as a function of acquisition times (e.g. plotting FRR(duration) against duration) "should" be provided showing separately accepted and rejected verification durations — used for comparison of systems, where thresholds for sample quality and allowed duration for sample acquisition are not set to the same values.

Table D.1 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-1:2021 Required/Recommended/Optional test documentation (required unless stated)	
	12.6 (referencing 9.5.5) Generalized false accept rate (GFAR) and Generalized false reject rate (GFRR) (optional)	The method of generalisation. GFAR and GFRR — recommended when comparing systems having different FTER / FTAR error rates.
	12.6 (referencing 9.10.2 b) Computational workload of verification (optional)	Computational workload (e.g. CPU operations, memory used)
Reporting - Identification System Performance		
Test plan/ Test strategy (7.2.7)	12.7 (referencing 9.6.2 and 9.6.3) False-positive identification rate (FPIR) and False-negative identification rate (FNIR)	FPIR FNIR — both reported over the range of decision thresholds and identification ranks tested. — DET plot is recommended in the case of multiple operating points. Several DET plots "may" be shown corresponding to different numbers of identifiers returned, and different number of references in the enrolment database.
	12.7 Number of enrolled references	Enrolled references
	12.7 Failure to enrol rate (FTER)	FTER Enrolment policy — sample quality threshold for enrolment — decision threshold to confirm the enrolment is usable the number of attempts or time allowed for enrolment in an enrolment transaction OR a statement that FTER is unknown.
	12.7 Failure-to-acquire rate (FTAR)	FTAR plus thresholds for sample quality Either duration for sample acquisition or allowed number of presentations OR a statement that FTAR is unknown.

Table D.1 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-1:2021 Required/Recommended/Optional test documentation (required unless stated)	
	12.7 (referencing 9.6.5) Selectivity	Selectivity
	12.7 (referencing 9.6.6) Closed-set results (optional)	CMC plot (e.g. the rank-R identification rate as a function of R) OR FNIR-over-rank plot — with details of the number of enrolled subjects
	12.7 (referencing 9.9) Identification transaction duration (optional)	Average (mean or median) transaction duration Cumulative distribution function of acquisition times Brief listing of the actions of the capture subjects included in the transaction
	12.7 (referencing 9.10.2 c) and 9.10.4) Computation workload for an identification transaction (optional)	Each enrolment transaction is measured over: — Generation of a biometric feature set from the captured biometric sample — Pre-selection to reduce workload of identification search if it implemented — Identification search over the reference database — Production of candidate list and deciding identification outcome Computational workload "may" be measured for different numbers of references to show how workload scales with database size. Where workload reduction is used, metrics applicable to the workload reduction method, "should" be reported (e.g. in the case of pre-selection, the preselection error rate, and penetration rate "should" be reported).

D.2.3 Mapping of ISO/IEC 19795-2:2007 documentation to ISO/IEC/IEEE 29119-3:2021 documentation

Table D.2 shows the mapping from test documentation requirements for technology evaluation in ISO/IEC 19795-2:2007 to subclauses in ISO/IEC/IEEE 29119-3:2021, along with a brief description of the required test documentation.

Table D.2 — Technology evaluation documentation mapping from ISO/IEC 19795-2:2007 to ISO/IEC/IEEE 29119-3:2021

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-2:2007 Required/Recommended content (required unless stated)	
	6.1.3 Functionality to be tested	Types of comparison functionality (i.e. verification or identification) with rationale;
	6.1.7 Model testing	Model documentation, if a model is tested instead of actual implementation.

Table D.2 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-2:2007 Required/Recommended content (required unless stated)	
Test plan/ Context of testing (7.2.2)	6.4.2.1 Specifications	Acquisition devices: — manufacturer; — model; — version; — firmware, as applicable. Comparison algorithms: — provider; — version; — revision. Test platform information: — platform; — OS; — processing power; — memory; — manufacturer; — database type; — database size; — model.
	6.4.3.1 Architecture	Including: — biometric data acquisition, processing, and storage architecture; — data flow between system components.
	8.3 Basis for inclusion of test systems	Including: basis of inclusion of test items in the evaluation (e.g. open invitation, supplier contract, etc.) and selection criteria, where applicable.
	6.4.3.3 System acquisition and implementation	Including: — method of system acquisition — level of supplier involvement in implementation
Test plan/ Stakeholders (7.2.4)	8.1 Parties to a test	Including: — level of tester independence; — involvement of test organization in the configuration, modification, refinement, or adaptation of the implementation under test.
	6.2.2 Unique enrolment	Processes used to ensure samples are of different people.

Table D.2 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-2:2007 Required/Recommended content (required unless stated)	
Test plan/ Test strategy (7.2.7)	6.2.4 Test subject identification	Including: — identifier types used for test subjects; — amount and type of personal data collected.
	6.2.5 Corpus metadata	Metadata made available to the systems under test (e.g. sensor settings).
	6.2.6 Corpus representativeness	Including: — data suitability for test goals and application type; — information on test subject acclimatization, training, habituation, and guidance, where available.
	6.2.7 Supplier access	Information on access to and use of the corpus by suppliers.
	6.2.9 Corpus validation	Validation of data and its suitability for the test/application (including proportion and criteria for data removal).
	6.2.10 Corpus collection environment	Environmental conditions (e.g. temperature) during corpus acquisition (otherwise unavailability of these environmental conditions).
	6.2.11 Corpus pre-processing	Information on data pre-processing, including the failure at source (FAS) rate if samples were discarded.
	6.4.3 Data collection	Including: — data recording methods for each performance element, including those not logged by the system(s); auditing and validation processes for performance data, including those not logged by the system(s).
	6.4.3.2 Outputs	Including: — output types, including comparison scores, accept/reject decisions, candidate lists, enrolment quality scores, sample quality scores — range of comparison scores and thresholds — range of enrolment quality scores and thresholds — range of sample quality scores and thresholds — method for providing outputs
	6.1.8 Sequential use	The order of use of the test data.
	8.2 Fairness	Whether systems were tested on equivalent hardware and operating systems or whether images of the operating system were re-installed prior to each test (recommended).
	6.4.4.1 Disclosures	Including: — description of sample-related data provided to suppliers; — input, intermediate, and output material to be made available to non-suppliers (amount disclosed depends on level of disclosure).

Table D.2 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-2:2007 Required/Recommended content (required unless stated)	
Test completion report/ Summary of testing performed (7.4.2)	6.4.5 Executive summary	Executive summary of testing performed.
	6.4.1 Evaluation results.	Evaluation results.
	6.3.6.2 Test results/ evaluation and performance results	Including: — mean throughput, if calculated; — time for 1:N uniqueness determination (as part of throughput time), if it is observed or known to be implemented.
Test completion report/ Deviations from planned testing (7.4.3)	6.4.1 Evaluation results.	Unaddressed requirements and the reason.
test execution log (8.10)	6.4.3 Data collection	Data collection spreadsheets and logs, whether as screenshots or reproduced forms.
	8.2 Fairness	Intellectual or physical input by the test organization that affects the evaluation outcome.

D.2.4 Mapping of ISO/IEC 19795-2:2007 (scenario evaluation) documentation to ISO/IEC/IEEE 29119-3:2021 documentation

Table D.3 shows the mapping from test documentation requirements for scenario evaluation in ISO/IEC 19795-2:2007 to subclauses in ISO/IEC/IEEE 29119-3:2021, along with a brief description of the required test documentation.

Table D.3 — Scenario evaluation documentation mapping from ISO/IEC 19795-2:2007 to ISO/IEC/IEEE 29119-3:2021

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-2:2007 Required/Recommended content (required unless stated)	
	7.1.1.1 System under test	Specification of application being scenario tested
		Acquisition devices: — manufacturer; — model; — version; — firmware, as applicable. Comparison algorithms: — provider; — version; — revision.

Table D.3 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-2:2007 Required/Recommended content (required unless stated)	
Test plan/ Context of testing (7.2.2)	7.4.2.2 Specifications	Biometric application software: — provider; — title; — version; — build of application. Test platform information — platform; — OS; — processing power; — memory; — manufacturer; — model.
	7.4.2.3 Architecture	Including: — biometric data acquisition, processing, and storage architecture; — data flow between system components.
	8.3 Basis for inclusion of test systems	Including: — basis of inclusion of test items in the evaluation (e.g. open invitation, supplier contract, etc.) and selection criteria, where applicable.
	7.4.3 System acquisition and implementation	Including: — method of system acquisition; — level of supplier involvement in implementation.
Test plan/ Stakeholders (7.2.4)	8.1 Parties to a test	Including: — level of tester independence; — involvement of test organization in the configuration, modification, refinement, or adaptation of the implementation under test.
Test plan/ Test strategy (7.2.7)	7.4.2.4 Outputs	Including: — output types, including comparison scores, accept/reject decisions, candidate lists, enrolment quality scores, sample quality scores; — range of comparison scores and thresholds; — range of enrolment quality scores and thresholds; — range of sample quality scores and thresholds; — method for providing outputs.
	7.1.1.3 Evaluation environment	Test environment - indoor (type of facility) or outdoor (exposure to elements).

Table D.3 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-2:2007 Required/Recommended content (required unless stated)	
	7.1.2.2 Test subject training	Including: — extent and method of training provided to test subjects; — use of supplier-provided scripts, instructions, or other training tools.
	7.2.3 Test crew composition	Age/gender distribution of test crew.
	7.4.4 Physical layout of test environment	Including: — area dedicated to scenario testing; — natural and artificial lighting; — positioning of acquisition devices; — relative location of each system; — photos showing the positions of devices and test subjects during testing;
	8.2 Fairness	Whether systems were tested on equivalent hardware and operating systems or whether images of the operating system were re-installed prior to each test (recommended).
Test completion report/ Summary of testing performed (7.4.2)	7.4.5 Executive summary	Executive summary of testing performed.
	7.2.2	Error rates based on the level of habituation of test subjects (recommended).
	7.4.1 Evaluation results.	Evaluation results.
Test completion report/ Deviations from planned testing (7.4.3)	7.4.1 Reporting - General	Including: — out of scope or inapplicable test requirements; — unaddressed test requirements due to unavailable data.
Test model specification/ Test model (8.2.6)	7.1.3.3 Reference adaptation	Including: — accommodation of reference adaptation, where it occurs (recommended); — proportions of genuine and impostor recognition, where adaptation occurred (recommended).
test procedure specification/ Start up (8.4.5)	7.1.2.1 Test information and general test instructions	Instructions and training provided to test subjects.
	7.1.2.4 Guidance	Policies on providing guidance to test subjects.
	7.2.2 Habituation	Method of habituation of test crew.
	7.1.2.4 Guidance	Where operator guidance exceeds an agreed level;

Table D.3 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-2:2007 Required/Recommended content (required unless stated)	
test execution log (8.10)	7.1.2.5 Test order and acclimatization	Observed effects of ordering systems in a multi-system test.
	7.1.6 Data collection	Data collection spreadsheets and logs, whether as screenshots or reproduced forms.
	8.2 Fairness	Intellectual or physical input by the test organization that affects the evaluation outcome.

D.2.5 Mapping of ISO/IEC 19795-6:2012 (operational evaluation) documentation to ISO/IEC/IEEE 29119-3:2021 documentation

Table D.4 shows the mapping from test documentation requirements for operational evaluation in ISO/IEC 19795-6:2012 to subclauses in ISO/IEC/IEEE 29119-3:2021, along with a brief description of the required test documentation.

Table D.4 — Operational evaluation documentation mapping from ISO/IEC 19795-6:2012 to ISO/IEC/IEEE 29119-3:2021

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-6:2012 Required/Recommended content (required unless stated)	
		Acquisition devices: manufacturer; model; version; firmware, as applicable. Biometric algorithms: provider; version; revisions; parameter settings.

Table D.4 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-6:2012 Required/Recommended content (required unless stated)	
Test plan/ Context of testing (7.2.2)	6.1.3 System specification (all recommended)	Biometric application software: provider; title; version; build of application. Biometric system architecture: biometric data acquisition, processing, and storage architecture; data flow between system components; system configuration (e.g. whether reference updating is used) Test platform information platform; OS; processing power; memory; manufacturer; model.
	6.1.4 Biometric functionality	Rationale for the types of comparison functionality (i.e. enrolment, verification, or identification).
	6.2.2 Concept of operations	The concept of operations of the operational application, including: integration with external systems; authentication methods and systems that the biometric system is replacing or complementing; category of application (e.g. enrolment, physical or logical access control, identification).
	6.4.2 Enrolment analysis	Whether enrolment is in the scope of the testing.
	6.5.1 Reporting planned test results	Including: purpose and scope of the evaluation including description of the system under test; performance values to be measured in the evaluation, including estimation of statistical significance of these results; description of the application's characteristics.
Test plan/ Assumptions and constraints (7.2.3)	6.2.4 Levels of effort and decision policies	Including: enrolment attempt limits and decision policies. comparison attempt limits and decision policies.
	6.2.5 Multiple-instance systems	Including: whether multiple instances from same test subject are used; if so, the fusion techniques/methods used (recommended).

Table D.4 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-6:2012 Required/Recommended content (required unless stated)	
Test plan/ Test strategy (7.2.7)	6.2.6 Environment	Including: environmental conditions controlled by the operational system; environmental controls not applied in the field; area dedicated to operational testing (recommended); positions of natural and artificial lighting (recommended); positioning of acquisition devices (recommended).
	6.3.1 Test plan - general 6.3.2 System implementation and configuration	Including: required instrumentation and reconfiguration of the system; impact on performance attributable to the instrumentation and reconfiguration; scores recorded and/or output by the biometric system, including comparison scores, acceptance and rejection decisions, candidate lists, enrolment quality scores, and sample quality scores and the threshold values used for testing; methods used to record outputs from the biometric system during testing.
	6.3.1 Test plan - general 6.3.3 Test population	Including: relationship between test subjects and the biometric system operator; whether the test subjects normally use the system or just for this testing; representativeness of the test crew with the target population; identifier types used for test subjects; methods used to establish ground truth (and the impact of these on test subject interaction with the system); method used to determine the order in which test subjects interact with multiple components/systems; amount and type of demographic data on test crew to be collected; actual demographics of the test crew (recommended);
	6.3.4.1 Test transactions - General	Target number of transactions to be executed.
	6.3.4.2 Data recording processes	Including: methods used for recording data for each performance element; how test subject interaction with the system is recorded; processes for auditing and validating performance data collection; criteria for excluding transaction data from performance analysis.
	6.3.4.3 Genuine transactions 6.3.4.4 Impostor transactions	Methods used to confirm the identity of test subjects executing “genuine” and “impostor” transactions.

Table D.4 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-6:2012 Required/Recommended content (required unless stated)	
	6.4.1 Throughput	Including: throughput metrics and methods for measuring transaction times; separate measures for transaction durations for enrolled and un-enrolled subjects (recommended).
Test procedure specification/ Start up (8.4.5)	6.2.3 Guidance and instruction	Including: whether system is run as attended or unattended operation; guidance given to test subjects on how to use the system; type and extent of feedback provided to test subjects (by biometric system and by attendants); correction and recording of improper interaction with device; constraints on test subject appearance and apparel; differences in test guidance and feedback from that provided for operational use.
	6.2.8 Acclimatization	Method of acclimatization of the test crew, and justification if it differs from operational use.
	6.2.9 Habituation	Method of habituation of the test crew.
Test completion report/ Deviations from planned testing (7.4.3)	6.3.4.1 Test transactions - General	Including: discrepancies in generating transactions for genuine and impostor test transactions (recommended); modifications to system interaction introduced during the testing.
	6.5.1 Reporting planned test results	Including: deviations from the test plan; out of scope or inapplicable test requirements; unaddressed test requirements due to unavailable data.
	6.5.2 Reporting additional analyses	Reports of additional analyses not in the test plan, including potential biases in their results (recommended).
Test completion report/ Factors that blocked progress (7.4.5)	6.3.4.1 Test transactions - General	Unplanned events that are likely to have affected or invalidated the results (e.g. fire drills, repairs), and the decision on whether to include such transaction data.
	6.5.1 Reporting planned test results	Unaddressed test requirements due to unavailable data.

Table D.4 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-6:2012 Required/Recommended content (required unless stated)	
Test completion report/ Test measures (7.4.6)	6.3.4.1 Test transactions - General	Including: number of transactions executed; frequency the test subjects execute transactions.
	6.3.4.2 Data recording processes	Including metrics that were generated through automated data collection and those which were generated through manual data collection.
	6.4.2 Enrolment analysis	Throughput for enrolment transactions.
	6.5.3 Reporting observations	Statistical estimates of validity of reported observations (recommended).
Test model specification/ Test model (8.2.6)	6.4.2 Enrolment analysis	Including: number of test subjects and transactions used to derive throughput for enrolment; failure-to-enrol rate, and number of test subjects and transactions used to derive the failure-to-enrol rate; the proportion of the test subjects utilizing pre-existing enrolments; if enrolment is not performed by the system under test, information on the test subjects' prior enrolment, if available (recommended).
	6.4.3 Recognition analysis	Including: throughput for recognition transactions, and the number of test subjects and recognition transactions used to derive it; for verification: system rejection rate, and the number of test subjects and recognition transactions used to derive it; where ground truth is available, false reject rate (FRR) and false accept rate (FAR) and the number of test subjects, recognition transactions and number of enrolled individuals used to derive them; for identification: the system identification rate, and the number of test subjects, identification transactions and enrolled individuals used to derive it; where ground truth is available: false positive identification rates (FPIR) and corresponding false negative identification rates (FNIR) and the number of test subjects, recognition transactions and number of enrolled individuals used to derive them; for genuine identification transactions, distribution of the time between acquisition of enrolment and comparison data.

Table D.4 *(continued)*

ISO/IEC/IEEE 29119-3:2021 Test documentation	ISO/IEC 19795-6:2012 Required/Recommended content (required unless stated)	
Test completion report/ Summary of testing performed (7.4.2)	6.3.4.4 Impostor transactions	Impostor activity that can be estimated or measured (recommended).
	6.4.3.2 Recognition error rate analysis	Statistical significance of test results based on the number of errors, error rates, test population, and number of transactions executed.
	6.5.1 Reporting planned test results	Performance values measured in the evaluation, including estimation of statistical significance of these results.
Test execution log (8.10)	6.3.4.2 Data recording processes	Examples of data collection elements such as spreadsheets and logs.
	6.5.3 Reporting observations	Reported observations during the evaluation.
	6.6 Record keeping	Including: photos of the operational environment showing the relative positions of devices and subjects during testing; communications with suppliers on system configuration and operation; spreadsheets and matrices used for data entry; if all three points above are not recorded, this is documented, with an indication if this was for privacy.

Annex E
(informative)

Mapping from ISO/IEC 19795-1 to the ISO/IEC/IEEE 29119 series

E.1 General

This mapping shows how the requirements of ISO/IEC 19795-1 relate to the requirements of the ISO/IEC/IEEE 29119 series. The main purpose of the mapping is to allow users of ISO/IEC 19795-1 to understand how biometric performance testing and reporting principles and framework can be applied, while also complying with, or simply using, where appropriate, the more detailed requirements of the ISO/IEC/IEEE 29119 series of software testing standards.

E.2 Overview of ISO/IEC 19795-1

ISO/IEC 19795-1 specifies the generic requirements and practices concerned with the scientific "technical performance testing" of biometric systems and devices. Technical performance measures are defined that are generally applicable to all biometric systems and devices. Modality-specific technical performance tests are not considered in ISO/IEC 19795-1.

E.3 Conformance requirements of ISO/IEC 19795-1

To conform to ISO/IEC 19795-1, biometric performance testing is performed in accordance with the mandatory requirements defined in ISO/IEC 19795-1:2021, Clauses 7 to 12.

Conformance requirements change for the two evaluation approaches covered by ISO/IEC 19795-1 (technology and scenario). The requirements are also dependent on the comparison type of the system being evaluated (i.e. identification and verification systems). The relevant clauses are shown in Table E.1.

E.4 Mapping

Table E.1 shows the mapping from subclauses in ISO/IEC 19795-1:2021 to subclauses in ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021, along with the rationale for each mapping.

Table E.1 — Mapping from ISO/IEC 19795-1:2021 to the ISO/IEC/IEEE 29119 series

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 General biometric system 6.1 Conceptual representation of general biometric system	N/A	Description of a generic biometric system.
6 General biometric system 6.2 Conceptual components of a general biometric system 6.2.1 Data capture subsystem	N/A	Description of a generic biometric subsystem.
6 General biometric system 6.2 Conceptual components of a general biometric system 6.2.2 Transmission subsystem	N/A	Description of a generic biometric subsystem.
6 General biometric system 6.2 Conceptual components of a general biometric system 6.2.3 Signal processing subsystem	N/A	Description of a generic biometric subsystem.
6 General biometric system 6.2 Conceptual components of a general biometric system 6.2.4 Data storage subsystem	N/A	Description of a generic biometric subsystem.
6 General biometric system 6.2 Conceptual components of a general biometric system 6.2.5 Comparison subsystem	N/A	Description of a generic biometric subsystem.
6 General biometric system 6.2 Conceptual components of a general biometric system 6.2.6 Decision subsystem	N/A	Description of a generic biometric subsystem.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 General biometric system 6.2 Conceptual components of a general biometric system 6.2.7 Administration subsystem	N/A	Description of a generic biometric subsystem.
6 General biometric system 6.2 Conceptual components of a general biometric system 6.2.8 Interface to external application	N/A	Description of a generic biometric system interface options.
6 General biometric system 6.3 Functions of general biometric system 6.3.1 Enrolment	N/A	Description of a generic biometric system function.
6 General biometric system 6.3 Functions of general biometric system 6.3.2 Verification of a positive biometric claim	N/A	Description of a generic biometric system function.
6 General biometric system 6.3 Functions of general biometric system 6.3.3 Identification	N/A	Description of a generic biometric system function.
6 General biometric system 6.4 Enrolment, verification and identification transactions	N/A	Description of generic biometric system transaction approaches.
6 General biometric system 6.5 Performance measures 6.5.1 Error rates	N/A	Description of error rates in generic biometric systems.
6 General biometric system 6.5 Performance measures 6.5.2 Throughput rates 6.5.2.1	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4)	ISO/IEC 19795-1 recommends that measurement of throughput "should" take account of additional actions which can vary depending on the biometric system result (e.g. opening doors, proceeding through gates). Mainly, the transaction being measured needs to be clearly understood – e.g. in terms of how throughput rates change as number of stored references increases.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 General biometric system 6.5 Performance measures 6.5.2 Throughput rates 6.5.2.2	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends that the subject's complete transaction with the system is precisely defined to ensure the transaction initiation and termination are clearly understood. For instance, throughput can be based on sample acquisition alone, or multiple recognition attempts. This "should" be documented prior to the test (i.e. test design) and recorded in the test report.
6 General biometric system 6.5 Performance measures 6.5.3 Types of performance evaluation	N/A	ISO/IEC 19795-1 contains no mandatory ("shall") statements here but does state that "the actual testing needs to be done on data that has not previously been seen by algorithm developers" for technology evaluation.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Planning the evaluation 6.1 General 6.1.1	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b), c). 7.2.4.6 Design test strategy (TP5) a), b), c), d). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.4 Test basis ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.1 General	Both standards require test planning activities at the start of an evaluation. ISO/IEC 19795-1 expects this to result in a 'test protocol', while ISO/IEC/IEEE 29119-2 requires this to be documented in a test plan.
7 Planning the evaluation 7.1 General 7.1.2	N/A	This clause in ISO/IEC 19795-1 appears to be suggesting optional recording of differences in different biometric evaluations. As such there is no requirement and it seems to be more an aide memoire.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Planning the evaluation 7.1 General 7.1.3	N/A	ISO/IEC 19795-1 is specifying scope – stating that it covers basic principles and other parts cover more specific evaluations.
7 Planning the evaluation 7.2 Determine information about the system	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) c), e). ISO/IEC/IEEE 29119-2 7.3 Test monitoring and control process 7.3.4 Activities and tasks 7.3.4.2 Set-Up (TMC1) a), c). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.1 General	Data collection during testing is specified in more detail in ISO/IEC 19795-1. This clause also covers the test environment (e.g. system modifications for testing).
7 Planning the evaluation 7.3 Controlling factors that influence performance		
7 Planning the evaluation 7.3 Controlling factors that influence performance 7.3.1	N/A	Guidance on factors affecting performance.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Planning the evaluation 7.3 Controlling factors that influence performance 7.3.2	N/A	Requirement to classify factors that influence performance is not part of the ISO/IEC/IEEE 29119 series.
7 Planning the evaluation 7.3 Controlling factors that influence performance 7.3.3	N/A	Guidance on comparing algorithms.
7 Planning the evaluation 7.3 Controlling factors that influence performance 7.3.4	N/A	Recommendation to perform scenario testing on a real-world application.
7 Planning the evaluation 7.3 Controlling factors that influence performance 7.3.5	N/A	No requirement – just a statement that operational testing is confined to the operational system.
7 Planning the evaluation 7.3 Controlling factors that influence performance 7.3.6	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) e).	No requirement – but ISO/IEC 19795-1 states that adjustment to the devices and environment (including quality and decision thresholds) need to take place before testing.
7 Planning the evaluation 7.3 Controlling factors that influence performance 7.3.7	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d).	ISO/IEC 19795-1 requires that biometric probes and their mated biometric references be collected some time apart, ideally matching the expected interval in operation – a requirement on the test data.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Planning the evaluation 7.4 Test subject selection	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a), b), d).	ISO/IEC 19795-1 provides detailed instructions on the test inputs (in the form of test subjects). "The experimenter shall consider test subject engagement as part of test design." It also states that activities to implement the test design (e.g. instructions to test subjects) "should" be performed – and that test data requirements such as following data privacy regulations "shall" be followed.
7 Planning the evaluation 7.5 Test size 7.5.1 General	N/A	Introduction to test size and statistics with regards to evaluating biometric systems.
7 Planning the evaluation 7.5 Test size 7.5.2 Collecting multiple recognition transactions per test subject per system	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a).	ISO/IEC 19795-1 recommendations on number of transactions per test subject. This would be part of test design in ISO/IEC/IEEE 29119-2; hence the test design techniques are specified as part of the test strategy and the test coverage items correspond to the level of coverage per subject and transactions.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Planning the evaluation 7.5 Test size 7.5.3 Requirements on test size	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a).	Test size requirements from ISO/IEC 19795-1 correspond to specifying test strategy (in test design area) and test design and implementation in ISO/IEC/IEEE 29119-2.
7 Planning the evaluation 7.6 Multiple tests	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	The first clause (6.6.1) provides guidance on problems with technology evaluation and using a single corpus. The second clause (6.6.2) provides recommendations on how to use test subjects to test multiple systems, such as randomizing the order in which subjects use different systems (test design).

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.1 Avoidance of data collection errors 8.1.1	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	ISO/IEC 19795-1 requires great care to be taken in data collection and entry. In ISO/IEC/IEEE 29119-2 this can be required in the test strategy and implemented in the derivation of test cases.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.1 Avoidance of data collection errors 8.1.2	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a), d), e). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	ISO/IEC 19795-1 requires test data input to minimize manual data entry and be checked. This would be required as part of the test strategy and implemented as part of test case design in ISO/IEC/IEEE 29119-2. ISO/IEC 19795-1 also recommends automated logging and the saving of biometric samples, which would be implemented as a result of test environment requirements in the test strategy. ISO/IEC 19795-1 requires all excluded test inputs to be reported (and these must be against documented exclusion criteria). Such exclusion would be specified as part of the test data requirements and implemented as part of the test procedures.
8 Data collection 8.2 Data and details collected 8.2.1	N/A	ISO/IEC 19795-1 recommends that biometric systems "should" automatically log all enrolment, verification, and identification attempts, etc. This, however, is not a testing requirement and so not applicable to the ISO/IEC/IEEE 29119 series.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.2 Data and details collected 8.2.2	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	ISO/IEC 19795-1 requires close supervision on online tests where no logging is available. This would be required in the test strategy and implemented as part of the test procedures.
8 Data collection 8.2 Data and details collected 8.2.3	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	ISO/IEC 19795-1 requires systems that cannot return a comparison score to be evaluated using online tests with a range of 'security settings'. This would be required in the test strategy and implemented as part of the test procedures.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.2 Data and details collected 8.2.4	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a), b), d). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	ISO/IEC 19795-1 states that the test data requirements, such as following data privacy regulations, "shall" be followed.
8 Data collection 8.3 Enrolments 8.3.1 Enrolment transactions 8.3.1.1	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	Enrolment is a test action that would be described in the test procedure.
8 Data collection 8.3 Enrolments 8.3.1 Enrolment transactions 8.3.1.2	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a).	The decision to allow a subject to enrol with different biometric instances would be part of test design (more coverage items) and result from a requirement in the test strategy.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.3 Enrolments 8.3.1 Enrolment transactions 8.3.1.3	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	ISO/IEC 19795-1 recommends that any smoke tests of the matching algorithm "should" not be documented as part of the evaluation. In this respect these tests can be considered as preconditions on the testing and can be included as the initial part of the test procedure.
8 Data collection 8.3 Enrolments 8.3.2 Enrolment conditions	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) e). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1)	Enrolment conditions in this context relate to the test environment used for enrolment. Basically, ISO/IEC 19795-1 recommends a test environment that is representative of the target environment. These test environment requirements would be specified as part of the test strategy and implemented as part of the Test environment and data management process.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.3 Enrolments 8.3.3 Enrolment failures and presentation errors 8.3.3.1	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) e). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	Tuning of acceptance criteria for quality control modules would be part of test environment set-up. Actions on what to do in the event of an enrolment failure would be part of the relevant test procedures.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.3 Enrolments 8.3.3 Enrolment failures and presentation errors 8.3.3.2	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Test execution in ISO/IEC/IEEE 29119-2 includes recording of test execution and the test completion report includes test results.
8 Data collection 8.3 Enrolments 8.3.3 Enrolment failures and presentation errors 8.3.3.3	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4.4 Record test execution (TE3) a).	Test execution in ISO/IEC/IEEE 29119-2 includes recording of test execution including anomalous events.
8 Data collection 8.3 Enrolments 8.3.3 Enrolment failures and presentation errors 8.3.3.4	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4.4 Record test execution (TE3) a).	Test execution in ISO/IEC/IEEE 29119-2 includes recording of test execution including anomalous events.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.1 General 8.4.1.1	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.1 General	Test strategy and design (test coverage) would implement the requirements for representative test subjects.
8 Data collection 8.4 One-to-one comparison trials 8.4.1 General 8.4.1.2	N/A	ISO/IEC 19795-1 provides information on the difference between mated and non-mated trials.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.1 General 8.4.1.3	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a)	Test strategy and design (test coverage) would implement the requirements for representative test subjects and no deliberate non-mated use of test subjects.
8 Data collection 8.4 One-to-one comparison trials 8.4.1 General 8.4.1.4	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a).	ISO/IEC 19795-1 provides high-level requirements on how testing will be performed, suitable for inclusion in the organizational test practices.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.2 Collection conditions	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a), e). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements	Collection conditions in this context relate to the test environment used for comparison trials. These test environment requirements would be specified as part of the test strategy and implemented as part of the Test environment and data management process. The collection process would be specified as part of the test strategy.
8 Data collection 8.4 One-to-one comparison trials 8.4.3 Frequency of use	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	Frequency of use by test subjects is part of test design that would be incorporated in test procedures.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.4 Systems performing optimisation based on enrolled references	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	Normalisation is part of the system functionality being tested, and so would be part of the test design, described in test cases and/or test procedures.
8 Data collection 8.4 One-to-one comparison trials 8.4.5 Systems performing reference adaptation	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) e). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements	Reference adaptation, as described here by ISO/IEC 19795-1, can be considered part of the set-up of the test environment.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.6 Processes for data entry errors and system misuse	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-3 8.10 Test execution Log 8.10.1 Overview	Any unusual activities during test execution would be recorded in the test log.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.7 Failures to acquire	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) e). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-3 8.10 Test execution Log 8.10.1 Overview	Tuning of acceptance criteria for quality control modules would be part of test environment set-up. Actions on what to do in the event of a capture failure would be part of the relevant test procedures and would normally be captured in the test log.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.8 Adding test data to the corpus	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 8.10 Test execution log 8.10.1 Overview	Test execution in ISO/IEC/IEEE 29119-2 includes recording of test execution and the test completion report includes test results.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021		ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8	Data collection	ISO/IEC/IEEE 29119-2	ISO/IEC 19795-1 provides requirements on the design of online comparison trials in terms of test coverage and the recording of results.
8.4	One-to-one comparison trials	8.2 Test design and implementation process	
8.4.9	Online comparison trials	8.2.4.3 Identify test coverage items (TD2) a).	
		ISO/IEC/IEEE 29119-2	
		8.4 Test execution process	
		8.4.4.4 Record test execution (TE3) a).	
		ISO/IEC/IEEE 29119-3	
		8.10 Test execution log	
		8.10.1 Overview	

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.10 Offline comparison trials	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) e). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) Part3 8.8 Test environment readiness report 8.8.3 Description of status	ISO/IEC 19795-1 largely covers test design (and coverage) in this clause, with some requirements on the test environment.
8 Data collection 8.4 One-to-one comparison trials 8.4.11 Offline non-mated comparison trials when references are dependent	N/A	ISO/IEC 19795-1 provides informative guidance on the jack-knife approach to the offline non-mated comparison trials when references are dependent.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.4 One-to-one comparison trials 8.4.12 Offline non-mated comparison trials based on comparison of references	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	ISO/IEC 19795-1 provides requirements (constraints) on the test design (coverage/test cases) for the offline non-mated comparison trials based on comparison of references.
8 Data collection 8.4 One-to-one comparison trials 8.4.13 Use of samples from multi-capture comparison transactions	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	ISO/IEC 19795-1 provides requirements for test design of multi-capture comparison transactions.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.5 Identification trials 8.5.1 General	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.1 General	ISO/IEC 19795-1 requires trials (tests) to be designed in the same general way for comparison trials, with some additional recommendations on test recording (only this is included for the mapping to the ISO/IEC/IEEE 29119 series as the 'general way' is rather vague to map).

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Data collection 8.5 Identification trials 8.5.2 Identification testing with non-enrolled test subjects	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks e). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1)	ISO/IEC 19795-1 includes requirements for test design and test environment for identification testing with non-enrolled test subjects.
8 Data collection 8.5 Identification trials 8.5.3 Use of Jack-knife approach for identification testing	N/A	ISO/IEC 19795-1 provides informative guidance on the jack-knife approach to the offline non-mated comparison trials when references are dependent.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.1 General	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) c) ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	This clause from ISO/IEC 19795-1 is largely informative, but with a requirement to report any weighting of the test crew is used to address representativeness.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.2 Performance of biometric enrolment 9.2.1 Failure-to-enrol rate	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) b). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Defines the failure-to-enrol rate. So, includes recording and reporting of test results.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.2 Performance of biometric enrolment 9.2.2 Enrolment transaction duration	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends that enrolment transaction duration "should" be measured and reported. Thus, this recommendation would need to be part of test design, recording and reporting.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.3 Performance of biometric acquisition 9.3.1 Failure-to-acquire rate	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) b). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Defines the failure-to-acquire rate. So, includes recording and reporting of test results.
9 Analyses 9.3 Performance of biometric acquisition 9.3.2 Acquisition process duration	N/A	ISO/IEC 19795-1 provides informative guidance on comparing acquisition duration of systems.
9 Analyses 9.3 Performance of biometric acquisition 9.3.3 Other aspects of acquisition performance	N/A	ISO/IEC 19795-1 provides informative guidance on measuring causes of acquisition failure and segmentation accuracy.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.4 One-to-one comparison performance 9.4.1 False non-match rate	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) b). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Defines the false non-match rate. So, includes recording and reporting of test results.
9 Analyses 9.4 One-to-one comparison performance 9.4.2 False match rate 9.4.2.1	N/A	ISO/IEC 19795-1 provides an informative description of the false match rate.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.4 One-to-one comparison performance 9.4.2 False match rate 9.4.2.2	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) b). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Recommends what to report on the false match rate. So, includes recording and reporting of test results. Strangely, the requirement to quote false non-match rate along with the false match rate (in 8.4.1.2), is stated as a recommendation in 8.4.2.2.
9 Analyses 9.4 One-to-one comparison performance 9.4.2 False match rate 9.4.2.3	N/A	ISO/IEC 19795-1 provides informative guidance on the jack-knife approach to comparison trials when references are dependent.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.4 One-to-one comparison performance 9.4.2 False match rate 9.4.2.4	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.1 General	ISO/IEC 19795-1 requires the policy for measurement of false match rate in the presence of identical twins, etc. to be included in the test plan. This would be in the test strategy in ISO/IEC/IEEE 29119-3.
9 Analyses 9.4 One-to-one comparison performance 9.4.2 False match rate 9.4.2.5	N/A	ISO/IEC 19795-1 provides informative guidance on measuring false match rate where there are several non-mated comparison trials per test subject, or per reference.
9 Analyses 9.5 Verification system performance metrics 9.5.1 General	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	ISO/IEC 19795-1 requires measurement for transactions of multiple attempts to be derived directly rather than estimated from the DET curve. This requires test cases to be designed specifically.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.5 Verification system performance metrics 9.5.2 False reject rate	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) b). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Much of this clause is informative on measuring false reject rate (FRR), but it does also require that FRR is reported along with thresholds, etc. alongside FAR.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.5 Verification system performance metrics 9.5.3 False accept rate	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) b). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Much of this clause is informative on measuring false accept rate (FAR), but it does also require that FAR is reported along with thresholds, etc. alongside FRR.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.5 Verification system performance metrics 9.5.4 Verification transaction duration	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends that verification transaction duration "should" be measured and reported. Thus, this recommendation would need to be part of test design, recording and reporting.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.5 Verification system performance metrics 9.5.5 Generalized false reject rate and generalized false accept rate	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends how generalization "should" be performed and reported. Thus, this recommendation would need to be part of test design, recording and reporting.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.6 Identification system performance metrics 9.6.1 General	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 requires the three primary parameters used for identification to be 'declared'. Thus, they would need to be reported in the test completion report.
9 Analyses 9.6 Identification system performance metrics 9.6.2 False-negative identification rate	N/A	ISO/IEC 19795-1 provides informative guidance on calculating and presenting the false negative identification rate.
9 Analyses 9.6 Identification system performance metrics 9.6.3 False-positive identification rate	N/A	ISO/IEC 19795-1 provides informative guidance on calculating and presenting the false positive identification rate.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.6 Identification system performance metrics 9.6.4 Generalized false-negative identification rate and generalized false-positive identification rate	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.4 Record test execution (TE3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends the selection of an appropriate method for generalizing identification rates – and requires the reporting of the method.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.6 Identification system performance metrics 9.6.5 Selectivity	N/A	ISO/IEC 19795-1 provides informative guidance on calculating and presenting the selectivity.
9 Analyses 9.6 Identification system performance metrics 9.6.6 Closed-set test of identification performance	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends that when a single point identification rank is reported, it "should" be referenced directly to the database size. Also, it recommends how to present the cumulative match characteristic (CMC) plot derived from a closed-set test. Thus, it would need to be calculated as a test result and included in the test completion report.
9 Analyses 9.6 Identification system performance metrics 9.6.7 Estimation of identification error rates from one-to-one comparison results	N/A	ISO/IEC 19795-1 provides informative guidance on estimating the identification error rates from verification results.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.6 Identification system performance metrics 9.6.8 Predicting identification error rates in larger populations	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 requires the model used for extrapolating performance to be reported, when used. Thus, they would need to be reported in the test completion report.
9 Analyses 9.7 Analysis of performance across controlled experimental factors 9.7.1 Longitudinal analyses	N/A	ISO/IEC 19795-1 provides informative guidance on the use of longitudinal analyses (e.g. to take account of ageing).
9 Analyses 9.7 Analysis of performance across controlled experimental factors 9.7.2 Pairwise analyses	N/A	ISO/IEC 19795-1 provides informative guidance on the use of pairwise analyses (e.g. when subject use two different devices).

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.8 Detection error trade-off	ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 requires the DET to be developed using the comparison scores from the mated and non-mated comparison trials. It also requires any removal of outliers to be documented. Thus, it would need to be calculated as a test result and included in the test completion report.
9 Analyses 9.9 Transaction durations 9.9.1	N/A	ISO/IEC 19795-1 provides informative guidance on the measurement of throughput rates.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.9 Transaction durations 9.9.2	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends that the user interaction with the system be determined in advance (presumably as part of test design), considered when measuring throughput, and documented in the test report.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.9 Transaction durations 9.9.3	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends that the distribution of transaction durations "should" be reported in the test report (measurement of these would need to be included in the test cases).
9 Analyses 9.10 Computational workload 9.10.1	N/A	ISO/IEC 19795-1 provides informative guidance on the measurement of computational workload.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.10 Computational workload 9.10.2	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	ISO/IEC 19795-1 requires the workload to be measured over all components of a transaction. Scope of testing is part of test planning, while test case design specifies what is measured.
9 Analyses 9.10 Computational workload 9.10.3	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) e).	ISO/IEC 19795-1 recommends that when comparing algorithms the same hardware is used, which would be implemented as part of the test environment.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.10 Computational workload 9.10.4	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 requires specific measurement and reporting for the computational workload for systems that use binning, preselection, or indexing algorithms.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Analyses 9.11 Uncertainty of estimates	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 8.4 Test execution process 8.4.4 Activities and tasks 8.4.4.3 Compare test results (TE2) a).	ISO/IEC 19795-1 provides guidance on measuring uncertainty and requires that this uncertainty be estimated.
10 Graphical presentation of results 10.1 Score distributions 10.1.1 General	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 recommends considering rescaling of comparison scores on histograms (presumably in test reports).
10 Graphical presentation of results 10.1 Score distributions 10.1.2 Boxplots	N/A	ISO/IEC 19795-1 provides informative guidance on the use of boxplots.
10 Graphical presentation of results 10.2 Error rate vs threshold plot	N/A	ISO/IEC 19795-1 provides informative guidance on the use of error rate vs decision threshold plots.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
10 Graphical presentation of results 10.3 DET plot	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides recommendations on the use of DET plots and requires that the scaling used "shall" be reported.
10 Graphical presentation of results 10.4 CMC plot / FNIR over rank plot	N/A	ISO/IEC 19795-1 provides informative guidance on the use of CMC and FNIR over rank plots.
10 Graphical presentation of results 10.5 FNIR over number of enrolees plot	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides recommendations on the use of FNIR over number of enrolees plots.
10 Graphical presentation of results 10.6 Heat maps	N/A	ISO/IEC 19795-1 provides informative guidance on the use of heat maps.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
11 Record keeping	ISO/IEC/IEEE 29119-2 7.2 Test strategy and planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	ISO/IEC 19795-1 requires record keeping comply with regulations.
12 Reporting performance results 12.1 Reporting test details	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides requirements on what is included in the test report.
12 Reporting performance results 12.2 Summary statistics	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides requirements on how summary statistics are included in the test report.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
12 Reporting performance results 12.3 Reporting enrolment performance	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides requirements on how enrolment performance is included in the test report.
12 Reporting performance results 12.4 Reporting acquisition performance	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides requirements on how acquisition performance is included in the test report.
12 Reporting performance results 12.5 Reporting one-to-one comparison performance	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides requirements on how one-to-one comparison performance is included in the test report.

Table E.1 *(continued)*

ISO/IEC 19795-1:2021	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
12 Reporting performance results 12.6 Reporting verification system performance	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides requirements on how verification system performance is included in the test report.
12 Reporting performance results 12.7 Reporting identification system performance	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides requirements on how identification system performance is included in the test report.
12 Reporting performance results 12.8 Reporting performance across factors	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-1 provides recommendations on reporting performance across factors.

Annex F
(informative)

Mapping from ISO/IEC 19795-2 to the ISO/IEC/IEEE 29119 series

F.1 General

This mapping shows how the requirements of ISO/IEC 19795-2 relate to the requirements of the ISO/IEC/IEEE 29119 series. The main purpose of the mapping is to allow users of ISO/IEC 19795-2 to understand how the testing methodologies for technology and scenario evaluation for biometrics can be applied, while also complying with, or simply using, where appropriate, the more detailed requirements of the ISO/IEC/IEEE 29119 series of software testing standards.

NOTE ISO/IEC 19795-2:2007/Amd 1:2015, testing of multi-modal biometric implementations, has been included in this mapping.

F.2 Overview of ISO/IEC 19795-2

ISO/IEC 19795-2 specifies the requirements for test data generation, test execution and test reporting for two of the three biometric system evaluation approaches: technology and scenario evaluation (operational evaluation is not included in ISO/IEC 19795-2 but is covered in ISO/IEC 19795-6). See 6.1.2 for an explanation of the levels used for the evaluation of biometric systems. Use of ISO/IEC 19795-2 is meant to provide users (testers are not included in the expected users) with a means of benchmarking between different technologies, usage scenarios and test environments.

ISO/IEC 19795-2 builds on generic requirements and practices specified in ISO/IEC 19795-1.

ISO/IEC 19795-2:2007/Amd 1:2015 adds coverage of the testing of multi-modal biometric devices to the coverage of single mode biometric devices covered in ISO/IEC 19795-2:2007.

F.3 Conformance requirements of ISO/IEC 19795-2

Conformance requirements change for the two evaluation approaches covered by ISO/IEC 19795-2 (technology and scenario). The requirements are also dependent on the comparison type of the system being evaluated (i.e. identification and verification systems). The relevant clauses are shown in Table F.1.

Table F.1 — Conformance for evaluation approaches and comparison types

Evaluation approach	Comparison type	Required clauses
Technology or scenario	Identification or verification	Clauses 5 and 8
Technology	Identification	All of Clause 6, except 6.3.3
Technology	Verification	All of Clause 6, except 6.3.4
Scenario	Identification	All of Clause 7, except 7.3.4
Scenario	Verification	All of Clause 7, except 7.3.5

F.4 Mapping

Table F.2 shows the mapping from subclauses in ISO/IEC 19795-2:2007 (ISO/IEC 19795-2:2007/Amd 1:2015) to subclauses in ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021, along with the rationale for each mapping.

Table F.2 — Mapping from ISO/IEC 19795-2:2007 to ISO/IEC/IEEE 29119 series

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
5 Overview of technology evaluations and scenario evaluations.	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test completion report includes a summary of the testing performed and this can include the form of biometric evaluation performed.
6 Technology evaluation 6.1 Test design 6.1.1 Goals	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand Context (TP1) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	The test plan "should" include a description of the scope of the testing and this can include a description of the scope of the biometric evaluation (i.e. enrolment, acquisition and/or matching). Note: It has been assumed that technology evaluation does not always include all three functions, as suggested in ISO/IEC 19795-2.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.1 Test design 6.1.2 Application realism	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.2 Create test model (TD1) 8.2.4.3 Identify test coverage Items (TD2) 8.2.4.4 Derive test cases (TD3) 8.2.4.5 Create test procedures (TD4) ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) a) 6). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	The realism of the testing is determined, in large part, by the representativeness of the test model and the selection of suitable test coverage items (e.g. in this case, realistic functions and procedures). Test cases are subsequently derived to achieve coverage of the test coverage items and test procedures can be created to run the test cases in a realistic sequence. The test item (the implementation under test) is specified as part of the test planning process. If the specified test item "should" return the comparison score, then as long as that item is installed in the test environment, then the comparison score "should" be available.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.1 Test design 6.1.3 Determination of appropriate performance measures	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.5 Identify risk treatment approaches (TP4) a). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	The test plan "should" include a description of the scope of the testing and test requirements, and this can include a description and rationale for the type of technology test to be performed. The risk treatment approaches inform the test strategy, which "should" include the test completion criteria. If there is a requirement for the test item to produce biometric performance measures, then a risk treatment can be for the testing to supply these measures. These test completion criteria are used as the basis for identifying the test coverage criteria, which form part of the test strategy, which is used as the basis of the subsequent test design and implementation process and test execution process, where the tests will be designed and executed to provide these measures.
6 Technology evaluation 6.1 Test design 6.1.4 Implementation primacy	ISO/IEC/IEEE 29119-3 7.2 Test plan	The test plan requires no specification of implementation details for the test item.
6 Technology evaluation 6.1 Test design 6.1.5 Policies on disclosure of information to suppliers	N/A	The ISO/IEC/IEEE 29119 series do not include any requirements on disclosure of information to suppliers.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.1 Test design 6.1.6 Non-interchangeability of identification and verification attempts	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	The test plan requires the context and scope to be understood and documented prior to test design and execution.
6 Technology evaluation 6.1 Test design 6.1.7 Acknowledgement of models	N/A	The ISO/IEC/IEEE 29119 series do not include any requirement to verify the functional or non-functional attributes of models, approximations, or predictions of systems.
6 Technology evaluation 6.1 Test design 6.1.8 Sequential use	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements ISO/IEC/IEEE 29119-3 8.3 Test case specification 8.3.3 Test cases 8.3.3.6 Preconditions ISO/IEC/IEEE 29119-3 8.5 Test data requirements 8.5.1 Overview	ISO/IEC/IEEE 29119-3 includes test data requirements in the test plan, and, where necessary these are specified separately in the test data requirements documentation. Each test case specifies preconditions, which can include test data requirements, and test cases are described in execution order in the test procedure specification.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.1 Test design 6.1.9 Pre-test procedures 6.1.9.1 Installation and validation of correct operation	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) b). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process	Planning that the system (hardware and software) is installed correctly starts with test planning, continues with test design and implementation, and is implemented in the test environment and data management process.
6 Technology evaluation 6.1 Test design 6.1.9 Pre-test procedures 6.1.9.2 Data preparation	ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.3 Prepare test data (ED2)	Preparation of test data to meet test data requirement is a separate activity in ISO/IEC/IEEE 29119-2, however there is no explicit guidance on preventing suppliers gaming the test tests.
6 Technology evaluation 6.1 Test design 6.1.10 Generic test execution sequence	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4)	ISO/IEC/IEEE 29119-2 provides a separate activity for creation of the test procedures (which order the test cases and describe any necessary pre- and post-conditions) but does not provide any guidance specific to biometric systems.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.2 Unique enrolment	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) c). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) b). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process	Planning that the test data meet requirements starts with test planning and continues with test design and implementation. The test data requirements are implemented in the test environment and data management process.
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.3 Recurrence of data acquisition	N/A	ISO/IEC 19795-2 provides informative guidance on reusing test subjects to provide multiple transactions.
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.4 Test subject identification	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) c). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.3 Prepare test data (ED2) a) 5).	ISO/IEC/IEEE 29119-2 requires test cases, which include test data, and any separate test data to be approved and recorded, but it does not explicitly require them to be reported to anyone. ISO/IEC 19795-2 does not specify who the information related to subject identification is reported to.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.5 Provision of non-biometric information	ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.3 Prepare test data (ED2) ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 8.7 Test data readiness report ISO/IEC/IEEE 29119-3 8.8 Test environment readiness report	Preparation of test data to meet test data requirement is a separate activity in ISO/IEC/IEEE 29119-2, however there is no explicit guidance on the provision of biometric metadata to the test item. ISO/IEC/IEEE 29119-3 requires the test completion report to summarize the testing performed. This would list the test procedures and test cases executed, and these include descriptions of test data and test environment requirements (both are included in ISO/IEC 19795-2 as metadata) that are not included separately as part of the test data requirements and the test environment requirements.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.6 Representativeness of corpus	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) c). ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 8.5 Test data requirements ISO/IEC/IEEE 29119-3 8.7 Test data readiness report	ISO/IEC/IEEE 29119-2 requires test data requirements to be identified as part of test planning. ISO/IEC/IEEE 29119-3 requires the test completion report to summarize the testing performed. This would list the test procedures and test cases executed, and these include descriptions of test data requirements that are not included separately as part of the test data requirements and the test environment requirements. Specific biometric information pertaining to experimenter-test subject interaction is, however not explicitly described in the ISO/IEC/IEEE 29119 series.
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.7 Untainted corpus	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.3 Deviations from planned testing	ISO/IEC/IEEE 29119-3 requires the test completion report to summarize the testing performed (and the test data used). ISO/IEC 19795-2 states that if the testing was planned to use tainted biometric corpus data, this "shall" be recorded, and if the test data used does not follow the planned testing, any deviations "shall" also be recorded.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.8 Retirement of corpus	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) c). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) b).	The selection of test data can occur as part of the test planning or test design and implementation processes. ISO/IEC/IEEE 29119-2 does not cover the reuse of biometric data that has been previously used for tuning.
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.9 Corpus validation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements ISO/IEC/IEEE 29119-3 8.5 Test data requirements ISO/IEC/IEEE 29119-3 8.7 Test data readiness report	Any requirements for test data validation “should” be included as part of the test plan and/or test data requirements . If the test data requirements included coverage of validation of test data, then the Test Data Readiness Report “should” describe whether these requirements have been met.
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.10 Corpus collection environment	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements ISO/IEC/IEEE 29119-3 8.5 Test data requirements	Environmental conditions which form part of the test data requirements can be specified as part of the test plan and/or test data requirements .

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.2 Assembling an appropriate test corpus 6.2.11 Failure at source	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements ISO/IEC/IEEE 29119-3 8.5 Test data requirements ISO/IEC/IEEE 29119-3 8.7 Test data readiness report	Any requirements for test data processing "should" be included as part of the test plan and/or test data requirements . If the test data requirements included coverage of processing of test data, then the Test Data Readiness Report "should" describe whether these requirements have been met.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.3 Performance measurement 6.3.1 Enrolment	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as failure to enrol. The context and requirement to measure the failure to enrol rate of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan. Any test input data requirements, such as the number of samples to be part of the testing, "should" be included as part of the test case specification. The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as failure to enrol. The context and requirement to measure enrolment quality scores of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.3 Performance measurement 6.3.2 Failure to acquire	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a). ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	Any test input data requirements, such as the number of samples to be part of the testing, "should" be included as part of the test case specification. The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as failure to enrol. The context and requirement to measure the failure to acquire rate of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.3 Performance measurement 6.3.3 Verification metrics	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d). ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a).	The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as false match. The context and requirement to measure the false match rate of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan. The test planning "should" ensure a suitable test environment is specified. If test subjects are considered to be part of the test environment, then the number of test subjects required would be calculated as part of the determining the test environment requirements. The transactions represent a level of test coverage, and so would be identified as part of test design. The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as distribution of enrolment quality scores. The context and requirement to measure distribution of enrolment quality scores of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.3 Performance measurement 6.3.4 Identification metrics	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as uncertainty measures. The context and requirement to measure uncertainty measures of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan. The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as identification metrics. The context and requirement to measure identification metrics of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.
6 Technology evaluation 6.3 Performance measurement 6.3.5 Generalized error rates including failure to enrol and failure to acquire 6.3.5.1 General	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as generalized error rates. The context and requirement to measure generalized error rates of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.3 Performance measurement 6.3.5 Generalized error rates including failure to enrol and failure to acquire 6.3.5.2 Single-attempt transactions	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as generalized error rates. The context and requirement to measure generalized error rates of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.
6 Technology evaluation 6.3 Performance measurement 6.3.5 Generalized error rates including failure to enrol and failure to acquire 6.3.5.3 Multi-attempt transactions	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system performance measures, such as generalized error rates. The context and requirement to measure generalized error rates of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.1 General	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system throughput performance. The context and requirement to measure system throughput performance of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.2 Reporting throughput performance	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the test measures in the test completion report. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system throughput performance. The context and requirement to measure system throughput performance of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.3 Reporting comparison and throughput performance	N/A	Informative text.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.4 Measuring biometric reference generation and sample feature extraction timing	N/A	Informative text.
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.5 Simultaneous measurement of throughput and recognition error rates	N/A	Informative text.
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.6 Throughput in impostor and genuine user attempts	N/A	Informative text.
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.7 Post-enrolment “fixing” overhead	N/A	Informative text.
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.8 Uniqueness searches on enrolment	N/A	Informative text.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.3 Performance measurement 6.3.6 Throughput performance 6.3.6.9 Hardware	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d). ISO/IEC/IEEE 29119-3 8.3 Test case specification 8.3.3 Test cases 8.3.3.6 Preconditions	The test environment would be specified as part of test planning, while the requirement to re-start the system between tests would be specified as part of the preconditions for a test case.
6 Technology evaluation 6.4 Reporting 6.4.1 General	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b).	Test completion reporting can work at any test level and for any test type.
6 Technology evaluation 6.4 Reporting 6.4.2 System information 6.4.2.1 Specifications	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The summary of testing performed “should” include details of the test item (software and hardware) and the test environment. Note that there is no 6.4.2.2.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.4 Reporting 6.4.3 Data collection processes	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates ISO/IEC/IEEE 29119-3 8.10 Test execution log	The test completion report summarizes the testing performed, while the test plan specifies how the testing is expected to be performed in the description of planned test activities. The test execution log provides contemporaneous evidence of test execution.
6 Technology evaluation 6.4 Reporting 6.4.3 Data collection processes 6.4.3.1 Architecture	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The summary of testing performed "should" include details of the test item (software and hardware) and the test environment. The elements of the biometric system would be described where they interfaced with the test environment and provided actual results.
6 Technology evaluation 6.4 Reporting 6.4.3 Data collection processes 6.4.3.2 Outputs	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test completion report summarizes the testing performed, while the test plan specifies how the testing is expected to be performed in the description of planned test activities. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system outputs. The context and requirement to measure outputs of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.
6 Technology evaluation 6.4 Reporting 6.4.3 Data collection processes 6.4.3.3 Method of implementation	N/A	Reporting on system acquisition and supplier involvement in system implementation is outside the scope of the ISO/IEC/IEEE 29119 series of software testing standards.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Technology evaluation 6.4 Reporting 6.4.4 Disclosure 6.4.4.1 External reporting	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.4 Test deliverables	Test deliverables are documented as part of the test plan.
6 Technology evaluation 6.4 Reporting 6.4.4 Disclosure 6.4.4.2 Sample properties disclosure	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.4 Test deliverables	Test deliverables are documented as part of the test plan.
6 Technology evaluation 6.4 Reporting 6.4.5 Report structure	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed 7.4.3 Deviations from planned testing 7.4.4 Test completion evaluation 7.4.5 Factors that blocked progress 7.4.6 Test measures 7.4.7 Residual risks 7.4.8 Test deliverables 7.4.9 Reusable test assets 7.4.10 Lessons learned ISO/IEC/IEEE 29119-3 7.2 Test plan	The ISO/IEC/IEEE 29119-3 test completion report provides a summary of the testing performed, which covers the majority of sections required by ISO/IEC 19795-2. It does not include the 'full test plan' as that is a separate document (as shown) and duplicating it in the test completion report can lead to consistency issues in the event of updates (and the test plan is expected to be updated to reflect the changing risk profile in the ISO/IEC/IEEE 29119 series).
7 Scenario evaluation		This clause applies to scenario evaluations only. For identification comparisons, all clauses apply except for subclause 7.3.4, and for verification all clauses apply except for subclause 7.3.5.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.1 Test design 7.1.1 Characteristics of simulated application 7.1.1.1 Concept of operations	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test item (what is being tested).
7 Scenario evaluation 7.1 Test design 7.1.1 Characteristics of simulated application 7.1.1.2 Comparison functionality	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand Context (TP1) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.3 Test scope	The test planning requires the testers to determine the form of testing to be performed – and document this in the test plan. However, the ISO/IEC/IEEE 29119 series does not require the rationale for the selection of which types of comparison are tested to be documented.
7 Scenario evaluation 7.1 Test design 7.1.1 Characteristics of simulated application 7.1.1.3 Evaluation environment	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 8.8 Test environment readiness report ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-3 8.6 Test environment requirements	The test completion report includes a summary of the testing and any issues with the test environment not meeting requirements, typically based on the detailed test environment readiness report. The test plan describes the initial test environment requirements, while the Test environment requirements provide any necessary additional requirements.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.1 Test design 7.1.1 Characteristics of simulated application 7.1.1.4 Test platform	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d).	The test planning "should" ensure a suitable test environment is specified.
7 Scenario evaluation 7.1 Test design 7.1.2 Test execution 7.1.2.1 Test information and general test instructions	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements	The test subject are part of the test environment and so specific guidance that test subjects "should" receive is defined as part of the test environment requirements in the test strategy, which is typically part of the test plan.
7 Scenario evaluation 7.1 Test design 7.1.2 Test execution 7.1.2.2 Training	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-3 8.3 Test case specification 8.3.3 Test cases 8.3.3.6 Preconditions	The test subject are part of the test environment and so specific training that test subjects "should" receive is defined as part of the test environment requirements in the test strategy, which is typically part of the test plan. The test case preconditions "should" describe any necessary training or scripts required by test subjects for the particular system prior to running a test (and any constraints on how this training is provided).
7 Scenario evaluation 7.1 Test design 7.1.2 Test execution 7.1.2.3 Attended / unattended testing	ISO/IEC/IEEE 29119-3 8.3 Test case specification 8.3.3 Test cases 8.3.3.6 Preconditions	The required attendance of an administrator or operator during tests "should" be described as part of the preconditions for the test case.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.1 Test design 7.1.2 Test execution 7.1.2.4 Guidance	ISO/IEC/IEEE 29119-3 8.3 Test case specification 8.3.3 Test cases 8.3.3.6 Preconditions ISO/IEC/IEEE 29119-3 8.10 Test execution Log	The test case preconditions "should" describe any necessary guidance to be provided to test subjects during the running of tests (and constraints on it). The test execution log records any events outside the normal, such as where extra guidance was necessary.
7 Scenario evaluation 7.1 Test design 7.1.2 Test execution 7.1.2.5 Test order and acclimatization	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a). ISO/IEC/IEEE 29119-3 8.10 Test execution Log	The test procedure specification orders the test cases in the required order (such as to ensure 'balance' and minimize the effect of temporal conditions). The test execution log records any events outside the normal, such as where the ordering of tests has an observable effect on the results.
7 Scenario evaluation 7.1 Test design 7.1.2 Test execution 7.1.2.6 Test subject identifiers	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) c). ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.3 Prepare test data (ED2) a) 5).	ISO/IEC/IEEE 29119-2 requires test cases, which include test data, such as subject identifiers, and any separate test data to be approved and recorded.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.1 Test design 7.1.3 Levels of effort and decision policies 7.1.3.1 Enrolment level of effort and decision policies	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	As the effort and decision policies are part of the system's operational environment, then these are defined as part of the test environment for the testing of the system, and so "should" be recorded as part of the test environment requirements in the test strategy, which is typically part of the test plan. Where there are separate tests for each system, any specific test input data requirements, such as the number of presentation attempts for enrolment allowed for this system, "should" be included as part of the test case specification.
7 Scenario evaluation 7.1 Test design 7.1.3 Levels of effort and decision policies 7.1.3.2 Comparison level of effort and decision policies	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	As the effort and decision policies are part of the system's operational environment, then these are defined as part of the test environment for the testing of the system, and so "should" be recorded as part of the test environment requirements in the test strategy, which is typically part of the test plan. Where there are separate tests for each system, any specific test input data requirements, such as the number of presentation attempts for enrolment allowed for this system, "should" be included as part of the test case specification.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.1 Test design 7.1.3 Levels of effort and decision policies 7.1.3.3 Reference adaptation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items ISO/IEC/IEEE 29119-3 8.9 Actual results and test result ISO/IEC/IEEE 29119-3 8.10 Test execution log	The test plan specifies the test item (what is being tested), however there is no requirement in the test plan to describe how the functions being tested are implemented in the Test Item. If required the actual results can include additional details, such as the proportions of genuine and impostor recognition transactions in which biometric reference adaptation occurred. Alternatively, such information can be recorded in the test log as adaptation events.
7 Scenario evaluation 7.1 Test design 7.1.3 Levels of effort and decision policies 7.1.3.4 Appropriateness of levels of effort and decision policies	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	As the effort and decision policies are part of the system's operational environment, then these are defined as part of the test environment for the testing of the system, and so "should" be recorded as part of the test environment requirements in the test strategy, which is typically part of the test plan. Where there are separate tests for each system, any specific test input data requirements, such as the number of presentation attempts for enrolment allowed for this system, "should" be included as part of the test case specification.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.1 Test design 7.1.3 Levels of effort and decision policies 7.1.3.5 Implementation of native and customized levels of effort and decision policies	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.4 Derive test cases (TD3) a).	As the effort and decision policies are part of the system's operational environment, then these are defined as part of the test environment for the testing of the system, and so "should" be recorded as part of the test environment requirements in the test strategy, which is typically part of the test plan. Where there are separate tests for each system, any specific test input data requirements, such as the number of presentation attempts for enrolment allowed for this system, "should" be included as part of the test case specification.
7 Scenario evaluation 7.1 Test design 7.1.4 Multiple visits and transactions	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	Any requirements on multiple transactions "should" be specified as part of the test procedure specification.
7 Scenario evaluation 7.1 Test design 7.1.5 Executing genuine and impostor trials	ISO/IEC/IEEE 29119-3 8.3 Test case specification 8.3.3 Test cases 8.3.3.7 Inputs	Ways of testing different transaction types would be specified as part of the test case.
7 Scenario evaluation 7.1 Test design 7.1.6 Data collection	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.5 Create test procedures (TD4) a).	Methods for the collection of actual results would be specified as part of the creation of the test procedure – an 'other required action' (as shown in the note). Processes for auditing and validating performance data collection are outside the scope of the ISO/IEC/IEEE 29119 series.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.2 Test crew 7.2.1 General	ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) a) 4).	The crew can be considered as an element of the test environment. The crew requirements will typically be defined as part of test planning and they will be recruited as part of building the test environment.
7 Scenario evaluation 7.2 Test crew 7.2.2 Habituation	ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) b). ISO/IEC/IEEE 29119-3 8.9 Actual results and test result ISO/IEC/IEEE 29119-3 8.10 Test execution log ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d).	If the crew is considered to be part of the test environment, then their level of familiarity would be recorded as part of the recording of the status of the test environment. If required the actual results can include additional details, such as the crew categories. Alternatively, such information can be recorded in the test log. The summary of testing performed "should" include details of error rates per crew category if that information was collected as part of the actual results. If the crew is considered to be part of the test environment, then how they became habituated to each device can be recorded as part of the recording of the status of the test environment. The test planning "should" ensure a suitable test environment is specified. If the crew is considered to be part of the test environment, then ensuring they have the correct level of habituation "should" be specified in the test plan.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.2 Test crew 7.2.3 Crew composition	ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.2 Establish test environment (ED1) b).	If the crew is considered to be part of the test environment, then the crew composition can be reported as part of the test environment status.
7 Scenario evaluation 7.2 Test crew 7.2.4 Test subject management	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d).	The test planning ensures a suitable test environment is specified. If test subjects are considered to be part of the test environment, then management processes for them can be included as part of the test plan.
7 Scenario evaluation 7.3 Performance measurement 7.3.1 General	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-3 8.9 Actual results and test result ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The selection of performance measures "should" be made based on the test scope/requirements and perceived risk and specified in the test strategy. The actual results can include information on the time lapsed, error rates, etc. The test completion report includes a summary of the testing performed, thus it can include results of the analysis of actual results, such as results grouped by various attributes.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.3 Performance measurement 7.3.2 Enrolment	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) d).	The test results from the test execution process are collected and used to generate the performance measures in the test completion report. The context and requirement to measure the failure to enrol rate of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan. The test planning "should" ensure a suitable test environment is specified. If test subjects are considered to be part of the test environment, then the number of test subjects required would be calculated as part of the determining the test environment requirements. The transactions represent a level of test coverage, and so would be identified as part of test design.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
	ISO/IEC/IEEE 29119-2 8.2 Test design and implementation process 8.2.4 Activities and tasks 8.2.4.3 Identify test coverage items (TD2) a). ISO/IEC/IEEE 29119-3 8.9 Actual results and test result ISO/IEC/IEEE 29119-3 8.10 Test execution log ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	If required the actual results can include additional details, such as the effort level. Alternatively, such information can be recorded in the test log. The summary of testing performed "should" include details of failure to enrol rates for each effort level if that information was collected as part of the actual results. If required the actual results can include additional details, such as the effort level. Alternatively, such information can be recorded in the test log. The summary of testing performed "should" include details of failure to enrol rates for each effort level, if that information was collected as part of the actual results.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.3 Performance measurement 7.3.3 Failure to acquire	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 8.9 Actual results and test result ISO/IEC/IEEE 29119-3 8.10 Test execution log ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test results from the test execution process are collected and used to generate the performance measures in the test completion report. The context and requirement to measure the failure to acquire rate of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan. If required the actual results can include additional details, such as the number of presentations. Alternatively, such information can be recorded in the test log. The summary of testing performed "should" include details of number of presentations, the number of test subjects, etc., if that information was collected as part of the actual results.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.3 Performance measurement 7.3.4 Verification metrics	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the performance measures in the test completion report. The context and requirement to measure the false non-match rate, false accept rate, etc. of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.
7 Scenario evaluation 7.3 Performance measurement 7.3.5 Identification metrics	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the performance measures in the test completion report. The context and requirement to measure cumulative match characteristics, false match rate, false positive identification rate, etc. for the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.3 Performance measurement 7.3.6 Generalized error rates including failure to enrol and failure to acquire	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b). ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test results from the test execution process are collected and used to generate the performance measures in the test completion report. The context and requirement to measure generalized error rates for the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.
7 Scenario evaluation 7.3 Performance measurement 7.3.7 Interim analyses	ISO/IEC/IEEE 29119-2 7.3 Test monitoring and control process	The test monitoring and control process ensures that the testing is following the test plan and, where necessary, modifies the testing being performed and/or modifies the test plan (depending on the scale of the necessary changes). Test status reporting records the results of this process.
7 Scenario evaluation 7.4 Reporting 7.4.1 General	ISO/IEC/IEEE 29119-2 7.4 Test completion process 7.4.4 Activities and tasks 7.4.4.5 Report test completion (TC4) b).	Test completion reporting can work at any test level and for any test type.
7 Scenario evaluation 7.4 Reporting 7.4.2 System information 7.4.2.1 General	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The summary of testing performed "should" include details of the test item (software and hardware) and the test environment.
7 Scenario evaluation 7.4 Reporting 7.4.2 System information 7.4.2.2 Specifications	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The summary of testing performed "should" include details of the test item (software and hardware) and the test environment.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.4 Reporting 7.4.2 System information 7.4.2.3 Architecture	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The summary of testing performed "should" include details of the test item (software and hardware) and the test environment. The elements of the biometric system would be described where they interfaced with the test environment and provided actual results.
7 Scenario evaluation 7.4 Reporting 7.4.2 System information 7.4.2.4 Outputs	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The test completion report summarizes the testing performed, while the test plan specifies how the testing is expected to be performed in the description of planned test activities. The ISO/IEC/IEEE 29119 series do not specify any details about collection of specific biometric system outputs. The context and requirement to measure outputs of the biometric system would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.
7 Scenario evaluation 7.4 Reporting 7.4.3 System acquisition and implementation	N/A	Reporting on system acquisition and supplier involvement in system implementation is outside the scope of the ISO/IEC/IEEE 29119 series of software testing standards.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Scenario evaluation 7.4 Reporting 7.4.4 Physical layout of test environment	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 8.8 Test environment readiness report ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-3 8.6 Test environment requirements	The test completion report includes a summary of the testing and any issues with the test environment not meeting requirements, typically based on the detailed test environment readiness report. The test plan describes the initial test environment requirements, while the Test environment requirements provide any necessary additional requirements.
7 Scenario evaluation 7.4 Reporting 7.4.5 Report structure	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed 7.4.3 Deviations from planned testing 7.4.4 Test completion evaluation 7.4.5 Factors that blocked progress 7.4.6 Test measures 7.4.7 Residual risks 7.4.8 Test deliverables 7.4.9 Reusable test assets 7.4.10 Lessons learned ISO/IEC/IEEE 29119-3 7.2 Test plan	The ISO/IEC/IEEE 29119-3 test completion report provides a summary of the testing performed, which covers the majority of sections required by ISO/IEC 19795-2. It does not include the 'full test plan' as that is a separate document (as shown) and duplicating it in the test completion report can lead to consistency issues in the event of updates (and the test plan is expected to be updated to reflect the changing risk profile in the ISO/IEC/IEEE 29119 series).

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Other issues applicable to technology and scenario evaluations 8.1 Parties to a test	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.8 Degree of independence	The test completion report includes a summary of the testing and this would normally describe who (person/team) performed the summarized tests, and how the testing deviated from that described in the test plan, if at all. The test plan describes the level of independence of the testers.
8 Other issues applicable to technology and scenario evaluations 8.2 Fairness	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 8.8 Test environment readiness report ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-3 8.6 Test environment requirements	Any involvement by the testers in setting up the test item or other inputs to the testing will affect the test environment. The test environment requirements "should" be described in the test plan, while the test environment requirements provide any necessary additional requirements. The test completion report includes a summary of the testing and any issues with the test environment not meeting requirements (as specified in the test plan), typically based on the detailed test environment readiness report.
8 Other issues applicable to technology and scenario evaluations 8.3 Basis for inclusion of test systems	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b).	The need to test different biometric systems would be determined as part of the understand context activity in the test planning process and recorded as part of the test scope in the test plan.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Other issues applicable to technology and scenario evaluations 8.4 Use of Frequently Asked Questions	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.5 Testing communication	The ISO/IEC/IEEE 29119 series does not explicitly cover competitive evaluations and there is no coverage of FAQs. However, the test plan does include communication between the testers and other stakeholders.
8 Other issues applicable to technology and scenario evaluations 8.5 Legal issues	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	Legal issues and other constraints are covered in an explicit part of the test plan.
8 Other issues applicable to technology and scenario evaluations 8.6 Release of test source code	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.5 Testing communication	The ISO/IEC/IEEE 29119 series does not explicitly cover competitive evaluations and there is no coverage of the sharing of testware with suppliers. However, the test plan does include communication between the testers and other stakeholders.
8 Other issues applicable to technology and scenario evaluations 8.7 Supplier comment on test report	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.5 Testing communication ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.4 Test deliverables	The ISO/IEC/IEEE 29119 series does not explicitly cover the provision of pre-release test reports to suppliers. However, the test plan does include communication between the testers and other stakeholders and it also provides a list of test deliverables for the project.
Annex A Phases and activities for primary technology test types	N/A	The ISO/IEC/IEEE 29119 series require the use of a risk-based approach to testing, which informs the choice of test level/phases and activities, among other testing requirements. These risks are practically unique for each project and no set phases/activities are specified for specific forms of testing as described in ISO/IEC 19795-2.
Annex B Relationship between presentations, attempts, and transactions	N/A	This is an informative annex. The concepts of presentations, attempts, and transactions are specific to biometrics systems, and so are not covered as part of the ISO/IEC/IEEE 29119 series.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
Annex C Reporting effort levels	N/A	This is an informative annex. The effort level required comparison is a concept specific to biometrics systems, and so is not covered as part of the ISO/IEC/IEEE 29119 series.
Annex D Client-server testing	N/A	This is an informative annex. The client-server testing of biometric systems is specific to biometric systems, and so is not covered as part of the ISO/IEC/IEEE 29119 series.
Annex E Comparing results across systems in multi-system tests	N/A	This is an informative annex. The comparison of results from testing multiple biometric systems is specific to biometric systems, and so is not covered as part of the ISO/IEC/IEEE 29119 series.
Annex F Testing of multi-modal biometric implementations		This is a normative annex (part of the 2015 amendment).
Annex F Testing of multi-modal biometric implementations F.1 General	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a).	The test item is identified as part of understanding the context of testing at the start of test planning.
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.1 Decision-level fusion F.2.1.1 General	N/A	Informative text on decision-level fusion.
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.1 Decision-level fusion F.2.1.2 Technology evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.1 Decision-level fusion F.2.1.3 Scenario evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.2 Score-level fusion F.2.2.1 General	N/A	Informative text on score-level fusion.
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.2 Score-level fusion F.2.2.2 Technology evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.2 Score-level fusion F.2.2.3 Scenario evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.3 Feature-level fusion F.2.3.1 General	N/A	Informative text on feature-level fusion.
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.3 Feature-level fusion F.2.3.2 Technology evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.3 Feature-level fusion F.2.3.3 Scenario evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.4 Sample-level fusion F.2.4.1 General	N/A	Informative text on sample-level fusion.
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.4 Sample-level fusion F.2.4.2 Technology evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.2 Fusion scheme identification information for repeatable evaluation F.2.4 Sample-level fusion F.2.4.3 Scenario evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.3 Sensor type and presentation type information for repeatable evaluation F.3.1 General	N/A	Informative text on sample-level fusion.
Annex F Testing of multi-modal biometric implementations F.3 Sensor type and presentation type information for repeatable evaluation F.3.2 Technology evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.3 Sensor type and presentation type information for repeatable evaluation F.3.3 Scenario evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.4 Decision-level fusion parameters for repeatable evaluation F.4.1 General	N/A	Informative text on reporting evaluations based on decision-level fusion parameters.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
Annex F Testing of multi-modal biometric implementations F.4 Decision-level fusion parameters for repeatable evaluation F.4.2 Technology evaluation and scenario evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.5 Fusion Information Format (FIF) value for repeatable evaluation F.5.1 General	N/A	Informative text on reporting evaluations based on decision-level fusion parameters.
Annex F Testing of multi-modal biometric implementations F.5 Fusion Information Format (FIF) value for repeatable evaluation F.5.2 Technology evaluation and scenario evaluation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	The test plan specifies the test items (what is being tested).
Annex F Testing of multi-modal biometric implementations F.6 Factors in corpus collection (technology evaluation) and presentations (scenario evaluation) for repeatable evaluation F.6.1 General	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements	The testing requirements are determined at the initial stage of test planning. High-level test data requirements (and constraints) are specified as part of the test plan.
Annex F Testing of multi-modal biometric implementations F.6 Factors in corpus collection (technology evaluation) and presentations (scenario evaluation) for repeatable evaluation F.6.2 Technology evaluation	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a).	The specification of test activities, such as requiring samples to be gathered simultaneously, is determined as part of designing the test strategy during test planning.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
Annex F Testing of multi-modal biometric implementations F.6 Factors in corpus collection (technology evaluation) and presentations (scenario evaluation) for repeatable evaluation F.6.3 Scenario evaluation	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a).	The specification of test activities, such as requiring a multi-modal presentation environment, is determined as part of designing the test strategy during test planning.
Annex F Testing of multi-modal biometric implementations F.7 Failure-to-enrol and failure-to-acquire policies for repeatable evaluation F.7.1 General	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a).	The specification of test activities, such as evaluating all applicable acquisition policies, is determined as part of designing the test strategy during test planning.
Annex F Testing of multi-modal biometric implementations F.7 Failure-to-enrol and failure-to-acquire policies for repeatable evaluation F.7.2 Technology evaluation	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.8 Degree of independence	The test completion report includes a summary of the testing and this would record any FTE and multi-modal FTE policies, and the effect on the testing from that described in the test plan, if at all.
Annex F Testing of multi-modal biometric implementations F.7 Failure-to-enrol and failure-to-acquire policies for repeatable evaluation F.7.3 Scenario evaluation	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.8 Degree of independence	The test completion report includes a summary of the testing and this would record any FTE and multi-modal FTE policies, and the effect on the testing from that described in the test plan, if at all.

Table F.2 *(continued)*

ISO/IEC 19795-2:2007 incl. Amd.1:2015	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
Annex F Testing of multi-modal biometric implementations F.8 Multi-modal Performance evaluation Reporting	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.8 Degree of independence	The test completion report includes a summary of the testing and this would record any necessary information specific to multi-modal implementations, and the effect on the testing from that described in the test plan, if at all.

Annex G
(informative)

Mapping from ISO/IEC 19795-4 to the ISO/IEC/IEEE 29119 series

G.1 General

This mapping shows how the requirements of ISO/IEC 19795-4 relate to the requirements of the ISO/IEC/IEEE 29119 series. The main purpose of the mapping is to allow users of ISO/IEC 19795-4 to understand how interoperability performance testing for biometrics can be applied, while also complying with, or simply using, where appropriate, the more detailed requirements of the ISO/IEC/IEEE 29119 series of software testing standards.

G.2 Overview of ISO/IEC 19795-4

ISO/IEC 19795-4 defines tests to address the interoperability and sufficiency available from biometric data formatted to comply with established standards, such as with the ISO/IEC 19794 series that covers biometric data interchange formats.

NOTE The ISO/IEC 19794 series are being superseded by the ISO/IEC 39794 series.

Interoperability testing is concerned with the ability of components from different suppliers to effectively work together as part of the same biometric system. The components considered as part of this interoperability testing are shown in Figure G.1 in dark grey. In theory, each of these interoperable components can be provided by a separate supplier, and the interoperability testing determines whether the components can work together. Testing for interoperability requires different combinations of components to be tested and the resulting biometric performance measures compared.

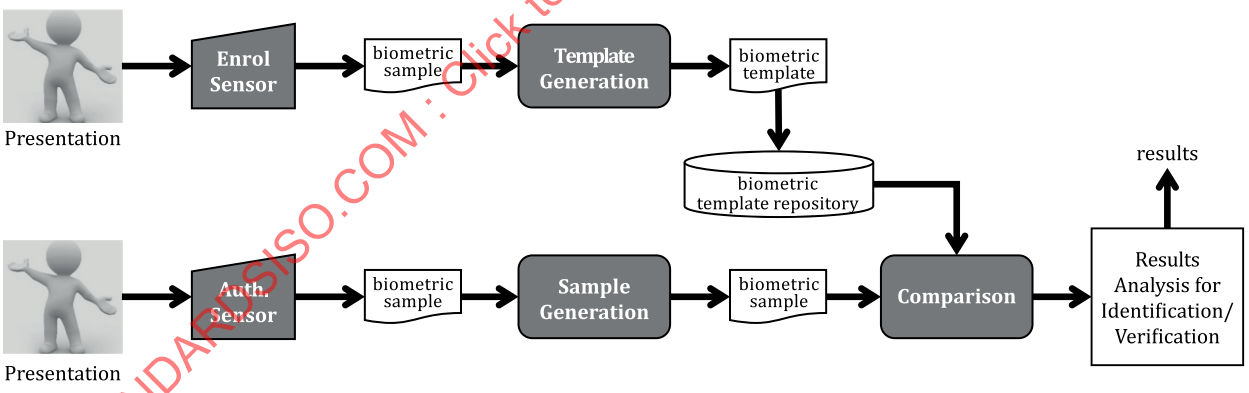

Figure G.1 — Biometric components considered for interoperability

Sufficiency testing checks the capability of an interchange standard (e.g. a standard for the format of biometric templates) against either an absolute value of performance or against a proprietary interchange format. Figure G.2 shows how a sufficiency test comparing a new set of standard interchange formats (shown by the dark grey parts) with a corresponding proprietary implementation format (shown by the light grey parts) can be set up. Sufficiency testing requires that the components working with the standard interchange conform to the standard.

Tests performed in line with ISO/IEC 19795-4 include both technology (referred to as offline) and scenario (referred to as online) tests.

Technology tests can be run using an available corpus of suitable sample data or using a corpus of sample data collected specifically for the purpose of the technology test under operational conditions that simulate the expected use of the biometric system. Technology tests are considered suitable where a corpus of suitable sample data is already available or when collecting such data is impractical and is not expected to influence the testing of interoperability (e.g. when testing the interoperability of the 'Comparison' component with the rest of the biometric system).

Scenario tests are expected to be used for interoperability testing where the devices capturing the biometric samples ('Enrol Sensor' and 'Auth Sensor' in Figure G.1) or the interaction with these devices by the subjects are expected to influence the performance of the biometric system due to interoperability issues.

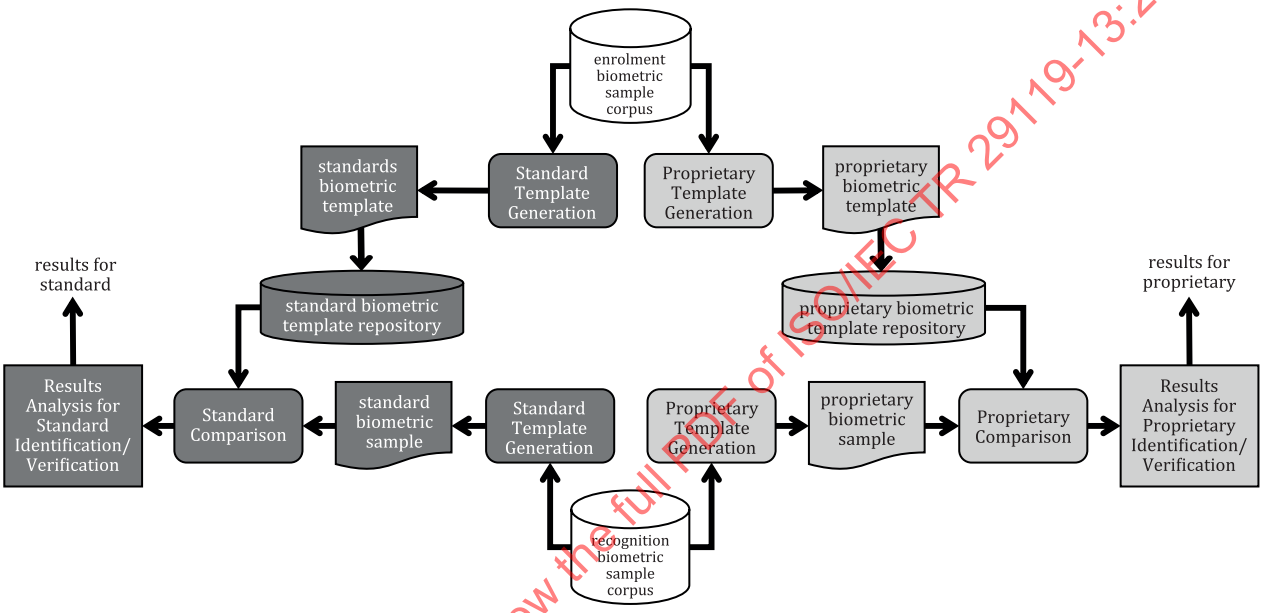

Figure G.2 — Logical set-up for a sufficiency test of a biometric interchange standard format

G.3 Conformance requirements of ISO/IEC 19795-4

An interoperability performance test conforms to ISO/IEC 19795-4 if it satisfies the requirements specified in ISO/IEC 19795-4:2008, Clauses 6, 7, 8 and 9.

G.4 Mapping

Table G.1 shows the mapping from subclauses in ISO/IEC 19795-4:2008 to subclauses in ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021, along with the rationale for each mapping.

Table G.1 — Mapping from ISO/IEC 19795-4:2008 to the ISO/IEC/IEEE 29119 series

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Goals 6.1 Coverage	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan includes a description of the aspects of interoperability that are being tested. The test completion report includes a summary of the testing performed and this would include the form of biometric evaluation being summarized and the details of who supplied the test items (the biometric components).
6 Goals 6.2 Target application 6.2.1 Biometric application 6.2.1.1 Defining a transaction	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 8.3 Test case specification 8.3.3 Test cases 8.3.3.7 Inputs	The test plan provides details of the expected testing activities. The test completion report includes a summary of the testing performed and this would include the form of the 'trials' (tests) undertaken. Any test input data requirements, such as the number of presentation attempts or number of samples input, "should" be included as part of the test case specification.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Goals 6.2 Target application 6.2.1 Biometric application 6.2.1.2 Reporting for identification systems	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan includes a description of the test items included as part of the testing. The test completion report includes a summary of the testing performed and this would include the form of biometric evaluation being summarized and the details of who supplied the various test items.
6 Goals 6.2 Target application 6.2.2 Interoperable application 6.2.2.1 Statement of coverage	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan includes a description of the scope of interoperability that is being tested. The test completion report includes a summary of the testing performed and this would include the scope of interoperability testing performed.
6 Goals 6.2 Target application 6.2.2 Interoperable application 6.2.2.2 Dimension of the interoperability space	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan would include a description of the dimensions of the interoperability space being tested and the number of suppliers and products involved. The test completion report includes a summary of the testing performed and this would include dimensions of the interoperability space that were tested, along with the products tested and their suppliers.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Goals 6.2 Target application 6.2.2 Interoperable application 6.2.2.3 Number of products	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan would include a description of the dimensions of the interoperability space being tested and the number of suppliers and products involved. The test completion report includes a summary of the testing performed and this would include dimensions of the interoperability space that were tested, along with the products tested and their suppliers.
6 Goals 6.3 Purpose 6.3.1 Interoperability testing	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.3 Test scope ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan includes a description of the objectives in terms of features to be tested. The test completion report includes a summary of the testing performed and this would include the test objectives covered by the testing. Note that this clause introduces the 'type 1 test' but provides no guidance on what this means. In the same clause it appears to define six test types, but these are labelled a to f. The following biometric standard mentions level tests (1, 2 and 3) and the book on security mentions type 1 tests, but there is little else from ISO, or on Google to help. From ISO/IEC 29109-1: 4.18 Level 1 testing conformance testing methodology that checks field-by-field and byte-by-byte conformance with the specification of the BDIR as specified in the base standard, both in terms of fields included and the ranges of the values in those fields NOTE This type of testing tests syntactic requirements of the base standard.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
6 Goals 6.3 Purpose 6.3.2 Sufficiency testing	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2.1 Projects / test levels / test types ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	Required test levels and activities are included in the test plan.
7 Metrics 7.1 General	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types 7.2.2.3 Test scope ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan includes a description of the scope of interoperability that is being tested. The test completion report includes a summary of the testing performed and this would include the scope of interoperability testing performed and the relevant performance metrics for the different configurations.
7 Metrics 7.2 Figures of merit 7.2.1 Recognition performance figure of merit	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Stakeholders 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.3 Test scope	Test planning defines the scope and testing requirements. The test plan includes a description of the features being tested as part of interoperability testing.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Metrics 7.2 Figures of merit 7.2.2 Measuring component failure	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Stakeholders 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.3 Test scope ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Test planning defines the scope and testing requirements. The test plan includes a description of the features being tested as part of interoperability testing. The test completion report includes a summary of the testing performed and this would include component-level failure rates.
7 Metrics 7.3 Interoperability matrices 7.3.1 General	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.2 Understand context (TP1) a), b).	Test planning defines the scope and testing requirements.
7 Metrics 7.3 Interoperability matrices 7.3.2 Three-way interoperability with sBDB generators	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	The test completion report would include any required performance matrix. The test plan can include the requirement for the inclusion of the performance matrix as part of the section of the test completion report on assumptions and constraints.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Metrics 7.3 Interoperability matrices 7.3.3 Two-way interoperability with sBDB generators	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	The test completion report would include any required performance matrix. The test plan can include the requirement for the inclusion of the performance matrix as part of the section of the test completion report on assumptions and constraints.
7 Metrics 7.3 Interoperability matrices 7.3.4 Fixed operating point interoperability	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	The test completion report would include any required performance matrix. The test plan can include the requirement for the inclusion of the performance matrix as part of the section of the test completion report on assumptions and constraints.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
7 Metrics 7.3 Interoperability matrices 7.3.5 Reporting failure of sBDB generators	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.3 Test scope ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	Note that there is no clause 7.2.3 in ISO/IEC 19795-4, which makes clause 7.3.5 more difficult to understand (and comply with). It is assumed that this "should" refer to clause 7.2.2. Test planning defines the scope and testing requirements. The test plan includes a description of the features being tested as part of interoperability testing. The test completion report includes a summary of the testing performed and this would include component-level failure rates.
7 Metrics 7.4 Proprietary performance	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	The test completion report would include any required performance matrix. The test plan can include the requirement for the inclusion of the performance matrix as part of the section of the test completion report on assumptions and constraints.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.1 Structure of test	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Stakeholders 7.2.4.2 Understand context (TP1) a), b). ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC 19795-4 states that the required content of the test "shall" be determined as part of test planning. The test completion report would summarize the testing performed.
8 Conducting a test 8.2 Sample data 8.2.1 Acquisition 8.2.1.1 General	N/A	No requirement in ISO/IEC 19795-4.
8 Conducting a test 8.2 Sample data 8.2.1 Acquisition 8.2.1.2 Offline acquisition	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) c).	Test data requirements are defined as part of the test strategy in the test plan.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.2 Sample data 8.2.1 Acquisition 8.2.1.3 Online acquisition	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 8.3 Test case specification 8.3.3 Test cases 8.3.3.7 Inputs	The test plan provides details of the expected testing activities. The test completion report includes a summary of the testing performed and this would include the form of the 'trials' (tests) undertaken. Any test input data requirements, such as the number of presentation attempts or number of samples input, "should" be included as part of the test case specification.
8 Conducting a test 8.2 Sample data 8.2.1 Acquisition 8.2.1.4 Hybrid acquisition	ISO/IEC/IEEE 29119-3 8.4 Test procedure specification 8.4.6 Ordered test cases ISO/IEC/IEEE 29119-3 8.10 Test execution log	Test procedures, test cases, a separate actual results document, or the test execution log can record the circumstances of the capture of samples.
8 Conducting a test 8.2 Sample data 8.2.1 Acquisition 8.2.1.5 Biometric capture device performance testing	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.6 Design test strategy (TP5) c), d).	Test data requirements for offline data would be defined as part of the test strategy in the test plan. If online acquisition is used the requirement to include a biometric capture device "should" be included as part of the test environment requirements.
8 Conducting a test 8.2 Sample data 8.2.2 Representative data	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.6 Design test strategy (TP5) c).	Test data requirements for size of data set, privacy, offline and covariate data would be defined as part of the test strategy in the test plan.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.2 Sample data 8.2.3 Collection of ancillary data	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.6 Design test strategy (TP5) c).	Test data requirements for size of data set, privacy, offline and covariate data would be defined as part of the test strategy in the test plan.
8 Conducting a test 8.2 Sample data 8.2.4 Corpus size	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.6 Design test strategy (TP5) c).	Test data requirements for size of data set, privacy, offline and covariate data would be defined as part of the test strategy in the test plan.
8 Conducting a test 8.2 Sample data 8.2.5 Removal of subject-specific metadata	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.6 Design test strategy (TP5) c).	Test data requirements for size of data set, privacy, offline and covariate data would be defined as part of the test strategy in the test plan.
8 Conducting a test 8.2 Sample data 8.2.6 Removal of unrepresentative metadata	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.6 Design test strategy (TP5) c).	Test data requirements for size of data set, privacy, offline and covariate data would be defined as part of the test strategy in the test plan.
8 Conducting a test 8.2 Sample data 8.2.7 Origin of samples	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test completion report summarizes the testing performed, the requirements for which would be documented in the test plan.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.2 Sample data 8.2.8 Untainted samples	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements ISO/IEC/IEEE 29119-2 8.3 Test environment and data management process 8.3.4 Activities and tasks 8.3.4.3 Prepare test data (ED2) a) 4).	The test plan includes requirements for the test data. The test environment and data management process includes tasks to ensure the test data meets the requirements.
8 Conducting a test 8.2 Sample data 8.2.9 Sequestered data	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements	The test plan includes test data requirements.
8 Conducting a test 8.3 Conformance testing 8.3.1 Conformance	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	The test completion report summarizes the testing, and the assumptions and constraints in the test plan can specify requirements on documentation of prior conformance tests.
8 Conducting a test 8.3 Conformance testing 8.3.2 Executing conformance tests	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	The test activities defined in the test plan can include the requirement to perform an interoperability or sufficiency test to assess the conformance of all sBDBs generated during the test.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.3 Conformance testing 8.3.3 Reporting	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.3 Assumptions and constraints	The test completion report summarizes the testing, and the assumptions and constraints in the test plan can specify requirements on documentation of whether conformance to the SIF was tested.
8 Conducting a test 8.4 Constraints on the sBDBs 8.4.1 Optional encodings	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements	The test plan includes test data requirements.
8 Conducting a test 8.4 Constraints on the sBDBs 8.4.2 Optional encodings from profile standards	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements	The test plan includes test data requirements.
8 Conducting a test 8.4 Constraints on the sBDBs 8.4.3 Deviation from the base standard	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements	The test plan includes test data requirements.
8 Conducting a test 8.4 Constraints on the sBDBs 8.4.4 Data encapsulation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.10 Test data requirements	The test plan includes test data requirements.
8 Conducting a test 8.5 Components 8.5.1 Components for sufficiency testing	N/A	There is nothing in the ISO/IEC/IEEE 29119 series that covers external factors (e.g. commercial decisions) deciding the scope of the testing.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.5 Components 8.5.2 Establishing modularity requirements	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	If the black boxes are used to define test levels, then the test plan records the test levels that will be used.
8 Conducting a test 8.5 Components 8.5.3 Components for interoperability testing	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items	Assuming that the components are what is being tested, then the test plan records the test items.
8 Conducting a test 8.5 Components 8.5.4 Underlying algorithms	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The algorithm embedded in comparison components is part of the test environment, which can be recorded as part of the test plan. The test completion report provides a summary of the testing and would confirm that the test plan had been followed (or deviations would be recorded).
8 Conducting a test 8.5 Components 8.5.5 Capture device user interfaces	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test completion report “should” record the test items that are tested as part of the test, and any recorded interoperability effects due to the user interfaces.
8 Conducting a test 8.5 Components 8.5.6 Multi-modal components	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test activities defined in the test plan can include the requirement to determine whether each mode in a multi-modal system is interoperable (i.e. successful results are achieved without using this mode). The test completion report provides a summary of the testing and would confirm that the test plan had been followed (or deviations would be recorded).

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.5 Components 8.5.7 Component variability	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The number of test items "should" be recorded in the test plan. The test environments for the testing "should" also be recorded in the test plan. The test activities defined in the test plan can include the requirement to test multiple copies of a component. The test completion report provides a summary of the testing and would confirm that the test plan had been followed (or deviations would be recorded).
8 Conducting a test 8.5 Components 8.5.8 Component reporting requirements	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The identification of test items "should" be recorded in the test plan. The test completion report provides a summary of the testing and would confirm that the test plan had been followed (or deviations would be recorded).

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.6 Planning decisions 8.6.1 Computational intensity	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	The test estimates defined in the test plan can include estimates of time required for test execution for each of the biometric system functions.
8 Conducting a test 8.6 Planning decisions 8.6.2 Supplier recruitment	N/A	Informational text (no requirements) on the number of components needed for different biometric interoperability tests.
8 Conducting a test 8.6 Planning decisions 8.6.3 Provision of samples to suppliers	N/A	The ISO/IEC/IEEE 29119 series do not cover the development of test items.
8 Conducting a test 8.6 Planning decisions 8.6.4 Equivalency of generator resources	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	The test environments (including limits on storage) for the testing "should" be recorded in the test plan. The test estimates defined in the test plan can include limits on the amount of time needed for testing. The test activities can describe the activities to handle violations of the limits.
8 Conducting a test 8.6 Planning decisions 8.6.5 Handling violations of test requirements	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	The test environments (including limits on storage) for the testing "should" be recorded in the test plan. The test estimates defined in the test plan can include limits on the amount of time needed for testing. The test activities can describe the activities to handle violations of the limits.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.6 Planning decisions 8.6.6 Comparison subsystem output data encapsulation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.11 Test environment requirements	Specific data representations for outputs of the test environment "should" be recorded in the test plan as part of the test environment requirements.
8 Conducting a test 8.6 Planning decisions 8.6.7 Fundamental generator requirement 8.6.7.1 Functional properties	N/A	The ISO/IEC/IEEE 29119 series do not cover the concept that tests can regard test items or elements of the test environment as black boxes.
8 Conducting a test 8.6 Planning decisions 8.6.7 Fundamental generator requirement 8.6.7.2 Generator implementation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	The required test levels can be recorded in the test plan.
8 Conducting a test 8.6 Planning decisions 8.6.7 Fundamental generator requirement 8.6.7.3 Failure to process	ISO/IEC/IEEE 29119-3 8.9 Actual results and test result ISO/IEC/IEEE 29119-3 8.10 Test execution log	The declaration of a failure to process (e.g. a sample) by a component is part of the actual outputs for a test. Unexpected events that occur during test execution can be logged in the test execution log.
8 Conducting a test 8.6 Planning decisions 8.6.7 Fundamental generator requirement 8.6.7.4 Generator error logging	ISO/IEC/IEEE 29119-3 8.9 Actual results and test result ISO/IEC/IEEE 29119-3 8.10 Test execution log	The declaration of a failure to process (e.g. a sample) by a component is part of the actual outputs for a test. Unexpected events that occur during test execution can be logged in the test execution log.
8 Conducting a test 8.6 Planning decisions 8.6.8 Fundamental comparison subsystem requirement		

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8.6.8.1 Functional requirement	N/A	The ISO/IEC/IEEE 29119 series do not cover the concept that tests can regard test items or elements of the test environment as black boxes.
8 Conducting a test 8.6 Planning decisions 8.6.8 Fundamental comparison subsystem requirement 8.6.8.2 Comparison subsystem implementation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.1 Projects / test levels / test types	The required test levels can be recorded in the test plan.
8 Conducting a test 8.6 Planning decisions 8.6.8 Fundamental comparison subsystem requirement 8.6.8.3 Comparison subsystem errors	ISO/IEC/IEEE 29119-3 8.9 Actual results and test result ISO/IEC/IEEE 29119-3 8.10 Test execution log	The declaration of a failure to process (e.g. a sample) by a component is part of the actual outputs for a test. Unexpected events that occur during test execution can be logged in the test execution log.
8 Conducting a test 8.6 Planning decisions 8.6.9 General requirements on software implementations	N/A	The ISO/IEC/IEEE 29119 series do not cover the implementation of test items.
8 Conducting a test 8.7 Prevention and detection of gaming	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a).	Gaming can be considered a project risk – and the test strategy "should" include suitable content to address the perceived risks. There is nothing specific in the ISO/IEC/IEEE 29119 series on the gaming of tests (or handling similar fraudulent behaviour).
8 Conducting a test 8.8 Test procedure 8.8.1 Primary test 8.8.1.1 Overview	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	These clauses in ISO/IEC 19795-4 talk about test procedures, but these are not test procedures as defined in the ISO/IEC/IEEE 29119 series. Instead, they are the sequence of activities required to perform interoperability testing of a biometric system. According to ISO/IEC/IEEE 29119-2, these test activities "shall" be defined as part of the overall test plan.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.8 Test procedure 8.8.1 Primary test 8.8.1.2 Verification	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	These clauses in ISO/IEC 19795-4 talk about test procedures, but these are not test procedures as defined in the ISO/IEC/IEEE 29119 series. Instead, they are the sequence of activities required to perform interoperability testing of a biometric system. According to ISO/IEC/IEEE 29119-2, these test activities "shall" be defined as part of the overall test plan.
8 Conducting a test 8.8 Test procedure 8.8.1 Primary test 8.8.1.3 Identification	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	These clauses in ISO/IEC 19795-4 talk about test procedures, but these are not test procedures as defined in the ISO/IEC/IEEE 29119 series. Instead, they are the sequence of activities required to perform interoperability testing of a biometric system. According to ISO/IEC/IEEE 29119-2, these test activities "shall" be defined as part of the overall test plan.
8 Conducting a test 8.8 Test procedure 8.8.2 Uncertainty measurement	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.9 Metrics to be collected	The test plan records the measures of interoperability, including the measure of uncertainty.
8 Conducting a test 8.8 Test procedure 8.8.3 Variance estimation	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	The sequence of test activities required to estimate variance for a biometric system would be defined as part of the test plan.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.8 Test procedure 8.8.4 Remedial testing	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates ISO/IEC/IEEE 29119-2 7.3 Test monitoring and control process 7.3.4 Activities and tasks 7.3.4.4 Control (TMC3) a). ISO/IEC/IEEE 29119-2 7.3 Test monitoring and control process 7.3.4 Activities and tasks 7.3.4.5 Report (TMC4) a).	The option for remedial testing of the interoperability of a biometric would be defined as part of the test plan, as would the need for repeating tests with different configurations. The test plan is implemented as part of the monitoring and control process, which also ensures reports on testing are provided.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
8 Conducting a test 8.8 Test procedure 8.8.5 Survey of configurable parameters	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates ISO/IEC/IEEE 29119-2 7.3 Test monitoring and control process 7.3.4 Activities and tasks 7.3.4.4 Control (TMC3) a). ISO/IEC/IEEE 29119-2 7.3 Test monitoring and control process 7.3.4 Activities and tasks 7.3.4.5 Report (TMC4) a).	The option for remedial testing of the interoperability of a biometric would be defined as part of the test plan, as would the need for repeating tests with different configurations. The test plan is implemented as part of the monitoring and control process, which also ensures reports on testing are provided.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.1 General	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.9 Metrics to be collected ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates	ISO/IEC/IEEE 29119-3 states that the test strategy (part of the test plan) "shall" include activities to be performed and the metrics to be collected. The test activities in the test plan would describe how to handle the situation where interoperability is confined to disjoint sets of suppliers.
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.2 Identifying interoperable combinations of subsystems 9.1.2.1 General	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.9 Metrics to be collected ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan records the measures of interoperability, while the test completion report summarizes the testing performed (and any deviations from the test plan).

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.2 Identifying interoperable combinations of sub-systems 9.1.2.2 Interoperability against a performance target 9.1.2.2.1 Method	N/A	The ISO/IEC/IEEE 29119 series allow users to interpret the results of testing as they wish – for instance, as required by ISO/IEC 19795-4.
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.2 Identifying interoperable combinations of sub-systems 9.1.2.2 Interoperability against a performance target 9.1.2.2.2 Reporting of data used in significance test computation	ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test completion report summarizes the testing performed and includes any relevant constraints on the results.
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.2 Identifying interoperable combinations of sub-systems 9.1.2.2 Interoperability against a performance target 9.1.2.2.3 Setting the significance level	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4 Activities and tasks 7.2.4.6 Design test strategy (TP5) c).	Test data requirements are required as part of the test strategy.
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.2 Identifying interoperable combinations of sub-systems 9.1.2.3 Interoperability relative to performance of a reference system	N/A	The ISO/IEC/IEEE 29119 series allow users to interpret the results of testing as they wish – for instance, as required by ISO/IEC 19795-4.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.2 Identifying interoperable combinations of sub-systems 9.1.2.4 Interoperability relative to the group under consideration	N/A	The ISO/IEC/IEEE 29119 series allow users to interpret the results of testing as they wish – for instance, as required by ISO/IEC 19795-4.
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.3 Acceptable numbers of interoperable subsystems	ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.2 Context of testing 7.2.2.2 Test items ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	The test plan records the items that are being tested, and the test summary report summarizes the testing performed against the test plan.

Table G.1 *(continued)*

ISO/IEC 19795-4:2008	ISO/IEC/IEEE 29119-2:2021 and ISO/IEC/IEEE 29119-3:2021	Rationale
9 Interpretation of the interoperability matrix 9.1 Determination of interoperable subsystems 9.1.4 Combinatorial search for maximum interoperability-classes	ISO/IEC/IEEE 29119-2 7.2 Test planning process 7.2.4.6 Design test strategy (TP5) a). ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.7 Test strategy 7.2.7.9 Metrics to be collected ISO/IEC/IEEE 29119-3 7.2 Test plan 7.2.8 Testing activities and estimates ISO/IEC/IEEE 29119-3 7.4 Test completion report 7.4.2 Summary of testing performed	ISO/IEC/IEEE 29119-3 states that the test strategy (part of the test plan) "shall" include activities to be performed and the metrics to be collected. The test activities would also describe how to handle the situation where interoperability is confined to disjoint sets of suppliers. The test completion report summarizes the testing performed against the test plan, which "should" record the method of searching.