



BSI Standards Publication

Software and systems engineering — Software testing

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

National foreword

This Published Document is the UK implementation of ISO/IEC TR 29119-13:2022.

The UK participation in its preparation was entrusted to Technical Committee IST/15/-/26, Software Testing.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 20567 1

ICS 35.080

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2022.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

**Software and systems engineering —
Software testing —**

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





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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

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

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms, 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	286

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 enrollees, 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 enrollees 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.

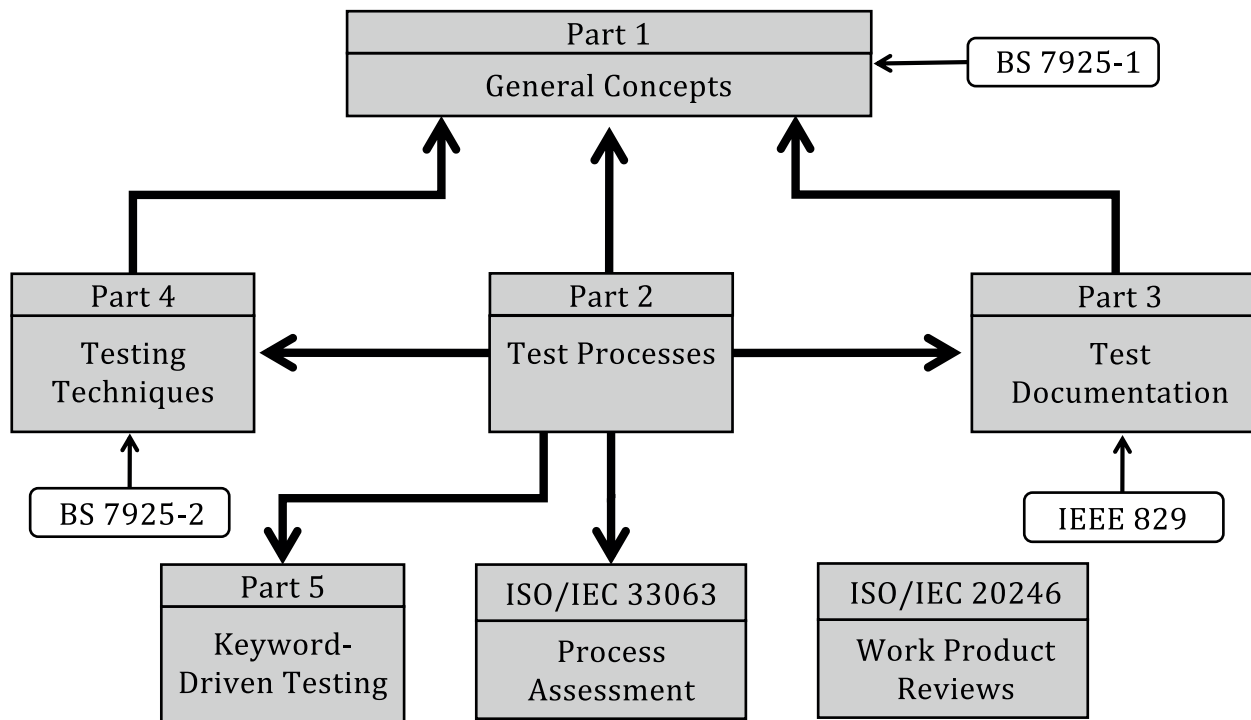


Figure 1 — ISO/IEC/IEEE 29119 software testing standards

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.

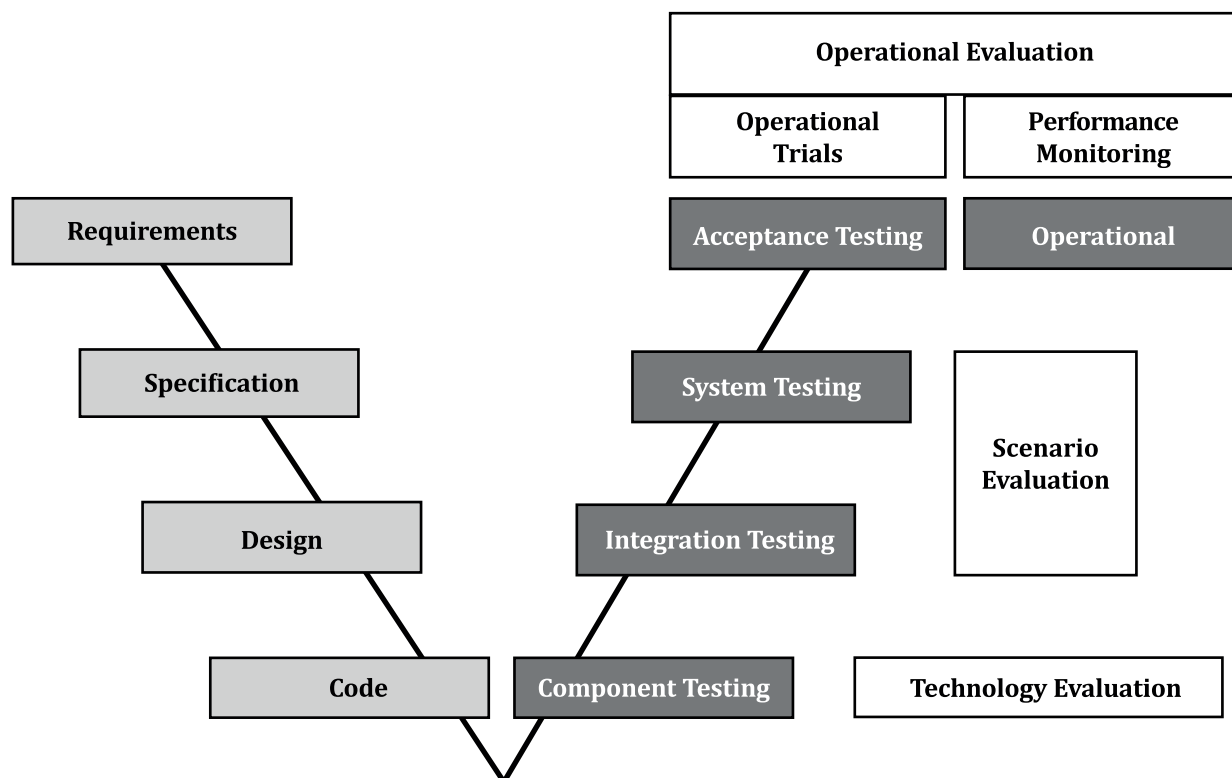


Figure 2 — Evaluation levels across the software lifecycle

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.

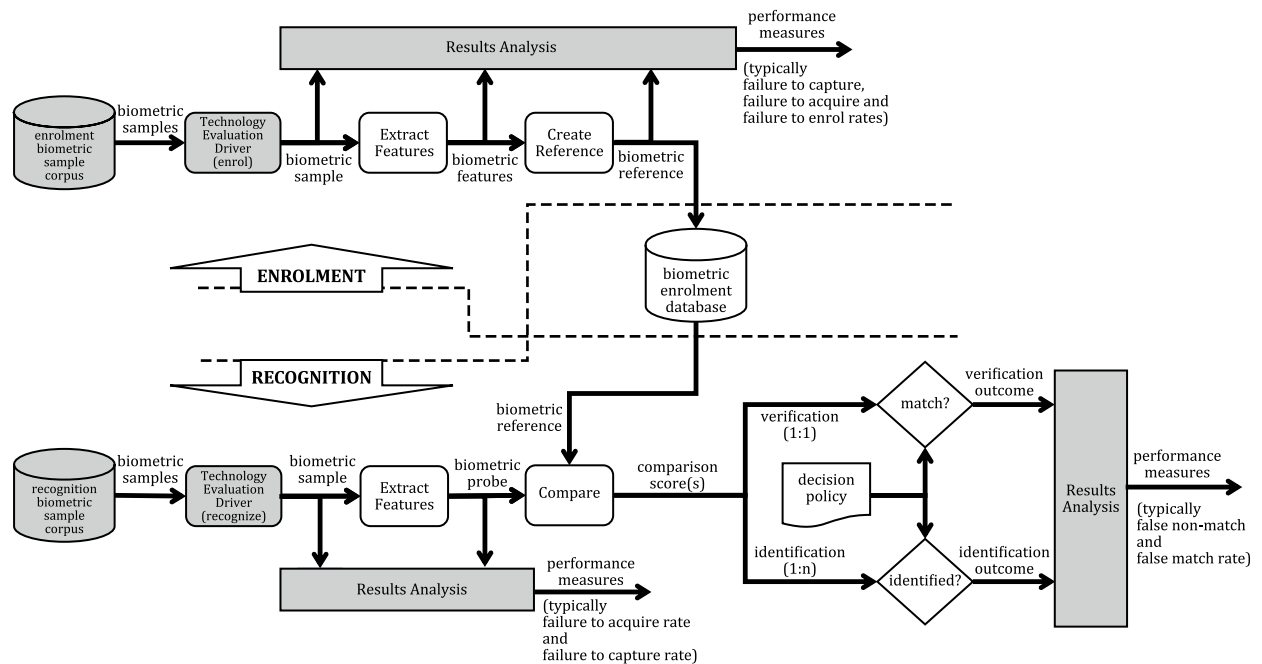


Figure 3 — Technology evaluation of biometric systems

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).

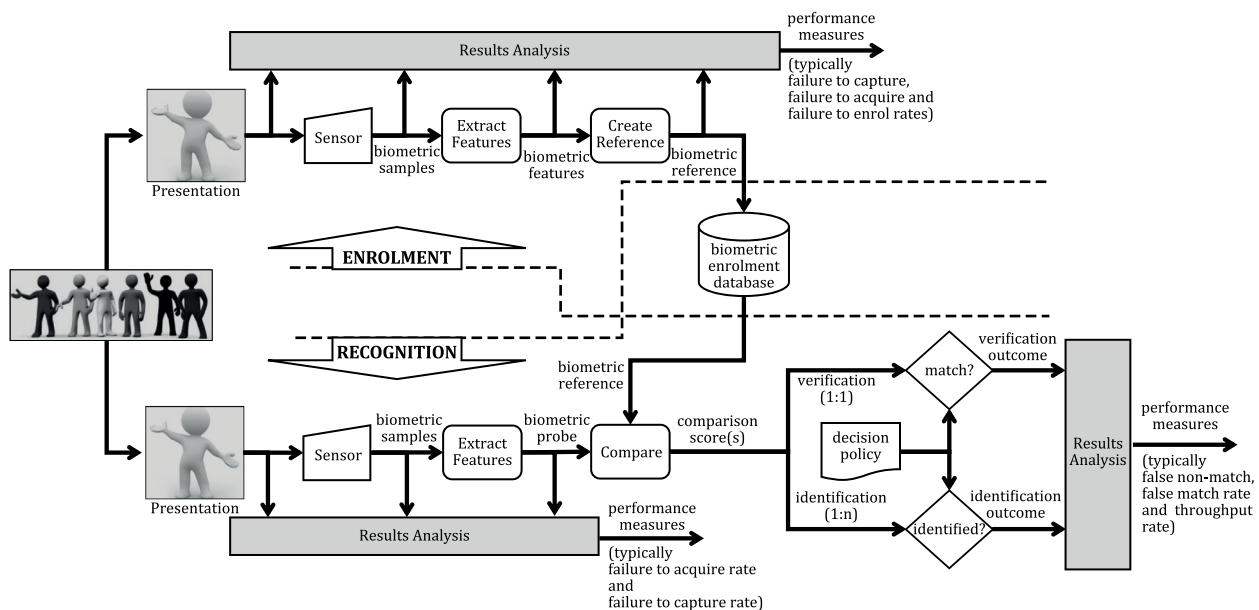


Figure 4 — Scenario evaluation of biometric systems

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.

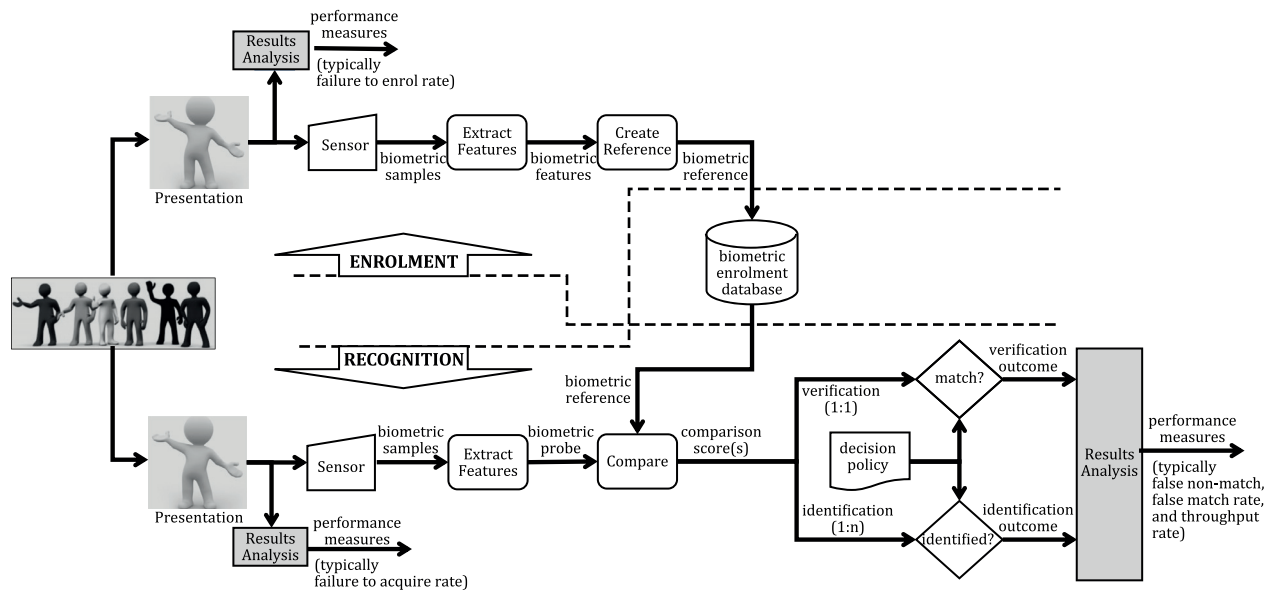


Figure 5 — Operational evaluation of biometric systems

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).

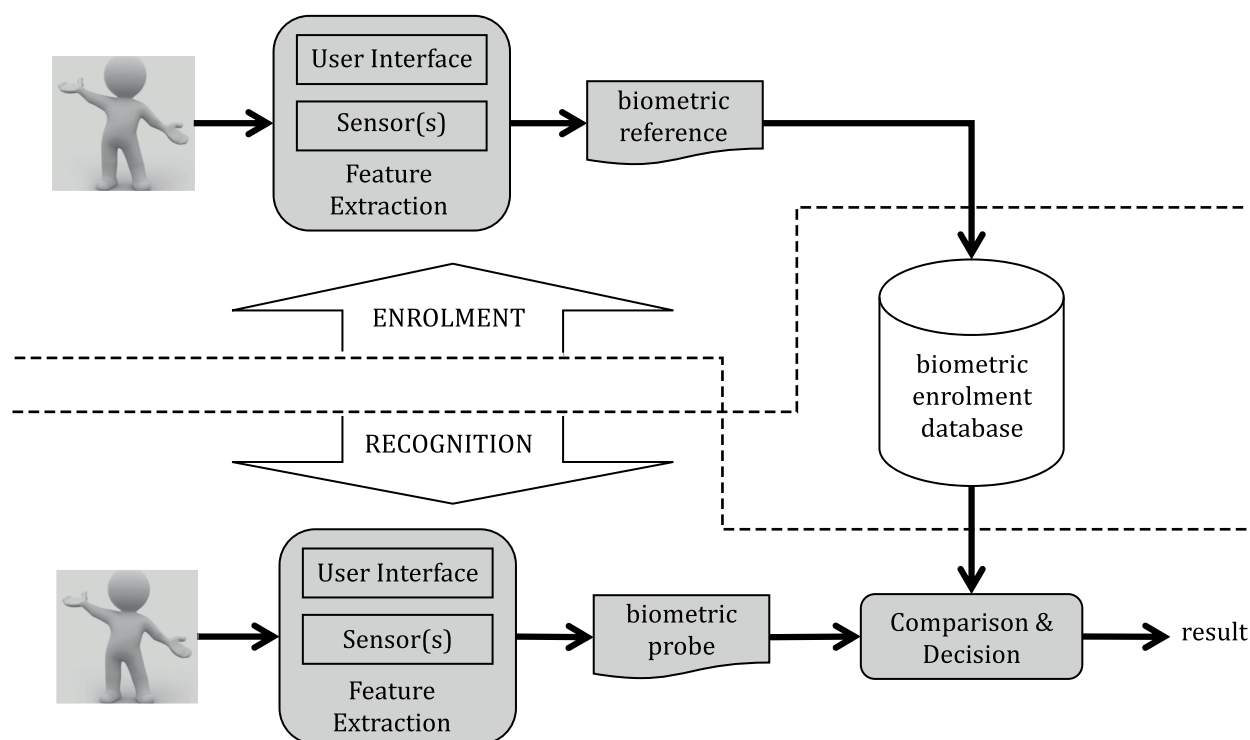


Figure A.1 — Generic biometric components – high level

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.

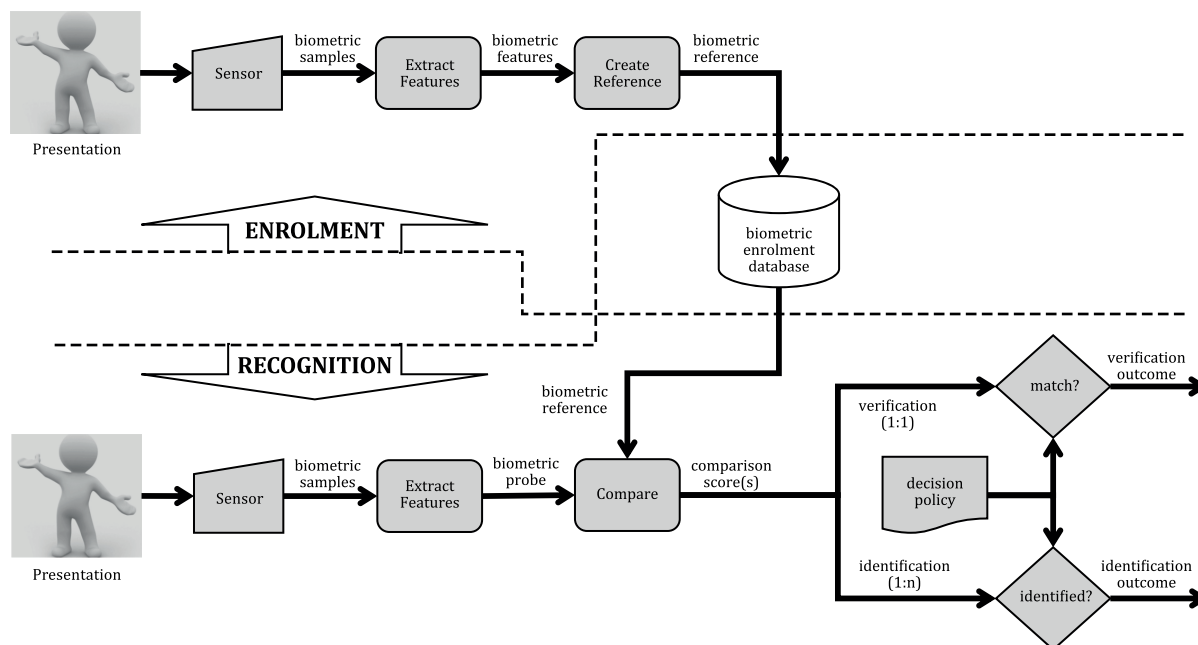


Figure A.2 — Generic biometric components - detailed

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.

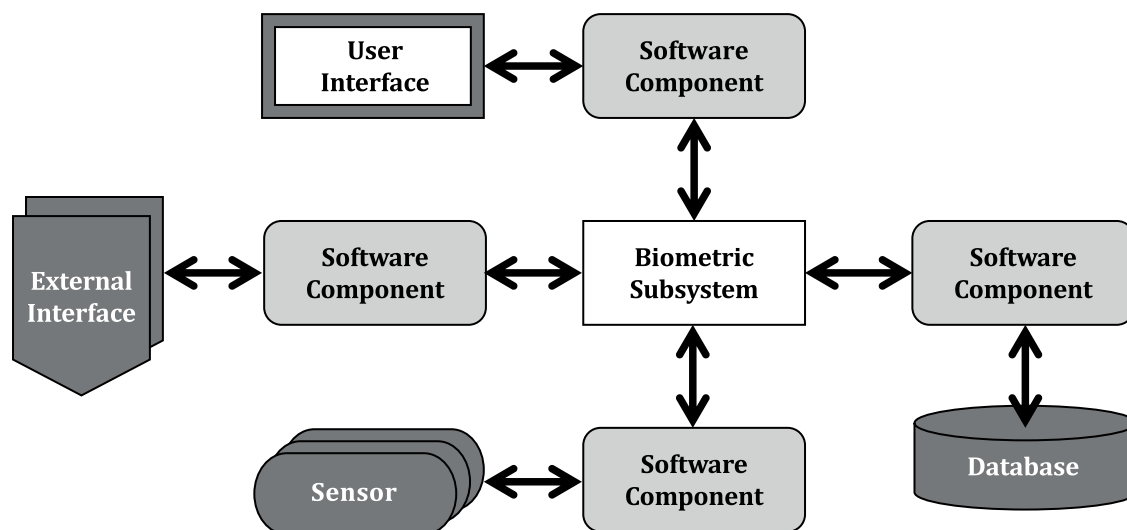


Figure A.3 — Generic biometric system

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).

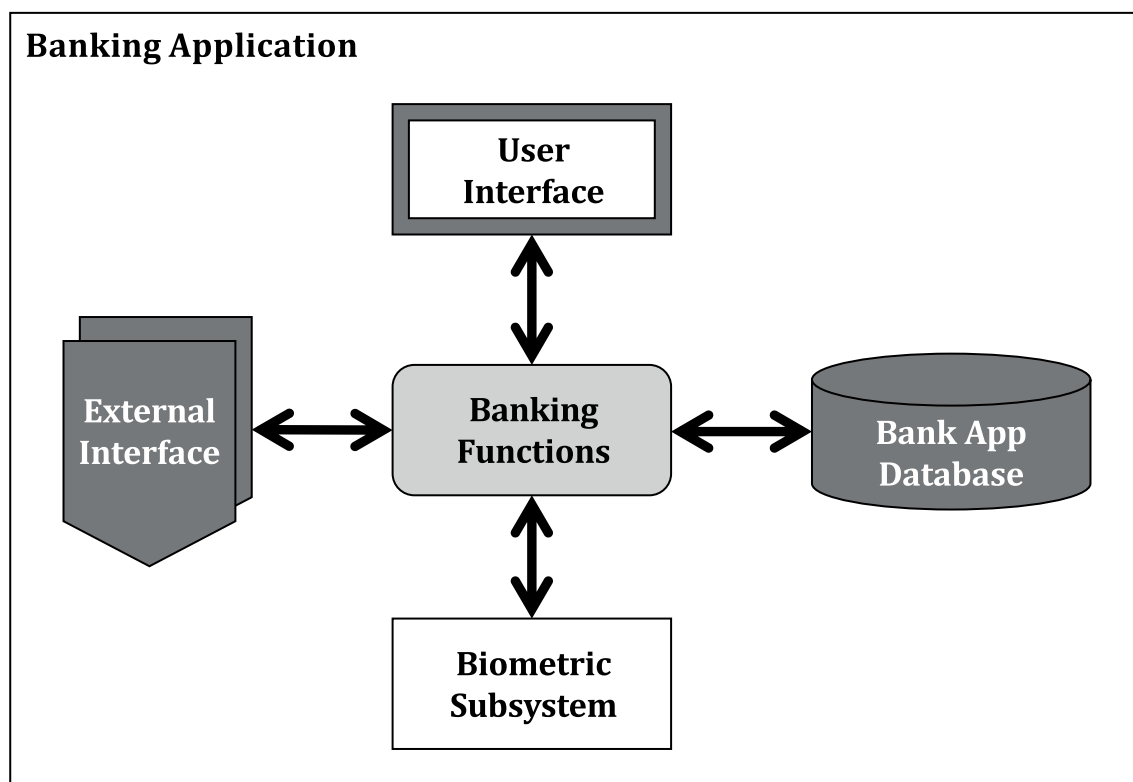


Figure A.4 — Example banking application with biometric subsystem

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 29197 describes 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.
It is possible the project is a new development (rather than an update to an existing biometric system)	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 technology to be implemented is new and/or complex	Review the required quality characteristics and confirm the requirements in this area are understood, testable, and clearly documented.
It is possible the biometric system will be implemented on multiple platforms	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 interface with multiple other systems	Test environments capable of simulating each platform are obtained for testing.
It is possible the biometric system will be implemented with biometric data stored on workstations	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 tokens or smartcards	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.
It is possible the biometric system will be implemented with biometric data stored on tokens or smartcards	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.
It is possible the biometric system will be implemented with biometric data stored on tokens or smartcards	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).
It is possible the assigned testers are inexperienced in biometrics	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 that training on biometrics is not available for testers	Employ testers with suitable skills and experience in biometrics, either on a permanent or contract basis to replace or supplement the assigned (inexperienced) testers.
It is possible there is insufficient time to train testers in biometrics	Train assigned testers in the area of biometrics.
It is possible the assigned testers are inexperienced in testing	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 the assigned testers become ill, or unavailable for some other reason	Employ new testers with experience in biometrics, either on a permanent or contract basis.
	Employ experienced testers, either on a permanent or contract basis to replace or supplement the assigned (inexperienced) testers.
	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.
It is possible the test tools were not selected based purely on technical merit	Train assigned testers in the area of test automation.
It is possible the test tools will not be available on time	Determine the suitability of the selected test tools and identify any gaps in test tool coverage.
It is possible the test tools are ineffective	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 environments are not ready on time	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.
	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.
It is possible the testers are not responsible for managing the test environments	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 that hardware is not available for system integration testing	Where test environments are managed separately, form a close relationship with those setting up and maintaining the test environments.
It is possible the sensor types/makes used for testing do not match the operational system sensor types/makes	Ensure that test environment requirements are provided as early as possible and in sufficient detail. 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 high cleanliness of sensors used for testing does not match the relatively poor operational system sensor cleanliness	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.
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	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.
It is possible the number and positioning of sensors used for testing do not match the operational system number and positioning	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 there is no clarity on who approves acceptance tests	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.
It is possible the number and positioning of sensors used for testing do not match the operational system number and positioning	Alternatively, source old sensors of the correct make and type for inclusion as part of the test environment.
It is possible there is no clarity on who approves acceptance tests	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.
It is possible there is no clarity on who approves acceptance tests	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.