



DPC: 23 / 30450875 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: + 44 (0)20 8996 9000

Fax: + 44 (0)20 8996 7400

www.bsigroup.com

Date: 1 May 2023

Origin: National

Latest date for receipt of comments: 14 July 2023

Project No. 2022/00099

Responsible committee: ICT/3 Trustworthy Software

Interested committees: IST/15 and IST/33/1

Title: Draft BS 10754-0 Information technology - Systems trustworthiness

Part 0: Overview and concepts

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 14 JULY 2023**

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: + 44(0)20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Editorial Project Manager: **Kevin Lavery**
Direct tel: **020 8996 7492**
E-mail: kevin.lavery@bsigroup.com

Introduction

Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international and European standards, comments will be reviewed by the relevant UK national committee before submitting the consensus UK vote and comments. If the draft standard is approved, it is usual for the resulting published standard to be adopted as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

BSI Committee Responsibilities

Whether or not the standard is published in its original (international) form, or as a formal British Standard Implementation the BSI committee's responsibilities are to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related International and European developments and promulgate them in the UK.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

Annotated drafts are not acceptable and will be rejected.

All comments should be submitted online at <http://standardsdevelopment.bsigroup.com>. You will need to register in order to comment.

BS 10754-0:2023

Information technology – Systems trustworthiness

Part 0: Overview and concepts

BS 10754-0:2023

BRITISH STANDARD

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 20955 6

ICS

The following BSI references relate to the work on this document:
Committee reference ICT/3
Draft for comment

Publication history

Amendments issued since publication

Date

Text affected

Contents

Foreword	5
0 Introduction	6
0.1 General	6
0.2 Purpose of BS 10754	7
0.3 Intended audiences	7
0.4 Structure of BS 10754 series	7
<i>Figure 1 – BS 10754 related to other standards</i>	9
1 Scope	9
2 Normative references	10
3 Terms, definitions and abbreviated terms	10
3.1 Terms and definitions	10
3.2 Abbreviated terms	32
4 Introduction to system and software trustworthiness	32
4.1 General	32
4.2 Context	32
4.3 What is a trustworthy entity?	33
4.4 Identification of trustworthiness characteristics by domains	33
4.5 Not all entity requires the same level of trustworthiness	33
4.6 Demonstrating trustworthiness	34
<i>Figure 2 – Assumption vs assurance during the trustworthiness risk management process</i>	34
5 Trustworthiness overview	34
5.1 Trustworthiness principles	34
<i>Figure 3 – Relationships between source of trustworthiness risks and required evidence</i>	35
5.2 Concepts	37
<i>Figure 4 – Example of environments of an entity during its life cycle</i>	38
<i>Figure 5 – Operational environment of an entity</i>	39
<i>Figure 6 – Types of information item to protect, related to an entity</i>	40
<i>Table 1 – Twelve types of information item involved in an entity</i>	40
<i>Figure 7 – Baseline trustworthiness characteristics</i>	42
<i>Table 2 – Risk and impact related to trustworthiness baseline characteristics</i>	43
<i>Table 3 – Non-baseline trustworthiness characteristics</i>	48
<i>Figure 8 – Sources of trustworthiness risks for an entity</i>	56
<i>Figure 9 – System requirement types and categories overview</i>	58
<i>Figure 10 – Trustworthiness control overview</i>	59
<i>Figure 11 – TC as a graph example</i>	61
<i>Figure 12 – TC library example</i>	62
<i>Figure 13 – Implementation of controls across the entity's life cycle</i>	64
<i>Figure 14 – Trustworthiness assurance level management overview</i>	66
<i>Figure 15 – Maturity levels overview adapted from CMMi</i>	68
5.3 Trustworthiness frameworks	68
<i>Table 4 – BS 10754 Frameworks</i>	68
<i>Figure 16 – Organization normative framework</i>	69
<i>Figure 17 – Entity normative framework</i>	73
<i>Figure 18 – Verification normative framework</i>	75
6 Trustworthiness overall approach	76
6.1 General	76
<i>Figure 19 – BS 10754 trustworthiness management approach</i>	77
6.2 Processes	77
<i>Figure 20 – ONF management processes overview</i>	78
<i>Figure 21 – Entity Trustworthiness management process</i>	79
<i>Figure 22 – Trustworthiness verification scheme management process</i>	81
Annex A (informative) Complete list of trustworthiness characteristics	83

Figure A.1 – Entity trustworthiness characteristics 83
Bibliography 84

Foreword

Publishing information

This part of BS 10754 is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on **XX Month 202X**. It was prepared by Technical Committee ICT/3, *Trustworthy Software*. A list of organizations represented on this committee can be obtained on request to the committee manager.

Supersession

Together with BS 101754-0:2023 and BS 10754-3:2023, this Part of BS 10754 supersedes BS 10754-1:2018, which is withdrawn.

Relationship with other publications

BS 10754, *Information technology – Systems trustworthiness*, comprises the following parts:

- Part 0: *Overview and concepts*;
- Part 2: *Implementation and management – Specification*; and
- Part 3: *Validation, verification and certification – Specification*.

Information about this document

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g., “organization” rather than “organisation”).

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.

Compliance with a British Standard cannot confer immunity from legal obligations.

0 Introduction

0.1 General

A system includes services, software and data, and can be used in many contexts for many purposes. The system has to conform to the laws and regulations applicable in the countries where it is developed, deployed and used.

Systems and software can be acquired through in-house development, outsourcing or purchase of a commercial product. They might also be acquired through a combination of these approaches, which can result in new risks related to trustworthiness that need to be assessed and managed.

People and organizations need to know that the information and technology they use are adequately protected so that they can use them with confidence. Traditionally, this has been addressed at the IT security level by protecting the perimeter and components of the technology infrastructure such as computers, devices, and networks, but this is generally insufficient.

However, systems and software also need to be protected against vulnerabilities that can:

- a) be inherent in an entity¹ itself (e.g. software defects);
- b) arise during the life cycle of the entity concerned (e.g. through changes due to system evolution); or
- c) occur as a result of the entity being used in an environment or contexts for which it was not intended.

Delivering entity trustworthiness is complex as it requires the simultaneous assessment of several other trustworthiness-related characteristics. Organizations also face growing needs that are not limited to information security, including the management of additional risks such as those related to safety, privacy and system reliability.

The goal of information security is to protect the information, regardless of the source of the threat.

The goal of system or software security is to protect the information involved in the use of this entity, regardless of the source of the threat.

The goal of entity trustworthiness is to mitigate trustworthiness risks and provide evidence that the entity is trustworthy in specific environments, regardless of the source of the threat.

A systematic approach to building trustworthiness in systems and software provides evidence that the trustworthiness risks associated with the entity are adequately mitigated.

Throughout its life cycle, a trustworthy entity has prerequisite trustworthiness characteristics, such as predictable performance and compliance, and meets trust-building requirements in terms of development, management and operation of its technology infrastructure and audits. Enhanced trustworthiness processes and practices, as well as qualified people to implement them, are required to create a trustworthy entity that does not increase risk exposure beyond an acceptable or tolerable level of residual risk.

In addition, a trustworthy entity takes into account several types of requirements (e.g. security, robustness, privacy, reliability, safety) arising from the type of data, the target environment (business, regulatory, technological, ecological, societal and ethical contexts) and the stakeholders, as well as the system specifications. Trustworthiness requires the ability to obtain at any time a demonstration supported by expected evidence that an acceptable (or tolerable) level of residual risk has been achieved and is being maintained.

¹ In this British standard, the term “entity” relates to a system or software.

When used as a standalone document for organizations with no current approach to system or software trustworthiness, BS 10754 facilitates the implementation of trustworthy frameworks (TFs) in their many guises, from embedded equipment through consumer devices, to IoT solutions and industrial control systems.

Where organizations already address entity trustworthiness through one or more trustworthiness characteristics in isolation BS 10754 provides a companion and complement to other relevant standards.

0.2 Purpose of BS 10754

BS 10754 sets out a standardized approach to:

- a) integrating trustworthiness into the entity life cycle process that is applicable to any entity:
 - 1) developed in-house; or
 - 2) acquired from third parties; or
 - 3) part or the complete development or the operation of which is outsourced; and
- b) conceptually determining, generating and collecting the agreed evidence needed to demonstrate in a verifiable way that the entity is trustworthy in a defined environment.

It identifies the trustworthiness ecosystem and provides frameworks for identifying, validating, implementing, verifying and demonstrating trustworthiness for an entity.

0.3 Intended audiences

Potential users of BS 10754 include developers and assurance case managers, as well as those wishing to develop, maintain, assess or acquire a system that meets the requirements of specific trustworthiness characteristics.

Specifically, this document is intended to be used by the following.

- a) **Organization experts**, such as system suppliers, acquirers, managers, architects, developers, and other IT experts who:
 - 1) manage risks, costs, trustworthiness requirements and resources, and who are potentially accountable for system trustworthiness;
 - 2) implement, maintain, and verify and demonstrate that a system or software is trustworthy; or/and
 - 3) have to demonstrate that the system satisfies trustworthiness requirements by implementing and managing trustworthiness controls throughout the system and/or software life cycle.
- b) **Authority experts**, such as authorities, certification bodies and auditors who evaluate, validate, verify and/or audit if trustworthiness was adequately implemented and maintained in a system or a software.
- c) **End users**, who need to be able to trust the software or system they are using.

0.4 Structure of BS 10754 series

0.4.1 Part 0 – Overview and concepts

Part 0 provides an overview of what can impact the trustworthiness of a system and software and introduces key elements that are addressed in the requirements other parts of BS 17054.

It introduces key definitions, concepts, frameworks, components and processes to assist organizations in integrating trustworthiness seamlessly throughout the life cycle of their systems or their software.

0.4.2 Part 2 – Implementation and management

Part 2 specifies the creation, maintenance and validation of an organization normative framework (ONF), its components and the organization-level processes for managing it, to deliver consistent and approved trustworthiness elements across the organization. It sets out the relationships between these processes, the activities associated with them, and the means by which they support the entity trustworthiness management process (ETMP). It specifies the components and activities an organization needs to integrate to implement trustworthiness in its existing processes.

It also specifies the processes involved in an entity (i.e. system, software) project: determining the requirements and environments, assessing the trustworthiness risks, creating and maintaining the entity normative framework (ENF), developing/sourcing/acquiring and operating the entity, and validating its trustworthiness throughout its life cycle. It specifies the relationships among these processes, their activities, and interdependencies, and how they introduce trustworthiness into a entity project. It sets out the components and activities to be integrated into an organization's existing processes to deliver trustworthiness on a project-level.

It also sets out how to create, maintain and validate trustworthy entity in a uniform way across the organization. It explains how the project team can implement and reuse an organization's approved system trustworthiness elements in their entity project.

0.4.3 Part 3 – Validation, verification and certification

Part 3 specifies the system/software trustworthiness validation, verification, audit and certification process for organizations, systems, software and people.

It specifies verification and auditing on three levels:

- a) **Organization level**, at which auditors validate the organization's system trustworthiness objectives and audit/attest that the organization satisfies the entity trustworthiness objectives and criteria;
- b) **System and software level**, at which auditors measure the entity's actual level of trustworthiness (LoT) and compare this with the entity's target LoT previously selected by the organization, to attest that the entity is as trustworthy as expected; and
- c) **People level**, at which it provides the criteria to be used with BS EN ISO/IEC 17024 for demonstrating the trustworthiness of individuals.

To assist organizations to verify and audit trustworthiness on organization, system, software and people, Part 3 specifies the use of the verification normative framework (VNF). It was developed to help an authority to define a trustworthiness verification scheme, help the organization to implement it, and help auditors to verify the compliance of organizations and entity to this verification scheme.

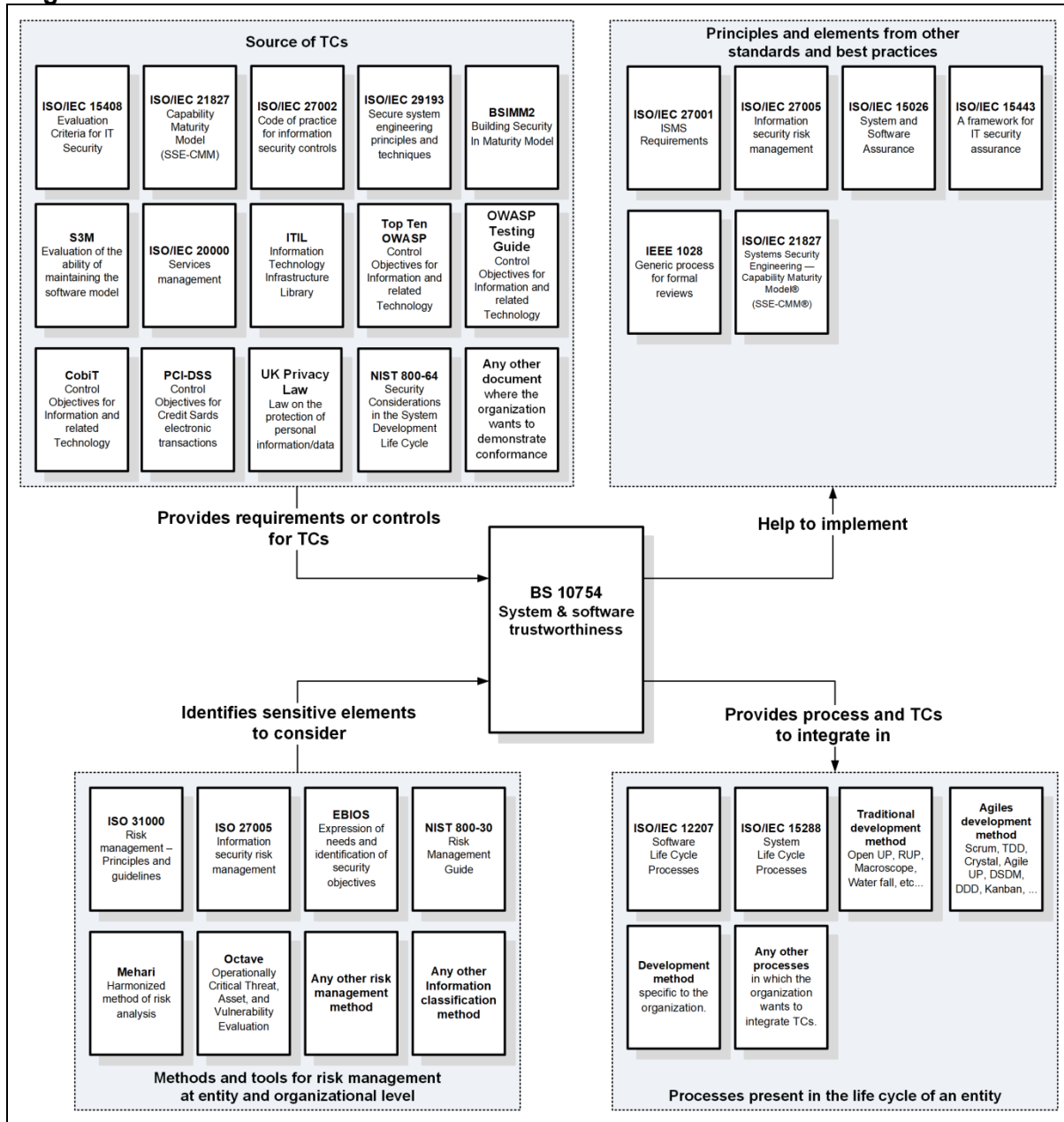
0.4.4 Relationship to other standards

BS 10754 provides a framework for achieving trustworthiness of systems that intersects with a variety of disciplines with which familiarity is necessary, in particular:

- a) system life cycle processes, as set out in ISO/IEC 12207, ISO/IEC 15288 and relevant standards from ISO/IEC JTC 1 SC7;
- b) security, as set out in ISO/IEC 27001, ISO/IEC 27002 and relevant amplifying standards from ISO/IEC JTC 1 SC27; and
- c) quality, as set out in ISO 9001.

Figure 1 shows the relationships between BS 10754 and four groups of documents: models, methods, national standards and international standards.

Figure 1 – BS 10754 related to other standards



The first group “Source of TCs” comprises documents that can be referenced as sources of requirements and controls that can be used to define trustworthiness controls. The second group “Principles and elements from other standards and best practices” comprises documents that can be implemented by conformity to BS 10754. The third group “Methods and tools for risk management at entity and organizational level” comprises documents that can be used to implement risk management in order to identify sensitive entities that need to be trustworthy. The final group comprises documents that propose methods and processes into which TCs can be incorporated.

1 Scope

This part of BS 1075 defines the overall concepts and principles for effective entity trustworthiness, including technical, physical, cultural and behavioural measures and effective leadership and governance. It presents frameworks and processes for delivering and demonstrating entity trustworthiness characteristics such as safety, reliability, availability, resilience and security.

It is intended to provide a widely applicable approach that can be customized for any organization adopting entity trustworthiness practices.

This part of BS 10754 does not provide detailed processes or actions for an organization to follow in order to achieve entity trustworthiness.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes provisions of this document.²⁾ For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS ISO/IEC 11179-5, *Information technology — Metadata registries (MDR) — Part 5: Naming principles*

BS ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

BS ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

BS ISO/IEC/IEEE 15288, *Systems and software engineering — System life cycle processes*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

3.1.1 Trustworthiness related definitions

3.1.1.1 entity

physical or abstract thing of interest having a distinct existence

NOTE For the purposes of this British Standard, “entity” can refer to a system or software of interest.

EXAMPLES

Enterprise, organization, solution, system (including software systems), subsystem, process, business, data (as a data item or data structure), application, information technology (as a collection), mission, product, service, software item, hardware item, product line, family of systems, system of systems, collection of systems, collection of applications.

[SOURCE: BS ISO/IEC 20924:2018, **3.1.18**, and BS ISO/IEC TR 24028:2020, **3.16**, modified]

3.1.1.2 entity of interest

subject which is under consideration

NOTE 1 This document distinguishes the entity of interest from other entities which are not under consideration.

NOTE 2 In this document, interest in an entity is intended to encompass interest in that entity’s environment, life cycle, architecture, requirements, design, implementation and operation. Such interests are captured via aspects, concerns and stakeholder perspectives.

[SOURCE: BS ISO/IEC/IEEE 42010:2022, **3.12**, modified]

3.1.1.3 interest in the entity

main purposes to be taken into account when assessing the entity

²⁾ Documents that are referred to solely in an informative manner are listed in the Bibliography.

NOTE The interest in the entity outlines its main objectives, functionality and stakeholders, and specifies the environments (3.1.1.4) in which it is to be developed, maintained, used and verified, and by whom.

3.1.1.4 environment

context of surrounding things, conditions, or influences upon an entity

NOTE 1 The environment of an entity of interest (3.1.1.2) includes external entities that can have various influences upon that entity, such as developmental, technological, business, operational, organizational, political, economic, legal, regulatory, ecological, and societal influences, as well as external physical effects such as electromagnetic radiation, charged particles, gravitational effects, and electric and magnetic fields.

NOTE 2 A label attached as a qualifier to the word environment identifies a particular sub-context within that environment, such as development environment, test environment, and operational environment.

NOTE 3 In this document, these surrounding things, conditions, or influences are referred as context, such as: business sector context, regulatory context, technological context, ecological context, societal and ethical context in which a system or a software is used and operated, including all actors, processes, products, information, and technology involved in these contexts.

[SOURCE: ISO/IEC/IEEE 42010:2022, **3.13**, modified]

3.1.1.5 stakeholder's trustworthiness expectations

list of expectations obtained from and associated with stakeholders (3.1.3.30) of interest

3.1.1.6 entity trustworthiness/system trustworthiness/software trustworthiness

entity's ability to meet stakeholders' trustworthiness expectations (3.1.1.5) in a verifiable (3.1.3.40) way throughout its life cycle

NOTE 1 Entity trustworthiness is reviewed and maintained during the entity's complete life cycle.

NOTE 2 Entity trustworthiness can be expressed with a level of trustworthiness (3.1.1.17).

3.1.1.7 trust

firm belief that an entity fulfils the stakeholder's trustworthiness expectations related to its environment

3.1.1.8 trustworthiness

ability to meet stakeholders' expectations (3.1.1.5) in a verifiable (3.1.3.40) way

NOTE 1 Depending on the context or sector, also on the specific product or service, data, technology and process used, different characteristics apply and need verification to ensure stakeholders' expectations are met.

NOTE 2 Characteristics of trustworthiness may include, for instance, accountability, accuracy, authenticity, availability, controllability, integrity, privacy, quality, reliability, resilience, robustness, safety, security, transparency and usability.

NOTE 3 Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as to organizations.

NOTE 4 Verifiability (3.1.3.40) includes measurability (3.1.3.17) and demonstrability by means of objective evidence.

[SOURCE: PD ISO/IEC TS 5723:2022, **3.1.1**, modified – notes has been added]

3.1.1.9 trustworthiness assumption

factor in the trustworthiness process that is considered to be true, real, or certain, without proof or demonstration

[SOURCE: A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Fifth Edition [1]]

[SOURCE: BS ISO/IEC/IEEE 24765:2017, **3.276**, modified]

3.1.1.10 trustworthiness assurance

grounds for justified confidence that a trustworthiness claim has been or will be achieved

NOTE 1 By definition, trustworthiness assurance is about expected evidence supporting a trustworthiness claim.

NOTE 2 The claim can be a conjunction of more than one claim.

[SOURCE: BS ISO/IEC/IEEE 15026-4:2021, **3.1**, modified]

3.1.1.11 trustworthiness control (TC)

control (**3.1.3.7**) required to address trustworthiness requirements and demonstrate related trustworthiness risks mitigation with expected supporting evidence

NOTE 1 A trustworthiness control includes the mitigation activity and the verification-measurement activity that will provide expected repeatable evidence that it is being implemented and is adequately mitigating the associated risks as intended.

NOTE 2 TCs require a data structure containing a precise enumeration and description of a trustworthiness activity and its associated verification-measurement activity to be performed at a specific moment in a system's life cycle

NOTE 3 Each TC is used to mitigate one or many unacceptable trustworthiness risks, specified by trustworthiness requirements.

3.1.1.12 trustworthiness ecosystem

complex system of interdependent organizations, peoples, processes, tools and other components from the public and private sectors that work together to enable trustworthiness within specific environments

[SOURCE: BS ISO 37106:2021, **3.1**, modified]

3.1.1.13 trustworthiness requirement

requirement expressed to mitigate a trustworthiness risk

3.1.1.14 trustworthiness risk

risk related to trustworthiness characteristics

NOTE 1 Any risk related to a trustworthiness characteristic can be considered as a trustworthiness risk such as: privacy risk, information security risk, safety risks or reliability risks.

NOTE 2 Assessing trustworthiness risks can be as simple as asking: "What will be the impact if risks related to this or these trustworthiness characteristics are not mitigated?"

3.1.1.15 trustworthy entity

entity that is considered trustworthy, dependable or reliable because its actual level of trustworthiness (**3.1.1.19**) is equal or greater than its target level of trustworthiness (**3.1.1.18**)

NOTE 1 At this point and beyond trust is completely based on assurance. An entity is only considered trustworthy when all evidence claims have been verified, and it has demonstrated its ability to meet stakeholders' trustworthiness requirements (i.e. stakeholders' expectations leading to unacceptable risks).

*NOTE 2 In this document, a system or a software is only considered trustworthy when its actual level of trustworthiness (**3.1.1.19**) is equal or greater than its target level of trustworthiness (**3.1.1.18**), as defined for specific environments by the system owner, an authority, a person, and/or an organization using the system (i.e., entity where the targeted LoT is confirmed by the actual LoT measurement).*

[SOURCE: BS ISO/IEC 27034-1:2011, **3.20**, modified]

3.1.1.16 level of trust/level of trustworthiness (LoT)

label identifying well-formed list of required trustworthiness controls (**3.1.1.11**) representing a point on the pre-defined assurance scale

NOTE 1 An entity level of trustworthiness is only valid for the environments in which it has been evaluated, taking into account the entity's specifications.

NOTE 2 The verification-measurement activity included in each trustworthiness control will produce the expected evidence that the control has been properly implemented, properly verified, and that it mitigates the targeted risks as expected.

[SOURCE: BS ISO/IEC 15408-1:2022, **3.39**, modified]

3.1.1.17 target level of trust/target level of trustworthiness (TLot)

list of trustworthiness controls (**3.1.1.11**) to be implemented and verified during an entity's life cycle

NOTE A target LoT is usually defined and/or required by the system owner or an authority.

3.1.1.18 actual level of trust/actual level of trustworthiness (ALot)

result of an audit process that provides supporting evidence that all trustworthiness controls (**3.1.1.11**) listed in the target level of trustworthiness (**3.1.1.18**) for an entity have been correctly implemented and verified at a specific time, and have produced the expected outcomes

[SOURCE: BS ISO/IEC 27034-1, **3.2**, modified]

3.1.1.19 organization normative framework (ONF)

authoritative repository that contains trustworthiness elements approved by the organization

3.1.1.20 entity normative framework (ENF)

authoritative repository linked to a specific entity, which contains the results of the trustworthiness processes and the elements required to implement entity trustworthiness during its life cycle

3.1.1.21 verification normative framework (VNF)

authoritative repository for processes and components used to define and maintain verification schemes, and perform measurable and repeatable entity trustworthiness verifications and audits

3.1.2 Trustworthiness characteristics

NOTE A complete list of trustworthy characteristics is given in Annex A.

3.1.2.1 accessibility

degree to which an entity is easy to use by all people, including those with disabilities

*NOTE This property is a sub-characteristic of interaction capability/usability (**3.1.2.45**).*

[SOURCE: ISO/IEC TR 13066-2:2016, **2.2**, modified]

3.1.2.2 accountability

property that ensures that the actions of an entity can be traced uniquely to person or the entity

*NOTE This property is a sub-characteristic of security (**3.1.2.75**).*

[SOURCE: ISO 17090-1:2013, **3.2.2**, modified]

3.1.2.3 accuracy/measurement accuracy/accuracy of measurement

closeness of agreement between a measured quantity value and a true quantity value of a quantity intended to be measured

NOTE 1 The concept "measurement accuracy" is not a quantity and is not given a numerical quantity value. A measurement is said to be more accurate when it offers a smaller measurement error.

NOTE 2 The term "measurement accuracy" is not the same as measurement trueness and the term "measurement precision" is not the same as "measurement accuracy", which, however, is related to both these concepts.

NOTE 3 "Measurement accuracy" is sometimes understood as closeness of agreement between measured quantity values that are being attributed to the measurand.

[SOURCE: ISO/IEC Guide 99:2007, **2.13** and **2.3**]

3.1.2.4 adaptability

degree to which an entity can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments

NOTE 1 Adaptability includes the scalability of internal capacity (e.g. screen fields, tables, transaction volumes, report formats).

NOTE 2 Adaptations include those carried out by specialized support staff, and those carried out by business or operational staff, or end users.

NOTE 3 This property is a sub-characteristic of flexibility (3.1.2.33) and replaceability (3.1.2.68).

[SOURCE: BS ISO/IEC 25010:2011, 4.2.8.1, modified]

3.1.2.5 analysability

degree of effectiveness and efficiency with which it is possible to assess the impact on an entity of an intended change to one or more of its parts, or to diagnose an entity for deficiencies or causes of failures, or to identify parts to be modified

NOTE 1 The implementation process can include providing mechanisms for the product or system to analyse its own faults and provide reports prior to a failure or other event.

NOTE 2 This property is a sub-characteristic of maintainability (3.1.2.49).

[SOURCE: BS ISO/IEC 25010:2011, 4.2.7.3, modified]

3.1.2.6 appropriateness recognizability

degree to which users (3.1.3.38) can recognize whether an entity is appropriate for their needs

NOTE 1 Appropriateness recognizability depends on the ability to recognize the appropriateness of the entity's functions from initial impressions of the entity and/or any associated documentation.

NOTE 2 The information provided by the entity can include demonstrations, tutorials, documentation or, for a web site, the information on the home page.

NOTE 3 This property is a sub-characteristic of interaction capability/usability (3.1.2.45).

[SOURCE: BS ISO/IEC 25010:2011, 4.2.4.1, modified].

3.1.2.7 authenticity

property that an entity can be proved to be the one claimed to be

NOTE 1 Authenticity applies to entities such as users, processes, systems, and information.

NOTE 2 This property is a sub-characteristic of security (3.1.2.75).

[SOURCE: BS EN ISO/IEC 27000:2020, 3.6, modified]

3.1.2.8 availability

property of being accessible and usable upon demand by an authorized entity and/or stakeholder

NOTE 1 This property applies as much to a system as it does to information.

NOTE 2 This property is a sub-characteristic of security (3.1.2.75) and dependability (3.1.2.19).

[SOURCE: BS EN ISO/IEC 27000:2020, 3.7, modified]

3.1.2.9 business continuity

capability of an organization to continue delivery of products, or services within acceptable time frames at predefined capacity during a disruption

NOTE This property is a sub-characteristic of continuity (3.1.2.17).

[SOURCE: BS EN ISO 22301:2019, 3.3, modified]

3.1.2.10 capacity

degree to which the maximum limits of an entity parameter meet requirements

NOTE 1 Parameters can include the number of items that can be stored, the number of concurrent users, the communication bandwidth, throughput of transactions, and size of database.

NOTE 2 This property is a subcharacteristic of performance efficiency (3.1.2.59).

[SOURCE: BS ISO/IEC 25010:2011, **4.2.2.3**, modified]

3.1.2.11 changeability

fact of being likely to change; fact of changing often

NOTE This property is a sub-characteristic of modifiability (3.1.2.52).

[SOURCE: Oxford dictionary]

3.1.2.12 co-existence

capability of an entity to perform its required functions efficiently while sharing a common environment and resources with other entities, without detrimental impact on any other entity

NOTE This property is a sub-characteristic of compatibility (3.1.2.13).

[SOURCE: BS ISO/IEC 25010:2011, **4.2.3.1**, modified]

3.1.2.13 compatibility

suitability of entities for use and/or interaction together under specific conditions to fulfil relevant requirements without causing unacceptable interactions

NOTE In addition, sub-characteristic specialization such as interoperability (3.1.2.46) and co-existence (3.1.2.12) can also be involved.

[SOURCE: ISO/IEC Guide 2:2004, **2.2**, modified]

3.1.2.14 confidentiality

property that entity or information is not made available or disclosed to unauthorized persons, entities, or processes

[SOURCE: BS EN ISO/IEC 27000, **3.10**, modified]

NOTE 1 This property applies as much to an entity as it does to information. See entity confidentiality (3.1.2.24), information confidentiality (3.1.2.40) and personal information/data confidentiality (3.1.2.60).

NOTE 2 This property is a sub-characteristic of security (3.1.2.5) and privacy (3.1.2.63).

3.1.2.15 conformity

compliance (3.1.3.4) with a specified requirement

[SOURCE: BS EN ISO 9000:2015, **3.6.11**]

3.1.2.16 consent traceability

property that ensures that the consent on personal data can be traced uniquely to the personal data and the personal data object from which it originates

NOTE This property is a sub-characteristic of privacy (3.1.2.63).

3.1.2.17 continuity

degree to which the service (3.1.3.27) is provided under all foreseeable circumstances, including mitigating the risks resulting from interruption to an acceptable level

[SOURCE: PD ISO/IEC TS 25011:2017, **3.2.4.1**, modified]

NOTE In addition, sub-characteristic specialization, such as business continuity (3.1.2.9), service continuity (3.1.2.77) and entity continuity (3.1.2.25) can also be involved.

3.1.2.18 controllability

ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures

EXAMPLE:

If the entity is a vehicle then persons involved can include the driver, passengers, or persons in the vicinity of the vehicle's exterior.

[SOURCE: BS ISO 26262-1:2018, **3.25**, modified]

NOTE 3 This property is a sub-characteristic of safety (3.1.2.73).

3.1.2.19 dependability

<of an item> ability to perform as and when required

NOTE 1 In addition, sub-characteristic such as availability (3.1.2.8), reliability (3.1.2.67), recoverability (3.1.2.66), maintainability (3.1.2.49), maintenance support performance (3.1.2.50), and, in some cases, other characteristics such as durability (3.1.2.22), safety (3.1.2.73) and security (3.1.2.75) can also be involved.

NOTE 2 Dependability is used as a collective term for the time-related quality characteristics of an item.

NOTE 3 Number of accidents or matters and damage cost can also be taken into account for the dependability risk assessment.

[SOURCE: BS ISO/IEC/IEEE 15026-1:2019, **3.1.7**, modified]

3.1.2.20 discoverability

requirement that the data be stored in such a manner that they can be accessed if necessary

[SOURCE: PD ISO/TS 15143-3:2020, **3.1.5**]

3.1.2.21 diversity

software development technique in which two or more functionally identical variants of a program are developed from the same specification by different programmers or programming teams with the intent of providing error detection, increased reliability, additional documentation, or reduced probability that programming or compiler errors will influence the end results

[SOURCE: BS ISO/IEC/IEEE 24765:2017, **3.3808**]

NOTE This property is a sub-characteristic of ethical (3.1.2.29).

3.1.2.22 durability

ability of an entity or any of its components to perform its required functions in its service environment over a specified period of time without unforeseen maintenance or repair

NOTE 1 Preventive or routine maintenance are foreseen measures intended to increase functional service life.

[SOURCE: BS ISO 20887:2020, **3.15**, modified]

NOTE 2 This property is a sub-characteristic of dependability (3.1.2.19).

3.1.2.23 entity availability

property of an entity to be accessible and usable upon demand by an authorized entity

[SOURCE: BS EN ISO/IEC 27000, **3.7**, modified]

NOTE This property is a sub-characteristic of availability (3.1.2.8).

3.1.2.24 entity confidentiality

property that a entity and/or its specifications are not made available or disclosed to unauthorized persons, entities, or processes

NOTE This property is a sub-characteristic of confidentiality (3.1.2.14).

[SOURCE: BS EN ISO/IEC 27000, **3.10**, modified]

3.1.2.25 entity continuity

capability of an entity to continue the delivery of its service (**3.1.3.27**) within predefined time frames, capacity and performance levels during a period of disruption as agreed between parties

NOTE 1 Entity continuity management can be a subset of service and business continuity management. BS ISO 22301 is a management system standard for business continuity management.

*NOTE 2 This property is a sub-characteristic of continuity (**3.1.2.17**).*

[SOURCE: BS ISO/IEC 30105-4:2022, **3.1.2**, modified]

3.1.2.26 entity integrity

property whereby a system is accurate, complete, and have not been altered in an unauthorized manner since they were created, transmitted, or stored

*NOTE This property is a sub-characteristic of integrity (**3.1.2.44**).*

[SOURCE: PD ISO/TS 17573-2:2020, **3.56**, modified]

3.1.2.27 entity security

preservation of confidentiality (**3.1.2.14**), integrity (**3.1.2.44**) and availability (**3.1.2.8**) of an entity

*NOTE 1 In addition, other properties, such as authenticity (**3.1.2.7**), accountability, non-repudiation (**3.1.2.55**), and reliability (**3.1.2.67**) can also be involved.*

*NOTE 2 This property is a sub-characteristic of security (**3.1.2.75**).*

[SOURCE: BS EN ISO/IEC ISO/IEC 27000:2018, **3.28**, modified]

3.1.2.28 environmental safety

expectation that an entity will not lead, under defined conditions, to a state in which the ecological environment such as air, water, or land is endangered

*NOTE This property is a sub-characteristic of safety (**3.1.2.73**).*

[SOURCE: BS ISO/IEC/IEEE 12207:2017, **3.1.48**, modified]

3.1.2.29 ethical

< ethical behaviour > behaviour that is in accordance with accepted principles of right or good conduct in the context of a particular situation and is consistent with international norms of behaviour (**3.1.3.15**)

[SOURCE: BS ISO 26000:2010, **2.7**]

*NOTE In addition, sub-characteristic specialization, such as diversity (**3.1.2.21**), fairness (**3.1.2.30**), non-discrimination (**3.1.2.54**), oversight (**3.1.2.58**), human governance (**3.1.2.38**) and wellbeing (**3.1.2.87**) can also be involved.*

3.1.2.30 fairness

principle that every assessment uses procedures that are equitable and as far as possible free from systematic bias

*NOTE This property is a sub-characteristic of ethical (**3.1.2.29**).*

[SOURCE: BS ISO 10667-1:2020, **3.13**, modified]

3.1.2.31 fault tolerance

ability of an entity to survive a certain number of faults; as a result, the performance of the system can be down-graded

*NOTE This property is a sub-characteristic of reliability (**3.1.2.67**) and resilience (**3.1.2.68**).*

[SOURCE: ISO 11519-1:1994, **3.17**, modified]

3.1.2.32 faultlessness

free from defect or error

[SOURCE: Oxford Dictionary]

NOTE This property is a sub-characteristic of reliability (3.1.2.67).

3.1.2.33 flexibility

degree to which an entity can be used with effectiveness, efficiency, freedom from risk, and satisfaction in contexts beyond those initially specified in the requirements

NOTE 1 Flexibility can be achieved by adapting a product for additional user groups, tasks and cultures.

NOTE 2 Flexibility enables products to take account of circumstances, opportunities and individual preferences that had not been anticipated in advance.

NOTE 3 If a product is not designed for flexibility, it might not be safe to use the product in unintended contexts.

NOTE 4 Flexibility can be measured either as the extent to which a product can be used by additional types of users to achieve additional types of goals with effectiveness, efficiency, freedom from risk, and satisfaction in additional types of contexts of use, or by a capability to be modified to support adaptation for new types of users, tasks and environments, and suitability for individualization as defined in BS EN ISO 9241-110.

NOTE 5 In addition, sub-characteristic specialization, such as adaptability (3.1.2.4), scalability (3.1.2.74), installability (3.1.2.43) and replaceability (3.1.2.67) can also be involved.

[SOURCE: BS ISO/IEC 25010:2011, **4.1.5.2**, modified]

3.1.2.34 functional appropriateness

degree to which the functions facilitate the accomplishment of specified tasks and objectives

EXAMPLE

A user is only presented with the necessary steps to complete a task, excluding any unnecessary steps.

NOTE 1 Functional appropriateness corresponds to suitability for the task.

[SOURCE: BS ISO/IEC/IEEE 24765:2017, **3.1686**]

NOTE 2 This property is a sub characteristic of functional suitability (3.1.2.37).

3.1.2.35 functional completeness

degree to which the set of functions on an entity covers all the specified tasks and stakeholders' objectives

NOTE This property is a sub-characteristic of functional suitability (3.1.2.37).

[SOURCE: BS ISO/IEC 25010:2011, **4.2.1.1**, modified]

3.1.2.36 functional correctness (correctness)

degree to which an entity provides the correct results with the needed degree of precision

NOTE This property is a sub characteristic of functional suitability (3.1.2.37).

[SOURCE: ISO/IEC 25010:2011, **4.2.1.2**, modified]

3.1.2.37 functional suitability

degree to which an entity provides functions that meet stated and implied needs when used under specified conditions

NOTE 1 Functional suitability is only concerned with whether the functions meet stated and implied needs, not the functional specification.

NOTE 2 In addition, sub-characteristic specialization, such as functional completeness (3.1.2.35), functional correctness (3.1.2.36) and functional appropriateness (3.1.2.34) can also be involved.

[SOURCE: BS ISO/IEC 25010:2011, **4.2.1**, note 2 added]

3.1.2.38 human governance

system by which an organization is directed and controlled, taking into account the organization's stakeholders (**3.1.3.30**) as well as human and social factors, at the highest and every level of decision making

NOTE This property is a sub-characteristic of ethical (3.1.2.29).

[SOURCE: BS ISO 30400:2022, **3.5.1**, modified]

3.1.2.39 information availability

property of the information to be accessible and usable upon demand by an authorized person

NOTE This property is a sub-characteristic of availability (3.1.2.8).

[SOURCE BS EN ISO/IEC 27000:2020, **3.7**, modified]

3.1.2.40 information confidentiality

property that information is not made available or disclosed to unauthorized persons, entities, or processes

NOTE This property is a sub characteristic of confidentiality (3.1.2.14).

[SOURCE: ISO/IEC 27000:2020, **3.10**, note added]

3.1.2.41 information integrity

property whereby information is accurate, complete, and have not been altered in an unauthorized manner since they were created, transmitted or stored

[SOURCE: PD ISO/TS 17573-2:2020, **3.56**, modified]

3.1.2.42 information security

preservation of confidentiality (**3.1.2.14**), integrity (**3.1.2.44**) and availability (**3.1.2.8**) of information

NOTE 1 In addition, other properties, such as authenticity (3.1.2.7), accountability, non-repudiation (3.1.2.55), and reliability (3.1.2.67) can also be involved.

NOTE 2 This property is a sub-characteristic of security (3.1.2.75).

[SOURCE: BS EN ISO/IEC 27000:2020, **3.28**]

3.1.2.43 installability

degree of effectiveness and efficiency with which an entity can be successfully installed and/or uninstalled in a specified environment

NOTE 1 If the product or system is to be installed by an end user, installability can affect the resulting functional appropriateness and operability.

NOTE 2 This property is a sub-characteristic of flexibility (3.1.2.33) and replaceability (3.1.2.68).

[SOURCE: BS EN ISO/IEC 25010:2011, **4.2.8.2**, modified]

3.1.2.44 integrity

property of accuracy (**3.1.2.3**) and completeness

NOTE 1 Whereby something is accurate, complete, and have not been altered in an unauthorized manner since they were created, transmitted or stored.

NOTE 2 This property applies as much to a system as it does to information. See entity integrity (3.1.2.26) and information integrity (3.1.2.41).

NOTE 3 This property is a sub-characteristic of security (3.1.2.75).

[SOURCE: BS EN ISO/IEC 27000:2020, **3.36**]

3.1.2.45 interaction capability/usability

extent to which an entity can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

NOTE 1 The “specified” users, goals and context of use refer to the particular combination of users, goals and context of use for which usability is being considered.

NOTE 2 The word “usability” is also used as a qualifier to refer to the design knowledge, competencies, activities and design attributes that contribute to usability, such as usability expertise, usability professional, usability engineering, usability method, usability evaluation and usability heuristic.

NOTE 3 In addition, sub-characteristic specialization, such as appropriateness recognizability (3.1.2.6), learnability (3.1.2.48), operability (3.1.2.56), user error protection (3.1.2.86), user interface aesthetics (3.1.2.87), accessibility (3.1.2.1), user engagement (3.1.2.85), user assistance (3.1.2.84) and self-descriptiveness (3.1.2.76) can also be involved.

[SOURCE: BS EN ISO 9241-11:2018, **3.1.1**, modified]

3.1.2.46 interoperability

ability of two or more entities to exchange information and to mutually use the information that has been exchanged

NOTE This property is a sub-characteristic of compatibility (3.1.2.13).

[SOURCE: BS ISO/IEC 22123-1:2023, **3.6.1**, modified]

3.1.2.47 intervenability

property that ensures that personal information subject (3.1.3.14), PII principals (3.1.3.24), PII controllers (3.1.3.23), PII processors (3.1.3.25) and supervisory authorities (3.1.3.2) can intervene in all privacy-relevant data processing

NOTE 1 The extent to which any of these stakeholders can intervene in data processing may be limited by relevant legislation or regulation.

NOTE 2 This property is a sub-characteristic of privacy (3.1.2.63).

[SOURCE: ISO/IEC TR 27550:2019, **3.6**]

3.1.2.48 learnability

degree to which an entity can be used by specified users to achieve specified goals of learning to use the entity with effectiveness, efficiency, freedom from risk, and satisfaction in a specified context of use

NOTE 1 Can be specified or measured either as the extent to which an entity can be used by specified users to achieve specified goals of learning to use the entity with effectiveness, efficiency, freedom from risk and satisfaction in a specified context of use, or by product properties corresponding to suitability for learning as defined in ISO 9241-110.

NOTE 2 This property is a sub-characteristic of interaction capability/usability (3.1.2.45).

[SOURCE: BS ISO/IEC/IEEE 24765:2017, **3.2201**, modified]

3.1.2.49 maintainability

ability of an entity or sub-entity to be maintained or restored to specified conditions within a given period of time

NOTE In addition, sub-characteristic specializations, such as modularity (3.1.2.53), reusability (3.1.2.71), analysability (3.1.2.5), modifiability (3.1.2.52) and testability (3.1.2.79), can also be involved.

[SOURCE: BS EN ISO 14907-1:2020, **3.19**, PD ISO/TS 17573-2:2020, **3.116**, modified]

3.1.2.50 maintenance support performance

ability of a maintenance organization, under given conditions and maintenance policy, to provide, upon demand, the resources required to maintain the treatment technology

NOTE 1 The given conditions are related to the treatment technology and to the conditions under which the treatment technology is used and maintained.

NOTE 2 When evaluating the treatment technologies, required maintenance support performance can be used as a given condition to evaluate the maintainability.

NOTE 3 The term “treatment technology” refers to the entity of interest.

NOTE 4 This property is a sub-characteristic of dependability (3.1.2.19).

[SOURCE: ISO 20468-1:2018, **3.1.10**, modified]

3.1.2.51 maturity

level of achievement in the implementation process measured on a scale of maturity for trustworthiness

NOTE This property is a sub-characteristic of reliability (3.1.2.66).

[SOURCE: BS EN ISO 14005:2019, **3.5.1**, modified]

3.1.2.52 modifiability

degree to which an entity can be effectively and efficiently modified without introducing defects or degrading existing product quality

NOTE 1 Implementation includes coding, designing, documenting, and verifying changes.

NOTE 2 Modularity (3.1.2.53) and analysability (3.1.2.5) can influence modifiability.

NOTE 3 Modifiability is a combination of changeability (3.1.2.11) and stability (3.1.2.79).

NOTE 4 This property is a sub-characteristic of maintainability (3.1.2.49).

[SOURCE: BS ISO/IEC 25010:2011, **4.2.7.4**, modified]

3.1.2.53 modularity

degree to which an entity is composed of discrete components such that a change to one component has minimal impact on other components

NOTE This property is a sub-characteristic of maintainability (3.1.2.49).

[SOURCE: BS ISO/IEC/IEEE 24765, **3.2507**; BS ISO/IEC 25010:2011, **4.2.7.1**, modified]

3.1.2.54 non-discrimination

<non-discriminatory> not making an unfair or prejudicial distinction between different categories of people or things

EXAMPLE 1

Enlistment is voluntary and non-discriminatory; any sex, any age.

EXAMPLE 2

A non-discriminatory policy was introduced.

NOTE This property is a sub characteristic of ethical (3.1.2.29).

[SOURCE: Oxford dictionary]

3.1.2.55 non-repudiation

degree to which actions or events can be proven to have taken place, so that the events or actions cannot be repudiated later

NOTE This property is a sub characteristic of security (3.1.2.75).

[SOURCE: BS ISO/IEC 25010:2011, **4.2.6.3**, modified]

3.1.2.56 operability

degree to which an entity has attributes that make it easy to operate and control

NOTE 1 Operability corresponds to controllability, (operator) error tolerance and conformity with user expectations as defined in BS EN ISO 9241-110.

NOTE 2 This property is a sub characteristic of interaction capability/usability (3.1.2.45).

[SOURCE: BS ISO/IEC 25010:2011, 4.2.4.3, modified]

3.1.2.57 operational safety

expectation that an entity will not lead, under defined conditions, to a state in which human life, health, property, or the operational environment, including ecology, air, water, flora and fauna, is endangered

NOTE This property is a sub-characteristic of safety (3.1.2.73).

[SOURCE: BS ISO/IEC/IEEE 12207:2017, 3.1.48, modified]

3.1.2.58 oversight

enforcement, monitoring and evaluation of the implementation of trust and trustworthiness mechanisms and management of associated tasks, services and products within an organization or within a community, in order to adapt to changes in internal or external circumstances

NOTE 1 Effective oversight needs general understanding of a situation. Oversight is one of the “principles of governance” covered in depth in BS ISO 37000:2021, 6.4.

[SOURCE: BS ISO/IEC 38507:2022, 3.2.1, modified]

NOTE 2 This property is a sub-characteristic of ethical (3.1.2.29).

3.1.2.59 performance efficiency

<efficiency> performance at specified rating conditions

NOTE In addition, sub-characteristic specialization, such as time behaviour (3.1.2.81), resource utilization (3.1.2.70) and capacity (3.1.2.10), can also be involved.

[SOURCE: BS ISO 16818:2008, 3.68]

3.1.2.60 personal information confidentiality/personal data confidentiality

property that personal information and/or data are not made available or disclosed to unauthorized persons, entities, or processes

NOTE This property is a sub-characteristic of privacy (3.1.2.63) and confidentiality (3.1.2.14).

[SOURCE: BS EN ISO/IEC 27000:2020, 3.10, modified]

3.1.2.61 portability

degree of effectiveness and efficiency with which an entity or a component can be transferred from one hardware, software or other operational or usage environment to another

NOTE Portability can be interpreted as either an inherent capability of the entity to facilitate porting activities, or the quality in use experienced for the goal of porting the product or system.

[SOURCE: BS ISO/IEC 25010:2011, 4.2.8, modified]

3.1.2.62 predictability

property that enables reliable assumptions by stakeholders about information and its processing by an entity

[SOURCE: NISTIR 8062; BS ISO/IEC TR 27550:2019, 3.12, modified]

3.1.2.63 privacy/data privacy/information privacy

rights and obligations of persons and organizations with respect to the collection, use, retention, disclosure and disposal of personal information (3.1.2.60)

NOTE In addition, other properties, such as confidentiality (3.1.2.14), consent traceability (3.1.2.16), unlinkability (3.1.2.83) and intervenability (3.1.2.47) can also be involved.

[SOURCE: PD CEN ISO/TS 14441:2013, 3.26]

3.1.2.64 provenance

degree to which ownership history of an entity or item of information can be reliably demonstrated

NOTE Defining the provenance involves specifying criteria and requirements to demonstrate the origin of an entity or information item in a verifiable way.

3.1.2.65 quality

degree to which a set of inherent characteristics fulfils requirements (3.1.3.26)

NOTE 1 There is a clear distinction between quality of the product [drinking water (BS ISO 24512:2007, 2.11) or treated wastewater (BS ISO 24512:2007, 2.51)] and quality of the service (3.1.3.27).

NOTE 2 There are many quality characteristics that are related to trustworthiness. See Figure 4 in Annex A.

[SOURCE: BS ISO 24512:2007, 3.32]

3.1.2.66 recoverability/reversibility

degree to which, in the event of an interruption or a failure, an entity can recover the data directly affected and re-establish the desired state of the entity

NOTE This property is a sub-characteristic of reliability (3.1.2.67) and dependability (3.1.2.19).

[SOURCE: BS ISO/IEC 25010:2011, 4.2.5.4, modified]

3.1.2.67 reliability

property of an entity and its parts to perform its mission accurately and without failure or significant degradation

NOTE 1 In addition, sub-characteristic specialization, such as faultlessness (3.1.2.32), maturity (3.1.2.51), fault tolerance (3.1.2.31) and recoverability (3.1.2.66) (e.g. recovery, reversibility, fall back plan) can also be involved.

NOTE 2 This property is a sub-characteristic of dependability (3.1.2.19).

[SOURCE: BS ISO/IEC 27036-3:2013, 3.1, modified]

3.1.2.68 replaceability

degree to which an entity can replace another specified entity for the same purpose in the same environment

NOTE 1 Replaceability of a new version of a software product is important to the user when upgrading.

NOTE 2 Replaceability can include attributes of both installability (3.1.2.43) and adaptability (3.1.2.4). The concept has been introduced as a sub characteristic of its own because of its importance.

NOTE 3 Replaceability will reduce lock-in risk: so that other software products can be used in place of the present one, for example by the use of standardized file formats.

NOTE 4 This property is a sub-characteristic of flexibility (3.1.2.33).

[SOURCE: BS ISO/IEC 25010:2011, 4.2.8.3, modified]

3.1.2.69 resilience

ability to anticipate and adapt to, resist, or quickly recover from a potentially disruptive event, whether natural or artificial

NOTE In addition, sub-characteristic specialization, such as robustness (3.1.2.72) and fault tolerance (3.1.2.31) can also be involved.

[SOURCE: BS ISO 15392:2019, 3.21, modified]

3.1.2.70 resource utilization

degree to which the amounts and types of resources used by an entity, when performing its functions, meet requirements

NOTE 1 Human resources are included as part of efficiency.

NOTE 2 This property is a sub-characteristic of performance efficiency (3.1.2.59).

[SOURCE: BS ISO/IEC 25010:2011, 4.2.2.2, modified]

3.1.2.71 reusability

degree to which an asset can be used in more than one entity, or in building other assets

NOTE This property is a sub-characteristic of maintainability (3.1.2.49).

[SOURCE: BS ISO/IEC 25010:2011, 4.2.7.2, modified]

3.1.2.72 robustness/error tolerance

degree to which an entity or component can function correctly in the presence of invalid inputs or stressful environmental conditions

NOTE This property is a sub-characteristic of resilience (3.1.2.69).

3.1.2.73 safety/living entity safety

degree to which an entity does not, under defined conditions, lead to a state in which living entity life, health, property, or the environment is endangered

NOTE 1 In addition, sub-characteristic specialization, such as operational safety (3.1.2.57), environmental safety (3.1.2.28), societal safety (3.1.2.78) and controllability (3.1.2.18) can also be involved.

NOTE 2 This property is a sub-characteristic of dependability (3.1.2.19).

[SOURCE: BS ISO/IEC/IEEE 12207:2017, 3.1.48, modified]

3.1.2.74 scalability

setting of the scope of capabilities of an entity as determined by its functionality

NOTE This property is a sub-characteristic of flexibility (3.1.2.33).

[SOURCE: ISO 17356-1:2005, 2.108, modified]

3.1.2.75 security

preservation of confidentiality (3.1.2.14), integrity (3.1.2.44) and availability (3.1.2.8) of an entity and its information items

NOTE 1 In addition, other properties, such as authenticity (3.1.2.2), accountability, non-repudiation (3.1.2.55), and reliability (3.1.2.67) can also be involved.

NOTE 2 This property applies as much to an entity as it does to information. See entity security (3.1.2.27) and information security (3.1.2.42).

NOTE 3 This property is a sub-characteristic of dependability (3.1.2.19).

[SOURCE: BS EN ISO/IEC ISO/IEC 27000:2018, 3.28, modified]

3.1.2.76 self-descriptiveness

degree to which an entity or component contains enough information to explain its objectives and properties

NOTE 1 See also maintainability (3.1.2.49), testability (3.1.2.80) and usability (3.1.2.45).

NOTE 2 This property is a sub-characteristic of interaction capability/usability (3.1.2.45).

[SOURCE: BS ISO/IEC/IEEE 24765:2017, 3.3673, modified]

3.1.2.77 service continuity

entity's capability to deliver a service (**3.1.3.27**) or support an organization's business service without interruption, or with consistent availability as agreed between parties

NOTE 1 Service continuity management can be a subset of business continuity management. BS EN ISO 22301 is a management system standard for business continuity management.

NOTE 2 This property is a sub-characteristic of continuity (3.1.2.17).

[SOURCE: BS ISO/IEC 20000-10:2018, **3.2.19**, modified]

3.1.2.78 societal safety

degree to which an entity will not lead, under defined conditions, to a state in which a society inhabitants, values, customs, or traditions are endangered

NOTE This property is a sub-characteristic of safety (3.1.2.73).

[SOURCE: BS ISO/IEC/IEEE 12207:2017, **3.1.48**, modified]

3.1.2.79 stability

<stability criteria> deviations from initial properties or behaviour at production state, which are acceptable

NOTE This property is a sub-characteristic of modifiability (3.1.2.52).

[SOURCE: PD ISO/TR 18811:2018, **3.4**, note added]

3.1.2.80 testability

degree to which an entity or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met

NOTE This property is a sub-characteristic of maintainability (3.1.2.49).

[SOURCE: BS ISO/IEC/IEEE 24765:2017, **3.4271** 3, modified]

3.1.2.81 time behaviour

degree to which the response and processing times and throughput rates of an entity, when performing its functions, meet requirements

NOTE This property is a sub characteristic of performance efficiency (3.1.2.59).

[SOURCE: BS ISO/IEC 25010:2011, **4.2.2.1**, modified]

3.1.2.82 understandability

ease with which an entity can be comprehended at both the entity-organizational and detailed-statement levels

NOTE Understandability has to do with the system's coherence at a more general level than readability does.

[SOURCE: BS ISO/IEC/IEEE 24765:2017, **3.4417**, modified]

3.1.2.83 unlinkability

property that allows a personal information subject (**3.1.3.14**) to make multiple uses of resources or services without others being able to link these uses together

NOTE This property is a sub-characteristic of privacy (3.1.2.63).

[SOURCE: ISO/IEC TR 27550:2019, **3.25**, modified]

3.1.2.84 user assistance

process by which the user can be supported in interacting with the entity

NOTE This property is a sub-characteristic of interaction capability/usability (3.1.2.45).