

BS 10754-1:2018



BSI Standards Publication

Information technology — Systems trustworthiness

Part 1: Governance and management specification



Publishing and copyright information

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

The British Standards Institution 2018

Published by BSI Standards Limited 2018

ISBN 978 0 580 96464 0

ICS 03.100.70, 35.030

The following BSI references relate to the work on this document:

Committee reference ICT/-/9

Draft for comment 17/30351843 DC

Amendments/corrigenda issued since publication

Date

Text affected

Contents

	Page
Foreword	ii
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Context	5
<i>Figure 1 — Facets of trustworthiness</i>	6
<i>Figure 2 — Mapping trustworthiness facets to the security triad</i>	6
5 Approach	7
<i>Figure 3 — Use during life cycle</i>	8
<i>Table 1 — Applicability</i>	9
<i>Table 2 — Trustworthiness level matrix</i>	10
<i>Figure 4 — Aspects of trustworthiness</i>	11
<i>Figure 5 — PDCA Cycle</i>	14
6 Implementation	14
<i>Figure 6 — Trustworthiness framework</i>	14
Annex A (Normative) Trustworthiness essentials	28
<i>Table A.1 — Summary of TSFr techniques applicable in baseline approach</i>	28
Annex B (Informative) Mapping BS 10754-1 Techniques to Trustworthiness Activities (TA) in the System Life Cycle	30
<i>Table B.1 — Techniques to Trustworthiness Activities (TA) in the System Life Cycle</i>	30
Annex C (Informative) Non-Functional Requirements	34
Annex D (Informative) IT System Archetypes	35
Bibliography	37

Summary of pages

This document comprises a front cover, and inside front cover, pages i to ii, pages 1 to 38, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 28 February 2018. It was prepared by Technical Committee ICT/-/9, *Trustworthy systems*. A list of organizations represented on this committee can be obtained on request to its secretary.

Information about this document

Reference to the Trustworthiness Levels (TL) and the Trustworthy Software Framework (TSF) are licensed under the terms of the Open Government Licence v3.0 (<https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/> [Last viewed 28 February 2018]).

Relationship with other publications

In addition to Part 1, Governance and management specification, it is expected that BS 10754, *Information technology – Systems trustworthiness*, will eventually comprise the following parts:

- *Part 2: Assurance cases; and*
- *Part 3: Application security controls.*

Presentation conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is “shall”.

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

Requirements in this standard are drafted in accordance with *Rules for the structure and drafting of UK standards*, subclause J.1.1, which states, “Requirements should be expressed using wording such as: ‘When tested as described in [Annex A](#), the product shall ...’”. This means that only those products that are capable of passing the specified test will be deemed to conform to this standard.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

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

1 Scope

This British Standard provides a specification for systems, software and services trustworthiness, that is intended to be a widely applicable approach that can be customized for any organization and software.

The requirements of this British Standard define the overall principles for effective trustworthiness, and include technical, physical, cultural and behavioural measures alongside effective leadership and governance. It identifies the necessary tools, techniques and processes and addresses safety, reliability, availability, resilience and security issues.

This British Standard does not specify the detailed processes or actions that an organization follows in order to achieve these outcomes.

NOTE 1 These processes are defined in other standards, or can be defined by the organization.

This British Standard includes a comprehensive Trustworthiness System Framework (TSFr), which provides a domain- and implementation-agnostic way to reference the large existing body of knowledge, including functional safety, information security, and systems and software engineering and acts as a collation of good practice for software trustworthiness.

When used as a standalone document for organizations with no current approach to software trustworthiness, this specification facilitates the deployment of the TSFr for software in its many guises from embedded equipment through consumer devices to industrial control systems.

Where organizations already address system trustworthiness through one or more of the five facets of trustworthiness in isolation (safety, reliability, availability, resilience and security), this specification provides a companion and complement to other relevant standards. This British Standard provides a benchmark of concepts, principles, expected techniques and management practices to achieve individual facets. This can be used to identify any gaps and enhancements for local implementation.

This British Standard does not specify how any technique should be applied to a specific application.

NOTE 2 This information is available in other standards, such as BS ISO/IEC 15408-1 and [BS EN ISO/IEC 27001](#) for information security, and [BS EN 61508](#) (all parts) for functional safety.

This British Standard is applicable to any organization aiming to adopt system trustworthiness practices.

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. 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 EN ISO/IEC 27001](#), *Information technology — Security techniques — Information security management systems — Requirements*

[BS EN ISO/IEC 27002](#), *Information technology — Security techniques — Code of practice for information security controls*

BS ISO/IEC/IEEE 15288:2015, *Systems and software engineering — System life cycle processes*

BS ISO/IEC/IEEE 42010, *Systems and software engineering — Architecture description*

3 Terms and definitions

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

3.1 adversity

superset of external factors likely to have undesirable effects on software, being the aggregate of the set of hazards and threats

3.2 best endeavours

commercially practicable actions (having regard to costs and degree of difficulty) which are taken, reasonable expenses being incurred if necessary, with the assumption resources might need to be diverted from elsewhere within the business

3.3 backdoor

means to access a system that bypasses security mechanisms

3.4 data

series of digital or analogue signals or encoded characters stored or transmitted electronically, or marks (e.g. writing, printed characters or graphics) on paper or microform, that are intended to convey information

NOTE The essential distinction between data and information is that data do not need to have any meaning attached to them. Data become information via context; the same data file can be considered as containing different information depending on the context: the data in the same file can be considered as containing ASCII characters as far as one computer program is concerned; another can regard the same data as a set of names and addresses; the user can know that these are customer names and addresses.

[SOURCE: BIP 0008-1]

3.5 defect

non-fulfilment of an explicit or implicit requirement, or the omission of a requirement, related to an intended or specified use

NOTE Defects can be technical or application specific.

3.6 deferral

documented and risk managed decision to not resolve a defect or deviation

3.7 deviation

nonconformity with specification

3.8 hazard

condition, event or circumstances which could induce a harmful effect

3.9 implicit requirement

functional or non-functional requirement, not explicitly stated in the trustworthiness policy set, arising from an external source that a reasonable person would expect to be fulfilledEXAMPLE: This can be legal or regulatory.

3.10 information

data interpreted in an application context (see also 3.4)

NOTE For example, a string of characters can be referred to generally as data; but if these characters are understood by a person or a computer program as someone's name, then the characters convey information. Information always involves the presence of data in some format, on some medium, which could be, for example, a physical document, a document image on a screen, or the contents of an electronic file.

[SOURCE: BIP 0008-1]

3.11 non-objective requirement

requirement that arises from user and usability preferences rather than from any functional need

3.12 organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

NOTE The concept of organization includes, but is not limited to, sole trader, company, corporation, firm, enterprise, authority, partnership, institution, charity or association, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: BS EN ISO 9000:2015, 3.2.1, modified]

3.13 reasonable endeavours

commercially practicable actions which are taken, but only to the extent that such action is not to the detriment of commercial interests, without the assumption of a requirement to divert resources from elsewhere within the business

3.14 risk management

coordinated activities to direct and control an organization with regard to risk

[SOURCE: BS EN ISO 22301:2014, 3.51]

3.15 susceptibility

existence of a generic vulnerability in a particular implementation such that it could lead to a defect

NOTE For example, susceptibilities in systems can arise from:

- initial implementation;
- changes to software, such as from adding new facilities or the correction of detected defects ("patching"); and
- use of utility programs, which might be capable of circumventing security measures in the controlling or application software.

3.16 system

combination of interacting elements organized to achieve one or more requirements

[SOURCE: BS ISO/IEC/IEEE 15288:2015, 4.1.46, modified]

3.17 tailoring

developing and applying trustworthiness concepts, principles and techniques to suit each specific environment

3.18 threats

directed, deliberate, hostile acts likely to have a deleterious effect upon an asset

3.19 through-life management

coherent and holistic approach to managing the whole-life costs and outlook across a system

3.20 trustworthiness activity (TA)

collection of processes and procedures used during specific parts of the life cycle

3.21 trustworthiness approach definition (TAD)

document(s) that explains the organizational implementation of trustworthiness concepts, principles and techniques as applicable to specification, realization and/or use of the system(s)

3.22 trustworthiness constraint and dependency model (TCDM)

document that explains all external constraints and dependencies involved in software deployment, configuration and operation

3.23 trustworthiness defect and deviation list (TDDL)

document that encapsulates all defects and deviations that have been identified, their status, and any short-term mitigations required to address deferrals until they can be resolved

3.24 trustworthiness system framework (TSFr)

domain- and implementation-agnostic reference to the existing body of knowledge, including functional safety, information security, systems and software which provides a consensus collation of good practice for software trustworthiness

3.25 trustworthiness policy (TP)

document that defines the organizational mandate for trustworthiness

3.26 trustworthiness release authority (TRA)

competent person or body responsible for ensuring that consideration has been given to all relevant trustworthiness concepts, principles and techniques before release, including the TCDM

3.27 trustworthiness release note (TRN)

document that summarizes for those deploying, configuring and operating the system item the facets of trustworthiness that have been addressed during its specification and realization, the constraints and dependencies that apply, and any unmitigated defects and deviations, along with any short-term mitigations required until they can be removed

3.28 management

person or group of people who directs and controls an organization at the highest level

[SOURCE: BS EN ISO 9000:2015, 3.2.7]

3.29 trustworthy

appropriately addresses safety, reliability, availability, resilience and security issues

3.30 untraceable requirement (UR)

requirement that arises as an artefact of the realization process that is not traceable to the higher level requirements

3.31 validation

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

[SOURCE: BS EN ISO/IEC 27043:2016, 3.16]

3.32 verification

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[SOURCE: BS EN ISO/IEC 27043:2016, 3.17]

3.33 vulnerability

instantiation of a generic weakness in a particular platform that could be exposed

NOTE 1 The exposure can arise either from malicious exploitation, errors or other collateral circumstances.

NOTE 2 Vulnerabilities can be:

- *the existence of a generic weakness in a particular platform, such as a buffer overflow weakness occurring in a specific operating system or application;*
- *interactions between multiple software elements that bypass intended controls;*
- *accidental actions of software developers that result in defects; and*
- *deliberate actions of software developers that bypass intended controls, such as trap doors that permit unauthorized access to the system.*

3.34 weakness

generic classes of defects in systems architecture, design or implementation that, if left unaddressed, could result in vulnerabilities

4 Context

4.1 Goals

The requirements of this British Standard shall be used as the basis for an organization to refine its needs for trustworthiness, to ensure that:

- a) controls are improved;
- b) operational effectiveness and efficiency are improved;
- c) organizational learning are improved;
- d) defects are reduced;
- e) traceability with regard to undesirable effects is improved;
- f) backdoors are eliminated;
- g) overall system quality is improved; and
- h) impacts on other bodies are reduced.

NOTE These in turn can result in:

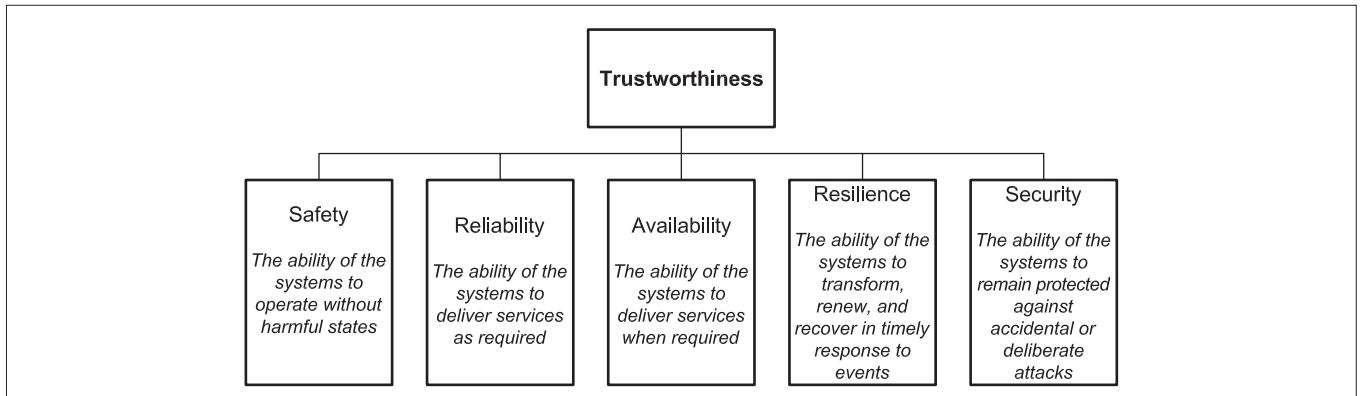
- *improved stakeholder confidence and trust;*
- *increased likelihood of achieving objectives;*
- *reduced risk; and*

- enhanced business reputation.

4.2 Relevance

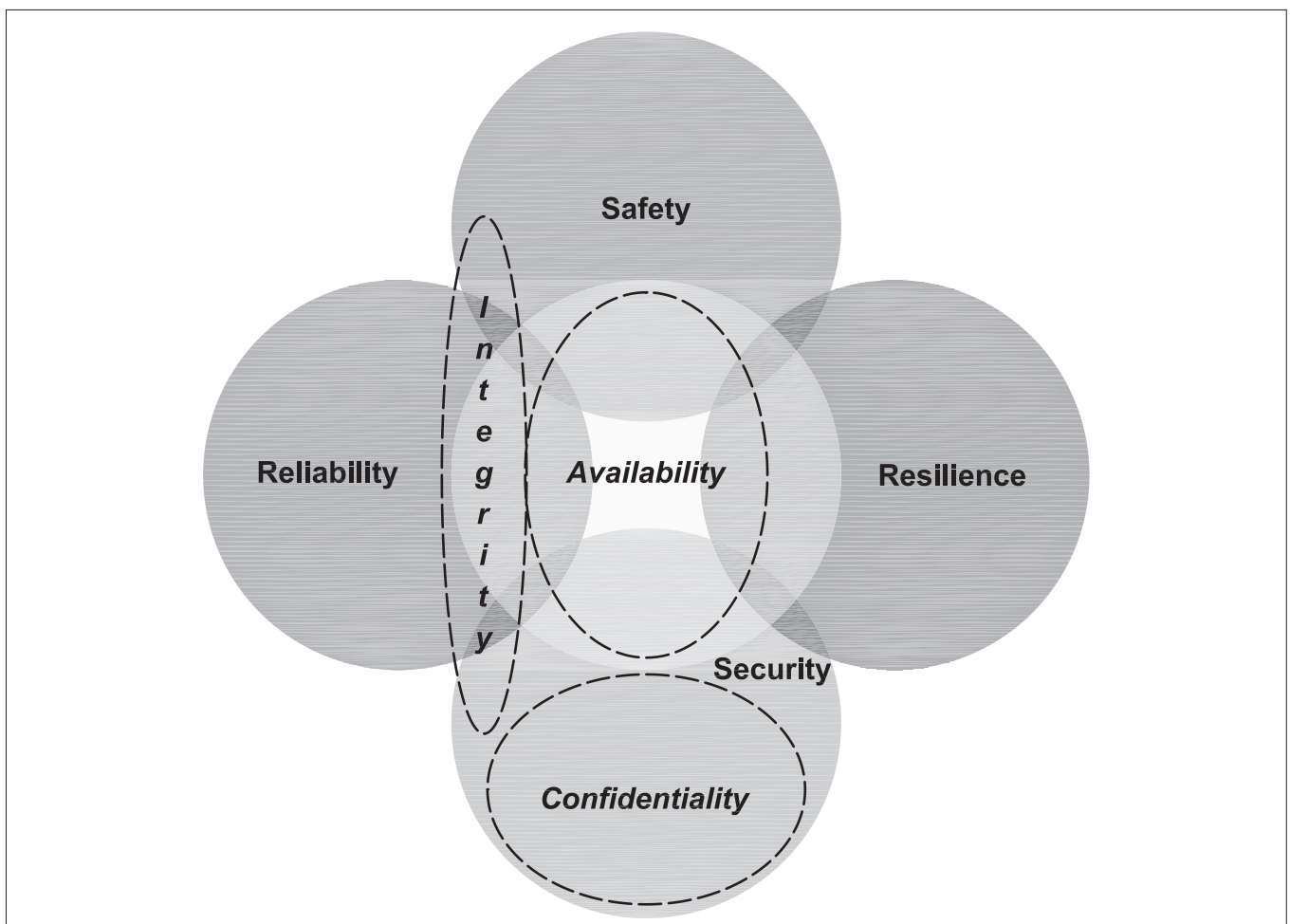
For this specification, trustworthiness is used to define the five facets, as described in [Figure 1](#), which shall be considered for applicability to all systems.

Figure 1 — Facets of trustworthiness



NOTE 1 [Figure 2](#) provides a mapping between these five facets and the security triad of confidentiality, integrity and availability.

Figure 2 — Mapping trustworthiness facets to the security triad



Once the aspects which apply have been considered, a set of principles and techniques to suit the context and intended use shall be derived.

NOTE 2 For each of these facets of trustworthiness (see [5.3](#)) there are objectives, of varying complexity, including:

- *sectoral practice;*
- *regulation; and*
- *legislation.*

4.3 Organizational controls

In order to deliver trustworthiness, an organization shall require a set of underpinning controls to provide assurance that:

- a) personnel are suitably qualified and experienced;
- b) adequate resources are allocated;
- c) all necessary communication takes place;
- d) activity proceeds in a series of organized steps;
- e) any required independences between specific steps are maintained;
- f) activity proceeds in a timely manner; and
- g) all verification processes are completed within the specified criteria.

The technical infrastructure shall provide assurance that:

- 1) all information, designs, algorithms and other such artefacts are retained for future use and analysis;
- 2) the design and coding artefacts are adequately documented;
- 3) all past and present versions of the system and components and facilities required to build it are available at any time and that future versions are similarly available;
- 4) all appropriate test data sets can be applied to the corresponding version and any future versions of the software; and
- 5) regression testing can be applied in order to ensure that the software changes only in the required manner.

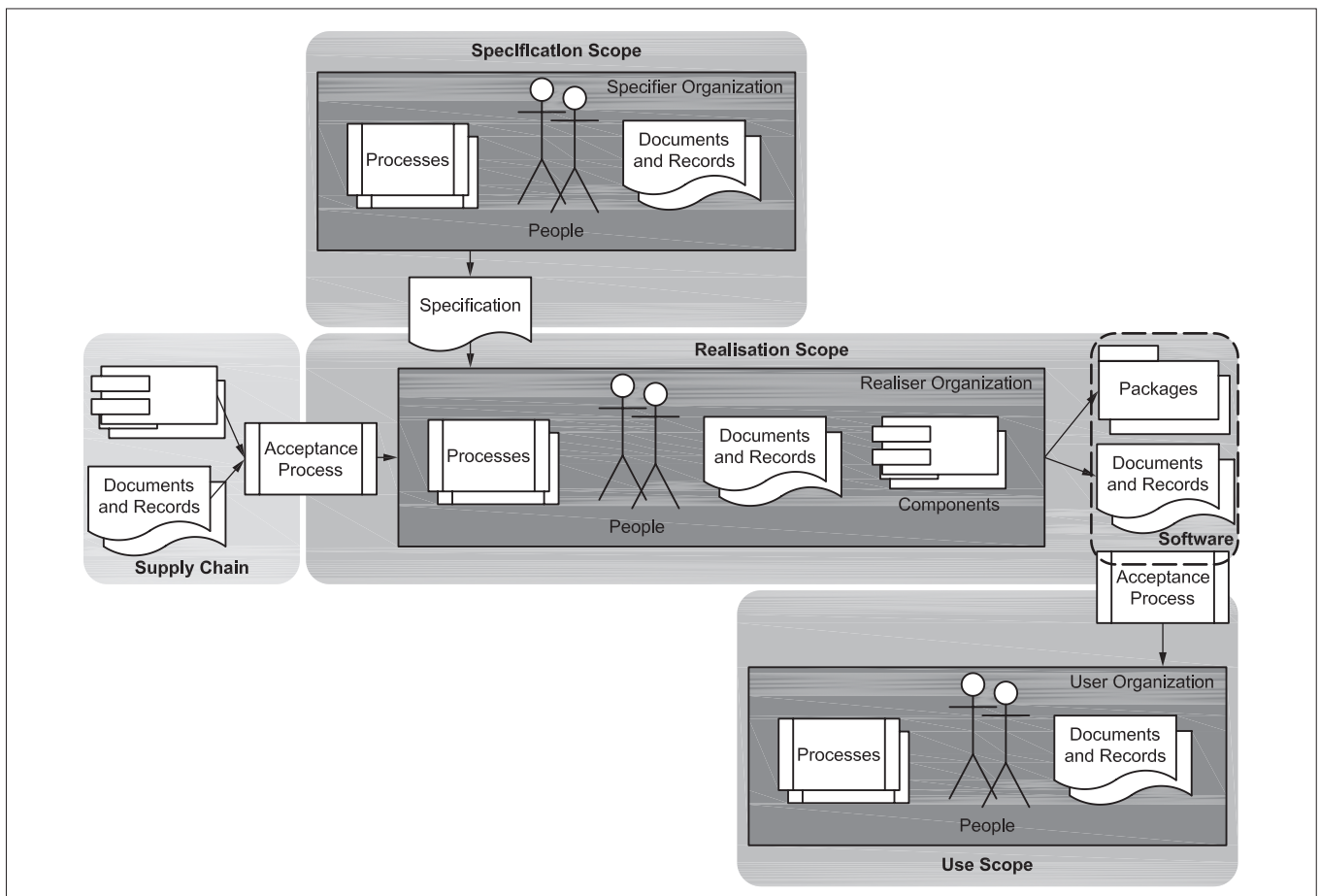
5 Approach

5.1 Applicability

The Trustworthy Systems Framework (TSFr) is designed to cover all aspects of the systems and software life cycle, in accordance with BS ISO/IEC/IEEE 15288, but shall only be applied to the phases of the life cycle as relevant to the organization specifying, delivering or using the systems, software or services, which for the purposes of this British Standard are grouped into three areas and illustrated in [Figure 3](#):

- Specification – collating the requirements for the explicit and implicit characteristics of software to be acquired;
- Realization – producing the system (a multi-phase activity including design; implementation; integration; test); and
- Use – deploying, configuring, operating and/or using the system.

NOTE These groupings can be used iteratively where the system(s) is replaced or augmented.

Figure 3 — Use during life cycle

In addition to consideration of the phase(s) of the life cycle relevant to the organization, a generic “prepare” phase shall apply to all organizations, which covers the background activity required before commencing consideration of the trustworthiness of one or more systems.

5.2 Categorization

Organizations shall review their incentives and requirements for trustworthiness, based on the following categories:

- mass market with implicit need (M/I) for software trustworthiness;
- mass market with explicit need (M/E) for software trustworthiness;
- niche markets with explicit need (N/E) for software trustworthiness.

NOTE 1 The way in which these map to TL and approaches are shown in [Table 1](#), predicated on the English common law contractual obligations expectation of performance, referred to as reasonable endeavours and best endeavours.

Reasonable endeavours in respect of systems trustworthiness are to follow a baseline (prescriptive) approach, referred to as trustworthiness essentials and represents a minimum subset of the TSFr that shall be applied to all usages, as itemized at [Annex A](#).

NOTE 2 The application of trustworthiness essentials is regarded as reasonable endeavours.

Where the baseline approach is used, the presumption is that all controls are used; in exceptional circumstances any control not able to be implemented shall be explicitly justified as a deviation that is fully documented and available to support the assurance argument (see [5.10](#)).

Table 1 — Applicability

Applicability		Risk Segment	Approach
(No requirement)		TL0	NA
Mass market/ implicit need (M/I)		TL1 – Fundamental practice	Reasonable endeavours
	Mass market/explicit need (M/E)	TL2 – Structured practices	
	Niche market/explicit need (N/E)	TL3 – Enhanced practices	Best endeavours
		TL4 – Specialist practices	

Best endeavours in respect of systems trustworthiness is to follow a comprehensive (descriptive) approach based upon consideration of the full set of controls from the TSFr for applicability to the implementation in question, and shall be the approach used where best endeavours are required. Where the comprehensive approach is used, any control not considered appropriate shall be explicitly justified as a deviation that is that is fully documented and available to support the assurance argument (see [5.10](#)).

5.3 Facets of trustworthiness

The TSFr is designed on the basis that the same principles can be invoked as building blocks for trustworthiness across the five facets of trustworthiness, and each item of software shall therefore be reviewed for both explicit and implicit requirements for delivery of these abilities:

- Safety – the ability of the system to operate without harmful states;
- Reliability – the ability of the system to deliver services as specified;
- Availability – the ability of the system to deliver services when requested;
- Resilience – the ability of the system to transform, renew and recover in timely response to events; and
- Security – the ability of the system to remain protected against accidental or deliberate attacks.

NOTE Explicit requirements only exist in the N/E and M/E use cases, which typically should also be supplemented by implicit, Non-Functional Requirements (NFR) for trustworthiness. For the M/I use case, all trustworthiness requirements are inherently Non-Functional (NFR).

5.4 Trustworthiness level (TL) assessment

For each item of software, having established which facet(s) of trustworthiness are required either explicitly or implicitly, a TL shall be established, based on an assessment of the role software plays in the overall system or service to be delivered, and the maximum impact that a defect or deviation in such software would have on the system or service.

The “Software Role” segmentation shall be based upon the degree to which the source of trustworthiness in a component, composed subsystem or system is dependent on software:

- paramount role: where a failure of software to be trustworthy is a critical risk;
- explicit role: where a failure of software to be trustworthy is a significant risk;

- implicit role: where a failure of software to be trustworthy is an emergent risk; and
- ancillary role: where a failure of software to be trustworthy is a minor risk.

Potential impacts shall be assessed, for which a simple four level scale shall be used, based upon the organizational context:

- none;
- routine;
- significant; and
- critical.

These assessments shall be used as shown at [Table 2](#).

Table 2 — *Trustworthiness level matrix*

Role	Impact			
	None	Routine	Significant	Critical
Paramount	N/A	TL3	TL4	TL4
Explicit	N/A	TL3	TL3	TL4
Implicit	N/A	TL2	TL3	TL3
Ancillary	TL0	TL1	TL2	TL3

The organization shall document the assessed TL, which shall be the basis for prioritizing efforts in software trustworthiness. This assessment shall be periodically reviewed throughout the software's life cycle.

NOTE 1 An informative set of interpretations of the TL against [BS ISO/IEC 15504](#) (SPICE) concepts would be:

- *TL0* Software trustworthiness not required;
- *TL1* Software trustworthiness delivered in a due diligence manner;
- *TL2* Software trustworthiness delivered by managed processes;
- *TL3* Software trustworthiness delivered by established processes; and
- *TL4* Software trustworthiness delivered by predictable or optimizing processes.

All assessments and treatments shall be applied in a pragmatic, appropriate and cost-effective (PACE) manner, using trustworthiness concepts, principles and techniques to suit each specific environment.

NOTE 2 For lower assessed TL requirements, rather than choosing and refining techniques from the descriptive set presented in the comprehensive TSF, the organization has the option of using a prescriptive baseline TSF subset which should provide Pareto coverage of the most commonly encountered risks.

5.5 Objectives

5.5.1 To achieve the “safety” objectives the implementation shall provide assurance that:

- a) the stated requirements for the software under consideration are accurate and appropriate;
- b) the safety issues are considered via safety requirements;
- c) the architecture and design are consistent with and reflect the stated requirements;
- d) the technical defects are minimized as much as practically possible;
- e) the stated requirements are identifiable in the low-level code and that all low-level code implements at least one stated requirement; and
- f) the test data sets reflect the stated requirements and provide adequate coverage.