BS 10754-1:2018

BSI Standards Publication

Information technology – Systems trustworthiness

Part 1: Governance and management specification

bsi.

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

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*.

Presentational 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*

