DRAFT INTERNATIONAL STANDARD ISO/IEC 30754

Attributed to ISO/IEC JTC 1 by the Central Secretariat

Voting begins on
2016-04-06

Voting terminates on
2016-07-06

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

FAST-TRACK PROCEDURE

Information technology — Software trustworthiness — Governance and management — Specification

Titre manque

ICS 35.080

This draft International Standard is submitted for JTC 1 national body vote under the "fast-track" procedure.

In accordance with Resolution 30 of the JTC 1 Berlin Plenary 1993, the proposer of this document recommends assignment of JTC1 to JTC 1.

The procedures used to develop this document are described in the ISO/IEC Directives, Part 1 - Consolidated JTC 1 Supplement.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© International Organization for Standardization, 2016
International Electrotechnical Commission, 2016



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016
All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

NOTE FROM ITTF

This draft International Standard is submitted for JTC 1 national body vote under the “fast-track” Procedure.

In accordance with Resolution 30 of the JTC 1 Berlin Plenary 1993, the proposer of this document recommends assignment of ISO/IEC 30754 to JTC 1.

“FAST-TRACK” PROCEDURE

1 Any P-member and any Category A liaison organization of ISO/IEC JTC 1 may propose that an existing standard from any source be submitted directly for vote as an enquiry draft (DIS). The criteria for proposing an existing standard for the fast-track procedure are a matter for each proposer to decide.

2 The proposal shall be received by the ITTF, which will take the following actions.

2.1 Settle the copyright and/or trademark situation with the organization having originated the proposed document, so that it can be freely copied and distributed to national bodies without restriction.

2.2 Assess in consultation with the JTC 1 secretariat which subcommittee (SC) is competent for the subject covered by the proposed document and ascertain that there is no evident contradiction with other International Standards.

2.3 Distribute the proposed document as an enquiry draft (DIS).

3 The period for combined enquiry voting (DIS) and the conditions for approval shall be as specified in Annex F.2.3 of the JTC 1 Supplement

4 At the end of the voting period, the comments received, whether editorial only or technical, will be dealt with by a working group (WG) appointed by the secretariat of the relevant SC.

5 If, after the deliberations of this WG, the conditions of approval are met, the draft standard shall progress to the approval stage (FDIS). If not, the proposal has failed and any further action shall be decided upon by the subcommittee to which the document was attributed.

In either case the WG shall prepare a full report which will be circulated by the ITTF.

6 If the proposed standard is accepted and published, its maintenance will be handled by JTC 1.

© ISO/IEC 2016 — All rights reserved

Contents

Contents ... **iii**

Foreword ... **v**

0 Introduction to Software Trustworthiness ... **vii**

0.1 Aims ... vii
0.2 Objectives ... vii
0.3 Claims of Conformance ... vii

0.3.1 General ... *vii*
0.3.2 Form of Claims ... *vii*
0.3.3 Basis of Claim ... *vii*

0.4 Context ... viii

0.4.1 Approach ... *viii*
0.4.2 Organizational Controls ... *ix*
0.4.3 Challenges ... *x*
0.4.4 Tailoring ... *xi*
0.4.5 Categorization ... *xii*
0.4.6 Continuous Improvement ... *xiii*

1 Scope ... **1**

2 Normative References ... **1**

3 Terms and Definitions ... **1**

3.1 adversity ... 1
3.2 cyber security ... 2
3.3 defect ... 2
3.4 deferral ... 2
3.5 deviation ... 2
3.6 organization ... 2
3.7 risk management ... 2
3.8 susceptibility ... 2
3.9 system ... 2
3.10 tailoring ... 3
3.11 through-life management ... 3
3.12 trustworthy software constraint and dependency model (TSCDM) ... 3
3.13 trustworthy software defect and deviation list (TSDDL) ... 3
3.14 trustworthy software framework (TSF) ... 3
3.15 trustworthy software management system (TSMS) ... 3
3.16 trustworthy software release authority (TSRA) ... 3
3.17 trustworthy software release note (TSRN) ... 3
3.18 top management ... 3
3.19 trustworthy ... 3
3.20 vulnerability ... 4
3.21 weakness ... 4

4 Abbreviated Terms ... **4**

© ISO/IEC 2016 – All rights reserved

5 Approach 4

5.1 Applicability 4
5.2 Categorization 5
5.3 Facets of Trustworthiness 5
5.4 Trustworthiness Level Assessment 6
5.5 Deployment 7
5.6 Fundamental Control Measures 8
5.7 Realization Control Measures 8

6 Concepts 8

6.1 Governance 8
6.2 Risk 9
6.3 Controls 9
6.4 Compliance 9

7 Principles 9

7.1 Applicability 9
7.2 Governance (GV) 10
7.3 Risk (RI) 10
7.4 Control (CO) 11
7.5 Compliance (CM) 15

Annex A (informative) ISO/IEC 30754 in the System Lifecycle 1

Annex B (informative) Delivery of ISO/IEC 30754 requirements: techniques 2

Annex C (informative) Bibliography 13

 © ISO/IEC 2016 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC DIS 30754 was prepared by British Standards Institution (BSI) for Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

Relationships with other publications

This Standard is intended to be used as a stand alone specification, or it can be used as a companion and complement to other relevant standards, by any organization that is looking for trustworthiness and confidence in its software.

This Standard contains requirements that define the principles required to achieve software trustworthiness but does not specify how to implement those principles. Annex A includes an example of the principles that can deliver the requirements of this Standard mapped again the lifecycle.

Use of this document

It has been assumed in the preparation of this Standard that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

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”.

© ISO/IEC 2016 – All rights reserved

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

The word “should” is used to express recommendations, the word “may” is used to express permissibility and the word “can” is used to express possibility, e.g. a consequence of an action or event.

Spelling conforms to The Shorter Oxford English Dictionary.

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 this Standard cannot confer immunity from legal obligations.

 © ISO/IEC 2016 – All rights reserved

0 Introduction to Software Trustworthiness

0.1 Aims

The aim of ISO/IEC 30754 is to provide a specification for software trustworthiness.

0.2 Objectives

This specification is intended to be widely applicable to software in its many guises from embedded equipment through consumer devices to industrial control systems. It aims to provide a consensus specification for software trustworthiness, either as a stand-alone document, or as a companion and complement to other relevant standards, by collating good practice from the five main facets of trustworthiness that currently typically operate in isolation (safety, reliability, availability, resilience and security).

By helping to improve software trustworthiness within organizations, this specification could result in significant savings for the economy and reduce the risk major disruptions to a range sectors.

NOTE See *Risk and Responsibility in a Hyperconnected World,* WEF[1]

The requirements of ISO/IEC xx754 can enable an organization to, for example:

- improve controls;
- improve operational effectiveness and efficiency;
- improve organizational learning.

These in turn can result in:

- improved stakeholder confidence and trust;
- increased likelihood of achieving objectives;
- reduced risk;
- enhanced business reputation.

0.3 Claims of Conformance

0.3.1 General

An organization may claim conformance with ISO/IEC 30754.

0.3.2 Form of Claims

All claims are required to include a reference to ISO/IEC 30754.

0.3.3 Basis of Claim

A claim of conformance can be made on the basis of:

a) a first-party conformity assessment performed by the organization (self assessment);

© ISO/IEC 2016 – All rights reserved

b) a second-party conformity assessment performed by, for example, a trade association; or
c) a third-party conformity assessment performed by an organization, such as a certification body, that is independent of both the organization and any linked trade association.

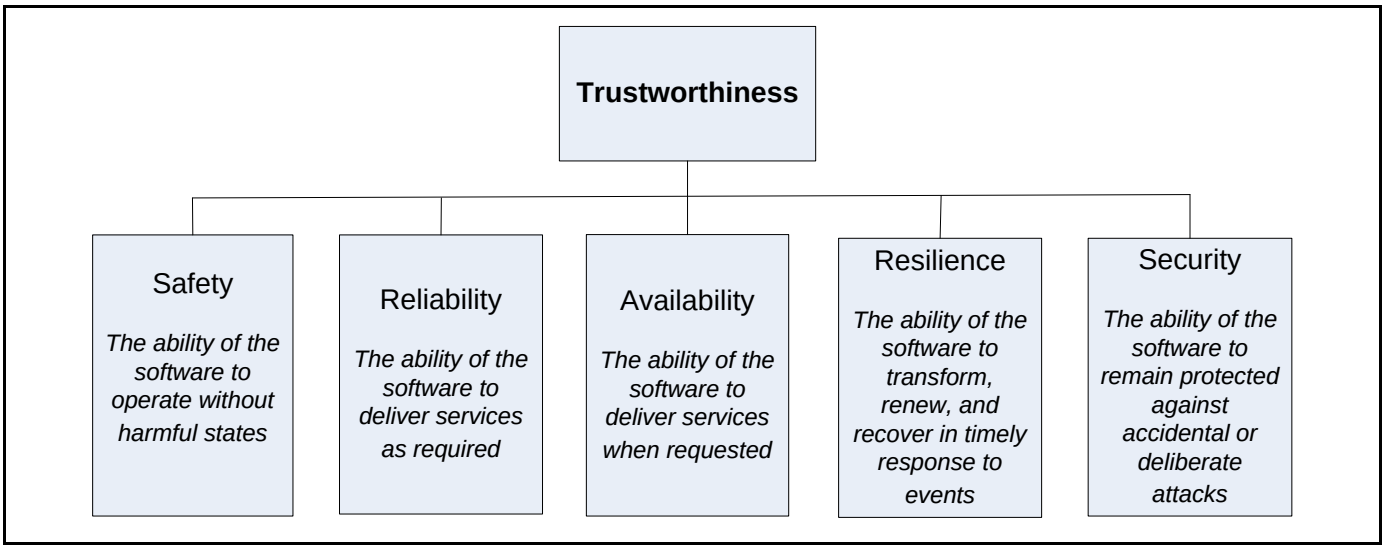
0.4 Context

0.4.1 Approach

ISO/IEC 30754 is intended for any organization that seeks to establish or improve confidence in its software trustworthiness. It is applicable to all organizations regardless of their size, type and the nature of their business.

For this specification, software trustworthiness is identified as consisting of five Facets, as described in Figure 1.

Figure 1 – Facets of trustworthiness



It is important that organizations review every software implementation to see which aspects apply and derive a set of principles and techniques to suit the context and intended use.

For each of these Facets of Trustworthiness there will be objectives, of varying complexity.

A common set of implied objectives apply to most software implementations, not least because of legal and regulatory requirements.

'Safety' aims to provide assurance that:

- the stated requirements are accurate and appropriate;
- safety issues are considered via safety requirements;
- the architecture and design are consistent with and reflect the stated requirements;
- technical defects are absent;
- application defects are absent;

 © ISO/IEC 2016 – All rights reserved

- the stated requirements are identifiable in the low-level code and that all low-level code implements at least one stated requirement;
- the test data sets reflect the stated requirements;
- the test data sets cover the low-level code to a specified degree.

'Reliability' aims to provide assurance that:

- all the patterns of use are reflected in the stated requirements;
- there are no technical defects;
- the test data sets reflect patterns of use;
- there are no application defects.

'Availability' aims to provide assurance that:

- the stated requirements are accurate and appropriate;
- the architecture and design are consistent with and reflect the stated requirements;
- technical defects are absent;
- application defects are absent;
- the test data sets reflect the stated requirements.

'Resilience' aims to provide assurance that:

- the stated requirements are accurate and appropriate;
- the architecture and design are consistent with and reflect the stated requirements;
- technical defects are absent;
- application defects are absent;
- the test data sets reflect the stated requirements.

'Security' aims to provide assurance that:

- the security requirements consider all security issues;
- the architecture and design satisfy the security requirements;
- there are no security defects in the code;
- the test data reflects the security requirements.

0.4.2 Organizational Controls

In order to deliver trustworthy software, an organization requires a set of underpinning controls that apply to all activities.

The software management system aims to provide assurance that:

- all personnel are appropriately qualified;

© ISO/IEC 2016 – All rights reserved

- adequate resources are allocated;
- all necessary communication takes place;
- activity proceeds in a series of measured steps;
- specific steps are performed independently;
- activity proceeds in a timely manner;
- all verification processes are completed within the specified criteria.

The software technical infrastructure aims to provide assurance that:

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

0.4.3 Challenges

Software problems are generally characterised as a one of three types:

- **Weaknesses**, which are generic classes of potential deficiency in software, such as buffer overflows.
- **Vulnerabilities**, which can be:
  - the existence of a generic weakness in a particular platform, such as a buffer overflow 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 errors;
  - deliberate actions of software developers that bypass intended controls, such as trap doors that permit unauthorised access to the system.
- **Susceptibilities**, which are the confirmed presence of one or more vulnerability within an implemented system, such as the presence of an operating system with a buffer overflow defect.

Susceptibilities in systems stem from:

- initial implementation;
- changes to software, such as from adding new facilities or the correction of detected errors ('patching');

 © ISO/IEC 2016 – All rights reserved

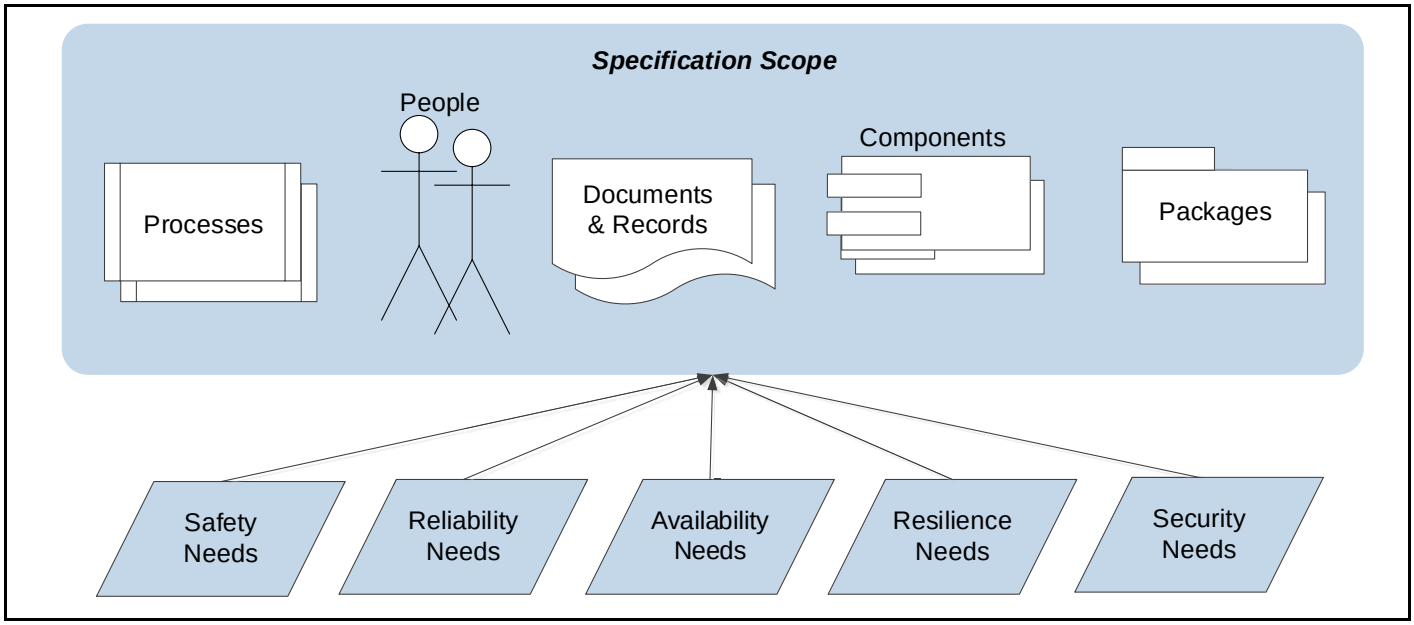
- use of utility programs, which may be capable of circumventing security measures in the controlling or application software.

For the application of these terms specifically to software, see Clause 3.

0.4.4 Tailoring

ISO/IEC 30754 is scoped to include all aspects that contribute to trustworthiness of software, as illustrated in Figure 2.

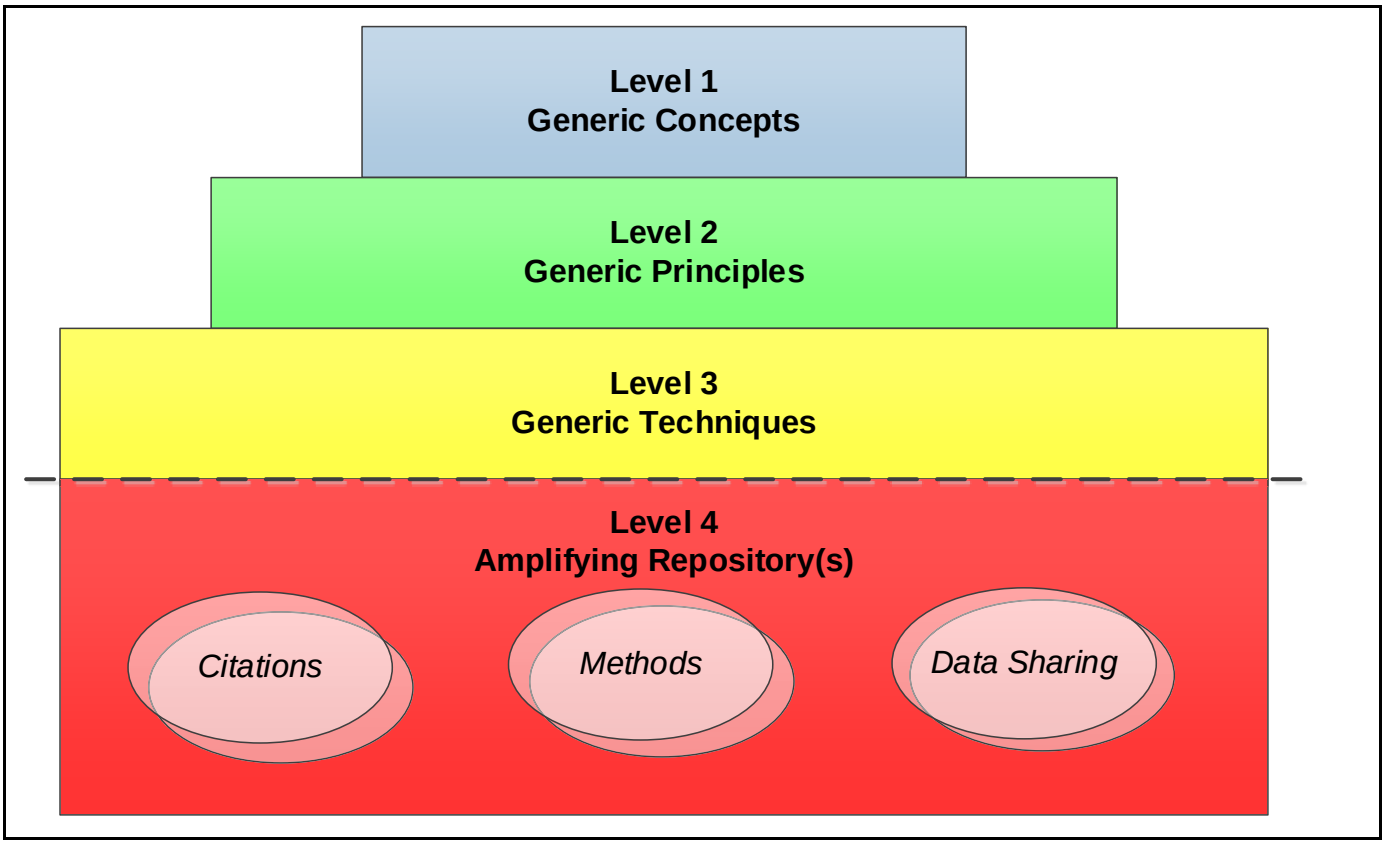
Figure 2 – Aspects of trustworthiness



This is achieved by using the appropriate elements of the framework of decomposed as shown in Figure 3 and detailed in Clauses **5** and **6** and the Annexes.

Figure 3 – Trustworthy Software Framework

© ISO/IEC 2016 – All rights reserved



This comprehensive Trustworthy Software Framework (TSF) 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 therefore acts as a collation of good practice for software trustworthiness.

When used as a stand-alone document for organizations with no current approach to software trustworthiness, this specification will facilitate the deployment of the TSF for software in its many guises from embedded equipment through consumer devices to industrial control systems.

For organizations that already address software trustworthiness though the lens of one or more of the five main facets of trustworthiness that typically operate in isolation (safety, reliability, availability, resilience and security), this specification provides a companion and complement to other relevant standards, and reviewing the concepts, principles and techniques in this specification alongside practices and Management Systems derived from individual facets allows the identification of gaps and enhancements.

This document does not specify how any technique should be applied to a specific domain of application. This information is available in other standards, such as ISO/IEC 15408 and ISO/IEC 27001 for information security, and IEC61508 for functional safety.

0.4.5 Categorization

For the purposes of this standard, the software audience can be divided into three groups:

 © ISO/IEC 2016 – All rights reserved

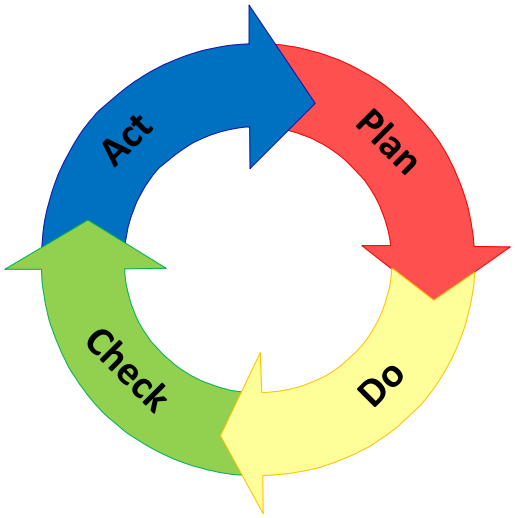
- Mass Market with an Implicit Need [1] (M/I) for software trustworthiness;
- Mass Market with an Explicit Need [2] (M/E) for software trustworthiness;
- Niche Market with an Explicit Need [3] (N/E) for software trustworthiness.

0.4.6 Continual Improvement

Any organization attempting trustworthy software practices should aim for continual improvement of its application of concepts, principles and techniques.

Its Trustworthy Software Management System (TSMS) should include recognition of the need for continual improvement using the PDCA (plan–do–check–act) cycle (see Figure 4) unless another approach is documented.

Figure 4 – PDCA Cycle



[1] For the Mass Market with Implicit Needs, a majority of software trustworthiness Requirements are perceived as Non-Functional e.g. a "Non Interference" property

[2] One or more Functional Requirements are for software trustworthiness

[3] For instance Government and Critical National Infrastructure (CNI)

© ISO/IEC 2016 – All rights reserved

Information technology – Software Trustworthiness – Governance and management – Specification

1 Scope

This International Standard provides a specification for software trustworthiness, that is intended to be a widely applicable approach that can be customised for any organization, and to software in its many guises from embedded equipment through consumer devices to industrial control systems.

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

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

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

NOTE 2 For organizations that already address software trustworthiness through the lens of one or more of the five main facets of trustworthiness that typically operate in isolation (safety, reliability, availability, resilience and security), this specification provides a companion and complement to other relevant standards, and reviewing the concepts, principles and techniques in this specification alongside practices and Management Systems derived from individual facets allows the identification of gaps and enhancements.

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

2 Normative References

The following documents, in whole or part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including and amendments) applies.

ISO/IEC 15288:2008 Systems and software engineering -- System life cycle processes

ISO/IEC 27001:2013, Information technology – Security techniques, Information security management systems – Requirements

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

3 Terms and Definitions

For the purposes of this document, 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 (undirected events) and threats (directed, deliberate, hostile acts).

3.2 cyber security

collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and users' assets.

NOTE Organization and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users' assets against relevant security risks in the cyber environment. The general security objectives include:

- *availability;*
- *integrity, which may include authenticity and non-repudiation;*
- *confidentiality.*

[ITU-T Recommendation X.1205]

3.3 defect

non-fulfilment of an explicit or implicit requirement related to an intended or specified use

3.4 deferral

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

3.5 deviation

non-conformity with specification

3.6 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.

[ISO 9000:2005, **3.3.1**]

3.7 risk management

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

[ISO 22301:2012, **3.51**]

3.8 susceptibility

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

3.9 system

combination of interacting elements organized to achieve one or more stated purposes

[ISO/IEC 15288]

 © ISO/IEC 2016 – All rights reserved

3.10 tailoring

developing and applying trustworthy software concepts, principles and techniques to suit each specific environment.

3.11 through-life management

coherent and holistic approach to managing the whole-life costs and outlook across equipment, a project or programme's life cycle.

3.12 trustworthy software constraint and dependency model (TSCDM)

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

3.13 trustworthy software defect and deviation list (TSDDL)

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

3.14 trustworthy software framework (TSF)

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

3.15 trustworthy software management system (TSMS)

document that explains the organization's approach to the implementation of trustworthy software concepts, principles and techniques as applicable to its participation in the specification, realisation and/or use of software

3.16 trustworthy software release authority (TSRA)

competent person responsible for ensuring that consideration has been given to all relevant trustworthy software concepts, principles and techniques before release, including the TSCDM

3.17 trustworthy software release note (TSRN)

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

3.18 top management

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

[ISO 9000:2005, **3.2.7**]

3.19 trustworthy

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

© ISO/IEC 2016 – All rights reserved

3.20 vulnerability

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

3.21 weakness

generic classes of potential deficiency in software.

4 Abbreviated Terms

PACE	Pragmatic, Appropriate and Cost Effective
TL	Trustworthiness Level
TPM	Trusted Platform Module
TRL	Technology Readiness Level

5 Approach

5.1 Applicability

The Trustworthy Software Framework (TSF) is designed to cover all aspects of the system and software lifecycle, as defined by ISO/IEC 15288, but shall only be applied to the element(s) of the lifecycle as relevant to the organization, which for the purposes of ISO/IEC 30754 are grouped as illustrated in Figure 5:

- Specification – Collating the requirements for the explicit and implicit characteristics of software to be acquired;
- Realisation – Producing the software (a multi-phase activity including design; implementation; integration; test);
- Use – Deploying, configuring, operating and/or using the software.

NOTE These groupings may be used iteratively where software is replaced or augmented

Figure 5 – Use During Lifecycle

 © ISO/IEC 2016 – All rights reserved