BS ISO/IEC 15026-4:2012

BSI Standards Publication

Systems and software engineering — Systems and software assurance

Part 4: Assurance in the life cycle

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO/IEC 15026-4:2012.

The UK participation in its preparation was entrusted to Technical Committee IST/15, Software and systems engineering.

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

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

Published by BSI Standards Limited 2012.

ISBN 978 0 580 75874 4

ICS 35.080

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2012.

Amendments issued since publication

Date	Text affected

BS ISO/IEC 15026-4:2012

INTERNATIONAL STANDARD

ISO/IEC 15026-4

First edition
2012-10-01

Systems and software engineering — Systems and software assurance —

Part 4: Assurance in the life cycle

Ingénierie du logiciel et des systèmes — Assurance du logiciel et des systèmes —

Partie 4: Assurance du cycle de vie

Reference number
ISO/IEC 15026-4:2012(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

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 shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15026-4 was prepared by Joint Technical Committee ISO/TC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

ISO/IEC 15026 consists of the following parts, under the general title *Systems and software engineering — Systems and software assurance*:

— *Part 1: Concepts and vocabulary* [Technical Report]

— *Part 2: Assurance case*

— *Part 3: System integrity levels*

— *Part 4: Assurance in the life cycle*

Introduction

In its entirety, ISO/IEC 15026 consists of multiple parts:

a) ISO/IEC TR 15026-1, *System and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

NOTE ISO/IEC TR 15026-1 is intended to be replaced by an International Standard.

b) ISO/IEC 15026-2, *System and software engineering — Systems and software assurance — Part 2: Assurance case*

c) ISO/IEC 15026-3, *System and software engineering — Systems and software assurance — Part 3: System integrity levels*

d) ISO/IEC 15026-4, *System and software engineering — Systems and software assurance — Part 4: Assurance in the life cycle*

Many specialized standards and guidelines address specific application areas and topics related to assurance and use different concepts and terminology when addressing common themes. ISO/IEC TR 15026-1 provides terminology and concepts used in all parts of ISO/IEC 15026.

ISO/IEC 15026-2 provides minimum requirements for the structure and contents of assurance cases that treat claims regarding properties of a system or software product selected for special treatment. The results of performing the life cycle activities and tasks referenced in this part of ISO/IEC 15026 can be recorded in the form of the assurance case described in ISO/IEC 15026-2.

ISO/IEC 15026-3 addresses the assignment of integrity levels for selected elements of a system. Where ISO/IEC 15026-2 is applicable, it can bring useful structure, aid, and direction to defining claims and showing their achievement through the use of integrity levels and accompanying integrity level requirements.

ISO/IEC 15026-2, ISO/IEC 15026-3 and ISO/IEC 15026-4 all use the concepts and vocabulary defined in ISO/IEC TR 15026-1; however, any part can be applied independently of the others and the use of one does not require the use of any others.

INTERNATIONAL STANDARD **ISO/IEC 15026-4:2012(E)**

Systems and software engineering — Systems and software assurance —

Part 4: Assurance in the life cycle

1 Scope

This part of ISO/IEC 15026 gives guidance and recommendations for conducting selected processes, activities and tasks for systems and software products requiring assurance claims for properties selected for special attention, called critical properties. This part of ISO/IEC 15026 specifies a property-independent list of processes, activities and tasks to achieve the claim and show the achievement of the claim. This part of ISO/IEC 15026 establishes the processes, activities, tasks, guidance and recommendations in the context of a defined life cycle model and set of life cycle processes for system and/or software life cycle management.

NOTE The stakeholders determine which of the system or software properties are selected for special attention and require assurance claims. This part of ISO/IEC 15026 uses the term “critical” to distinguish those properties from other requirements.

2 Conformance

Conformance may be claimed to this part of ISO/IEC 15026 with respect to the systems assurance process view and/or the software assurance process view. Thus, conformance to this part of ISO/IEC 15026 can be achieved in either or both of the following ways:

a) Demonstrating that the required outcomes of the systems assurance process view (6.1.2) have been achieved, in addition to conforming to the Agreement, Project, and Technical processes of ISO/IEC 15288.

b) Demonstrating that the required outcomes of the software assurance process view (6.2.2) have been achieved, in addition to conforming to the Agreement, Project, Technical, and Software Specific processes of ISO/IEC 12207:2008.

A claim of conformance is relevant only to specific claims regarding designated systems or software.

Conformance to ISO/IEC 15026 Part 2 can assist in achieving the outcomes required by the two process views in this part of ISO/IEC 15026.

NOTE Parties to an agreement may choose to incorporate selected portions of this part of the International Standard into the terms of the agreement. However, compliance with the agreement does not justify a claim of conformance to this part of the International Standard. A claim of conformance can only be justified as explained above.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced documents (including any amendments) applies.

ISO/IEC TR 15026-1, *Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary*

This part requires activities and tasks in the context of complete sets of life cycle processes that comprise life cycle models for projects. The two sets of life cycle processes are provided in:

ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*

The assurance guidance and recommendations referenced in this part of ISO/IEC 15026 are to be understood in terms of their being in the context of the processes, activities and tasks of ISO/IEC 15288 and ISO/IEC 12207.

4 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 15026-1, ISO/IEC 15288:2008, and ISO/IEC 12207:2008 apply.

5 Key concepts for and use of this part of ISO/IEC 15026

5.1 Life cycle approach

It is presumed that the user of this International Standard is using a defined life cycle model and set of life cycle processes for system and/or software life cycle management. Across the life cycle, the systems and software process views in Clause 6 use the guidance and recommendations in Clause 7 for the performance of specific processes, activities, and tasks in order to achieve and show the achievement of assurance claims. Since all processes of ISO/IEC 15288 and ISO/IEC 12207 are applied iteratively and recursively in the life cycle, the guidance and recommendations for assurance are also applied iteratively and recursively. In that way, the achievement of assurance can be checked during each iteration or recursion.

NOTE See ISO/IEC TR 24748-1 for more information about life cycle models and the iteration and recursion of processes.

5.2 Assurance claims

When system or software product requirements call for assurance of one or more critical properties of the system or software product, the overall claims for assurance regarding these properties' values are referred to in ISO/IEC 15026 as assurance claims. Commonly, such critical properties are in areas where substantial risk or consequences are involved such as reliability and maintainability, safety, security, or human factors.

NOTE The material in this clause is adopted from ISO/IEC 15026-2.

Achieving assurance claims normally includes all the considerations involved in achieving stringent requirements. A requirement is defined in ISO/IEC 29148 as “statement which translates or expresses a need and its associated constraints and conditions” and a claim is defined in ISO/IEC TR 15026-1 as “statement of something to be true including associated conditions and limitations.” This part of ISO/IEC 15026 considers requirements to be statements of values for variables and claims to be statements of requirements to be true.

While assurance claims can be derived from a number of sources, they are normally motivated by potential real-world adverse consequences related to the intended uses of the system and justified as deriving from system or software requirements. Each assurance claim is fully and unambiguously specified including:

a) “Assurance claims” — that is, the top-level claims, including

    1) Values for the variables of the critical property required for its achievement.

    2) Limitations on allowable uncertainties regarding this achievement.

    3) Conditions and/or durations of applicability under which it applies.

4) The set of versions or instances of the system or software product covered by the claims.

c) “Justification for assurance claims” — that is, the justification for selecting and specifying these particular assurance claims.

d) “Body of information showing achievement of assurance claims” or more succinctly as the “information showing [or assuring] the achievement of assurance claims”.

This last item includes the evidence, the rationale or argument showing how the evidence supports the claims, and any assumptions underlying this rationale. Normally, this rationale has multiple levels of derived claims internal to it, e.g., claims about system elements at each level of decomposition that need to be true in order for the assurance claims about the system or software product to be true. The body of information also includes information on the validity, integrity, relevance, and significance of the evidence.

The rationale often includes several different kinds of arguments, e.g., arguments based on design rationale, use of defensive design techniques, verification and validation results, performance of similar systems or products, conformance to standards, or field data. These are combined to achieve an overall conclusion and an estimate of the remaining uncertainty regarding the achievement of the assurance claims.

The body of information composing and organizing these three items is an element (or elements) of the system or software product and, as such, is maintained and updated throughout the system life cycle, to include development as well as maintenance. As a system element, all the processes, activities, and tasks regarding a system element apply to it, such as configuration management, verification, and validation.

5.3 Using this part of ISO/IEC 15026

This part of ISO/IEC 15026 can be used for an agreement between an acquirer and supplier, for regulation purposes, or for assessment of internal development processes to improve achieving and showing the achievement of assurance claims for the system or software product. Its use is, however, not limited to these three purposes.

5.3.1 Use for an agreement

This part of ISO/IEC 15026 can be used for an agreement between an acquirer and a supplier concerning achieving and showing the achievement of an assurance claim about the value of variables for a critical property of the system or software product being acquired. The acquirer and supplier relationship can occur at different levels of the supply chain (prime-supplier, internal to one organization, etc.).

NOTE An agreement may range in formality from a written contract to a verbal understanding.

5.3.2 Use for regulation

An authoritative body can use this part of ISO/IEC 15026 for regulation for assuring some critical property of a system or software product. The need for such regulation can arise to assure or certify a critical property of a system or software product, to clarify their assurance in the condition of trade, or to do some other action.

5.3.3 Use for development

This part of ISO/IEC 15026 can be used for an internal assessment by a developer in improving its processes for achieving and showing the achievement of assurance claims for critical properties of systems and software products it develops.

6 Process view purposes and required outcomes

6.1 Systems assurance process view

The following clauses define the purpose and required outcomes of the systems assurance process view.

6.1.1 Purpose

The purpose of the Systems Assurance Process View is to achieve the assurance claims regarding the system properties selected for special attention and to provide a body of information showing the achievement of those claims. The Systems Assurance Process View covers the system of interest including any constituent software.

6.1.2 Required outcomes

The following outcomes shall result from the successful implementation of the Systems Assurance Process View:

a) A subset of requirements for the achievement of critical properties is defined.

b) Assurance claims, their justification, and the body of information showing the achievement of the assurance claims for the critical properties are established as an element of the system.

c) A strategy for achieving these assurance claims and showing their achievement is defined.

d) The extent of achievement of the assurance claims is communicated to affected stakeholders.

6.2 Software assurance process view

The following clauses define the purpose and required outcomes of the software assurance process view.

6.2.1 Purpose

The purpose of the Software Assurance Process View is to achieve the assurance claims regarding the software properties selected for special attention and to provide a body of information showing the achievement of those claims.

6.2.2 Required outcomes

The following outcomes shall result from the successful implementation of the Software Assurance Process View:

a) A subset of requirements for achievement of the critical properties for application of this process view is defined.

b) Assurance claims, their justification, and the body of information showing achievement of the assurance claims for the critical properties are established as an element of the system.

c) A strategy for achieving these assurance claims and showing their achievement is defined.

d) The extent of achievement of the assurance claims is communicated to affected stakeholders.

7 Assurance guidance and recommendations for selected processes

7.1 Introduction

Clause 7 cites the activities and tasks from the Agreement, Project, and Technical categories of processes in ISO/IEC 15288:2008 and in ISO/IEC 12207:2008 that require extension or special interpretation when a defined level of assurance is to be demonstrated. The numbers of those activities and tasks correspond to the numbers in the parent standards (ISO/IEC 15288 and ISO/IEC 12207). Assurance-claim-related guidance and recommendations are provided for performing these activities and tasks to achieve the outcomes of the process views. This guidance and recommendations assume and depend upon the full application of ISO/IEC 15288 and ISO/IEC 12207 as indicated in Clause 3. The processes and activities not cited in this clause are considered adequate as defined in ISO/IEC 15288:2008 and ISO/IEC 12207:2008 to achieve the claims for the critical properties.

7.2 Acquisition process

The Acquisition Process (ISO/IEC 15288:2008, 6.1.1 and ISO/IEC 12207:2008 6.1.1) obtains a product or service in accordance with the acquirer's requirements. When the acquisition is for a system element, this process should ensure that all requirements for achieving or showing the achievement of any assurance claim associated with that system element is passed to the supplier through the agreement.

7.2.1 Relevant activities and tasks

Activities from 15288	Activities from 12207
6.1.1.3 c) Initiate an agreement. 1) Negotiate an agreement with the supplier. d) Monitor the agreement. 1) Assess the execution of the agreement. 2) Provide data needed by the supplier and resolve issues in a timely manner.	6.1.1.3.4 Contract agreement. 6.1.1.3.4.2 The acquirer shall then prepare and negotiate an agreement with the supplier that addresses the acquisition requirements, including the cost and schedule, of the software product or service to be delivered. The contract shall address proprietary, usage, ownership, warranty and licensing rights associated with the reusable off-the-shelf software products. 6.1.1.3.5 Agreement monitoring. 6.1.1.3.5.1 The acquirer shall monitor the supplier's activities in accordance with the Software Review Process and the Software Audit Process. The acquirer should supplement the monitoring with the Software Verification Process and the Software Validation Process as needed.

7.2.2 Assurance guidance and recommendations

The project should ensure that the agreement considers the variables and their values of the critical properties for the system element being acquired. The agreement should include integrity requirements (i.e., guarding against counterfeit parts, tampering, system elements with vulnerabilities, and revealing of confidential information including information about vulnerabilities to ensure that what is received is what is expected. The project should derive the claims for the system element being acquired from the system's assurance claims and incorporate them into the request for the supply of the system element. In addition, the project should incorporate the following considerations into the negotiations and the agreement with the supplier:

a) Confidence that the appropriate controls regarding dependability (e.g., trustworthiness) of their personnel and those of their associated organizations are effectively implemented.

b) Confidence that the supplier guards against counterfeit parts, tampering, and other threats to system or product integrity as well as against revealing confidential information.

c) Confidence that the system element transferred, received, and, to the extent practicable, installed and operated, is the one intended.

d) Confidence that the product development environment has appropriate resources in place to protect the integrity of the product and its critical properties during development.

e) Confidence that the system or software development life cycle model chosen by the supplier is appropriate to the nature of any assurance claims to be achieved.

f) Confidence that the appropriate controls regarding implementation of dependability and safety requirements and the achievement of system dependability and safety integrity requirements are effectively implemented.

g) Confidence that the development lifecycle is conducted using well documented, repeatable processes that are monitored in accordance with a quality management plan appropriate to the nature of the claims to be achieved.

The project should revisit the approaches to showing achievement of claims when considering an acquisition from a supplier when the supplier relationship changes (i.e. new, acquired by another entity, merged with another entity) or if the acquirer's requirements change to ensure that the supplier does not deny required information, enable a new threat, or undermine the safeguards already in place to protect the system.

The project should submit a request for proposal (RFP) that can be correctly understood by the supplier and other stakeholders and establish a procedure for resolving problems, which may even expand to a change in the agreement in the case of extensive problem resolution. Upon a change of agreement, the project should ensure that the stakeholder requirements defined in the Stakeholder Requirements Definition process are the starting point of the change. The project should consider a multi-stage agreement when appropriate.

NOTE Refer to ISO/IEC 12207:2008 Annex F.3 of for a description of the Contract change management process.

7.3 Supply process

The Supply Process (ISO/IEC 15288:2008, 6.1.2 and ISO/IEC 12207:2008 6.1.2) provides an acquirer with a product or service that meets agreed requirements. When a system element is being supplied, this process should ensure that all requirements for achieving or showing the achievement of any assurance claim associated with that system element are passed to the acquirer.

7.3.1 Relevant activities and tasks

Systems Assurance Process View	Software Assurance Process View
6.1.2.3 c) Initiate an agreement 1) Negotiate an agreement with the acquirer. d) Execute the agreement. 1) Execute the agreement according to the Supplier's established project plans and in accordance with the agreement. 2) Assess the execution of the agreement.	6.1.2.3.4 Contract execution. 6.1.2.3.4.8 The supplier shall monitor and control the progress and the quality of the software products or services of the project throughout the contracted life cycle. This shall be an ongoing, iterative task, which shall provide for: a) Monitoring progress of technical performance, costs, and schedules and reporting of project status. b) Problem identification, recording, analysis, and resolution.

7.3.2 Assurance guidance and recommendations

The project should ensure that the agreement considers the feasibility of the variables and their values of the critical properties for the system element being supplied, from the technical and resources aspects. The agreement should include integrity requirements to ensure that what is supplied is what is expected. The project should provide the evidence and argument for the claims for the system element derived from the system's assurance claims. In addition, the project should incorporate the following considerations into the negotiations and the agreement with the acquirer, in order to achieve assurance which offsets the resource available to the project:

a) Confidence that there is a means to fulfil major requirements in a practical manner from technical and other aspects.

b) Consideration of a multistage agreement, in the case that the precise cost estimation is difficult to achieve.

c) Consideration of stepwise commencement of operations of the system, should there be a possibility of missing the deadline due to unexpected reason.

7.4 Project planning process

The Project Planning Process (ISO/IEC 15288:2008, 6.3.1 and ISO/IEC 12207:2008, 6.3.1) produces and communicates effective and workable project plans. For assurance, project plans include adequate resources to achieve the assurance claims and show the achievement of the claims.

NOTE The assurance claims and showing achievement of those claims can be captured in an assurance case with the structure and format as in Part 2 of ISO/IEC 15026.

7.4.1 Relevant activities and tasks

Activities from 15288	Activities from 12207
6.3.1.3 a) Define the project. 1) Identify the project objectives and constraints. 3) Define and maintain a life cycle model that is comprised of stages using the defined life cycle models of the organization. b) Plan the project resources. 1) Define and maintain a project schedule based on project objectives and work estimates. 2) Define project achievement criteria for the life cycle stage decision gates, delivery dates and major dependencies on external inputs or outputs. 3) Define the project costs and plan a budget. 4) Establish the structure of authorities and responsibilities for project work. 5) Define the infrastructure and services required by the project. 6) Plan the acquisition of materials, goods and enabling system services supplied from outside the project c) Plan the project technical and quality management. 1) Generate and communicate a plan for technical management and execution of the project, including reviews.	6.3.1.3.1 Project initiation. 6.3.1.3.1.1 The manager shall establish the requirements of the project to be undertaken. 6.3.1.3.2 Project planning. 6.3.1.3.2.1 The manager shall prepare the plans for execution of the project. The plans associated with the execution of the project shall contain descriptions of the associated activities and tasks and identification of the software products that will be provided. These plans shall include, but are not limited to, the following: a) Schedules for the timely completion of tasks. b) Estimation of effort. c) Adequate resources needed to execute the tasks. d) Allocation of tasks. e) Assignment of responsibilities. f) Quantification of risks associated with the tasks or the process itself. g) Quality assurance measures to be employed throughout the project. h) Costs associated with the process execution. i) Provision of environment and infrastructure. j) Definition and maintenance of a life cycle model that is comprised of stages using the defined life cycle models for projects of the organization.

7.4.2 Assurance guidance and recommendations

The project should include assurance objectives for the critical properties in the project objectives. These assurance objectives should include constraints and reflect the laws, regulations, and standards for project compliance to achieve those objectives, ensuring that activities and tasks for obtaining necessary licenses or certifications is included in the planning. For example, for a critical property such as safety, obtaining required safety certifications should be reflected in project planning.

NOTE Assurance objectives are based on the defined critical properties by identifying the dangers and adverse consequences including harm, threats, and hazards that are to be managed or affected by the system and by considering the tolerable values of the variables for those critical properties and maximum acceptable uncertainties.

These objectives should be communicated to as many stakeholders in the project as possible, including top management, customers and suppliers.

The development method, environment and tools should be determined according to the requirements of the system.

NOTE Each of the development methodologies, such as process oriented, data oriented and object oriented methods, has its own suitability to different applications. The development method should be chosen according to an analysis of the work flow and information processed by the system.

The project should ensure that personnel have sufficient skills and authority to adequately cover all the requirements related to the critical properties and to address achieving and showing the achievement of the claims for those critical properties.

The project plan should include planning to achieve assurance claims and to show that project progress is consistent with the claims being met in a timely manner, including planning to deal with the potential effects from vulnerabilities and weaknesses that can affect claims. The project should clarify the tasks and responsibility with respect to the claims.

The project should plan for independent reporting regarding assurance claims including responsibilities for claims-related reporting and issues management; document these issues and reports; and determine how reporting and information dissemination will be coordinated throughout the organization (including customers and suppliers as needed).

The project should incorporate decision points and milestones to manage cost, schedule, and performance risks associated with uncertain, ambiguous and emerging requirements that contribute to achieving the claim. These decision points should be at the relevant points in the project so that important decisions and requirements from stakeholders are not postponed, regardless of their complexity.

The project should determine the ancillary actions required for showing the achievement of claims for critical properties, besides software and system development, and calculate the cost, timescales and resources necessary for their completion. The goal for these ancillary actions should be given quantitatively whenever possible. Quantitative estimation is necessary for achievement evaluation in the Operation Process. The achievement evaluation should be continued throughout the period of applicability of the relevant assurance claim (e.g., safety monitoring equipment within the nuclear industry).

The project should evaluate the use of off-the-shelf and bespoke products as system elements according to the project needs. In the evaluation, the project should consider how using off-the-shelf system elements may affect achieving the claims and showing the achievement of the claims for the critical properties because of the risk that may be caused by black-boxing the functionality performed by those system elements. Where customisation is required, particular attention should be given to ensuring that assurance claims are not invalidated.

7.5 Decision Management process

The Decision Management Process (ISO/IEC 15288:2008, 6.3.3 and ISO/IEC 12207:2008 6.3.3) selects the most beneficial course of project action where alternatives exist. For assurance the Decision Management Process activities need to ensure that the consequences of achieving the claim and showing the achievement of the claim for the critical property are considered whenever a decision is made.

7.5.1 Relevant activities and tasks

Activities from 15288	Activities from 12207
6.3.3.3 a) Plan and define decisions. 1) Define a decision management strategy. 2) Identify the circumstances and need for a decision. 3) Involve relevant parties in the decision-making in order to draw on experience and knowledge. b) Analyze the decision information. 2) Identify desired outcomes and measurable success criteria.	6.3.3.3.1 Decision planning: 6.3.3.3.1.1 The project shall define a decision-making strategy. 6.3.3.3.1.2 The project shall involve relevant parties in the decision-making in order to draw on experience and knowledge. 6.3.3.3.1.3 The project shall identify the circumstances and need for a decision. 6.3.3.3.2 Decision analysis: 6.3.3.3.2.1 The project shall select and declare the decision-making strategy for each decision situation. The project shall identify desired outcomes and measurable success criteria.

7.5.2 Assurance guidance and recommendations

The project should include assurance-claims-related decisions as a category of decision types in the decision management strategy. The decision management strategy should ensure that any effects on achieving and showing the achievement of assurance claims are included in the evaluation of consequences and associated risks of alternative actions in any decisions affecting policies, procedures, plans, personnel, environment, products, services, and critical supporting infrastructure. Once a decision relevant to claims has been made, its effect should be reflected in the approaches to showing their achievement. Decision criteria for trade-offs and other decisions should protect the assurance of the critical property and should involve the stakeholders of that critical property.

7.6 Risk Management process

The Risk Management Process (ISO/IEC 15288:2008, 6.3.4 and ISO/IEC 12207:2008 6.3.4) identifies, analyzes, treats and monitors the risks continuously and can be applied to risks related to the acquisition, supply, development, maintenance, operation or disposal of a system. The activities and tasks of the risk management process are a key part of the approach to showing achievement of claims.

NOTE Although the first sentence above is taken from 15288, the Part of ISO/IEC 15026 added “supply” due to the assurance risks inherent in the supply of a system.

7.6.1 Relevant activities and tasks

Activities from 15288	Activities from 12207
6.3.4.3 a) Plan risk management. 1) Define risk management policies. b) Manage the risk profile. 3) Establish and maintain a risk profile. c) Analyze risks. d) Treat risks. 2) Implement risk treatment alternatives for which the stakeholders determine that actions should be taken to make a risk acceptable. e) Monitor risks. 2) Implement and monitor measures to evaluate the effectiveness of risk treatments.	6.3.4.3.1 Risk management planning. 6.3.4.3.1.1 Risk management policies describing the guidelines under which risk management is to be performed shall be defined. 6.3.4.3.1.2 A description of the Risk Management Process to be implemented shall be documented. 6.3.4.3.1.3 The parties responsible for performing risk management and their roles and responsibilities shall be identified. 6.3.4.3.1.4 The responsible parties shall be provided with adequate resources to perform the Risk Management Process. 6.3.4.3.1.5 A description of the process for evaluating and improving the Risk Management Process shall be provided. 6.3.4.3.2 Risk profile management. 6.3.4.3.2.1 The context of the Risk Management Process shall be defined and documented. 6.3.4.3.2.2 Risk thresholds, defining the conditions under which a level of risk may be accepted, shall be documented. 6.3.4.3.2.3 A risk profile shall be established and maintained. 6.3.4.3.2.4 The relevant risk profile shall be communicated periodically to stakeholders based upon their needs. 6.3.4.3.3 Risk analysis. 6.3.4.3.3.1 Risks shall be identified in the categories described in the risk management context. 6.3.4.3.3.2 The probability of occurrence and consequences of each risk identified shall be estimated. 6.3.4.3.3.3 Each risk shall be evaluated against its risk thresholds. 6.3.4.3.3.4 For each risk that is above its risk threshold, recommended treatment strategies shall be defined and documented. Measures indicating the effectiveness of the treatment alternatives shall also be defined and documented.

7.6.2 Assurance guidance and recommendations

Managing assurance-related risks should be thoroughly integrated throughout the risk management process in priority setting, decision making, establishing and maintaining the risk profile, and risk treatment. The information justifying the selection and specification of the assurance claims, the body of information showing achievement of the claims, and the required limitations on uncertainty can be used as a framework for organizing and addressing systems assurance risks. This information should contain the relevant assumptions, data, judgments, and calculations needed to underpin risk analysis and allow risk estimates to be reviewed, reconstructed, and audited.

Throughout the system life cycle, emphasis should be given to causal factors and conditions for their occurrence, warning signs and indications of emerging risks, and the consequences of risks. In addition, careful attention should be given to difficulties in achieving needed evidence, in ensuring prompt reporting and assessment of reports, and in maintenance of complete records. Practices to analyze and mitigate adverse effects on assurance should be developed and used when suppliers of off-the-shelf or bespoke products make changes to these products without providing detailed information about those changes.

Risks and sources of risks attributable to security vulnerabilities and weaknesses, threats, hazards, faults, human error and changes to the system or its environment should be identified throughout the system life cycle. The project should assume the existence of intelligent and malicious adversaries in establishing and maintaining its risk profile because of the crucial nature of the risks involved. When estimating the probability of occurrence and consequences of each identified risk, the project should consider the complete chain of effects that an intelligent adversary could cause. A risk of subversion exists during any of the system life cycle processes including the risk management process itself.

The possibilities of failing to achieve the assurance claims and failing to acceptably show this achievement should be realistically considered, including the risks of having to redo parts of the system. The project should evaluate the potential for not being able to achieve the necessary systems assurance in a timely manner, resulting in a risk to the system certification or accreditation or resulting in the system not being used as intended. Contingency action in the event that assurance claims cannot be achieved in a timely manner should be identified, planned, and approved by the relevant stakeholders.

7.7 Configuration management process

The Configuration Management Process (ISO/IEC 15288, 6.3.5, and ISO/IEC 12207, 6.3.5) establishes and maintains the integrity of all identified artefacts of a project or process and makes them available to concerned parties. For assurance, two relationships exist: (1) Effective configuration management of the system elements is evidence in the information showing achievement of assurance claims; (2) the information showing achievement of the assurance claims itself is under configuration management.

7.7.1 Relevant activities and tasks

Activities from 15288	Activities from 1207
6.3.5.3 a) Plan configuration management. 1) Define a configuration management strategy. b) Perform configuration management. 1) Maintain information on configurations with an appropriate level of integrity and security.	6.3.5.3.1 Configuration management planning. 6.3.5.3.1.1 The project shall define a configuration management strategy. 6.3.5.3.2 Configuration management execution. 6.3.6.3.2.1 The project shall maintain information on configurations with an appropriate level of integrity and security.

7.7.2 Assurance guidance and recommendations

The configuration management strategy should be developed to determine how to get relevant information from the configuration management process into the information assuring claims, including during maintenance, and to provide protection of configuration item data and meta-data, both in repositories and under modification.

The project should identify planned assurance-claim-related information and periodically combined it into an identified configuration to constitute an organized version of the information assuring claims. Review and audit of configuration management procedures and activities should be done to prevent accidental or unauthorized modifications of controlled products and to recommend corrective and preventive actions relating to assurance claims.

The project should ensure consistency of the integrity and security of the structure and information contained in the information assuring claims with the approach to showing achievement of claims. Required assurance information should be identified and periodically combined in an identified configuration to constitute an organized version of the information assuring claims. Access and distribution control, storage, and protection should be maintained throughout the product or service life cycle.

The project should tailor configuration management to facilitate the achieving and assuring of claims. At a minimum:

a) Employing rigor and protective measures commensurate with the criticality of the system, data, mission, and the assuring of claims and are flexible enough to enable addressing a wide variety of threats.

b) Adjusting granularity within the configuration management process to support the approach to showing achievement of claims.

The project should establish and maintain required confidentiality, integrity, availability, authentication, accountability (including non-repudiation), and auditability of information assuring claims, including incorporating the following strategies and techniques for configuration management processes and supporting tools:

a) Strong per user authentication. If passwords are used for authentication, they should always be encrypted for transmission over a network, and never stored as plain text anywhere.

b) Repositories hardened against attack. For example, on the platform supporting the centralized repository, limit the number of other services being run to reduce the risk that these other services could expose the repository to attack. Restrict and monitor network access for the CM system.

c) Quality acceptance criteria to avoid introducing unacceptable elements or documents.

d) Audits of the configuration management repositories and administration.

e) Records and measurements regarding access and updates to the data, to determine if there is unexpected or unusual activity (e.g., activity with unusual times, locations, systems, or people; individuals updating an unusually large number of configuration items, etc.).

f) Physical protection of configuration management systems (e.g., by locking them up) and controlled access to the system.

g) Processes to help counter data loss or subversion of a configuration management repository.

h) Controlled entry points for those needing access to the configuration management data.

The project should assess the risks arising from the use of the configuration management process including risks from human error, including maliciousness, unless documented justification is provided for doing otherwise.

NOTE Additional guidance for these configuration management practices is available in ISO/IEC 27002, *Information technology Security techniques Code of practice for information security management*, and ISO 10007:2003, *Quality management systems Guidelines for configuration management*.

7.8 Information Management process

The Information Management Process (ISO/IEC 15288, 6.3.6, and ISO/IEC 12207, 6.3.6) provides relevant, timely, valid and, if required, confidential information to designated parties during and, as appropriate, after the system life cycle. For assurance, this process provides the information about the achievement of assurance claims to the relevant stakeholders and provides for delivery of the body of information showing achievement of assurance claims to relevant stakeholders, including regulatory or approval authorities.

7.8.1 Relevant activities and tasks

Activities from 15288	Activities from 12207
6.3.6.3 a) Plan information management. 1) Define the items of information that will be managed during the system life cycle and, according to organizational policy, agreements, or legislation, maintained for a defined period beyond. 2) Designate authorities and responsibilities regarding the origination, generation, capture, archiving and disposal of items of information. 3) Define the rights, obligations and commitments regarding the retention of, transmission of and access to information items. 4) Define the content, semantics, formats and medium for the representation, retention, transmission and retrieval of information. 5) Define information maintenance actions. b) Perform information management. 3) Retrieve and distribute information to designated parties as required by agreed schedules or defined circumstances.	6.3.6.3.1 Information management planning. 6.3.6.3.1.1 The project shall define the items of information that will be managed during the system life cycle and, according to organizational policy or legislation, maintained for a defined period beyond. 6.3.6.3.1.2 The project shall designate authorities and responsibilities regarding the origination, generation, capture, archiving and disposal of items of information. 6.3.6.3.1.3 The project shall define the rights, obligations and commitments regarding the retention of, transmission of and access to information items. 6.3.6.3.1.4 The project shall define the content, semantics, formats and medium for the representation, retention, transmission and retrieval of information. 6.3.6.3.1.5 The project shall define information maintenance actions. 6.3.6.3.2 Information management execution. 6.3.6.3.2.3 The project shall retrieve and distribute information to designated parties as required by agreed schedules or defined circumstances.

7.8.2 Assurance guidance and recommendations

The project should plan for and establish a documented body of information providing grounds for confidence in the assurance claims consisting of assumptions, arguments, structured evidence, and relationships among these that show how the claims will be or have been satisfied.

NOTE Part 2 of this International Standard provides a structure for this information in the form of an assurance case if an assurance case is required by the stakeholders interested in the assurance of a particular critical property.

EXAMPLE When such claims are made for the critical properties of “safety” or “security” of the system, the body of information should provide an argument covering the full required scope for the safety or security. The arguments and supporting evidence should be built, collected, and maintained throughout the life cycle and are typically derived from multiple sources.

The project should also collect, organize, and analyze the following additional relevant information related to assuring claims:

a) Existing information and evidence including relevant information from prior versions and similar systems and their similar sets of information including any arguments and justification for using it to mitigate risks and generate for both successes and failures.

b) Information concerning the validity and integrity of the information assuring claims.

c) Information and reports related to failure, human errors, faults, weaknesses, and incidents related to assuring claims.

The project should manage and control information related to assuring claims to preserve its integrity and validity. This includes protecting information related to assuring claims, including protection from malicious actions; limiting access to sensitive information, including threat and hazard information, and maintaining the required confidentiality; and responding to incidents involving the information assuring claims.

Whenever a change is made in the information related to assuring claims, the part of the agreement that is relevant to the change and the relationship between the change and the relevant part of the agreement should be clarified.

The project should provide reports that summarize this set of information, changes to it, and its quality and completion status at planned intervals and as necessary for effective oversight and management. This includes establishing reporting channels that provide visibility to relevant information needed by stakeholders in decision making. Such information includes what the system is expected to do in typical usage circumstances in order for users to identify when the system does something unexpected because this may indicate a potential breach of compliance with restrictions. The user should know how to report or act upon non-routine or emergent conditions and any breaches of compliance with restrictions so users do not compromise compliance with restrictions.

The written documents that affect stakeholder agreements should be managed so that any discrepancy with a stakeholders’ interpretation is minimised. Such documents include, but are not limited to, the request for proposals (RFPs) by the acquirer and the proposal by the project.

7.9 Stakeholder Requirements Definition process

The Stakeholder Requirements Definition Process (ISO/IEC 15288:2008, 6.4.1 and ISO/IEC 12207:2008 6.4.1) defines the requirements for a system that can provide the services needed by users and other stakeholders in a defined environment. It identifies stakeholders, or stakeholder classes, involved with the system throughout its life cycle, and their needs, expectations, and desires. It analyzes and transforms these into a common set of stakeholder requirements. As a subset of these requirements, critical properties for which a high degree of confidence is required for their achievement are identified and documented.

7.9.1 Relevant activities and tasks

Activities form 15288	Activities from 12207
6.4.1.3 c) Analyze and maintain stakeholder requirements 1) Analyze the complete set of elicited requirements. 6) Maintain stakeholder requirements traceability to the sources of stakeholder need.	6.4.1.3.3 Requirements evaluation. This activity consists of the following task: 6.4.1.3.3.1 The project shall analyze the complete set of elicited requirements. 6.4.1.3.4 Requirements agreement. This activity consists of the following tasks: 6.4.1.3.4.2 The project shall feed back the analyzed requirements to applicable stakeholders to ensure that the needs and expectations have been adequately captured and expressed. 6.4.1.3.4.3 The project shall establish with stakeholders that their requirements are expressed correctly.

7.9.2 Assurance guidance and recommendations

A set of critical properties should be determined by analysis of the complete set of requirements collected from the stakeholders. As stakeholders define their requirements, some will emerge as requiring high confidence in their achievement because they are associated with important consequences, risks, regulations or other mandates (e.g., anti-tamper, security), relating to properties of the system. Requirements requiring high confidence can be used to identify the critical properties of the system or software product. The project should aid in this selection from the technical point of view, such as by identifying additional risks, consequences and related uncertainties, and compliance requirements.

As part of selecting critical properties, the project should define preliminary requirements for showing achievement of these properties, paying particular attention to tradeoffs related to stakeholder tolerance for risks. Stakeholders need to identify their tolerance for failure, degradation, and compromise or loss, e.g., degraded modes of operation. The project also should identify any cultural, social, and organizational context of a system that might affect achievement or showing the achievement of a particular property. This activity is aided by using experience and records regarding previous versions or similar systems and operational environments as well as known intentions or predictions regarding the use of the system in its environment.

The project should prioritize properties in order to select which ones are the most critical for providing assurance claims. The selected critical properties with the justification and rationale for their selection should be documented and become part of the traceability to that particular stakeholder need and maintained for later investigation when necessary. This documentation and maintenance of the rationale is done as a part of maintaining stakeholder requirements traceability to the sources of stakeholder need. The selected critical properties are used for the top-level assurance claims.

During the analysis of the stakeholder requirements, the fact that each stakeholder has their own circumstance and set of values should be taken into account.

NOTE The project should work across the set of technology-knowledgeable stakeholders to determine the feasibility of requirements across the lifecycle. The full lifecycle should be considered to determine the requirements feasibility and avoid modifications that drive undesirable changes in costs, schedule and/or performance later in the lifecycle when more technical detail about the system is known.

The project should strive to eliminate indeterminate items in the set of elicited stakeholder requirements. Both functional and nonfunctional requirements should be examined and defined, reflecting the information about peak amounts of work, monthly accountant deadlines, and practical experience of development and operation. Doing so should minimise the technically oriented risks so as to enable more precise estimation of the human resources, deadlines and cost for the system life cycle. Should the indeterminate items remain or technically oriented risks be unavoidable, the project should make them explicit and manage them in the risk management process in as early a stage of the life cycle as possible.

NOTE 1 Refer to ISO/IEC 29148:2011, Requirements Engineering, to understand and include all the types of requirements and operational concepts.

NOTE 2 The acquirer should define and mange requirements based on the type of life cycle for the project in order to enable the project to estimate cost and start development, and the project should estimate cost early based on the final requirements in order to enable the acquirer to judge the investment. These actions may not be their first inclinations because of anticipation of hidden risks.

The stakeholder requirements should be kept as simple as possible because complicated requirements tend to result in a complicated system with high cost for development and operation and may make the critical property more difficult to assure.

The project should ensure that decisions necessary in the later stages of the life cycle are based on the stakeholder requirements defined in this process.

The project should ensure the involvement of all relevant stakeholders (e.g., those stakeholders familiar with the business need for the critical property and knowledge of the critical property) in requirements definition to keep the introduction of additional stakeholder requirements to a minimum in later stages of the life cycle.

NOTE Collaboration is essential in defining the purpose of the system or software product (e.g. new business enabled by the new system or software). The project personnel have the system or software development technology knowledge but no detailed image of the use of the system or software, while the acquirers, customers, or users understand what the use of the system or software would be without the technical skill to build it.

The project should try to minimize both the number of work items that are necessary but not listed in the stakeholder requirements and any duplication of work items in the stakeholder requirements. These actions help minimize the risk of misunderstanding between stakeholders.

The project should provide support to stakeholders as required. Some stakeholders may not have a technical background and may need technical assistance in defining stakeholder requirements or in negotiation to resolve conflicting stakeholder requirements. Explicit interpretation of the stakeholder’s requirements and the technical application of those requirements may be necessary to ensure a common understanding among both technical and non-technical stakeholders.

The stakeholders should agree that they all share the duty of requirements definition, in the sense that they need to provide their requirements in a proper manner. The system analyst may have the responsibility for eliciting the requirements, but then the other stakeholders have the duty to act cooperatively with the analyst.

The project should ensure that the approach to achieving and showing the achievement of the assurance claims of the chosen critical properties of the system or software product is reconciled in the context of the business or concept of operations to be conducted with the system or software product.

In the case of updating an existing system, the analyst conducting the stakeholder requirements definition process should be cautious about the phrase “the same as the present system” in stakeholder requirements. When such requirements arise, the analyst should thoroughly examine whether the current use of the system or the current values of the system variables will in fact be kept unmodified in the updated system. Special attention should be given to the critical properties and the claims for those properties in the current system when a system is updated.

Although essential requirements are defined and confirmed under this process, Stakeholder Requirements Definition, they are subject to change as a result of resolving conflicts between requirements of different stakeholders and limitations from the system considerations when conducting the activities of the next process, Requirements Analysis. The activities and tasks of these two processes are, therefore, conducted iteratively. Due to cost, schedule, and other constraints or changes in stakeholder needs, requirements will evolve. As agreements on changes in requirements are made, impacts on the ability to achieve agreements related to the critical properties should also be addressed, although an agreement should be respected and should not be changed too easily, even if no legal or financial action results.

NOTE 1 Refer to ISO/IEC 29148:2011, Requirements engineering, Clause 5, for more discussion of the iterative nature of these activities and tasks.

NOTE 2 A process for conducting a change of agreement is included in ISO/IEC 12207:2008, Annex F.3, Contract Change Management Process.

7.10 Requirements Analysis process

The Requirements Analysis Process (ISO/IEC 15288:2008, 6.4.2) and the System Requirements Analysis process (ISO/IEC 12207:2008 6.4.2) transforms the stakeholder, requirement-driven view of desired services into a technical view of a required product that could deliver those services. The Software Requirements Analysis process (ISO/IEC 12207, 7.1.2) establishes the requirements of the software elements of the system. The main assurance-claim-related purpose of requirements analysis is to derive a set of assurance claims from critical properties. Requirements Analysis takes the selected critical properties from the Stakeholder Requirements Definition process and assigns variables for evaluating the property and values to those variables for measuring the property. The assurance claim is then a statement about the value of the variables for that property.

NOTE In Part 1, a claim is defined to be a “statement of something to be true including associated conditions and limitations.” Here, the “something” is the “value of the variables for the property.”

7.10.1 Relevant activities and tasks

Activities from 15288	Activities from 12207	
Requirements Analysis	**System Requirements Analysis**	**Software Requirements Analysis**
6.4.2.3 a) Define system requirements. 1) Define the functional boundary of the system in terms of the behaviour and properties to be provided. 2) Define each function that the system is required to perform. 3) Define necessary implementation constraints that are introduced by stakeholder requirements or are unavoidable solution limitations. 4) Define technical and quality in use measures that enable the assessment of technical achievement. 5) Specify system requirements and functions, as justified by risk identification or criticality of the system, that relate to critical qualities, such as health, safety, security, reliability, availability and supportability.	6.4.2.3.1 Requirements specification. 6.4.2.3.1.1 The specific intended use of the system to be developed shall be analyzed to specify system requirements. The system requirements specification shall describe: functions and capabilities of the system; business, organizational and user requirements; safety, security, human-factors engineering (ergonomics), interface, operations, and maintenance requirements; design constraints and qualification requirements. The system requirements specification shall be documented.	7.1.2.3.1 Software requirements analysis. 7.1.2.3.1.1 The implementer shall establish and document software requirements (including the quality characteristics specifications) described below. a) Functional and capability specifications, including performance, physical characteristics, and environmental conditions under which the software item is to perform. b) Interfaces external to the software item. c) Qualification requirements. d) Safety specifications, including those related to methods of operation and maintenance, environmental influences, and personnel injury. e) Security specifications, including those related to compromise of sensitive information. f) Human-factors engineering (ergonomics) specifications, including those related to manual operations, human-equipment interactions, constraints on personnel, and areas needing concentrated human attention, that are sensitive to human errors and training. g) Data definition and database requirements. h) Installation and acceptance requirements of the delivered software product at the operation and maintenance site(s). i) User documentation requirements. j) User operation and execution requirements. k) User maintenance requirements.

7.10.2 Assurance guidance and recommendations

System requirements definition is conducted to define the values for the variables for the critical properties chosen out of the collected stakeholder requirements in the Stakeholder Requirements Definition process. The functional boundary of the system related to the critical properties, the functions related to the critical properties, and the implementation constraints related to the critical properties should be explicitly specified. Among the measures defined, those measures related to the values of the variables of the critical properties should be explicitly specified, and system requirements related to the critical properties should be explicitly specified in terms of values for variables pertaining to those critical properties. Moreover, the priority among the system requirements related to the critical properties should be defined and the traceability maintained to the stakeholder requirements.

EXAMPLE If functional safety is chosen as the critical property, the part of system requirements required to be specified in this process view would be “safety lifecycle requirements,” as described in IEC 61508-1.

The constraints for the system environment required to achieve and show achievement of claims are identified by performing analysis of risks or consequences. This analysis is facilitated by capturing the following information for each claim:

a) Allowable risks associated with the system not achieving this claim.

b) Allowed values of variables related to important claims.

c) Allowable degree of uncertainty related to the claim and its achievement.

d) Applicable conditions related to the claim.

Before completing requirements analysis, the project should review the system requirements related to the critical properties to determine whether they are consistent with stakeholder requirements and whether they have adequately captured those critical properties whose violation has severe consequences and in whose achievement stakeholders require high confidence. The ultimate set of claims to be achieved and shown to be achieved can then be selected and validated. The project should document the selected set of assurance claims and their relationships to stakeholder and system requirements that justify them.

The project should provide a framework to validate that the requirements define a system that does what it is intended to do and nothing else in its transition, operational, and disposal environments.

The system requirements must be unambiguous and well examined; an unexamined ambiguous set of requirements tends to result in cost increase, schedule slippage, and lower quality of the system.

7.11 Verification process

For the systems assurance process view, the Verification Process (ISO/IEC 15288:2008, 6.4.6) confirms that the specified design requirements are fulfilled by the system. This process provides the information required to effect the remedial actions that correct non-conformances in the realized system or the processes that act on it. The Software Verification Process (ISO/IEC 12207:2008, 7.2.4) confirms that each software work product and/or service of a process or project properly reflects the specified requirements. For assurance, the project should make a verification plan that is consistent with the strategy for achieving and showing the achievement of the assurance claims.

7.11.1 Relevant activities and tasks

Activities from 15288	Activities from 12207
Verification	**Software Verification**
6.4.6.3 a) Plan verification. 1) Define the strategy for verifying the system entities throughout the life cycle.) 2) Define a verification plan based on system requirements. 3) Potential constraints on design decisions are identified and communicated. NOTE This includes practical limitations of accuracy, uncertainty, repeatability that are imposed by the verification enabling systems, the associated measurement methods, the need for system integration, and the availability, accessibility and interconnection with enabling systems.	7.2.4.3.1 Process Implementation. 7.2.4.3.1.1 A determination shall be made if the project warrants a verification effort and the degree of organizational independence of that effort needed. The project requirements shall be analyzed for criticality. Criticality may be gauged in terms of: a) The potential of an undetected error in a system or software requirement for causing death or personal injury, mission failure, or financial or catastrophic equipment loss or damage; b) The maturity of and risks associated with the software technology to be used; 7.2.4.3.1.5 Based upon the verification tasks as determined, a verification plan shall be developed and documented. The plan shall address the life cycle activities and software products subject to verification, the required verification tasks for each life cycle activity and software product, and related resources, responsibilities, and schedule. The plan shall address procedures for forwarding verification reports to the acquirer and other involved organizations.

7.11.2 Assurance guidance and recommendations

The project should conduct verification planning to be consistent with assurance-claim-related plans including the planned approach to showing achievement of the claims for the critical properties. This includes identifying verification and measurement criteria used in the approach to showing achievement of claims and establishing criteria for how assurance-claim-related problems should be resolved and reflected in the body of information assuring claims. Once values for assurance-related uncertainties are established, the verification plans, activities, and decisions should ensure meeting these uncertainty requirements. For example, the project should consider the contribution of tool reliability to the uncertainty of achieving the result.

7.12 Operation process

The Operation Process (ISO/IEC 15288, 6.4.9) uses the system in order to deliver its services. The Software Operation process (ISO/IEC 12207, 6.4.9) operates the software product in its intended environment and provides support to the customers of the software product. For assurance, plans for this process should consider achievement of the critical properties throughout the life of the system.

7.12.1 Relevant Activities and Tasks

Activities from 15288	Activities from 12207
Operation	**Software Operation**
6.4.9.3 a) Prepare for operation. 1) Prepare a strategy for operation.	6.4.9.3.1 Preparation for operation. This activity consists of the following tasks: 6.4.9.3.1.1 The operator shall develop a plan and set operational standards for performing the activities and tasks of this process. The plan shall be documented and executed.

7.12.2 Assurance guidance and recommendations

The project should plan that the operation of the system conforms to operational restrictions and is consistent with the assumptions from the approach to showing achievement of the assurance claims. The plan should ensure that violations of these restrictions are reported, recorded, and resolved and contain training information on how to establish and maintain compliance with assurance-claim-related restrictions. The plan should include how to modify the approach to showing achievement of claims and the related body of information to reflect changes in operational conditions not encompassed in the claims.

The plan should provide for assessment of the effects of changes in the system or its operational environment on the assurance-claim-related usability of the system and on the validity of the assumptions necessary for showing achievement of the claims. The plan should provide for regular audits of operation records to verify that there is no evidence that the system or the achievement and showing achievement of claims have been unknowingly subverted. The plan should ensure that adequate measures exist to prevent loss of sensitive information or harm if the control of the system is lost or transferred.

The project should establish reporting systems and procedures for investigation and disposition of assurance-claims-related incidents such as attempted violations and violations of claims, product vulnerabilities or weakness that might contribute to violations; and new sources of danger potentially resulting in claim violation /throughout the life of the system. Appropriate safeguards should be put in place for required confidentiality when communicating the plan and reporting the incidents.

7.13 Maintenance process

The Maintenance process (ISO/IEC 15288, 6.4.10) sustains the capability of the system to provide a service. The Software Maintenance process (ISO/IEC 12207, 6.4.10) provides cost-effective support to a delivered software product. For assurance, plans for this process should consider achievement of the critical properties throughout the life of the system.

7.13.1 Relevant activities and tasks

Activities from 15288	Activities from 12207
Maintenance	**Software Maintenance**
a) Plan maintenance: 1) Prepare a maintenance strategy.	6.4.10.3.1 Process implementation. 6.4.10.3.1.1 The maintainer shall develop, document, and execute plans and procedures for conducting the activities and tasks of the Software Maintenance Process.

7.13.2 Assurance guidance and recommendations

The project should ensure that the maintenance plan provides for evaluating the effect on assurance-claim-related information of changes made to the system or system elements during system maintenance. The plan should include resources for updating the approach to showing the achievement of claims and the related body of information as required, including new evidence. The plan should include provision for the controlled update and release of assurance=claim=related artefacts. The plan should include assessment of the effects of changes in the system or its operational environment on the assurance-claim-related usability of the system. This assessment should include ongoing measurement of the critical properties when maintenance changes are made.

NOTE 1 All proposed product changes should undergo claims-related effects analyses. Approved changes that have an effect on achieving and showing achievement of claims should be returned to the appropriate phase of the life cycle and all subsequent phases repeated for the changes. Information with claims-related implications should be disseminated widely and should be clear, concise, and easy to read. Information can be disseminated by means of formal reports to management and by safety newsletters, bulletins, and training for all staff.

NOTE 2 The maintenance plan should include provisions to ensure the critical properties of the systems are not compromised throughout the lifecycle as a result of replacement, retired, or disposed parts or components of the system.

The plan should have provisions for informing the risk management strategy of claim-related risk information and guidance related to modifications, workarounds, and other maintenance-related risks. A risk assessment or claim-related effects analysis of these changes should be performed in order to ensure that the achievement of claims, the approach to showing the achievement of claims and the related body of information can be maintained.

NOTE All proposed product changes, including changes to non-assurance-claims-related requirements, design, and components, should undergo assurance-claims-related impact analyses.

Bibliography

For additional guidance in assurance-related fields, the users of this part of ISO/IEC 15026 are encouraged to consult the extensive bibliography in ISO/IEC TR 15026-1. The bibliography here focuses on process standards.

[1] ISO/IEC 90003:2004, *Software engineering — Guidelines for the application of ISO 9001:2000 to computer software*

[2] ISO/IEC 15026-2:2011, *System and software engineering — System and software assurance — Part 2: Assurance case*

[3] Software and Systems Engineering Vocabulary (sevocab). Available at: www.computer.org/sevocab/

[4] ISO/IEC 15289:2011, *System and software engineering — Content of life cycle information products (documentation)*

[5] ISO/IEC 15504-1:2004, *Information Technology — Process Assessment— Par 1: Concepts and vocabulary*

[6] ISO/IEC 15504-2:2003, *Information Technology — Process Assessment — Part 2: Performing an Assessment*

[7] ISO/IEC 15504-3:2004, *Information Technology — Process Assessment — Part 3: Guidance on performing a process improvement and process capability determination*

[8] ISO/IEC 15504-5:2012, *Information Technology — Process Assessment — Part 5: An exemplar software process assessment model*

[9] ISO/IEC TR 15504-6:2008, *Information Technology — Process Assessment — Part 6: An exemplar system life cycle process assessment model*

[10] ISO/IEC 15504-7:2008, *Information Technology — Process Assessment — Part 7: Assessment of organizational maturity*

[11] ISO/IEC 15939:2007, *Systems and software engineering — Measurement process*

[12] ISO/IEC 16085:2006, *Systems and software engineering — Life cycle processes — Risk management*

[13] ISO/IEC 16326:2009, *System and Software engineering — Life cycle Processes — Project management*

[14] ISO/IEC 21827:2008, Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)

[15] ISO/IEC TR 24748-1:2010, *Systems and software engineering — Life cycle management — Part 1: Guide for life cycle management*

[16] ISO/IEC TR 24748-2:2011, *Systems and software engineering — Life cycle management — Part 2: Guide for the application of ISO/IEC 15288 (System life cycle processes)*

[17] ISO/IEC TR 24748-3:2011, *Systems and software engineering — Life cycle management — Part 3: Guide for the application of ISO/IEC 12207 (Software life cycle processes)*

[18] ISO/IEC 25000:2005, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE*

[19] ISO/IEC 25010:2011, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*

[20] ISO/IEC 25012:2008, Software Engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Data Quality Model

[21] ISO/IEC 25020:2007, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Measurement reference model and guide*

[22] ISO/IEC 25030:2007, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Quality requirements*

[23] ISO/IEC 25040:2011, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process*

[24] ISO/IEC 25051:200, *Software engineering — Software product Quality Requirements and Evaluation (SQuaRE) — Requirements for quality of Commercial Off-The-Shelf (COTS) software product and instructions for testing*

[25] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[26] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[27] ISO/IEC 29148:2011, *Systems and software engineering — Requirements engineering*

ICS 35.080
Price based on 24 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™