INTERNATIONAL STANDARD

ISO/IEC 29110-3-2

First edition
2018-04

Systems and software engineering — Lifecycle profiles for Very Small Entities (VSEs) —

Part 3-2: Conformity certification scheme

Ingénierie des systèmes et du logiciel — Profils de cycle de vie pour très petits organismes (TPO) —

Partie 3-2: Programme de certification de la conformité

Reference number
ISO/IEC 29110-3-2:2018(E)

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

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

A list of all parts in the ISO/IEC 29110 series can be found on the ISO website.

Introduction

Very Small Entities (VSEs) around the world are creating valuable products and services. For the purpose of ISO/IEC 29110, a Very Small Entity (VSE) is an enterprise, an organization, a department or a project having up to 25 people. Since many VSEs develop and/or maintain system elements and software components used in systems, or sold to be used by others, a recognition of VSEs as suppliers of high quality products is required.

According to the Organization for Economic Co-operation and Development (OECD) SME and Entrepreneurship Outlook report (2005) 'Small and Medium Enterprises (SMEs), i.e. Enterprises which employ fewer than 250 persons, constitute the dominant form of business organization in all countries world-wide, accounting for over 95 % and up to 99 % of the business population depending on country'. The challenge facing OECD governments is to provide a business environment that supports the competitiveness of this large heterogeneous business population and that promotes a vibrant entrepreneurial culture.

From studies and surveys conducted, it is clear that the majority of International Standards do not address the needs of VSEs. Implementation of and conformance with these standards is difficult, if not impossible. Subsequently VSEs have no, or very limited, ways to be recognized as entities that produce quality systems/system elements including software in their domain. Therefore, VSEs are often cut off from some economic activities.

It has been found that VSEs find it difficult to relate International Standards to their business needs and to justify the application of standards to their business practices. Most VSEs can neither afford the resources, in terms of number of employees, expertise, budget and time, nor do they see a net benefit in establishing systems or software lifecycle processes. To rectify some of these difficulties, a set of guidelines has been developed according to a set of VSE characteristics. The guidelines are based on subsets of appropriate standards processes, activities, tasks, and outcomes, referred to as Profiles. The purpose of a profile is to define a subset of International Standards relevant to the VSEs' context; for example, processes, activities, tasks, and outcomes of ISO/IEC/IEEE 12207 for software; and processes, activities, tasks, and outcomes of ISO/IEC/IEEE 15288 for systems; and information products (documentation) of ISO/IEC/IEEE 15289 for software and systems.

VSEs can achieve recognition through implementing a profile and by being audited against ISO/IEC 29110 specifications.

ISO/IEC 29110 series of standards and technical reports can be applied at any phase of system or software development within a lifecycle. This series of standards and technical reports is intended to be used by VSEs that do not have experience or expertise in adapting/tailoring ISO/IEC/IEEE 12207 or ISO/IEC/IEEE 15288 to the needs of a specific project. VSEs that have expertise in adapting/tailoring ISO/IEC/IEEE 12207 or ISO/IEC/IEEE 15288 are encouraged to use those standards instead of ISO/IEC 29110.

ISO/IEC 29110 is intended to be used with any lifecycles such as: waterfall, iterative, incremental, evolutionary or agile.

Systems in the context of ISO/IEC 29110, are typically composed of hardware and software components.

The ISO/IEC 29110 series, targeted by audience, has been developed to improve system or software and/or service quality, and process performance. See Table 1.

Table 1 — ISO/IEC 29110 target audience

ISO/IEC 29110	Title	Target audience
ISO/IEC 29110-1	Overview	VSEs and their customers, assessors, standards producers, tool vendors and methodology vendors.
ISO/IEC 29110-2	Framework for profile preparation	Profile producers, tool vendors and methodology vendors. Not intended for VSEs.
ISO/IEC 29110-3	Certification and assessment guidance	VSEs and their customers, assessors, accreditation bodies.
ISO/IEC 29110-4	Profile specifications	VSEs, customers, standards producers, tool vendors and methodology vendors.
ISO/IEC 29110-5	Management, engineering and service delivery guidelines	VSEs and their customers.

If a new profile is needed, ISO/IEC 29110-4 and ISO/IEC/TR 29110-5 can be developed without impacting existing documents.

ISO/IEC TR 29110-1[5] defines the terms common to the ISO/IEC 29110 series. It introduces processes, lifecycle and standardization concepts, the taxonomy (catalogue) of ISO/IEC 29110 profiles and the ISO/IEC 29110 series. It also introduces the characteristics and needs of a VSE and clarifies the rationale for specific profiles, documents, standards and guidelines.

ISO/IEC 29110-2 introduces the concepts for systems and software engineering profiles for VSEs. It establishes the logic behind the definition and application of profiles. For standardized profiles, it specifies the elements common to all profiles (structure, requirements, conformance, and assessment). For domain-specific profiles (profiles that are not standardized and developed outside of the ISO process), it provides general guidance adapted from the definition of standardized profiles.

ISO/IEC 29110-3 defines certification schemes, assessment guidelines and compliance requirements for process capability assessment, conformity assessments, and self-assessments for process improvements. ISO/IEC 29110-3 also contains information that can be useful to developers of certification and assessment methods and developers of certification and assessment tools. ISO/IEC 29110-3 is addressed to people who have direct involvement with the assessment process, e.g. the auditor, certification and accreditation bodies and the sponsor of the audit, who need guidance on ensuring that the requirements for performing an audit have been met.

ISO/IEC 29110-4-m provides the specification for all profiles in one profile group (a profile group may contain a single profile or multiple profiles). A profile is specified in terms of requirements imported from appropriate base standards.

ISO/IEC TR 29110-5-m provides management, engineering and service delivery guidelines for the profiles in a profile group.

This document defines the process certification scheme, assessment guidelines and compliance requirements needed to meet the purpose of the defined Profiles.

Figure 1 describes the ISO/IEC 29110 International Standards (IS) and Technical Reports (TR) and positions the parts within the framework of reference. Overview, assessment guidelines, management and engineering guidelines are available from ISO as freely available Technical Reports (TR). The Framework document, profile specifications and certification schemes are published as International Standards (IS).

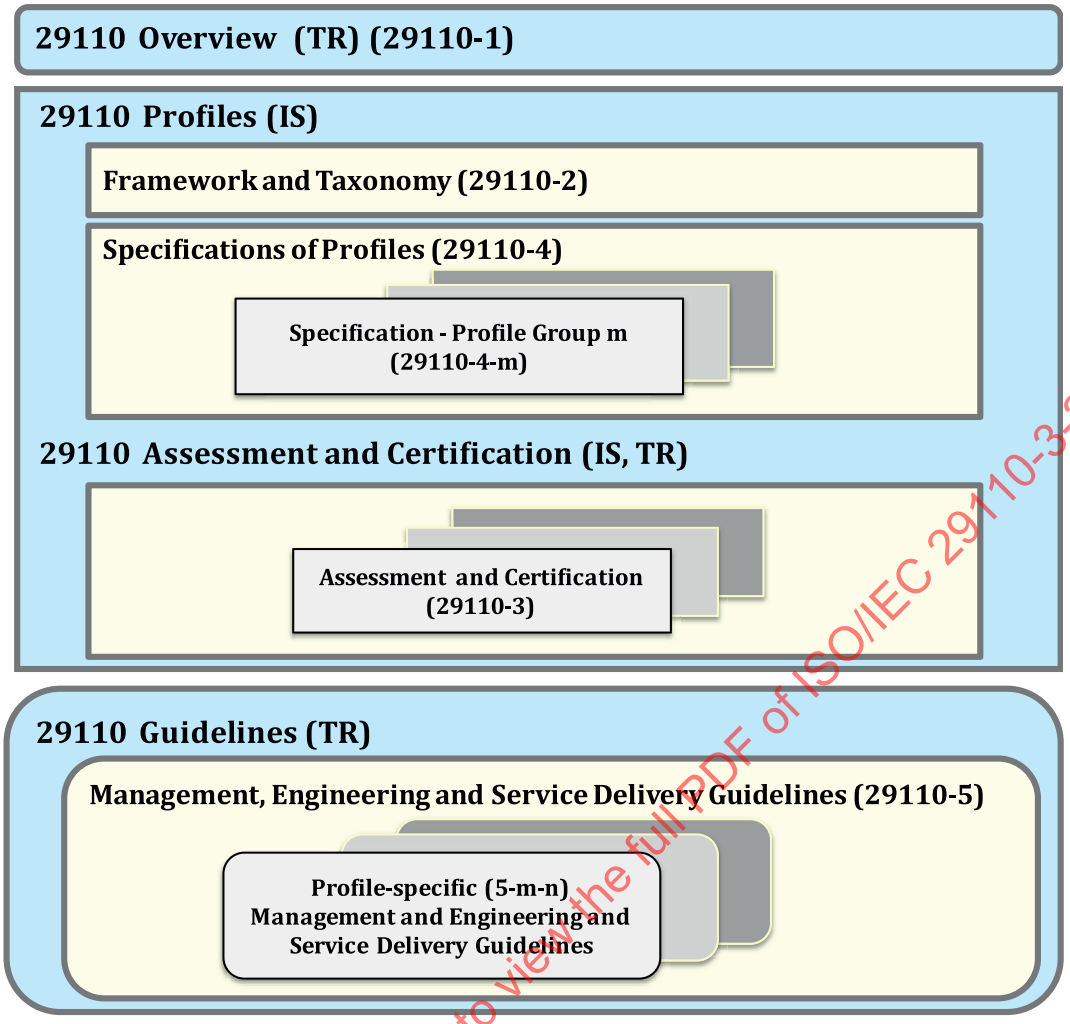

Figure 1 — ISO/IEC 29110 series

Systems and software engineering — Lifecycle profiles for Very Small Entities (VSEs) —

Part 3-2: Conformity certification scheme

1 Scope

This document:

— defines the rules applicable for certification of the implementation of systems engineering, software engineering and service delivery processes complying with the requirements given in ISO/IEC 29110-4-m, Profile specifications; and

— provides the necessary information and confidence to customers about the way certification of their suppliers has been granted.

Certification of the implementation of systems and software engineering processes (named "certification" in this document) is a third-party conformity assessment activity (see ISO/IEC 17000:2004, 5.5). Bodies performing this activity are therefore third-party conformity assessment bodies (named "certification body/bodies" in this document).

NOTE This document is primarily intended to be used as a criteria document for the accreditation or peer assessment of certification bodies which seek to be recognized as being competent to certify that a Very Small Entity (VSE) complies with ISO/IEC 29110-4-m, Profile Specifications. Some of its requirements could also be found useful by any other parties involved in the conformity assessment of such certification bodies.

Systems and software engineering processes certification does not attest the fitness of the systems and or software products offered by a VSE.

It is important to note that certification of the implementation of systems and software engineering processes according to ISO/IEC 29110-4-m, Profile Specifications, is a process certification and not a management systems certification neither a product certification.

Certification of the implementation of systems and software engineering processes (SEP) of a very small entity (VSE) is one means of providing assurance that the VSE has implemented systems and software engineering processes to the development or maintenance of systems and or software.

Requirements for the implementation of SEP can originate from a number of sources, and this International Standard has been developed to assist in the certification of SEP that fulfil the requirements of ISO/IEC 29110-4-m, Profile Specifications. The contents of this document can also be used to support certification of SEP that are based on other sets of specified SEP requirements.

This document is intended for use by bodies that carry out audit and certification of SEP for VSEs. It gives generic requirements for such certification bodies performing audit and certification in the field of SEP for VSEs. Such bodies are referred to as certification bodies. This wording is not intended to be an obstacle to the use of this document by bodies with other designations that undertake activities covered by the scope of this document. Indeed, this document is intended to be usable by anyone involved in the assessment of SEP for VSEs.

Certification activities involve the audit of a VSE's SEP. The form of attestation of conformity of a VSE's SEP to a specific lifecycle profile standard setting the applicable SEP (for example ISO/IEC 29110-4-1 or ISO/IEC 29110-4-3) or other specified requirements are normally a certification document or a certificate.

This certification is outside the scope of ISO/IEC 29169 to the assessment to process quality characteristics and organizational maturity, and does not cover the results of process assessment. ISO/IEC 29110-3-3 describes such a scheme.

It is for the VSE being certified to develop its own processes (including ISO/IEC 29110-4-m SEP), other sets of specified SEP requirements, other processes and it is for the VSE to decide how the various components of these will be arranged. It is therefore for certification bodies that operate in accordance with this document to take into account the culture and practices of their clients with respect to the implementation of SEP, including, if applicable, within the wider organization.

2 Normative references

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

ISO/IEC 29110-2-1, *Software engineering — Lifecycle profiles for Very Small Entities (VSEs) — Part 2-1: Framework and taxonomy*

ISO/IEC 17000, *Conformity assessment — Vocabulary and general principles*

ISO/IEC 17065:2012, *Conformity assessment — Requirements for bodies certifying products, processes and services*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 29110-2-1, ISO/IEC 17000, ISO/IEC 17065:2012 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

3.1
certification body
third-party conformity assessment body operating certification schemes

Note 1 to entry: A certification body can be non-governmental or governmental (with or without regulatory authority).

[SOURCE: ISO/IEC 17065:2012]

3.2
client
<for certification> organization that is responsible to a certification body for ensuring certification requirements, including product requirements are fulfilled

[SOURCE: ISO/IEC 17065:2012, modified — Definition editorially revised and Note 1 to entry removed.]

4 Symbols and abbreviated terms

4.1 Abbreviated Terms

The following abbreviations are used in this document:

SEP Systems and Software Engineering Process

VSE Very Small Entity

5 General requirements

5.1 General

All the requirements given in ISO/IEC 17065:2012, Clause 4 apply.

5.2 Management of impartiality

The certification body and any part of the same legal entity shall not offer or provide systems and software engineering processes consultancy.

The fact that the organization employing the auditor is known to have provided systems and software engineering processes consultancy to the VSE, within two years following the end of the consultancy, is likely to be considered as a high threat to impartiality.

6 Structural requirements

All the requirements given in of ISO/IEC 17065:2012, Clause 5 apply.

7 Resource requirements

7.1 Certification body personnel

7.1.1 General

All the requirements given in ISO/IEC 17065:2012, 6.1, apply.

Additionally, the certification body shall have processes to ensure that personnel have appropriate knowledge relevant to the market in which it operates.

7.1.2 Management of competence for personnel involved in the certification process

All the requirements given in ISO/IEC 17065:2012, 6.1.2, apply.

7.1.3 Contract with the personnel

All the requirements given in of ISO/IEC 17065:2012, 6.1.3, apply.

7.1.4 Personal attributes

The certification body shall ensure that all personnel involved in the certification activities possess the following personal attributes. The personnel shall be:

a) ethical, i.e. fair, truthful, sincere, honest and discreet;

b) open-minded, i.e. willing to consider alternative ideas or points of view;

c) diplomatic, i.e. tactful in dealing with people;

d) observant, i.e. actively observing physical surroundings and activities;

e) perceptive, i.e. aware of and able to understand situations;

f) versatile, i.e. able to readily adapt to different situations;

g) tenacious, i.e. persistent and focused on achieving objectives;

h) decisive, i.e. able to reach timely conclusions based on logical reasoning and analysis;

i) self-reliant, i.e. able to act and function independently whilst interacting effectively with others;

j) acting with fortitude, i.e. able to act responsibly and ethically, even though these actions may not always be popular and may sometimes result in disagreement or confrontation; and

k) open to improvement, i.e. willing to learn from situations, and striving for better audit results.

7.1.5 Generic SEP competence requirements

7.1.5.1 General considerations

The certification body shall have processes to ensure that personnel have appropriate knowledge relevant to SEP.

It shall determine the competence required for each technical area (as relevant for the specific certification scheme) and for each function in the certification activity.

It shall determine the means for the demonstration of competence prior to carrying out specific functions.

7.1.5.2 Personnel carrying out contract review

The certification body shall ensure that personnel carrying out contract review demonstrate the ability to apply knowledge and skills in the following areas:

a) assessment of applicant products, processes and practices;

b) deployment of systems and software engineering processes for VSEs auditor competences and requirements;

c) determination of audit time and duration requirements; and

d) certification body's policies and procedures related to contract review.

7.1.6 Competence requirements for Personnel granting certification

7.1.6.1 General

The certification body shall ensure that the personnel who take the decision on granting certification have the same education, systems and software engineering processes training, audit training and work experience as required for an auditor in one category.

7.1.6.2 Competences

The certification body shall ensure that personnel granting certification demonstrate the ability to apply knowledge and skills in the following areas:

a) systems and software engineering processes standards or other documents used as audit criteria;

b) the application of systems and software engineering processes standards;

c) implementation of systems and software engineering processes and the ability to assess the effectiveness of their implementation;

d) corrections and corrective actions to be taken with regards to systems and software engineering processes;

e) laws and regulations relevant to systems and software engineering processes, in order to be able to conduct an effective audit;

f) systems and software products, processes and practices;

g) relevant systems and software engineering processes requirements;

h) relevant standards;

i) assessment and review of an audit report for accuracy and completeness relevant systems and software engineering processes requirements;

j) assessment and review of the effectiveness of corrective actions; and

k) the certification process.

7.1.7 Competence requirements for SEP auditors

7.1.7.1 General

All the requirements given in ISO 19011:2011, 5.4.7 c) apply.

The competences of auditors shall be recorded. The certification body shall provide evidence of a successful evaluation of SEP auditors.

The certification body shall ensure that auditors demonstrate the ability to apply knowledge and skills in the following areas.

7.1.7.2 Work experience

The certification body shall ensure that the auditor has relevant work experience in the systems and software industry, including in systems and software development life cycle processes functions, within systems and software development or maintenance, inspection or enforcement, or the equivalent.

7.1.7.3 Audit experience

The certification body shall ensure that the auditor has performed systems and software engineering processes audits in organizations under the leadership of a qualified auditor.

For maintaining the qualification of the auditor, the certification body shall ensure that auditors have all the necessary competences updated.

7.1.7.4 Audit principles, procedures and techniques

To enable the auditor to apply the principles, procedures and techniques as appropriate to different audits and to ensure that audits are conducted in a consistent and systematic manner, an auditor shall be able to:

a) apply audit principles, procedures and techniques;

b) plan and organize the work effectively;

c) conduct the audit within the agreed time schedule;

d) prioritize and focus on matters of significance;

e) collect information through effective interviewing, listening, observing and reviewing documents, records and data;

f) understand the appropriateness and consequences of using sampling techniques for auditing;

g) verify the accuracy of collected information;

h) use work documents to record audit activities;

i) confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;

j) assess those factors that can affect the reliability of the audit findings and conclusions;

k) prepare audit reports;

l) maintain the confidentiality and security of information; and

m) communicate effectively, either through personal linguistic skills or through an interpreter.

7.1.7.5 Systems and software engineering standards for VSE and normative documents

Personal involved in VSE SEP auditing shall have knowledge of:

a) relevant standards of 29110 family;

b) 29110 normative documents used in SEP and their application; and

d) 29110-4-m requirements and their application.

7.1.7.6 Systems and software engineering processes and reference documents

To enable the auditor to comprehend the scope of the audit and apply audit criteria, knowledge and skills in this area shall cover:

a) the application of systems and software engineering processes in the development and maintenance of systems and software in different organizations;

b) interaction between the components of systems and software engineering processes;

c) systems and software engineering processes standards, applicable procedures or other documents used as audit criteria;

d) recognizing differences between, and the priority of, the reference documents;

e) application of the reference documents to different audit situations; and

f) information systems and technology for authorization, security, distribution and control of documents, data and records.

7.1.7.7 Organizational situations

To enable the auditor to comprehend the organization's operational context, knowledge and skills in this area shall cover:

a) organizational size, structure, functions and relationships;

b) general business processes and related terminology;

c) cultural and social customs of the auditee; and

d) the VSE SEP characteristics and context.

7.1.7.8 Applicable laws, regulations and other requirements relevant to the discipline

To enable the auditor to work within, and be aware of, the requirements that apply to the organization being audited, knowledge and skills in this area shall cover:

a) local, regional and national codes, laws and regulations;

a) contracts and agreements; and

b) other requirements to which the organization subscribes.

7.1.7.9 Terminology, knowledge and skills in the following systems and software engineering processes

The certification body shall ensure that auditors demonstrate the ability to apply terminology, knowledge and skills in the following systems and software engineering processes:

a) methodologies used for implementation and management of systems and software engineering processes and the ability to assess the effectiveness of this processes;

b) corrections and corrective actions to be taken with regards to systems and software engineering processes;

c) laws and regulations relevant to the deliver and maintenance of systems and/or software in order to be able to conduct an effective audit;

d) systems and/or software products, processes and practices of the sector;

e) relevant systems and software engineering processes requirements; and

f) relevant systems and software engineering processes standards.

NOTE It is not necessary for each individual to have the same competence, however the collective competence of the group needs be sufficient to achieve the objective of these functions.

7.1.7.10 Selection of the audit team

The certification body shall ensure that the systems and software engineering processes audit team have competences in the application of systems and software engineering processes required by the audit.

7.2 Resources for evaluation

All the requirements given in ISO/IEC 17065:2012, 6.2 apply.

8 Process requirements

8.1 General

All the requirements given in ISO/IEC 17065:2012, 7.1 apply.

8.2 Application

The certification body shall obtain all the necessary information to complete the certification process in accordance with the relevant certification scheme.

NOTE 1 The following are examples of necessary information:

— the product(s) developed using the systems and software engineering processes;

— the standards and/or other normative documents for which the client is seeking certification (see 7.1.2);

— the general features of the client, including its name and the address(es) of its physical location(s), significant aspects of its process and operations (if required by the relevant certification scheme), and any relevant legal obligations;

— general information concerning the client, relevant to the field of certification for which the application is made, such as the client's activities, its human and technical resources and its functions and relationship in a larger corporation, if any;

— information concerning all outsourced processes used by the client that will affect conformity to requirements; if the client has identified a legal entity/entities for delivering or developing parts of the systems and/or software that is different from the client, then the certification body can establish appropriate contractual controls over the legal entity/entities concerned, if necessary for effective surveillance; if such contractual controls are needed, they can be established prior to providing formal certification documentation (see 8.7); and

— all other information needed in accordance with the relevant certification requirements, such as information for initial evaluation and surveillance activities, e.g. the locations where the systems and/or software is developed or maintained and contact personnel at these locations.

NOTE 2 A variety of media and mechanisms can be used to collect this information at various times, including an application form. Such information gathering can be in conjunction with, or separate from, the completion of the legally binding agreement (the certification agreement) specified in ISO/IEC 17065:2012, 4.1.2.

NOTE 3 Application for an extension of the certification scope could involve similar products, different locations, etc.

8.3 Application review

All the requirements given in ISO/IEC 17065:2012, 7.3 apply.

8.4 Evaluation

8.4.1 Evaluation Plan

The evaluation plan shall be developed to clearly identify the audit activity(ies) required to demonstrate that the client's systems and software engineering processes fulfils the requirements for certification to the selected standard(s) within the ISO/IEC 29110-4-m series or other normative document(s).

The evaluation plan shall include a two-stage initial audit, surveillance audits in the first and second years, and a recertification audit in the third year prior to expiration of certification. The three-year certification cycle begins with the certification or recertification decision. The determination of the evaluation plan and any subsequent adjustments shall consider the size of the client organization, the scope and complexity of its systems and software engineering processes and products as well as demonstrated level of software engineering processes effectiveness and the results of any previous audits.

NOTE Annex A lists additional items that can be considered when developing or revising an audit programme.

Where a certification body is taking account of certification or other audits already granted to the client, it shall collect sufficient, verifiable information to justify and record any adjustments to the audit programme.

8.4.2 Audit plan

8.4.2.1 General

The certification body shall ensure that an audit plan is established for each audit identified in the evaluation plan to provide the basis for agreement regarding the conduct and scheduling of the audit activities. This audit plan shall be based on documented requirements of the certification body.

8.4.2.2 Determining audit objectives, scope and criteria

The audit objectives shall be determined by the certification body according to the requirements of applicable ISO/IEC 29110-4-m series. The audit scope and criteria, including any changes, shall be established by the certification body after discussion with the client.

The audit objectives shall describe what is to be accomplished by the audit and shall include the following:

a) determination of the conformity of the client's systems and software engineering processes with audit criteria;

b) evaluation of the ability of the systems and software engineering processes to ensure the client organization meets applicable contractual requirements; and

NOTE 1 A systems and software engineering processes certification audit is not a legal compliance audit.

c) as applicable, identification of areas for potential improvement of the systems and software engineering processes.

The audit scope shall describe the extent and boundaries of the audit, such as physical locations, organizational units, activities and processes to be audited. Where the initial or re-certification process consists of more than one audit (e.g. covering different locations), the scope of an individual audit may not cover the full certification scope, but the totality of audits shall be consistent with the scope in the certification document.

NOTE 2 Annex A lists additional items that can be considered when preparing or revising the audit scope.

The audit criteria shall be used as a reference against which conformity is determined, and shall include:

— the requirements of ISO/IEC 29110-4-m standard or a defined normative document on systems and software engineering processes; and

— the defined processes and documentation of the systems and software engineering processes developed by the client.

8.4.2.3 Preparing the audit plan

The audit plan shall be appropriate to the objectives and the scope of the audit. The audit plan shall at least include or refer to the following:

a) the audit objectives;

b) the audit criteria;

c) the audit scope, including identification of the organizational and functional units or processes to be audited;

d) the dates and sites where the on-site audit activities are to be conducted, including visits to temporary sites, as appropriate;

e) the expected time and duration of on-site audit activities; and

f) the roles and responsibilities of the audit team members and accompanying persons.

NOTE 1 The audit plan information can be contained in more than one document.

NOTE 2 Annex A lists additional items that can be considered when preparing or revising the audit plan.

8.4.3 Audit team selection and assignments

The certification body shall have a process for selecting and appointing the audit team, including the audit team leader, taking into account the competence needed to achieve the objectives of the audit. If there is only one auditor, the auditor shall have the competence to perform the duties of an audit team leader applicable for that audit.

In deciding the size and composition of the audit team, consideration shall be given to the following:

a) audit objectives, scope, criteria and estimated time of the audit;

b) whether the audit is a combined, integrated or joint audit;

c) the overall competence of the audit team needed to achieve the objectives of the audit;

d) certification requirements;

e) language and culture; and

f) whether the members of the audit team have previously audited the client's systems and software engineering processes.

The necessary knowledge and skills of the audit team leader and auditors may be supplemented by technical experts, translators and interpreters who shall operate under the direction of an auditor. Where translators or interpreters are used, they are to be selected such that they do not unduly influence the audit.

NOTE The criteria for the selection of technical experts are determined on a case-by-case basis by the needs of the audit team and the scope of the audit.

Auditors-in-training may be included in the audit team as participants, provided an auditor is appointed as an evaluator. The evaluator shall be competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training.

The audit team leader, in consultation with the audit team, shall assign to each team member responsibility for auditing specific processes, functions, sites, areas or activities. Such assignments shall take into account the need for competence, and the effective and efficient use of the audit team, as well as different roles and responsibilities of auditors, auditors-in-training and technical experts. Changes to the work assignments may be made as the audit progresses to ensure achievement of the audit objectives.

8.4.4 Determining audit time

The certification body shall have documented procedures for determining audit time, and for each client the certification body shall determine the time needed to plan and accomplish a complete and effective audit of the client's systems and software engineering processes. The audit time determined by the certification body, and the justification for the determination, shall be recorded. In determining the audit time, the certification body shall consider, among other things, the following aspects:

a) the requirements of the relevant systems and software engineering processes standard;

b) size and complexity;

c) technological context;

d) any outsourcing of any activities included in the scope of the systems and software engineering processes;

e) the results of any prior audits;

f) number of sites and multi-site considerations;

g) the risks associated with the products, processes or activities of the organization; and

h) when audits are combined, joint or integrated.

The time spent by any team member that is not assigned as an auditor (i.e. technical experts, translators, interpreters, observers and auditors-in-training) shall not count in the above established audit time.

NOTE The use of translators, interpreters can necessitate additional audit time.

8.4.5 Multi-site sampling

Where multi-site sampling is utilized for the audit of a client's systems and software engineering processes covering the same activity in various locations, the certification body shall develop a sampling programme to ensure proper audit of the systems and software engineering processes. The rationale for the sampling plan shall be documented for each client.

8.4.6 Communication of audit team tasks

The tasks given to the audit team shall be defined and shall be made known to the client organization, and shall require the audit team to:

a) examine and verify the structure, policies, processes, procedures, records and related documents of the client organization relevant to the systems and software engineering processes;

b) determine that these meet all the requirements relevant to the intended scope of certification; and

c) determine that the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the client's systems and software engineering processes.

8.4.7 Communication concerning audit team members

The certification body shall provide the name of and, when requested, make available background information on each member of the audit team, with sufficient time for the client organization to object to the appointment of any particular auditor or technical expert and for the certification body to reconstitute the team in response to any valid objection.

8.4.8 Communication of audit plan

The audit plan shall be communicated and the dates of the audit shall be agreed upon, in advance, with the client organization.

8.4.9 Conducting on-site and remote audits

8.4.9.1 General

The certification body shall have a process for conducting on-site and remote audits. This process shall include an opening meeting at the start of the audit and a closing meeting at the conclusion of the audit.

NOTE In addition to visiting physical location(s), "on-site" can include remote access to electronic site(s) that contain(s) information that is relevant to the audit of the systems and software engineering processes.

8.4.9.2 Conducting the opening meeting

A formal opening meeting, where attendance shall be recorded, shall be held with the client's management and, where appropriate, those responsible for the functions or processes to be audited. The purpose of the opening meeting, which shall usually be conducted by the audit team leader, is to provide a short explanation of how the audit activities will be undertaken and shall include the

following elements. The degree of detail shall be consistent with the familiarity of the client with the audit process:

a) introduction of the participants, including an outline of their roles;

b) confirmation of the scope of certification;

c) confirmation of the audit plan (including type and scope of audit, objectives and criteria), any changes, and other relevant arrangements with the client, such as the date and time for the closing meeting, interim meetings between the audit team and the client's management;

d) confirmation of formal communication channels between the audit team and the client;

e) confirmation that the resources and facilities needed by the audit team are available;

f) confirmation of matters relating to confidentiality;

g) confirmation of relevant work safety, emergency and security procedures for the audit team;

h) confirmation of the availability, roles and identities of any guides and observers;

i) the method of reporting, including any grading of audit findings;

j) information about the conditions under which the audit may be prematurely terminated;

k) confirmation that the audit team leader and audit team representing the certification body is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails;

l) confirmation of the status of findings of the previous review or audit, if applicable;

m) methods and procedures to be used to conduct the audit based on sampling;

n) confirmation of the language to be used during the audit;

o) confirmation that, during the audit, the client will be kept informed of audit progress and any concerns; and

p) opportunity for the client to ask questions.

8.4.9.3 Communication during the audit

The following issues shall be considered while communicating audit progress status:

a) During the audit, the audit team shall periodically assess audit progress and exchange information. The audit team leader shall reassign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the client.

b) Where the available audit evidence indicates that the audit objectives are unattainable or suggests the presence of an immediate and significant risk (e.g. safety), the audit team leader shall report this to the client and, if possible, to the certification body to determine appropriate action. Such action may include reconfirmation or modification of the audit plan, changes to the audit objectives or audit scope, or termination of the audit. The audit team leader shall report the outcome of the action taken to the certification body.

c) The audit team leader shall review with the client any need for changes to the audit scope, which becomes apparent as on-site auditing activities progress and report this to the certification body.

8.4.9.4 Observers and guides

8.4.9.5 Observers

The presence and justification of observers during an audit activity shall be agreed to by the certification body and client prior to the conduct of the audit. The audit team shall ensure that observers do not influence or interfere in the audit process or outcome of the audit.

NOTE Observers can be members of the client's organization, consultants, witnessing accreditation body personnel, regulators or other justified persons.

8.4.9.6 Guides

Each auditor shall be accompanied by a guide, unless otherwise agreed to by the audit team leader and the client. Guide(s) are assigned to the audit team to facilitate the audit. The audit team shall ensure that guides do not influence or interfere in the audit process or outcome of the audit.

NOTE The responsibilities of a guide can include:

a) establishing contacts and timing for interviews;

b) arranging visits to specific parts of the site or organization;

c) ensuring that rules concerning site safety and security procedures are known and respected by the audit team members;

d) witnessing the audit on behalf of the client; and

e) providing clarification or information as requested by an auditor.

8.4.9.7 Collecting and verifying information

During the audit, information relevant to the audit objectives, scope and criteria (including information relating to interfaces between functions, activities and processes) shall be collected by appropriate sampling and verified to become audit evidence.

Methods to collect information shall include, but are not limited to:

a) interviews;

b) observation of processes and activities; and

c) review of documentation and records.

8.4.9.8 Identifying and recording audit findings

1) Audit findings summarizing conformity and detailing nonconformity and its supporting audit evidence shall be recorded and reported to enable an informed certification decision to be made or the certification to be maintained.

2) Opportunities for improvement may be identified and recorded, unless prohibited by the requirements of a systems and software engineering processes certification scheme. Audit findings, however, which are nonconformities in accordance with 8.6.2 b) and c) shall not be recorded as opportunities for improvement.

3) A finding of nonconformity shall be recorded against a specific requirement of the audit criteria, contain a clear statement of the nonconformity and identify in detail the objective evidence on which the nonconformity is based. Nonconformities shall be discussed with the client to ensure that the evidence is accurate and that the nonconformities are understood. The auditor however shall refrain from suggesting the cause of nonconformities or their solution.

NOTE Nonconformities, consistent with the requirements of 8.6.2 b), can be classified as major, whereas other nonconformities [8.6.2 c)] can be classified as minor nonconformities.

4) The audit team leader shall attempt to resolve any diverging opinions between the audit team and the client concerning audit evidence or findings, and unresolved points shall be recorded.

8.4.9.9 Preparing audit conclusions

Prior to the closing meeting, the audit team shall:

a) review the audit findings, and any other appropriate information collected during the audit, against the audit objectives;

b) agree upon the audit conclusions, taking into account the uncertainty inherent in the audit process;

c) identify any necessary follow-up actions; and

d) confirm the appropriateness of the audit programme or identify any modification required (e.g. scope, audit time or dates, surveillance frequency, competence).

8.4.9.10 Conducting the closing meeting

A formal closing meeting, where attendance shall be recorded, shall be held with the client's management and, where appropriate, those responsible for the functions or processes audited. The purpose of the closing meeting, which shall normally be conducted by the audit team leader, is to present the audit conclusions, including the recommendation regarding certification. Any nonconformities shall be presented in such a manner that they are understood, and the timeframe for responding shall be agreed.

NOTE "Understood" does not necessarily mean that the nonconformities have been accepted by the client.

The closing meeting shall also include the following elements. The degree of detail shall be consistent with the familiarity of the client with the audit process:

a) advising the client that the audit evidence collected was based on a sample of the information; thereby introducing an element of uncertainty;

b) the method and timeframe of reporting, including any grading of audit findings;

c) the certification body's process for handling nonconformities including any consequences relating to the status of the client's certification;

d) the timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit;

e) the certification body's post audit activities; and

f) information about the complaint handling and appeal processes.

The client shall be given opportunity for questions. Any diverging opinions regarding the audit findings or conclusions between the audit team and the client shall be discussed and resolved where possible. Any diverging opinions that are not resolved shall be recorded and referred to the certification body.

8.4.9.11 Audit report

The certification body shall provide a written report for each audit. The audit team may identify opportunities for improvement but shall not recommend specific solutions. Ownership of the audit report shall be maintained by the certification body.

The audit team leader shall ensure that the audit report is prepared and shall be responsible for its content. The audit report shall provide an accurate, concise and clear record of the audit to enable an informed certification decision to be made and shall include or refer to the following:

a) identification of the certification body;

b) the name and address of the client and the client's management representative;

c) the type of audit (e.g. initial, surveillance or recertification audit);

d) the audit criteria;

e) the audit objectives;

f) the audit scope, particularly identification of the organizational or functional units or processes audited and the time of the audit;

g) identification of the audit team leader, audit team members and any accompanying persons;

h) the dates and places where the audit activities (on site or offsite) were conducted;

i) audit findings, evidence and conclusions, consistent with the requirements of the type of audit; and

j) any unresolved issues, if identified.

8.4.9.12 Cause analysis of nonconformities

The certification body shall require the client to analyse the cause and describe the specific correction and corrective actions taken, or planned to be taken, to eliminate detected nonconformities, within a defined time.

8.4.9.13 Effectiveness of corrections and corrective actions

The certification body shall review the corrections, identified causes and corrective actions submitted by the client to determine if these are acceptable. The certification body shall verify the effectiveness of any correction and corrective actions taken. The evidence obtained to support the resolution of nonconformities shall be recorded. The client shall be informed of the result of the review and verification.

NOTE Verification of effectiveness of correction and corrective action can be carried out based on a review of documentation provided by the client, or where necessary, through verification on-site.

8.4.9.14 Additional audits

The client shall be informed if an additional full audit, an additional limited audit, or documented evidence (to be confirmed during future surveillance audits) will be needed to verify effective correction and corrective actions.

8.4.10 Initial certification audit

8.4.10.1 General

The initial certification audit of systems and software engineering processes shall be conducted in two stages: stage 1 and stage 2.

8.4.10.2 Stage 1 audit

The stage 1 audit shall be performed to:

a) audit the client's systems and software engineering processes documentation;

b) evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine the preparedness for the stage 2 audit;

c) review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance or significant aspects, processes, objectives and operation of the systems and software engineering processes;

d) collect necessary information regarding the scope of the systems and software engineering processes and location(s) of the client, and related statutory and regulatory aspects and compliance (e.g. legal aspects of the client's operation, etc.);

e) review the allocation of resources for stage 2 audit and agree with the client on the details of the stage 2 audit;

f) provide a focus for planning the stage 2 audit by gaining a sufficient understanding of the client's systems and software engineering processes and site operations in the context of possible significant aspects; and

g) evaluate if the level of implementation of the systems and software engineering processes substantiates that the client is ready for the stage 2 audit.

For most systems and software engineering processes, it is recommended that at least part of the stage 1 audit be carried out at the client's premises in order to achieve the objectives stated above.

1) Stage 1 audit findings shall be documented and communicated to the client, including identification of any areas of concern that could be classified as nonconformity during the stage 2 audit.

2) In determining the interval between stage 1 and stage 2 audits, consideration shall be given to the needs of the client to resolve areas of concern identified during the stage 1 audit. The certification body may also need to revise its arrangements for stage 2.

8.4.10.3 Stage 2 audit

The purpose of the stage 2 audit is to evaluate the implementation, including effectiveness, of the client's systems and software engineering processes. The stage 2 audit shall take place at the site(s) of the client. It shall include at least the following:

a) information and evidence about conformity to all requirements of the applicable systems and software engineering processes standard or other normative document;

b) the client's systems and software engineering processes and performance as regards legal compliance; and

c) operational control of the client's processes.

8.4.11 Initial certification audit conclusions

The audit team shall analyse all information and audit evidence gathered during the stage 1 and stage 2 audits to review the audit findings and agree on the audit conclusions.

8.4.12 Personnel for evaluation

The certification body shall assign personnel to perform each evaluation task that it undertakes with its internal resources (see ISO/IEC 17065:2012, 6.2.1).

NOTE Outsourced tasks are completed by personnel usually assigned by the organization to which the task is outsourced. Such personnel are not normally assigned by the certification body.

8.4.13 Information for evaluation

The certification body shall ensure all necessary information and/or documentation is made available for performing the evaluation tasks.

8.4.14 Resources for evaluation

The certification body shall carry out the evaluation activities that it undertakes with its internal resources (see ISO/IEC 17065:2012, 6.2.1) and shall manage outsourced resources (see ISO/IEC 17065:2012, 6.2.2) in accordance with the evaluation plan (see 8.4.1). The systems and software engineering processes shall be evaluated against the requirements covered by the scope of certification and other requirements specified in the certification scheme.

8.4.15 Use of evaluations results completed prior to the application for certification

The certification body shall only rely on evaluation results related to certification completed prior to the application for certification, where it takes responsibility for the results and satisfies itself that the body that performed the evaluation fulfils the requirements contained in ISO/IEC 17065:2012, 6.2.2, and those specified by the certification scheme.

NOTE This can include work carried out under recognition agreements between certification bodies.

8.4.16 Nonconformities

The certification body shall inform the client of all nonconformities.

8.4.17 Additional evaluation tasks

If one or more nonconformities have arisen, and if the client expresses interest in continuing the certification process, the certification body shall provide information regarding the additional evaluation tasks needed to verify that nonconformities have been corrected. If the client agrees to completion of the additional evaluation tasks, the process specified in 8.4.2 shall be repeated to complete the additional evaluation tasks.

8.4.18 Results of evaluation

The results of all evaluation activities shall be documented prior to review (see 8.5).

NOTE This documentation can provide an opinion as to whether systems and software engineering processes requirements have been fulfilled.

8.5 Review

All the requirements given in ISO/IEC 17065:2012, 7.5 apply.

8.6 Certification decision

8.6.1 General

All the requirements given in ISO/IEC 17065:2012, 7.6 apply.

8.6.2 Actions prior to making a decision

The certification body shall confirm, prior to making a decision, that:

a) the information provided by the audit team is sufficient with respect to the certification requirements and the scope for certification;