For IEC use only

CAB/2034A/DC

2020-10-26

INTERNATIONAL ELECTROTECHNICAL COMMISSION

CONFORMITY ASSESSMENT BOARD (CAB) **Meeting 48, Geneva, 2020-11-09&10**

SUBJECT

Agenda item 5.1

CA in ISO/IEC FDIS 27034-4

BACKGROUND

This A version corrects and replaces the CAB document CAB/2034/DC. The number of the standard indicated (~~17034-4~~) on the cover page of the original version, was incorrect and has been corrected to 27034-4, in this A version. Since the closing date for comments has already passed there is no Action required on this A version.

Following CAB Decision 45/25 – *CA in ISO/IEC standards*, the Secretariats of ISO/TMB, IEC/SMB, ISO/CASCO and IEC/CAB, held a meeting and agreed on the procedure given in document CAB/1942/INF.

Following this new procedure, the document ISO/IEC FDIS 27034-4 (see the Annex) was detected as a document with issues.

Given the short timeframe provided in the new procedure for CAB review, a small subgroup of members of CAB was quickly assembled to review this document. Their recommendation was to stop the development of this publication.

This issue was raised with the SMB Secretariat, who also reviewed the document and agreed with the CAB subgroup recommendation.

The reply returned to CASCO was that the development of this document should stop immediately and that it was hoped that the CASCO Secretariat would give the same recommendation to TMB.

It was considered important that SMB and TMB be aligned on this issue.

ACTION

This A version simply corrects an error on the cover page of the original version. Since this A version is circulated after the closing date for comments of the original version, there is no action requested by CAB on this document.

ANNEX

ISO/IEC JTC 1/SC 27 N21038

Date: 2020-07-10

ISO/IEC FDIS 27034-4:2020(E)

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Information technology — Application security — Part 4: Validation and verification

Technologie de l'information — Sécurité des applications — Partie 4 : Validation et vérification

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.

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

For an explanation of 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 World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 27034 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 General

The ISO/IEC 27034 series proposes framework elements, including roles, processes and components that can be implemented in an organization and/or application to improve application security. Not all organizations or applications are the same and the ISO/IEC 27034 series' frameworks can be implemented in different ways to address different specific security requirements. If no guidance is provided by the ISO/IEC 27034 series' frameworks, how can application security verification and audits be performed and declared successful?

This document defines processes and elements required for managing, validating and verifying how the ISO/IEC 27034 series' frameworks were implemented to enforce application security.

Table 1 — ISO/IEC 27034 series' frameworks

Document	Scope	ISO/IEC 27034 framework	What it represents
ISO/IEC 27034-2	**Organization**	Organization normative framework (ONF)	A centralized repository of pre-approved and reusable application security elements, used as an authoritative source of information by the organization.
		ONF management process	A process to maintain and continuously improve required ONF elements to protect the organization's sensitive information involved by the use of applications.
ISO/IEC 27034-3	**Application**	Application normative framework (ANF)	A repository for all processes, application security controls (ASCs), reports and other outcomes related to an application.
		Application security management process	A risk-based process that uses the ANF to build, support and operate secure applications.
ISO/IEC 27034-4	**Organization and application**	Verification scheme framework (VSF)	Repository for processes and components used to define and perform measurable and repeatable application security verifications and audits.
		Application security validation and verification process	Group of processes and frameworks used to build, validate, verify and maintain a verification scheme and conduct application security validations, verifications, and audits based on its requirements.
ISO/IEC 27034-7	**Application security control** (ASC)	Assurance prediction framework	A set of processes and components used to define a prediction application security rationale (PASR) that replace an ASC for a specific application, and provide context for this prediction.
		Assurance prediction management process	A risk-based process to replace an ASC with a PASR in order to reduce an application's security cost and expect to maintain the same security level.

Organization-level frameworks and processes are provided by the organization normative framework (ONF). The ONF, its elements and supporting processes are defined in ISO/IEC 27034-2.

Application-level frameworks and processes are provided by ISO/IEC 27034-3. The application security management process (ASMP) helps a project team apply relevant portions of the ONF to a specific application project and formally record AS objective evidence of the processes in an ANF.

AS validation, verification and audit-level frameworks and processes are provided by ISO/IEC 27034-4. This framework helps organizations and relevant authorities to measure and verify application security compliance of applications and organizations.

Note: As there is no "shall" in this document, it is not a certifiable standard by itself.

0.2 Purpose

The purpose of this document is to provide guidance and requirements for the application security validation, verification and audit processes implementation, i.e. to help the organization to perform a repeatable demonstration that a verification scheme's requirements were met.

EXAMPLE 1 Demonstrate that a specific verification scheme was validated and approved by an application security (AS) authority and its elements are clear, complete, measurable and verifiable.

EXAMPLE 2 Demonstrate that a specific application's actual level of trust (LoT) equals or exceeds the targeted LoT required in the verification scheme.

EXAMPLE 3 Demonstrate that an organization is addressing and managing the security of its applications as required in the verification scheme.

0.3 Targeted audience

0.3.1 General

The following audiences will find value and benefits from this document when carrying their designated organizational roles:

a) managers;

b) provisioning and operation team;

c) acquirers;

d) suppliers;

e) auditors;

f) users.

0.3.2 Managers

Managers are persons involved in the management of an application. Examples of managers are:

a) information security managers;

b) project managers;

c) administrators;

d) verification body;

e) audit client;

f) development managers;

g) application owners;

h) line managers, who supervise employees.

Typically, managers need to:

a) review auditor's reports recommending application acceptance or rejection based on proper implementation of required application security controls;

b) ensure compliance with standards, laws and regulations according to an application's regulatory context;

c) manage the audit or the implementation of a secure application;

d) determine which security controls and corresponding verification-measurements should be implemented and tested;

e) make certain proper information security clearances are in place as required by applicable information security policies and procedures;

f) base their decisions on lessons learned derived from knowledgebase records.

0.3.3 Application security authority

Application security authority (AS authority) are individuals or organizations who wish to use a verification scheme to define and receive AS objective evidence that significant security risks have been mitigated to acceptable levels. Examples of AS authority are:

a) governments and regulators, that want to enforce laws or regulations;

b) organizations recognized as authorities in their business sector that want to enforce best practices;

c) contracting parties or potential clients;

d) internal verification groups.

0.3.4 Provisioning and operation team

Members of the provisioning and operations teams (known collectively as the project team) are people involved in an application's design, development and maintenance throughout its whole life cycle. Examples of provisioning and operations team roles include:

a) architects;

b) analysts;

c) programmers;

d) testers;

e) system integration engineers;

f) IT administrators, such as system administrators, database administrators, network administrators, and application administrators.

Typically, members need to:

a) understand which application security controls should be applied at each stage of an application's life cycle and why;

b) understand which controls should be implemented in the application itself;

c) make sure that introduced controls meet the requirements of the associated measurements;

d) obtain access to tools and best practices in order to streamline development, testing and documentation.

0.3.5 Acquirers

This includes all persons involved in acquiring a product or service.

Typically, acquirers need to:

a) prepare requests for proposals that include requirements for security controls;

b) select suppliers that comply with such requirements;

c) verify evidence of security controls applied by outsourcing services.

0.3.6 Suppliers

This includes all persons involved in supplying a product or service.

Typically, suppliers need to:

a) comply to application security requirements from requests for proposals;

b) provide AS objective evidence that required security controls are implemented correctly in proposed products or services.

0.3.7 Auditors

Auditors are persons who need to:

a) understand the scope and procedures involved in verification-measurements for the corresponding controls;

b) ensure that audit results are repeatable;

c) establish a list of verification-measurements which generate AS objective evidence that an application has reached the Targeted LoT as required by management;

d) apply standardized audit processes based on the use of verifiable AS objective evidence.

0.3.8 Users

Users are persons who need to:

a) trust that it is deemed secure to use or deploy an application;

b) trust that an application produces reliable results consistently and in a timely manner while protecting the confidentiality of the data;

c) trust that the controls and their corresponding verification-measurements are positioned and functioning correctly as expected.

Information technology — Application security — Part 4: Validation and verification

Scope

This document provides a detailed description of an application security process to develop, validate, implement, verify and continuously improve verification schemes used to audit and verify application security in an organization.

Application security validation can be done on a verification scheme to validate and verify if it clearly defines clear AS requirements and AS controls to mitigate all risks to acceptable levels and reach application security objectives for specific contexts and environments.

Application security verification and audit can be done on an organization or an application, to verify if it complies with a verification scheme.

Note: As there is no "shall" in ISO/IEC 27034-4, it is not a certifiable standard by itself.

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.

<std>ISO/IEC 17021-1, *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*</std>

<std>ISO/IEC 17024, *Conformity assessment — General requirements for bodies operating certification of persons*</std>

<std>ISO 19011, *Guidelines for auditing management systems*</std>

<std>ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*</std>

<std>ISO/IEC 27034-1, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*</std>

<std>ISO/IEC 27034-2, *Information technology — Security techniques — Application security — Part 2: Organization normative framework*</std>

<std>ISO/IEC 27034-3, *Information technology — Application security — Part 3: Application security management process*</std>

Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1, ISO/IEC 17024, ISO 19011, ISO/IEC 27000, ISO/IEC 27034-1, ISO/IEC 27034-2, ISO/IEC 27034-3, and the following apply.

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

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

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

3.1
accreditation authority
authoritative body that performs accreditation

3.2
application security
AS
protection of information and/or underlying system implied by the provisioning and the operation of an application

3.3
application security audit
AS audit
systematic, independent and documented process used to determine if all expected outcomes, including *AS objective evidence* (3.5), have been produced by the verification of application security activities and to evaluate them objectively to determine the extent to which the *AS audit criteria* (3.4) required by an *application security authority* (3.7) are fulfilled.

Note 1 to the entry: For an organization, this is the process used to determine if all ONF elements identified by an authority, have been implemented and successfully passed their verification process.

Note 2 to the entry: For an application, this is the process used to determine if all ASCs identified by the LoT of an application, have been implemented and successfully passed their verification process.

Note 3 to the entry: Internal audits, sometimes called first party audits, are conducted by the organization itself, or on its behalf, for management review and other internal purposes (e.g. to confirm the effectiveness of the management system or to obtain information for the improvement of the ONF management process). Internal audits can form the basis for an organization's self-declaration of conformity to an ONF or an application.

Note 4 to the entry: External audits include second- and third-party audits. Second-party audits are conducted by parties having an interest in the organization, such as government, customers, suppliers or by other persons on their behalf. Third-party audits are conducted by independent auditing organizations, such as regulators.

Note 5 to the entry: When two or more ONF management processes of different disciplines (e.g. quality, environmental, occupational health and safety) are audited together, this is termed a combined audit.

Note 6 to the entry: Combined audits are not allowed for application security audit.

Note 7 to the entry: When two or more auditing organizations cooperate to audit a single *auditee* (3.5), this is termed a joint audit.

Note 8 to the entry: To ensure that no elements' verification outcomes have been forged, an application security audit can be included to reverify elements included in the scope of an application security verification.

[SOURCE: ISO/IEC 27034-3:2018, 3.1, modified — Notes 1 to 8 to entry have been added.]

3.4
application security audit criteria
AS audit criteria
set of policies, procedures, ASC or requirements used as a reference against which *AS objective evidence* (3.5) is compared

Note 1 to the entry: Explicit list of verifiable elements defining the security quality of a subject, such as ASCs.

Note 2 to the entry: If the AS audit criteria are legal (including statutory or regulatory) requirements, the terms “compliant” or “non-compliant” are often used in an *audit finding* (3.13).

Note 3 to the entry: The term "audit evidence" has been replaced by "objective evidence", to keep vocabulary aligned with ISO 9000.

3.5
application security objective evidence
AS objective evidence
records, ASCs outcomes, statements of fact or other information which are relevant to the *application security audit criteria* (3.4) and verifiable

Note 1 to the entry: AS objective evidence can be qualitative or quantitative.

Note 2 to the entry: When provided, ASCs and ONF processes’ expected results/outcomes should be considered as AS objective evidence.

3.6
verification scope
extent and boundaries of an *application security audit* (3.3)

Note 1 to the entry: The application verification scope should include a description of the physical locations, organizational units, ANF, ASCs, activities and processes, as well as the time period covered in the report.

Note 2 to the entry: The organization verification scope should include a description of the physical locations, organizational units, ONF, activities and processes, as well as the time period covered in the report.

3.7
application security authority
AS authority
verification scheme owner
person or organization responsible for defining, developing and maintaining a *verification scheme* (3.11)

Note 1 to the entry: It can be any entity, internal or external, having an accepted or recognized authority on a verification scheme, such as the application owner, the organization owner, the ONF committee or a government body.

Note 2 to the entry: An AS authority of a verification scheme can also be seen as this verification scheme’s owner.

Note 3 to the entry: The organization can be a verification body, a governmental authority or other recognized authority.

3.8
application security compliance verification
AS compliance verification
successful result of a third-party validation and verification conducted by a verification body

3.9
application security validation
AS validation
process used to validate that the verification scheme appropriately addresses the application security risks, and the rationale provided by the responsible party (e.g. application owner) to support its approval

Note 1 to the entry: For an organization, this should be used to validate required ONF elements and security activities enforced in the organization.

Note 2 to the entry: For an application, this process should be used to validate the targeted LoT identified for an application.

3.10
application security verification
AS verification
process used to determine if intended outcomes were produced by the implementation of an application security activity

Note 1 to the entry: For an organization, this is the process used to determine if the required outcomes produced by the ONF management process implementation are conforming to the expected results, and to consolidate evidence in the ONF for later demonstration.

Note 2 to the entry: For an application, this is the process used to determine if the required outcomes of an ASC implementation are conforming to the expected results, and to consolidate evidence in the ANF for later demonstration.

3.11
verification scheme
framework component defining what will be preformed by an individual *application security audit* (3.3)

Note 1 to the entry: In addition to defining an *AS audit programme* (3.19), objective (e.g. needs, purpose), *verification scope* (3.6) and *AS audit criteria* (3.4), including specific ONF and ANF elements, required by an *AS authority* (3.7) for an *application security audit* (3.3), a verification scheme can include the following:

a) determination of the extent of conformity of the management system to be audited, or parts of it, with AS audit criteria;

b) determination of the extent of conformity of activities, processes and products with the requirements and procedures of the management system;

c) evaluation of the capability of the management system to ensure compliance with legal and contractual requirements and other requirements to which the organization is committed;

d) evaluation of the effectiveness of the management system in meeting its specified objectives;

e) identification of areas for potential improvement of the management system;

f) verification of ASCs.

Note 2 to the entry: The verification scope should be consistent with the audit objectives.

3.12
audit conclusion
outcome of an *AS audit* (3.3), after consideration of the audit objectives and all *audit findings* (3.13)

3.13
audit finding
results of the evaluation of the collected *AS objective evidence* (3.5) against *AS audit criteria* (3.4)

Note 1 to the entry: Audit findings indicate conformity or nonconformity.

Note 2 to the entry: For application audit, audit findings indicate a conformity or nonconformity to a LoT. Audit findings of an application identify its actual LoT.

Note 3 to the entry: Audit findings can lead to the identification of opportunities for improvement or recording good practices.

Note 4 to the entry: If the AS audit criteria are selected from legal or other requirements, the audit finding is termed compliant or non-compliant.

3.14
audit team
one or more *auditors* (3.16) conducting an *AS audit* (3.3), supported if needed by *domain experts* (3.20)

Note 1 to the entry: One auditor of the audit team is appointed as the audit team leader.

Note 2 to the entry: The audit team may include auditors-in-training.

3.15
auditee
organization, application or person being audited

3.16
auditor
person who conducts an *AS audit* (3.3) and provides recommmendations to the *verification body* (3.17)

3.17
verification body
person or organization that manages an audit complying to the objectives, purposes, verification scope and AS audit criteria defined by the application security authority, and delivers an application security compliance attestation to the auditee

3.18

certification scheme for AS experts

competence and other requirements related to specific occupational or skill categories of people

3.19

application security audit programme

AS audit programme

set of one or more audits planned for a specific time frame and directed towards a specific purpose

3.20

domain expert

person who is an expert in a particular domain, area or topic that provides specific knowledge or expertise to the *audit team* (3.14)

Note 1 to the entry: Specific knowledge or expertise is that which relates to the organization, the process or activity to be audited, as well as language or culture.

Note 2 to the entry: A domain expert does not act as an *auditor* (3.16) in the audit team.

3.21

personal certification body

person or organization that defines knowledge, verification scope and AS audit criteria required by an application security auditor, and certifies application security auditors

Abbreviated terms

ANF	application normative framework
ASC	application security control
LoT	level of trust
ONF	organization normative framework

verification scheme framework (VSF)

General

As introduced in ISO/IEC 27034-1, the framework of this document proposes a verification scheme framework used for validating and verifying that:

a) an application can be considered secure;

b) an organization adequately manages the security of its applications.

This process can be used to verify or audit the security of an application or an organization during the provisioning stage or during the operational stage as presented by the application security life cycle reference model (ASLCRM).

Purpose

The purpose of the verification scheme framework is to allow:

a) an AS authority to define, validate, communicate and maintain verification schemes;

b) an organization to measure and verify security elements of an auditee and compare results with the expected ones using the verification scope, processes and components defined in a verification scheme.

Concepts
Principles

Application security validation and verification principles

In addition to principles introduced in ISO/IEC 27034 (all parts), AS authorities creating and maintaining the components and processes in the VSF should be guided by the following principles:

a) application security is to protect information involved by an application, i.e. an application should be protected only if it collects, stores, processes, shares or discloses information deemed sensitive;

b) any AS verification should be performed against at least one verification scheme;

c) each element in a verification scheme should be validated and approved by the AS authority who owns the verification scheme;

d) the outcomes of an application security audit should be repeatable, i.e. they should be independent of the auditor;

e) application security risks should be known in order to be managed;

f) application security should be demonstrated (see ISO/IEC 27034-1).

Principles of AS verifications and audits

This document applies key principles promoted by ISO 19011 and ISO/IEC 17021-1 to inspire confidence in the security audits of applications that have been prepared and implemented using the AS framework, such as:

a) **intellectual integrity** – by being honest, having strong moral principles, and by holding oneself to consistent values and ethical standards;

b) **impartiality and independence** – by imposing a segregation of duties, a verification scheme definition, and verification activities that include expected results to make AS audit findings repeatable and independent of auditors to ensure the impartiality of the audit and objectivity of the audit conclusions;

c) **evidence-based approach** – by imposing a verification scheme definition, and verification activities that include measurable and verifiable expected results (i.e. AS objective evidence) for reaching reliable and reproducible audit conclusions in a systematic audit process;

d) **fair presentation** – by reporting truthful, accurate and clear information;

e) **competence and due professional care** – by requiring key role qualifications identification to maximize the quality of AS elements implementation, measures and verifications and ensure the application of diligence and judgment in auditing;

f) **responsibility** – by clearly identifying the responsibilities, using RACI tables, of the key roles involved in processes realization, as well as in their verification;

g) **openness** – by requiring AS authorities to make verification schemes public;

h) **confidentiality** – by ensuring that information will only be communicated to authorized persons;

i) **risk-based approach** – by enforcing the risk management approach provided by ISO/IEC 27034-3 when defining and maintaining a verification scheme;

j) **responsiveness to complaints** – by providing timely feedback, communication and improvement processes that can be used by audit clients, auditees, auditors, verification bodies, and AS authorities.

NOTE 1 ISO/IEC 17021-1:2015, Clause 4, specifies principles for inspiring confidence on audits.

NOTE 2 ISO 19011:2018, Clause 4, specifies principles of auditing.

Application security parties for AS validation, verification and audit

General

Eight parties are involved in application security validation processes. Figure 1 shows the interrelations between those parties and two components related to the VSF of this document.

27034-4_ed1fig1.eps

Key

27034-4_ed1fig1_key1.eps	Actor	27034-4_ed1fig1_key2.eps	Element defined in this document	27034-4_ed1fig1_key3.eps	International Standard influencing a process
27034-4_ed1fig1_key4.eps	Process described in this document	27034-4_ed1fig1_key5.eps	Process not described in this document		

Figure 1 — Parties and components involved in application security verification processes

To be verifiable, an AS implementation should be aligned with at least one verification scheme (Clause 11).

Application security authority

General

The AS authority is a person or an organization that has a recognized authority (such as by law, business regulations or assignment), reputation recognized by an industry. The AS authority is responsible for managing a verification scheme that it owns. This includes the management of the AS audit programme provided with the verification scheme, such as defining the security needs, purpose, verification scope and AS audit criteria of an AS audit or verification of an Auditee.

The AS authority should have the necessary competence to manage the programme and its associated risks effectively and efficiently, as well as knowledge and skills in the following areas:

a) audit principles, procedures and methods;

b) management system standards and reference documents;

c) activities, products and processes of the auditee;

d) applicable legal and other requirements relevant to the activities and products of the auditee;

e) customers, suppliers and other interested parties of the auditee, where applicable.

The AS authority owns and manages the establishment of the verification scheme. As threat contexts change without notice and on an ongoing basis, the AS Authority should be prepared to continuously review and maintain its AS verification system in response to these changes. The AS authority should engage in appropriate continual professional development activities to maintain the necessary knowledge and skills to manage the verification scheme and its AS audit programme.

Processes and activities under the responsibility of the AS authority are presented in Clause 6.

The AS authority may require to validate and/or approve an application security compliance attestation proposal by a verification body before its delivery to an auditee.

Structural requirements for AS authorities

Verification schemes should be structured and managed so as to safeguard impartiality.

The AS authority should identify the roles and responsibilities for each of the following:

a) ensuring impartiality;

b) development, validation, management and communication of verification schemes;

c) decisions on compliance;

d) management and communication of decisions on compliance attestation.

Organizational structure and top management for AS authorities

The AS authority should document its organizational structure, duties, responsibilities and authorities of management and other personnel involved in a verification scheme and its committees. When the AS authority is a defined part of a legal entity, the structure should include the line of authority and the relationship to other parts within the same legal entity.

Verification and compliance verification activities should be structured and managed so as to safeguard unambiguous and repeatable measurement results, and impartiality.

The AS authority should identify the top management (board, group of persons, or person) having overall authority and responsibility for each of the following:

a) development of management system verification schemes;

b) supervision of the implementation of the policies, processes and procedures;

c) ensuring impartiality;

d) decision criteria on compliance;

e) delegation of authority to committees or individuals, as required, to undertake defined activities on its behalf;

f) specify adequate resources for verification and compliance verification activities

The AS authority should have formal rules for the appointment, terms of reference and operation of any committee that are involved in the compliance verification activities.

Resource requirements for AS authorities

The AS authority should identify the resources it needs for:

a) managing a verification scheme and its AS audit programme (see Clause 6);

b) making the decision on granting, refusing, maintaining, renewing, suspending, restoring or withdrawing compliance attestation;

c) identifying and estimating the resources required (e.g. time, cost, specific tools) to implement and verify a verification scheme.

This responsibility of making the above decisions should not be outsourced.

Competence of personnel

The AS authority shall have processes to identify personnel required competency, knowledge and skills relevant to the verification scheme, including ASCs and other activities that need to be realized or verified on the auditee.

Verification body

General

The verification body is a person or an organization that is recognized by the organization as a verification authority. It is responsible for conducting an audit against a verification scheme defined by the AS authority, and delivers an application security compliance attestation to the auditee. The verification body manages the verification scheme implementation.

Processes and activities under the responsibility of the verification body are presented in Clause 7.

Note: Consider that responsibilities and activities related to certification bodies in ISO/IEC 17021-1 are bound to the role of verification bodies in this document.

Structural requirements for verification bodies

The guidelines from ISO/IEC 17021-1:2015, Clause 6, apply, except 6.1.3 e) and g).

Organizational structure and top management for verification bodies

The guidelines from ISO/IEC 17021-1:2015, 6.1, apply except 6.1.3 e).

Operational control for verification bodies

The guidelines from ISO/IEC 17021-1:2015, 6.2, apply.

Resource requirements for verification bodies

The guidelines from ISO/IEC 17021-1:2015, Clause 7, apply, except 7.2.8 and 7.5.2.

In addition, the following AS-specific guidance applies:

a) In the whole of ISO/IEC 17021-1:2015, Clause 7, the term "management system" should be understood as "verification scheme".

b) The group or individual that makes the recommendation to the AS authority on granting, refusing, maintaining, renewing, suspending, restoring or withdrawing compliance attestation, should understand the applicable standard and compliance verificationrequirements, and should have demonstrated competence to evaluate the outcomes of the audit processes including related recommendations of the audit team.

c) Recommendations for granting, refusing, maintaining of compliance attestation, renewing, suspending or restoring, or withdrawing of compliance attestation should not be outsourced.

Lead auditor and auditor

The auditor is a certified person that conducts an application security audit on an auditee, complying with a verification scheme, and provides audit recommendations to the verification body. A lead auditor manages the audit engagement while an auditor performs the audit.

Processes and activities under the responsibility of the auditor are presented in Clause 8.

Certification bodies for persons

The certification body for persons is a person or an organization responsible to conduct an examination, which uses objective criteria to measure competence and scoring. While it is recognized that such an examination, if well planned and structured by the certification body for persons, can substantially serve to ensure impartiality of operations and reduce the risk of a conflict of interest (see ISO/IEC 17024).

Processes and activities under the responsibility of the certification body for persons are presented in Clause 10.

Auditee

The auditee is an application or an organization that is the target of an application security audit or compliance verification and can have to comply with a verification scheme.

Other parties

The accreditation authority is a person or an organization responsible for the accreditation of verification bodies, certification bodies and personal certification bodies.

The training supplier is a person or an organization responsible to train implementers and auditors, according to the certification scheme for AS experts defined by the personal certification body.

The personal certification body is a person or an organization that defines knowledge, verification scope and AS audit criteria required by an application security auditor or implementer, and certifies them.

The implementer is a certified person who implements AS frameworks (e.g. ONF, ANF, VSF) elements. In particular, the implementer implements elements from a verification scheme provided by an AS authority.

The audit client is a person or organization requesting an audit.

Verification scheme framework elements

General requirements

The verification scheme framework (VSF) provides elements such as components and processes for developing, maintaining and communicating a verification scheme.

A simplified graphical representation of the contents of the VSF is shown in Figure 2.

27034-4_ed1fig2.eps

Figure 2 — Verification scheme framework

NOTE For the purposes of this document, two types of elements are defined: components and processes. Components are represented in Figure 2 using square boxes, and processes are represented using rounded boxes.

The verification scheme management process is defined in Clause 6.

The AS compliance verification process is defined in Clause 7.

The AS audit process is defined in Clause 8.

The AS verification process is defined in Clause 9.

Certification schemes for AS experts are defined in Clause 10.

The verification scheme components and processes are defined in Clause 11.

Information requirements

Verification scheme

The verification scheme is a publicly available set of documents, describing processes and components required to implement or confirm an auditee's application security compliance.

Certification schemes for application security experts

The guidelines from ISO/IEC 17024:2012, Clause 8, apply. In addition, the specific guidance in Clause 10 applies.

Process requirements

Verification scheme processes

The processes required to develop and enforce verification schemes are:

a) verification scheme management process — to help AS authorities to develop, validate, maintain and communicate verification schemes (see Clause 6);

b) AS compliance verification process — to help verification bodies manage AS audit projects using verification schemes (see Clause 7);

c) AS audit and verification process — to help auditors to verify and audit auditees using verification schemes (see Clause 8).

Application security verification process

Verification process and expected outcomes specified by an AS authority in its verification scheme to guide auditors and domain experts during an AS audit.

Application security audit process

Audit process and expected outcomes specified by an AS authority in its verification scheme to guide verification bodies and auditors during an AS audit.

Use of RACI charts in description of activities, roles and responsibilities
This document uses RACI charts for assigning roles and responsibilities for carrying out activities in processes. Such charts identify actors responsible, accountable, consulted or informed for the realization of an activity. Abbreviations are used for describing responsibilities of actors. Those are enumerated in Table 2.

Table 2 — Abbreviations for responsibilities used in RACI charts

Code	Responsibility
R	Responsible for the realization of an activity
A	Accountable for the realization of an activity
C	Consulted during the realization of an activity
I	Informed of the realization of an activity

Use of RACI charts within an organization implementing this document is not required. Organizations should align guidance provided in this document with their own method of clarifying roles and responsibilities.

When conducting verifications and audit activities, it is critical for organizations to determine the resources that are responsible, accountable, consulted, and informed. Table 2 provides a starting point for discussion during the realization of verifications and audit.

Verification scheme management process

General

The AS authority should ensure that a verification scheme is established and maintained, including at least one AS audit programme, to direct the planning and conduct of audits.

This subclause presents guidelines for an AS authority to define a verification scheme to be used to audit the conformance of an auditee (organization or application).

A verification scheme can be defined at two levels:

1) the organization level — where the AS audit programme addresses how an organization manages the security of its applications;

2) the application level — where the AS audit programme addresses how an organization manages the security of a specific application.

Purpose

The purpose of the verification scheme management process is to help an AS authority to clearly define and communicate the processes and components used for verifying compliance.

Outcomes

As a result of the successful performance of this process, a verification scheme including at least one AS audit programme (see Clause 11) is established, implemented, monitored, reviewed and improved.

Realization activities

Figure 3 shows a graphical representation of the verification scheme management process.

27034-4_ed1fig3.eps

Figure 3 — Verification scheme management process

Table 3 enumerates the realization activities for the verification scheme management process.

Table 3 — RACI chart for process “verification scheme management process”

Realization activities	AS authority	Audit client	Verification body	Lead auditor, Auditor	Domain expert	Auditee
Establishing the verification scheme (6.5.2)	A/R			I	C	
Implementing the verification scheme (6.5.3)	A/R			I	C	
Monitoring the verification scheme (6.5.4)	A/R			I	C	
Reviewing and improving the verification scheme (6.5.5)	A/R			I	C	

Guidance

General

The guidelines from ISO 19011:2018, 5.1, apply. In addition, the following specific guidance applies.

Establishing the verification scheme

Determining audit parameters

The AS Audit programme should provide:

a) objectives, scope and criteria of the AS audit;

b) competence of persons (roles, responsibilities and qualifications);

c) extent of the audit programme;

d) risks;

e) procedures;

   1) expected inputs;

   2) activities;

   3) outcomes;

f) records;

g) resources.

Establishing the AS audit programme objectives

The AS authority should ensure that the audit programme objectives are established to direct the planning and conduct of audits.

These objectives can be based on consideration of the following:

a) AS authority priorities;

b) commercial and other business intentions;

c) characteristics of processes, products and projects, and any changes to them;

d) legal and contractual requirements and other requirements to which the AS authority is committed;

e) needs and expectations of interested parties, including customers;

f) risks to the auditee;

g) results of previous audits.

Examples of audit programme objectives include the following:

a) to ensure uniformity of audits conducted under the audit programme;

b) to ensure the objectivity of audits conducted under the audit programme;

c) to lower the complexity of audits;

d) to contribute to the improvement of the security for an application;

e) to contribute to the improvement of an organization's management of its applications' security;

f) to fulfill external requirements;

g) to verify conformity with contractual requirements.

Establishing the audit programme

The AS authority should determine the following requirements for an audit programme:

a) roles, responsibilities and competence of the person(s) managing the audit programme;

b) competence of auditors;

   1) auditor evaluation criteria;

   2) auditor evaluation method;

c) audit team selection criteria;

   1) auditors;

   2) observers, domain experts and guides;

d) extent of the audit programme.

The AS authority should determine the extent of the audit programme, which can vary depending on the size and nature of the auditee, as well as on the nature, functionality, complexity, the level of maturity of and matters of significance to the organization or the application to be audited.

NOTE In certain cases, depending on the auditee's structure or its activities, the audit programme can consist only of a single audit (e.g. a small project activity).

Other factors impacting the extent of an audit programme include the following:

1) the objective, scope and duration of each audit and the number of audits to be conducted, including audit follow up, if applicable;

2) the number, importance, complexity, similarity and locations of the activities to be audited;

3) those factors influencing the effectiveness of the management system;

4) applicable AS audit criteria, such as planned arrangements for the relevant management standards, legal and contractual requirements and other requirements to which the organization is committed;

5) conclusions of previous internal or external audits;

6) results of a previous audit programme review;

7) language, cultural and social issues;

8) the concerns of interested parties, such as customer complaints or non-compliance with legal, significant changes to the auditee or its operations;

9) availability of information and communication technologies to support audit activities, in particular the use of remote audit methods (see B.1);

10) the occurrence of internal and external events, such as product failures, information security leaks, health and safety incidents, criminal acts or environmental incidents;

e) audit programme risks;

There are many different risks associated with establishing, implementing, monitoring, reviewing and improving an audit programme that can affect the achievement of its objectives. The AS authority managing the audit programme of a verification scheme should consider these risks in its development. These risks can be associated with the following:

1) planning, e.g. failure to set relevant audit objectives and determine the extent of the audit programme;

2) resources, e.g. allowing insufficient time for developing the audit programme or conducting an audit;

3) selection of the audit team, e.g. the team does not have the collective competence to conduct audits effectively;

4) implementation, e.g. ineffective communication of the audit programme;

5) records and their controls, e.g. failure to adequately protect audit records to demonstrate audit programme effectiveness;

6) monitoring, reviewing and improving the audit programme, e.g. ineffective monitoring of audit programme outcomes;

f) procedures for the audit programme;

The AS authority managing the audit programme of a verification scheme should establish one or more procedures, addressing the following, as applicable:

1) planning and scheduling audits considering audit programme risks;

2) ensuring information security and confidentiality;

3) select required ONF and ANF elements to include in the verification scheme;

4) for each selected element, defines the verification activity, expected outcomes and measure criteria;

5) assuring the competence of auditors, audit team leaders and experts' domain;

6) selecting appropriate audit teams and assigning their roles and responsibilities;

7) conducting audits, including the use of appropriate sampling methods;

8) conducting audit follow-up, if applicable;

9) reporting to the management on the overall achievements of the audit programme;

10) maintaining audit programme records;

11) monitoring and reviewing the performance and risks, and improving the effectiveness of the audit programme;

g) identifying audit programme resources;

When identifying resources for an audit programme, the AS authority managing the verification scheme should consider:

1) the financial resources necessary to develop, implement, manage and improve audit activities;

2) audit methods;

3) the availability of auditors and domain experts having competence appropriate to the particular audit programme objectives;

4) the extent of the audit programme and audit programme risks;

5) travel time and cost, accommodation and other auditing needs;

6) the availability of information and communication technologies;

h) verification body evaluation criteria.

Conducting AS risks analysis on the verification scheme

The AS authority usually has an understanding of the kind of organizations and applications that is verified using its verification scheme. In fact, it already knows the business context and the regulatory context, and some key application specifications and application data that need to be protected. It also knows if it wants a verification scheme at the application level, for verifying a specific type of applications, or at the organization level, for verifying that an organization can correctly manage the security of what the authority considers sensitive/critical applications.

The AS authority should implement the first three steps of the ASMP (see ISO/IEC 27034-3).

a) It should define a generic application architecture as a reference to identify functionalities, information flows, processes and roles the application will involve. It should also specify the business, regulatory and technological contexts so that sources of AS risks can be identified.

b) It should perform a high-level AS risk analysis, that will lead to evaluation of AS risks, definition of AS requirements to mitigate them, and identification of processes and ASCs needed to address these AS requirements.

c) It should select relevant elements from the ONF and/or ANF that apply to its generic auditee (application and/or organization). This helps to define a verification scope.

An AS risk analysis is conducted on the generic application in three stages:

a) identifying the application requirements and environment (see ISO/IEC 27034-3:2018, 6.1);

b) assessing application security risks (see ISO/IEC 27034-3:2018, 6.2);

c) creating and maintaining the application normative framework (see ISO/IEC 27034-3:2018, 6.3).

Establishing the verification scope

General

As mentioned in 6.5.2.4, a risk analysis determines which ONF elements should be implemented according to the verification scheme being established.

ISO/IEC 27034-2 provides a detailed description of each AS-related, organization-level ONF element that can become part of the scope of an application security audit. It also provides the expected content for each of these elements.

Security requirements in the ANF are derived from the assessment of risks associated with the use of the application by the organization, as performed in step 2 of the ASMP.

For each application project, the ANF is created and completed with the relevant technological, regulatory, and business contexts, application specifications and appropriate ASCs needed for the project.

Establishing the ONF

Components and processes related to the ONF that can be defined in the verification scheme, are:

a) business context;

b) regulatory context;

c) technological context;

d) application specifications repository;

e) roles, responsibilities and qualifications repository;

f) organization ASC library;

g) application security control;

h) categorized information;

i) application security life cycle reference model;

j) application security life cycle model;

k) processes related to application security, such as:

   1) ONF management process;

   2) application security management process;

   3) application security risk analysis process;

   4) application security verification process.

This list determines the maximum scope of an audit based strictly on the ISO/IEC 27034 series. An AS authority may also add any additional audit element to a specific verification scheme.

Establishing the ANF

Components and processes related to the ANF that can be defined in the verification scheme are:

a) business context related to the application environment;

b) regulatory context related to the application environment;

c) technological context related to the application environment;

d) application specifications;

e) selected ASCs for the application stages and targeted LoT;

f) application actors: roles, responsibilities and qualifications;

g) categorized information groups repository associated with the application's environment and its specifications (repository of categorized information groups involved by the application);

h) AS risks and requirements related to this application;

i) artefacts and results produced during the application's lifecycle;

j) application security life cycle model for the application project;

k) proesses related to the security of the application, such as:

   1) application security management process (ANF management process);

   2) verifying the application requirements and environment;

   3) assessing application security risks.

Establishing an AS audit process

The AS authority should define a process by which the auditor verifies, for each element required in the verification scheme, that outcomes of this element's verification-measurement activities were defined.

Establishing an AS verification process

The AS verification process and verification-measurement activities are defined in the verification scheme and should already have been realized and relevant outcomes presented to the auditor.

The AS verification process can include rerunning some process or a verification-measurement activity, as defined by the AS authority, to verify if outcomes obtained during this verification are compliant with the related verification scheme requirement and similar with the one presented by the auditee.

Determining auditor competence to fulfil the needs of the audit programme

Guidelines from ISO 19011:2018, 7.2, apply.

Establish criteria (qualifications/competencies) required by key application security experts

Personal behaviour

Guidelines from ISO 19011:2018, 7.2.2 apply.

Knowledge and skills

The AS authority should specify required knowledge and skills, such as:

a) generic knowledge and skills of management system auditors;

b) discipline and sector-specific knowledge and skills of management system auditors;

c) generic knowledge and skills of an audit team leader;

d) knowledge and skills for auditing management systems addressing multiple disciplines.

Achieving auditor competence

Audit team leaders

Implementing the verification scheme

General

The AS authority managing the audit programme of a verification scheme should implement the audit programme by means of the following:

a) communicating the pertinent parts of the audit programme to relevant parties and informing them periodically of its progress;

b) defining objectives, scope and criteria for each individual audit;

c) coordinating and scheduling audits and other activities relevant to the audit programme;

d) ensuring the selection of audit teams with the necessary competence;

e) providing necessary resources to the audit teams;

f) ensuring the conduct of audits in accordance with the audit programme and within the agreed time frame;

g) ensuring that audit activities are recorded and that records are properly managed and maintained.

Defining the objectives, scope and criteria for an individual audit.

Each individual audit should be based on documented audit objectives, verification scope and AS audit criteria. These should be defined by the AS authority managing the audit programme of an AS verification and be consistent with the overall audit programme objectives.

The audit objectives define what is to be accomplished by the individual audit and can include the following:

a) determination of the extent of conformity of the management system to be audited, or parts of it, with AS audit criteria;

b) determination of the extent of conformity of activities, processes and products with the requirements and procedures of the management system;

c) evaluation of the capability of the management system to ensure compliance with legal and contractual requirements and other requirements to which the organization is committed;

d) evaluation of the effectiveness of the management system in meeting its specified objectives;

e) identification of areas for potential improvement of the management system.

The verification scope should be consistent with the AS audit programme and AS audit objectives. It includes such factors as physical locations, organizational units, activities and processes to be audited, as well as the time period covered by the audit.

The AS audit criteria are used as a reference against which conformity is determined and can include applicable policies, procedures, standards, legal requirements, management system requirements, contractual requirements, sector codes of conduct or other planned arrangements.

In the event of any changes to the audit objectives, verification scope or AS audit criteria, the audit programme should be modified if necessary.

When two or more management systems of different disciplines are audited together (a combined audit), it is important that the audit objectives, verification scope and AS audit criteria are consistent with the objectives of the relevant audit programmes.

Selecting the audit methods.

The AS authority managing the audit programme of a verification scheme should select and determine the methods for effectively conducting an audit, depending on the defined audit objectives, verification scope and AS audit criteria.

NOTE Guidance on how to determine audit methods is given in ISO 19011:2018, Annex B.

Where two or more auditing organizations conduct a joint audit of the same auditee, the persons managing the different audit programmes should agree on the audit method and consider implications for resourcing and planning the audit. If an auditee operates two or more management systems of different disciplines, combined audits may be included in the audit programme.

Selecting the audit team members.

An audit team should be selected, taking into account competences and qualifications needed to achieve the objectives of the individual audit, defined within the verification scheme by the AS authority. If there is only one auditor, the auditor should perform all applicable duties of an audit team leader.

The verification body performing the audit programme should appoint the members of the audit team, including the team leader and any domain experts needed for the specific audit.

NOTE ISO 19011:2018, Clause 7, contains guidance on determining the competence required for the audit team members and describes the processes for evaluating auditors.

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

a) the overall competence of the audit team needed to achieve audit objectives, taking into account verification scope and AS audit criteria;

b) complexity of the audit and whether the audit is a combined or joint audit;

c) the audit methods that have been selected;

d) legal and contractual requirements and other requirements to which the organization is committed;

e) the need to ensure the independence of the audit team members from the activities to be audited and to avoid any conflict of interest [see principle in 5.3.1.2 b)];

f) the ability of the audit team members to interact effectively with the representatives of the auditee and to work together;

g) the language of the audit, and the auditee's social and cultural characteristics. These issues can be addressed either by the auditor's own skills or through the support of a domain expert.

To assure the overall competence of the audit team, the following steps should be performed:

a) identification of the knowledge and skills needed to achieve the objectives of the audit;

b) selection of the audit team members so that all the necessary knowledge and skills are present in the audit team.

If all the necessary competencies are not covered by the auditors in the audit team, domain experts with additional competence should be included in the team. Domain experts should operate under the direction of an auditor but should not act as auditors.

Auditors-in-training may be included in the audit team but should participate under the direction and guidance of an auditor.

Adjustments to the size and composition of the audit team can be necessary during the audit, i.e. if a conflict of interest or competence issue arises. If such a situation arises, it should be discussed with the appropriate parties (e.g. audit team leader, the person managing the audit programme, audit client or auditee) before any adjustments are made.

Assigning responsibility for an individual audit to the audit team leader

The AS authority managing the audit programme of a verification scheme should define required qualifications to assign the responsibility for conducting the individual audit to an audit team leader.

The assignment should be made in sufficient time before the scheduled date of the audit, in order to ensure the effective planning of the audit.

To ensure effective conduct of the individual audit, the following information should be provided to the audit team leader:

a) audit objectives;

b) AS audit criteria and any reference documents;

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

d) audit methods and procedures;

e) composition of the audit team;

f) contact details of the auditee, the locations, dates and duration of the audit activities to be conducted;

g) allocation of appropriate resources to conduct the audit;

h) information needed for evaluating and addressing identified risks to the achievement of the audit objectives.

The assignment information should also cover the following, as appropriate:

a) working and reporting language of the audit where this is different from the language of the auditor or the auditee, or both;

b) audit report contents and distribution required by the audit programme;

c) matters related to confidentiality and information security, if required by the audit programme;

d) any health and safety requirements for the auditors;

e) any security and authorization requirements;

f) any follow-up actions, e.g. from a previous audit, if applicable;

g) coordination with other audit activities, in the case of a joint audit.

Where a joint audit is conducted, it is important to reach agreement among the organizations conducting the audits, before the audit commence, on the specific responsibilities of each party, particularly regarding the authority of the team leader appointed for the audit.

Managing the audit programme outcome.

The AS authority managing the audit programme of a verification scheme, by requesting relevant information to the verification body, should ensure that the following activities are performed:

a) review and approval of audit reports, including evaluating the suitability and adequacy of audit findings;

b) review of root cause analysis and the effectiveness of corrective actions and preventive actions;

c) distribution of audit reports to the management and other relevant parties;

d) determination of the necessity for any follow-up audit.

Managing and maintaining audit programme records.

The AS authority managing the audit programme of a verification scheme should ensure that audit records are created, managed and maintained to demonstrate the implementation of the audit programme. Processes should be established to ensure that any confidentiality needs associated with the audit records are addressed.

The verification body performing an audit programme stemming from a verification scheme should inform the AS authority, and should archive audit records and AS objective evidence as the following:

a) records related to the audit programme, such as:

   1) documented audit programme objectives and extent;

   2) those addressing audit programme risks;

   3) reviews of the audit programme effectiveness;

b) records related to each individual audit, such as:

   1) audit plans and audit reports;

   2) nonconformity reports;

   3) corrective and preventive action reports;

    4) audit follow-up reports, if applicable;

c) records related to audit personnel covering topics such as:

    1) competence and performance evaluation of the audit team members;

    2) selection of audit teams and team members;

    3) maintenance and improvement of competence.

The form and level of detail of the records should comply with the verification scheme requirements to demonstrate that the objectives of the audit programme have been achieved.

Monitoring the AS verification scheme

The AS authority managing the audit programme of a verification scheme should monitor its implementation considering the need to:

a) evaluate conformity with audit programmes, schedules and audit objectives;

b) evaluate the performance of the audit team members;

c) evaluate the ability of the audit teams to implement the audit plan;

d) evaluate feedback from management, auditees, auditors and other interested parties. Some factors can determine the need to modify the audit programme, such as the following:

    1) audit findings;

    2) demonstrated level of management system effectiveness;

    3) changes to the client's or the auditee's management system;

    4) changes to standards, legal and contractual requirements and other requirements to which the organization is committed;

    5) change of supplier.

Reviewing and improving the verification scheme

The AS authority managing the audit programme should review the audit programme to assess whether its objectives have been achieved. Lessons learned from the audit programme review should be used as inputs for the continual improvement process for the verification scheme.

The audit programme review should consider the following:

a) results and trends from audit programme monitoring;

b) conformity with audit programme procedures;

c) evolving needs and expectations of interested parties;

d) audit programme records;

e) alternative or new auditing methods;

f) effectiveness of the measures to address the risks associated with the audit programme;

g) confidentiality and information security issues relating to the audit programme.

The AS authority managing the audit programme should request overall implementation review of the audit programme to verification bodies, to identify areas of improvement, amend the programme if necessary, and should also:

a) review the continual professional development of auditors;

b) report the results of the audit programme review to the management.

AS compliance verification process

In order to perform an AS compliance verification process, the verification body should obtain the relevant verification scheme (including verification scope and AS audit programme) from the AS authority.

The verification body should follow the certification process of ISO/IEC 17021-1:2015, Clauses 9 and 10, as the compliance verification process.

NOTE ISO/IEC 17021-1:2015, 9.2.1, can be omitted, as the audit objectives, verification scope and AS audit criteria are already determined in the verification scheme.

The AS audit programme can provide additional or superseding requirements or guidance.

AS audit process

The purpose of this process is to conduct a repeatable application security audit under a verification scheme.

In order to perform an AS audit, the auditor should obtain the relevant verification scheme from the AS authority. This verification scheme contains the verification scope and the AS audit programme. The auditor is not allowed to modify the verification scheme.

The auditor should follow the audit process and guidelines provided in ISO 19011:2018, Clauses 6 and 7. ISO 19011:2018, Clause 5 does not apply, as the audit programme, verification scope and AS audit criteria are already determined in the verification scheme by the AS authority, and are not subject to review or discussion by the auditor or the auditee.

The verification scheme can provide additional requirements or guidelines that add to, or supersede, parts of the audit process described in ISO 19011.

AS verification process

Each component and process in an ONF or ANF includes its own verification activity, e.g. ASCs and processes include verification activities. The AS verification process consists of verifying that each of these verification activities completed successfully. The audit team should perform this process as part of the audit, unless a different process is required in the audit programme.

For the purposes of verifying an application, the AS verification process is step 5 of the application security management process, as described in ISO/IEC 27034-3:2018, 6.5.

To ensure that no verification activity outcomes have been forged, an AS authority may require in the AS audit programme that the audit team performs again the verification activity of selected elements included in the verification scope (see also Note 8 to entry 3.3).

EXAMPLE 1 The AS authority can require that a random selection of 5 % of verification activities be performed again.

EXAMPLE 2 The AS authority can require that verification measurement activities of some critical ASCs be performed again during each audit.

Certification schemes for AS experts

General

The certification scheme for application security experts is a component of this document used to identify competences and other requirements related to specific occupational or skill categories of persons needed to implement or audit the frameworks of the ISO/IEC 27034 series.

The overall purpose of application security certification of persons is to recognize an individual's competence to perform a task or job related to application security.

In the information security industry, certification schemes are usually defined for auditors (lead auditor scheme) and for compliance project managers (lead implementer scheme). In this document, lead auditor and lead implementer scheme requirements are defined. Some other schemes related to application security may be defined by a personal certification body to address specific needs of the market, e.g. application security risk manager.

Certification of persons provides value through public confidence and trust. Public confidence relies on a valid assessment of competence, by a third party, reconfirmed at defined intervals. The trust and the confidence that the public has for a certification of an ONF or an ANF depends on their trust in the competence of the persons that have implemented the ONF (or ANF) and the auditor that performed the verification.

The third party that has the competence to evaluate the skills of a candidate with impartiality is a certification body for persons accredited in accordance to ISO/IEC 17024.

Certification scheme for AS Lead implementer

Knowledge and skill requirements

Lead implementers should possess the necessary knowledge and skills in application security principles and techniques from the ISO/IEC 27034 series to lead the implementation of an ONF and an ANF. The following is a list of minimum knowledge requirements:

a) the terminology of the ISO/IEC 27034 series;

b) fundamental principles and concepts in the application security of the ISO/IEC 27034 series;

c) implementing and maintaining an ONF;

d) application security control (ASC), its structure, development, validation, verification and implementation mentation;

e) preparation of an application security project based on the ISO/IEC 27034 series;

f) implementation of an application security project based on the ISO/IEC 27034 series;

g) performance evaluation, monitoring and measurement of an application security project based on the ISO/IEC 27034 series;

h) continuous improvement of an application security project based on the ISO/IEC 27034 series;

i) preparation of an application security certification audit.

Certification scheme for AS Lead auditor

General

Confidence in the audit process and the ability to achieve its objectives depends on the competence of those individuals who are involved in planning and conducting audits, including auditors and audit team leaders. Competence should be evaluated through a process that considers personal behaviour and the ability to apply the knowledge and skills gained through education, work experience, auditor training and audit experience.

Knowledge and skill requirements

Lead auditors should possess the necessary knowledge and skills in application security and in auditing principles/techniques to lead the audit of an AS verification scheme, including the ONF and the ANF. The following is a list of minimum knowledge requirements:

a) the terminology of ISO/IEC 27034 series;

b) fundamental principles and concepts in information security;

c) fundamental principles and concepts in application security;

d) fundamental audit concepts and principles;

e) preparation of an audit using the ISO/IEC 27034 series;

f) conducting an application security audit project based on the ISO/IEC 27034 series;

g) conclusion and follow-up of an audit using the ISO/IEC 27034 series.

The following is a list of optional knowledge recommendations:

a) ISO/IEC 27001;

b) ISO/IEC 27002;

c) ISO/IEC 27005;

d) ISO/IEC 27021;

e) further standards of the ISO/IEC 27000 family on security controls and services depending on the verification scope, e.g. ISO/IEC 27036 if the audit focus is on IT security in the supply chain.

Requirements in auditor competence, including skills in auditing techniques and personal behavior requirements, are provided in ISO 19011:2018, 7.2.

Requirements for certification bodies

The certification body has a responsibility to ensure that only those persons who demonstrate competence are awarded certification on application security.

The certification body should be a legal entity, or a defined part of a legal entity, such that it can be held legally responsible for its certification activities. A governmental certification body is deemed to be a legal entity on the basis of its governmental status.

The certification body should be accredited against ISO/IEC 17024, which specifies requirements, which ensure that certification bodies for persons (5.3.2.5) operating certification schemes for AS experts) operate in a consistent, comparable and reliable manner.

The certification body should have sufficient personnel available with the necessary competence in application security to perform certification functions relating to the type, range and volume of work performed such as developing examinations, corrections, reviews of candidate applications, etc.

There should be a certification scheme for each category of certification. A certification body can develop and manage one or many certification schemes. For each scheme, personal behaviour, knowledge and skills should be defined.

The certification body should provide information regarding education and training if they are used as pre-requisites for being eligible for an application security certification.

Verification scheme

General

The verification scheme is the component of the ISO/IEC 27034 series used to communicate what is under verification, describe how the verification is conducted and what expected outcomes should be under scrutiny. Any verification scheme should belong to an AS authority and be public.

Verification schemes should be available to anyone that wants to establish, implement, comply or want to audit the conformity of an organization or an application, to application security objectives and requirements defined by an AS authority, related on the implementation of an organization normative framework (ONF) (see ISO/IEC 27034-2) and an application normative framework (ANF) (see ISO/IEC 27034-3) when required.

27034-4_ed1fig4.eps

Figure 4 — Application security life cycle reference model

A verification scheme can define ONF and ANF elements, including processes, components, roles and required qualifications, to audit and/or verify the security of an auditee during the two stages of the application security life cycle reference model (Figure 4):

a) the provisioning stages:

   1) for organizations that supply applications, i.e. that develop, outsource or acquire some or all of the applications' components;

   2) to verify if an application was supplied accordingly to the expected targeted LoT;

b) the operation stages:

   1) for organizations using applications to support their business purposes;

   2) to verify if an application is operated, maintained and used in a manner to maintain its targeted LoT.

Verification scope

General

ISO/IEC 27034-2 provides a detailed description of each application security-related, organization-level process that can become part of the verification scheme of an application security audit, such as the ONF and its management process. It also provides outcomes and verification activities for each of these processes.

ISO/IEC 27034-3 provides a detailed description of each application security-related, application-level process that can become part of the scope of an application security audit, such as the ANF and its management process. It also provides outcomes and verification activities for each of these processes.

The AS authority may decide to include in a verification scheme any element from the ONF or ANF. The AS authority selects relevant elements and defines evaluation criteria for each. The verification scope should be detailed as follows:

a) initial verification scope;

b) surveillance audit scope;

c) reverification audit scope.

NOTE Subclause 11.2 determines the current scope of an audit based strictly on the ISO/IEC 27034 series. The AS authority can add any additional audit element to a specific AS verification scope.

Tailoring

The AS authority may allow certification bodies to apply a certain amount of tailoring to the AS verification scope. The AS authority should then specify which elements of the AS verification scope may be tailored, and the limits and conditions of such tailoring.

Organization normative framework (ONF)

General

Figure 5 presents a graphical overview of the ONF elements.

27034-4_ed1fig5.eps

Figure 5 — Organization normative framework – simplified graphical representation

For the purposes of correctly addressing application security concerns, an organization should have a formal ONF containing the following components:

a) business context;

b) regulatory context;

c) technological context;

d) application specifications repository;

e) roles, responsibilities and qualifications repository;

f) organization ASC library;

g) categorized information;

h) ONF management process;

i) application security risk analysis process;

j) application security management process;

k) application security life cycle reference model;

l) application security life cycle model.

Application normative framework (ANF)

General

Figure 6 shows a graphical representation of the ANF.

27034-4_ed1fig6.eps

Figure 6 — Application normative framework

The ANF for a specific application project contains the following elements:

a) business context associated with the application’s environment;

b) regulatory context associated with the application’s environment;

c) technological context associated with the application’s environment;

d) application specifications and functionalities;

e) categorized information groups repository associated with the application’s environment and its specifications;

f) application security life cycle model for the application project;

g) application actors: roles, responsibilities and qualifications;

h) processes related to the security of the application;

i) artefacts and results produced during the application’s lifecycle;

j) selected ASCs in the application's targeted level of trust;

k) AS risks and requirements related to this application.

AS Audit programme

The AS authority should define an AS audit programme for the verification scheme. The audit programme should include information and identify resources to enable audits to be conducted effectively and efficiently within the specified time frames. The information should include:

a) objectives for the audit programme;

b) risks and opportunities associated with the audit programme and the actions to address them;

c) reference to the verification scope;

d) schedule (number, duration, frequency) of audits;

e) audit types, such as internal or external;

f) AS audit criteria;

g) audit methods;

h) criteria for selecting audit team members;

i) relevant documented information;

j) expected outcomes of audits: format and contents of summary and detailed reports, including at least:

   1) the verification scheme against which the audit was conducted;

   2) the expected and observed results;

3) an analysis of results leading to a recommendation;

4) a recommendation.

Guidance on audit reports is provided in ISO 19011:2018, 6.5, and in ISO/IEC 17021-1:2015, 9.4.8. Addtional guidance on establishing an audit programme is provided in ISO 19011:2018, Clause 5.

Bibliography

<std>[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*</std>

<std>[2] ISO 9001, *Quality management systems — Requirements*</std>

<std>[3] ISO/IEC/IEEE 12207, *Systems and Software Engineering — Software life cycle process*</std>

<std>[4] ISO/IEC 15026 (all parts), *Systems and software engineering — Systems and software assurance*</std>

<std>[5] ISO/IEC/IEEE 15288, *Systems and software engineering — Software Life Cycle Processes*</std>

<std>[6] ISO/IEC/IEEE 15289, *Systems and software engineering — Content of systems and software life cycle process information products (Documentation)*</std>

<std>[7] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*</std>

<std>[8] ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*</std>

<std>[9] ISO/IEC 17065, *Conformity assessment — Requirements for bodies certifying products, processes and services*</std>

<std>[10] ISO/IEC 17067, *Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes*</std>

<std>[11] ISO/IEC 18019, *Software and system engineering — Guidelines for the design and preparation of user documentation for application software*</std>

<std>[12] ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*</std>

<std>[13] ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*</std>

<std>[14] ISO/IEC 21827, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model (SSE-CMM®)*</std>

<std>[15] ISO/IEC 24759, *Information technology — Security techniques — Test requirements for cryptographic modules*</std>

<std>[16] ISO/IEC/IEEE 24765, *Systems and software engineering — Vocabulary*</std>

<std>[17] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*</std>

<std>[18] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*</std>

<std>[19] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*</std>

<std>[20] ISO/IEC 27006, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*</std>

<std>[21] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*</std>

<std>[22] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*</std>

<std>[23] ISO/IEC 27021, *Information technology — Security techniques — Competence requirements for information security management systems professionals*</std>

<std>[24] ISO/IEC/IEEE 29148, *Software and systems engineering — Life cycle processes — Requirements engineering*</std>

<std>[25] ISO/IEC Guide 60, *Conformity assessment — Code of good practice*</std>

<std>[26] ISO/IEC TS 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*</std>

<std>[27] ISO/IEC TR 90005, *Systems engineering — Guidelines for the application of ISO 9001 to system life cycle processes*</std>

<other>[28] NIST Special Publication 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations</other>