INTERNATIONAL STANDARD

ISO/IEC 27034-3

First edition
2018-05

Information technology — Application security —

Part 3: Application security management process

Technologie de l'information — Sécurité des applications —

Partie 3: Processus de gestion de la sécurité d'une application

Reference number
ISO/IEC 27034-3:2018(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 World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

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

Introduction

0.1 General

A systematic approach to integrate security controls throughout the engineering lifecycle provides an organization with evidence that information being used or stored by its applications is being adequately protected.

The ISO/IEC 27034 series assists organizations in integrating security throughout the life cycle of their applications by providing frameworks and processes scoped at organization and application levels.

This document defines the processes required for managing the security of an application identified as processing critical information by the organization.

Table 1 — ISO/IEC 27034 Framework overview

Scope	ISO/IEC 27034 framework	What it represents
Organization	Organization Normative Framework (ONF)	One centralized repository of application security information
	ONF Management process	Process is in place to maintain and continuously improve ONF
Application	Application Normative Framework (ANF)	Repository for all ASCs of an application
	Application Security Management Process	A risk based process that uses the ANF to build and validate applications

As shown in Table 1, organization-level framework and process are provided by the Organization Normative Framework (ONF). The ONF, its elements and supporting processes are defined in ISO/IEC 27034-2.

Application-level framework and processes are provided by this document in Clauses 5, 6 and 7. The Application Security Management Process (ASMP) helps a project team apply relevant portions of the ONF to a specific application project and formally record evidence of the outcomes in an Application Normative Framework (ANF).

Processes for determining the application requirements and environment are included in 6.1 to 6.5. Subclause 6.1 addresses the identification of the application requirements and its environment, assessing the application security risks. Evaluating the application's Targeted Level of Trust is addressed in 6.2, creating and maintaining the ANF and Application Security Controls (ASCs) is covered in 6.3, and processes pertaining to realizing and operating the application are included in 6.4. Finally, 6.5 presents a process to verify that the ANF and the ASCs are properly implemented.

0.2 Purpose

The purpose of this document is to provide requirements and guidance for the Application Security Management Process and the Application Normative Framework.

0.3 Targeted audience

0.3.1 General

Although this document provides best practices for a general audience, it is especially useful for the following actors:

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 including the Chief Information Security Officer (CISO);

b) project managers;

c) product line managers;

d) development managers;

e) application owners;

f) line managers including the Chief Information Officer (CIO), who supervise employees.

Typically, managers need to:

a) ensure that any application projects, initiatives or processes are based on the results of risk management;

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

c) manage the implementation of a secure application;

d) provide security awareness, training and oversight to all actors;

e) balance the cost of implementing and maintaining application security against the risks and value it represents for the organization;

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

g) ensure the documentation of security policies and procedures for the application;

h) stay abreast of all application-related security plans throughout the organization's network;

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

j) authorize the targeted level of trust according to the context specific to the organization;

k) periodically review the applications for security weaknesses and threats and take corrective and preventive actions;

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

m) ensure that security flaws are prevented through secure coding practices;

n) base their decisions on lessons learned derived from knowledge base records.

0.3.3 Provisioning and operation team

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

a) architects;

b) analysts;

c) programmers;

d) testers;

e) 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) minimize the impact of introducing controls into the development, test and documentation activities within the application life cycle;

d) make sure that introduced controls meet the requirements;

e) obtain access to tools and best practices in order to streamline development, testing and documentation;

f) facilitate peer review;

g) participate in acquisition planning and strategy;

h) arrange disposal of residual items after work is completed, (e.g. property management/disposal).

0.3.4 Acquirers

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

Typically, acquirers need to:

a) establish business relationships to obtain needed goods and services, (e.g. for the solicitation, evaluation and awarding of contracts);

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

c) select suppliers that comply with such requirements;

d) verify evidence of security controls applied by outsourcing services;

e) evaluate products by verifying evidence of correctly implemented application security controls.

0.3.5 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) select appropriate application security controls for proposals, with respect to their impact on cost;

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

0.3.6 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 evidence that an application has reached the Targeted Level of Trust;

d) apply standardized audit processes based on the use of verifiable evidence, according to ISO/IEC 27034 (all parts).

0.3.7 Users

Users are persons who need to trust that:

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

b) an application produces reliable results consistently and in a timely manner;

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

Information technology — Application security —

Part 3:
Application security management process

1 Scope

This document provides a detailed description and implementation guidance for the Application Security Management Process.

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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

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

ISO/IEC 27034-5, *Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1, ISO/IEC 27034-2, and ISO/IEC 27000 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 https://www.electropedia.org/

3.1
application security audit
AS audit
systematic, independent and documented process for obtaining audit evidence from the verification of application security activities, and evaluating it objectively to determine the extent to which the audit criteria required by an application security authority are fulfilled

3.2
application security verification
process of reviewing and verifying security activity outcomes by performing the associated verification-measurement activity

Note 1 to entry: For an organization, required ONF elements and security activities meet ONF specifications and are compliant with ONF management process.

Note 2 to entry: For an application, a security activity and its associated verification-measurement activity may be part of an ASC.

3.3
critical information
information which, if compromised, can result in an unacceptable risk

3.4
domain expert
person who is an expert in a particular domain, area or topic

3.5
risk management
coordinated activities to direct and control an organization with regard to risk

Note 1 to entry: This document uses the term "process" to describe risk management overall. The elements within the risk management process are termed "activities".

[SOURCE: ISO Guide 73:2009, 2.1]

4 Abbreviated terms

AS	Application Security
ASC	Application Security Control
ASMP	Application Security Management Process
ANF	Application Normative Framework
ASLCRM	Application Life Cycle Security Reference Model
ONF	Organization Normative Framework

5 Application Security Management Process

5.1 General

The Application Security Management Process (ASMP) is the overall process for managing security on each specific application used or developed by an organization.

The ONF Committee is responsible for implementing and maintaining the ASMP by use of the ONF management process (see ISO/IEC 27034-2:2015, 5.4.3). This committee is also responsible for ensuring that the ASMP is applied to all application projects in the organization.

The Application owner is accountable for ensuring an ASMP is in place for the application project (see Table 3).

For each application project, the project manager is responsible for implementing and using the ASMP in the course of the project (see Table 3).

The Application Security Management Process is performed in five steps:

a) identifying the application requirements and environment;

b) assessing application security risks;

c) creating and maintaining the Application Normative Framework;

d) provisioning and operating the application;

e) auditing the security of the application.

The first 3 steps of the ASMP are focused on identifying and recording appropriate application security controls (ASCs) for an application. Considering that security up front is a fundamental aspect of application security, the optimal point to define security requirements for a software project is during the initial planning stages. This early definition of requirements allows project teams to identify key milestones and deliverables, and permits the integration of security in a way that minimizes any disruption to plans and schedules.

The last 2 steps of the ASMP are focused on implementation and verification of ASCs.

ISO/IEC 27034 (all parts) provides components, processes and frameworks that help an organization to acquire, implement and use applications it can trust, at an acceptable security cost determined by the organization. Moreover specifically, these components, processes and frameworks provide demonstrable evidence that applications reach and maintain a targeted level of trust.

As shown in Figure 1, these components, processes and frameworks are part of two overall processes:

a) the ONF Management Process;

b) the Application Security Management Process (ASMP).

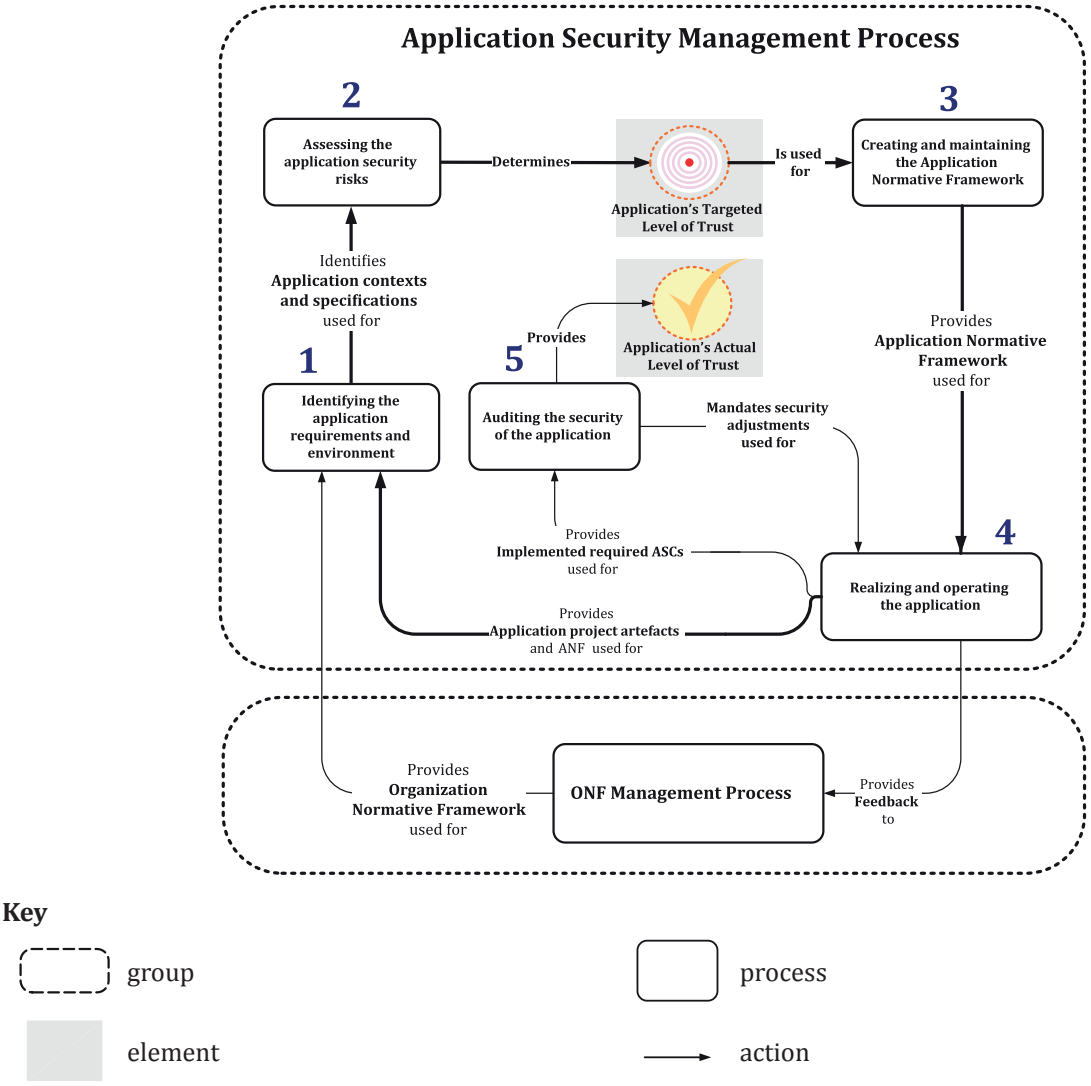


Figure 1 — Application Security Management Process

These two processes are used at different levels and time frames in the organization and have different scopes. The ONF Management Process (see ISO/IEC 27034-2) is a continuous organizational-level process and the ASMP is used for managing security on each specific application project.

5.2 Purpose

The Application Security Management Process allows an organization to manage security for each application it uses.

5.3 Principles and concepts

5.3.1 General

In addition to principles introduced in ISO/IEC 27034-1, organizations creating, operating or maintaining applications should be guided by the following principles:

a) every application should be assigned a Targeted Level of Trust;

b) any security component or process used in an application project should be selected from the ONF;

c) all ASCs selected with the Targeted Level of Trust should be implemented, verified and audited.

5.3.2 Clearly communicate 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 realization and verification activities, it is critical for organizations to determine the resources that are responsible, accountable, consulted, and are informed. Table 2 provides a starting point for discussion during the realization of an ANF.

5.3.3 Relationship of the ASMP with the Organizational Normative Framework (ONF)

The ONF, which is covered in detail in ISO/IEC 27034-2, provides an organization-level context for the ASMP. This context includes all processes involved in application security, as well as regulations, laws, best practices, roles, and responsibilities accepted by the organization. The ASMP uses this context to create and maintain the Application Normative Framework (ANF) for each application project. In return, the ASMP supports continual improvement of the ONF through feedback of new knowledge, application security control improvement suggestions and practices gained in the course of an application's development and deployment.

5.3.4 Use approved tools

Project teams should take advantage of new security analysis functionality and protections by leveraging approved tools and their associated security checks, such as compiler/linker options and warnings. A list of approved tools should be provided as part of the Organization Normative Framework. If the project team is aware of a tool that exceeds what is currently outlined in the ONF's approved list, it should use the ONF's feedback process to inform the ONF Committee about the tool.

NOTE The description, purpose and role of the ONF committee is described in ISO/IEC 27034-2:2015, 5.4.3.

5.3.5 Level of Trust

A "Level of Trust" is a label that identifies a set of applicable ASCs from the Application Security Control Library in the ONF. The ISO/IEC 27034 framework proposes two types of Levels of Trust that can be associated with an application:

a) Targeted Level of Trust;

b) Actual Level of Trust

The Targeted Level of Trust should be derived using an organizationally relevant implementation of the risk management process outlined in ISO/IEC 27005.

5.3.6 Application's Targeted Level of Trust

Applicable security controls for a Targeted Level of Trust can either be pre-defined in the ONF or be derived from a workflow that identifies the applicable controls based on the selected Level of Trust and more refined application security specifications. The workflow may leverage automation and tools, such as Secure Application Lifecycle Management systems, to make the process consistent across multiple applications.

The risk assessment process produces the security requirements from which the application's Targeted Level of Trust is derived. This in turn becomes the goal for the application's project team.

The application Targeted Level of Trust can aid in conveying a level of confidence needed by the organization so that it would be willing to use or deploy the application after accepting the residual risks determined by the risk assessment.

The application Targeted Level of Trust is vital to the security of the application because it directly determines the appropriate Application Security Controls to be selected from the ASC library and implemented in the application life cycle.

The application Targeted Level of Trust should be one of (or within the range of) the levels of trust defined in the Organization ASC Library (see ISO/IEC 27034-1:2011, 8.1.2.6), which is part of the ONF.

The ASC library (ISO/IEC 27034-1:2011, Figure 4) can be represented as a table and the application Targeted Level of Trust as a column in that table. Thus selecting a level of trust means selecting all ASCs in that column.

The following is a sample breakdown of Levels of Trust that an organization may define:

EXAMPLE 1 Business critical applications, internal applications, public applications.

EXAMPLE 2 Generic Web Public Application: Targeted Level of Trust is public applications, technology context is a web based application with a database, and business context is that the application stores and processes end user passwords.

5.3.7 Application's Actual Level of Trust

The application's Actual Level of Trust is the maximum confidence level demonstrated by the verification team according to the verification measurements of all the application's ASCs.

Each ASC included in the ANF for any given application project provides a specific and detailed measurement activity to be performed by the verification team, along with a pointer to the specific stage in the application life cycle in which the measurement should be performed.

The application's Actual Level of Trust is obtained during the application security review by verifying the ASCs that should completed at a specific point in the application's life cycle. If any ASC fails verification, the organization should take appropriate measures to correct the situation.

Successful achievement of the application Targeted Level of Trust is confirmed when the successful verification of all its ASCs have been performed and with the generation of all the necessary supporting evidence from the verification measurement activities.

If some ASCs fail verification, the application owner should take appropriate measure to address the problem.

Given the application's Targeted Level of Trust has been authorized by the application owner during step 2 of the ASMP, the application would be deemed secure by the organization for use or deployment for a specific period of time based on the verification team's agreement of the supporting evidence demonstrating that the application Targeted Level of Trust was achieved. The security status of the application is valid only for a specific period of time because of the periodical revision requirement of step 2 of the ASMP.

An application is considered secure according to ISO/IEC 27034 (all parts), if the application's Actual Level of Trust is equal or greater than its Targeted Level of Trust, e.g. if all ASCs required by the "Blue" level of trust are successfully implemented and verified, then the application can be considered secured as "Actual Level of Trust Blue".

5.3.8 Impact of this document on an application project

A typical application project (before an organization implements this document) is driven by an execution team, supported by processes, often automated by technology, with the goal of generating an application product. The verification team role can be done by the quality assurance team, following test plans to verify the application functionalities against the accepted functional requirements.

Figure 2 shows how this document adds new roles, responsibilities, components and processes to a typical application project.

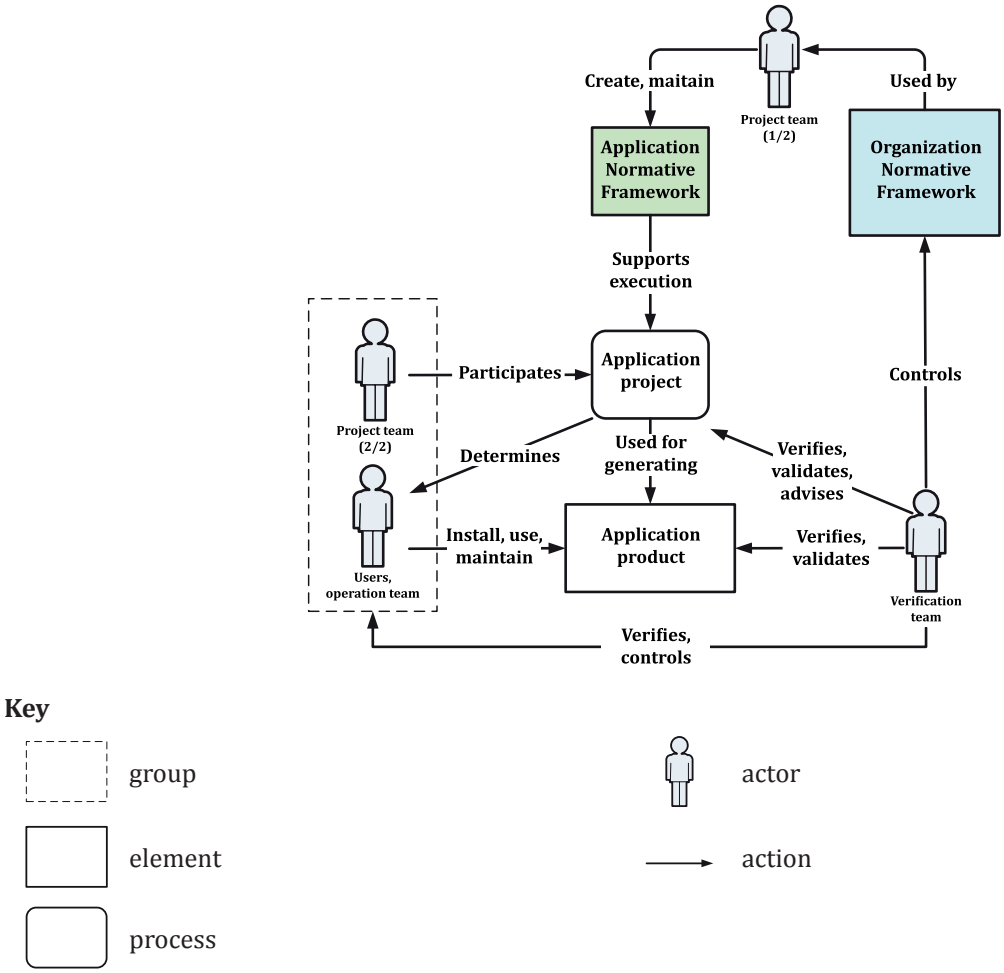


Figure 2 — Impact of this document on roles and responsibilities in a typical application project

The technology itself, the development methodology used by the execution team, the process maturity, the quality of the artefacts produced, and the qualifications of the actors involved in the project are rarely verified and such verification processes, if performed, are usually not formally defined.

6 ASMP steps

6.1 Identifying the application requirements and environment

6.1.1 General

The identification of the application environment allows the organization to specify the contexts (business, technological, regulatory) of the application, its main specifications, actors and processes, and information involved in its acquisition and use.

This step corresponds to the “context establishment” step in the risk management process established by ISO/IEC 27005. It provides necessary information for the subsequent risk assessment step.

The first step of the ASMP aims to identify all application requirements, including:

a) actors;

b) specifications;

c) information;

d) environment.

The application environment consists of:

a) a technological context;

b) a business context;

c) a regulatory context.

Contexts are presented in more detail in ISO/IEC 27034-1:2011, 8.1.2.1 to 8.1.2.2.

6.1.2 Purpose

The purpose of this step is to gather all relevant information to organize security requirements and support the following activities of ASMP.

This step is required to:

a) identify the application owner;

b) identify, inventory and consolidate the information needed to carry out the summary of the application security risk analysis;

c) define a preliminary version of the ANF.

6.1.3 Outcomes

The principal outcomes of this step include:

a) a person is officially designated as the owner of the application;

b) a preliminary ANF, containing:

1) brief description of the three contexts;

2) both functional and non-functional requirements;

3) application architecture (also considering the environment of operation);

4) information groups involved in the provisioning and operation of the application.

6.1.4 Realization activities

Table 3 shows roles and responsibilities for carrying out realization activities for process "Identifying the application requirements and environment".

Table 3 — RACI chart for process “Identifying the application requirements and environment”

Realization activities	ONF committee	Application owner	Project manager
1) Identify and appoint the application owner.	A/R		
2) Implement the ASMP in this project.		A	R
3) Identify the needs of the organization leading to the characteristics of the application.	A	A/R	I
4) Identify the requirements of the application, i.e. all of the requirements and specifications that the application should meet.	C	A/R	I
5) Identify and classify information groups involved by the application and the information flow between application components and between the application and other systems (see Figure 11).	C	A/R	I

Table 3 *(continued)*

Realization activities	ONF committee	Application owner	Project manager
6) Identify the business context of the application, including processes, actors and business requirements required or affected by the implementation and use of the application.	C	A/R	I
7) Identify the regulatory context of the application, i.e. the laws and regulations that apply to the application.	C	A/R	I
8) Identify the technological context of the application, i.e. all IT components required to develop, deploy, monitor and maintain the application.	C	A/R	C/I
9) Validate, verify and integrate the results of this activity to the preliminary ANF.	C	A/R	C/I

6.1.5 Verification activities

Table 4 shows roles and responsibilities for carrying out verification activities for process "Identifying the application requirements and environment".

Table 4 — RACI chart for verification for process "Identifying the application requirements and environment"

Verification activities	ONF Committee	Project Manager	Application owner	Auditors	Project team
1) Verify that an application owner was appointed to this application project.	A			R	
2) Collect application security contexts documentation (Business, Regulatory and Technological).		C	I	A/R	C
3) Collect application specifications and related processes description.		C	I	A/R	C
4) Collect the categorized information groups inventory and information flow diagrams.		C	I	A/R	C
5) Collect evidence that actors were identified and details about each actor were documented.		C	I	A/R	C
6) Collect application specifications, requirements documents, and architecture diagrams.		C	I	A/R	C

6.1.6 Guidance

6.1.6.1 General

The process determining application requirements and environment involves identifying the components, starting with actors.

The actors identified provide the information needed to determine the environment and context of the application.

The activities needed to identify application requirements and environment include:

a) identify the actors;

b) Identify organizational application security specifications;

c) understand information flows involved by the application;

d) establish the application's environment.

6.1.6.2 Identify the actors

Expected roles, responsibilities and qualifications should be specified.

After identifying the actors, it is recommended to make actors participate in the realization process as they can provide the information needed to determine the environment and context of the application.

The components need to be documented using the choices applicable to each component within the Organization Normative Framework. In addition, evidence of gathering the information needs to be stored to allow verification of the correctness of the information at later steps.

6.1.6.3 Identify organizational application security specifications

Application security specifications may already be found at this stage in organizational application project sources, such as:

a) software requirements specification such as TLS, SSH, SFTP;

b) organizational security requirement policies, such as minimum password requirements;

c) regulatory and compliance documents;

d) organizational and business objectives and/or visions;

e) architecture diagrams.

6.1.6.4 Understand information flows involved by the application

Flows of information related to the application should be understood and named, including data provided by any user, front-end to back-end data flow for the application, data transmitted by the application, data derived from technological routines, data structures, configuration data, and data stored.

Data packet flow across the internal network is critical to validate the data are being requested from the source and to the destination.

6.1.6.5 Establish the application's environment

The environment of the application is identified by detailing the application's technological, business and regulatory context.

NOTE It is necessary to record all relevant information produced in each activity to create the ANF and to verify the correctness of the information and the process itself at later steps.

The following examples demonstrate processes and activities that organizations may perform at this step:

EXAMPLE 1 Organizations can perform an initial security requirements analysis during project inception to determine the technical, business, and regulatory context.

EXAMPLE 2 Organizations can negotiate ASCs for each development phase. ASCs contain predefined security and verification processes, criteria and expected results for how to handle security bugs or application security risks. For example, they can agree all SQL Injection vulnerabilities must be triaged and fixed in a specific way prior to code check-in.

EXAMPLE 3 Organizations can categorize its ASCs, such as “mandatory”, “important” and “nice to have”, and use this categorization as allowable bug threshold levels to communicate to stakeholders the severity thresholds of security vulnerabilities addressed. These thresholds can be seen as a Targeted Level of Trust that applies to the entire application project. For example, an organization can define a Level of Trust requiring all “mandatory” and “important” ASCs addressing known “critical” or “high” vulnerabilities be implemented in the application at time of release. In that example, the allowable bug threshold level requires that at least all “mandatory” and “important” ASCs be successfully implemented and verified.

EXAMPLE 4 Organizations can use survey tools to capture characteristics and application security risks to form an application profile, and consequently generate a list of applicable application security requirements identifying corresponding ASCs. Using automation and tools increases the consistency in application security requirements across multiple applications. Tools can also be used to manage and uniformly enforce Targeted Levels of Trust across applications.

NOTE To minimize the impact on organizations and to reduce resistance from stakeholders that implement or use it, this document does not require organizations to adopt or change any specific vocabulary, actor names, or process names to be implemented. This document is development methodology-and operational processes-agnostic and can be adapted/integrated to any of them.

6.2 Assessing application security risks

6.2.1 General

The second step of the ASMP corresponds to the process of assessing the risk for a specific application project.

This step corresponds to the “information security risk assessment” step and a part of the “information security risk treatment” step in the risk management process established by ISO/IEC 27005, but with a finer granularity level and a scope limited to a single application project.

According to ISO/IEC 27005, “Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or could exist), identifies the existing controls and their effect on the risk identified, determines the potential consequences and finally prioritizes the derived risks and ranks them against the risk evaluation criteria set in the context establishment.”

Risk assessment includes three sub-steps: risk identification, risk analysis and risk evaluation. Therefore, this step of the ASMP also involves a “Selection of risk treatment options” to target an accepted and approved level of risk. For this reason, this step also corresponds to the “information security risk treatment” step in the risk management process established by ISO/IEC 27005.

This step of the ASMP also produces application security requirements, which will be used to select the required ASCs for the application as illustrated in Figure 3.

Figure 3 — Logical flow from application security risks to mitigated risks

Application security risks, derived from the application's context and environment [identified in step 1 (see 6.1)], define the security requirements and associated set of applicable ASCs. In Figure 3, “n..n” expresses a many-to-many relationship, whereas “1..n” expresses a one-to-many relationship.

The risk assessment step of the ASMP results in identifying the application's Targeted Level of Trust (see ISO/IEC 27034-1:2011, 8.2.4) which should be approved by the application owner.

NOTE 1 A methodology for organization-level security risk analysis is maybe not able to identify all risks and security controls required for safe operation of an application. To be effective, the security risk analysis method used here will have been specifically developed or adapted to ensure that the specificities of an application and its environment are taken into account..

NOTE 2 For the applications that include Personally Identifiable Information (PII), the privacy risks are also considered during the risk assessment process.

NOTE 3 Privacy risks are dependent on applicable privacy acts, laws and local regulations which are mentioned in the regulatory context.

6.2.2 Purpose

The purpose of this process is:

a) For the project: identify, analyse and evaluate security risks, obtain the resulting security requirements, the Targeted Level of Trust, and required ASCs to secure the application.

b) For the organization: consolidate and maintain applications risk information in the ONF.

6.2.3 Outcomes

In carrying out the activities of this process, the following results are obtained, specifically:

a) a preliminary version of the ANF is produced and contains information about the application environment and the information produced by this process, including:

   1) a list of application security risks;

   2) security requirements for mitigating those risks;

   3) the application's Targeted Level of Trust, identifying the list of ASCs that are required during the application's life cycle;

b) application security information in the ONF is updated.

6.2.4 Realization activities

Table 5 shows roles and responsibilities for carrying out realization activities for process "Assessing application security risks".

Table 5 — RACI chart for realization of ASMP step "Assessing application security risks"

Realization activities	ONF committee	Application owner	Project team
1) Identify and assess security risks brought about by the application.	C	A/R	C
2) Identify and assess the extent that previously identified security risks have been resolved by the application.	C	A	R
3) Identify security requirements for the minimum security required for the application (from unacceptable security risks).	C	A/R	C
4) Determine the Targeted Level of Trust for the application, meeting all identified security requirements.	C	A/R	C
5) Validate and approve the Targeted Level of Trust.	I	A	R
6) Collect the information produced by the risk analysis, as enumerated in 6.1.3.	C	A/R	C

Table 5 *(continued)*

Realization activities	ONF committee	Application owner	Project team
7) Update the contents of the ANF.	A	I	R
8) Update the contents of the ONF.	A/R	C	C
9) Make information accessible to those concerned.	I	A/R	I

6.2.5 Verification activities

Table 6 shows roles and responsibilities for carrying out verification activities for process "Identifying the application requirements and environment".

Table 6 — RACI chart for verification of ASMP step "Assessing application security risks"

Verification activities	Managers	Application owner	Verification team
1) Collect application security risk analysis inputs and outcomes.	C	C/I	A/R
2) Ensure that application security risk was analysed, including high-level and detailed application risk analysis.	C	C/I	A/R
3) Ensure that application security risk was evaluated accurately given the determined set of application security controls.	C	C/I	A/R
4) Ensure that the application's Targeted Level of Trust was defined and approved.	C	C/I	A/R
5) Ensure that the application owner accepted the residual risks associated with the application.	C	C/I	A/R

6.2.6 Guidance

6.2.6.1 Scope of the application security risk assessment

The risk assessment should consider risks involving processes, activities and actors involved in the four layers of the Application Security Life Cycle (see example in Figure 4). It is important to note that the life cycle does not only contain provisioning stages. Risks applying to operation stages are equally important.

Therefore, the ASMP applies to all stages and layers of the life cycle. This is especially relevant to organizations that operate applications, in contrast to organizations that act only as providers or vendors.

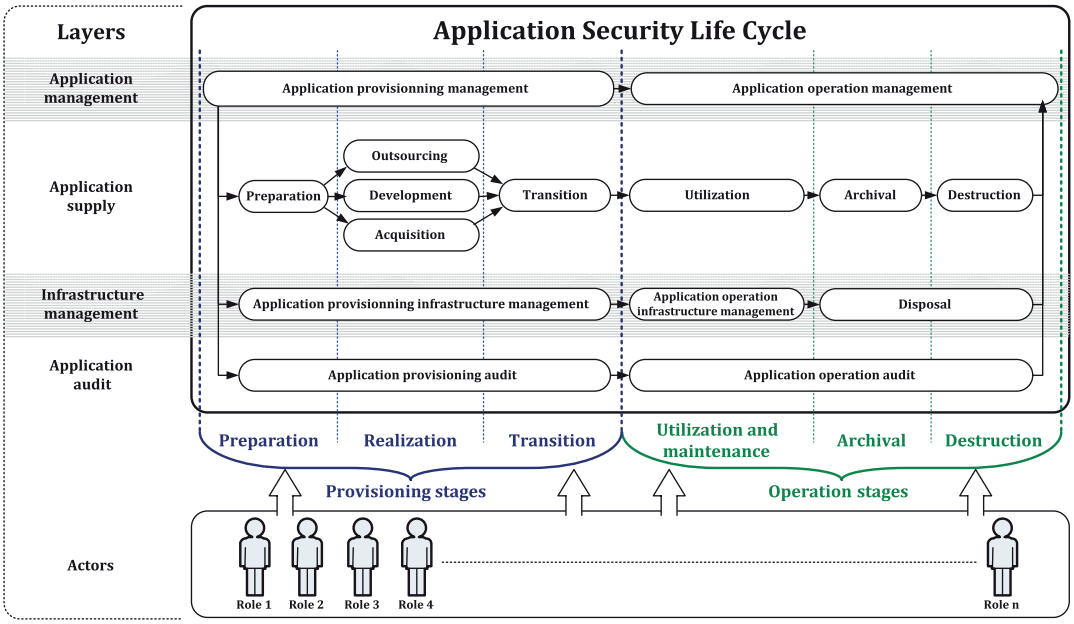


Figure 4 — Example of an application security life cycle

6.2.6.2 Application risk identification

Application security risk identification is a process of finding, recognizing and describing risks concerning information received, stored, processed, used and communicated by the application. It should consider risks whether or not their source is under the control of the organization, such as business, regulatory and technological contexts.

Risk identification involves the identification of risk sources, events, their causes and their potential impact. It can rely on historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

6.2.6.3 Application risk analysis

6.2.6.3.1 General

Risk analysis is the first step of risk assessment. An application risk analysis is often performed in two steps:

a) high-level risk analysis;

b) detailed risk analysis.

6.2.6.3.2 High-level application risk analysis

The high-level application risk analysis process is usually performed in the preparation stage of the application's life cycle, as defined in ISO/IEC 27034-1:2011, 8.2.2.1.

The high-level risk analysis defines, in a simple "rule of thumb" manner, the application's Targeted Level of Trust of the application according to the basic application specifications and based on the application's technological, regulatory, and business contexts.

The owner for the specific application project should appoint an explicit role with the responsibility of performing this analysis using a methodology adequate for an application-level analysis. An organization-level risk analysis methodology may not be adequate for this task.

The following are examples of the questions addressed during the high-level application risk analysis to identify application specifications and contexts:

EXAMPLE 1 Is the application used by internal users only or used over the Internet?

EXAMPLE 2 Is it a web or a desktop application?

EXAMPLE 3 Does the application handle credit card data?

EXAMPLE 4 Does the application have a mobile device component?

6.2.6.3.3 Detailed application risk analysis

The detailed application risk analysis process is performed in the realization phase of the application's life cycle, as defined in ISO/IEC 27034-1:2011, 8.2.2.2.

This process identifies more precisely the residual risks associated with the application before the consideration of any Application Security Controls and reconfirms the application's Targeted Level of Trust determined during the high-level application risk analysis, taking into account the detailed application specifications and the organization's technological, regulatory, and business contexts for the application.

As a result of this detailed application risk analysis process, the application owner can change the application Targeted Level of Trust for the application project, thus changing the ASCs involved in the project. This would change the actors involved and the estimated cost of the project. However, those security impacts due to the ASC update are easily predicted since such information as actors, professional qualifications and estimated cost are already part of each ASC and documented in the organization's ASC library.

The owner for the specific application project should appoint an explicit role with the responsibility of performing this analysis using a methodology adequate for an application-level analysis. An organization-level risk analysis methodology might not be adequate for this task.

The following are examples of the questions addressed during the detailed application risk analysis:

EXAMPLE 1 Does the application have an authentication feature including appropriate protection of credentials?

EXAMPLE 2 Is the authentication against a database or Active Directory?

EXAMPLE 3 Does the application support role-based authorization?

EXAMPLE 4 Does the application include JavaScript code?

The answers provided for the questions that are addressed during the risk analysis process result in creation of security requirements. These security requirements are documented in the ANF (refer to 6.3 for more details). The following is an example:

EXAMPLE 5 If the application provides a form-based authentication feature (this is derived from the answer to a risk analysis question), then the authentication must be protected against user enumeration attacks (this is the security requirement part).

6.2.6.3.4 Techniques for detailed application risk analysis

6.2.6.3.4.1 General

The organization may include in its ONF some well-known techniques, examples of which are provided below.

6.2.6.3.4.2 Threat modelling

Threat modelling is used in environments where there is meaningful security risk. It is a practice that allows project teams to consider, document, and discuss the security implications of designs in the context of their planned operational environment and in a structured fashion. Threat modelling also allows consideration of security risks at the component or application level. Threat modelling is a team exercise, encompassing program/project managers, developers, and testers, and represents the primary security analysis task performed during the software design stage.

6.2.6.3.4.3 Threat model and attack surface review

It is common for an application to deviate from the functional and design specifications created during the requirements and design phases. As a result, the project teams should revisit the threat models and attack surface measurements of a given application when the code is complete. This review ensures that any design or implementation changes have been accounted for, and that any new attack vectors exposed as a result of the changes have been reviewed and mitigated. The threat model and attack surface review process may lead to a change in the Targeted Level of Trust.

For project teams that follow a waterfall development model, this review occurs after the implementation phase or after major changes. In an agile development model, this activity should be performed upon every iteration of the model.

6.2.6.4 Application risk evaluation

According to ISO/IEC 27005, "Risk evaluation uses the understanding of risk obtained by risk analysis to make decisions about future actions." Decisions should include:

a) whether an activity should be undertaken;

b) priorities for risk treatment considering estimated levels of risks.

In this document, this step takes the form of selecting the application Targeted Level of Trust, which in turn determines which Application Security Controls should be implemented for risk treatment.

As a result of the risk evaluation, the application owner may change the application's Targeted Level of Trust for the application project. This changes the applicable ASCs selected for the project, which has an impact on actors involved and the estimated cost of the project.

6.2.6.5 Application security risk assessment activities

The following proposes key activities that organizations may perform when conducting an application security risk assessment:

a) Obtain required information from the ANF. This information, usually provided by the first step of the ASMP, should include:

    1) the requirements for the application;

    2) the application's environment:

        i) business context;

        ii) regulatory context;

        iii) technological context;

    3) the information captured, stored, processed or supplied by the application;

    4) the security categorization for this information;

    5) the flow of this information within the application;

6) identification of which of this information the organization considers critical;

7) the application's specifications, features and components, and which information they act upon;

8) the application's processes, organization processes interacting with the application, and which information they act upon;

9) actors involved in these specifications and processes;

b) categorize specifications, processes and actors according to the categorization of the information they act upon, (they inherit the information's categorization);

c) determine which specifications, processes and actors are to be considered critical;

d) determine threats to critical information based on the application's environment and critical specifications, processes and actors (see 6.2.6.3.4);

e) determine vulnerabilities based on the application's environment and critical specifications, processes and actors;

f) determine impacts to the organization, based on the intrinsic and operational value of the application's critical information;

g) determine application security risks, based on the information gathered above; determine acceptable and unacceptable risks based on organization's criteria;

h) define strategies to mitigate these risks;

i) for each unacceptable risk, determine a preferred mitigation strategy, e.g. treat, transfer, tolerate or terminate;

j) for each unacceptable risk, define application security requirements accordingly.

6.2.6.6 Application security requirements

In most types of application projects, security risks should be considered after the design requirements are completed to make sure resulting security requirements will also address security risks coming from design requirements (e.g. functional requirements). Once defined, these security requirements may produce a feedback loop and impact the application's design requirements. Mitigation of security risks is much less expensive when performed during the design phase and before the implementation of the code.

The purpose of a security requirement is to clearly define what outcomes should be expected from an ASC that will be implemented to mitigate a risk to an acceptable level.

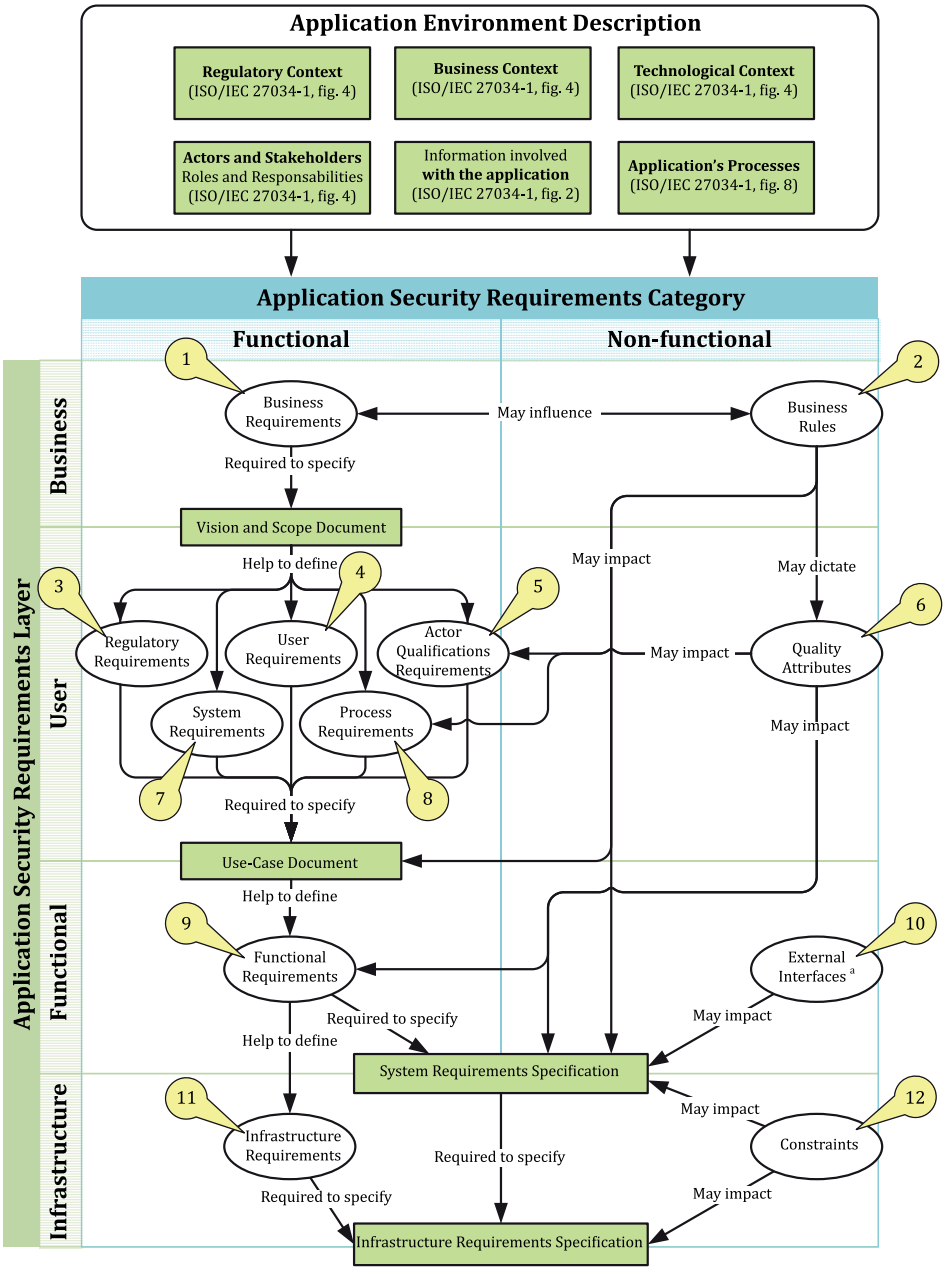
The main difference between software requirements (or system requirements) and security requirements is that software and system requirements are created to describe how to address needs, (i.e organizations' needs, users' needs or applications' needs), while security requirements are created to address risks.

Once completed, security requirements should also describe how to securely implement and deploy all functionality provided by a given feature. The project team should validate design specifications against the application's functional specification. It should provide end-to-end coverage, including devices that access the application system, inter-system interfaces and any external connections.

It is not always easy to define precise and useful security requirements covering all risks the application is subject to. The following guidance proposes an ad hoc taxonomy that some organizations can find helpful.

The type of a security requirement is defined by identifying the actor that requires this requirement. For example, if a security requirement specifies that a user must enter a password, this requirement

will be identified as a user requirement. If a security requirement specifies that the application should keep a log of certain critical transactions, this requirement will be identified as a system requirement.



Key

type of requirement

container (documents, diagrams, databases, etc.)

Figure 5 — Application security requirement types

As shown on Figure 5, security requirements, as is the case for software requirements, can be mapped in two categories (functional and non-functional), three levels (business, users, and functional), and can also be divided in 12 types:

1) **Business requirements** — A business security requirement addresses at least one security risk from the business context of the organization, such as: practices, the objectives of the organization, information to protect the targeted clientele, etc.

2) **Business rules** — A business security rule addresses at least one security risk from the organization's operating rules, such as directives, internal regulations, codes of conduct, etc.

3) **Regulatory requirements** — A regulatory requirement addresses at least one security risk from the regulatory context to which the organization is subject.

4) **User requirements** — A user security requirement addresses at least one security risk from the actions that can be performed by an actor in operating the application, such as: a manager, a member of technical team, an operator, a user, a listener.

5) **Qualification requirements** — A qualification security requirement addresses at least one security risk from constraints or qualifications required before an actor is allowed to perform an action in the application's development or operational environments. This type of requirements may apply to a person or a system component.

EXAMPLE 1 Before being allowed to develop a new Java component, a developer is required to possess the necessary qualifications, such as a degree in the field, a minimum number of years of experience, specific knowledge or specific professional certification.

EXAMPLE 2 Before it can be deployed in an environment, an application component is required to be certified as able to detect and respond to a distributed denial of serviceattack, attempts at unauthorized modification of data or failure of another system component.

6) **Quality** a**ttributes** — A quality attribute addresses at least one security risk concerning a threat to the achievement of quality objectives for the application, such as: reusability, usability, integrity, portability, interoperability, maintainability, etc.

7) **System requirements** — A system security requirement addresses at least one security risk from services and features offered by the application.

8) **Process requirements** — A process security requirement addresses at least one security risk brought from or impacted by any implementation or operation processes, such as development, deployment, delegation, use, maintenance, contingency and archiving processes.

9) **Functional requirements** — A functional security requirement addresses at least one security risk brought from the features that are offered by the system, such as online payment, data transfer, shopping cart, remote control, etc.

10) **External interfaces** — An external interface security requirement addresses at least one security risk from the various interfaces offered by the system such as: web interfaces and communication interfaces to other applications.

11) **Infrastructure requirements** — An infrastructure security requirement addresses at least one security risk from the physical infrastructure environment that supports the application.

12) **Constraints** — A security constraint addresses at least one security risk from restrictions imposed or required for the application. For example, the application must be accessible via the Internet, no application component should be developed in Java, or a specific activity can be carried out only by the simultaneous action of two players. Constraints can describe measurable criteria such as required performance, charge or multi-sites response-time, but also qualitative constraint such as maintainability, and usability.

To improve clarity, a security requirement should at least include the following elements:

a) the role of the actor who should perform an action (who);

b) the desired action to reduce the risk (how);

c) the moment the action should happen (when);

d) where this action will be conducted (where);

e) the information concerned by this requirement (what); and

f) risk or source of risk addressed by this security requirement (why).

In the same way that an ASC can be represented as a graph (see ISO/IEC 27034-1:2011, Figure 7), a general or high-level security requirement should generate a set of more specific security requirements.

To speed up this requirement design activity, a security requirement drafted during an application project may be replaced with an equivalent security requirement (mitigating the same security risk to an acceptable level for the project) that already exists in the ONF. The Organization ASC Library contains the information linking risks, requirements and controls (see ISO/IEC 27034-2:2015, 5.5.7).

Verifying that requirements are met is often a problem in software engineering. Verifying that application security requirements are met is much simpler. As shown in Figure 3, for achieving each requirement, one or more ASCs are selected. Verifying that those ASCs are correctly implemented ensures that the requirement is achieved.

6.2.6.7 Determination of the application's Targeted Level of Trust

Once the application security risk analysis and security requirements are defined and validated, the application's Targeted Level of Trust should be identified from those existing in the organization's ASC Library. This identification should be done by comparing security requirements produced for the application with security requirements listed in the organization's ASC Library. When two security requirements are nearly identical (assessing the same security risk to the same acceptable level), it can be decided to replace the security requirement defined for the application with the one existing in the ASC library. This ensures that similar security requirements will always be addressed with the same ASCs.

If a security requirement defined for an application has no equivalent in the ASC Library, an ASC request, which may include an ASC proposition, should be sent to the ONF committee, through the "Monitoring and reviewing the ONF" process (see ISO/IEC 27034-2:2015, 5.4.6).

Once all security requirements defined for the application are mapped to ones existing in the ASC Library, the identification of the required Targeted Level of Trust for this application will be the Level of Trust that includes at least all security requirements.

The application project team should then prepare for presentation to the application owner, for approval:

a) the list of security risks and related impacts evaluated for this application project;

b) the list of security requirements to address these security risks adequately;

c) the Level of Trust that includes ASCs addressing these security requirements, that should be targeted for this application.

The project team should present this information and other ancillary information in such a way as to help the application owner make an informed decision.

EXAMPLE The team can show links between security risks, requirements, ASCs and costs, in a tabular or graphical presentation, helping the application owner understand the impact and cost of mitigating each risk to an acceptable level and of approving the application's Targeted Level of Trust.

6.2.6.8 Application owner acceptance

The application owner has the responsibility of accepting the residual risks associated with a specific application after the risk evaluation is performed. This step corresponds to the "information security risk acceptance" step in the risk management process established by ISO/IEC 27005.

The application owner performs this acceptation in two ways:

a) by approving the application's Targeted Level of Trust in step 2 of the ASMP;

b) by approving the results of step 5 of the ASMP, in which the application's Actual Level of Trust is measured and compared to the application's Targeted Level of Trust. This step can be required at

any time by the application owner. For additional validation, the application owner can require this step to be performed by an external verification team.

The following is an example of a residual risk that the application owner may accept:

EXAMPLE Allow the "remember me" feature on the login page of the applications used by internal users.

In the above example, the application owner confirms that the risk imposed by the "remember me" feature for internal applications is at an acceptable level. The "remember me" feature introduces risks such as unauthorized access to the application should an attacker gain physical access to the victim's workstation while it is unlocked. The application owner may accept this risk, considering that the likelihood of such unauthorized physical access is low in the organization's internal office space.

Once the owner has accepted the residual risks, it is the project team's responsibility to achieve the application's Targeted Level of Trust by implementing the relevant ASCs at the appropriate stages in the life cycle.

6.3 Creating and maintaining the Application Normative Framework

6.3.1 General

The third step of the ASMP is to select all elements of the ONF which apply to a specific application project and complete the ANF for this application. The process of creating the ANF for a specific application is essential. As shown in Figure 6, the ANF is a subset or refinement of the ONF that contains only the applicable information required for a specific application, such as the application's Targeted Level of Trust, required ASCs, the application contexts (regulatory, business and technological), the actors' responsibilities and professional qualifications, and the application's specifications. This information is defined or generated through steps 1 and 2 of the ASMP and are documented and stored in the ANF.

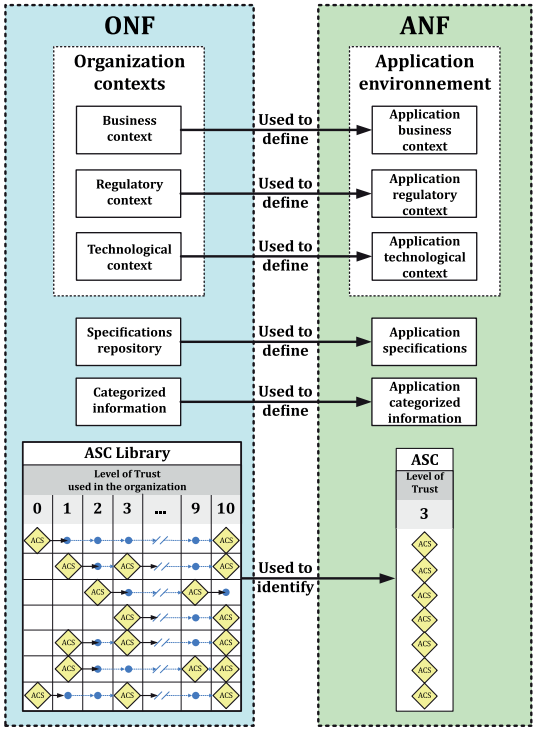


Figure 6 — Creating the ANF from the ONF

During this step, the organization should also derive the application's life cycle for the application project. The application life cycle is a subset of the Application Security Life Cycle Reference Model (see ISO/IEC 27034-1:2011, 8.1.2.7) contained in the ONF. The life cycle for the specific project will contain

only processes needed for the application project. For example, a project developed entirely in-house would not require an outsourcing process.

This step is also performed to validate that relevant elements from the ONF that apply to a specific application project are properly recorded in the Application Normative Framework (ANF).

NOTE 1 This step corresponds to the “information security risk treatment” step in the risk management process established by ISO/IEC 27005.

NOTE 2 The application's life cycle for the application project is derived from the relevant Application Security Life Cycle Model stored in the ONF. An application's life cycle model is a mapping between the ASLCRM and specific methods or process in place in the organization, such as outsourcing process, acquisition process, development process (e.g. RUP, RAD), operation and management process (e.g. SCRUM), IT management and maintenance process (e.g. ITIL), (see ISO/IEC 27034-2:2015, 5.5.10).

6.3.2 Purpose

The purpose for establishing this step is to manage and maintain the content of the ANF throughout the life cycle of a specific application by revisiting, validating, importing and consolidating relevant elements from the ONF, including:

a) ASCs identified by the application's Targeted Level of Trust;

b) information produced at different steps of the ASMP;

c) the application's life cycle.

NOTE This step corresponds to the “Preparing and implementing risk treatment plans” part of the “risk treatment” step in the risk management process established by ISO/IEC 27005.

6.3.3 Outcomes

The principal outcomes of this step include:

a) a full ANF updated and released, containing all the necessary elements to secure the application;

b) an application life cycle for the application project;

c) applicable ASCs for the application project.

6.3.4 Realization activities

Table 7 shows roles and responsibilities for carrying out realization activities for process "Creating and maintaining the Application Normative Framework".

Table 7 — RACI chart for process “Creating and maintaining the Application Normative Framework”

Realization activities	Project manager	Project team	Application owner
1) Identify and select processes and key activities from the ONF to establish the ANF.	A	R	C
2) Check the alignment of the internal Application Security Life Cycle Models used in this application project, with corresponding ASLCRM stages and activities.	A	R	C
3) Import into the ANF required processes and ASCs identified by the Level of Trust assigned to the application.	R	I	A
4) Maintain and communicate the ANF to the persons concerned.	A	R	I

6.3.5 Verification activities

Table 8 shows roles and responsibilities for carrying out verification activities for process "Creating and maintaining the Application Normative Framework".

Table 8 — RACI chart for verification of process "Creating and maintaining the Application Normative Framework"

Verification activities	Project manager	Auditors
1) Ensure that the Application Normative Framework was defined.	I	A/R
2) Ensure that the application life cycle for the application project was derived.	I	A/R
3) Ensure that security controls for the application project were selected.	I	A/R
4) Ensure that the content of the ANF was validated and signed off by the application owner.	I	A/R

6.3.6 Guidance

6.3.6.1 General

The activities needed to ensure that application requirements and environment were effectively identified include:

a) establish the ANF

Information from the ONF that influences the application development project should be recorded in the ANF.

This information should be derived, at least, from: application Targeted Level of Trust, the application contexts (regulatory, business and technological), the actors' responsibilities and professional qualifications, the application specifications, design requirements, as well as processes related to the definition, management and verification of application security.

The ANF for an application project evolves throughout the lifetime of the application. At the inception of an application project an initial ANF is created. This initial ANF is then enhanced as more knowledge is gathered throughout the application project.

b) derive the application's life cycle

Application Security Life Cycle Reference Model (ASLCRM), contained in the ONF, should be analysed to specify the application life cycle for the application project. That is, an instantiation of ASLCRM is prepared and transformed in a specialized application security life cycle that contains necessary and detailed information (processes) for the application project.

c) select security controls for the application project — ASCs are copied from the ONF to the ANF

Based on application Targeted Level of Trust, organization's needs for application, and application's specific contexts and specifications, applicable security controls for the application project should be selected.

NOTE ASCs can be updated for this application only under Application owner and ONF committee approval.

d) ensure that application security was specified considering supporting documents, such as regulatory or software requirements specification;

e) ensure that flows of information were detailed;

f) ensure that application technological, business and regulatory context were identified;

g) identify whether the actors were involved in the realization process;

h) verify that all relevant information produced was recorded to create the ANF;

i) preserve the results of the verification process in the ANF.

Verification of the components in the ANF should be performed:

a) before the major gates in the application project;

b) when the technological, business or regulatory context has changed;

c) at periodic audits.

It is recommended that the responsibility for the verification of the ANF is described by a RACI similar to Table 8.

6.3.6.2 Application Security Processes

Relevant processes related to the definition, management and verification of application security should be included in the ANF. This is a refinement of the "Processes related to application security" component of the ONF. Some examples of these processes are: vulnerability testing procedures, code review procedures, incident response plans, etc.

In order to ensure that the ANF for a specific application is complete and up to date and accurate it is recommended that responsibilities are defined for the different components of the ANF.

6.3.6.3 Processes related to the ANF

The organization should define and document processes for creating, approving and maintaining the ANF. Roles, responsibilities and required professional qualifications for actors involved in the organization's ANF for the specific application should be specified. While ASCs in the ONF are linked to stages of the Application Security Life Cycle Reference Model, ASCs in the ANF are linked to stages in the life cycle for the specific application project.

ISO/IEC 27034-1:2011, 8.1.2.7.1 states that there should be a persistent mapping between the processes in the Application Life Cycle Security Reference Model and the processes in every life cycle in use in the organization.

The ANF creation process defines a specific Application Security Life Cycle for the application project by selecting relevant processes and actors from the ONF. The ANF creation process also selects ASCs from the ASC library, according to the application Targeted Level of Trust accepted by the application owner.

Organizations should validate the ANF and have it signed off by the application owner after the validation is complete.

6.4 Provisioning and operating the application

6.4.1 General

Step four of the ASMP involves the use of the ASCs provided by the ANF for the specific application in its life cycle. For example, an organization may decide to develop, acquire and/or operate an application. This ASMP step should be applied to both provisioning and operation application life cycle stages and help to integrate ASCs identified by the targeted Level of Trust to any existing application processes or components. This step also includes verifying all ASC activities have been integrated into the life cycle of the application.

At this step, the project and verification teams are supplied with the ASCs associated with the Targeted Level of Trust for their project. ASCs are also used by the verification team as they provide detailed

information about what verification measurements should be performed to provide evidence that security activities have been performed correctly and produced the expected results.

Figure 7 presents key actors who may perform security activities from ASCs.

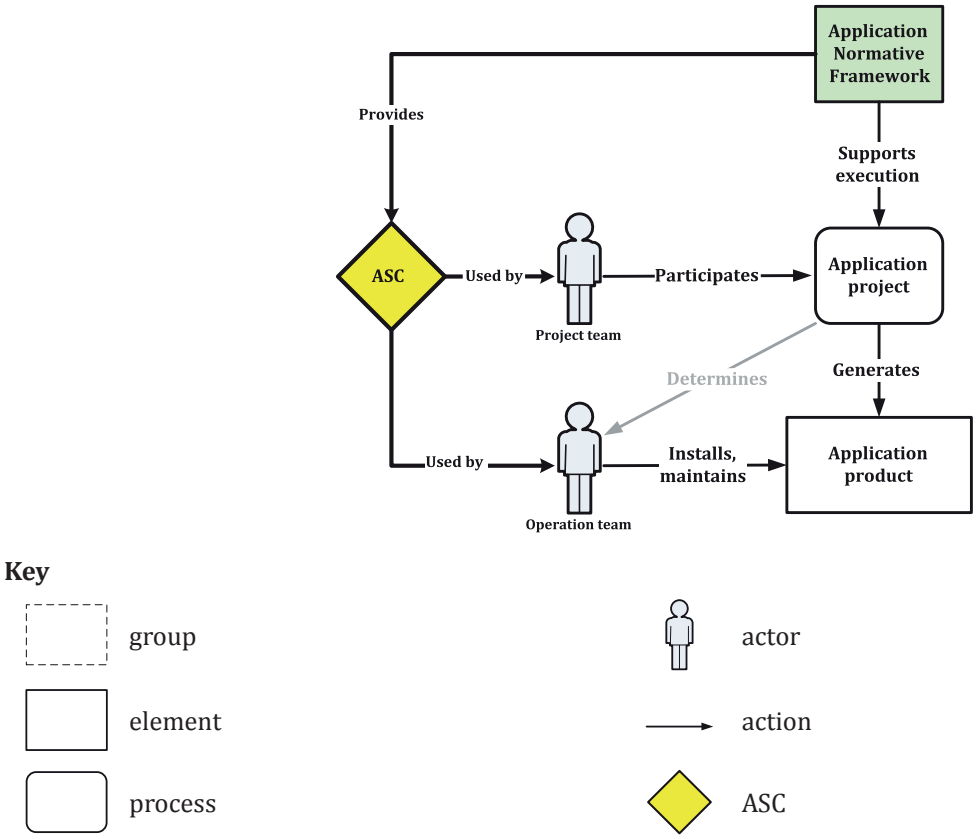


Figure 7 — ASC used to implement a security activity

Project managers should find detailed information in the ASC, such as the required tasks, resources and qualifications, the cost per task in days-person and the exact stage in the life cycle at which each task should be performed.

NOTE 1 This step corresponds to the "information security risk treatment" step in the risk management process established by ISO/IEC 27005.

NOTE 2 Secure application life cycle management systems can be optionally used by the project and verification teams to manage and track security activities outlined in the ASCs throughout the application life cycle.

6.4.2 Purpose

The objective of the implementation of this process is to establish the elements of ANF that are relevant to the steps, phases and activities covered by the project.

The project team implements the ASCs from the ANF:

a) the security activity part of each ASC is realized by the actor identified in the ASC; and

b) the security measurement part of each ASC is realized by the actor identified in the ASC.

6.4.3 Outcomes

As a result of the successful performance of this process, the following information should be produced:

a) a list of completed ASC and the results produced by their implementations;

b) the application artefacts, including an updated ANF;

c) feedback to the ONF management process if applicable;

d) knowledge of any gaps between the Targeted Level of Trust and the Actual Level of Trust, as an outcome of step 5;

e) the reports and results of the audit of each application's ASC including in particular the scope of the audit, the status of each ASC, shortcomings and possible solutions to address them, including:

   1) results of implementing the security activities of ASCs associated with the Targeted Level of Trust for the application project;

   2) results of verification measurements performed based on the use of the ASCs in the application project;

f) the Actual Level of Trust for the application, as an outcome of step 5;

g) a prototype of the application (functional subset of the application) or the entire application, depending on the iteration in the life cycle, with corresponding ASCs implemented and verified.

6.4.4 Realization activities

Table 9 shows roles and responsibilities for carrying out realization activities for process "Provisioning and operating the application".

Table 9 — RACI chart for process "Provisioning and operating the application"

Realization activities	Project Manager	Project Team	Application owner	Auditors
1) Conduct detailed application security risk analysis of the application.	A/R	R	C	I
2) Implement the security activity of every ASC.	A	R	I	I
3) Implement the verification measurement of every ASC.	C	C	I	A/R
4) Provide feedback to the ONF management process as needed.	A/R	I	I	I

6.4.5 Verification activities

Table 10 shows roles and responsibilities for carrying out verification activities for process "Provisioning and operating the application".

Table 10 — RACI chart for verification of process "Provisioning and operating the application"

Verification activities	Managers	Auditors
1) Ensure that the organization has a list of security activities of ASCs associated with the Targeted Level of Trust for the application project.	I	A/R
2) Ensure that security activities of this list were performed.	I	A/R
3) Ensure that the organization has a list of verification measurement activities that is part of ASCs.	I	A/R
4) Ensure that measurement activities of this list were performed in the course of an application project.	I	A/R
5) Ensure that a prototype of the application with corresponding ASCs was implemented and verified.	I	A/R

6.4.6 Guidance

6.4.6.1 General

Should the project team determine, while performing this step of the ASMP, e.g. while performing a detailed risk analysis or detailed architecture, that ASCs in the ANF need to be adapted, corrected or otherwise modified, or that new ASCs are needed for correctly addressing a security requirement for the application, it should communicate this need to the ONF management process, so that the required changes be performed in a manner acceptable for the organization.

Figure 1 illustrates this communication as an arrow labelled "Provides feedback to". ISO/IEC 27034-2:2015, Figure 1 shows that this communication is targeted more precisely at the "Monitoring and reviewing the ONF" sub process. ISO/IEC 27034-2:2015, 5.4.6.5 states, with examples, that "Feedback from application projects should also be used as an important input with regard to continuous improvement of quality and effectiveness of ASCs deployed in projects".

Some organizations may find acceptable that project teams provide in this communication a proposition for an updated or new ASC, especially if the required specific expertise for such work currently resides in the project team; other organizations may not. In any case, new or updated ASCs are made available to the organization's project teams as an outcome of the "Improving the ONF" sub process of the ONF management process (see ISO/IEC 27034-2:2015, 5.4.7.2).

NOTE Some guidance on realizing and operating the application is provided in Annex A.

6.5 Auditing the security of the application

6.5.1 General

The fifth and final step of the ASMP is to verify the application security, i.e. to verify the verification measurement activity outcomes of every ASC specified in the Target Level of Trust that should be implemented in the application. The results produced by these ASC verification activities provide evidence that applicable ASCs at time of the verification have been implemented as expected. This step of the ASMP can be performed at any time during the application's life cycle. Depending on the application's Targeted Level of Trust, this step can be one-off, periodic or event-driven.

This process results in the Actual Level of Trust at a given time. The application is considered secure when the Actual Level of Trust is equal to or exceeds the corresponding Target Level of Trust approved by the owner of the application at a given time.

The verification measurement part of the ASCs specifies security activities that should be verified to provide evidence that the activity was performed correctly, by a qualified actor, and produced the expected results.

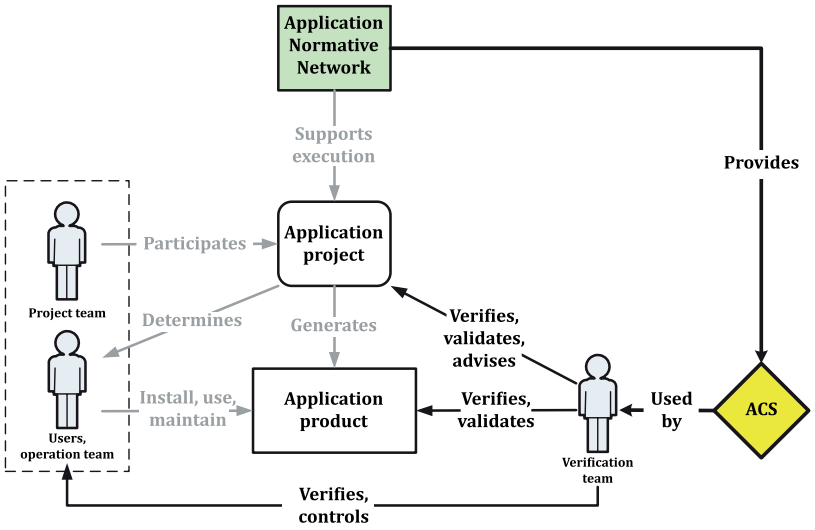


Figure 8 — ASC used to implement a verification-measurement activity

Figure 8 shows that the verification measurement part of an ASC is used as a control gate in an application project's life cycle for the verification team to verify and validate the application and the project, and provide advice to the application owner so that he can decide to authorize whether the application project should proceed to its next step of execution. For example, an ASC can require that a server clustering service be used to ensure the application availability. The verification measurement part of the ASC verifies that such a service was indeed implemented.

Figure 8 also shows that the verification measurement part of an ASC can be used to verify the qualifications of actors who performed the processes in the application life cycle. For example, an ASC can require that a senior developer implements an application critical component. The verification measurement part of the ASC verifies the qualifications of the developer who did implement the component.

By the end of this step, an organization can claim an application as "secure" when its Actual Level of Trust is equal to its Target Level of Trust. It keeps its status of being claimed "secure" until the next mandated verification, whether it is a periodical audit required by the ASMP or some other verification required by the organization.

NOTE 1 Despite the name given to this step, its purpose and description as provided by this document make it more closely related to the concept of Application Security Review than to the concept of Application Security Audit (see 3.1). "Reviewing the security of the application" would be a better name for this step. The current name however is kept in order to maintain consistency with ISO/IEC 27034-1.

6.5.2 Purpose

The purpose of the fifth ASMP step is to verify and formally record the supporting evidence of whether or not a specific application has attained and is maintaining the application's Targeted Level of Trust at a specific time.

6.5.3 Outcomes

The principal outcomes of this step are:

a) results of performing an application security review process that demonstrate that all verification measurements provided by all the ASCs in the ANF for the specific application have been performed and that the results were verified;

b) indication of the application's Actual Level of Trust at a specific time;

c) evidence of whether or not a specific application has attained and is maintaining its Targeted Level of Trust at a specific time;

d) results of verification and recorded evidence about attaining and maintaining the Targeted Level of Trust at a specific time.

6.5.4 Realization activities

Table 11 shows roles and responsibilities for carrying out realization activities for process "Verifying the security of the application".

Table 11 — RACI chart for process "Verifying the security of the application"

Realization activities	Managers	Auditors
1) Ensure that all ASCs associated with the Targeted Level of Trust were imported into the ANF and implemented in the application.	I	A/R
2) Verify the Actual Level of Trust of the application to the corresponding Targeted Level of Trust.	I	A/R
3) Record the supporting evidence of whether or not a specific application has attained and is maintaining the application's Targeted Level of Trust at a specific time.	I	A/R
4) Ensure that verification activities of ASCs present in the ANF were implemented and that expected results were obtained and verified.	I	A/R
5) Measure the application's Actual Level of Trust.	I	A/R

6.5.5 Verification activities

Table 12 shows roles and responsibilities for carrying out verification activities for process "Verifying the security of the application".

Table 12 — RACI chart for verification for process "Verifying the security of the application"

Verification activities	Managers	Auditors
1) Ensure that the results of an application security review process demonstrate that all verification measurements provided by all the ASCs in the ANF for the specific application have been performed and that the results were verified.	I	A/R
2) Ensure that the application's Actual Level of Trust at a specific time was measured.	I	A/R
3) Ensure it was informed whether or not a specific application has attained and is maintaining the application's Targeted Level of Trust at a specific time.	I	A/R
4) Ensure results of verification, and evidence about attaining and maintaining the Targeted Level of Trust at a specific time, were recorded.	I	A/R

6.5.6 Guidance

For an organization, this will be the process used to determine if all ONF elements identified by an authority have been implemented and successfully pass their verification process.

For an application, this will be the process used to determine if all ASCs identified by the Targeted Level of Trust have been implemented and successfully pass their verification process.

This step may be performed by an internal or an external verification team. 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.

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 or those providing certification.

To ensure that no elements' verification outcomes have been forged, an application security auditor may choose to verify again selected elements included in the scope of an application security certification.

Defining the scope of an application security review or audit is often problematic. ISO/IEC 27034 (all parts) helps solve this problem: the maximum scope of an application security review or audit is the verification activities from the ASCs contained in the application's ANF.

The verification team and the security team may find the ASC concept useful because each ASC for a specific application provides detailed information on the security activity and the corresponding verification measurement. According to ISO/IEC 27034-1:2001, 8.1.2.6.5.4, verification procedures and expected results are specified in the "verification measurement" part of the ASC.

Application project management may find the ASC concept an efficient tool for addressing application security. An ASC details the required verification tasks, the needed professional resources with specific qualifications, the estimated cost, for example, in person-days for the verification measurement tasks and the exact stages in the application life cycle at which the verification measurement activities should be performed.

This process can also be used by the audit process and certification to retest ASCs of an application, and is the "information security risk treatment" step in the risk management process established by ISO/IEC 27005.

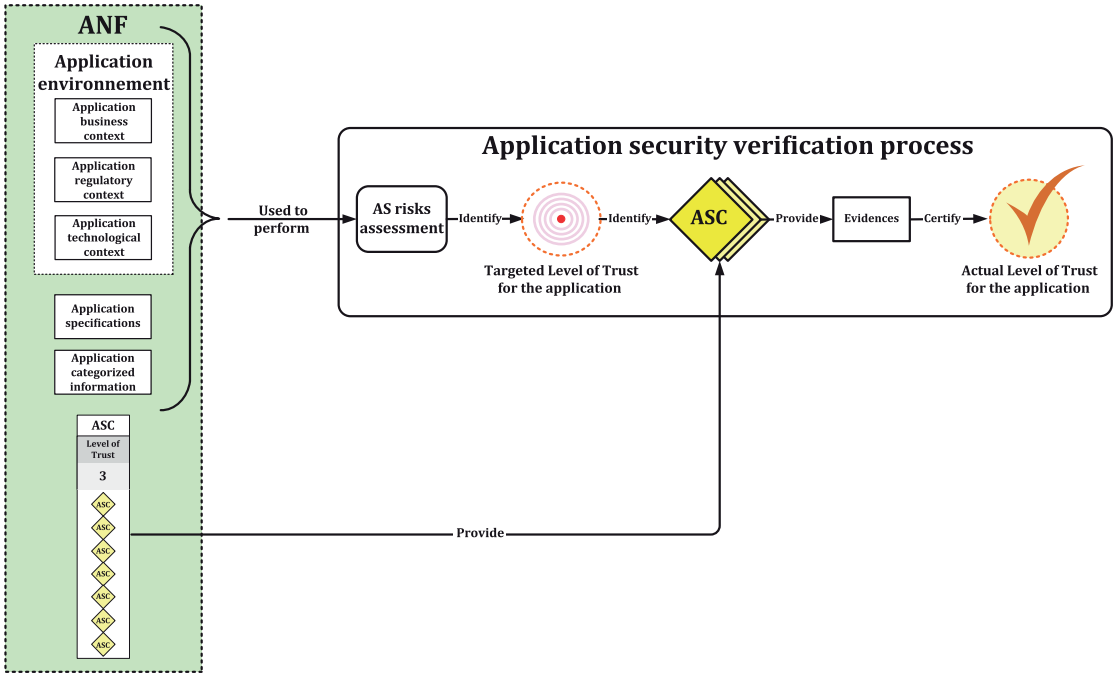


Figure 9 — Application security verification process

Figure 9 illustrates key steps of the application security verification process that need to be performed to measure an Actual Level of Trust for an application. This process includes the following activities:

a) identify and validate ANF elements from the ONF;

b) identify and assess security risks brought by the application;

c) identify and validate application security requirements including minimum security objectives required for the application;

d) identify and validate the target level of trust for the application, that meets all identified security requirements;

e) validate the Target Level of Trust with application owner approval;

f) perform ASCs verification-measurement activities;

g) update the ANF.

An organization can declare an application "secure" when its Actual Level of Trust is equal or greater to its Targeted Level of Trust.

NOTE This step corresponds to the "information security risk acceptance" step in the risk management process established by ISO/IEC 27005. This risk acceptance is performed both before and after the realization of the application project, in steps 2 and 5 of the ASMP.

7 ANF elements

7.1 General

7.1.1 Purpose

The Application Normative Framework (ANF) is the authoritative source for the detailed information required for a specific application to reach its application Targeted Level of Trust.

It provides the history of the elements, decisions and results accumulated during the application's life cycle.

7.1.2 Description

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. Therefore, the ANF is a subset or refinement of the ONF.

The ANF for a specific application project contains components as detailed below. Figure 10 shows a graphical representation of the ANF.

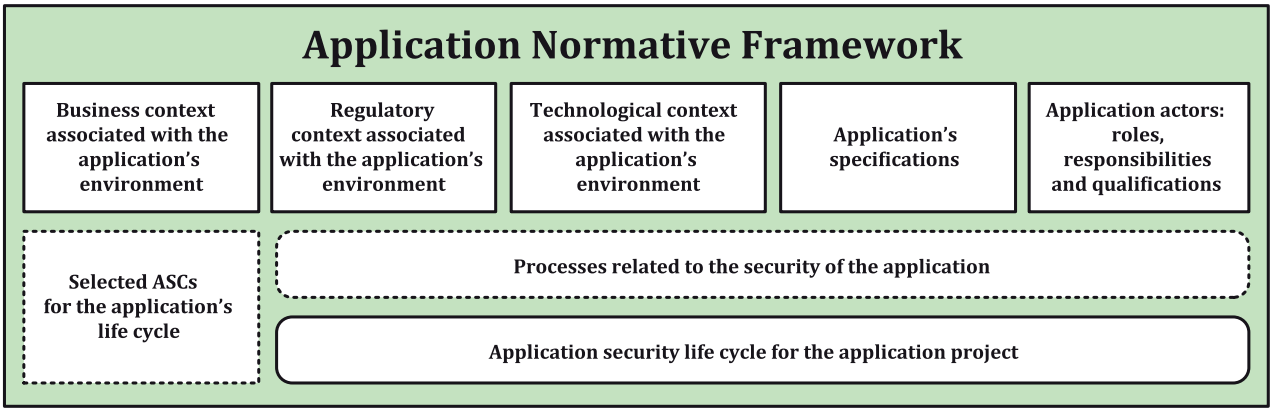


Figure 10 — Application Normative Framework

This ANF exists and may evolve during the entire life cycle of the application. For example, the regulatory context for the application may change, or the application owner may give the application

project team a new Targeted Level of Trust for the application. In such cases, new elements can be added to or removed from the ANF by the organization.

Changes to the ANF may have an impact on the security of the application. These changes should have their corresponding approvals from the application owner.

The ANF for a specific application project contains various components that are defined in the rest of this Clause 7.

7.2 Component: Application business context

7.2.1 Purpose

This component is used to store business elements defined, identified and addressed by an application project. It introduces an approved standardized approach for mitigating risks associated with the application's business context during its security life cycle. It describes the business choices that are applicable to the target application. The business properties of the application determined in this step are used to look up specific portions of the ONF when compiling the ANF.

7.2.2 Description

The application's business context is a documented inventory of all business processes, standards and best practices related to an application project, mainly coming from the ONF. Realizing and operating an application may cause risk. An organization should assess risk, define security requirements and identify ASCs for mitigating these risks. ASC implementers need to know why an ASC is being provided, i.e. what security requirement the ASC is addressing. They should find this required information in the business context component of the ANF.

7.2.3 Contents

The business context should provide:

a) a list of all business lines pertaining to all parts of the organization in which the application will run or will be used;

b) documents or data presenting business realities, constraints and ways of doing things in this organization and its business lines, such as processes to operate the application, business processes adapted for the application, including business line's directives and internal regulations;

c) for each business line, a list of processes, policies and best practices, that pertain to the usage of the application in that domain, such as:

   1) business, project management, development, risk analysis, operational, audit and control and change management processes;

   2) parts of the organization's security policy relevant to the application project;

   3) a list of the organization's relevant information assets with their security classification;

   4) the development methodology used in the application project;

   5) best practices for programming languages, maintenance, support or contingence processes employed in the application project and listed in the technological context;

   6) standards relevant to the application project, such as ISO/IEC International Standards and industry standards, to which the organization mandates compliance;

d) a list of risks introduced by the above processes, policies and best practices, that are relevant to the security of this application;

e) a list of security requirements for mitigating the above risks;

f) a Targeted Level of Trust and an Actual Level of Trust;

g) a list of ASCs that should be implemented and verified, including their outcomes.

The business context includes a description of what the application is intended to do and how it is supposed to do it.

7.2.4 Guidance

Business functionality within the activities of a process should be worked out and defined as elementary requirements for the application.

Within the business functionality control scenarios should be defined as a requirement.

7.3 Component: Application regulatory context

7.3.1 Purpose

This component is used to store relevant legal and regulatory requirements applicable in the location(s) where the application is used or deployed. It provides justifications for some of the application's security requirements and ASCs.

7.3.2 Description

The regulatory context of the application refers to all laws, regulations and common rules stemming from the territory or jurisdiction, which can impact the application's realization, operation or its utilization of data (e.g. privacy laws, risks stemming from the different national laws in countries where the same application is in use).

7.3.3 Contents

The regulatory context should provide:

a) a list of laws and regulations applicable in the location(s) where the application is used or deployed;

b) a list of risks brought by the above laws and regulations, that are relevant to application security; and

c) a list of security requirements for mitigating the above risks.

7.3.4 Guidance

Periodic review of legal and regulatory controls is required to keep current with industry standards and technology updates to protect consumer's PII data.

The determination of what regulatory specifications are applicable to the application is based on the following examples.

a) Users of the application: For example, if children under certain age are the target users of the application, certain regulations may be applicable to the application.

b) Data handled by the application: For example, certain financial data such as credit card information have regulatory specifications governing the handling and management of the data.

c) Business context of the application: For example, publicly traded companies are subject to certain financial accuracy regulations that can affect applications that handle transactions in the organization.

d) Geographic context: There are several aspects of the location that affect the regulations the application is subject to. For example, the location of the organization operating the software, and

the location of the target audience and the location data are stored each can have a different impact based on the regulatory context.

Other examples:

a) data are personal data and data related to products that have export restrictions;

b) personally Identifiable Information (PII) data which are governed in several countries by privacy or data protection laws.

See ISO/IEC 27034-2:2015, 5.5.3.4 for more guidance about this component.

7.4 Component: Application technological context

7.4.1 Purpose

This component helps to determine security risks coming from the application's technological infrastructure. It provides information as to what IT components may be used in support of ASCs that require such support.

7.4.2 Description

The technological context is a documentation of the application's IT components (e.g. physical components, applications, services including their configuration and parameters) and the organization's own best practices and rules which apply to the use of such components.

7.4.3 Contents

The technological context should provide:

a) a list of IT components used in the application that are relevant to application security;

b) a list of risks brought to the application by the above IT components;

c) a list of security requirements for mitigating the above risks.

The technological context includes information about how an application is developed (e.g. in-house, outsourced, hybrid), how an application is acquired (e.g. COTS, custom, open source, hybrid), and how an application is deployed (e.g. private data centre, public cloud, customer premise, hybrid). It should include a description of the application hardware and components (database servers, application servers, etc.) and the programming languages, framework(s), open-source, or third party products used for the application. Each of these will specify the application's methods for achieving the agreed SLA and should be considered when ASCs are being chosen and implemented.

7.4.4 Guidance

The technological context component provides the technological description and requirements for an application. It gives specification to the availability, integrity and confidentiality of the data used by the application. This will establish a service level agreement (SLA) the application will have with the organization.

The application's SLA will define the technological methods used to satisfy those requirements.

EXAMPLE Clustering software on virtual servers using redundant hardware components that access highly dependable storage that have very built-in redundancy for off-site storage replication for disaster recovery processes.

The ONF committee will help define the business requirements around availability, integrity, and confidentiality of the data used by the application.

The application's technological context is derived or refined from the organization's ONF technological context and it includes all technological components of the application, such as its architecture, infrastructure, protocols and programming languages.

The technological context portion of the environment for the application specifies the technological stack and/or infrastructure that application is built on, uses, or interacts with. This portion of the application's specification will be used in the future steps of the ASMP to determine applicable Application Security Controls (ASCs) from the Organization Normative Framework (ONF) and include the resulting matches in the Application Normative Framework (ANF).

In addition, the technological context allows specific training material to be included in the ASC that demonstrates the development and testing guidelines for each requirement in the technological context the application is using.

7.5 Component: Application specifications

7.5.1 Purpose

This component is used to store information helping to determine and mitigate security risks coming from the application's specifications, and to mitigate the risk of incorrectly implementing and/or misusing these specifications.

7.5.2 Description

The application specifications component is a documentation of the application's general IT functional requirements. It should include all specifications, functionalities and services included in or offered by the application, including documents and best practices to implement, use and verify them.

Application specifications take the form of functional, non functional and security requirements.

The security specifications and specifications that affect security are of special importance to the ASMP. Examples of security specifications are minimum security requirements such as password storage, transfer, and configuration and session management controls. Examples of specifications that affect security are requirements on how the end-users and application-tiers authenticate to each other.

7.5.3 Contents

The application specifications repository should provide:

a) a list of all application specifications included in or offered by the application;

b) for each specification, a list of processes and best practices approved by the organization, that pertain to its implementation, use, maintenance or verification;

c) a list of risks brought to the application by the above specifications;

d) a list of security requirements for mitigating the above risks.

7.5.4 Guidance

The application specifications detail the steps required to complete each function of the application. In addition, all data used, stored, processed, shared or transferred by the application should be listed and categorized. This includes all input and output data, configuration data, application data, and user data.

Information for building this ANF component should be obtained from the documented architecture of the application.

Whenever possible, the application's specifications should be linked with the organization's pre-approved solutions available in the ONF "application specifications repository" component. Pre-approved solutions are often processes, products or code libraries that the organization makes

recommended or mandatory practice through rules, policies or enterprise architecture within a specific environment. Such solutions are typically mature and continuously improved. The advantage of reusing such solutions in application projects is obvious.

See ISO/IEC 27034-2:2015, 5.5.5.4 for more guidance about this component.

7.6 Component: Application's actors: roles, responsibilities and qualifications

7.6.1 Purpose

This component helps to determine and mitigate security risks coming from the people involved with the application. It also helps to ensure that all critical roles for all processes are filled, that all responsibilities are defined, that conflicts of interest are avoided, and that people assigned to the roles have sufficient professional qualifications.

7.6.2 Description

This component is a documentation of roles, responsibilities and required qualifications for actors involved with the application.

7.6.3 Contents

This list of roles originates from ISO/IEC 27034-5:2017, 6.6.

a) Any role	All actors and stakeholders listed below belong to this role.
b) Acquirer	An individual who acquires or procures a product or service from a supplier. The actors playing this role are members of the Business Management group.
c) Application architect	An individual responsible for defining the application architecture, which includes making the key technical decisions that constrain the overall design, maintenance and its implementation. The actors playing this role are members of the Development Team group.
d) Application administrator	An individual responsible for the parameterization and granting access to the application. The actors playing this role are members of the IT Management group.
e) Application operator	An individual responsible to run and manage an application. NOTE Application operator can be responsible to manage application user's rights, application's functionalities and interfaces (e.g. sysop, sysadmin).
f) Accountable management	The highest ranking executives responsible for application security in the organization. The actors playing this role are members of the Executive Management group.
g) Auditor	An individual who conducts an official, systematic security inspection of an application. The individual playing that role can be member of an internal (conducting internal audit) or external (conducting external audit) experts group.
h) Chief Security Officer (CSO/CISO)	An individual responsible for defining and maintaining security controls in the organization. The actors playing this role are members of the Executive Management group.

i) Developer	An individual responsible for developing a part or a complete application such as designing, prototyping, implementing, unit-testing and integrating components in the solution. The actors playing this role are members of the Development Team group.
j) Domain expert	An individual who is familiar with a domain and can provide detailed information about the domain. The actors playing this role are members of the External experts group.
k) IT infrastructure administrator	An individual responsible for the parameterization and granting access to the application's infrastructure. The actors playing this role are members of the IT Management group.
l) IT infrastructure architect	An individual responsible for designing the technological infrastructure required to provide service. The actors playing this role are members of the IT Management group.
m) IT Infrastructure expert	An individual responsible for implementing and maintaining a technological infrastructure. The actors playing this role are members of the IT Management group. e.g. Agents, operators, support personnel, administrators of the applications, system administrators for which the application is running on, disaster recovery teams and processing and infrastructure security teams.
n) Laws and regulations expert	An individual who is familiar with the Laws and regulations domain and can provide detailed information about the domain. The actors playing this role are members of the External experts group.
o) Manager	An individual responsible for planning and directing the work of a group of individuals, monitoring their work, and taking corrective action when necessary. The actors playing this role are members of the Business Management group. e.g. Business continuity
p) Information owner	An individual accountable for defining, maintaining and approving the secure utilization of the information under their responsibility. The actors playing this role are members of the Business Management group. NOTE The same information can be used by multiple applications and it is important that the information protection in various applications are approved by the information owner in addition to the application owner.
q) Application owner	An individual accountable for defining, maintaining and approving the secure utilization of the application under their responsibility. The actors playing this role are members of the Business Management group.
r) Process owner	An individual accountable for defining, maintaining and approving the secure utilization of the process under its responsibility. The actors playing this role are members of the Business Management group.
s) Project manager	An individual responsible for planning and coordinating the resources needed by a project to reach its goal, within the predicted cost, time and quality estimates. The actors playing this role are members of the Business Management group.
t) Security architect	An individual responsible for designing security controls to mitigate security risks to an acceptable level. The actors playing this role are members of the Development Team group.

u) Supplier	Organization or individual that enters into an agreement with the acquirer for the supply of a product or service. The actors playing this role are members of the Business Management group and may be supported with representatives of External experts group.
v) Tester	An individual responsible for implementing and realizing tests to ensure that deployed releases and the resulting services meet expectations. The actors playing this role may be members of the development, quality assurance or IT security testing group.
w) Trainer	An individual who trains people. The individual playing that role can be member of an internal or external experts group.
x) User	An individual who performs one or more tasks with an application. The actors playing this role are members of the Users group.

7.6.4 Guidance

7.6.4.1 General

Information for building this component should come from the application's business architecture. .

At a minimum, each ANF should include the application owner. All other actors who interact with the application during its life cycle should be determined. For every applicable actor, the expected roles, responsibilities and qualifications should be specified. Information about required qualifications should come from the “Roles, responsibilities and qualifications repository” ONF component.

Actors are persons or automated processes that perform an activity during an application's life cycle or initiate interaction with any process provided by or impacted on by an application.

Additional actors may be recorded in the ANF. The following provides a non-comprehensive list of common roles and persons that are involved (interacting directly or indirectly) with applications:

7.6.4.2 Project team

The project team comprises persons involved in the application project during the provisioning stages or the operation stages of the application life cycle, such as architects, analysts, programmers and testers.

These persons are also responsible for selecting elements from the ONF to create or maintain the Application Normative Framework for the application project.

7.6.4.3 Operation team

The operation team comprises persons involved in the management and maintenance of the application during the operation stage of the application life cycle, such as system administrators, database administrators, network administrators or technical personnel.

7.7 Component: Selected ASCs for the application's life cycle stages

7.7.1 Purpose

This component documents security controls selected for the application, in order to facilitate their approval, usage, verification and communication.

7.7.2 Description

Application security controls are methods, processes and/or procedures used to mitigate risk introduced into the organization by adding the specific application.

7.7.3 Contents

This component should provide a list of ASCs selected for the application. Each ASC contains detailed information. ISO/IEC 27034-1 and ISO/IEC 27034-5 shall be referred to for details.

7.7.4 Guidance

The application needs to be continually monitored for risk throughout the life cycle of the Application. All risks need to be identified and mitigated according to the Targeted Level of Trust.

Through steps 1 and 2 of the ASMP, the application ASCs are selected from the organization ASC library for a specific application according to the following criteria:

a) the application's Targeted Level of Trust;

b) the organization's requirements for the application;

c) the application's specific contexts and specifications.

The ANF stores and documents the applicable ASCs.

Each ASC provides a security activity that should be performed by the application project team to mitigate a specific security risk. It also provides a verification measurement performed by the verification team to confirm that the corresponding security activity has been successfully carried out by examining the supporting evidence. Each ASC also provides pointers to specific stages in the application life cycle where said activity and measurement is to be performed.

ASCs are defined and approved by the organization prior to development. Developers no longer need to design them for each new application project. This ensures a consistent approach by the organization in addressing application security requirements.

Selected ASCs should include at a minimum all the ASCs that the ONF committee has authorized for level zero of trust, which is defined as the minimum level of trust the organization accepts. The ASCs authorized for level zero of trust should not be changed by the project team in the course of an application project.

7.8 Processes related to the security of the application

7.8.1 Purpose

The purpose of this ANF component is to help the project team define, manage and verify the security of the application.

7.8.2 Description

These processes help the project team integrate security activities into the life cycle processes they are already familiar with.

7.8.3 Contents

This component describes application-level processes such as:

a) application security processes (see 6.3.6.2);

b) processes related to the ANF (see 6.3.6.3).

7.8.4 Guidance

When building the ANF, relevant processes should be selected from the ONF and imported in the ANF. This ensures each application project's processes comply with organization requirements and are normalized throughout the organization.

7.9 Component: Application life cycle

7.9.1 Purpose

The purpose of this component is to allow the project team to seamlessly integrate security activities and verification measurements defined in ASCs with activities occurring during the life cycle of the application, with which the project team is already familiar.

7.9.2 Description

The application life cycle is a subset of the Application Security Life Cycle Reference Model (see ISO/IEC 27034-1:2011, 8.1.2.7) contained in the ONF. The life cycle for the specific project will contain only processes needed for the application project. For example, a project developed entirely in-house would not require an outsourcing process.

7.9.3 Contents

This ANF component should provide a mapping of the application's life cycle with the Application Security Life Cycle Reference Model.

7.9.4 Guidance

It is usual practice in organizations that different life cycle models are used by different development teams, in different parts of the organization, in different projects.

For this reason, ASCs, which in the ONF make references to activities from the standardized Application Security Life Cycle Reference Model, should be “translated” before being communicated to project teams, so that they can be integrated with each team’s familiar life cycle model and activities. The ONF contains this translation (also called “mapping”) for each of the organization's life cycle models (see ISO/IEC 27034-2:2015, 5.5.10).

The mapping provided by this component is used for this purpose. It can be as simple as the “Enumeration types” tables provided in ISO/IEC TS 27034-5-1.

When building an application's ANF, the relevant mapping is then instanciated into the ANF, keeping only the life cycle stages and activities relevant to the particular application project.

The application life cycle and its standard counterpart the Application Life Cycle Security Reference Model have already been discussed in ISO/IEC 27034-1:2001, 8.1.2.7. It is in the various processes in the application security life cycle, which the execution team and the verification team are already familiar with, that the activities and measurements defined by the ASCs are performed. This presents a process-oriented view of application security activities and controls with their interdependencies. The preferred approach is thus to smoothly integrate ASCs as integral parts of the application life cycle, rather than as security activities distinct from the life cycle.

7.10 Information involved by the application

7.10.1 Purpose

The purpose of this ANF component is to facilitate the security categorization of the application's information/data, allowing the project team to map the flow of critical information and to perform an application security risk assessment.

7.10.2 Description

Based on the classification of the application's information/data, access management of the data is defined for each established role.

7.10.3 Contents

A description of each of the application's relevant information group (see 7.10.4) with metadata describing the information's security categorization as regards to confidentiality, integrity and availability.

7.10.4 Guidance

Understanding the information that flows within an application is a key step in deriving security requirements. Information is derived from various sources. This subclause addresses all information involved by the application, including contexts description, processes description, application code, application parameters, user data, etc. All this information should be identified and categorized.

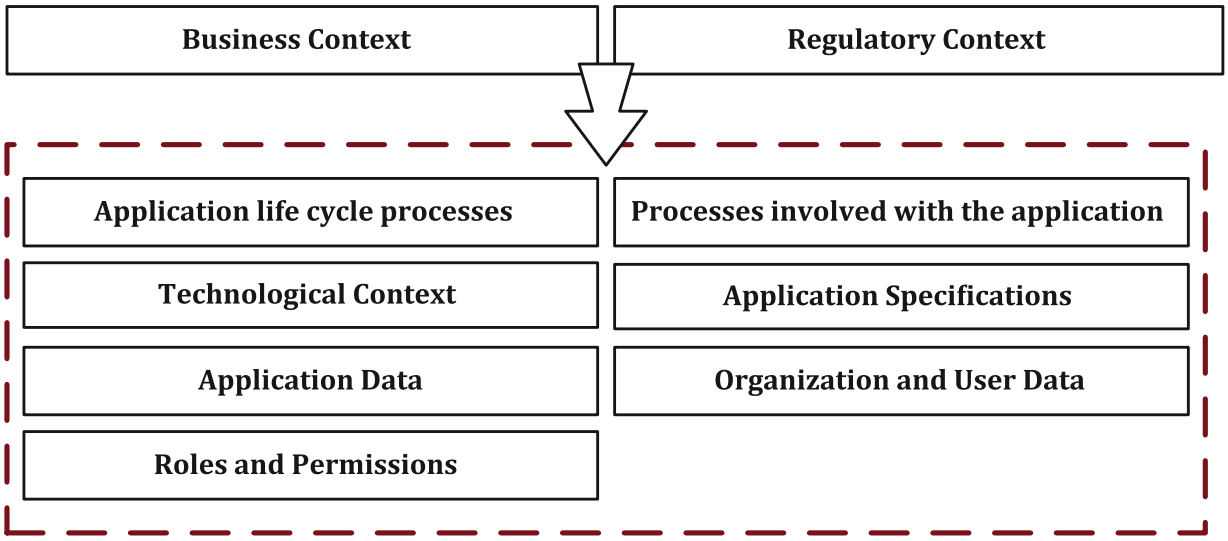


Figure 11 — Application Security Scope

ISO/IEC 27034-1:2011, 6.3 broadly defines information involved by an application and presents it as grouped information (see Figure 11). This representation does not mean that all elements in the above scope are part of the application, but rather that all these elements should be protected in order to secure the application. Information to be protected includes:

a) Information defined by the business context of the application.

   The business context refers to all business-related best practices, regulations and constraints stemming from business domains where the application is realized or operated.

   It may include critical information that should be protected (see 7.2).

b) Information defined by the regulatory context of the application.

   The regulatory context information repository of an application includes only relevant information for this application (see 7.3).

   1) Sets of laws, directives and regulations that apply or restrict the use of the application:

      i) in geographic areas where this application is used, operated, supported, accessed, or/and its data will be stored or backed up;

ii) by actors connecting to this application and accessing and/or storing information from these geographic areas.

c) Information defined by the life cycle processes of this application.

Information defined by the life cycle processes of the application refers to the description and outcomes of required or existing organizational processes involved and performed during the applications life cycle that may need to be protected.

This application life cycle processes information repository includes information such as:

1) roles, responsibilities and qualifications of all involved actors;

2) process associated with the mechanism and related services provided by the application;

3) training of stakeholders;

4) auditing and qualification processes;

5) realization processes (development, project management, maintenance, versioning, testing, etc.);

6) operational processes (operation, support etc.).

d) Information included by the processes involved with the application.

Information included by the processes involved with the application refers to required or existing organizational processes created or impacted by the application critical specifications and critical data that can need to be protected.

1) Processes description of using and operate the application, such as:

i) inspection process;

ii) process distribution and installation/update of the application;

iii) utilization and management processes;

iv) process maintenance, repair and replacement of application components, etc.;

v) contingency, backup and restore processes;

vi) distribution and deployment processes;

vii) processes impacted or required by the application.

2) Roles, responsibilities and qualifications.

3) Stakeholders' training.

e) Information included by the technological context of an application.

Information included by the technological context of the application refers to product and technological components including their configuration data and related processes supporting the application may need to be protected.

This is generally the data that is generated by the specific technological context used to achieve the business needs.

1) terminal, network and other authorized peripherals;

2) operating system, configuration and services;

3) authorized communication links and ports;

4) COTS and other products, such as Database Management Systems DBMS used by the application and its technological infrastructure;

5) qualification and other processes associated with the technological context;

6) components and products impacted or used by the application;

7) application‘s allowed devices;

8) operating system, configuration and external services needed by the application;

9) transportation and communication links allowed used by the application and its technological infrastructure;

10) physical and electrical environment specifications of the application (e.g. back office, servers rooms, cloud supplier, etc.);

11) application‘s terminals, (e.g. smart phone, tablet, laptop and etc.

f) Information included by the application specifications of an application.

Information included by the application's specifications refer to functionalities description, configuration data and operation processes that may need to be protected, such as:

1) client-side application specifications;

2) server and n-tiers application specification,

3) hardware specifications;

4) security specifications;

5) application functionalities;

6) client terminal specifications;

7) back office specifications.

g) Information included by the roles and permissions of an application.

Information included by application's roles and permissions refer to identity management and permissions information that may need to be protected, such as:

1) identity management data;

2) identification and authentication data;

3) authorization data.

h) Information included by the application data of an application.

Application data refers to application information that may need to be protected.

An example of such data are session IDs generated by the application framework to facilitate providing a session to the user. Note that this data might not be apparent from a blackbox-style observation of the application/system. Another example are logs generated by the application and GPS data.

The data associated with the application shall be classified according to the classification model used by the organization e.g. availability, confidentiality, integrity.

1) application configuration data;

2) application binary code;

3) application source code;

4) application and library components;

5) application documentation of critical components and functionalities.

i) Information included by the organization and user data of an application.

Organization and user data of an application refers to information coming from the organizations that realize or operate the application including data coming from the users that may need to be protected, such as:

1) certificates (public key information);

2) private key;

3) transactions;

4) logs;

5) configuration;

6) credit card or financial data;

7) personally identifiable data;

8) data gathered by the various inputs to the application;

9) certificates;

10) mission-critical data;

11) personal data;

12) user configuration data.

Annex A
(informative)

Guidance text related to the ASMP step: (6.4) Realizing and operating the application

A.1 Guidance

A.1.1 General

This step is made easier for the execution team and the verification team by presenting to them in the ANF only the ASCs required for reaching the Targeted Level of Trust for their specific project and because each ASC contains detailed information needed for performing a security activity and an associated verification measurement at a specific life cycle stage. It is not necessary for them to be aware of the processes leading to the creation of the ANF.

The application project execution team implements or follows up all the specific security activities described in the ASC "Security Activity" part (as explained in ISO/IEC 27034-1:2011, 8.1.2.6.5.3) in each ASC contained in the ANF for the application.

Project managers will find the ASC an efficient tool because it details the required tasks, the needed resources and their required qualifications, the cost in days-person for the tasks and the exact stage in the life cycle at which the tasks should be performed.

The verification team will also find the ASC concept an efficient tool because it provides detailed information about what verification measurements should be performed to provide evidence that security activities have been performed correctly with expected results. This allows the verification team to make sure the application meets the security requirements, though the formal recording of the supporting evidence, before the application delivery.

The security team and the technology team will also find the ASC concept useful because the ASCs in the ANF for a specific application provide a list of all security requirements, thus allowing advance planning of needed professional resources.

A.1.2 Static analysis

Project teams should perform static analysis of source code. Static analysis of source code provides a scalable capability for security code review and can help ensure that secure coding policies are being followed. The security team and the verification team are responsible for ultimately signing off on ASR, use verification team. This team can also include SME and consulting type service during the execution of ASC should be aware of the strengths and weaknesses of static analysis tools and be prepared to augment static analysis tools with other tools or human review as appropriate.

A.1.3 Dynamic program analysis

Run-time verification of software programs is necessary to ensure that a program's functionality works as designed. This verification task should specify tools that monitor application behaviour for memory corruption, user privilege issues, and other critical security problems. The process uses run-time tools along with other techniques such as fuzz testing, to achieve desired levels of security test coverage.

A.1.4 Fuzz testing

Fuzz testing is a specialized form of dynamic analysis used to induce program failure by deliberately introducing malformed or random data to an application. The fuzz testing strategy is derived from

the intended use of the application and the functional and design specifications for the application. The verification team may require additional fuzz tests or increases in the scope and duration of fuzz testing.

A.1.5 Exception process

A.1.5.1 General

If the project team concludes that some of the security requirements outlined in the ASCs cannot be implemented, they need to submit an exception request to the verification team. The verification team reviews the exception request, and if the overall security risk of not implementing the security requirements is acceptable, exception may be granted.

A.1.5.2 Exception process

The organization should define and establish a process for handling the cases where the ASCs are not applicable or implementable for a specific application. Exceptions should be recorded in the ANF and validated by the verification team. Exceptions that require accepting residual risk should be signed off on by the application owner and periodically reviewed to determine if the residual risk can be reduced and/or determine that the residual risk remains acceptable.

A.1.5.3 Change management process

This ANF exists throughout the application's life cycle and can evolve over time. For example, the regulatory context for the application can change during the course of the project, which in turn can lead to a new Targeted Level of Trust. In these cases, new elements can be added to or removed from the ANF. Changes to the ANF have an impact on the application's security. These changes should be tracked and receive corresponding approvals from the application owner.

During the life cycle of the application and prior to designing any changes, a review of ASCs should be conducted to ensure the Targeted Level of Trust is at maximum required level (as per ASC).

EXAMPLE An Internal facing application with confidential data can be designed and implemented such that the password controls are as per ASC for internal applications, similarly when the application is made public facing an expanded set of ASC can be needed, (e.g using https for web based applications as a mandatory requirement).

A.1.5.4 Feedback process

The organization should define and establish a process for continuously improving the ONF through feedback of new knowledge, ASC improvement suggestions and experiences gained in the course of an application's development and deployment. The feedback process should tie into an ONF management process. This process is shown on Figure 1 as "Provides feedback to". This process should tie in with an ONF maintenance process shown in ISO/IEC 27034-1:2001, Figure 8 as "Feedback from previous and current application projects".

The following is an example feedback to ONF:

EXAMPLE 1 Capturing of the applications threat landscape can be enhanced by using newer and more innovative tools.

EXAMPLE 2 New controls can be added to the ASC to lower the likelihood of attacks on specific features.

Bibliography

[1] ISO/IEC/IEEE 12207, *Systems and Software Engineering — Software life cycle process*

[2] ISO/IEC 15026 (all parts), *Systems and software engineering — Systems and software assurance*

[3] ISO/IEC/IEEE 15288, *Systems and software engineering — Software Life Cycle Processes*

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

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

[6] ISO/IEC/IEEE 24765, *Systems and software engineering — Vocabulary*

[7] ISO/IEC 26514, *Systems and software engineering — Requirements for designers and developers of user documentation*

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

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

[10] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[11] ISO/IEC/IEEE 29148, *Software and systems engineering — Life cycle processes — Requirements engineering*

ICS 35.030

Price based on 47 pages