

BS ISO/IEC 27034-1:2011

Incorporating corrigendum January 2014



BSI Standards Publication

Information technology — Security techniques — Application security

Part 1: Overview and concepts

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO/IEC 27034-1:2011, incorporating corrigendum January 2014.

The start and finish of text introduced or altered by corrigendum is indicated in the text by tags. Text altered by ISO/IEC corrigendum January 2014 is indicated in the text by AC1 AC1.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

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

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

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 84428 7

ICS 35.040

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

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2011.

Amendments/corrigenda issued since publication

Date	Text affected
28 February 2014	Implementation of ISO/IEC corrigendum January 2014

**Information technology — Security
techniques — Application security —**

**Part 1:
Overview and concepts**

*Technologies de l'information — Techniques de sécurité — Sécurité
des applications —*

Partie 1: Aperçu général et concepts



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Published in Switzerland

Contents

Page

FOREWORD	VII
INTRODUCTION	VIII
0.1 GENERAL	VIII
0.2 PURPOSE	VIII
0.3 TARGETED AUDIENCES	IX
0.3.1 General	ix
0.3.2 Managers	ix
0.3.3 Provisioning and operation teams	x
0.3.4 Acquirers	xi
0.3.5 Suppliers	xi
0.3.6 Auditors	xi
0.3.7 Users	xi
0.4 PRINCIPLES	XI
0.4.1 Security is a requirement	xi
0.4.2 Application security is context-dependent	xii
0.4.3 Appropriate investment for application security	xii
0.4.4 Application security should be demonstrated	xii
0.5 RELATIONSHIP TO OTHER INTERNATIONAL STANDARDS	XIII
0.5.1 General	xiii
0.5.2 ISO/IEC 27001, Information security management systems — Requirements	xiii
0.5.3 ISO/IEC 27002, Code of practice for information security management	xiii
0.5.4 ISO/IEC 27005, Information security risk management	xiii
0.5.5 ISO/IEC 21827, Systems Security Engineering — Capability Maturity Model® (SSE CMM®)	xiii
0.5.6 ISO/IEC 15408-3, Evaluation criteria for IT security — Part 3: Security assurance components	xiii
0.5.7 ISO/IEC TR 15443-1, A framework for IT security assurance — Part 1: Overview and framework, and ISO/IEC TR 15443-3, A framework for IT security assurance — Part 3: Analysis of assurance methods	xiv
0.5.8 ISO/IEC 15026-2, Systems and software engineering — Systems and software assurance — Part 2: Assurance case	xiv
0.5.9 ISO/IEC 15288, Systems and software engineering — System life cycle processes, and ISO/IEC 12207, Systems and software engineering — Software life cycle process	xiv
0.5.10 ISO/IEC 29193 (under development), Secure system engineering principles and techniques	xiv
1 SCOPE	1
2 NORMATIVE REFERENCES	1
3 TERMS AND DEFINITIONS	1
4 ABBREVIATED TERMS	4
5 STRUCTURE OF ISO/IEC 27034	5
6 INTRODUCTION TO APPLICATION SECURITY	6
6.1 GENERAL	6
6.2 APPLICATION SECURITY VS SOFTWARE SECURITY	6
6.3 APPLICATION SECURITY SCOPE	6
6.3.1 General	6
6.3.2 Business context	7
6.3.3 Regulatory context	7
6.3.4 Application life cycle processes	7
6.3.5 Processes involved with the application	7

6.3.6	<i>Technological context</i>	8
6.3.7	<i>Application specifications</i>	8
6.3.8	<i>Application data</i>	8
6.3.9	<i>Organization and user data</i>	8
6.3.10	<i>Roles and permissions</i>	8
6.4	APPLICATION SECURITY REQUIREMENTS	8
6.4.1	<i>Application security requirements sources</i>	8
6.4.2	<i>Application security requirements engineering</i>	9
6.4.3	<i>ISMS</i>	9
6.5	RISK	9
6.5.1	<i>Application security risk</i>	9
6.5.2	<i>Application vulnerabilities</i>	10
6.5.3	<i>Threats to applications</i>	10
6.5.4	<i>Impact on applications</i>	10
6.5.5	<i>Risk management</i>	10
6.6	SECURITY COSTS	10
6.7	TARGET ENVIRONMENT	10
6.8	CONTROLS AND THEIR OBJECTIVES	11
7	ISO/IEC 27034 OVERALL PROCESSES	11
7.1	COMPONENTS, PROCESSES AND FRAMEWORKS	11
7.2	ONF MANAGEMENT PROCESS	12
7.3	APPLICATION SECURITY MANAGEMENT PROCESS	13
7.3.1	<i>General</i>	13
7.3.2	<i>Specifying the application requirements and environment</i>	13
7.3.3	<i>Assessing application security risks</i>	13
7.3.4	<i>Creating and maintaining the Application Normative Framework</i>	13
7.3.5	<i>Provisioning and operating the application</i>	14
7.3.6	<i>Auditing the security of the application</i>	14
8	CONCEPTS	14
8.1	ORGANIZATION NORMATIVE FRAMEWORK	14
8.1.1	<i>General</i>	14
8.1.2	<i>Components</i>	15
8.1.3	<i>Processes related to the Organization Normative Framework</i>	28
8.2	APPLICATION SECURITY RISK ASSESSMENT	30
8.2.1	<i>Risk assessment vs risk management</i>	30
8.2.2	<i>Application risk analysis</i>	31
8.2.3	<i>Risk Evaluation</i>	31
8.2.4	<i>Application's Targeted Level of Trust</i>	31
8.2.5	<i>Application owner acceptance</i>	31
8.3	APPLICATION NORMATIVE FRAMEWORK	32
8.3.1	<i>General</i>	32
8.3.2	<i>Components</i>	33
8.3.3	<i>Processes related to the security of the application</i>	33
8.3.4	<i>Application's life cycle</i>	34
8.3.5	<i>Processes</i>	34
8.4	PROVISIONING AND OPERATING THE APPLICATION	34
8.4.1	<i>General</i>	34
8.4.2	<i>Impact of ISO/IEC 27034 on an application project</i>	35
8.4.3	<i>Components</i>	36
8.4.4	<i>Processes</i>	36
8.5	APPLICATION SECURITY AUDIT	37
8.5.1	<i>General</i>	37
8.5.2	<i>Components</i>	38

ANNEX A (INFORMATIVE) MAPPING AN EXISTING DEVELOPMENT PROCESS TO ISO/IEC 27034 CASE STUDY	39
A.1 GENERAL.....	39
A.2 ABOUT THE SECURITY DEVELOPMENT LIFECYCLE	39
A.3 SDL MAPPED TO THE ORGANIZATION NORMATIVE FRAMEWORK	40
A.4 BUSINESS CONTEXT	41
A.5 REGULATORY CONTEXT	41
A.6 APPLICATION SPECIFICATIONS REPOSITORY.....	42
A.7 TECHNOLOGICAL CONTEXT.....	42
A.8 ROLES, RESPONSIBILITIES AND QUALIFICATIONS	43
A.9 ORGANIZATION ASC LIBRARY	44
A.9.1 <i>Training</i>	45
A.9.2 <i>Requirements</i>	45
A.9.3 <i>Design</i>	46
A.9.4 <i>Implementation</i>	47
A.9.5 <i>Verification</i>	47
A.9.6 <i>Release</i>	48
A.10 APPLICATION SECURITY AUDIT	49
A.11 APPLICATION LIFE CYCLE MODEL	51
A.12 SDL MAPPED TO THE APPLICATION SECURITY LIFE CYCLE REFERENCE MODEL	53
ANNEX B (INFORMATIVE) MAPPING ASC WITH AN EXISTING STANDARD	55
B.1 ASC CANDIDATE CATEGORIES	55
B.1.1 <i>Common security control-related considerations</i>	55
B.1.2 <i>Operational/environmental-related considerations</i>	55
B.1.3 <i>Physical Infrastructure-related considerations</i>	55
B.1.4 <i>Public access-related considerations</i>	55
B.1.5 <i>Technology-related considerations</i>	56
B.1.6 <i>Policy/regulatory-related considerations</i>	56
B.1.7 <i>Scalability-related considerations</i>	56
B.1.8 <i>Security objective-related considerations</i>	56
B.2 CLASSES OF SECURITY CONTROLS	57
B.3 SUB-CLASSES IN THE ACCESS CONTROL (AC) CLASS	58
B.4 DETAILED ACCESS CONTROL CLASSES	59
B.4.1 <i>AC-1 Access control policy and procedures</i>	59
B.4.2 <i>AC-2 Account management</i>	59
B.4.3 <i>AC-17 Remote access</i>	60
B.5 DEFINITION OF AN ASC BUILT FROM A SAMPLE SP 800-53 CONTROL.....	61
B.5.1 <i>Control AU-14 as described in SP 800-53 Rev. 3</i>	61
B.5.2 <i>Control AU-14 as described using ISO/IEC 27034 ASC format</i>	62
ANNEX C (INFORMATIVE) ISO/IEC 27005 RISK MANAGEMENT PROCESS MAPPED WITH THE ASMP	65
BIBLIOGRAPHY	67

Figures	Page
Figure 1 – Relationship to other International Standards	xiii
Figure 2 – Application Security Scope	6
Figure 3 – Organization Management Processes	12
Figure 4 – Organization Normative Framework (simplified)	15
Figure 5 – Graphical representation of an example of an Organization ASC Library	18
Figure 6 – Components of an ASC	20
Figure 7 – Graph of ASCs	21
Figure 8 – Top-level view of the Application Security Life Cycle Reference Model	24
Figure 9 – ONF Management Process	28
Figure 10 – Application Normative Framework	32
Figure 11 – Impact of ISO/IEC 27034 on roles and responsibilities in a typical application project.....	35
Figure 12 – ASC used as a security activity	36
Figure 13 – ASC used as a measurement.....	37
Figure 14 – Overview of the application security verification process.....	38
Figure A.1 – Security Development Lifecycle	40
Figure A.2 – SDL mapped to the Organization Normative Framework	40
Figure A.3 – Example of an ASC tree.....	45
Figure A.4 – Example of a Line of Business Application for Application Security Audit.....	50
Figure A.5 – SDL Process Illustration.....	52
Figure A.6 – SDL mapped to the Application Security Life Cycle Reference Model.....	53
Figure A.7 – Detailed mapping of SDL phases with stages in the Application Security Life Cycle Reference Model	53
Figure C.1 – ISO/IEC 27005 risk management process mapped with the ASMP.	65

Tables	Page
Table 1 – Application Scope vs Application Security Scope	7
Table 2 – Mapping of ISMS and application security-related ONF management subprocesses	29
Table B.1 – Security control classes, families, and identifiers	57
Table B.2 – Security control classes and security control baselines for low-impact, moderate-impact, and high-impact information systems	58
Table B.3 – SP800-53 control AU-14 described using ISO/IEC 27034 ASC format.....	62

Foreword

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

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

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

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

ISO/IEC 27034-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 27034 consists of the following parts, under the general title *Information technology — Security techniques — Application security*:

— *Part 1: Overview and concepts*

The following parts are under preparation:

— *Part 2: Organization normative framework*

— *Part 3: Application security management process*

— *Part 4: Application security validation*

— *Part 5: Protocols and application security control data structure*

Introduction

0.1 General

Organizations should protect their information and technological infrastructures in order to stay in business. Traditionally this has been addressed at the IT level by protecting the perimeter and such technological infrastructure components as computers and networks, which is generally insufficient.

In addition, organizations are increasingly protecting themselves at the governance level by operating formalized, tested and verified information security management systems (ISMS). A systematic approach contributes to an effective information security management system as described in ISO/IEC 27001.

However, organizations face an ever-growing need to protect their information at the application level.

Applications should be protected against vulnerabilities which might be inherent to the application itself (e.g. software defects), appear in the course of the application's life cycle (e.g. through changes to the application), or arise due to the use of the application in a context for which it was not intended.

A systematic approach to increased application security provides evidence that information being used or stored by an organization's applications is adequately protected.

Applications can be acquired through internal development, outsourcing or purchasing a commercial product. Applications can also be acquired through a combination of these approaches which might introduce new security implications that should be considered and managed.

Examples of applications are human resource systems, finance systems, word-processing systems, customer management systems, firewalls, anti-virus systems and intrusion detection systems.

Throughout its life cycle, a secure application exhibits prerequisite characteristics of software quality, such as predictable execution and conformance, as well as meeting security requirements from a development, management, technological infrastructure, and audit perspective. Security-enhanced processes and practices—and the skilled people to perform them—are required to build trusted applications that do not increase risk exposure beyond an acceptable or tolerable level of residual risk and support an effective ISMS.

Additionally, a secure application takes into account the security requirements stemming from the type of data, the targeted environment (business, regulatory and technological contexts), the actors and the application specifications. It should be possible to obtain evidence that is shown to demonstrate that an acceptable (or tolerable) level of residual risk has been attained and is being maintained.

0.2 Purpose

The purpose of ISO/IEC 27034 is to assist organizations in integrating security seamlessly throughout the life cycle of their applications by:

- a) providing concepts, principles, frameworks, components and processes;
- b) providing process-oriented mechanisms for establishing security requirements, assessing security risks, assigning a Targeted Level of Trust and selecting corresponding security controls and verification measures;
- c) providing guidelines for establishing acceptance criteria to organizations outsourcing the development or operation of applications, and for organizations purchasing from third-party applications;
- d) providing process-oriented mechanisms for determining, generating and collecting the evidence needed to demonstrate that their applications can be used securely under a defined environment;
- e) supporting the general concepts specified in ISO/IEC 27001 and assisting with the satisfactory implementation of information security based on a risk management approach; and
- f) providing a framework that helps to implement the security controls specified in ISO/IEC 27002 and other standards.

ISO/IEC 27034:

- a) applies to the underlying software of an application and to contributing factors that impact its security, such as data, technology, application development life cycle processes, supporting processes and actors; and
- b) applies to all sizes and all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) exposed to risks associated with applications.

ISO/IEC 27034 does not:

- a) provide guidelines for physical and network security;
- b) provide controls or measurements; or
- c) provide secure coding specifications for any programming language.

ISO/IEC 27034 is not:

- a) a software application development standard;
- b) an application project management standard; or
- c) a software development life cycle standard.

The requirements and processes specified in ISO/IEC 27034 are not intended to be implemented in isolation but rather integrated into an organization's existing processes. To this effect, organizations should map their existing processes and frameworks to those proposed by ISO/IEC 27034, thus reducing the impact of implementing ISO/IEC 27034.

Annex A (informative) provides an example illustrating how an existing software development process can be mapped to some of the components and processes of ISO/IEC 27034. Generally speaking, an organization using any development life cycle should perform a mapping such as the one described in Annex A, and add whatever missing components or processes are needed for compliance with ISO/IEC 27034.

0.3 Targeted audiences

0.3.1 General

The following audiences will benefit from ISO/IEC 27034 while carrying out their designated organizational roles:

- a) managers;
- b) provisioning and operation teams;
- c) acquisition personnel;
- d) suppliers; and
- e) auditors.

0.3.2 Managers

Managers are persons involved in the management of the application during its complete life cycle. The applicable stages of the application life cycle include the provisioning stages and the production stages. Examples of managers are:

- a) information security managers;
- b) project managers;
- c) administrators;
- d) software acquirers;
- e) software development managers;
- f) application owners;
- g) line managers, who supervise employees.

Typically managers need to:

- a) balance the cost of implementing and maintaining application security against the risks and value it represents for the organization;
- b) review auditor's reports recommending acceptance or rejection based on whether an application has attained and maintained its Targeted Level of Trust;
- c) ensure compliance with standards, laws and regulations according to an application's regulatory context (see 8.1.2.2);
- d) oversee the implementation of a secure application;
- e) authorize the Targeted Level of Trust according to the organization's specific context;
- f) determine which security controls and corresponding verification measurements should be implemented and tested;
- g) minimize application security verification costs;
- h) document security policies and procedures for an application;
- i) provide security awareness, training and oversight to all actors;
- j) put in place proper information security clearances required by applicable information security policies and procedures; and
- k) stay abreast of all system-related security plans throughout the organization's network.

0.3.3 Provisioning and operation teams

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

- a) architects,
- b) analysts,
- c) programmers,
- d) testers,
- e) system administrators,
- f) database administrators,
- g) network administrators, and
- h) technical personnel.

Typically members need to:

- a) understand which 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 of the associated measurements;
- 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) establish business relationships to obtain needed goods and services, (e.g. for the solicitation, evaluation and awarding of contracts); and
- i) 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) prepare requests for proposals that include requirements for security controls;
- b) select suppliers that comply with such requirements;
- c) verify evidence of security controls applied by outsourcing services; and
- d) 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; and
- 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 as required by management; and
- d) apply standardized audit processes based on the use of verifiable evidence.

0.3.7 Users

Users are persons who need to:

- a) trust that it is deemed secure to use or deploy an application;
- b) trust that an application produces reliable results consistently and in a timely manner; and
- c) trust that the controls and their corresponding verification measurements are positioned and functioning correctly as expected.

0.4 Principles

0.4.1 Security is a requirement

Security requirements should be defined and analyzed for each and every stage of an application's life cycle, adequately addressed and managed on a continuous basis.

Application security requirements (see 6.4) should be treated in the same manner as functionality, quality and usability requirements (see ISO/IEC 9126 for an example of a quality model). In addition, security-related requirements to conform to the established limitations on residual risk should be instituted.

According to ISO/IEC/IEEE 29148 (under development), requirements should be necessary, abstract, unambiguous, consistent, complete, concise, feasible, traceable and verifiable. The same characteristics apply to security requirements. Vague security requirements such as "The developer should discover all important security risks for the application" are too often encountered in application projects' documentation.

0.4.2 Application security is context-dependent

Application security is influenced by a defined target environment. The type and scope of application security requirements are determined by the risks to which the application is subjected, which in turn depend on three contexts:

- a) business context: specific risks arising from the organization's business domain (phone company, transport company, government, etc.);
- b) regulatory context: specific risks arising from the geographical location where the organization is doing business (intellectual property rights and licensing, restrictions on cryptography protection, copyright, laws and regulations, privacy legislation, etc.);
- c) technological context: specific risks from the technologies used by the organization in the course of business [reverse engineering, security of build tools, protection of source code, use of third-party pre-compiled code, security testing, penetration testing, bounds checking, code checking, information and communication technology (ICT) environment in which the application runs, configuration files and uncompiled data, operating system privileges for installation and/or operation, maintenance, secure distribution, etc.].

The technological context encompasses applications' technical specifications (security functionality, secure components, online payments, secure log, cryptography, permissions management, etc.).

An organization can affirm that an application is secure, but this affirmation is only valid for this particular organization in its specific business, regulatory and technological contexts. If, for example, the application's technological infrastructure changes, or the application is used for the same purposes in another country, these new contexts might impact the security requirements and the Targeted Level of Trust. The current Application Security Controls might no longer adequately address the new security requirements and the application might no longer be secure.

0.4.3 Appropriate investment for application security

The costs of applying Application Security Controls and performing audit measurements should be commensurate with the Targeted Level of Trust (see 8.1.2.6.4) required by the application owner or by management.

These costs can be considered as an investment because they reduce the costs, application owner responsibilities and legal consequences of security breaches.

0.4.4 Application security should be demonstrated

The application auditing process in ISO/IEC 27034 (see 8.5) makes use of the verifiable evidence provided by Application Security Controls (see 8.1.2.6.5).

An application cannot be declared secure unless the auditor agrees that the supporting evidence generated by the corresponding verification measurements of the applicable Application Security Controls demonstrates that it has reached management's Targeted Level of Trust.

0.5 Relationship to other International Standards

0.5.1 General

Figure 1 shows relationships between ISO/IEC 27034 and other International Standards.

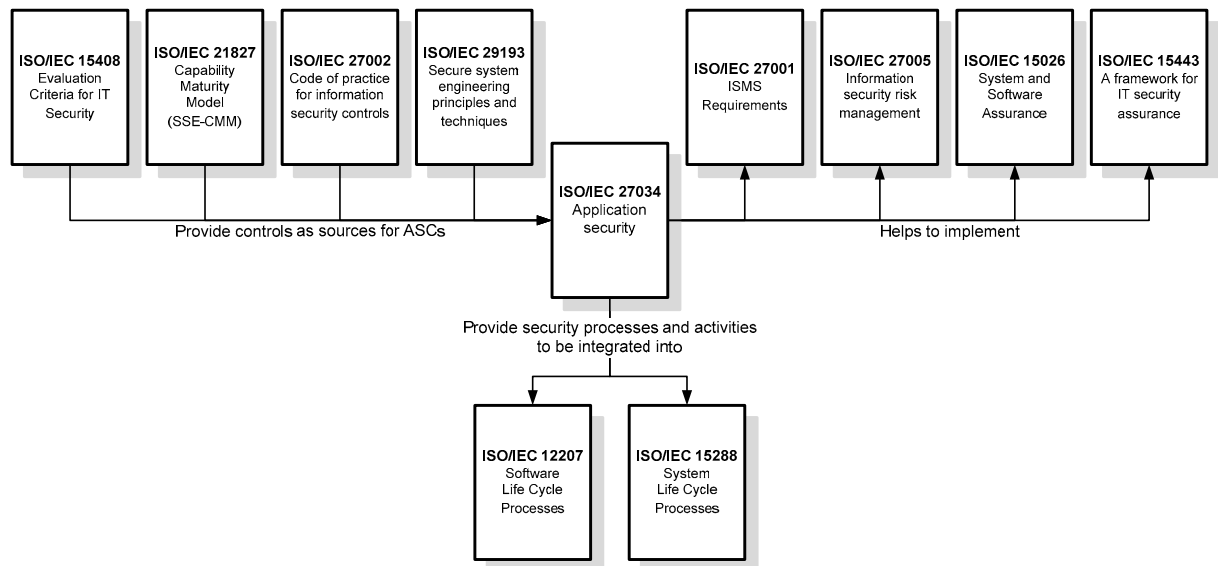


Figure 1 – Relationship to other International Standards

0.5.2 ISO/IEC 27001, Information security management systems — Requirements

ISO/IEC 27034 helps to implement, with a scope limited to application security, recommendations from ISO/IEC 27001. In particular, the following approaches are used:

- a) systematic approach to security management;
- b) “Plan, Do, Check, Act” process approach; and
- c) implementation of information security based on risk management.

0.5.3 ISO/IEC 27002, Code of practice for information security management

ISO/IEC 27002 provides practices that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034. Of utmost interest are controls from the following clauses in ISO/IEC 27002:2005:

- a) clause 10: Communications and Operations Management;
- b) clause 11: Access Control; and most importantly
- c) clause 12: Information Systems Acquisition, Development and Maintenance.

0.5.4 ISO/IEC 27005, Information security risk management

ISO/IEC 27034 helps to implement, with a scope limited to application security, the risk management process proposed by ISO/IEC 27005. See Annex C (informative) for a more detailed discussion.

0.5.5 ISO/IEC 21827, Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

ISO/IEC 21827 provides security engineering base practices that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034. In addition, processes from ISO/IEC 27034 help to attain several of the capabilities that define the capability levels in ISO/IEC 21827.

0.5.6 ISO/IEC 15408-3, Evaluation criteria for IT security — Part 3: Security assurance components

ISO/IEC 15408-3 provides requirements and action elements that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034.

0.5.7 ISO/IEC TR 15443-1, A framework for IT security assurance — Part 1: Overview and framework, and ISO/IEC TR 15443-3, A framework for IT security assurance — Part 3: Analysis of assurance methods

ISO/IEC 27034 helps to enforce and reflect the principles of security assurance from ISO/IEC TR 15443-1 and to contribute to the assurance cases of ISO/IEC TR 15443-3.

0.5.8 ISO/IEC 15026-2, Systems and software engineering — Systems and software assurance — Part 2: Assurance case

Use of processes and Application Security Controls from ISO/IEC 27034 in application projects directly provides assurance cases about the security of the application. In particular,

- a) claims and their justifications are provided by the application security risk analysis process,
- b) evidence is provided by Application Security Controls' built-in verification measurements, and
- c) compliance to ISO/IEC 27034 can be used as argument in many such assurance cases.

See also 8.1.2.6.5.1.

0.5.9 ISO/IEC 15288, Systems and software engineering — System life cycle processes, and ISO/IEC 12207, Systems and software engineering — Software life cycle processes

ISO/IEC 27034 provides additional processes for the organization, as well as Application Security Controls that an organization can insert as additional activities into its existing systems and software engineering life cycle processes as provided by ISO/IEC 15288 and ISO/IEC 12207.

0.5.10 ISO/IEC TR 29193 (under development), Secure system engineering principles and techniques

ISO/IEC TR 29193 provides guidance for secure system engineering of ICT systems or products that an organization can implement as Application Security Controls as proposed by ISO/IEC 27034.

Information technology — Security techniques — Application security —

Part 1: Overview and concepts

1 Scope

ISO/IEC 27034 provides guidance to assist organizations in integrating security into the processes used for managing their applications.

This part of ISO/IEC 27034 presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.

ISO/IEC 27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.

2 Normative references

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

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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

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

ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and the following apply.

3.1

actor

person or process that performs an activity during an application's life cycle or initiates interaction with any process provided by or impacted on by an application

3.2

Actual Level of Trust

result of an audit process that provides supporting evidence that all Application Security Controls required by the application's Targeted Level of Trust were correctly implemented and verified, and produced the expected results

3.3

application

IT solution, including application software, application data and procedures, designed to help an organization's users perform particular tasks or handle particular types of IT problems by automating a business process or function

NOTE Business processes include both people and technologies.

3.4

Application Security Life Cycle Reference Model

life cycle model used as a reference for the introduction of security activities into processes involved in application management, application provisioning and operation, infrastructure management and application audit

3.5

Application Normative Framework

ANF

set of normative elements relevant for a specific application project, selected from the Organization Normative Framework

3.6

application owner

organizational role responsible for the management, utilization and protection of the application and its data

NOTE 1 The application owner makes all decisions pertaining to the application's security.

NOTE 2 The term "owner" is used throughout this part of ISO/IEC 27034 as a synonym for "application owner".

3.7

application project

endeavour with defined start and finish criteria undertaken to acquire an application in accordance with specified resources and requirements

[SOURCE: ISO/IEC 12207:2008, definition 4.29, modified – specialized for application scope.]

NOTE For the purposes of ISO/IEC 27034, the start and finish criteria are such that the entire life cycle of the application is included in the application project.

3.8

Application Security Control

ASC

data structure containing a precise enumeration and description of a security activity and its associated verification measurement to be performed at a specific point in an application's life cycle

3.9

Application Security Management Process

ASMP

overall management process for security activities, actors, artefacts and audit for each application used by an organization

3.10

application software

software designed to help users perform particular tasks or handle particular types of problems, as distinct from software that controls the computer itself

[SOURCE: ISO/IEC/IEEE 24765:2010, definition 3.130-1]

3.11

audit

systematic and documented process for obtaining evidence and evaluating it objectively to determine the extent to which measurement criteria have been fulfilled

[SOURCE: ISO 9000:2005, definition 3.9.1, modified – generalized.]

3.12

environment

business, regulatory and technological context in which an application is used, including all processes, products, information and actors involved in the application

3.13

life cycle

evolution of a system, product, service, project or other human-made entity from conception through retirement

[SOURCE: ISO/IEC 12207:2008, definition 4.16]

3.14

life cycle model

framework of processes and activities concerned with the life cycle that may be organized into stages, which also acts as a common reference for communication and understanding

[SOURCE: ISO/IEC 12207:2008, definition 4.17]

3.15

maintenance

any change performed on an application after its delivery

EXAMPLES Error correction, added functionality, improved performance, ensuring the application's functionality.

3.16

Organization Normative Framework

ONF

organization-wide internal structure containing a set of normative application security processes and elements

3.17

ONF committee

organizational role responsible for maintaining and approving application security-related components within the ONF

3.18

operating environment

external surroundings of a program existing or expected to exist during its execution

[SOURCE: ISO/IEC 2382-7:2000, definition 07.11.07]

3.19

product

result of a process

[SOURCE: ISO 9000:2005, definition 3.4.2]

3.20

secure application

application for which the Actual Level of Trust is equal to the Targeted Level of Trust, as defined by the organization using the application

3.21

Targeted Level of Trust

name or label of a set of Application Security Controls deemed necessary by the application owner to lower the risk associated with a specific application to an acceptable (or tolerable) level, following an application security risk analysis

3.22

user

person who uses or operates something

[SOURCE: Concise Oxford English Dictionary]

NOTE For the purposes of ISO/IEC 27034, the term “user” includes not only the end user, but also maintenance and operation roles, such as system administrator and database administrator.

3.23

validation

confirmation, through the provision of objective evidence, that requirements for a specific intended use or application have been fulfilled

NOTE 1 The term “validated” is used to designate the corresponding status.

NOTE 2 The use conditions for validation can be real or simulated.

[SOURCE: ISO 9000:2005, definition 3.8.5]

NOTE 3 In layman’s terms, “validation” means “Is the right application being built?”

3.24

verification

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

NOTE 1 The term “verified” is used to designate the corresponding status.

NOTE 2 Confirmation can comprise activities such as performing alternative calculations, comparing a new design specification with a similar proven design specification, undertaking tests and demonstrations, and reviewing documents prior to issue.

[SOURCE: ISO 9000:2005, definition 3.8.4]

NOTE 3 In layman’s terms, “verification” means “Is the application being built correctly?”

4 Abbreviated terms

ANF	Application Normative Framework
ASC	Application Security Control
ASMP	Application Security Management Process
COTS	Commercial-Off-The-Shelf
ICT	Information and Communication Technology
ISMS	Information Security Management System
ONF	Organization Normative Framework
XML	eXtended Markup Language

5 Structure of ISO/IEC 27034

ISO/IEC 27034 consists of six documents or parts. This part of ISO/IEC 27034 presents an overview and necessary concepts. It is self-contained and sufficient for the purposes of evaluating the need for implementation of ISO/IEC 27034 in an organization, and for presentation and training purposes. This part of ISO/IEC 27034 by itself is not sufficient for implementing ISO/IEC 27034.

ISO/IEC 27034-2, -3 and -4 should be acquired by organizations wishing to implement ISO/IEC 27034. They contain in-depth discussions, enumerations, structures and descriptions for all concepts presented in this part of ISO/IEC 27034.

ISO/IEC 27034-5 will be especially useful for organizations interested in acquiring or distributing controls, by providing a standard data structure and a standard protocol for the distribution of controls. For example, a large organization might be interested in automated distribution and updates of controls to all of its sub-units.

ISO/IEC 27034-6 provides examples of controls for specific application security requirements and will be useful to organizations wishing to implement ISO/IEC 27034, or by organizations wishing to develop specific controls.

The contents of the six parts are as follows:

PART 1 – Overview and concepts

Part 1 presents an overview of application security. It introduces definitions, concepts, principles and processes involved in application security.

PART 2 – Organization normative framework

Part 2 presents an in-depth discussion of the Organization Normative Framework, its components and the organization-level processes for managing it. This part explains the relationships among these processes, the activities associated with them, and the means by which they support the Application Security Management Process. This part will discuss how an organization should implement ISO/IEC 27034 and integrate it into its existing processes.

PART 3 – Application security management process

Part 3 presents an in-depth discussion of the processes involved in an application project: determining the application requirements and environment, assessing the application security risks, creating and maintaining the Application Normative Framework, realizing and operating the application and validating its security throughout its life cycle. It explains the relationships among these processes, their activities and interdependencies, and how they introduce security into an application project.

PART 4 – Application security validation

Part 4 presents an in-depth discussion of the application security validation and certification process that measures the application's Actual Level of Trust and compares it with the application's Targeted Level of Trust previously selected by the organization.

PART 5 – Protocols and application security control data structure

Part 5 presents the protocols and XML schema for the Application Security Control (ASC) based on the ISO/IEC TS 15000 series: Electronic business eXtensible Markup Language (ebXML). It will be used to help organizations validate the data structure of their ASCs and other components of ISO/IEC 27034, and to help automate the distribution, updating and use of ASCs.

PART 6 – Security guidance for specific applications

Part 6, if necessary, could provide examples of ASCs tailored for specific application security requirements.

6 Introduction to application security

6.1 General

Application security is a process performed to apply controls and measurements to an organization's applications in order to manage the risk of using them.

Controls and measurements can be applied to the application itself (its processes, components, software and results), to its data (configuration data, user data, organization data), and to all technology, processes and actors involved in the application's life cycle.

6.2 Application security vs software security

An application is an IT solution that includes software (see definition in clause 3). Application security is thus a broader concept that encompasses software security.

6.3 Application security scope

6.3.1 General

Application security protects the critical data computed, used, stored and transferred by an application as required by the organization. This protection ensures not only the data's availability, integrity and confidentiality, but also the authentication and non-repudiation of users who access it. The criticality of data and other assets should be defined by the organization through its security risk assessment process.

The critical data requiring protection also includes application source code, binary code and the runtime code on which it executes.

Figure 2 shows a graphical representation of the application security scope, represented as the area delimited by the dotted line.

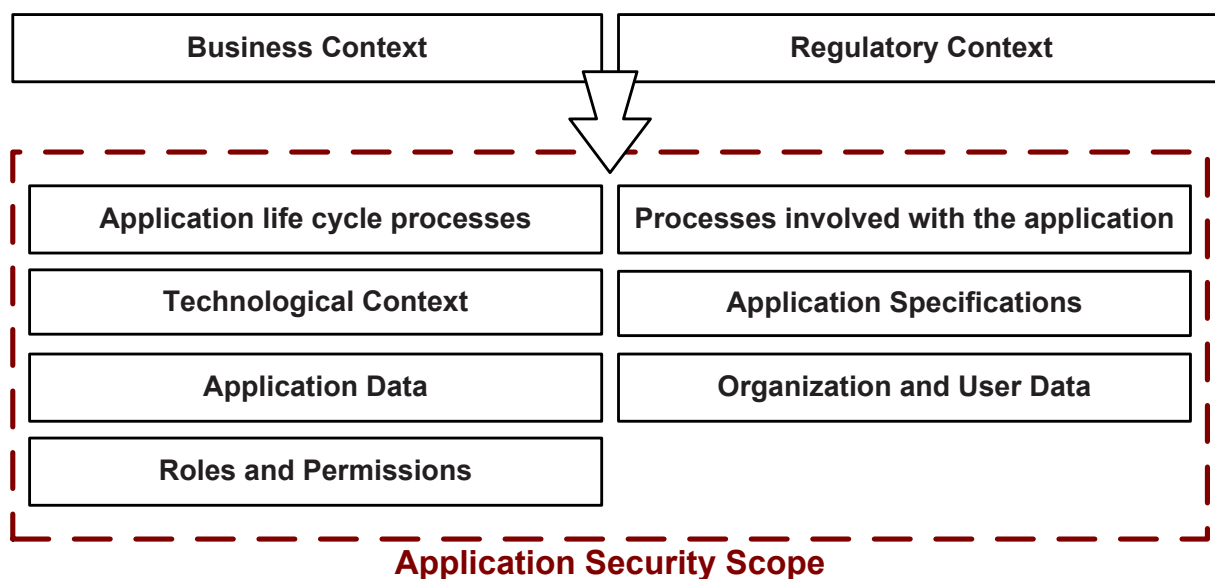


Figure 2 – Application Security Scope

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. Thus, the scope of application security is larger than the scope of the application itself. The following Table illustrates this difference.

Table 1 – Application Scope vs Application Security Scope

Related elements	In Application Scope	In Application Security Scope
Organization and user data (6.3.9)		✓
Application data (6.3.8)	✓	✓
Roles and permissions (6.3.10)	✓	✓
Application specifications (6.3.7)	✓	✓
Technological context (6.3.6)		✓
Processes involved with the application (6.3.5)		✓
Application life cycle processes (6.3.4)		✓
Business Context (6.3.2)		✓
Regulatory Context (6.3.3)		✓

The following data and processes are within the scope of application security and should be protected.

6.3.2 Business context

The business context refers to all business-related best practices, regulations and constraints stemming from the business domain of the organization.

6.3.3 Regulatory context

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

6.3.4 Application life cycle processes

All required or existing organizational processes involved in the applications life cycle should be protected, such as:

- a) training, auditing and qualification processes;
- b) realization processes (development, project management, maintenance, versioning, testing, etc.); and
- c) operational processes.

6.3.5 Processes involved with the application

All required or existing organizational processes impacted by the application critical specifications and critical data should be protected, such as:

- a) utilization and management processes;
- b) maintenance and backup processes;
- c) distribution and deployment processes; and
- d) processes impacted or required by the application.

6.3.6 Technological context

All product and technological components supporting critical specifications or critical data should be protected, such as:

- a) terminal, network and other authorized peripherals;
- b) operating system, configuration and services;
- c) authorized communication links and ports;
- d) COTS and other products, such as Database Management Systems DBMS used by the application and its technological infrastructure;
- e) qualification and other processes associated with the technological context; and
- f) products impacted or used by the application.

6.3.7 Application specifications

All application specifications should be protected against unauthorized modifications, such as:

- a) hardware specifications;
- b) security specifications;
- c) application functionalities;
- d) client terminal specifications; and
- e) back office specifications.

6.3.8 Application data

All critical application information should be protected, such as:

- a) application configuration data;
- b) application binary code;
- c) application source code;
- d) application and library components; and
- e) application documentation of critical components and functionalities.

6.3.9 Organization and user data

All critical organization and user information should be protected, such as:

- a) certificates;
- b) private keys;
- c) mission-critical data;
- d) personal data; and
- e) user configuration data.

6.3.10 Roles and permissions

All critical identity management and permissions information should be protected, such as:

- a) identity management data;
- b) identification and authentication data; and
- c) authorization data.

6.4 Application security requirements

6.4.1 Application security requirements sources

As discussed in ISO/IEC 27005, application security requirements are identified by risk assessment and risk treatment, and are dictated by such factors as application specifications, the application's target environment (business, regulatory and technological contexts), critical data and choices made by the application owner.

Functional security requirements dictate which security functionalities will be implemented in the application. Non-functional security requirements address security qualities that the application should exhibit. These controls should already have been globally defined and approved by the organization.

6.4.2 Application security requirements engineering

Application requirements engineering is the broader process of gathering, analysing and specifying requirements for an application. It should be enhanced with risk assessment to incorporate security requirements.

As with any requirement, risk assessment should involve the use of repeatable and systematic procedures that will ensure that the set of requirements obtained is complete, consistent, and easy to understand and analysable by the application owner. Also, the requirements and the achievement thereof should be measurable.

6.4.3 ISMS

6.4.3.1 Organization ISMS

All information held and processed by an organization is subject to risks of error, flood, fire, theft, etc., and to hazards related to the technology in use. The term 'information security' is predicated on information as an asset with an assigned value requiring appropriate protection. According to ISO/IEC 27000, an Information Security Management System (ISMS) provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of an organization's information assets based on a business risk approach. The protection of organization information assets should be aligned with associated risks and business acceptance levels.

This management of risks relies on information security and covers all forms of risk associated with all forms of information usage by the organization.

6.4.3.2 Application security in the context of an ISMS

Application security supports organization-wide ISMS goals by providing a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of the organization's information assets associated with its applications. Application security should provide adequate controls and evidence to prove to the organization's managers that the risks involved in utilizing an application are managed adequately.

ISMS governs application security by ensuring that all risks involving organizational information are managed, including information accessed by applications. The controls required by the ISMS are extended down to the application level.

6.5 Risk

6.5.1 Application security risk

Application security risk is the risk to an organization posed by use of a specific application.

Application security risk comes from:

- a) threats targeting the information accessed by an application;
- b) vulnerabilities; and
- c) impact of successful exploitation of vulnerabilities by threats.

The activity of identifying, tracking, storing, measuring, and reporting application risks is of the utmost importance. Application security requirements and the controls to address them are a reaction to this risk. An application security risk assessment process is needed because risk changes over time, resulting in the need for continuous and consistent identification and storage of risk information.

6.5.2 Application vulnerabilities

Vulnerabilities are the result of inadequate or nonexistent controls. Inadequately controlled vulnerabilities result in unacceptable application risk.

Vulnerabilities come from:

- a) actors, such as programmers who write poor code, users who make errors using the software and technicians and developers who make errors while maintaining the application;
- b) processes, such as inadequate testing procedures, poor project management, insufficient focus on security throughout the life cycle processes, unanticipated interactions among applications, users and operators, inadequate change management processes;
- c) the technological context, such as bad choices of technological infrastructure or products; and
- d) specifications, such as inadequate design, vulnerabilities due to system interactions or errors in component interfaces.

6.5.3 Threats to applications

A threat has the potential to harm critical information in the application scope, and thereby the organization itself. Threats come from:

- a) the application's environment: regulatory context, business context and technological context; and
- b) actors.

6.5.4 Impact on applications

An impact is the cost to an organization of suffering a breach in availability, integrity or confidentiality of its critical application data.

6.5.5 Risk management

Application security risk management is the process of maintaining application security risks within acceptable levels. This is achieved by treating application security risks that are judged to be unacceptable, more specifically by applying controls to them.

Risk management is a key concept in information security. According to ISO/IEC 27005, *"the information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service), any information system, existing or planned or particular aspects of control (e.g. business continuity planning)."*

The information security risk management process presented in ISO/IEC 27005 consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review.

An application security risk management process should use the same process elements, with finer granularity and a scope adjusted to the application level.

6.6 Security costs

The cost to an organization of implementing, maintaining and verifying security controls should be minimized to an acceptable (or tolerable) level after proper consideration of the risks and related impacts of using an application. The cost of security should take into account the potential impact of threats and vulnerabilities.

6.7 Target environment

The target environment is comprised of the regulatory, business and technological contexts within which the organization will use its application. All threats that might harm an application come from its environment. For this reason, the application's target environment should be clearly defined at the beginning of an application project.

To successfully and securely deploy the application, the organization's technological context should comply with the application's target environment requirements. Once the application has been implemented, the organization's technological context might add new products and hardware that could impact the security of other applications and influence the organization's security risks.

Because risks for an organization to use the application come from the application's target environment, new application security requirements should be defined to address these new risks and select controls that mitigate these risks to an acceptable (or tolerable) level. These security controls can be introduced into the application life cycle processes (such as the Acquisition Process or the Disposal Process), added to the application's source code or integrated elsewhere in the application life cycle (see 8.3.4) as needed by the organization.

6.8 Controls and their objectives

As specified in ISO/IEC 27001, controls and their objectives should be selected and implemented to meet the requirements determined by the risk assessment and risk treatment processes. In application security, the risk assessment process determines the control objectives as defined by the application security requirements.

7 ISO/IEC 27034 overall processes

7.1 Components, processes and frameworks

ISO/IEC 27034 provides components, processes and frameworks to help organizations acquire, implement and use trustworthy applications, at an acceptable (or tolerable) security cost. More specifically, these components, processes and frameworks provide verifiable evidence that applications have reached and maintained a Targeted Level of Trust.

All components, processes and frameworks are part of two overall processes, as shown in Figure 3:

- a) the ONF Management Process, and
- b) the Application Security Management Process (ASMP).

These two processes are used at different levels and time frames within the organization and have different scopes. The ONF Management Process is a continuous organizational-level process and the ASMP is used for managing security on specific application projects.

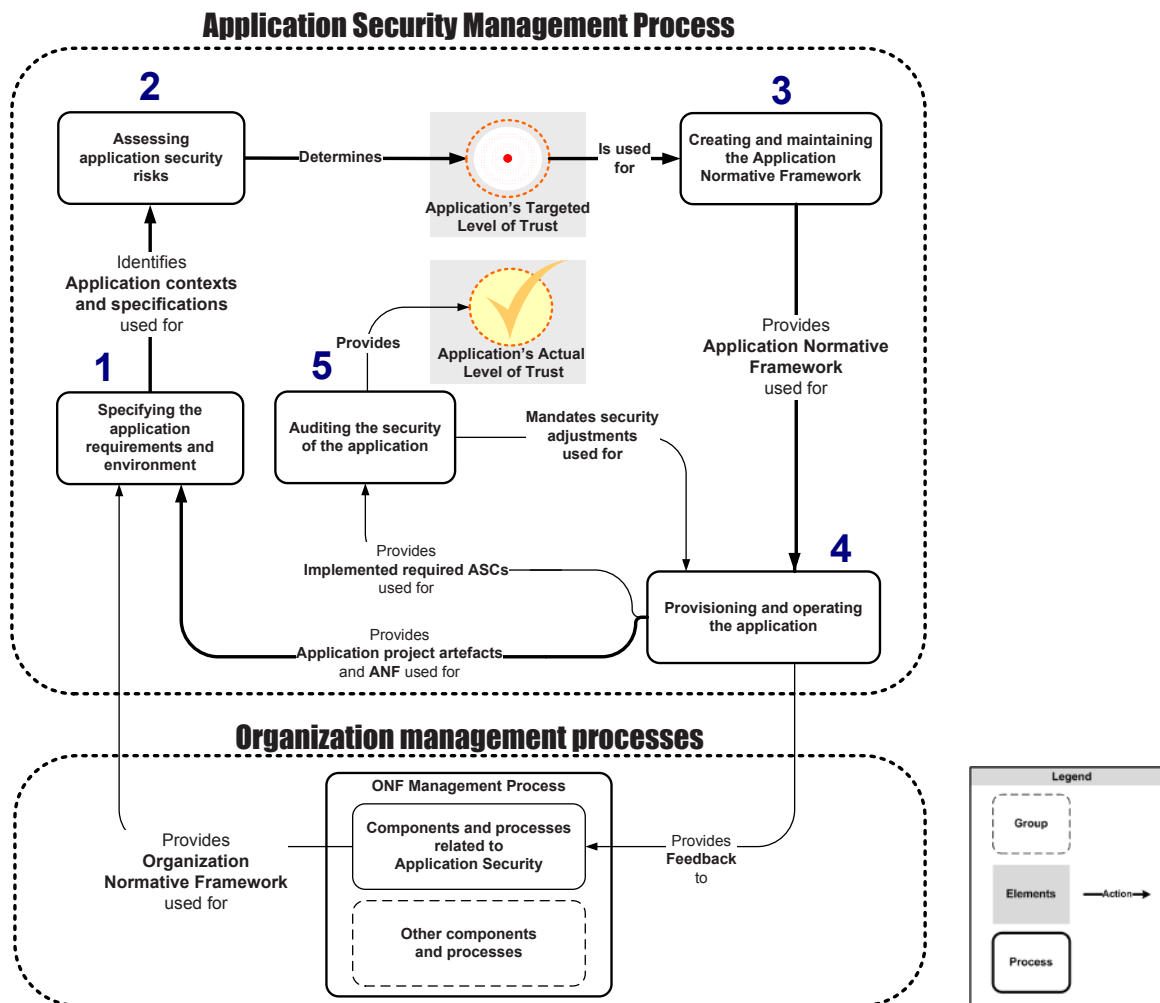


Figure 3 – Organization Management Processes

7.2 ONF Management Process

This process should be used for managing the **application security-related** aspects of the ONF (Organization Normative Framework, see 8.1). This framework contains all processes involved in application security, as well as regulations, laws, best practices, roles and responsibilities accepted by the organization. It defines all organization's contexts and becomes the unique referential for application security within the organization.

NOTE 1 The organization normally uses its normative framework for other purposes that fall outside the scope of ISO/IEC 27034, and normally has defined processes for managing it. Thus, the ONF and its management process, for the purposes of ISO/IEC 27034, is a subset of the existing ONF and related processes.

Application security-related processes should be part of the ONF.

Oversight and responsibility for maintaining and approving the application security-related components of the ONF should be assigned to an organizational role, which is referred to as the "ONF committee" in ISO/IEC 27034.

NOTE 2 The ONF Management Process and its associated components and sub-processes are presented in more detail in subclause 8.1.3.2, as well as in ISO/IEC 27034-2.

7.3 Application Security Management Process

7.3.1 General

The Application Security Management Process is the overall process for managing security for each application used by an organization. Annex C demonstrates that the ASMP is a specialization of the risk management process presented in ISO/IEC 27005.

The Application Security Management Process is performed in five steps:

- a) Specifying the application requirements and environment;
- b) assessing application security risks;
- c) creating and maintaining the Application Normative Framework;
- d) provisioning and operating the application; and
- e) auditing the security of the application.

NOTE The ASMP is presented in more detail in clause 8, as well as in ISO/IEC 27034-3.

7.3.2 Specifying the application requirements and environment

The first step of the ASMP is to specify all application requirements, including:

- a) actors;
- b) specifications;
- c) information; and
- d) environment.

The application's environment consists of

- a) a technological context,
- b) a business context, and
- c) a regulatory context.

NOTE Contexts are presented in more detail in clauses 8.1.2.1 to 8.1.2.2.

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.

7.3.3 Assessing application security risks

The second step of the ASMP is a process corresponding to the “risk assessment” step and a part of the “risk treatment” step in the risk management process established by ISO/IEC 27005, with a finer granularity level and a scope limited to a single application project.

Risk assessment consists of risk identification, risk analysis and risk evaluation.

This step of the ASMP also produces security requirements, which are used to obtain the desired level of trust for the application. This is called the application's Targeted Level of Trust (see 8.2.4). It should be approved by the application owner.

For this reason, this step also corresponds to the “Selection of risk treatment options” part of the “risk treatment” step in the risk management process established by ISO/IEC 27005.

7.3.4 Creating and maintaining the Application Normative Framework

The third step of the ASMP selects all the relevant elements from the ONF that apply to a specific application project. This results in the Application Normative Framework (ANF). The application's Targeted Level of Trust, the application contexts (regulatory, business and technological), the actors' responsibilities and professional qualifications, and the application specifications determine the exact contents of the ANF.

It is also during this step that the organization derives the life cycle for the application project, which contains only those activities needed for the application project. For example, a project developed entirely in-house does not require outsourcing activities.

In addition, the organization selects the applicable Application Security Controls for the application project.

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.

NOTE This step of the ASMP and its associated components and processes is presented in more detail in 8.3.

7.3.5 Provisioning and operating the application

The fourth step of the ASMP is the actual use of the Application Security Controls, as provided by the ANF in the application's life cycle. The project team implements the Application Security Controls under the ANF, in two sub-steps:

- a) the security activity part of each ASC is performed by the corresponding actor assigned in the ASC; and
- b) the security measurement part of each ASC is performed by the corresponding actor assigned in the ASC.

This fourth 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.

NOTE This step of the ASMP and its associated components and processes is presented in more detail in 8.4.

7.3.6 Auditing the security of the application

The fifth and final step of the ASMP is the security audit of the application.

In this step, a verification team verifies that all the verification measurements provided by all the ASCs in the Application Normative Framework have been performed and that the expected results were attained.

This step corresponds to the “Monitoring and review” step in the risk management process established by ISO/IEC 27005.

NOTE This step of the ASMP and its associated components and processes is presented in more detail in 8.5.

8 Concepts

8.1 Organization Normative Framework

8.1.1 General

The Organization Normative Framework (ONF) is a framework where all application security best practices recognized by the organization are stored, or from which they will be refined or derived. It comprises essential components, processes that utilize these components, and processes for managing the ONF itself.

The ONF is the foundation of application security in the organization and all the organization's application security decisions are based on it. For example, an activity of code review can only be performed as a mandatory Application Security Control if coding guidelines exist in the ONF.

As shown in Figure 3, the ONF is the main input for the ASMP which is performed for each application project in the organization.

Figure 4 shows a high-level view of the ONF contents.

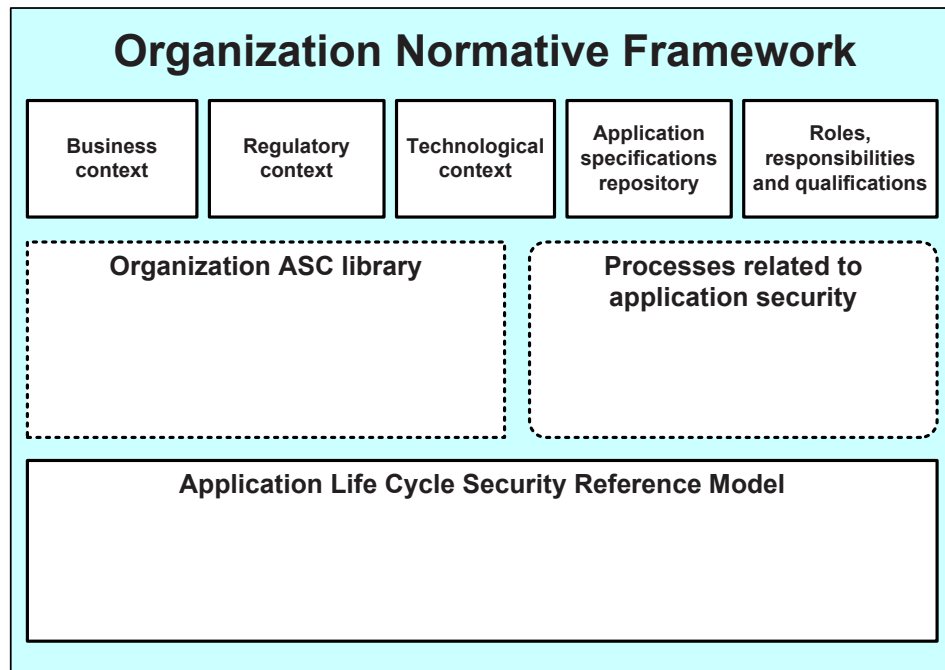


Figure 4 – Organization Normative Framework (simplified)

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

- a) business context;
- b) regulatory context;
- c) technological context;
- d) application specifications repository;
- e) roles, responsibilities and qualifications;
- f) organization ASC Library;
- g) processes related to application security;
- h) Application Security Life Cycle Reference Model.

Also, the formal ONF should contain the following processes:

- a) ONF Management Process; and
- b) ONF management subprocesses.

8.1.2 Components

8.1.2.1 Business context

The business context lists and documents all standards and best practices adopted by the organization that could impact application projects.

The business context includes:

- a) project management, development, risk analysis, operational, audit and control processes;
- b) the organization's security policy;
- c) practices for the business domain;
- d) the development methodology used by the organization;
- e) best practices for all programming languages employed by the organization and listed in the technological context;

- f) the organization's formal project management process; and
- g) the adoption of other relevant ISO/IEC International Standards, such as ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 15288.

8.1.2.2 Regulatory context

The regulatory context lists and documents any law or regulation, in any of the organization's business locations, that could impact application projects. It includes laws, rules and regulations of the countries or jurisdictions where the application is developed and/or deployed and/or used.

An organization deploying and/or using the same application in more than one country might have to meet different security requirements for each country.

8.1.2.3 Application specifications repository

The application specifications repository lists and documents the organization's general IT functional requirements and corresponding pre-approved solutions. Application specifications should include:

- a) specifications about how applications should compute, store and transfer information;
- b) usual application parameters, functionalities, services and requirements; and
- c) source code, binary code, libraries and products or services used or relied upon by applications.

Additional specifications may include those detailing how the application interacts with:

- a) other systems;
- b) the runtime infrastructure upon which it depends; and
- c) the list of controls within the runtime environment.

8.1.2.4 Technological context

The technological context comprises the inventory of all IT products, services and technologies available to the organization for application projects. These products, services and technologies determine the threats to which applications are exposed.

The technological context includes computers, tools, IT products and services, communication infrastructure and other technical devices.

EXAMPLE 1 Technological contexts that might have an impact on application security include client-server infrastructure, web infrastructure, network infrastructure and development environment and tools.

The technological context also determines the feasibility of introducing certain Application Security Controls into an application.

EXAMPLE 2 If the technological context does not include the TLS 1.0 authentication mechanism to support "bi-directional authentication" functionality, a TLS 1.0 based ASC may not be included in an application. A project team would have to select an alternative ASC in order to obtain the bi-directional authentication functionality, if that functionality is required at the application's Targeted Level of Trust.

The technological context should include:

- a) technologies available for application projects in the organization;
This inventory of technologies should be continuously updated by the organization's ONF committee via feedback from previous application projects.
- b) technologies required by an application;
The list of new technologies comes from new functional requirements specified in the course of the instigation planning of an application project. Such requirements should be added to the ONF and an organizational process should ensure that security characteristics of the technologies set apart for fulfilling the new requirements are understood and documented before being approved for inclusion in the organization's inventory of technologies; and
- c) available technologies;
This comes from research, trend analysis, and technology monitoring.

8.1.2.5 Roles, responsibilities and qualifications

The ONF should contain:

- a) lists and descriptions of all roles, responsibilities and required professional qualifications for actors involved in creating and maintaining the ONF and/or roles for creating and maintaining ASCs; and
- b) lists and descriptions all roles, responsibilities and required professional qualifications for actors involved in the organization's application life cycle, such as information security managers, project managers, administrators, software acquirers, software development managers, application owners, user managers, architects, analysts, programmers, testers, system administrators, database administrators, network administrators and technical personnel.

This is an organization-wide policy that will help ensure that all critical roles for all processes are filled, that all responsibilities are defined, that conflicts of interest are avoided, and that people filling the roles have sufficient professional qualifications.

8.1.2.6 Organization ASC Library

8.1.2.6.1 General

AC1 The organization should define a library of controls for application security. **AC1** This library is called an Application Security Control Library (ASC Library). It lists and documents all ASCs recognized by the organization. These ASCs evolved from standards, best practices and roles, responsibilities, and professional qualifications, technological, business, and regulatory contexts and application specifications.

Application Security Controls within this library are organized in sets according to the level of protection they provide against security threats. **AC1** Each set receives a label called 'level of trust' to inform managers of the degree of security obtained from a particular defined set of controls. **AC1** If a set of controls is described as having a low level of trust, it provides limited protection of information security. If a set of controls is defined as having a high level of trust, then it provides a high level of protection. Levels of trust are further described in 8.1.2.6.4.

Precise and detailed ASCs for each specific application project are selected from this organizational ASC library.

8.1.2.6.2 Example of an Organization ASC Library

Figure 5 shows a simple example of an organization's existing ASC Library. The organization in this example develops applications in the field of aeronautics. The library contains all of the controls that the organization needs for implementing functionalities, best practices, standards, applicable laws and regulations.

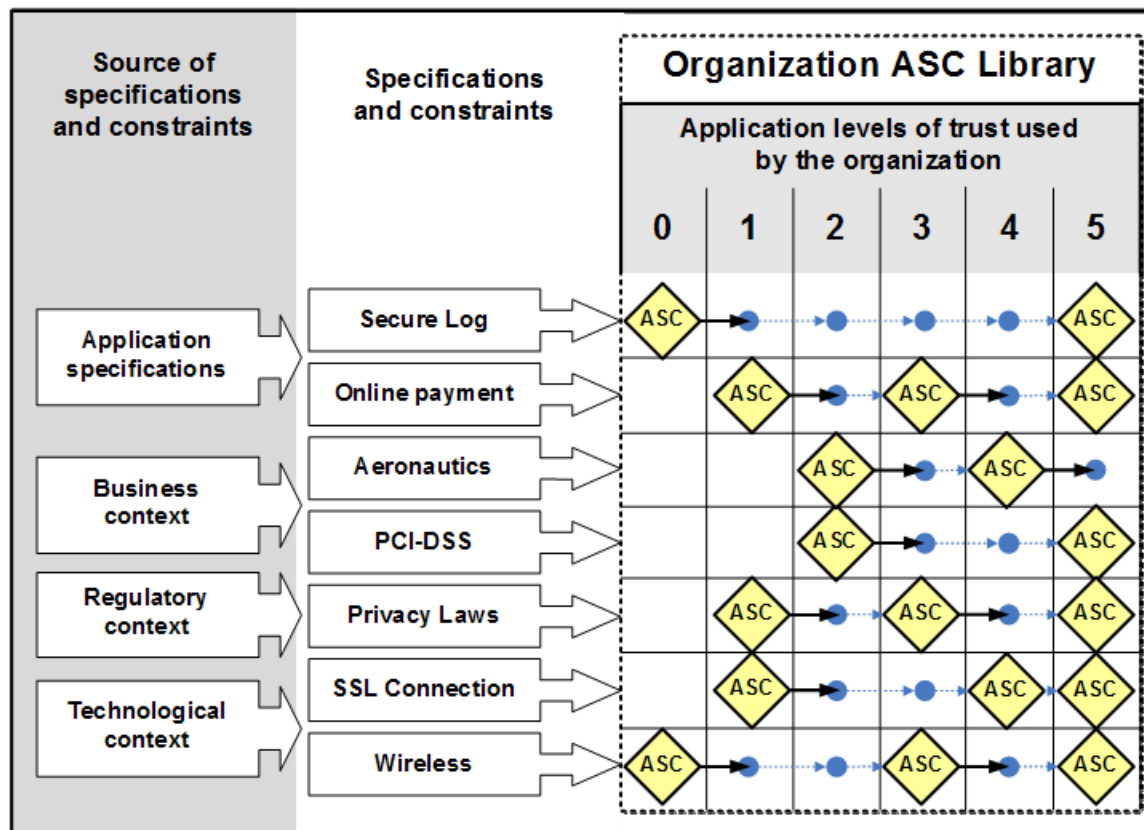


Figure 5 – Graphical representation of an example of an Organization ASC Library

In this example, the organization has defined two application specifications: secure logging and on-line payment. The business context in which this particular organization is the field of aeronautics, and it implements the PCI-DSS industry standard. The regulatory context imposes compliance with certain privacy laws. The technological context shows that this organization has defined controls for SSL connections and for wireless networking.

This simple example shows that the organization's application specifications, as well as its business, regulatory and technological contexts determine the contents of an organization's ASC Library. Each organization's ASC Library will thus be specific to that particular organization.

8.1.2.6.3 Process for creating the Organization ASC Library

The process for creating the ASC Library is simple and can be easily performed by even the smallest organizations.

The library is empty at first. ASCs are added by grouping them in columns corresponding to needed levels of trust (see the columns in Figure 5). An organization might need more than one level of trust for its applications.

It is the ONF committee's responsibility to build an ASC library that satisfies the organization's particular needs and requirements.

This goal is best achieved by analyzing the organization's new or existing applications. This analysis involves determining the security risks and requirements for the application, then selecting or creating ASCs to meet those requirements. For each application analyzed, the result is a set of ASCs.

This set of ASCs can match the existing ASC library in three possible ways:

- a) the entire set of ASCs already comprises an existing level of trust in the library, in which case nothing is added to the library;
- b) an existing level of trust closely matches the full set of ASCs, in which case the library can be completed by ASCs from the set; or
- c) a new level of trust is created in the library from the set of ASCs.

Thus, an organization might decide to build from its existing expertise by re-using security controls from its existing applications, or it could create or acquire new controls, or both.

The organization's ASC library expands in response to feedback from each new application project, as outlined in 8.1.3.2.

8.1.2.6.4 Application Level of Trust

A Level of Trust is a label which simplifies the communication between actors from different domains, with different forms of involvement in application security within an organization. It is defined by an organization for the purpose of unambiguously identifying a particular set of controls.

EXAMPLE 1 In Figure 5, the organization has defined six levels of trust, represented by the rightmost columns labeled "0" to "5".

EXAMPLE 2 In Figure 5, Level of Trust "1" identifies a set of three ASCs pertaining to online payment, privacy laws and SSL connections. Furthermore, ASCs pertaining to secure logging and wireless, defined in Level of Trust zero, also apply at level 1, as shown by arrows ending with a blue dot.

An application's Level of Trust is not the result of a calculation, unlike the concept of risk, which is the calculated result of a risk analysis. Level of Trust is thus not complementary to risk.

Rather, a Level of Trust is similar to the concept of a "security plan", which is a set of controls authorized by an organization in order to reduce the risk that was determined by a risk analysis. For any given organization, each Level of Trust is thus similar to a pre-defined, re-usable security plan.

The organization should define its own range (or domain, or scale) of Levels of Trust that the organization's ONF committee should authorize as possible values for an application's Targeted Level of Trust. This range can be defined in any way that suits the organization.

EXAMPLE 3 An organization might use, as in the example in Figure 5, numeric levels from 0 to 5. Another organization might use a domain of defined values such as [low, medium high], [green, yellow, red]. Another organization might use criteria based on risk acceptance criteria.

The organization should define a minimum acceptable Level of Trust for each of its applications. ISO/IEC 27034 uses the name "level zero of trust" to identify the minimum acceptable level of trust (as opposed to the maximum acceptable risk). An organization may use any name for this level of trust.

The organization should monitor the Level of Trust achieved by applications and take corrective action if any application falls below level zero at any time, especially after the application has been deployed.

EXAMPLE 4 In Figure 5, the ONF committee has defined an ASC at level zero of trust for any application using secure logs or wireless transmission. Even if the application's Targeted Level of Trust determined by the risk analysis for this application is the level zero of trust, this ASC should still be performed.

8.1.2.6.5 Application Security Control

8.1.2.6.5.1 General

The Application Security Control is a central concept in ISO/IEC 27034. It is used for introducing security activities into the application's life cycle and articulates the supporting evidence needed to verify its successful application.

The concept of security control is widely used in the information security industry. Thousands of relevant security controls are published and widely available from sources such as ISO/IEC 15408-3 and NIST Special Publication 800-53.

An ASC is a security control used in application projects, defined using a precise structure presented in the following sub clauses. Annex B provides an example illustrating how security controls from NIST SP 800-53 can be described using the ASC structure.

For organizations having implemented the concept of assurance case as defined in ISO/IEC TR 15026-2, ASCs are useful for simplified management and timely provision of evidence needed to support claims and arguments about the security of an application. Further support to arguments is provided by the organization's consistent use of processes proposed by this IS for the creation, approval and use of each ASC. Because the whole set of ASCs selected for the application project originates from the application security risk analysis, it directly supports top-level claims, justifications and arguments about the security of the application.

ASCs can be used for:

- a) securing application components, including software, data, COTS and infrastructure;
- b) adding security activities to processes used during stages in the application's life cycle;
- c) verifying roles, responsibilities and professional qualifications of all actors involved in a project;
- d) determining evaluation/acceptance criteria for components; and
- e) helping to determine the application's Actual Level of Trust.

Figure 6 shows that the ASC provides the application project team with a security activity (i.e., to reduce or limit a specific security risk, and the verification team with a verification measurement activity (i.e., to confirm that the corresponding security activity has been successfully performed by examining the supporting evidence).

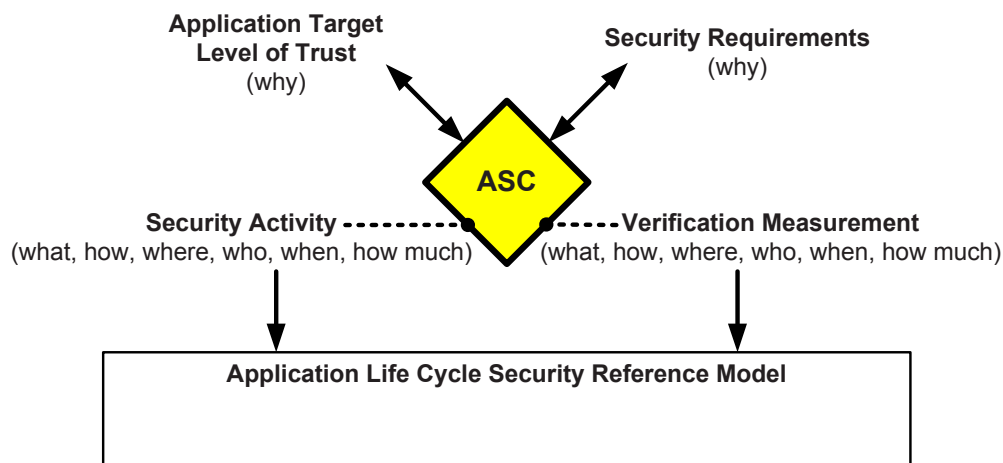


Figure 6 – Components of an ASC

The activity portion of the ASC specifies how security issues for the application project are addressed.

The measurement portion of the ASC specifies how to provide evidence that the activity was performed correctly, by a qualified actor, and that the expected results were obtained.

Both the activity and the measurement provide an estimated cost which will help the organization to evaluate and approve the total cost of security controls in regard to the Targeted Level of Trust.

ASCs can be linked together in a graph, so that, once the activity in an ASC has been performed, it can be followed by the activities of children ASCs. This ASC characteristic is useful for:

- a) providing only relevant information to the different actors, by concealing unnecessary complexity;
- b) facilitating communication by grouping relevant ASCs under headings using appropriate vocabulary, for example, using business-level language when communicating with managers;
- c) facilitating distribution of ASCs by grouping them into related sets; and
- d) ensuring that all security activities in linked ASCs are performed and none are bypassed.

Figure 7 shows an example of this graph relationship, in which a set of ASCs are linked together under the heading “Online payment”. In this example, all ASCs relating to online payment can be used as a single set and this complexity can be concealed if necessary.

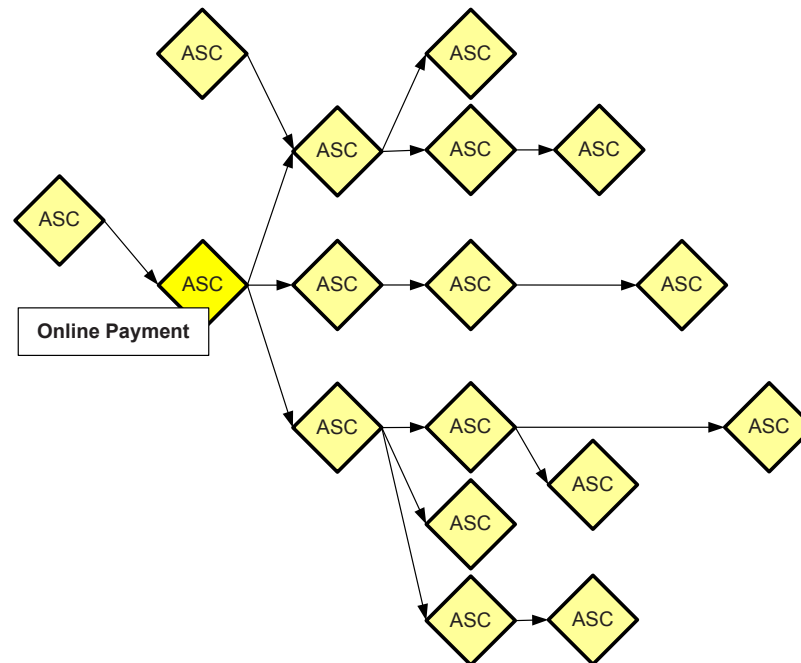


Figure 7 – Graph of ASCs

An ASC is a complex data structure which will be further detailed in document “PART 5 – Protocols and ASC data structure”. A brief overview follows.

NOTE Although ISO/IEC 27034-5 will formalize the structure of the ASC, organizations may still refer to ISO/IEC 15289 for guidance on specifying information items to be produced during their applications' life cycles.

8.1.2.6.5.2 ASC Identification

The ASC identification section contains information such as:

- a) ASC information: ASC name, ID, author, date, description, etc.;
- b) pointers to parent and children ASCs (an ASC can be represented as a graph structure); and
- c) pointers to the relevant business, regulatory, and technological contexts, as well as the application specifications that provide the security requirements for this ASC (see Figure 5).

8.1.2.6.5.3 ASC Objective

The ASC objective specifies “why” this ASC exists, namely the security requirements for which this ASC was designed.

The ASC objective specifies:

- a) which elements of its security activity need to produce supporting evidence for their corresponding verification measurements;
- b) for which levels of trust the ASC is mandatory;
- c) application specifications or requirements with which the ASC is associated, and which can refer to applicable regulations, standards and best practices; and
- d) security threats and assumptions about the application’s operating environment.

An ASC can be associated with several levels of trust.

EXAMPLE In Figure 5, an ASC has been defined at the level 1 of trust for any applications involving online payment. This ASC is mandatory for all projects which develop an application involving online payment where a Targeted Level of Trust from 1 to 2 has been

assigned by the application owner. If the application owner wishes to assign the application a targeted level 3 of trust, then an ASC with a stronger security activity and/or measurement is needed.

8.1.2.6.5.4 ASC Security Activity

This element describes the steps or procedures required to implement the activity. It should define at the very least:

- a) What:
 - 1) complete description of the security activity;
 - 2) activity's complexity;
 - 3) artefacts produced by this activity. This artefact articulates the supporting evidence necessary to demonstrate the presence of the introduced application security control processes or procedures (i.e., the ASC activity);
 - 4) expected ASC activity outcomes (namely, a description of the resulting situation, status or precise artefact value produced by the activity);
- b) How: technique for performing this activity and obtaining the artefact, such as identification of source code used for implementing secure connections to a LDAP service, identification of library used for encryption, or document providing guidance for performing the activity;
- c) Where: the target of the security activity, such as source code, application parameters, infrastructure component, process.
- d) Who: required qualifications for actors who should perform this activity. Actors are subjected to ASCs (possibly in the form of formal organizational appointments) because the organization should ensure that the required professional qualifications for each role are attained, and that the principle of separation of duties is respected. ASCs should be written for the express purpose of verifying professional qualifications;
- e) When: pointer to a specific activity in a stage in the Application Security Life Cycle Reference Model (see 8.1.2.7) where this activity should be performed;
- f) How much: estimated cost to perform this ASC activity.

8.1.2.6.5.5 ASC Verification Measurement

This part presents the verification control that is performed for verifying the successful performance of the corresponding ASC activity. The Verification Measurement should define at least:

- a) What:
 - 1) complete description of the security measurement. This description specifies how to verify the existence and correctness of the artefact produced by its ASC activity;
 - 2) measurement complexity;
 - 3) artefact produced by this measurement. This artefact articulates the supporting evidence necessary to demonstrate that the ASC has been verified;
 - 4) expected results (situation, status or precise artefact value description); and
- b) How: technique for performing this measurement and obtaining the artefact, such as code review tools and settings, or document providing guidance for performing the measurement;
- c) Where: the target of the verification activity, namely the precise characteristics of the artefact produced by corresponding ASC activity that are being verified.
- d) Who: professional qualifications required for actors involved in the verification control. Actors are subjected to ASCs (possibly in the form of formal organizational appointments) because the organization should ensure that required professional qualifications for each role are attained, and that the principle of separation of duties is respected. ASCs should be written for the express purpose of verifying professional qualifications;
- e) When: a pointer to a specific activity in a stage in the Application Security Life Cycle Reference Model (see 8.1.2.7) where this measurement should be performed. This measurement can be performed periodically if required;
- f) How much: estimated cost to perform one occurrence of this verification measurement activity.

8.1.2.7 Application Security Life Cycle Reference Model

8.1.2.7.1 General

An organization whose business involves developing, outsourcing or acquiring applications generally uses a framework of defined processes and activities organized into stages. This framework is commonly named “life cycle model”. Depending on the context, it is referred to as either “application life cycle model”, “system life cycle model” or “software life cycle model”. It is not a new concept brought by ISO/IEC 27034. Its definition is found in International Standards ISO/IEC 12207 and ISO/IEC 15288.

Such a framework is unique and customized for a particular organization. It has been in use and refined over the years.

A specific application’s life cycle, i.e. the evolution of the application from conception through retirement, is an instantiation of the organization’s life cycle model.

It is possible for different groups within complex organizations to use different application life cycle models for different projects. Such is often the case in large organizations which are formed through mergers or which are decentralized. Other organizations have developed different specialized application life cycle models related to specific application contexts such as web applications, real-time applications, embedded applications, medical applications, etc.

Activities performed during stages in a software or system life cycle are part of organization-wide processes which should be compatible with the normative requirements provided in ISO/IEC 12207 and ISO/IEC 15288. In addition, ISO/IEC TR 24748 provides additional guidance and describes models for system and software development life cycles, life cycle stages and their relationship to life cycle processes.

ISO/IEC 27034 does not impose or even recommend a change in the organization’s application life cycle model. ISO/IEC 27034 instead adds activities called “Application Security Controls” (ASCs) to the activities usually performed in the stages defined by the organization’s application life cycle model.

As previously discussed in 8.1.2.6.5, ASCs include pointers to specific point in a stage in the life cycle, thus specifying “when” security activities and verification measurements should be performed.

Currently, there are many software and system life cycle models from which an organization can choose for its internal needs. It is neither possible nor desirable for ISO/IEC 27034 to refer to all of them or to prefer one over another. It is thus impossible to have an ASC in the standard pointing directly to a stage, process or activity in a particular life cycle model. This would make the ASC concept of ISO/IEC 27034 less portable to organizations in the wider community.

The solution to this problem is to present an Application Security Life Cycle Reference Model as a standardized reference for the addition of ASCs to activities performed for application management, application provisioning and operation, infrastructure management and application audit. This model is a representation of generic stages and activities commonly found in application life cycle models.

This model is not limited to software development. It also makes references to activities from other domains such as governance, software and infrastructure maintenance, project management, audit and control.

The purpose of the Application Security Life Cycle Reference Model is to:

- a) **[AC1]** help the organization to validate each of its application life cycles by specifying all activities and actors potentially involved in application security; **[AC1]**
- b) help the organization to ensure that the security concerns are correctly addressed at all stages of its application life cycles;
- c) help the organization to minimize the cost and impact of introducing ISO/IEC 27034 practices in its application projects by maintaining existing application life cycles;
- d) provide the organization with a standard model for sharing ASCs between its application project teams, despite differing application life cycles; and
- e) provide organizations with a standard model for sharing ASCs with other organizations, despite differing application life cycles.

Figure 8 shows a graphical representation of the Application Security Life Cycle Reference Model proposed by ISO/IEC 27034.

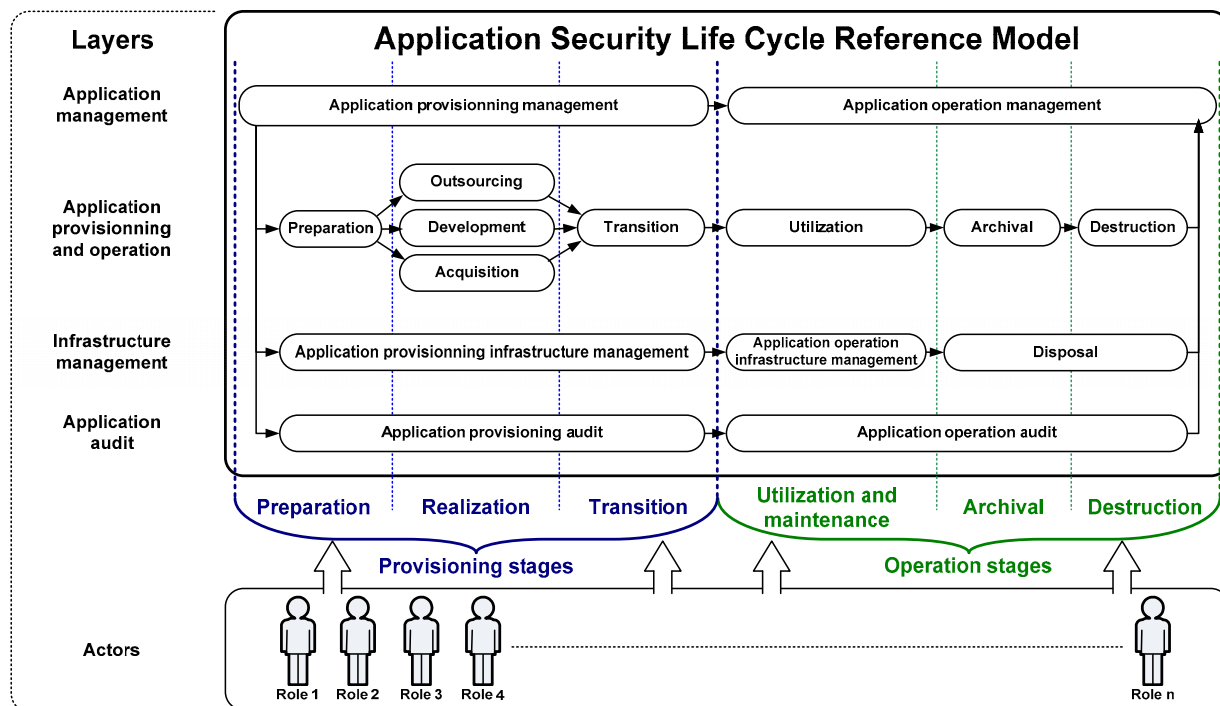


Figure 8 – Top-level view of the Application Security Life Cycle Reference Model

The organization should define a persistent mapping between the stages and activities defined in this reference model and the stages and activities already in use in each of the organization's own model(s). This provides a way to indicate at which point in the organization's own stages and activities ASCs are applied.

The organization's ONF committee will determine the placement of ASCs in the Application Security Life Cycle Reference Model. This act of allocation ensures that minimally acceptable ASCs for the Targeted Level of Trust are uniformly followed during the instigation planning for every application project in the organization.

This reference model is divided horizontally into two main stages: Provisioning, during which activities are performed for obtaining and deploying an application, and Operation, during which post-deployment activities are performed.

Provisioning and Operation stages can be further divided into stages as follows:

- Provisioning stages consist of three stages: Preparation, Realization and Transition;
- Operation stages consist of three stages: Utilization and maintenance, Archival and Destruction.

This reference model is divided vertically into four main layers:

- Application management:** this layer comprises activities from the governance domain, such as project management and application operation management. Such activities are usually performed within processes defined in the organization's ISMS;
- application provisioning and operation:** this layer comprises activities relating to the provisioning and use of the application itself. Such activities are usually performed within processes recommended by standards such as ISO/IEC 15026 Series, ISO/IEC 15288, ISO/IEC 12207 and ISO/IEC 21827;
- infrastructure management:** this layer comprises activities relating to the organization's IT service management infrastructure supporting the application. Such activities are usually performed within processes recommended by standards such as ISO/IEC TR 20000-4; and guidance products, such as ITIL; and

- d) application audit: this layer comprises activities relating to control and verification. Such activities are usually performed within processes recommended by standards such as ISO/IEC 15288, ISO/IEC 12207 and industry practice documents, such as CobiT.

Actors represent all persons involved in all stages of all layers of the model, such as project managers, developers, system administrators, database administrators, user managers, application owners, auditors, end-users, support technicians, network administrators, etc.

Activities usually performed in the stages of the Application Security Life Cycle Reference Model and shown in Figure 8 are described as follows.

8.1.2.7.2 Application provisioning management

Application provisioning management activities are carried out by project managers and organizational managers, during the provisioning stages of the application life cycle.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from the Project processes group defined by ISO/IEC 12207, such as Human Resource Management Process, Project Planning Process, Project Assessment and Control Process, and Decision Management Process.

8.1.2.7.3 Application operation management

Application operation management activities are related to the management and use of the application during the operation stages.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Decision Management Process and Information Management Process.

Usually, an application is under the responsibility of its owner who may elect to share some of this responsibility with other actors such as user managers.

Changes to the application during operation stages, such as changes stemming from new regulatory requirements or threats, should be initiated by the application owner, who is responsible of ensuring that the application correctly and continuously addresses the organization's changing security needs.

Through these processes, the application owner will provide the organization's ISMS with the needed assurance and evidence that the governance of application projects is being addressed.

8.1.2.7.4 Preparation

During the preparation stage, the provisioning team carries out preliminary or preparation activities. Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as subclauses 6.3.3 Decision Management Process and 6.3.6 Information Management Process.

8.1.2.7.5 Preparation processes

This set of processes includes activities performed during the preparation stage of an application project.

NOTE These processes include software engineering processes from ISO/IEC 12207 such as subclauses 6.4.1 Stakeholder Requirements Definition Process, System Requirements Analysis and Risk Management.

8.1.2.7.6 Outsourcing

During the realization stage, activities related to the implementation of software are performed by the provisioning team. If the organization is outsourcing some implementation activities, it might need to add specific ASCs to its implementation activities in order to achieve the application's Targeted Level of Trust. For this reason, the Application Security Life Cycle Reference Model presents a specific activities area for outsourcing.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Acquisition Process, Software Documentation Management Process, Software Configuration Management Process and Risk Management Process.

8.1.2.7.7 Development

Activities related to the implementation of software are performed by the provisioning team during the realization stage. If the organization is performing internally some implementation activities, the ASCs added to its implementation activities might be different from those added when purchasing or outsourcing the implementation or application components. For this reason, the Application Security Life Cycle Reference Model presents a specific area for development activities resulting in the implementation of internally developed software.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Risk Management Process, System Architectural Design, Software Architectural Design Process, Software Detailed Design Process, Software Construction Process, Software Documentation Management Process, Software Configuration Management Process, Software Verification Process, Software Validation Process, Software Review Process, Domain Engineering Process and Reuse Asset Management Process.

8.1.2.7.8 Acquisition

Acquisition activities may be carried out by the provisioning team for the purpose of obtaining externally or purchasing the product and/or service that satisfies the needs of the organization. Specific ASCs may be added to those activities. For this reason, the Application Security Life Cycle Reference Model presents a specific area for acquisition activities resulting in the implementation of acquired application components.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Acquisition Process, Software Documentation Management Process, Software Configuration Management Process, Risk Management Process and Implementation Process.

8.1.2.7.9 Transition

This area in the Transition stage includes activities performed by the provisioning team for preparing, configuring, testing and deploying the application in the operating environment defined by the organization.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Software Configuration Management Process, System Integration Process and System Qualification Testing Process.

8.1.2.7.10 Utilization

During the Utilization and maintenance stage, activities involved in the actual use of the application in the operating environment by all users including end-users. Such activities include user and access management, logging, monitoring, security training, etc.

Other activities are carried out for software maintenance and change management, including the updating of application software in order to meet changing information requirements, such as adding new functions and changing data formats. It also includes fixing bugs and adapting the software to new hardware devices.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Software Operation Process and Software Maintenance Process.

8.1.2.7.11 Archival

Archival activities are performed by the operation team when the application is no longer needed in its active state. They include the archival of all the application's information, including the archival of all tools and processes to protect and securely access this information even if the application is not running in the operating environment anymore.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as the Software Disposal Process.

8.1.2.7.12 Destruction

Destruction activities are involved in the secure destruction of all the application's information, including user data, organization's information, user logs, application parameters, etc.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as the Software Disposal Process.

8.1.2.7.13 Application provisioning infrastructure management

This activities area in the provisioning stages includes activities involved in providing and maintaining a secure technological infrastructure in support to the activities of the provisioning team. This includes services, facilities, tools, and communications and information technology assets in the development environment and various test environments.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Infrastructure Management Process and Configuration Management Process.

8.1.2.7.14 Application operation infrastructure management

This activities area in the provisioning stages includes activities involved in providing and maintaining a secure technological infrastructure for the operation stages of an application's life cycle. This includes services, facilities, tools, and communications and information technology assets in the application's operating environment.

Other activities should also be carried out during the operation stages for the secure maintenance of the infrastructure supporting the application. Infrastructure maintenance includes system and network hardware maintenance, backup and recovery, disaster recovery, etc.

Such activities are usually performed as part of organization-wide processes. These include system engineering processes from ISO/IEC 15288 such as Operation Process and Maintenance Process.

8.1.2.7.15 Disposal

Disposal activities are carried out in order to provide an assurance that all information stored on the servers, systems and others technological components used by an application are securely deleted. This allows for the disposal or recycling of these components without undue security risk for the organization.

Such activities are usually performed as part of organization-wide processes. These include system engineering processes from ISO/IEC 15288 such as the Disposal Process.

8.1.2.7.16 Application provisioning audit

Audit activities are performed on all activities, actors, processes, artefacts and application components used or produced during the application's life cycle.

These activities may be performed once or periodically by internal or external audit teams, depending on the Targeted Level of Trust of the application project. They provide the application owner with the needed assurance and evidence that security requirements for the application are met as expected.

Audit activities performed during the provisioning stages are usually different from those carried out during the operation stages. Organizations developing but not operating applications (such as software vendors) might never need to audit applications in operation stages. For this reason, the Application Security Life Cycle Reference Model presents a specific area for audit activities performed during provisioning stages.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Software Audit Process.

8.1.2.7.17 Application operation audit

Audit activities performed during the operation stages are usually different from those carried out during the provisioning stages. Organizations operating only acquired applications might never need to audit applications in provisioning stages. For this reason, the Application Security Life Cycle Reference Model presents a specific area for audit activities performed during operation stages.

Such activities are usually performed as part of organization-wide processes. These include software engineering processes from ISO/IEC 12207 such as Software Audit Process.

8.1.2.8 Processes related to application security

The ONF is the repository for all processes used by the organization. As a result, all of the processes related to the definition, management and verification of application security in the organization should be described in a formal manner in the ONF, including:

- all processes described in ISO/IEC 27034 in clause 8 of this part of ISO/IEC 27034;
- all processes described in subsequent parts of ISO/IEC 27034;
- all processes referred to in ASCs such as incident response plans, business continuity plans, code review procedures and vulnerability testing procedures.

8.1.3 Processes related to the Organization Normative Framework

8.1.3.1 General

Organizational contexts evolve over time. Because of this, ONF components representing these contexts (such as technological, business and regulatory contexts and application specifications) should be kept up to date.

The organization's ONF committee should define, document and authorize processes for creating, approving and maintaining the ONF and all of its components. Roles, responsibilities and required professional qualifications for actors involved in these processes should be specified. For example, Figure 9 shows an overview of the ONF maintenance process.

These processes are mentioned in the present overview and will be discussed in more detail in ISO/IEC 27034-2.

8.1.3.2 ONF Management Process

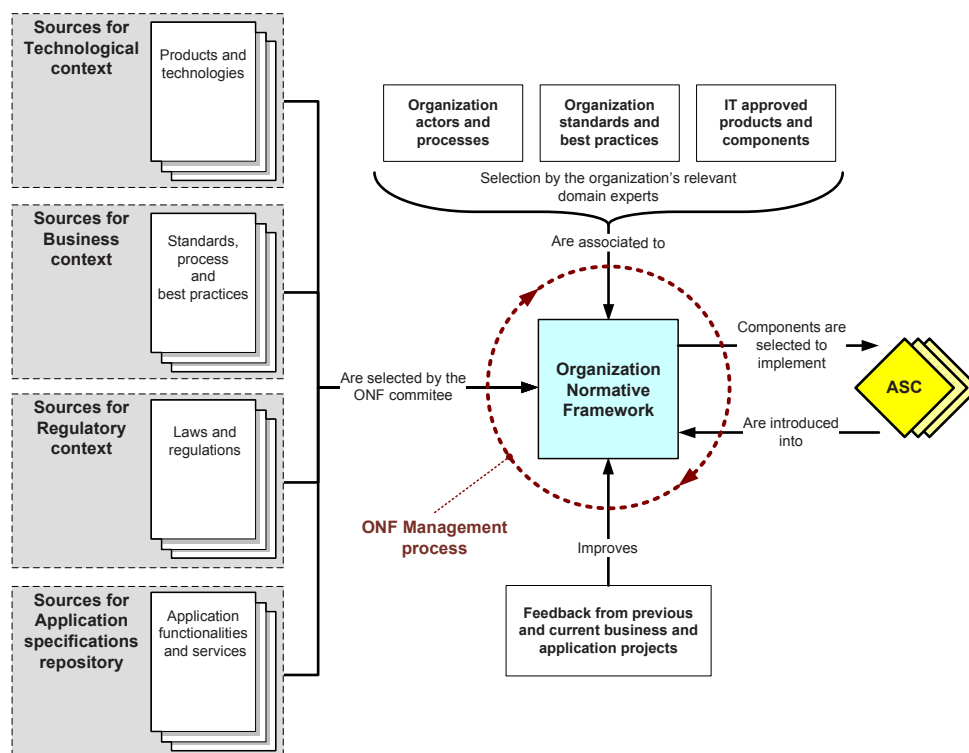


Figure 9 – ONF Management Process

The ONF Management Process (Figure 9) and its sub-processes are permanent, organization-wide processes carried out by the organization's ONF committee. These processes are independent from, and are performed in parallel with, the organization's application projects, as shown in Figure 3.

Goals of the ONF Management Process include:

- a) ensuring that application security needs and the approval of the ASC library and the levels of trust, especially level zero of trust, are still aligned with the organization's business needs;
- b) ensuring that ONF components are updated to reflect changes originating outside the organization; for example, changes to laws can change the regulatory context defined in the ONF;
- c) securing high-management approval of all organization-wide security policies and senior management acknowledgement of the importance of all ONF components;
- d) ensuring approved ASCs are adequately and uniformly applied in an organization-wide manner;
- e) communicating ONF components to all teams in the organization; and
- f) providing feedback to the ONF to include new knowledge, ASC improvement suggestions and new practices gained over the course of an application project.

8.1.3.3 ONF Management subprocesses

All application security-related processes should be part of the ONF. They should also be compliant with the organization's ISMS. The following table shows how application-security-related ONF management subprocesses map to the four stages of the ISMS process.

Table 2 – Mapping of ISMS and application security-related ONF management subprocesses

ISMS Process	ONF management subprocess
Plan	Designing the ONF
Do	Implementing the ONF
Check	Monitoring and reviewing the ONF
Act	Continually improving the ONF

As shown in Table 2, the ONF Management Process can be divided into different subprocesses as follows:

- a) **Designing the ONF:** establishing the application-security-related components of the ONF, including the ASMP, the ASC Library and all related processes;
 - 1) specifying and documenting the possible contexts (business, regulatory and technological) in which the applications will be used;
 - 2) creating, documenting and maintaining the application specifications repository:
 - a. analyzing the specifications for each new application during the supply stage;
 - b. analyzing the specifications of existing applications in the organization;
 - 3) specifying actors and processes:
 - a. analyzing and documenting people and processes involved in the complete application life cycle;
 - b. specifying (or developing) and approving a formal application-level risk analysis methodology based in ISO/IEC 27005;

- 4) analyzing relevant best practices and standards such as ISO/IEC 12207, ISO/IEC 15288 and ISO/IEC 15026 Series and defining ASCs from this analysis;

a. ASC creation and update;

When required by the organization, an ASC is created or updated to address specific security requirements.

Domain experts should define the security activity and the verification measurement, as discussed in 8.1.2.6.5.

EXAMPLE 1 An ASC required to enforce software code security should be created or updated by a senior programmer competent in a specific programming language.

EXAMPLE 2 An ASC required to enforce an application identity management process should be created or updated by an identity management specialist.

b. ASC validation and integration;

A verification team, composed of senior managers and expert developers, IT personnel and auditors, should be responsible for validating an ASC, ensuring it will be clearly understandable for those who use it, and for validating that this ASC in fact mitigates the defined risk. The verification team should also specify at which defined levels of trust this ASC is required.

Approval of all ASCs falls under the ultimate responsibility of the ONF committee.

- 5) analyzing, comparing to the Application Security Life Cycle Reference Model and, as required, adapting the organization's current application life cycle model and other processes;

- 6) defining and implementing the organization's ASC Library;

- 7) acquiring (or developing), updating and validating ASCs required by the organization and integrating them into the ASC Library;

- 8) analyzing, adapting and validating feedback from application projects;

b) **Implementing the ONF:** implementing and communicating the ONF;

c) **Monitoring and reviewing the ONF:** ensuring application projects correctly use the ONF components and gathering feedback from projects:

- 1) requiring a Targeted Level of Trust and an Actual Level of Trust for all applications used by the organization;

- 2) requiring a periodic application risk assessment for all applications used by the organization; and

d) **Continually improving the ONF:** maintaining and improving all components in the ONF, by periodically reviewing the organization-wide contexts, people, processes and technology, finding all changes with a possible impact on the ASMP and integrating them into the ONF.

8.2 Application security risk assessment

8.2.1 Risk assessment vs risk management

Risk assessment is the second step of the risk management process described in ISO/IEC 27005. By the same token, application security risk assessment is the second step of the ASMP, which applies the risk assessment process at the application level. Other steps of risk management are performed by other steps of the ASMP.

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.

8.2.2 Application risk analysis

8.2.2.1 High-level application risk analysis

This is a high level risk analysis performed during the preparation stage of the application's life cycle. It defines, in a simple "rule of thumb" manner, the application's Targeted Level of Trust according to the basic application specifications and the application's technological, regulatory, and business contexts.

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

8.2.2.2 Detailed application risk analysis

This is performed during the realization stage of the application's life cycle. It identifies more precisely the residual risks associated with the specific application before considering any ASCs for the application and reconfirms the application's Targeted Level of Trust (defined during the high-level application risk analysis) for this application according to 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, the application owner might change the application's Targeted Level of Trust for the application project. This changes the ASCs selected for the project, which has an impact on actors involved and the estimated cost of the project. However, such impacts are easily predicted since such information as actors, professional qualifications and estimated cost is already part of each ASC and has already been documented in the organization's ASC library.

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

8.2.3 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; and*
- b) *Priorities for risk treatment considering estimated levels of risks.*"

In ISO/IEC 27034, this step takes the form of selecting the application's Targeted Level of Trust, which in turn determines which ASCs should be implemented for risk treatment.

8.2.4 Application's Targeted Level of Trust

The application's Targeted Level of Trust can aid in achieving the level of confidence required by the organization in order to use or deploy the application in a secure manner, after accepting the residual risks determined by the risk assessment.

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

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's Targeted Level of Trust should be one of (or within the range of) the levels of trust defined in the Organization ASC Library (see 8.1.2.6), which is part of the ONF.

The ASC library (Figure 5) can be represented as a table and the application's Targeted Level of Trust as a column in that table. Thus selecting a level of trust involves selecting all ASCs in that column.

8.2.5 Application owner acceptance

The application owner has the responsibility of accepting the residual risks associated with a specific application.

The application owner performs this acceptance in two ways:

- a) by approving the application's Targeted Level of Trust in step 2 of the ASMP; and
- b) by approving the results of the application security audit in 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.

Once the owner has performed this acceptance, 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.

8.3 Application Normative Framework

8.3.1 General

The Application Normative Framework (ANF) is a subset or refinement of the ONF that contains only the detailed information as required for a specific application to reach the Targeted Level of Trust required by the application owner during the final acceptance process element of step 2 of the ASMP.

Security requirements in the ANF are derived from the assessment of risks associated with the organization's use of the application 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.

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

Changes to the ANF have an impact on the application's security. These changes should receive corresponding approvals from the application owner.

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

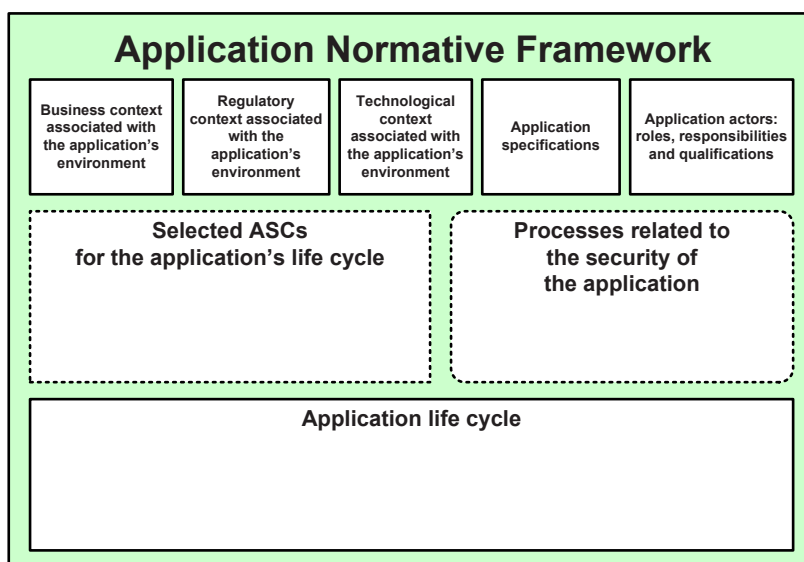


Figure 10 – Application Normative Framework

8.3.2 Components

8.3.2.1 Business context associated with the application's environment

All business processes, methodologies, standards and actors involved in the application project, including external business processes required to provide adequate business integrity in operating environments, are derived or refined from the organization's ONF business context (see 8.1.2.1) for the application.

8.3.2.2 Regulatory context associated with the application's environment

All legal and regulatory requirements applicable in the location(s) where the application is used or deployed are refined or derived from the organization's ONF Regulatory context (see 8.1.2.2) for the application.

8.3.2.3 Technological context associated with the application's environment

All technological components of the application, such as its architecture, infrastructure, protocols and languages, are derived or refined from the organization's ONF technological context (see 8.1.2.4) for the application.

8.3.2.4 Application specifications

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

All data used, stored, computed, shared or transferred by the application should be listed and categorized. This includes organizational data, user data, configuration data, parameters and other data used by the application. This also includes any output from the application.

8.3.2.5 Application actors: roles, responsibilities and qualifications

All actors who interact with the application during its life cycle should be determined. Actors include security officers, application owners, project managers, audit officers, architects, testers, developers, end users, administrators, database administrators and technicians.

8.3.2.6 Selected ASCs for the application's life cycle

As seen in 8.1.2.6, the precise and detailed ASCs for a specific application project are selected from the organization ASC library, according to the following criteria:

- a) the application's Targeted Level of Trust;
- b) the organization's requirements for the application; and
- c) the application's specific contexts and specifications.

Each ASC provides both a security activity performed by the application project team to mitigate a specific security risk, and 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 will no longer need to design them for each new application project. This ensures a constant 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 will accept. The ASCs authorized for level zero of trust should not be changed by the project team in the course of an application project.

8.3.3 Processes related to the security of the application

All relevant processes related to the definition, management and verification of application security, as described in ISO/IEC 27034, should be included in the ANF. This is a refinement of the "Processes related to application security" component of the ONF, as described in subclause 8.1.2.8.

8.3.4 Application's life cycle

The application life cycle component designates the stages and activities selected from the ONF for a specific application project. More specifically, the application's life cycle is a subset of the Application Security Life Cycle Reference Model (see 8.1.2.7) contained in the ONF.

The application life cycle and its standard counterpart the Application Security Life Cycle Reference Model have already been discussed in 8.1.2.7.

It is via the various processes used during the application's life cycle, with which the project and verification teams are already familiar, that the activities and measurements defined by the ASCs are performed.

The preferred approach is therefore to smoothly integrate ASCs as integral parts of processes used during the application life cycle, rather than as distinct external security activities.

8.3.5 Processes

8.3.5.1 Processes related to the Application Normative Framework

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.

The ANF creation process for a specific application is vital. This process transforms the generic information contained in the ONF into specific information required by the ANF for a specific application and its requirements.

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 a specific application's life cycle.

8.3.5.2 Feedback process

The organization should define a process for continuously improving 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.

This process is shown on Figure 3 as "Provides feedback to".

This process should tie into an ONF maintenance process shown in Figure 9 as "Feedback from previous and current business and application projects".

8.4 Provisioning and operating the application

8.4.1 General

The fourth step of the ASMP involves the deployment and follow-up within the application project of the specific ASCs provided by the ANF. Specifically, the application's project team implements the specific security activities described in the ASC "Security Activity" part (as explained in 8.1.2.6.5.4) for each ASC contained in the application's ANF.

This step is made easier for the project and verification teams by supplying them only those ASCs required to reach the Targeted Level of Trust for their specific project. It is not necessary for the teams to be aware of the processes leading to the ANF's.

Project managers will find the ASC to be an efficient tool because it details 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.

The verification team will also find the ASC 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.

The security and technology teams will also find the ASC concept useful because the ASCs contained in a specific application's ANF provide a detailed list of security requirements, thus allowing advance planning of required resources.

8.4.2 Impact of ISO/IEC 27034 on an application project

A typical application project (prior to an organization's implementation of ISO/IEC 27034) is driven by a project team, supported by processes, often automated by technology, with the goal of generating an application. Usually, the quality assurance team follows a test plan to verify the application functionalities against the accepted functional requirements.

The technology itself, the development methodology used by the project 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.

Figure 11 shows how ISO/IEC 27034 adds new roles, responsibilities, components and processes to a typical application project.

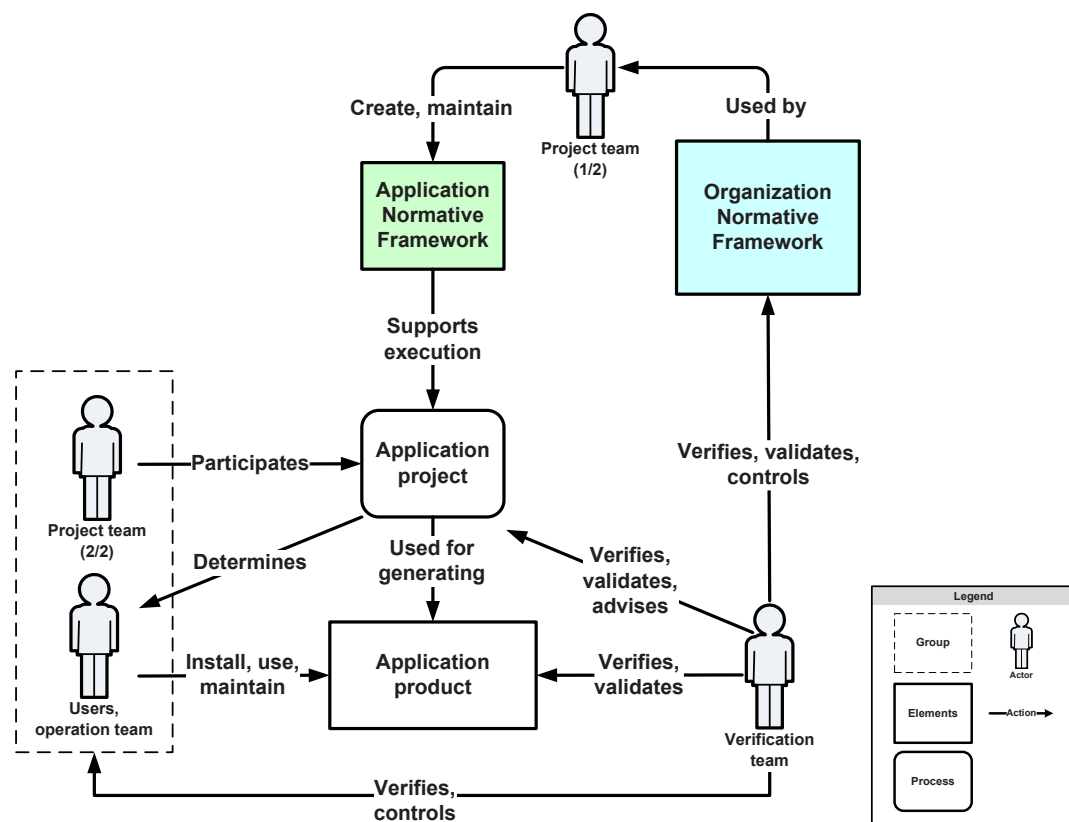


Figure 11 – Impact of ISO/IEC 27034 on roles and responsibilities in a typical application project

Figure 11 shows how roles and responsibilities will be formally specified henceforth. It also shows two vital new components: the ONF and the ANF. The ONF, an organization-wide framework, is not acting directly on the application project. The project team, the verification team and the users will only be impacted by the ANF, a project-specific framework that provides precise and detailed Application Security Controls and corresponding verification measurements.

A verification team has the responsibility of verifying the ONF. This is not only done at the project level (see 8.4.4.2) but at the organization level as well, as part of the ONF Management Process (see 8.1.3.3.d)).

8.4.3 Components

8.4.3.1 Project team

The project team is comprised of 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 ANF for the application project.

8.4.3.2 Operation team

The operation team is comprised of 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.

8.4.4 Processes

8.4.4.1 Performing security activities in the course of an application project

Figure 12 shows how the project team and the operation team use the ASC as a tool for performing security activities during a specific application project. Only ASCs from the project's ANF will be used in the project.

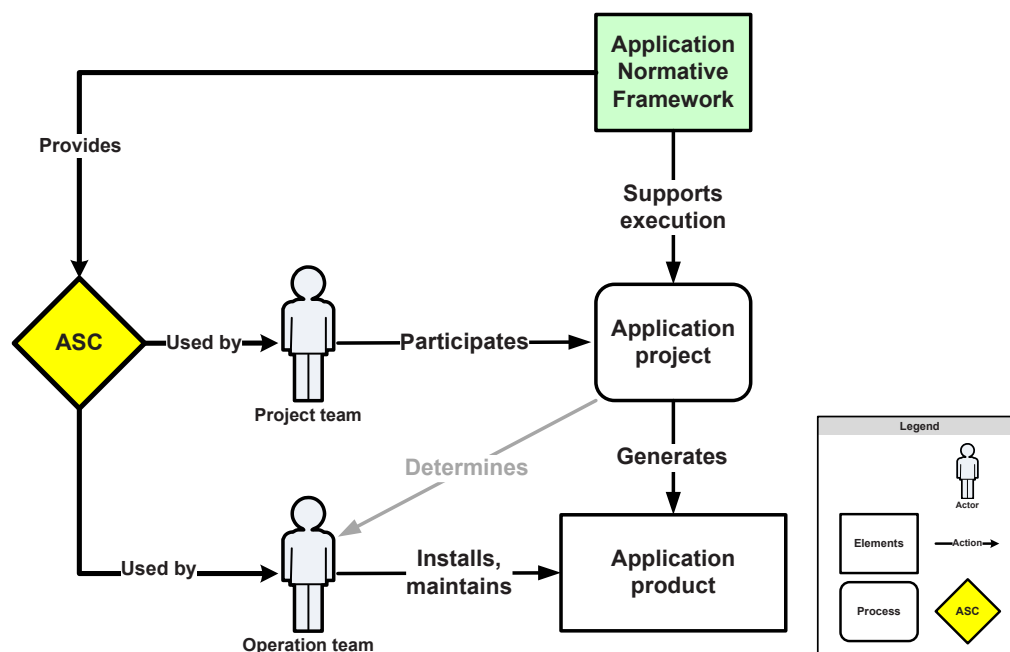


Figure 12 – ASC used as a security activity

8.4.4.2 Performing verification measurements in the course of an application project

The verification measurement part of the ASC implements the principle that all security activities should be verified to provide evidence that the activity was performed correctly, by a qualified actor, and that the expected results were met.

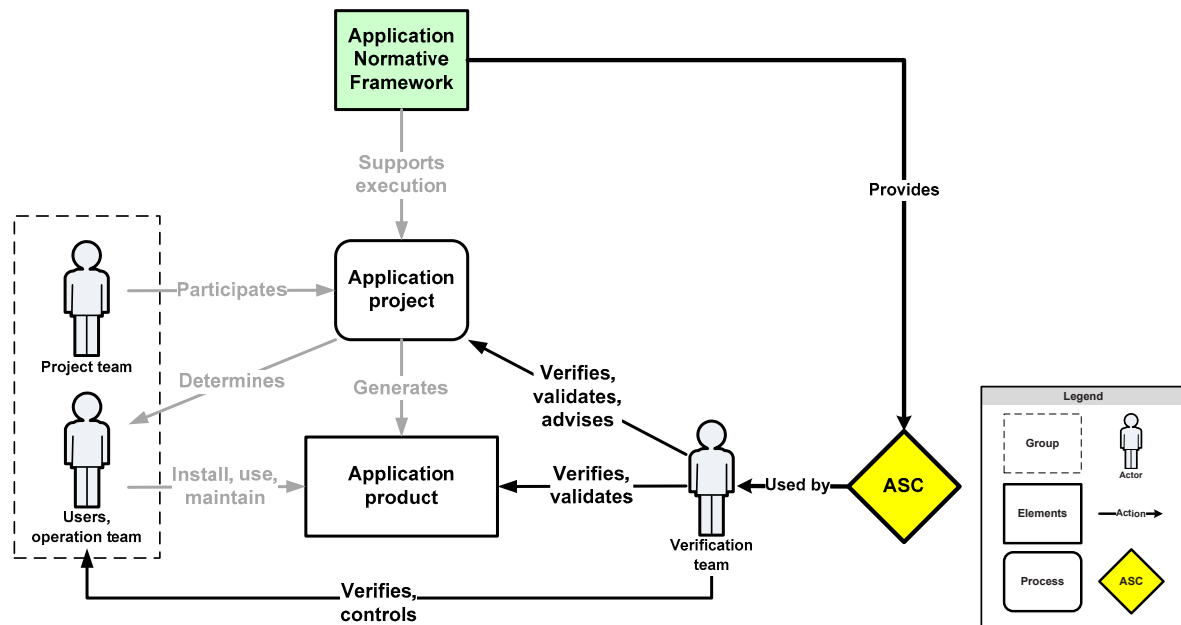


Figure 13 – ASC used as a measurement

Figure 13 shows that the verification measurement part of an Application Security Control 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 whether or not to authorize the application project to proceed to its next step of execution. For example, an ASC might 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 correctly.

Figure 13 also shows that the verification measurement part of an ASC can be used to verify the qualifications of the actors performing the application life cycle activities. For example, an ASC may require that a senior developer implement an application critical component. The verification measurement part of the ASC verifies the qualifications of the developer who implemented the component.

8.5 Application Security Audit

8.5.1 General

The purpose of this 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.

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.

EXAMPLE 1 An organization could periodically perform this step to monitor the status of security implementation during the realization stage of an application.

EXAMPLE 2 An organization could perform this step to demonstrate an application's Actual Level of Trust before it can be approved for deployment.

EXAMPLE 3 An organization could perform this step during the operation stages of an application's life cycle as part of the organization's annual security audit.

In this step, an internal or external verification team (depending on organizational policies contained in the ONF) verifies 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. The purpose of this step is to demonstrate the application's Actual Level of Trust at a specific time. An organization can declare an application "secure" when its Actual Level of Trust is equal to its Targeted Level of Trust.

This step corresponds to the "risk acceptance" step in the risk management process established by ISO/IEC 27005.

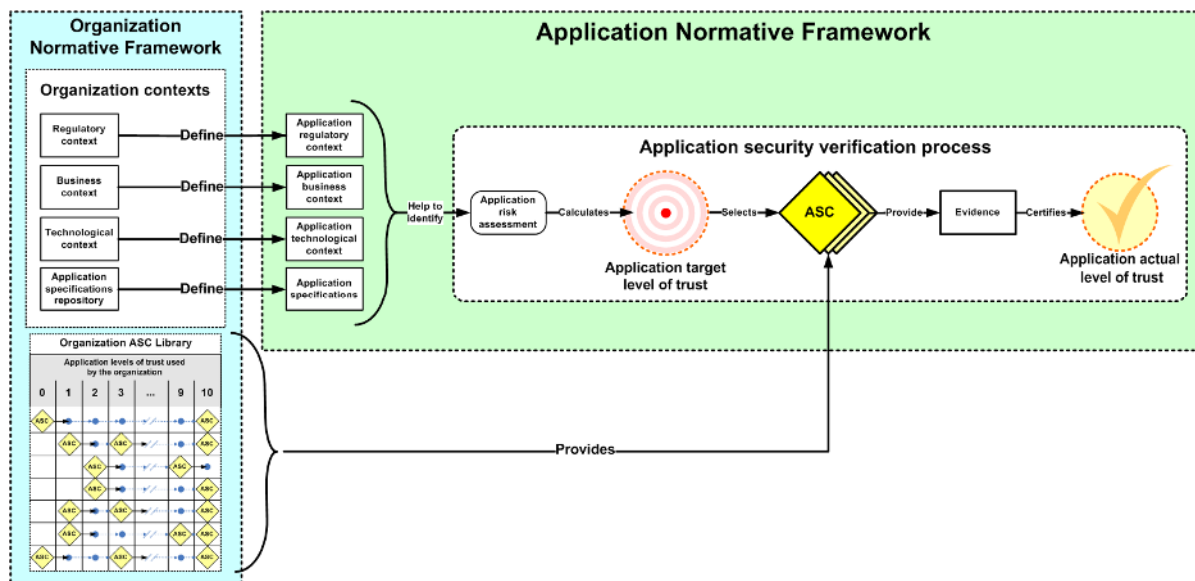


Figure 14 – Overview of the application security verification process

8.5.2 Components

8.5.2.1 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 during which the measurement is to be performed.

The application's Actual Level of Trust is obtained by verifying the ASCs that ought to be 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's Targeted Level of Trust is confirmed when verification of supporting evidence from the verification measurement activities of all expected ASCs has been successfully performed.

Following this confirmation, the application is considered secure by the organization for use or deployment from the specific moment of the achievement until the moment of the next verification mandated by the periodical revision requirement of step 5 of the ASMP or by other organizational requirements.

Annex A (informative)

Mapping an existing development process to ISO/IEC 27034 Case Study

A.1 General

The purpose of this annex is to illustrate with an example how an actual security-focused software development process (the SDL) can successfully map to several components and processes of ISO/IEC 27034.

Unless specifically noted, this case study assumes that all activities and performance outcomes discussed conform to ISO/IEC 27034.

This Annex will illustrate the following concepts in support of ISO/IEC 27034;

- a) A short overview of the Security Development Lifecycle
- b) A mapping of security development practices to the Organization Normative Framework. In particular, this Annex:
 - 1) explains the interconnections between the technological, business and regulatory contexts;
 - 2) discusses the processes for creating and maintaining application specifications;
 - 3) outlines the roles and responsibilities for various individuals involved in the application development process;
 - 4) shows the Application Security Controls (ASCs) in place;
 - 5) discusses the Application Security Verification process;
 - 6) provides a visual illustration of the Application Security Life Cycle Reference Model;
 - 7) provides examples of additional activities an organization using SDL might have to perform in order to comply with ISO/IEC 27034.

For ease of review, verbatim descriptions of the controls outlined in this part of ISO/IEC 27034 are referenced in text boxes for each section below; each of them is then followed by an example of its application.

Wherever possible, references to public sources of information are provided; web links to specific discussions of processes, tools and other ancillary information can be found throughout this document.

It is important to note that the author of this Annex has chosen to focus *solely on the security software development methodology used for shipping commercial software applications and online services*. There are other processes that cover IT security tasks; the groups that administer these processes are bound by similar technology and regulatory contexts, but do not create application software intended for broad public use. While an illustration of both the IT and security software development methodologies might prove interesting to some readers, it would not necessarily provide more compelling evidence of the practicality of ISO/IEC 27034.

Usage of the Security Development Lifecycle (SDL) in this illustrative context does not constitute endorsement of the SDL by the International Organization for Standardization (ISO).

A.2 About the Security Development Lifecycle

The Security Development Lifecycle (SDL) is a software security assurance process. As a company-wide initiative and a mandatory policy since 2004, the SDL has played a critical role in embedding security and privacy in software and culture of the adopting company. Combining a holistic and practical approach, the SDL introduces security and privacy throughout all phases of the development process. References to proprietary technologies and resources have been omitted from this Annex.

The SDL is composed of 7 stages as shown in Figure A.1 below.

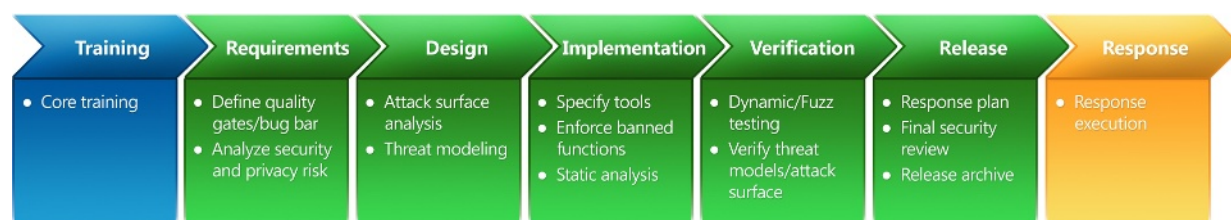


Figure A.1 – Security Development Lifecycle

A.3 SDL mapped to the Organization Normative Framework

A simple illustration of the application of the SDL to the Organization Normative Framework is included below. The following discussion of the SDL will adhere to this format.

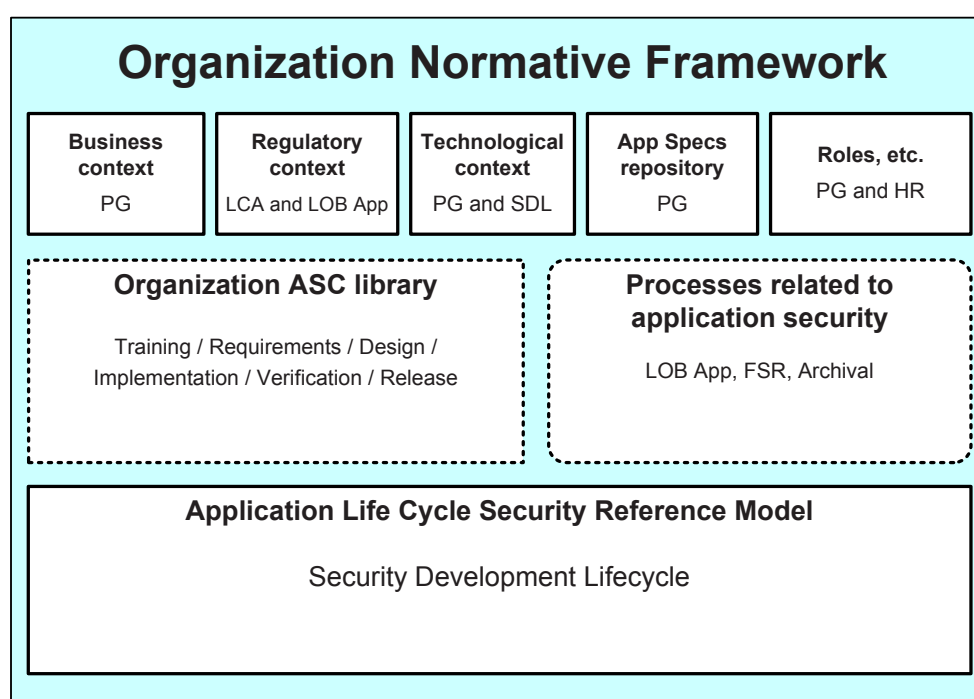


Figure A.2 – SDL mapped to the Organization Normative Framework

Key to acronyms:

PG:	Product Group
LCA:	Legal and Corporate Affairs
LOB App:	Proprietary line of applications used in support of business and technological contexts
SDL:	Security Development Lifecycle
HR:	Human Resources
FSR:	Final Security Review

A.4 Business Context

8.1.2.1 The business context lists and documents all standards and best practices adopted by the organization that could impact application projects.

The business context includes:

- a) project management, development, risk analysis, operational, audit and control processes;
- b) the organization's security policy;
- c) practices for the business domain;
- d) the development methodology used by the organization;
- e) best practices for all programming languages employed by the organization and listed in the technological context;
- f) the organization's formal project management process; and
- g) the adoption of other relevant ISO/IEC International Standards, such as ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 15288.

Business context is set by a combination of corporate-wide policies, region-specific policies, technical context and market drivers of the individual business units within the corporation.

Security and privacy in software product development is mandated *company-wide* per the Security Development Lifecycle (SDL)ⁱ The SDL also requires determination of people (security and privacy leads), processes and controls to be used to track progress against security and privacy goals.ⁱⁱ

Given the broad spectrum of deployment scenarios and development platforms, mandatory adherence to a fixed set of development methodologies or tools is not feasible. Therefore, business groups are permitted to address technical challenges that are not directly covered by SDL policy (e.g. compiler and tool mandates on different platforms) in consultation with security subject matter experts (outlined in greater detail in the Roles, Responsibilities and Qualifications section below).

A.5 Regulatory Context

8.1.2.2 The regulatory context lists and documents any law or regulation, in any of the organization's business locations, that could impact application projects. It includes laws, rules and regulations of the countries or jurisdictions where the application is developed and/or deployed and/or used.

An organization deploying and/or using the same application in more than one country might have to meet different security requirements for each country.

Regulatory compliance and geopolitical analysis are covered by existing business processes and are proactively used to inform the design and development efforts of project teams. Policies are analyzed by the business units and Legal and Corporate Affairs to insure that all aspects of software creation and release meet any *known* legal or regulatory criteria in place in different regions of the world and that any new projects operate within the bounds of existing policy mandates.

Line of applications (in combination with the reviews mentioned above) are used by the product teams to automate the process of ensuring regulatory compliance for software applications developed for public release.

Finally, the output of regulatory and geopolitical reviews are archived with the outputs created by the Application Security Verification Process (discussed below) to create an objective and comprehensive representation of the application security development process. However, it is important to note that *regulatory and geopolitical policies are not addressed by the Security Development Lifecycle*.

A.6 Application Specifications Repository

8.1.2.3 The application specifications repository lists and documents the organization's general IT functional requirements and corresponding pre-approved solutions. Application specifications should include:

- a) specifications about how applications should compute, store and transfer information;
- b) usual application parameters, functionalities, services and requirements; and
- c) source code, binary code, libraries and products or services used or relied upon by applications;

Additional specifications might include those detailing how the application interacts with:

- a) other systems;
- b) the runtime infrastructure upon which it depends; and
- c) the list of controls within the runtime environment.

Specifications are authored and stored by individual business units and generally consist of both functional guidance (outlining how a particular component should compute, store and transfer information) and technical guidance (specifying programming languages, compilers, libraries, etc.). In certain cases, the SDL sets policy for components or other technologies that have a security context (e.g. libraries for cryptographic services) to ensure that application security and privacy are not compromised by functionality requirements or convenience.

A.7 Technological Context

8.1.2.4 The technological context comprises the inventory of all IT products, services and technologies available to the organization for application projects. These products, services and technologies determine the threats to which applications are exposed.

The technological context includes computers, tools, IT products and services, communication infrastructure and other technical devices.

EXAMPLE Technological contexts that might have an impact on application security include client-server infrastructure, web infrastructure, network infrastructure and development environment and tools.

Technological context is often different across business units, and is derived from a combination of market drivers, interoperability and compatibility scenarios and technical standards for a particular group. Given the variation in standards for IT products, services and technologies across business units, the technological context is set independently by each business unit to allow them to meet their needs. However, business units should also ensure that software projects are using IT services and technologies that allow them to meet the security and privacy criteria set by both business and regulatory contexts.

A.8 Roles, Responsibilities and Qualifications

8.1.2.5 The ONF should contain:

- a) lists and descriptions of all roles, responsibilities and required professional qualifications for actors involved in creating and maintaining the ONF and/or roles for creating and maintaining ASCs; and
- b) lists and descriptions all roles, responsibilities and required professional qualifications for actors involved in the organization's application life cycle, such as information security managers, project managers, administrators, software acquirers, software development managers, application owners, user managers, architects, analysts, programmers, testers, system administrators, database administrators, network administrators and technical personnel.

This is an organization-wide policy that will help ensure that all critical roles for all processes are filled, that all responsibilities are defined, that conflicts of interest are avoided, and that people filling the roles have sufficient professional qualifications.

Personnel job categories are created and maintained by Human Resources, with input from the business units. These categories include high level descriptions of the tasks and competencies unique to each job role. While Human Resources maintains common job descriptions, it is generally up to the business units to decide how to specifically specify job categories with respect to security and privacy competence and to use those criteria to help with delegation of security oversight responsibility within a development team.

The SDL has general criteria and job descriptions for security and privacy roles; these roles are assigned during the Requirements Phase of the SDL process.ⁱⁱⁱ These specific job roles should be defined prior to the start of the development stage. These roles are consultative in nature, and provide the framework necessary to identify, catalog and mitigate security and privacy issues present in a software development project. These roles include:

Supervisory Roles: These roles are designed to provide project oversight and may include both qualitative and quantitative advice to project teams as to minimal acceptable security and privacy assurance thresholds for a software project. The supervisory roles should also be vested with the authority to accept or reject security and privacy plans from a project team.

- a) **Security Advisor:** This role is filled by an individual security subject matter expert from outside the project team. The role can either be filled by a qualified member of an independent, centralized security group within the organization or, by seeking the services of an expert external to the organization. The person chosen for this task should fill two sub-roles:
 - i. **Auditor:** This individual should monitor each phase of the security development process and attest to successful completion of each stage requirement. The security advisor should have the freedom to attest to compliance (or non-compliance) with security requirements without interference from the project team.
 - ii. **Expert:** The person chosen for the security advisor role should possess verifiable subject matter expertise in security.
- b) **Privacy Advisor:** This role is filled by an individual privacy subject matter expert from outside the project team. The role can either be filled by a qualified member of an independent, centralized privacy group within the organization or, by seeking the services of an expert external to the organization. The person chosen for this task should fill two sub-roles:
 - i. **Auditor:** This individual should monitor each phase of the privacy development process and attest to successful completion of each stage requirement. The privacy advisor should have the freedom to attest to compliance (or non-compliance) with privacy requirements without interference from the project team.
 - ii. **Expert:** The person chosen for the privacy advisor role should possess verifiable subject matter expertise in privacy.

Combination of Advisory Roles: The role of security advisor may be combined with the role of privacy advisor, assuming that an individual with the appropriate skills and experience can be identified.

Team Lead Roles: The team lead roles should be filled by subject matter experts who will represent the project development team during discussions with the security and privacy advisors. This role is responsible for the negotiation, acceptance and tracking of minimum security requirements and maintaining clear lines of communication with advisors and other decision makers during the duration of a software development project.

- a) **Security Team Lead(s):** This individual (or group of individuals) does not have sole responsibility for ensuring that a software release has addressed all security issues – however he or she is responsible for coordinating and tracking security issues for the project. This role also is responsible for status reporting to the security advisor and to other relevant parties (e.g. development and test leads) on the project team.
- b) **Privacy Team Lead(s):** This individual (or group of individuals) does not have sole responsibility for ensuring that a software release has addressed all privacy issues – however he or she is responsible for coordinating and tracking privacy issues for the project. This role also is responsible for status reporting to the privacy advisor and to other relevant parties (e.g. development and test leads) on the project team.

A.9 Organization ASC Library

8.1.2.6 The organization should define at least one library of controls for application security. This library is called an Application Security Control Library (ASC Library). It lists and documents all ASCs recognized by the organization. These ASCs evolved from standards, best practices and roles, responsibilities, and professional qualifications, technological, business, and regulatory contexts and application specifications.

Seventeen ASCs have been identified as part of the SDL process illustrated below; this example includes both mandatory and optional tasks. ASCs that are not mandatory may be added as necessary by business units to achieve desired security and privacy targets. The ASCs are outlined below; they are presented in the order that they occur - using the traditional waterfall development metaphor. In the interest of brevity, full discussions of each ASC are omitted.

The leftmost ASC below can be considered a “root” ASC – in essence the “parent node” of increasingly detailed ASC trees as shown in the figure. This hypothetical illustration shows that ASCs could be applied by an organization with increasing levels of complexity and detail in order to meet the Targeted Level of Trust for an application, which the organization chose prior to the start of the application project.

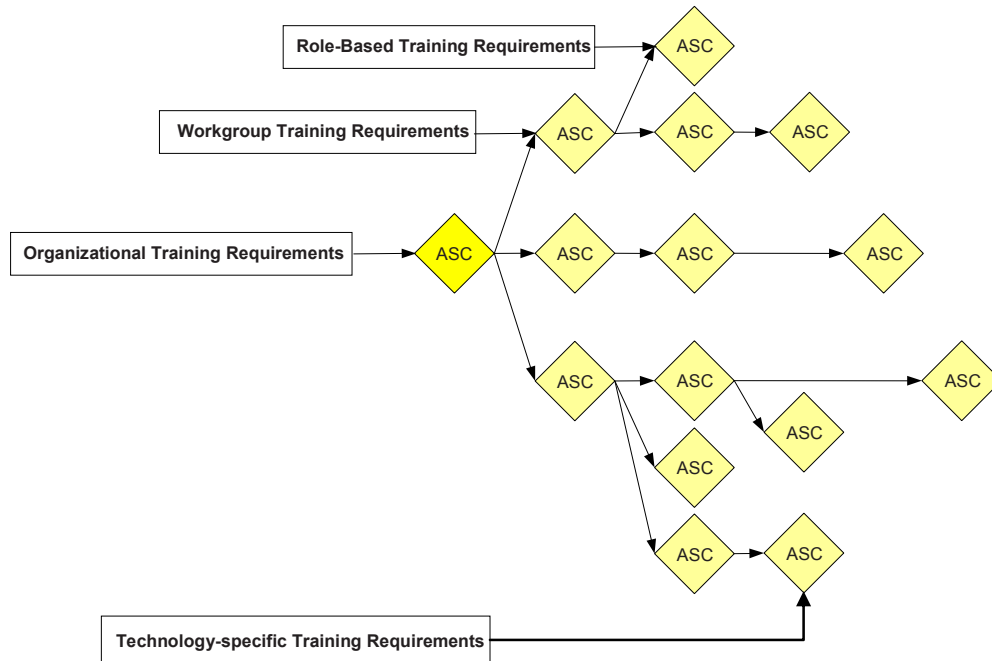


Figure A.3 – Example of an ASC tree

A.9.1 Training

1. **Training Requirements:** All members of software development teams should receive appropriate training to stay informed about security basics and recent trends in security and privacy. Individuals in technical job roles (developers, testers, and program managers) that are directly involved with development of software programs should attend at least one security training class each year. Basic software security training should cover foundational concepts such as secure design, threat modeling, attack surface measurement, secure coding, security testing and privacy.^{iv}

A.9.2 Requirements

2. **Security Requirements:** The need to consider security and privacy at a foundational level is a fundamental aspect of system development. The optimal point to stipulate trustworthiness requirements for a software project is during the initial planning stages of a new release. This allows development teams to identify key milestones and deliverables and permits the integration of security and privacy in such a way that it minimizes any disruption to plans and schedules. Security and privacy requirements analysis is performed at project inception and consists of various mandatory actions, including (at a minimum): determination of SDL applicability; determination of individuals responsible for security and privacy oversight (see 8.1.2.5 – Roles, responsibilities and qualifications above); specification of minimum security requirements; and specification and deployment of a vulnerability/work item tracking system.^v
3. **Quality Gates/Bug Bars:** Quality gates and “bug bars” are used to establish minimum acceptable levels of security and privacy quality.^{vi vii} Defining these criteria at the start of a project improves understanding of risks associated with security issues and enables teams to identify and fix security bugs during development. A project team should negotiate quality gates for each development phase and have them approved by the security advisor with project-specific clarifications and more stringent security requirements specified by the security advisor (as appropriate). The project team should also illustrate compliance with the negotiated quality gates in order to comply with verification requirements in the Final Security Review. A “bug bar” is a quality gate that applies to the entire software development project. It is used to define severity boundaries for security bugs (e.g. no *known* bugs in the application with a “critical” rating at time of release). The “bug bar” should never be relaxed, even as a project’s release date nears.

NOTE The concept of quality gates/bug bars, applied to security, is close to the concept of Targeted Level of Trust, as it is used to establish minimum acceptable levels of security and privacy.

4. **Security and Privacy Risk Assessment:** Security and privacy risk assessments (SRAs) are mandatory processes to identify functional aspects of the software that might require deep review. Given that program features and intended functionality might be different from project to project, it is wise to start with simple risk assessments and expand as necessary to meet the project scope. Such assessments should include the following information:
- a) (Security) Which portions of the project will require threat models (see ASC #7 below) before release?
 - b) (Security) Which portions of the project will require security design reviews before release?
 - c) (Security) Which portions of the project (if any) will require penetration testing (pen testing) by a mutually agreed upon group that is external to the project team? Any portion of the project that requires penetration testing should resolve issues identified during penetration testing before it is approved for release.
 - d) (Security) Any additional testing or analysis requirements the security advisor deems necessary to mitigate security risks.
 - e) (Security) Clarification of the specific scope of fuzz testing requirements (see ASC #12 below).
 - f) (Privacy) Determination of Privacy Impact Rating:^{viii ix}
 - i. P1 – High Privacy Risk: The feature, product, or service stores or transfers Personally Identifiable Information (PII) changes settings or file type associations; or installs software.
 - ii. P2 – Moderate Privacy Risk: The sole behavior that affects privacy in the feature, product, or service, is a one-time user-initiated anonymous data transfer (e.g., the user clicks on a link and goes out to a website).
 - iii. P3 – Low Privacy Risk: No behaviors exist within the feature, product, or service that affect privacy. No anonymous or personal data is transferred, no PII is stored on the machine, no settings are changed on the user's behalf, and no software is installed.

A.9.3 Design

5. **Design Requirements:** The optimal time to influence a project's trustworthy design is early in its lifecycle. It is critically important to consider security and privacy concerns carefully during the design phase – mitigation of security and privacy issues is much less expensive when performed during the opening stages of a project lifecycle. Project teams should refrain from the practice of “bolted on” security and privacy near the end of a project's development.

In addition, it is crucially important for project teams to understand the distinction between “secure features” and “security features” – it is quite possible to implement security features, which are in fact, insecure. Secure features are defined as features whose functionality is well engineered with respect to security, including rigorous validation of all data before processing, or cryptographically robust implementation of libraries for cryptographic services. Security features describe program functionality with security implications (e.g. Kerberos authentication).

Functional design specifications might need to describe security features or privacy features that will be directly exposed to users, such as requiring user authentication to access specific data or user consent before use of a high-risk privacy feature. As a result, all design specifications should:

- a) Accurately and completely describe how to implement these features
- b) Describe how to securely implement all functionality enabled by a given feature
- c) Describe how to deploy the feature in a secure fashion.

The design requirements exercise contains a number of required actions, which include, but are not limited to: security design review, privacy design review and specification, and implementation of minimal cryptographic design requirements.^x

6. **Attack Surface Reduction:** Attack surface reduction is closely aligned with threat modeling, although it addresses security issues from a slightly different perspective. Attack surface reduction is a means of reducing risk by giving attackers less opportunity to find a weak spot or vulnerability. Attack surface

reduction embodies employing layered defenses, shutting off or restricting access to system services and applying the principle of least privilege wherever possible.

7. **Threat Modeling:** Threat modeling is a mandatory process performed during the design phase that allows development teams to consider, document and discuss the security implications of designs in a structured fashion. It also allows for the deliberate consideration of security issues at the component or application level. Threat modeling is a team exercise encompassing program/project managers, developers and testers and represents the primary security analysis task performed during the software design stage.^{xi}

A.9.4 Implementation

8. **Use Approved Tools:** All development teams should define and publish a list of approved tools (and specific security functionality such as compiler/linker options, warnings, etc.) to be used on software projects.^{xii xiii} This list should be reconciled and approved by the security advisor for the project team. Generally speaking, development teams should strive to use the latest version of approved tools to take advantage of new security functionality.
9. **Deprecate Unsafe Functions:** Many commonly used functions and APIs are not secure in the face of the current threat environment. Project teams should analyze all functions and APIs that will be used in conjunction with a software development project and prohibit those that are determined to be unsafe.^{xiv} Once the banned list is determined, project teams should use header files, newer compilers or code scanning tools to check code (including legacy code where appropriate) for the existence of banned functions and replace them with safer alternatives.
10. **Static Analysis:** Project teams should perform static code analysis of source code. Static analysis of source code provides a scalable solution for security code review and can be used to ensure that secure coding policies set by the security team lead and security advisor are being followed. Static code analysis by itself is generally insufficient to perform a thorough security review – the security team and security advisors should be aware of the strengths and weaknesses of static analysis tools and be prepared to embellish code review tasks with other tools or human review as appropriate. Lightweight static analysis occurs in the SDL at code check-in time by use of the */analyze* function in Visual Studio.^{xv} Other static analysis tasks are performed as necessary.

A.9.5 Verification

11. **Dynamic Program Analysis:** Run-time verification of software programs is necessary to ensure that a software program's functionality works as designed. This verification task should specify tools that monitor application behavior for memory corruption, user privilege issues and other critical security issues. The SDL process uses run-time tools such as AppVerifier with other techniques such as fuzz testing to achieve desired levels of security test coverage.^{xvi}
12. **Fuzz Testing:** Fuzz testing is used to induce program failure by deliberately introducing malformed or random data to the inputs of an application. The SDL specifies that fuzz testing be performed on a variety of program interfaces. The fuzz tests performed are derived from the intended use of the application and the functional and technical specifications for the application. The security advisor may require additional fuzz tests or increases in the scope and duration of the testing based on the intended behaviour of the application.^{xvii}
13. **Threat Model / Attack Surface Review:** It is common for an application to deviate significantly from the functional and technical specifications created during the requirements and design phases of a software development project. Therefore it is critical to re-review threat models and attack surface measurement of a given application when it is "code complete." This review will ensure that any changes to the system have been accounted for and that any new attack vectors have been reviewed and mitigated.
14. **Manual Code Review (Optional):** Manual code review is an optional task in the SDL. Manual code review is usually performed by the application security team at the recommendation of the security advisor. While analysis tools can do much of the work of finding and flagging vulnerabilities, they are not perfect; as a result, manual code review is usually focused on the "critical" components of an application. Most often it is used where sensitive data such as personally identifiable information (PII) is involved. It is also used to examine other critical components such as crypto implementations.

A.9.6 Release

15. **Incident Response Plan:** Every software release subject to the requirements of the SDL should include an incident response plan.^{xviii} Even programs with no known vulnerabilities at the time of release can be subject to new threats that emerge over time. The incident response plan should include the following at a minimum;
- a) An identified sustaining engineering (SE) team, or if the team is too small to have SE resources, an Emergency Response Plan that identifies three to five engineering staff, three to five marketing and customer communications staff and at least two management staff to act as points of first contact in a security emergency.
 - b) 24 X 7 X 365 on call contacts with decision-making authority.
 - c) Security servicing plans for code inherited from other groups within the organization.
 - d) Security servicing plans for licensed third party code – this includes filenames, versions, source code, 3rd party contact information and contractual permission to make changes (if appropriate).
16. **Final Security Review:** The Final Security Review (FSR) is a deliberate examination of all the security activities performed on a software application prior to release. The FSR is performed by the security advisor with assistance from the regular development staff and the security and privacy team leads. The FSR is not a “penetrate and patch” exercise, nor is it a chance to perform security activities that were previously ignored or forgotten. The FSR usually includes an examination of threat models, exception requests, tool output and performance against the previously determined quality gates or bug bars.^{xix} The FSR will result in one of three different outcomes:
- a) **Passed FSR** – all security and privacy issues identified by the FSR process are fixed or mitigated.
 - b) **Passed FSR with exceptions** – all security and privacy issues identified by the FSR process are fixed; those that cannot be addressed (e.g. vulnerabilities posed by design level issues) are logged and corrected in the next release.
 - c) **FSR with escalation** – If a team does not meet all SDL requirements and the security advisor and the product team cannot reach an acceptable (or tolerable) compromise, the security advisor cannot approve the project, and the project cannot be released. Teams should either address whatever SDL requirements that they can prior to launch, or escalate to executive management for a decision.
- NOTE The result of the FSR is close to the concept of Actual Level of Trust, as the FSR is a deliberate examination of all the security activities performed on a software application prior to release.
17. **Release / Archive:** Software release to manufacturing (RTM) or to the Web (RTW) is conditional on completion of the SDL process. The security advisor assigned to the release should certify that the project team has satisfied security requirements. Similarly, for all products that have at least one component with a privacy impact rating of P1, the project's privacy advisor should certify that the project team has satisfied the privacy requirements before the software can be shipped.

In addition, all pertinent information and data should be archived to allow for post-release servicing of the software; this includes all specifications, source code, binaries, symbols, threat models, emergency response plans and any other data necessary to perform post-release servicing tasks.

A.10 Application Security Audit

8.5.1 The purpose of this 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.

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.

EXAMPLE 1 An organization could periodically perform this step to monitor the status of security implementation during the realization stage of an application.

EXAMPLE 2 An organization could perform this step to demonstrate an application's Actual Level of Trust before it can be approved for deployment.

EXAMPLE 3 An organization could perform this step during the operation stages of an application's life cycle as part of the organization's annual security audit.

In this step, an internal or external verification team (depending on organizational policies contained in the ONF) verifies 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. The purpose of this step is to demonstrate the application's Actual Level of Trust at a specific time. An organization can declare an application "secure" when its Actual Level of Trust is equal to its Targeted Level of Trust.

The process of auditing application security to measure the Actual Level of Trust involves a number of different actors and processes in the SDL:

- A specially designed line of business application is used to track compliance with the SDL – tool log uploads, threat models and other automated and manual attestations are centrally stored.
- The security and privacy team leads are responsible for ensuring that the data necessary for an objective judgment is categorized and entered into the tracking application.
- This information entered into the tracking application is then used by the security and privacy advisors to provide the framework for the Final Security Review (outlined above).
- The security and privacy advisors are then responsible for reviewing the data entered into the tracking application (including the FSR results and other additional security tasks assigned by the advisor(s)) and certifying that all requirements are met and/or all exceptions are resolved.

A screen capture of the line of application used to track and verify security tasks is shown in Figure A.4.

Demo for Scoping Questions - Windows Internet Explorer

https://My/DynamicModule.aspx?ModuleId=155&ProjectId=...

Questionnaire

I need to...

Home | Dashboard | Project Home | Phase 4: Verification | Tool Compliance

Click to Rate and Give Feedback

General
Create Project
Scratch Pad
Training Reports
Search
About

My
Dashboard
Settings
Contact Info
Training History

Project Menu
Project Home
Permissions
Applicability
Exception Status
Fill Out a Survey
Advisor Only

Security Advisor
Dashboard
Exceptions
Search
Queue
Reviews
Reports

Tool Compliance: Demo for Scoping Questions

Phase 0 Pre-Phase Phase 1 Scope Phase 2 Design Phase 3 Test Phase 4 Verify Phase 5 Release

Upload the results of the SDL tools this product is required to run on this page.

File Fuzzing [Give feedback on this tool](#)

Upload file fuzzing reports for each file extension that requires fuzzing (i.e. - docx, btd, xml, etc.) [?]

☐ Check here if none exist.

NO FILE TYPES HAVE BEEN ADDED

Have you fuzz tested each file type which requires fuzz testing and corrected issues as described in the [SDL Bug Bar](#)? [?]

☐ Yes ☐ Request Exception

RPC Fuzzing [Give feedback on this tool](#)

Upload the report for each RPC interface that 24 hour dumb fuzzing with RPCTest in RPCAttack mode was performed on [?]

NO UPLOADED RPC DUMB FUZZING FILES

Upload the report for each RPC interface that 24 hour smart fuzzing with RPCVerifier was performed on [?]

NO UPLOADED RPC FUZZING FILES

ActiveX Fuzzing [Give feedback on this tool](#)

Upload the report for each ActiveX control you fuzzed [?]

NO UPLOADED ACTIVEX FUZZING FILES

Have you fuzz-tested all ActiveX controls that are marked as either Safe for Scripting or Safe for Initialization with 100+ bad values? [?]

☐ Yes ☐ Request Exception

Have all issues identified by ActiveX fuzz testing been corrected as described in the [SDL Bug Bar](#)? [?]

☐ Yes ☐ Request Exception

App Verifier [Give feedback on this tool](#)

Has all unmanaged code in the project been tested while running AppVerifier as described in the [SDL AppVerifier Requirements](#)? [?]

☐ Yes ☐ Request Exception

Recommendations

The below questions are recommendations relevant to this stage of the SDL for your project. These are not SDL requirements and do not affect completion percentage, but certain work items are recommended to improve the security of your product.

Have you used a fuzzing tool on your webservices? [?]

☐ Yes ☐ No

Have you created and completed security testing plans? [?]

☐ Yes ☐ No

Has your product been penetration tested? [?]

☐ Yes ☐ No

Have you developed regression tests for previously known security vulnerabilities? [?]

☐ Yes ☐ No

For online services, have you conducted data flow testing? [?]

☐ Yes ☐ No

For online services, have you conducted replay testing? [?]

☐ Yes ☐ No

Have you followed the [SDL Network Protocol Fuzzing Recommendations](#)? [?]

☐ Yes ☐ No

[Previous](#) | [Next](#)

javascript:window.showModalDialog('http://My/... Local intranet | Protected Mode: Off 95%

Figure A.4 – Example of a Line of Business Application for Application Security Audit

A.11 Application Life Cycle Model

8.1.2.7.1 An organization whose business involves developing, outsourcing or acquiring applications habitually uses a framework of defined processes and activities organized into stages. This framework is commonly named “life cycle model”. Depending on the context, it is referred to as either “application life cycle model”, “system life cycle model” or “software life cycle model”.

Such a model is usually unique and customized for a particular organization. It has often been in use for quite some time and has been refined over the years. It is not a new concept brought by this International Standard.

A specific application’s life cycle, i.e. the evolution of the application from conception through retirement, is usually an instantiation of the organization’s life cycle model.

Sometimes, different groups within a complex organization use different application life cycle models for different application projects. This is often the case in large organizations which are formed through mergers or which are decentralized. Other organizations have developed different specialized application life cycle models related to specific application contexts such as web applications, real-time applications, embedded applications, medical applications, etc.

In this case study, the application life cycle model used for mapping security activities is the SDL. The previous sections of this document outline the technical, business and regulatory contexts and the roles that serve in each of those areas.

A simple illustration of the SDL process can be found in Figure A.5. This diagram is a visualization of the Application Security Controls used on a hypothetical project; from the training of employees to application release. This is not an exhaustive diagram – as noted previously, many teams add other security and privacy tasks that are specific to their projects.

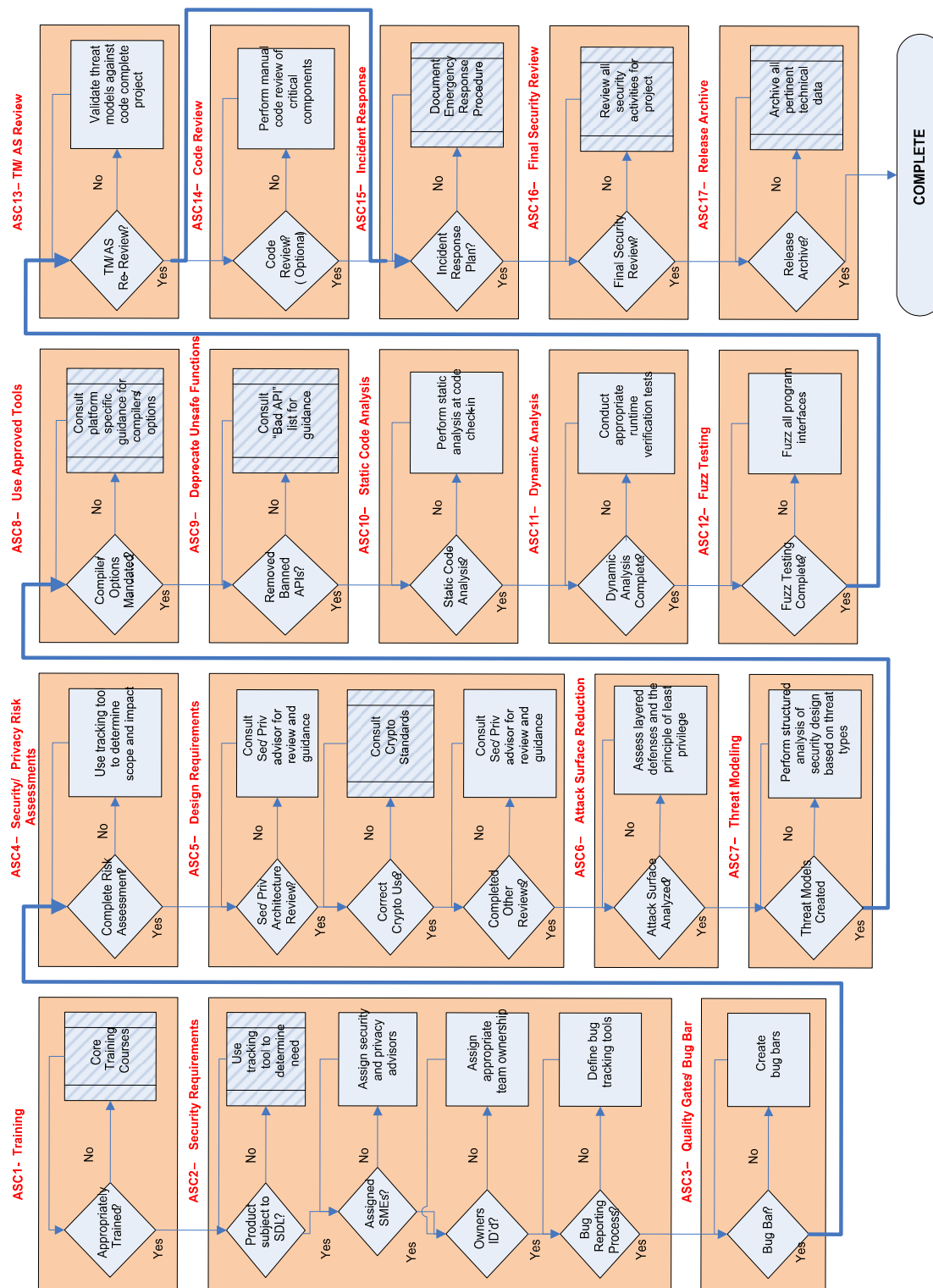


Figure A.5 – SDL Process Illustration

A.12 SDL mapped to the Application Security Life Cycle Reference Model

In the interest of reader clarity, the SDL process can be mapped to the Application Security Life Cycle Reference Model diagram included in ISO/IEC 27034. Reference Model stages covered by the SDL process are printed in bold in Figure A.6.

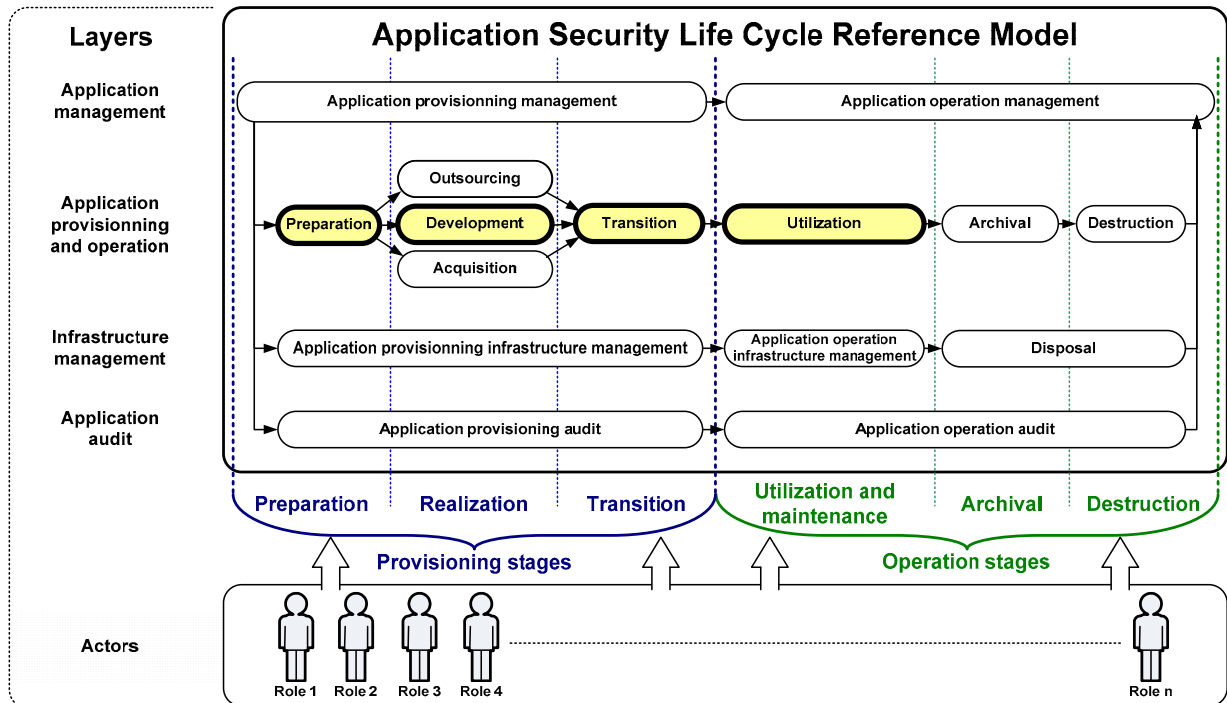


Figure A.6 – SDL mapped to the Application Security Life Cycle Reference Model

In addition, Figure A.7 shows a more detailed mapping of SDL phases with stages in the Application Security Life Cycle Reference Model.

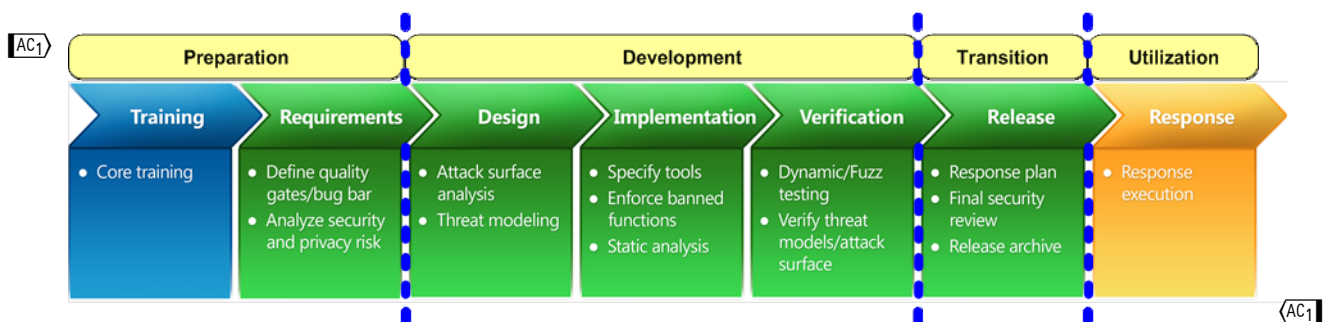


Figure A.7 – Detailed mapping of SDL phases with stages in the Application Security Life Cycle Reference Model

Endnotes for Annex A

Business Context

- i <http://msdn.microsoft.com/en-us/library/cc307748.aspx>
- ii <http://msdn.microsoft.com/en-us/library/cc307412.aspx>

Roles, Responsibilities and Qualifications

- iii <http://msdn.microsoft.com/en-us/library/cc307412.aspx>

Organization ASC Library

Training

- iv <http://msdn.microsoft.com/en-us/library/cc307407.aspx>

Requirements

- v <http://msdn.microsoft.com/en-us/library/cc307412.aspx>
- vi <http://msdn.microsoft.com/en-us/library/cc307404.aspx> (Security)
- vii <http://msdn.microsoft.com/en-us/library/cc307403.aspx> (Privacy)
- viii <http://msdn.microsoft.com/en-us/library/cc307393.aspx>
- ix <http://www.microsoft.com/downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&displaylang=en>

Design

- x <http://msdn.microsoft.com/en-us/library/cc307414.aspx>
- xi <http://msdn.microsoft.com/en-us/library/cc307415.aspx>

Implementation

- xii <http://msdn.microsoft.com/en-us/library/cc307417.aspx>
- xiii <http://msdn.microsoft.com/en-us/library/cc307395.aspx>
- xiv <http://msdn.microsoft.com/en-us/library/bb288454.aspx>
- xv <http://msdn.microsoft.com/en-us/library/cc307395.aspx>
- xvi <http://msdn.microsoft.com/en-us/library/cc307418.aspx>
- xvii <http://msdn.microsoft.com/en-us/library/cc307418.aspx>
- xviii <http://msdn.microsoft.com/en-us/library/cc307408.aspx>
- xix <http://msdn.microsoft.com/en-us/library/cc307409.aspx>

Annex B (informative)

Mapping ASC with an existing standard

Case Study: mapping security controls as described in NIST SP 800-53 Rev. 3 with ASCs as described in ISO/IEC 27034

The purpose of this annex is to illustrate how security controls from an existing source such as NIST SP 800-53 Rev. 3 can be integrated as ASCs for use in accordance with ISO/IEC 27034.

B.1 ASC candidate categories

This subclause tries to address the possible aspects of the ASC candidate categories as directly cited from SP 800-53 Rev. 3.

The organization can define ASC categories related to application security, such as:

B.1.1 Common security control-related considerations

Security controls designated by the organization as common controls are, in most cases, managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls can greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular baseline. Every control in a baseline should be fully addressed either by the organization or the information system owner.

B.1.2 Operational/environmental-related considerations

Security controls that are dependent on the nature of the operating environment are applicable only if the information system is employed in an environment necessitating the controls. For example, certain physical security controls might not be applicable to space-based information systems, and temperature and humidity controls might not be applicable to remote sensors that exist outside of the indoor facilities that contain information systems.

B.1.3 Physical Infrastructure-related considerations

Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, boundary protection devices, and communications equipment).

B.1.4 Public access-related considerations

Security controls associated with public access information systems should be carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) might not be applicable to users accessing information systems through public interfaces. For example, while the baseline controls require identification and authentication of organizational personnel that maintain and support information systems providing the public access services, the same controls might not be required for access to those information systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication would be required for users

accessing information systems through public interfaces in some instances, for example, to access/change their personal information.

B.1.5 Technology-related considerations

Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.

Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.³⁹ For example, when information system components are single-user, not networked, or only locally networked, one or more of these characteristics might provide appropriate rationale for not applying selected controls to that component.

Security controls that can be either explicitly or implicitly supported by automated mechanisms, do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. In situations where automated mechanisms are not readily available, cost-effective, or technically feasible, compensating security controls, implemented through nonautomated mechanisms or procedures, should be used to satisfy specified security controls or control enhancements (see terms and conditions for applying compensating controls below).

B.1.6 Policy/regulatory-related considerations

Security controls that address matters governed by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

B.1.7 Scalability-related considerations

Security controls are scalable with regard to the extent and rigor of the control implementation. Scalability is guided by the FIPS 199 security categorization of the information system being protected. For example, a contingency plan for a FIPS 199 high-impact information system can be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for a FIPS 199 low-impact information system can be considerably shorter and contain much less implementation detail. Organizations should use discretion in applying the security controls to information systems, giving consideration to the scalability factors in particular environments. This approach facilitates a cost-effective, risk-based approach to security control implementation that expends no more resources than necessary, yet achieves sufficient risk mitigation and adequate security.

B.1.8 Security objective-related considerations

Security controls that uniquely support the confidentiality, integrity, or availability security objectives can be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark;⁴⁰ (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.⁴¹ The following security controls are recommended candidates for downgrading: (i) confidentiality [AC-15, MA-3 (3), MP-2 (1), MP-3, MP-4, MP-5 (1) (2) (3), MP-6, PE-5, SC-4, SC-9]; (ii) integrity [SC-8]; and (iii) availability [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6].⁴²

B.2 Classes of security controls

This subclause tries to address the possible aspects of the ASC candidate classifications as directly cited from SP 800-53 Rev. 3.

Table B.1 – Security control classes, families, and identifiers

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

B.3 Sub-classes in the Access Control (AC) class

This section tries to address the candidate material which can be used to create Application Security Controls related to access control as directly cited from SP 800-53 Rev. 3.

Table B.2 – Security control classes and security control baselines for low-impact, moderate-impact, and high-impact information systems

CNTL NO.	CONTROL NAME			
	Access Control	LOW	MOD	HIGH
AC-1	Access Control Policy and Procedures	AC-1	AC-1	
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Control for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)

B.4 Detailed access control classes

This section shows three families of Access Control classes, AC-1, AC-2, AC-17, and AT-1 as directly cited from SP800-53.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

B.4.1 AC-1 Access control policy and procedures

Control: The organization develops, disseminates, and periodically reviews/updates:

- (1) A formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- (2) Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Priority and Baseline Allocation:

Control Enhancements: None. LOW AC-1	MOD AC-1	HIGH AC-1
--------------------------------------	----------	-----------

B.4.2 AC-2 Account management

Control: The organization manages information system accounts, including:

- (1) Identifying account types (i.e., individual, group, and system);
- (2) Establishing conditions for group membership;
- (3) Identifying authorized users of the information system and specifying access rights/privileges;
- (4) Requiring appropriate approvals for requests to establish accounts;
- (5) Authorizing, establishing, activating, modifying, disabling, and removing accounts;
- (6) Reviewing accounts [Assignment: organization-defined frequency];
- (7) Specifically authorizing and monitoring the use of guest/anonymous accounts;
- (8) Notifying account managers when information system users are terminated; transferred, or information system usage or need-to-know/need-to-share changes; and
- (9) Granting access to the information system based on: (i) a valid need-to-know or need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage.

Supplemental Guidance: The identification of authorized users of the information system and the specification of access rights/privileges is consistent with the requirements in other security controls in the security plan. Related controls: AC-1, AC-3, AC-4, AC-5, AC-6, AC-10, AC-13, AC-17, AC-19, AC-20, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SI-9, SC-13.

Control Enhancements:

- (1) The organization employs automated mechanisms to support the management of information system accounts.
- (2) The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].
- (3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period].
- (4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.
- (5) The organization reviews currently active information system accounts [Assignment: organization-defined frequency] to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy.
- (6) The organization prohibits the use of information system account identifiers as the identifiers for user electronic mail accounts.

Priority and Baseline Allocation:

LOW AC-2	MOD AC-2 (1) (2) (3) (4) (5) (6)	HIGH AC-2 (1) (2) (3) (4) (5) (6)
----------	----------------------------------	-----------------------------------

B.4.3 AC-17 Remote access

Control: The organization:

- (1) Documents allowed methods of remote access to the information system;
- (2) Establishes usage restrictions and implementation guidance for each allowed remote access method;
- (3) Authorizes remote access to the information system prior to connection; and
- (4) Enforces requirements for remote connections to the information system.

Supplemental Guidance: Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Virtual Private Network (VPN) when adequately provisioned, may be treated as an organization-controlled network. With regard to wireless, radiated signals within organization-controlled facilities, typically qualify as outside organizational control. Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions to the information system associated with remote connections is accomplished by control AC-3. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. NIST Special Publications 800-48 and 800-97 provide guidance on wireless network security. NIST Special Publication 800-94 provides guidance on wireless intrusion detection and prevention. Related controls: AC-1, AC-3, AC-20, IA-2, IA-8.

Control Enhancements:

- (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.
- (2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the FIPS 199 impact level of the information. Related controls: SC-8, SC-9.
- (3) The information system routes all remote accesses through a limited number of managed access control points.

- (4) The organization authorizes remote access for privileged commands and security-relevant information only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

Enhancement Supplemental Guidance: Related control: AC-6.

- (5) The information system protects wireless access to the system using authentication and encryption.

Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary.

- (6) The organization monitors for unauthorized remote connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*] and takes appropriate action if an unauthorized connection is discovered.

Enhancement Supplemental Guidance: Organizations proactively search for unauthorized remote connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

- (7) The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issue.

- (8) The organization does not allow users to independently configure wireless networking capabilities.

- (9) The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

- (10) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ additional security measures [*Assignment: organization-defined security measures*] and are audited.

- (11) The organization disables peer-to-peer wireless networking capability within the information system except for explicitly identified components in support of specific operational requirements.

- (12) The organization disables Bluetooth wireless networking capability within the information system except for explicitly identified components in support of specific operational requirements.

Priority and Baseline Allocation:

LOW AC-17	MOD AC-17 (1) (2) (3) (4) (5)	HIGH AC-17 (1) (2) (3) (4) (5) (6)
-----------	-------------------------------	--

B.5 Definition of an ASC built from a sample SP 800-53 control

This section presents in an informal manner how control AU-14 from SP800-53 Rev. 3 can be described using the ISO/IEC 27034 ASC structure.

The complete and precise ASC data structure will be discussed in ISO/IEC 27034-5.

B.5.1 Control AU-14 as described in SP 800-53 Rev. 3

Control AU-14 is described in SP 800-53 Rev. 3 as follows:

AU-14 SESSION AUDIT

Control: The information system provides the capability to:

- Capture/record and log all content related to a user session; and
- Remotely view/hear all content related to an established user session in real time.

Supplemental Guidance: Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Control Enhancements:

(1) The information system initiates session audits at system start-up.

References: None.

Priority and Baseline Allocation:

LOW Not Selected	MOD Not Selected	HIGH Not Selected
------------------	------------------	-------------------

B.5.2 Control AU-14 as described using ISO/IEC 27034 ASC format

Control AU-14 can be described as an ASC in conformity with ISO/IEC 27034 as described in Table B.3 below.

Table B.3 – SP800-53 control AU-14 described using ISO/IEC 27034 ASC format

Field	Description	Value
ASC Identification:		
ASC-AU-14_Id-Label:	Text: ASC Name	Session Audit
ASC-AU-14_Id-UID:	Text: ASC Unique Identification number	ASC-AU-14
ASC-AU-14_Id-Description:	Text: ASC Description in plain text.	The information system provides the capability to: <ul style="list-style-type: none"> a. Capture/record and log all content related to a user session; and b. Remotely view/hear all content related to an established user session in real time. Supplemental Guidance: Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance.
ASC-AU-14_Id-Author name	Text: Last name, first name, middle name	Wubu, Daming
ASC-AU-14_Id-Author company name	Text:	ACME corporation.
ASC-AU-14_Id-Author email	Text: eMail address	Wdaming@ACME.com
ASC-AU-14_Id-Author signature	Signed hash of the original ASC	8947358970734205279067248
ASC-AU-14_Id-Organization UID:	Organisation's ID	JTC1/SC27 WG4 27034-1 WD3 01-001
ASC-AU-14_Id-Creation date:	Date: yyyy-mm-dd	2009-04-08
ASC-AU-14_Id-Pointer to parent:	Parents ASC: List of ASC ID or NULL.	NULL
ASC-AU-14_Id-Pointer to children:	Children ASC: List of ASC ID or NULL.	NULL
ASC-AU-14_Id-Pointers to the business context:	List of B_Context or NULL	Financial
ASC-AU-14_Id-Pointer to the regulatory context:	List of R_Context or NULL	Privacy Law #RF76G7, article 4.11
ASC-AU-14_Id-Pointer to the technological context:	List of T_Context or NULL	NULL
ASC-AU-14_App_Specification:	Specifications of the application that provide the security requirements for the ASC:	Application establishes a persistent session.
ASC-AU-14_Id-ASC XML version	Version of ASC XML Schema: Version number.	v1.0 Beta

Field	Description	Value
ASC Objectives:		
ASC-AU-14_Obj-Level-of-Trust:	1 or n - Levels of trust targeted: On which level of trust this ASC is active. May be associated to several levels.	5, 6, 7, 8, 9.
ASC-AU-14_Obj-why:	Why this ASC exists. Identify the needs for the manager, the team leader, the development team, the auditor, etc. The objective also precises what will be evaluated.	Ensure that the user complies with the Privacy Law #RF76G7, article 4.11, and organization acceptable use policy.
ASC-AU-14_LevelOfTrust-TotalLevels:	Range of levels of trust used by organisation	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
ASC-AU-14_LevelOfTrust-why:		Session audit is resource-intensive and only required for applications that manipulate personal information.
ASC-AU-14_AppSpec_ComplToReg_Stand&BestPractices:	Standards to which this ASC is associated (ITIL, Cobit, ISO17799, RUP, design pattern name, etc.)	NIST SP-800-53 Rev. 3, AU-14
ASC Security Activity:		
ASC-AU-14_SecAct-Label:	Text: Activity name	Implement Session Audit class from approved Security Library
ASC-AU-14_SecAct-UID:	Text: Security Activity Unique ID	ACT-001-JAVA027
ASC-AU-14_SecAct-Description:	Complete description of the activity. It presents who does what. Roughly, it describes the processes and actors needed to implement or evaluate the measure.	Use the Organisation approved JAVA security Library to implement the secured audit session process in the application.
ASC-AU-14_SecAct-Complexity:	Activity complexity: Simple, Standard, Complex, Very complex.	Simple
ASC-AU-14_SecAct-who_Role:	Existing role in the organization	Developer
ASC-AU-14_SecAct-who_Responsability:	R = Realization, P = Participation, ...	R
ASC-AU-14_SecAct-who_Qualification:	Activity qualification: Presents the qualifications required for the actors.	Developer level intermediate or more
ASC-AU-14_SecAct-When:	Target an activity in the ISO/IEC 27034 Application Security Life Cycle Reference Model	Development phase, unit development activity
ASC-AU-14_SecAct-Artefact:	Artefact: Name and description of the artefact produced by this activity.	Call to the relevant JAVA case
ASC-AU-14_SecAct-Result_Expected:	Results expected: Situation, status or precise artefact value description.	For each transaction, the class is required to send the transactions particulars to the organisation secure logging service. The unit test results and strategy documentation are expected at the end of this activity.
ASC-AU-14_SecAct-cost:	Activity cost: The cost to complete this activity. (Days/person, money, etc.)	10 days-person
ASC Verification Measurement:		
ASC-AU-14_VerfMeas-Label:		Session Audit components implementation verification
ASC-AU-14_VerfMeas-UID:		VeM-001-JAVA453
ASC-AU-14_VerfMeas-Description:		Verify that for each transaction, the class sends the transactions particulars to the organisation secure logging service. Verify that the unit test results and strategy documentation are presented and successful.

Field	Description	Value
ASC-AU-14_VerfMeas-Complexity	Verification Measurement complexity: Simple, Standard, Complex, Very complex.	Standard
ASC-AU-14_VerfMeas-who_Role:		Senior code reviewer
ASC-AU-14_VerfMeas-who_Responsability:	R = Realization, P = Participation, ...	R
ASC-AU-14_VerfMeas-who_Qualification:	Control activity qualification: Presents the qualifications required for the actors.	Senior Java developer
ASC-AU-14_VerfMeas-when_Phase:	Target an activity in the ISO/IEC 27034 Application security life cycle reference model.	Development phase, functional test activity
ASC-AU-14_VerfMeas-Artifact:		Result must be TRUE for all verification measurements.
ASC-AU-14_VerfMeas-cost:	Control activity cost: The cost to verify this activity. (Days/person, money, etc.) May specify that a periodic evaluation will be required.	1 day-person

Annex C (informative)

ISO/IEC 27005 risk management process mapped with the ASMP

It is possible to consider the ASMP from a risk management point of view, thus following a process similar to the risk management process defined by ISO/IEC 27005.

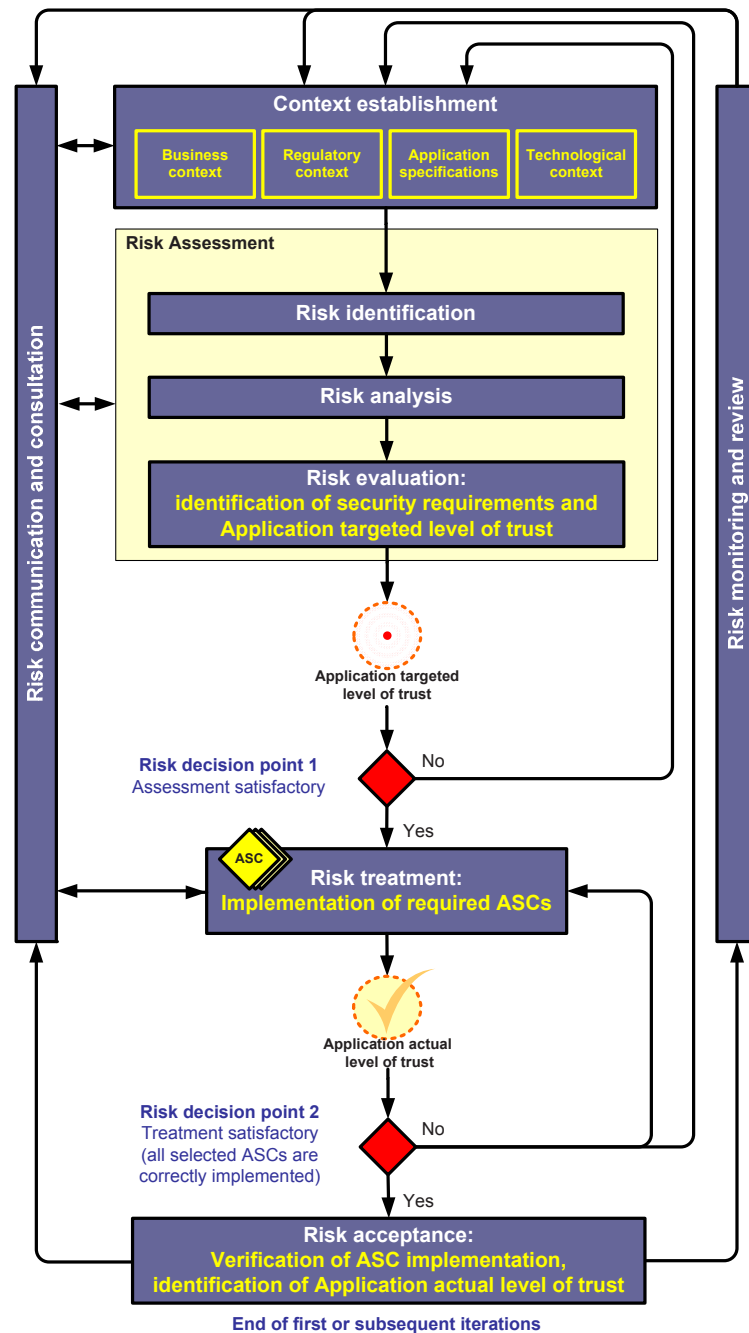


Figure C.1 – ISO/IEC 27005 risk management process mapped with the ASMP.

The following process elements are performed. The application context is established first. Then an application-level risk assessment is conducted. If this provides sufficient information to effectively determine the controls required to mitigate the risks for the organization to use this application to a degree acceptable (or tolerable) to the application owner, then the task is complete and risk treatment follows. If the information is insufficient, another iteration of the risk assessment with revised risk criteria and application environment (e.g. business, regulatory and technological contexts, application specifications, risk evaluation criteria, risk acceptance criteria, impact criteria, etc.) will be conducted, possibly on limited parts of the total application scope.

The effectiveness of risk treatment depends on the results of the risk assessment. If the risk and the derived security requirements for an application are not well identified, the application will not be adequately secured, because security requirements are needed to identify the application's Targeted Level of Trust (8.2.3). It is possible that the risk treatment will not immediately lead to an acceptable (or tolerable) residual risk. In that case, another iteration of the risk assessment with more precise context parameters (e.g. application specifications, security requirements, level of trust, required ASC, etc.), is performed. If necessary, security acceptance can be required by a formal internal or external validation.

According to ISO/IEC 27005, risk acceptance is done at the end of the risk management process. Because security cannot be implemented on an application at the end of its realisation stage, acceptance of application risk should be done earlier in the ASMP by the application owner. This should be done at the end of the risk assessment process, when the owner is identifying the Targeted Level of Trust for a specific application.

During the whole application security risk management process it is important that risks, level of trust and related ASCs are communicated to the appropriate teams. Also, the application owner should ensure risk monitoring and review during the whole application life cycle.

Awareness by managers and staff of the risks, the nature of the controls in place to mitigate the risks and the areas of concern to the organization assist in dealing with incidents and unexpected events in the most effective manner. As defined in ISO/IEC 27005, the detailed results of every activity of the risk management process and from the two risk decision points should be documented.

Bibliography

- [1] ISO/IEC 2382-7:2000, *Information technology — Vocabulary — Part 7: Computer programming*
- [2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*
- [3] ISO/IEC 9126 (all parts), *Software engineering — Product quality*
- [4] ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*
- [5] ISO/TS 15000 (all parts), *Electronic business eXtensible Markup Language (ebXML)*
- [6] ISO/IEC 15026 (all parts), *Systems and software engineering — Systems and software assurance*
- [7] ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*
- [8] ISO/IEC 15289:2006, *Systems and software engineering — Content of systems and software life cycle process information products (Documentation)*
- [9] ISO/IEC 15408-3:2008, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*
- [10] ISO/IEC TR 15443 (all parts), *Information technology — Security techniques — A framework for IT security assurance*
- [11] ISO/IEC 18019:2004, *Software and system engineering — Guidelines for the design and preparation of user documentation for application software*
- [12] ISO/IEC TR 20000-4:2010, *Information technology — Service management — Part 4: Process reference model*
- [13] ISO/IEC 21827:2008, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)*
- [14] ISO/IEC/IEEE 24765:2010, *Systems and software engineering — Vocabulary*
- [15] ISO/IEC/IEEE 29148 (to be published), *Systems and software engineering — Life cycle processes — Requirements engineering*
- [16] ISO/IEC TR 29193 (under development), *Secure system engineering principles and techniques*
- [17] NIST Special Publication 800-48:2008, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*
- [18] NIST Special Publication 800-53 Revision 3:2009, *Recommended Security Controls for Federal Information Systems and Organizations*
- [19] NIST Special Publication 800-77:2005, *Guide to SSL VPNs*
- [20] NIST Special Publication 800-94:2007, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- [21] NIST Special Publication 800-97:2007, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*

British Standards Institution (BSI)

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

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

About us

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

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

Information on standards

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

Buying standards

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

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

Subscriptions

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

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

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

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

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

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

Revisions

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

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

Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

Useful Contacts:

Customer Services

Tel: +44 845 086 9001

Email (orders): orders@bsigroup.com

Email (enquiries): cservices@bsigroup.com

Subscriptions

Tel: +44 845 086 9001

Email: subscriptions@bsigroup.com

Knowledge Centre

Tel: +44 20 8996 7004

Email: knowledgecentre@bsigroup.com

Copyright & Licensing

Tel: +44 20 8996 7070

Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK



...making excellence a habit.™