INTERNATIONAL STANDARD

ISO/IEC 27034-6

First edition
2016-10-01

Information technology — Security techniques — Application security —

Part 6: Case studies

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

Partie 6: Études de cas

Reference number
ISO/IEC 27034-6:2016(E)

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

Contents

Page

Foreword

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

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

Introduction

0.1 General

There is an increasing need for organizations to focus on protecting their information at the application level. A systematic approach towards increasing the level of application security provides an organization with evidence that information being used or stored by its applications is being adequately protected.

ISO/IEC 27034 (all parts) provides concepts, principles, frameworks, components and processes to assist organizations in integrating security seamlessly throughout the life cycle of their applications.

The application security control (ASC) is one of the key components of this document.

To facilitate the implementation of ISO/IEC 27034 (all parts) application security framework and the communication and exchange of ASCs, a formal structure should be defined for representing ASCs and certain other components of the framework.

0.2 Purpose

The purpose of this document is to provide examples of security guidance for organizations to acquire, develop, outsource and manage security for their specific applications through their life cycle.

0.3 Targeted Audiences

0.3.1 General

The following audiences will find values and benefits when carrying their designated organizational roles:

a) domain experts.

0.3.2 Domain experts

Domain experts contributing knowledge in application provisioning, operating or auditing, who need to

a) participate in ASC development, validation and verification,

b) participate in ASC implementation and maintenance, by proposing strategies, components and implementation processes for adapting ASCs to the organization's context, and

c) validate that ASCs are useable and useful in application projects.

Information technology — Security techniques — Application security —

Part 6: Case studies

1 Scope

This document provides usage examples of ASCs for specific applications.

NOTE Herein specified ASCs are provided for explanation purposes only and the audience is encouraged to create their own ASCs to assure the application security.

2 Normative references

There are no normative references cited in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1 apply.

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

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

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

4 Abbreviated terms

ASC application security control

ASLC application security life cycle

ASLCRM application security life cycle reference model

ONF organization normative framework

5 Security guidance for specific applications

5.1 General

Guidelines play an important role for companies trying to implement any best practice or ISO standard because they instruct how to institutionalize the practices or rules and, sometimes, the guidance is based on common examples.

Companies benefit from this guidance as it demonstrates, as a practical example, how to structure ASCs for specific applications using the recommended XML data structure defined in ISO/IEC 27034-5-1 and for the implementation of the Organizational Normative Framework.

5.2 ASC example: Java code revision for mobile applications

5.2.1 General

Code review seams trivial but when an application is built from thousands of lines of code, it may be unproductive and/or too expensive to revise everything.

This example presents an ASC designed by a fictive organization called *ORGANIsation Inc.* This ASC implements the security activity of code review.

5.2.2 Purpose

The purpose of 5.2 is to provide an intuitive description of an example ASC named "Code Review" for an organization developing Java mobile applications. For the sake of brevity and readability, a simplified subset of the ASC is presented in English only (language="EN"), but the ASC requirements defined in ISO/IEC 27034-5 allows any object in an ASC to be described in any characters sets, as presented by the Table A.1.

5.2.3 Context

ORGANIsation Inc. is an international organization developing Java mobile applications for its own use and on behalf of its clients. ORGANIsation software development offices are located in Montreal, Vancouver and Moscow. For this reason, ORGANIsation's policy is that any development documentation, guideline or training should be available in English, French and Russian languages.

ORGANIsation's implementation strategy for ISO/IEC 27034 (all parts) prioritizes the design of ASCs for reducing security vulnerabilities in Java mobile code. The ORGANIsation ONF committee mandates the Application Security Department (ASD) to design and submit Java code review ASCs.

5.2.4 ORGANIsation Information classification guidelines

ORGANIsation utilizes approved internal classification guidelines for classifying the information into four levels:

a) restricted;

b) confidential;

c) secret;

d) top secret.

5.2.5 Levels of trust included in the ORGANIsation ASC Library

ORGANIsation had previously conducted an organization-wide security risk assessment, for the purpose of which it divided its applications into six categories according to their impact on organizational risk. Following this, domain experts mandated by the ONF committee decided to use those six categories as a template for defining ORGANIsation's application levels of trust. An informal definition along with a descriptive label for each level of trust is given in Table 1.

Table 1 — ORGANIsation's application levels of trust

Level of trust	Name	Description
0	Baseline	All ORGANIsation's applications shall comply with this Level of Trust.
1	Isolated — Local network only	This Level of Trust is appropriate for applications used on isolated corporate networks, with no connection to external networks.
2	Low — Internet, public information only	This Level of Trust is appropriate for Internet-facing applications sharing public information without any privacy concern.
3	Medium — Internet, corporate users	This Level of Trust is appropriate for Internet-facing, transactional applications used by corporate users, allowing access to corporate services, user files and/or transactions under $5 000.
4	High — Secure transactions and privacy protection over Internet	This Level of Trust is appropriate for Internet-facing, transactional applications, used by corporate users, allowing access to user private information and/or transactions from $5 000 to $25 000.
5	Private	This Level of Trust is appropriate for transactional applications requiring highly secure transactions, privileged access and/or secure critical storage. Access to critical information and/or transactions over $25 000 is authorized.

5.2.6 Outcome

The application security department was mandate to select and acquire an automatic source code review tool suitable for the Java language, with user-configurable review rules. After analysis of vendor propositions, the department selected a tool named "Efficient-Reviewer version 2.2".

At the end of this project, version 1.0 of five ASCs were developed and implemented.

Table 2 — ORGANIsation's ASCs for code review

ID	Name	Level of trust	Description
ORGANIsation-ASD-042	Code Review	— Baseline — Isolated – Local network only — Low – Internet, public information only — Medium – Internet, corporate users — High – Secure transactions and privacy protection over Internet — Private	This ASC is used to help developers to perform a code review control for JAVA applications.
ORGANIsation-ASD-043	Code Classification	— Baseline — Isolated – Local network only — Low – Internet, public information only — Medium – Internet, corporate users — High – Secure transactions and privacy protection over Internet — Private	Classify all Java classes in the packages needed by the application. Any class should inherit its classification from the highest-classified information it processes.

Table 2 *(continued)*

ID	Name	Level of trust	Description
ORGANIsation-ASD-044	Basic Automatic Code Review	— Baseline — Isolated – Local network only — Low – Internet, public information only	This ASC is used to help developers to implement a code review control for Java applications by providing an automatic source code security review process for Java classes classified as "Strategic" and "Critical".
ORGANIsation-ASD-045	Advanced Automatic Code Review	— Medium – Internet, corporate users — High – Secure transactions and privacy protection over Internet — Private	This ASC is used to help developers to implement a code review control for Java applications by providing an automatic source code security review process for all of the application's Java classes.
ORGANIsation-ASD-046	Manual Code Review	— High – Secure transactions and privacy protection over Internet — Private	This ASC is used to help developers to implement a code review control for Java applications by providing a manual source code security review process for Java classes classified as "Strategic" and "Critical".

NOTE The ASC with ID "ORGANIsation-ASD-042" is the root of the code-review ASC hierarchy.

5.2.7 ORGANIsation stakeholders involved in these ASCs

For each of these ASCs, the following responsibilities were determined.

NOTE This subclause consist consist of informal descriptions of ASC data elements, followed by the formal description of same using XML notation.

Table 3 — Names and responsibilities of Java code review ASCs stakeholders

Role/responsibility	Name	Notes/ORGANIsation directives
Author	Jules Vernes	
Owner	Douglas Adams	— M. Adams requested to start numbering ORGANIsation's ASCs from 42.
Creation Request:	Herbert George Wells	— A PDF version of the creation request, explaining why this ASC is required by the organization will be included in each ASC. — The PGP signature of M. Wells will be required to seal the ASC. — The date when this activity will be completed shall be specified.
Design	Jules Verne	
Validation	Arthur C. Clarke	
Development	Frank Herbert	
Verification	Ray Bradbury William Gibson	— The security activity and the measurement and verification activity shall both be verified in both languages.
Approval	Robert Heinlein	— The PGP signature of M. Heinlein will be required to seal the ASC.
Final Owner approval	Douglas Adams	— The PGP signature of the owner is required to seal the ASC.

Table 3 *(continued)*

Role/responsibility	Name	Notes/ORGANIsation directives
Published for training	Isaac Asimov	
Active	Mary Shelley	
Expired	Not defined.	

Additional information recorded in each ASC includes coordinates of each actor (department, e-mail address, phone number, physical address) and the completion date for each activity.

The ASC structure allows each version of an ASC to be electronically signed for integrity purposes. ORGANIsation directives in Table 3 specify which electronic signatures are mandatory. This provides assurance that critical stages of the ASC's life cycle were performed and verified according to ORGANIsation's policy.

In Figure 1, the cloud-shaped region illustrates the part of the ASC protected by electronic signatures.

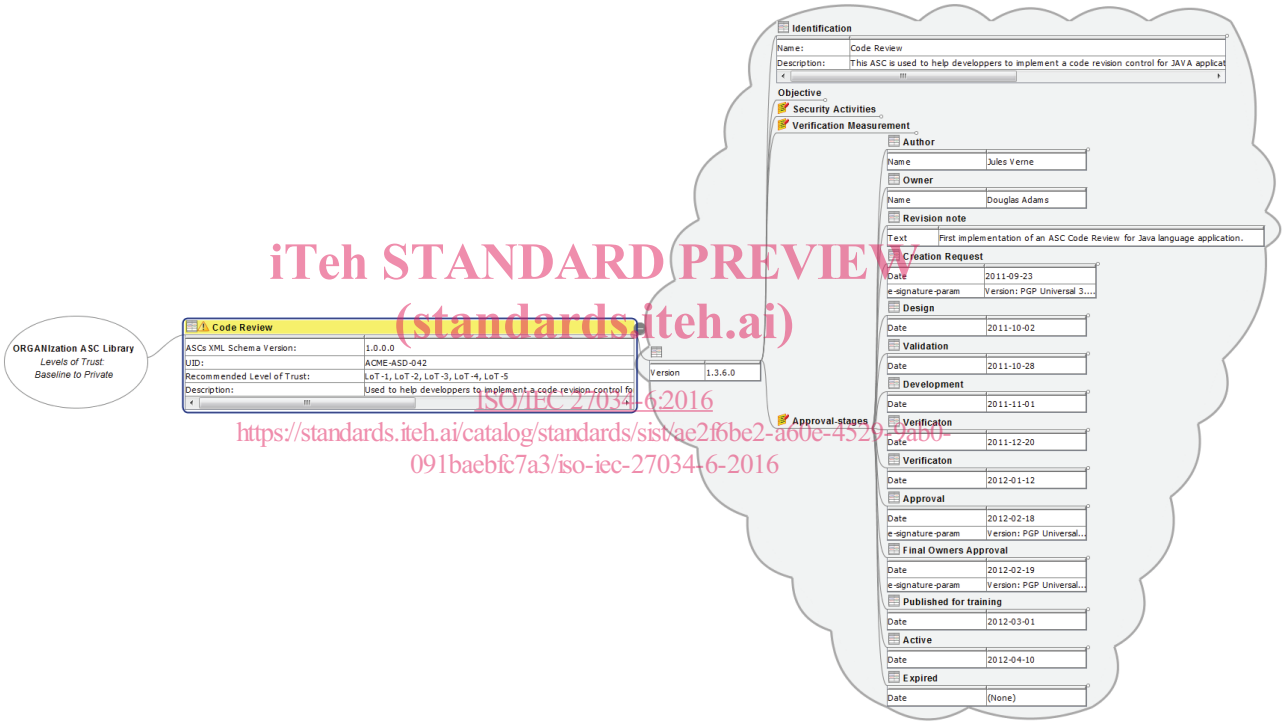

Figure 1 — Integrity scope of stakeholder's electronic signatures

See Table A.2.

"ASC ORGANIsation-ASD-042 - Code Review" is a "Head ASC" and does not contain any security activity or verification and measurement activity. Instead, it refers to four children ASCs, which are required to implement code review in the organization's Java development process. Figure 2 illustrates this concept of ASC hierarchy. It is also to be noted that the "Head ASC" omits some of the mandatory ASC attributes defined by ISO/IEC 27034-1:2011, Figure 6. These will be provided by the child ASCs.

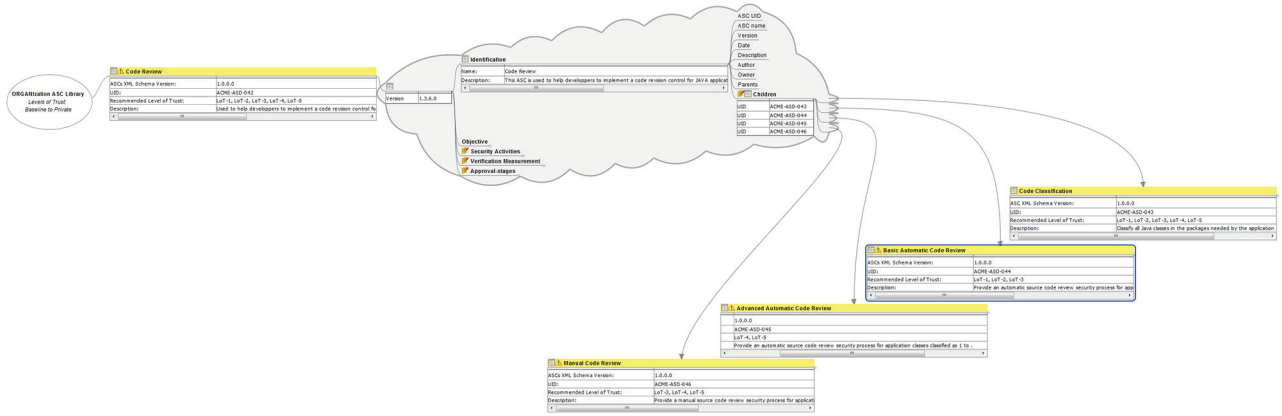

Figure 2 — Code review ASC graph

See Table A.3.

5.2.8 Descriptions of sample ASCs

5.2.8.1 General

This subclause describes the head ASC (Code review) and its four children ASCs developed and implemented in the ORGANIsation ASC Library.

5.2.8.2 ASC ORGANIsation-ASD-042: Code review

ASC	Code Review
ASC UID	ORGANIsation-ASD-042
Identification	
ASC UID	ORGANIsation-ASD-042
ASC name	Code Review
Version	1.3.6.0
Date	2016-01-04
Description	This ASC is used to help developers to perform a code review control for JAVA applications.
Author	Jules Verne Application Security Department ORGANIsation inc. 1234 Street ave W, Beautiful city, Quebec, Canada Email office: JVernes@ORGANIsation.com Phone office: +1.234.567.8901

Owner	Douglas Adams Application Security Department ORGANIsation inc. 1234 Street ave W, Beautiful city, Quebec, Canada Email office: DAdams@ORGANIsation.com Phone office: +1.109.876.5432
Parents	None
Children	ORGANIsation-ASD-043 ORGANIsation-ASD-044 ORGANIsation-ASD-045 ORGANIsation-ASD-046

See Table A.4.

Approval-stages	(See the ASC approval-stages XML example in 5.2.7.)

Objective			
Objective description	Top-level ASC whose objective is to group the various leaf ASCs related to code review in Java.		
Requirements addressed	-- Content removed for simplification --		
Assigned Levels of trust	0, 1, 2, 3, 4, 5		
Context of use	Technological context		
Levels of trust range	**Level of Trust**	**Name**	**Description**
	0	Baseline	All ORGANIsation's applications shall comply with this Level of Trust.
	1	Isolated – Local network only	This Level of Trust is appropriate for applications used on isolated corporate networks, with no connection to external networks.
	2	Low – Internet, public information only	This Level of Trust is appropriate for Internet-facing applications sharing public information without any privacy concern.
	3	Medium – Internet, corporate users	This Level of Trust is appropriate for Internet-facing, transactional applications used by corporate users, allowing access to corporate services, user files and/or transactions under $5 000.
	4	High – Secure transactions and privacy protection over Internet	This Level of Trust is appropriate for Internet-facing, transactional applications, used by corporate users, allowing access to user private information and/or transactions from $5 000 to $25 000.

	5	Private	This Level of Trust is appropriate for transactional applications requiring highly secure transactions, privileged access and/or secure critical storage. Access to critical information and/or transactions over $25 000 is authorized.
	(See Table 2)		
Pre-conditions	-- Content removed for simplification --		

See Table A.5.

Security Activity	None.
Verification Measurement	None.

5.2.8.3 ASC ORGANIsation-ASD-043: Code classification

ASC	Code Classification
ASC ID	ORGANIsation-ASD-043
Identification	
ASC UID	ORGANIsation-ASD-043
ASC name	Code Classification
Date	2015-12-25
Description	Classify all Java classes in the packages needed by the application. Any class should inherit its classification from the highest-classified information it processes.
Version	2.6.1.1
Author	-- Content removed for simplification --
Owner	-- Content removed for simplification --
Parents	ORGANIsation-ASD-042
Children	None

Approval-stages	(See the ASC approval-stages XML example in 5.2.7.)

Objective	
Objective description	Define the scope of the code review.
Requirements addressed	Business requirements: ORGANIsation Development guidelines v2.1, Section 5.6 – Application components classification.
Assigned Levels of trust	0, 1, 2, 3, 4, 5
Levels of trust range	(See Table 2)
Pre-conditions	-- Content removed for simplification --

See Table A.6.

Security activity	
Name (what)	Classify classes and packages
Description	Identify and categorize the application's Java classes and packages.
Target information group	Application Data (see ISO/IEC 27034-1:2011, 6.3)
Target information sub-group	Development documentation
Target information group name	Application's Java code architecture
Outcome general description	Categorized classes and packages information merged in the application's Java code architecture documentation.
Supporting expert ressource	Orson Scott Card ORGANIsation inc. Email: Orson.Scott.Card@ORGANIsation.com
Complexity	COMPLEX
Complexity description	This activity should be performed by someone able to identify, from the application architecture documents, what information is manipulated by each Java class and to identify security risks that may threaten sensitive information.
Global estimated effort (how much)	— Average of 1 h to classify and document 10 Java classes. — Average of 15 h to update the Application Security Risk Analysis.
Role (who)	APPLICATION ARCHITECT
Responsibility	RESPONSIBLE
Required qualifications	1. Passed an examination on the ORGANIsation Java coding best practices. 2. Minimum 5 years experience in Java Development. 3. Active CSSLP Certification.
Pre-condition	— The application classes and packages identification section of the Application design document is completed. — A list of categorized information groups involved by the application already exists.
Security activity description (how)	Classify the application classes to be developed or maintained in this project. 1. Identify contexts, roles, and information involved with the application module. Ref.: ORGANIsation Development guidelines v2.1. 2. Realize or update the Application Security Risk Analysis. 3. Classify all classes in the packages needed by the application in the Application Class Classification section of the Application design document. Ref.: ORGANIsation Code Classification Guide, v1.4, and Application Class Classification section – Template v2.3.
Localization (where)	— Application development environment