DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27034-6

ISO/IEC JTC **1**/SC **27** Secretariat: **DIN**

Voting begins on:
2015-07-27

Voting terminates on:
2015-10-27

Information technology — Security techniques — Application security —

Part 6:
Security guidance for specific applications

Technologies de l'information — Techniques de securite — Securite des applications

ICS: 35.040

Reference number
ISO/IEC DIS 27034-6:2015(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

Figures

Page

Tables

Page

1

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 27034-6 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second/third/... edition cancels and replaces the first/second/... edition (), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

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

— *Part 1: Overview and concepts*

— *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*

— *Part 5-1: Protocols and application security controls data structure – XML Schemas*

— *Part 6: Security guidance for specific application*

— *Part 7: Application security assurance prediction*

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.

The ISO/IEC 27034 International Standard 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 International Standard.

To facilitate the implementation of the ISO/IEC 27034 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 part 6 of the ISO/IEC 27034 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.

Editors' note: This clause will be aligned with audiences targeted by specific examples that will be included in clause 5.

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

Part 6 of this International Standard 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

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 27034-1:2011, Information technology — Security techniques — Application security — Part 1: Overview and concepts

ISO/IEC 27034-2:– [1] *, Information technology — Security techniques — Application security — Part 2: Organization normative framework*

ISO/IEC 27034-5:– [1]*, Information technology — Security techniques — Application security — Part 5: Protocols and application security control data structure*

ISO/IEC 27034-5-1:– [1]*, Information technology — Security techniques — Application security — Part 5-1: Protocols and application security control data structure – XML Schemas*

3 Terms and definitions

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

4 Abbreviated terms

ASLC	Application Security Life Cycle
ASLCRM	Application Security Life Cycle Reference Model
ASC	Application Security Control
ONF	Organization Normative Framework

[1] To be published.

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 this clause 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 – XML example of an ASC name written in three languages in Annex A.

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 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 6 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

LoT	Name	Description
0	Baseline	All ORGANIsation's applications must 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 critical storage security. Access to critical information and/or transactions over 25,000$ is authorized.

5.2.6 Outcome

The application security department's mandate was 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* to *Private*	This ASC is used to help developers to perform a code review control for JAVA applications.
ORGANIsation-ASD-043	Code Classification	*Baseline* to *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.
ORGANIsation-ASD-044	Automatic Code Review Light	*Baseline* to *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	Automatic Code Review	*Medium* and *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

ID	Name	Level of Trust	Description
			process for all of the application's Java classes.
ORGANIsation-ASD-046	Manual Code Review	*High* and *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 The following clauses 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 must 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 must 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.
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.