

# ISO/IEC 27034-1:2011-11 (E)

## Information technology - Security techniques - Application security - Part 1: Overview and concepts

---

<b>Contents</b>	<b>Page</b>
<b>FOREWORD</b> .....	<b>VII</b>
<b>INTRODUCTION</b> .....	<b>VIII</b>
0.1 GENERAL.....	VIII
0.2 PURPOSE .....	VIII
0.3 TARGETED AUDIENCES .....	IX
0.3.1 <i>General</i> .....	ix
0.3.2 <i>Managers</i> .....	ix
0.3.3 <i>Provisioning and operation teams</i> .....	x
0.3.4 <i>Acquirers</i> .....	xi
0.3.5 <i>Suppliers</i> .....	xi
0.3.6 <i>Auditors</i> .....	xi
0.3.7 <i>Users</i> .....	xi
0.4 PRINCIPLES .....	XI
0.4.1 <i>Security is a requirement</i> .....	xi
0.4.2 <i>Application security is context-dependent</i> .....	xii
0.4.3 <i>Appropriate investment for application security</i> .....	xii
0.4.4 <i>Application security should be demonstrated</i> .....	xii
0.5 RELATIONSHIP TO OTHER INTERNATIONAL STANDARDS .....	XIII
0.5.1 <i>General</i> .....	xiii
0.5.2 <i>ISO/IEC 27001, Information security management systems — Requirements</i> .....	xiii
0.5.3 <i>ISO/IEC 27002, Code of practice for information security management</i> .....	xiii
0.5.4 <i>ISO/IEC 27005, Information security risk management</i> .....	xiii
0.5.5 <i>ISO/IEC 21827, Systems Security Engineering — Capability Maturity Model® (SSE CMM®)</i> .....	xiii
0.5.6 <i>ISO/IEC 15408-3, Evaluation criteria for IT security — Part 3: Security assurance components</i> .....	xiii
0.5.7 <i>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</i> .....	xiv
0.5.8 <i>ISO/IEC 15026-2, Systems and software engineering — Systems and software assurance — Part 2: Assurance case</i> .....	xiv
0.5.9 <i>ISO/IEC 15288, Systems and software engineering — System life cycle processes, and ISO/IEC 12207, Systems and software engineering — Software life cycle process</i> .....	xiv
0.5.10 <i>ISO/IEC 29193 (under development), Secure system engineering principles and techniques</i> .....	xiv
<b>1 SCOPE</b> .....	<b>1</b>
<b>2 NORMATIVE REFERENCES</b> .....	<b>1</b>
<b>3 TERMS AND DEFINITIONS</b> .....	<b>1</b>
<b>4 ABBREVIATED TERMS</b> .....	<b>4</b>
<b>5 STRUCTURE OF ISO/IEC 27034</b> .....	<b>5</b>
<b>6 INTRODUCTION TO APPLICATION SECURITY</b> .....	<b>6</b>
6.1 GENERAL.....	6
6.2 APPLICATION SECURITY VS SOFTWARE SECURITY .....	6
6.3 APPLICATION SECURITY SCOPE .....	6
6.3.1 <i>General</i> .....	6
6.3.2 <i>Business context</i> .....	7
6.3.3 <i>Regulatory context</i> .....	7
6.3.4 <i>Application life cycle processes</i> .....	7
6.3.5 <i>Processes involved with the application</i> .....	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
<b>7</b>	<b>ISO/IEC 27034 OVERALL PROCESSES</b> .....	<b>11</b>
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
<b>8</b>	<b>CONCEPTS</b> .....	<b>14</b>
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

<b>ANNEX A (INFORMATIVE) MAPPING AN EXISTING DEVELOPMENT PROCESS TO ISO/IEC 27034 CASE STUDY .....</b>	<b>39</b>
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
<b>ANNEX B (INFORMATIVE) MAPPING ASC WITH AN EXISTING STANDARD.....</b>	<b>55</b>
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
<b>ANNEX C (INFORMATIVE) ISO/IEC 27005 RISK MANAGEMENT PROCESS MAPPED WITH THE ASMP .....</b>	<b>65</b>
<b>BIBLIOGRAPHY .....</b>	<b>67</b>

<b>Figures</b>	<b>Page</b>
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

<b>Tables</b>	<b>Page</b>
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