INTERNATIONAL STANDARD

ISO/IEC 27034-2

First edition
2015-08-15

Information technology — Security techniques — Application security —

Part 2: Organization normative framework

Technologie de l'information — Sécurité des applications —

Partie 2: Cadre normatif de l'organisation

Reference number
ISO/IEC 27034-2:2015(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

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *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*

— *Part 2: Organization normative framework*

The following parts are under preparation:

— *Part 3: Application security management process*

— *Part 4: Application security validation*

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

— *Part 6: Security guidance for specific applications*

— *Part 7: Application security assurance prediction*

Introduction

General

Organizations must protect their information and technological infrastructures in order to stay in business. There is an increasing need for organizations to focus on protecting their information at the application level. A systematic approach towards improving application security provides an organization with evidence that information being used or stored by its applications is being adequately protected.

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

The Organization Normative Framework (ONF) is the most important of those components.

The ONF is an organization-wide framework where all application security best practices recognized by the organization are stored. It comprises essential components, processes that utilize these components, and processes for managing the ONF itself. It is the foundation of application security in the organization and all the organization's future application security decisions should be made by referring to this framework. The ONF is the authoritative source for all components and processes related to application security in the organization.

This part of ISO/IEC 27034 defines the processes required to manage the security of applications in the organization. These processes are presented in 5.4. It also introduces security-related elements of applications (processes, roles and components) that should be integrated into the ONF. These elements are presented in 5.5.

Finally, this part of ISO/IEC 27034 presents the Auditing the ONF process, needed by an organization for verifying its ONF and verifying compliance of all applications with the requirements and controls in the ONF. This process is presented in 5.4.8.

Purpose

The purpose of this part of ISO/IEC 27034 is to assist organizations to create, maintain and validate their own ONF in compliance with the requirements of this International Standard.

This part of ISO/IEC 27034 is designed to enable an organization to align or integrate its ONF with the organization's enterprise architecture and/or the organization's information security management system requirements. However, implementing an information security management system as described in ISO/IEC 27001 is not a requirement for the implementation of this International Standard.

Targeted Audiences

General

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

a) managers;

b) ONF committee;

c) domain experts;

d) auditors.

Managers

Managers should read this International Standard because they are responsible for the following:

a) improving application security through the ONF and other aspects of ISO/IEC 27034;

b) ensuring the ONF stays aligned with the organization's information security management system and application security needs;

c) leading the establishment of the ONF in the organization;

d) ensuring the ONF is available, communicated and used in application projects with proper tools and procedures all across the organization;

e) determining the appropriate level(s) of management that the ONF Committee reports to.

ONF Committee

The ONF Committee is responsible for managing the implementation and maintenance of the application-security-related components and processes in the Organization Normative Framework. The ONF Committee needs to

a) manage the cost of implementing and maintaining the ONF,

b) determine what components and processes should be implemented in the ONF,

c) make sure introduced components and processes respect the organization's priorities for security requirements,

d) review auditor reports for acceptance or rejection that the ONF conforms to this International Standard and meets the organization's requirements,

e) provide processes and tools for managing compliance with standards, laws and regulations according to the regulatory context of the organization,

f) communicate security awareness, training and oversight to all actors, and

g) promote compliance with the ONF for all application projects throughout the organization.

ONF development team

Experts who have been assigned by the ONF Committee with the task of developing and implementing one or more ONF element(s), who need to

a) develop and implement a designed ONF element,

b) determine training in the use of ONF elements by its different actors, and

c) collaborate in providing adequate training to actors.

Domain experts

Provisioning, operation, acquisition and audit experts who need to

a) participate in ONF implementation and maintenance,

b) validate that the ONF is useable and useful in the course of an application project, and

c) propose new components and processes.

Auditors

Auditors are personnel performing roles in the audit processes, who need to participate in ONF validation and verification.

NOTE Auditors may be external or internal to the organization, depending on the target and circumstances of the audit, and according to the organization's audit policies and conformance requirements.

Information technology — Security techniques — Application security —

Part 2: Organization normative framework

1 Scope

This part of ISO/IEC 27034 provides a detailed description of the Organization Normative Framework and provides guidance to organizations for its implementation.

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

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

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

NOTE Additional detail about the relationship between ISO/IEC 27034 and other standards is available in ISO/IEC 27034-1:2011, 0.5.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1, ISO/IEC 27000, and ISO/IEC 27005 apply.

4 Abbreviated terms

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

5 Organization Normative Framework

5.1 General

An organization's normative framework is the sum of all regulations, policies, practices, roles and tools used by the organization. Every organization should already have a normative framework, more or less formally documented.

The Organization Normative Framework (ONF) concept described in this International Standard is an organization-wide framework containing a subset of the organization's processes and components that are relevant to application security and are normative inside the organization.

Although an informal ONF is a first step towards securing the organization's applications, this International Standard recommends a formalized and standardized ONF, as described in this International Standard.

5.2 Purpose

The purpose of implementing the ONF is to:

a) assign responsibility for application security and establish a process that can evolve to improve application security visibility;

b) ensure all elements (components, roles and processes) involved in application security are approved by the appropriate decision-makers and accepted by all relevant actors and stakeholders;

c) minimize resistance to changes brought by these new application security elements;

d) standardize application security elements to ensure a uniform implementation and verification throughout the organization;

e) help the organization to improve its maturity level (as defined in ISO/IEC 15504 and other standards such as SEI/CMMI) by formalizing and revising all application security elements to keep them up to date with the organization's evolving environment; and

f) establish mechanisms to ensure that an appropriate level of security can be achieved in a cost-effective manner, for example, through reusing existing approved application security elements.

5.3 Principles

Organizations creating and maintaining the components and processes in the ONF should be guided by the following principles:

a) the contents of ONF should be adapted to the organization's business needs;

b) any element defined in the ONF should be approved by the ONF committee;

c) contents of the ONF should be available and communicated organization-wide;

d) because the threat context changes continuously and without notice, the organization should be prepared to review the ONF in response to those changes; and

e) the ONF should be auditable.

5.4 ONF Management Process

5.4.1 General

The organization should establish, implement, maintain and improve an organization-level process for the management of its ONF.

The ONF Management Process comprises six sub processes.

Four of them are adapted from the “Plan, Do, Check, Act” processes of the general PDCA model, and are tailored for the development and implementation of application security elements in the ONF.

The following table shows how ONF management sub processes map to the four stages of the PDCA model and to information security management system processes.

Table 1 — Mapping of PDCA stages, information security management system processes and application security-related ONF management sub processes

PDCA Stage	ISO/IEC 27001 **Information security management process**	ISO/IEC 27034 **ONF Management Process**
Plan	Planning	Designing the ONF
Do	Support / Operation	Implementing the ONF
Check	Performance evaluation	Monitoring and reviewing the ONF
Act	Improvement	Improving the ONF

Another sub process, “Establishing the ONF committee”, is used first, to mandate the ONF committee and demonstrate appropriate accountable management’s commitment to application security. Finally, the “Auditing the ONF” sub process is used for verifying the ONF and verifying compliance of applications with the requirements and controls in the ONF.

The organization should perform the ONF Management Process iteratively in order to incrementally implement the ONF. This reduces impact and achieves quicker gains by prioritizing in each iteration those elements that are more urgently needed.

A graphical representation of the ONF Management Process is shown in Figure 1. The figure also shows how this process relates to the organization’s other management processes, and to the Application Security Management Process which makes use of the ONF for adding Application Security Controls to application projects.

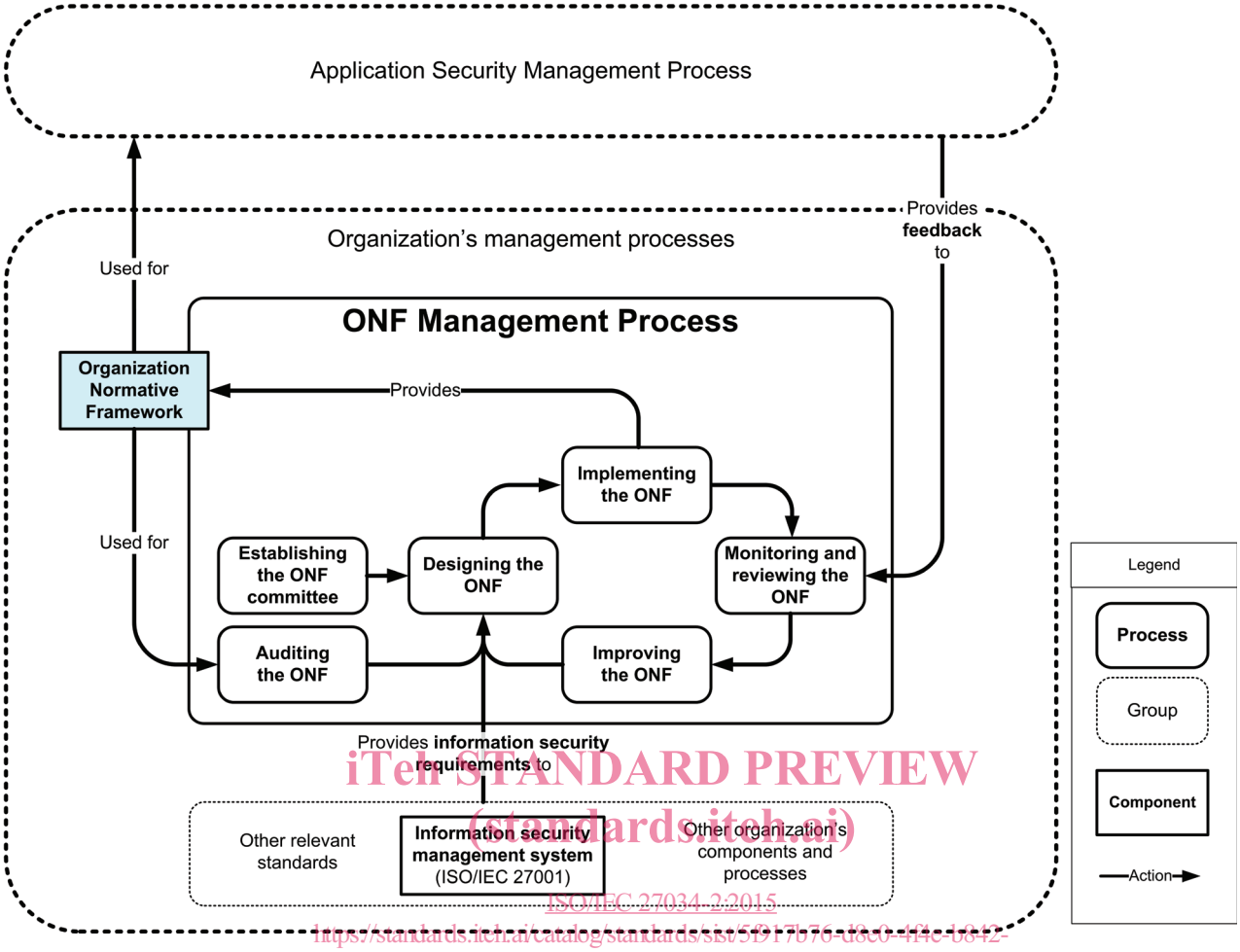

Figure 1 — ONF Management Process

5.4.2 Use of RACI charts in description of activities, roles and responsibilities

This International Standard uses RACI charts for assigning roles and responsibilities for carrying out activities in processes. Such charts identify actors responsible, accountable, consulted or informed for the realization of an activity. Abbreviations are used for describing responsibilities of actors. Those are enumerated in Table 2.

Table 2 — Abbreviations for responsibilities used in RACI charts

Code	*Responsibility*
R	*Responsible for the realization of an activity*
A	*Accountable for the realization of an activity*
C	*Consulted during the realization of an activity*
I	*Informed of the realization of an activity*

Use of RACI charts within organizations implementing this standard is not required. Organizations should align guidance provided in this standard with their own method of clarifying roles and responsibilities.

When conducting realization and verification activities, it is critical for organizations to determine the resources that are responsible, accountable, consulted, and informed. The tables below provide a starting point for discussion during the realization of an ONF.

5.4.3 Establishing the ONF committee

5.4.3.1 Purpose

The purpose of this process is to establish an ONF committee with the required authority and resources for the development, implementation and evolution of the ONF, and to demonstrate appropriate accountable management's commitment.

5.4.3.2 Outcomes

As a result of the successful performance of this process:

a) roles and responsibilities for ONF Committee members are defined;

b) a candidate is appointed for each role;

c) the ONF committee is officially mandated to establish and maintain the ONF and this is communicated within the organization;

d) the ONF committee is made accountable for the implementation, quality, and utilization of the ONF in the organization;

e) the ONF committee is provided with the necessary resources for assuming its responsibilities; and

f) the ONF committee is provided with sufficient authority for relevant internal communication.

5.4.3.3 Realization activities

Table 3 — RACI chart for realization of process "Establishing the ONF committee"

Realization activities	Managers
1) Define roles and responsibilities for ONF Committee members.	A/R
2) Appoint a candidate for each role.	A/R
3) Officially mandate the ONF committee to establish and maintain the ONF and communicate this within the organization.	A/R
4) Make the ONF committee accountable for the ONF implementation, quality, and utilization in the organization.	A/R
5) Provide the ONF committee with the necessary resources for assuming its responsibilities.	A/R
6) Provide the ONF committee with sufficient authority for relevant internal communication.	A/R

5.4.3.4 Verification activities

Table 4 — RACI chart for verification of process "Establishing the ONF committee"

Verification activities	Managers	Auditors
1) Verify the existence of official communication from appropriate accountable management demonstrating that outcomes a), b), c) and d), were achieved.	A	R
2) Evaluate from official communication from appropriate accountable management whether outcomes e) and f) were achieved.	A	R

5.4.4 Designing the ONF

5.4.4.1 Purpose

The purpose of this process is to determine goals for application security, determine which elements should be implemented in the ONF in the current iteration of the ONF management process, and design those elements.

5.4.4.2 Outcomes

As a result of the successful performance of this process:

a) the scope of the current iteration of the ONF management process is defined, approved by appropriate accountable management and communicated, and

b) in-scope ONF elements are designed.

5.4.4.3 Realization activities

Table 5 — RACI chart for process "Designing the ONF"

Realization activities	Managers	ONF Committee
1) Determine application security goals.	A	R
2) Define the scope and implementation strategy of the current iteration of the ONF management process.	A	R
3) Define the organization's application security posture, priorities and plans.		A/R
4) Establish an inventory and a security classification of information involved with applications and integrate it within the organization's information architecture.		A/R
5) Design ONF elements.		A/R

5.4.4.4 Verification activities

Table 6 — RACI chart for verification for process "Designing the ONF"

Verification activities	Managers	Auditors
1) Verify that the scope of the current iteration of the ONF management process is defined, approved by appropriate accountable management and communicated.	A	R
2) Verify that the ONF elements in scope for the current iteration are designed correctly.	A	R

5.4.4.5 Guidance

Possible inputs for this process are:

a) outcomes of the organization's security risk management process, such as organization-level security objectives or plans;

b) outcomes of the "Improving the ONF" process, such as documented needs to redesign ONF elements or design new ONF elements;

c) outcomes of the "Auditing the ONF" process;

d) outcomes of an organization's information security audit;

e) training needs, strategy, metrics, policies, and up to date knowledge of attacks and mitigations; and

f) other ISO/IEC standards including supply chain (27036), evaluation (15408), assurance (15026), software life cycle processes (12207), system life cycle processes (15288) – see ISO/IEC 27034-1:2011, 0.5 and Figure 1.

ONF elements that should be designed are described in 5.5. Specific guidance for the design of those elements is also found in 5.5.

ONF elements should be designed and built in an iterative process. In the course of this process, the ONF committee should:

a) prioritize elements based on the organization's priorities and available resources;

b) assign responsibility and sufficient resources for the design of in-scope elements;

c) monitor and validate the design of ONF elements;

d) integrate the ONF's processes into the organization's business processes;

e) ensure that the ONF's application security policy is aligned with the organization's other policies and the organization's information security management system;

f) ensure that the ONF is aligned with the organization's security architecture, information architecture and business architecture;

g) ensure that ONF risk management performance indicators are aligned with other performance indicators used in the organization;

h) ensure that ONF risk management objectives are aligned with the objectives and strategies of the organization;

i) ensure legal and regulatory compliance;

j) ensure that the outcomes of its activities are communicated to all relevant parties;

k) designate an information repository to act as the authoritative source for consolidating and communicating information on the ONF and all its elements;

l) establish communication and reporting mechanisms (internal, external, interfaces with application projects, etc.); and

m) provide guidance on how to implement the requirements from this International Standard in the organization, by establishing an application security management policy.

NOTE It should not be expected that every member or partner of the organization will read this International Standard. It should be expected that they conform to the policy.

When approving the scope of a given iteration of the ONF management process, appropriate accountable management should:

a) verify that the ONF and its management processes are compatible with the strategic direction, information security objectives and policy of the organization; and

b) verify that the ONF is aligned with and supports the organization's existing enterprise architecture.

When verifying that the ONF elements in scope for the current iteration are designed correctly, auditors may consider criteria such as:

a) definition of scope and implementation strategy of the current iteration of the ONF management process;

b) definition of the organization's strategic application security posture, priorities and plans;

c) establishment of an application security management policy;

d) inventory and security classification (i.e. in terms of confidentiality, integrity and availability) of information involved with applications integrated within the organization's information architecture;

e) definition of roles for the implementation project for every component and process in the ONF;

f) assignment of people to such roles;

g) results of projects monitoring; and

h) communication and reporting mechanisms.

5.4.5 Implementing the ONF

5.4.5.1 Purpose

The purpose of this process is to implement ONF elements that have been designed in the current iteration of the ONF management process, provide application security solutions such as components and processes, and distribute them to be used throughout the organization as application security guidelines, services or mandatory practices.

5.4.5.2 Outcomes

As a result of the successful performance of this process, ONF elements are developed and implemented, and training is provided to relevant actors for the use of implemented ONF elements.

5.4.5.3 Realization activities

Table 7 — RACI chart for realization of process "Implementing the ONF"

Realization activities	ONF Committee	ONF element development team	Domain experts
a) Analyse the impact and complexity of developing and implementing the ONF elements designed within the scope of the current ONF management process iteration.	A/R		C
b) For each designed ONF element: 1) assign a development team;	A/R		
2 communicate management objectives and direction to thedevelopment team;	A/R		
3) provide adequate resources to the development team;	A/R	C	
4) develop and implement the ONF element;	A	R	C
5) determine training to use the ONF element by its different actors; and		A/R	C
6) provide adequate training to actors.	A/R	C	C

5.4.5.4 Verification activities

Table 8 — RACI chart for verification of process "Implementing the ONF"

Verification activities	ONF Committee	Auditors	Domain experts
1) Verify that designed ONF elements are developed and implemented according to the outcomes of the "Designing the ONF" process.	A	R	C

Table 8 *(continued)*

Verification activities	ONF Committee	Auditors	Domain experts
2) Verify that training identified by the ONF element development team is provided to relevant actors.	A	R	C

5.4.5.5 Guidance

The following should be used as prerequisite inputs for this process:

a) ONF implementation strategy for the current iteration of the ONF management process; and

b) design of ONF elements for current iteration.

Where an organization chooses to outsource or acquire any ONF elements that affect conformity to the ONF requirements, it should be ensured that the ONF committee management requirements are communicated to and implemented by those entities to which elements have been outsourced or from which they are acquired.

When assigning a development team for the implementation of an ONF element, the ONF committee should make available to the team the required resources and expertise, notably in the form of domain experts for the particular domain for which the ONF element applies.

EXAMPLE Legal experts, forensic experts, technology experts, cryptography experts, privacy experts.

When verifying that designed ONF elements are developed and implemented, auditors may consider criteria such as:

a) management of ONF projects and application security investments;

b) establishment of communication and reporting mechanisms of the ONF;

c) use of interfaces in application security projects for accessing the ONF elements;

d) communication of the importance of effective application security management, conforming to the organization's information security management system;

e) documentation and communication of information as defined in the ISO/IEC 27001:2013 International Standard;

f) implementation of ONF elements for all critical applications, depending on the ONF implementation strategy; and

g) accountability of everyone involved with the implementation and utilization of the ONF.

In addition, for each designed ONF element auditors may consider criteria such as:

a) identification of an owner;

b) management objectives and direction;

c) competence of persons doing work;

d) training to use the ONF element by its different actors; and

e) implementation and management of ONF element.

Specific guidance for the implementation of some ONF elements is found in 5.5.