INTERNATIONAL
STANDARD

ISO/IEC 27036-3

First edition
2013-11-15

Information technology — Security techniques — Information security for supplier relationships —

Part 3: Guidelines for information and communication technology supply chain security

Technologies de l'information — Techniques de sécurité — Sécurité d'information pour la relation avec le fournisseur —

Partie 3: Lignes directrices pour la sécurité de la chaîne de fourniture des technologies de la communication et de l'information

Reference number
ISO/IEC 27036-3:2013(E)

COPYRIGHT PROTECTED DOCUMENT

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

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 27036-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 27036 consists of the following parts, under the general title *Information technology — Security techniques — Information security for supplier relationships*:

— *Part 1: Overview and concepts*

— *Part 2: Requirements*

— *Part 3: Guidelines for information and communication technology supply chain security*

The following part is under preparation:

— *Part 4: Guidelines for security of cloud services.*

Introduction

Information and Communication Technology (ICT) products and services are developed, integrated, and delivered globally through deep and physically dispersed supply chains. ICT products are assembled from many components provided by many suppliers. ICT services throughout the entire supplier relationship are also delivered through multiple tiers of outsourcing and supply chaining. Acquirers do not have visibility into the practices of hardware, software, and service providers beyond first or possibly second link of the supply chain. With the substantial increase in the number of organizations and people who "touch" an ICT product or service, the visibility into the practices by which these products and services are put together has decreased dramatically. This lack of visibility, transparency, and traceability into the ICT supply chain poses risks to acquiring organizations.

This standard provides guidance to ICT product and service acquirers and suppliers to reduce or manage information security risk. This standard identifies the business case for ICT supply chain security, specific risks and relationship types as well as how to develop an organizational capability to manage information security aspects and incorporate a lifecycle approach to manage risks supported by specific controls and practices. Its application is expected to result in:

— Increased ICT supply chain visibility and traceability to enhance information security capability;

— Increased understanding by the acquirers of where their products or services are coming from, and of the practices used to develop, integrate, or operate these products or services, to enhance the implementation of information security requirements;

— In case of an information security compromise, the availability of information about what may have been compromised and who the involved actors may be.

This international standard is intended to be used by all types of organizations that acquire or supply ICT products and services in the ICT supply chain. The guidance is primarily focused on the initial link of the first acquirer and supplier, but the principle steps should be applied throughout the chain, starting when the first supplier changes its role to being an acquirer and so on. This change of roles and applying the same steps for each new acquirer-supplier link in the chain is the essential intention of the standard. By following this international standard, information security implications can be communicated among organizations in the chain. This helps identifying information security risks and their causes and may enhance the transparency throughout the chain. Information security concerns related to supplier relationships cover a broad range of scenarios. Organizations desiring to improve trust within their ICT supply chain should define their trust boundaries, evaluate the risk associated with their supply chain activities, and then define and implement appropriate risk identification and mitigation techniques to reduce the risk of vulnerabilities being introduced through their ICT supply chain.

ISO/IEC 27001 and ISO/IEC 27002 framework and controls provide a useful starting point for identifying appropriate requirements for acquirers and suppliers. ISO/IEC 27036 provides further detail regarding specific requirements to be used in establishing and monitoring supplier relationships.

Information technology — Security techniques — Information security for supplier relationships —

Part 3: Guidelines for information and communication technology supply chain security

1 Scope

This part of ISO/IEC 27036 provides product and service acquirers and suppliers in ICT supply chain with guidance on:

a) gaining visibility into and managing the information security risks caused by physically dispersed and multi-layered ICT supply chains;

b) responding to risks stemming from the global ICT supply chain to ICT products and services that can have an information security impact on the organizations using these products and services. These risks can be related to organizational as well as technical aspects (e.g. insertion of malicious code or presence of the counterfeit information technology (IT) products);

c) integrating information security processes and practices into the system and software lifecycle processes, described in ISO/IEC 15288 and ISO/IEC 12207, while supporting information security controls, described in ISO/IEC 27002.

This part of ISO/IEC 27036 does not include business continuity management/resiliency issues involved with the ICT supply chain. ISO/IEC 27031 addresses business continuity.

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 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements*