DRAFT INTERNATIONAL STANDARD ISO/IEC DIS 27036-1

ISO/IEC JTC **1** Secretariat: **ANSI**

Voting begins on
2013-01-17

Voting terminates on
2013-04-17

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОММИСИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Part 1: Overview and concepts

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

Partie 1: Aperçu général et concepts

ICS 35.040

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Pour accélérer la distribution, le présent document est distribué tel qu'il est parvenu du secrétariat du comité. Le travail de rédaction et de composition de texte sera effectué au Secrétariat central de l'ISO au stade de publication.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Copyright notice

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 27036-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *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 (ICT) supply chain security*

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

Introduction

Most (if not all) organizations around the world, whatever their size or domains of activities, have relationships with suppliers of different kinds that deliver products or services.

Such suppliers may have either a direct or indirect access to the information and information systems of the acquirer, or will provide elements (software, hardware, processes or human resources) that will be involved in information processing. Acquirers may also have physical and/or logical access to the information of the supplier when they control or monitor production and delivery processes of the supplier.

Thus, acquirers and suppliers can cause information security risks to each other. These risks need to be assessed and treated by both acquirer and supplier organizations through appropriate management of information security and the implementation of relevant controls. In many instances, organizations have adopted the International Standards of ISO/IEC 27001 and/or ISO/IEC 27002 for the management of their information security. Such International Standards should also be adopted in managing supplier relationships in order to effectively control the information security risks inherent in those relationships.

This International Standard provides further detailed implementation guidance on the controls dealing with supplier relationships that are described as general recommendations in ISO/IEC 27002.

Supplier relationships in the context of this International Standard include any supplier relationship that can have information security implications, e.g., janitorial services, consulting services, R&D partnerships, outsourced applications (ASPs) or cloud computing services (such as Software, Platform or Infrastructure as a Service).

This International Standard describes the information security issues from both the acquirer's and supplier's perspectives. Both the supplier and acquirer are expected to implement a number of fundamental processes (e.g. governance, business management, operational and human resources management) that support the accomplishment of business objectives and the achievement of objectives in the supplier / acquirer relationship to adequately address information security risks in accordance with the requirements and guidelines of this International Standard.

Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts

1 Scope

This international standard is an introductory part of the multipart standard, ISO/IEC 27036, Information Security for Supplier Relationships. This standard, which is Part 1 of the multipart standard, provides an overview of the guidance intended to assist organizations in securing their information and information systems within the context of supplier relationships. It also introduces concepts that will be described in detail in the other parts of the ISO/IEC 27036. This standard addresses perspectives of both acquirers and suppliers.

2 Normative references

The following referenced documents are indispensable for the application of this document. 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 27001, *Information technology – Security techniques – Information security management systems — Requirements*

ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls*

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1
acquirer
organization or an individual that procures a product or service from another party [adopted from ISO/IEC 15288]

NOTE 1 Stakeholder is an organization or an individual when used in ISO/IEC 27036.

NOTE 2 Procurement may or may not involve the exchange of monetary funds.

3.2
acquisition
the process for obtaining a product or service [adopted from ISO/IEC 15288]

3.3
agreement
mutual acknowledgement of terms and conditions under which a working relationship is conducted [ISO/IEC 15288]

3.4
lifecycle
evolution of a system, product, service, project or other human-made entity from conception through retirement [ISO/IEC 15288]

3.5
downstream
refers to the handling, processes and movements of products and services that occur after an entity in the supply chain takes custody of the products and responsibility for services [adopted from ISO 28001]

3.6
outsourcing
acquisition of services (with or without products) in support of a business function for performing activities using supplier's resources rather than the acquirer's

3.7
process
set of interrelated or interacting activities which transforms inputs into outputs [ISO 9000:2005]

3.8
supplier
organization or an individual that enters into agreement with another party for the supply of a product or service [ISO/IEC 15288]

NOTE Types of suppliers include those organizations that permit agreement negotiation with an acquirer and those that do not permit negotiation with agreements, e.g., end-user license agreements, terms of use, or open source products copyright or intellectual property releases.

3.9
supplier relationship
agreement or agreements between acquirers and suppliers to conduct business, deliver products or services and realize business benefit

3.10
supply chain
set of organizations with linked set of resources and processes, each of which acts as an acquirer, supplier or both to form successive supplier relationships established upon placement of a purchase order, agreement or other formal sourcing agreement [adopted from ISO 28001]

NOTE 1 A supply chain can include vendors, manufacturing facilities, logistics providers, distribution centers, distributors, wholesalers and other organizations involved in the manufacturing, processing, design and development, handling and delivery of the products, or service providers involved in the operation, management and delivery of the services.

NOTE 2 The supply chain view is relative to the position of the acquirer.

3.11
system
combination of interacting elements organized to achieve one or more stated purposes

NOTE 1 A system can be considered as a product or as the services it provides.

NOTE 2 In practice, the interpretation of its meaning is frequently clarified by the use of an associative noun, e.g., aircraft system. Alternatively, the word "system" may be substituted simply by a context-dependent synonym, e.g., aircraft, though this can then obscure a system principles perspective. [ISO/IEC 15288]

3.12
trust
relationship between two entities and/or elements, consisting of a set of activities and a security policy in which element ‘x’ trusts element ‘y’ if and only if ‘x’ has confidence that ‘y’ will behave in a well-defined way (with respect to the activities) that does not violate the given security policy [adopted from ISO/IEC 10181-1, 3.3.28, ISO/IEC 13888-1]

3.13
upstream
refers to the handling, processes and movements of products and services that occur before an entity in the supply chain takes custody of the products and responsibility for ICT services [adopted from ISO 28001]

3.14
visibility
property of a system or process that enables system elements and processes to be documented and available for monitoring and inspection

4 Symbols and abbreviated terms

The following symbols (and abbreviated terms) are used in this standard:

ICT	Information and Communication Technologies
RFP	Request for Proposal
ASP	Application Service Provider
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
BPaaS	Business Process as a Service
BCP	Business Continuity Plan(ning)
R&D	Research & Development
NDA	Non-Disclosure Agreement

5 Problem definition and key concepts

5.1 Motives for establishing supplier relationships

Organizations often choose to form and/or retain supplier relationships for a variety of business reasons to take advantage of the benefits they can provide. The following summarizes potential motivations for establishing a supplier relationship:

a) Focusing internal resources on core business functions which can result in a cost reduction and improved return on investment (e.g., outsourcing IT services).

b) Acquiring a short-term or highly specialized competency that an organization does not already possess (e.g., hiring an advertising firm).