FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/IEC FDIS 27036-1

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2021-06-14

Voting terminates on:
2021-08-09

Cybersecurity — Supplier relationships —

Part 1: Overview and concepts

Cybersécurité — Relations avec le fournisseur —

Partie 1: Aperçu général et concepts

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.

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.

Reference number
ISO/IEC FDIS 27036-1:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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 27036-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity, and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 27036-1:2014), of which this constitutes a minor revision.

The main changes compared to the previous edition are as follows:

- change of title;
- revision of Clause 2;
- alignment with drafting rules;
- ISO/IEC 27036 (all parts) added in Bibliography.

A list of all parts in the ISO/IEC 27036 series can be found on the ISO website

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 can 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 can also have physical and 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 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 document 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 document include any supplier relationship that can have information security implications, e.g. information technology, healthcare services, janitorial services, consulting services, R&D partnerships, outsourced applications (ASPs), or cloud computing services (such as software, platform, or infrastructure as a service).

Both the supplier and acquirer should take equal responsibility to achieve the objectives in the supplier-acquirer relationship and adequately address information security risks that can occur. It is expected that they implement the requirements and guidelines of this document. Furthermore, fundamental processes should be implemented to support the supplier-acquirer relationship (e.g. governance, business management, and operational and human resources management). These processes will provide support in terms of information security as well as the accomplishment of business objectives.

Cybersecurity — Supplier relationships —

Part 1:
Overview and concepts

1 Scope

This document is an introductory part of ISO/IEC 27036. It 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 are described in detail in the other parts of ISO/IEC 27036. This document addresses perspectives of both acquirers and suppliers.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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*

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
acquirer
stakeholder that procures a product or service from another party

Note 1 to entry: Procurement may or may not involve the exchange of monetary funds.

Note 2 to entry: A stakeholder is an individual or organization with interest in an asset in the supplier relationship.

[SOURCE: ISO/IEC 15288:2008, 4.1, modified — Original Note was removed, the word "acquires" was removed from the definition, and Note 1 and Note 2 to entry were added.]

3.2
acquisition
process for obtaining a product or service

[SOURCE: ISO/IEC 15288:2008, 4.2, modified — The word "system" was removed.]

3.3
agreement
mutual acknowledgement of terms and conditions under which a working relationship is conducted

[SOURCE: ISO/IEC 15288:2008, 4.4]

3.4
life cycle
evolution of a system, product, service, project, or other human-made entity from conception through retirement

[SOURCE: ISO/IEC 15288:2008, 4.11]

3.5
downstream
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

[SOURCE: ISO 28001:2007, 3.10, modified — The word "goods" was replaced by "products and services", and the definition was changed to better reflect this change in focus.]

3.6
outsourcing
acquisition (3.2) of services (with or without products) in support of a business function for performing activities using supplier's resources rather than the *acquirer's* (3.1)

3.7
process
set of interrelated or interacting activities which transforms inputs into outputs

[SOURCE: ISO 9000:2005, 3.4.1, modified — Notes were removed.]

Note 1 to entry: For the purpose of this document, an asset is information associated with products and services.

3.8
supplier
organization or an individual that enters into *agreement* (3.3) with the *acquirer* (3.1) for the supply of a product or service

Note 1 to entry: Other terms commonly used for supplier are contractor, producer, seller, or vendor.

Note 2 to entry: The acquirer and the supplier can be part of the same organization.

Note 3 to entry: 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.

[SOURCE: ISO/IEC 15288:2008, 4.30, modified — Note 3 to entry was added.]

3.9
supplier relationship
agreement or *agreements* (3.3) between *acquirers* (3.1) and *suppliers* (3.8) 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* (3.7), each of which acts as an *acquirer* (3.1), *supplier* (3.8), or both to form successive *supplier* (3.8) relationships established upon placement of a purchase order, *agreement* (3.3), or other formal sourcing *agreement* (3.3)

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

Note 2 to entry: The supply chain view is relative to the position of the acquirer.

[SOURCE: ISO 28001:2007, 3.24, modified — The definition was changed to focus more on the organization and relationships; Note 2 to entry was added.]

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

Note 1 to entry: A system can be considered as a product or as the services it provides.

Note 2 to entry: 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” can be substituted simply by a context-dependent synonym, e.g. aircraft, though this can then obscure a system principles perspective.

[SOURCE: ISO/IEC 15288:2008, 4.31]

3.12
trust
relationship between two entities 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

[SOURCE: ISO/IEC 13888-1:2009, 3.59, modified — The note was removed.]

3.13
upstream
handling *processes* (3.7) and movements of products and services that occur before an entity in the *supply chain* (3.10) takes custody of the products and responsibility for information and communication technology (ICT) services

[SOURCE: ISO 28001:2007, 3.27, modified — The word “goods” was replaced by “products and services”, and the definition was changed to better reflect this change in focus.]

3.14
visibility
property of a *system* (3.11) or *process* (3.7) that enables system elements and *processes* (3.7) to be documented and available for monitoring and inspection

4 Symbols and abbreviated terms

The following symbols and abbreviated terms are used in this document:

API	Application Programming Interface
ASP	Application Service Provider
BCP	Business Continuity Plan(ning)
BPaaS	Business Process as a Service
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
PaaS	Platform as a Service
R&D	Research & Development
SaaS	Software as a Service

5 Problem definition and key concepts

5.1 Motives for establishing supplier relationships

Organizations often choose to form and 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 ICT services).

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

c) Acquiring a utility or basic service that is common or readily available (e.g. electric power and telecommunications) that cannot efficiently be provided by the organization.

d) Enabling business operations in a different geographical location.

e) Acquiring new or replacement ICT equipment or services (e.g. laptops, printers, servers, routers, software applications, storage capacity, network connectivity, ICT managing services etc.) that enable workforce productivity and other business computing needs.

Suppliers can provide a multitude of products or services, including IT outsourcing, professional services, basic utilities (equipment maintenance service, security guards service, cleaning and delivering services etc.), cloud computing services, information and communication technology (ICT), knowledge management, R&D, manufacturing, logistics, health care services, Internet services, and many others.

5.2 Types of supplier relationships

5.2.1 Supplier relationships for products

When an acquirer enters a supplier relationship for products, it typically purchases products with agreed specifications for a predetermined period for manufacturing the acquirer's products.

The supplier can have access to the acquirer's information when delivering and supporting the product which can result in information security risks to the acquirer's information. Failures to fulfil requirements, software vulnerabilities and malfunctions of products and inadvertent release of sensitive information can also cause information security risks to the acquirer.

To manage these information security risks, the acquirer may wish to control supplier's access to the acquirer's information. The acquirer may also wish to control elements of the supplier's production processes to maintain quality of the products and to reduce information security risks derived from vulnerabilities, malfunctions or other failures to fulfil requirements. This, in turn, can pose information security risks to the supplier because the acquirer can have access to the supplier's information when controlling elements of the supplier's processes.

Further, the acquirer may wish to have assurances regarding the specification of products, by monitoring or auditing of the production processes or requiring the supplier to obtain an independent certification to demonstrate existence of good practices and required processes. These assurance requirements need be agreed between the acquirer and supplier.

5.2.2 Supplier relationships for services

When an acquirer procures services, the supplier generally has access to the acquirer's information. This causes potential information security risks to the acquirer. In the case of business process outsourcing, e.g. that of marketing, call centre operation or the organization's ICT infrastructure, a significant portion of the acquirer's critical business information can be put under management of the supplier. Other kinds of services have generally limited access to the acquirer's information, such as food services and janitorial services.

Delivery of some services requires the acquirer's information to be located within acquirer's premises and to be accessed onsite or remotely by the supplier. In other cases, acquirer's information is located at the supplier's site. These specific conditions can impact selection of controls applicable to the acquirer or supplier. See Table 2 for examples of how location can have an impact on supplier's accesses to the acquirer's information.

When acquiring services, acquirers should establish rules for how to control supplier access to acquirer's information. The acquirer may also wish to control the quality of the service to reduce information security risks, including the ability to meet availability requirements over time. A service level agreement is a general way of agreeing on the quality of service. For the supplier, a service level agreement can be a tool for communicating how the supplier will satisfy quality expectations to the acquirer.

The acquirer may wish to have assurance regarding the quality of the service by monitoring or auditing the supplier service processes or requiring the supplier to obtain a certification to demonstrate existence of good practices or required processes. These assurance requirements need also be agreed between the parties.

5.2.3 ICT supply chain

ICT supply chain is a set of organizations with a linked set of resources and processes that form successive supplier relationships of ICT products and services. An ICT product or service can be composed of components, resources and processes produced by a supplier which can have been produced, in whole or in part, by another supplier. As such, an ICT service, in its entirety, may have been sourced by multiple suppliers. As depicted in Figure 1, an organization in an ICT supply chain is an acquirer in relation to the upstream organization, and a supplier in relation with downstream organization. The adjacent downstream organization is often called a customer from the perspective of the organization that provides products or services to it. The customer at the end of the ICT supply chain is referred to as an end customer, or consumer. Generally, the end customer has limited control over their direct supplier's information security requirements and no control over information security requirements beyond the direct supplier.

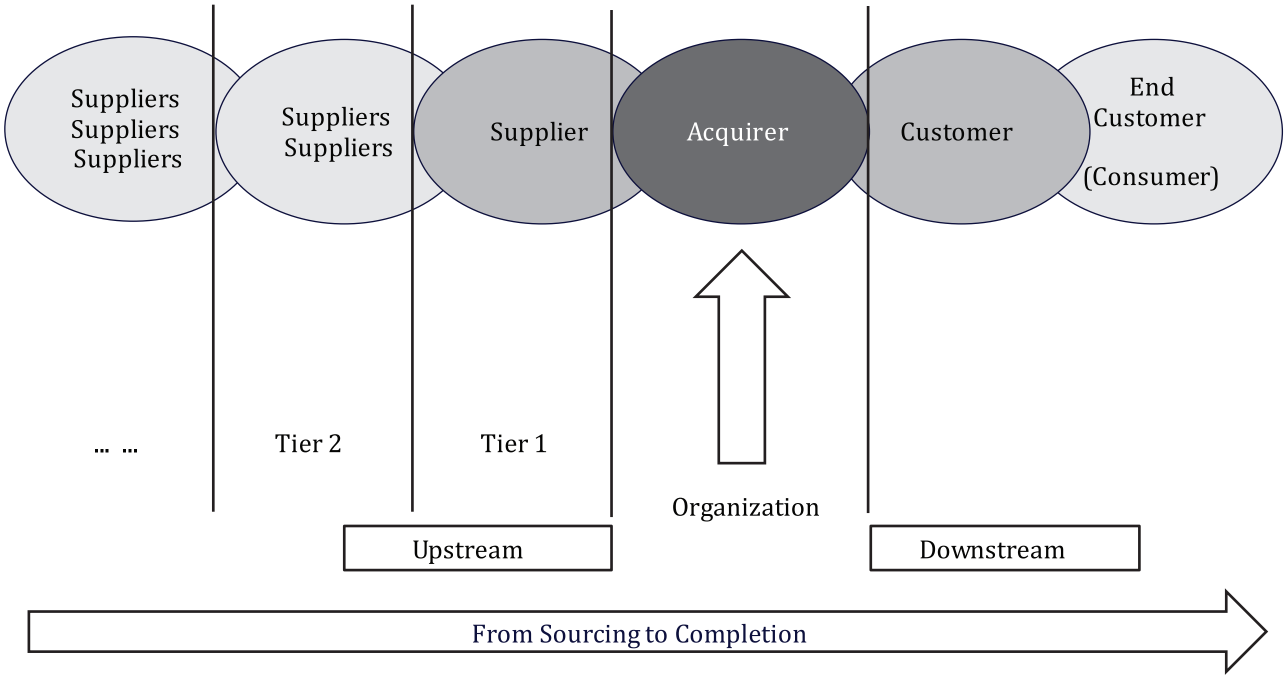

Figure 1 — Supply chain relationships