

ISO/IEC JTC 1/SC 27 N11993

Date: 2012-11-10

ISO/IEC DIS 27036-1

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: ANSI

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

Élément introductif — Élément central — Partie 1: Titre de la partie

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

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.

Document type: International Standard

Document subtype:

Document stage: (40) Enquiry

Document language: E

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

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

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
5 Problem definition and key concepts.....	3
5.1 Motives for establishing supplier relationships.....	3
5.2 Types of supplier relationships	4
5.2.1 Supplier relationships for products	4
5.2.2 ICT supply chain.....	5
5.2.3 Cloud computing	5
5.3 Information security risks in supplier relationships and associated threats	6
5.4 Managing information security risks in supplier relationships.....	8
5.5 ICT supply chain considerations	9
6 Overall ISO/IEC 27036 structure and overview	10
6.1 Purpose and Structure.....	10
6.2 Overview of Part 1: Overview and concepts	10
6.3 Overview of Part 2: Requirements.....	10
6.4 Overview of Part 3: Guidelines for Information and Communication Technology (ICT) supply chain security.....	10
6.5 Overview of Part 4: Guidelines for security of cloud services	11
Bibliography.....	12

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).

- c) Acquiring a utility or basic service that is common or readily available (e.g., electric power and telecommunications).
- d) Enabling business operations in a different geographical location.
- e) Acquiring new or replacement ICT equipment or services (e.g. laptops, printers, servers, routers).

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 Telecommunication 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 may 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. These risks can include failures to fulfil requirements, software vulnerabilities, malfunctions, inadvertent release of sensitive information, or other causes.

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 may 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 parties.

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 may require 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 may be located at the supplier's site. These specific conditions can impact selection of controls applicable to the acquirer or supplier. See Table 1 for examples of how location may have an impact supplier accesses to acquirer 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 ability to meet availability requirements over time. Service level agreement is a general way of agreeing on the quality of service. For the supplier, 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 certification to demonstrate existence of good practices or required processes. These assurance requirements need also be agreed between the parties.

5.2.2 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 may 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, and in general, does not have control over or dictate the supplier's information security requirements.

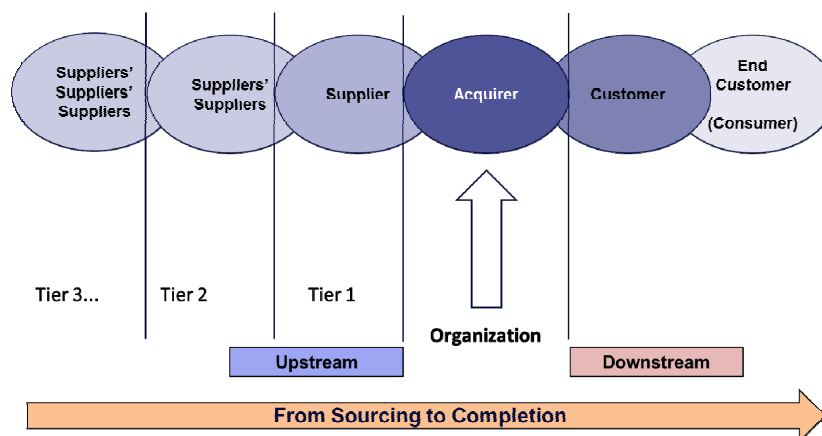


Figure 1 — Supply Chain Relationships

ICT supply chain inherits each of information security risks of the supplier relationships for products and services (see 5.2.1 and 5.2.2). Additionally, ICT supply chain poses specific information security risks to the acquirers and suppliers participating in the ICT supply chain. Lack of direct management of suppliers or other suppliers in the supply chain can introduce additional information security risks to the acquirer and intermediate suppliers. The acquirer's enforcement of the source suppliers' controls can be more difficult in an ICT supply chain environment. This requires a management and communication between acquirers and suppliers within the ICT supply chain context to appropriately manage the information security risks.

5.2.3 Cloud computing

Cloud computing is a form of a supplier relationship, in that, a cloud computing service, in its entirety, may be sourced from multiple suppliers. The purpose of cloud computing is to enable utility based or per-use compute and storage services and capabilities based on business requirements for scalability, availability and elasticity service expectations. In a cloud computing service, a supplier is commonly referred to as the cloud service provider and the acquirer referred to as the cloud service customer. In some cases, the cloud service provider delegates the management or control over components, resources and processes to the cloud service customer in an environment potentially shared by another cloud service customer, commonly referred to as a multi-tenant cloud environment. Similarly to general ICT supply chain, it is therefore incumbent upon both the supplier and acquirer to manage information security risks introduced as a result of a shared compute and storage model in the ICT supply chain involving any of the cloud service delivery model, i.e., IaaS, PaaS and SaaS.

5.3 Information security risks in supplier relationships and associated threats

Information security risks in supplier relationships are a matter of concern, not only for the acquirer and supplier, also for customers and other interested parties. It is a question of trust in business activities in society. Both the supplier and acquirer should consider the inherent and residual information security risks associated with establishing a supplier relationship.

Acquirer and supplier are equally responsible for making their agreement trustworthy and for managing their information security risks which includes establishing delineated roles and responsibility for information security and implementation of controls.

While each supplier relationship of an organization is established for a specific purpose, the number of such relationships tends to grow over time and are not always well managed or controlled by acquirers. Specifically, large organizations tend to have a significantly high number of supplier relationships that were established by different internal entities using a variety of processes and arrangements. Within many of these supplier relationships also exist multiple layers of the supply chain. This multiplicity can result in making it increasingly more difficult for an organization to ensure that the information security risks created by those supplier relationships have been appropriately addressed.

The supply and support of a product or service may be dependent upon either the acquirer or supplier transfer of information and/or information systems to the other party, resulting in the lack of clarity and impacts of the effectiveness of either organizations' established information security management and controls implementation. When an organization establishes a supplier relationship, the acquirer and supplier should agree on a mutually acceptable set of controls and responsibility for implementation; otherwise, they may experience the following:

- a) Gaps in controls due to different information security requirements possibly related to different governance, risk tolerance and compliance practices or different cultural or organizational attitudes between the acquirer and supplier.
- b) Control dependencies due to reliance upon external business capabilities designed to ensure the compliance with acquirer's own information security requirements.
- c) Conflicting or different controls that interfere or weaken the acquirer's information security.

These and other concerns should be considered throughout the lifecycle of a supplier relationship – from relationship planning to termination exit to address the following information security risks:

- a) Lack or weakness of governance:
 - 1) Acquirers lose control over how their information is stored, processed, transmitted, created, modified and destroyed.
 - 2) Suppliers, unless specifically included in the agreement, may outsource a subset of resources and processes to another supplier, thus reducing or limiting the acquirer's control, and potentially exposing the acquirer to further risk and / or exposure.
- b) Miscommunication and misunderstanding:
 - 1) Controls put in place by the supplier do not address the risks identified by the acquirer, leaving the acquirer vulnerable to risks presumed to be addressed and managed by the supplier.
 - 2) Confidentiality, integrity and availability requirements of the acquirer may not be communicated properly to the supplier and hence not correctly met.
 - 3) Requirements concerning availability / BCP for information or information systems that support the on-time and on-delivery of products or services by the supplier to the acquirer cannot be specified, leading to interruptions in supply.

- 4) Suppliers fail to allocate sufficient resources, including skilled staff, to protect the acquirer's information.
- c) Geographical, social and cultural differences:
- 1) The acquirer is inadvertently in breach of legislation or regulation, leading to reputational damage and financial penalties.
 - 2) Reference to a law or a standard as a requirement in an agreement allows for misinterpretation by acquirer and supplier and subsequent dispute.
 - 3) Acquirer may delegate responsibility for information security and implementation of controls in an agreement while still accountable, thus putting the acquirer's goodwill at risk in event of a security breach on the supplier side.
 - 4) The service can be provided in a location either unknown or not permitted by the acquirer, leading to breaches of legislation or regulation.

Specific information security risks to acquirer's and/or supplier's information and information systems can be directly correlated with inadequate control awareness, ownership and accountability. Examples of such issues may be applicable to the supply of both products and services. Issues in supplier relationships for products are described in Table 1. Whereas, with services, information security risks associated with access to information or information systems may be introduced and managed in the supplier relationship. Table 2 provides examples of services related supplier access to acquirer information and information systems.

Table 1 — Issues in supplier relationships for products

No.	Type	Description
1	Information security feature	In the case where supplied products have vulnerability, the acquirer's derived products, services or processes will be vulnerable.
2	Quality	Poor quality of supplied products can cause information security weakness of the acquirer's derived products, services and processes.
3	Intellectual property rights	Unidentified intellectual property rights can cause later dispute in relation with the acquirer's derived products or services.
4	Authenticity	In the case where fake or fraudulent products were supplied, the acquirer's expectation for information security feature, quality and identification of intellectual property rights are threatened, and likely to have information security weakness and to lose its confidence in business relationships.
5	Assurance	Without appropriate information security features, product quality, and identification of intellectual property rights and authenticity, the acquirer may lack confidence in reliance upon the supplier's products.

Table 2 — Access examples of supplier relationships for services

No.	Type	Description	Example Use Case(s)
1	Physical access onsite	Supplier has physical access to the information processing facilities of the acquirer but does not have logical access.	Security guard service, delivery services, a cleaning service or an equipment maintenance service
2	Access to information and information systems onsite	Supplier personnel are onsite and have logical access to information and information systems of the acquirer, through the use of acquirer's equipment.	Outsourced expertise working onsite and integrated in acquirer's teams
3	Remote access to in-house	Supplier has remote access to information and information systems of the acquirer	Remote development and maintenance activities, remote

No.	Type	Description	Example Use Case(s)
	information and information systems		information system and equipment management, logistics, call centre operation, automated facilities management systems
4	Processing of information offsite	Information under the responsibility of the acquirer is processed by the supplier offsite, using applications and systems under the control and the management of the supplier.	Consulting (market research, sales promotion, technical studies, etc.), information processing, R&D, manufacturing, storage and archival, application service (ASP), Business Process as a Service (BPaaS) such as travel or financial services, Infrastructure as a Service (IaaS) or Software as a Service (SaaS) providers
5	Applications offsite	Applications controlled and managed by the acquirer are running on equipment and systems under the control and management of the supplier.	Platform as a Service (PaaS) if supplier provides development platform or IaaS providers if supplier provides network, compute and storage services
6	Equipment offsite	Equipment dedicated to the acquirer and owned by the acquirer are hosted offsite, on the supplier site.	Offsite hosting of information systems housing or Infrastructure as a Service (IaaS) providers
7	Storage of information offsite	An acquirer outsources the storage of information to a supplier for offsite retention and/or archival services.	Organization maintains backup copies of information on tape, cartridges, or SaaS based storage provider.
8	Source code escrow	Services involving supplier artifacts used by the acquirer are held in escrow by a trusted third party and are made available to the acquirer under defined circumstances.	Source code held by an independent third party to maintain usefulness of software by the acquirer in the case that the supplier of the software goes out of business.

5.4 Managing information security risks in supplier relationships

In supplier relationship, acquirer's or supplier's access to or handling of the other organization's information can introduce information security risks for both the acquirer and supplier. The acquirer and supplier evaluate risks, and select, implement and maintain controls to mitigate them. In the context of supplier relationships, the controls consist of:

- Those that directly address information security risks associated with access to or handling of the each organization's information;
- Those of the supplier addressing quality of products that affects the acquirer's and its customer's information security risks; and
- Those enforcing a) or b) above on the other organization, e.g., by managing and reporting requirements, monitoring, auditing and certification.

The agreement between the acquirer and supplier binds both organizations in implementing and maintaining those controls. The agreement can also specify requirements in place of some controls a) or b) leaving allowance to the other organization in selecting controls.

Regardless of the nature of the provided product or service, visibility of information security should be considered as an important part of establishing supplier relationships to ensure information security risks to the acquirer's information and information systems are managed. In order to identify and manage these information security risks, the acquirer should obtain assurance from the supplier that the it has implemented

adequate information security management and controls. The acquirer needs to negotiate what specific information security management and controls that should be implemented by the supplier. In the case where these are not negotiable, the acquirer should select a supplier's product or service based on criteria which include requirements for information security management and controls to avoid or mitigate risks to an acceptable level.

5.5 ICT supply chain considerations

The acquirer's acceptance of a supplier's production, delivery and operation of products and services should be based on criteria which ensures levels of information security which the acquirer wishes to have within its own organization. These could include any of the following:

- Management of political, legal and information security risks relating to the local environment which impact the acquirer's information security, including continuity of information, information systems and services
- Management of confidentiality of physical and electronic documents and other information relating to the supplied products and services
- Management of integrity of materials and elements to ensure proper handling, i.e., unique markings and protective labelling
- Management of physical security of facilities from which products and services are delivered
- Management of information security relating to any aspect of the suppliers business and suppliers business with other clients
- Management of information security as it relates to the supplier agreement throughout the supply chain

To appropriately manage information security in supplier relationships throughout the supply chain, acquirers should adopt a framework with the following set of standardized organization-wide processes for the acquisition of products and services:

- a) Establish security and compliance requirements for the secure exchange or sharing of information and information systems.
- b) Prior to acquisition, assess and monitor the information security risks associated with the supplier relationship.
- c) Establish a process for negotiation or re-negotiation of the supply chain agreement or agreements incorporating the security and compliance requirements, inclusive of conditions for right to audit and restricting upstream suppliers throughout the multiple layers of the supply chain.
- d) Continuously monitor and report on the performance of suppliers within the supply chain adhering to security and compliance requirements, especially as a result of a supplier relationship change.

This framework should be flexible to allow for a range of supply chain agreements that may be tailored based on the nature of the product or service being acquired and the risk that it is expected to create.

6 Overall ISO/IEC 27036 structure and overview

6.1 Purpose and Structure

ISO/IEC 27036 is a multi-part standard that provides requirements and guidance for suppliers and acquirers on how to secure information in supplier relationships. Figure 2 provides notional architecture of this multipart standard.

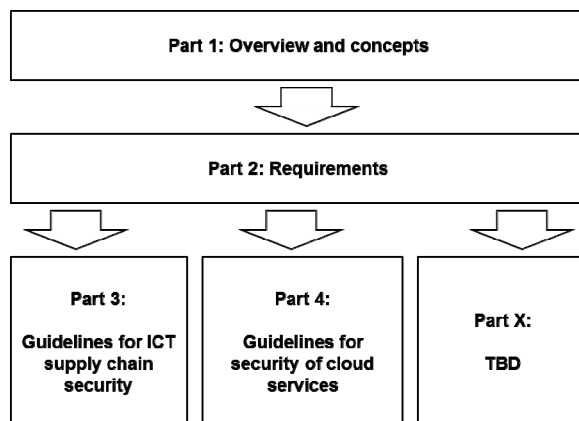


Figure 2 — ISO/IEC 27036 Architecture

Parts 3-5 address specific aspects of information security supplier relationships including challenges associated with those related to ICT products and services (Part 3), outsourcing of services (Part 4), and acquiring cloud computing services (Part 5).

6.2 Overview of Part 1: Overview and concepts

Part 1 (this document) provides overview and concepts associated with information security in supplier relationships. Part 1 is an informative document.

6.3 Overview of Part 2: Requirements

Part 2 provides a high level framework for establishing information security requirements and expectations in supplier relationships. This framework includes governance, lifecycle processes, and relevant high-level requirements statements. Part 2 is a normative standard that acquirers can use as a source of agreement requirements to define, manage, and monitor supplier agreements. The requirements from this standard may also serve as additional certification criteria for the purpose of ISO/IEC 27001 certification or other certification schemas as deemed pertinent to the acquirer. For example, an acquirer may require that a supplier be certified in accordance with ISO/IEC 27001 and include additional requirements and applicable controls in accordance with ISO/IEC 27036 with respect to the products or services being offered. Acquirers may either use the entire standard or extract individual clauses for use as requirements statements.

6.4 Overview of Part 3: Guidelines for Information and Communication Technology (ICT) supply chain security

In supplier relationships, a product or service procured by the acquirer is not necessarily manufactured or operated solely by the supplier. For example, a product often contains parts that are made by other suppliers and provided to the supplier that is in direct relationship with the acquirer. Alternatively, an information processing service can be built on other information processing services as its underlying infrastructure. For instance, the supplier has an agreement with another supplier to maintain the hardware, to store backups on an external location or may even have the entire backup process outsourced. Thus, supply chains are formed by successive supplier relationships with inherent interdependencies.

In a supply chain, information security management and controls implemented by the supplier in direct relationship with the acquirer are not always sufficient to manage information security risks of a product or service. The acquirer's management of an indirect supplier's (supplier of the supplier) product or service can be essential for information security: this requires visibility into the supply chain.

Conversely, suppliers can also experience increased information security risks caused by the interconnectedness of acquirer and supplier systems that sometimes results from the ICT supply chain. For example, acquirer may require invasive audits of supplier systems that can result in acquirer access to supplier intellectual property.

ISO/IEC 27036 Part 3 provides guidelines to acquirers and suppliers for managing information security risks associated with the ICT products and services supply chain. It builds on the requirements in Part 2 and provides additional practices that augment high-level requirements from Part 2.

6.5 Overview of Part 4: Guidelines for security of cloud services

Organizations use cloud computing services to take advantage of the economies of scale provided by highly resilient and elastic compute and storage service capabilities. These capabilities are made available on a utility based or per-usage model. Cloud computing can be provided in a number of different cloud service delivery models, e.g., IaaS, PaaS and SaaS. However, this has introduced information security risks associated with greater complex interconnectedness of acquirer and supplier systems. Similar to ICT supply chain information security risks, there is potential for lack of clarity on roles and responsibilities for information security management and controls implementation.

For example, there may be the risk of legal, statutory or regulatory infringement of compliance obligations by either acquire or supplier if information within cloud computing service workloads traverses national boundaries or the ability of the cloud service customer to control how the cloud service is delivered. Additionally, multi-tenancy and the use of technologies, e.g., virtualization and application programming interfaces (APIs), may introduce new information security risks of cloud customer confidentiality as a consequence from inadequate access controls and lack of cloud service customer segregation.

ISO/IEC 27036 Part 5 provides guidelines for information security of cloud computing services throughout the supply chain from the perspective of both the acquirer and supplier of such services. Specifically, it involves managing the information security risks associated with cloud computing services throughout the lifecycle. It builds on the requirements in Part 2 and provides additional practices that can augment high-level requirements from Part 2 and guidance from Part 3.

Bibliography

- [1] ISO/IEC 15288, *Systems and software engineering – System life cycle processes*
- [2] ISO/IEC 12207, *Systems and software engineering – Software life cycle processes*
- [3] ISO/IEC 27014, *Information Technology – Security Techniques – Governance of Information Security*
- [4] ISO/IEC 27035, *Information technology -- Security techniques – Security incident management*
- [5] ISO/IEC 20000, *Information technology – Service management – Part 1: Service management system requirements*
- [6] ISO/IEC 27000, *Information technology – Security techniques – Information security management systems -- Overview and vocabulary*
- [7] ISO 28000, *Specification for security management systems for the supply chain*
- [8] ISO 28001, *Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance*
- [9] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*


**EXPLANATORY REPORT
RAPPORT EXPLICATIF**
ISO/IEC DIS 27036-1
ISO/IEC JTC 1/SC 27

 Secretariat **DIN**

This form should be sent to the ISO Central Secretariat, together with the English and French versions of the committee draft, by the secretariat of the technical committee or subcommittee concerned.

Ce formulaire doit être envoyé au Secrétariat central de l'ISO en même temps que les versions anglaise et française du projet de comité, par le secrétariat du comité technique ou du sous-comité concerné.

The accompanying document is submitted for circulation to member body vote as a DIS, following consensus obtained from the P-members of the committee.

Le document ci-joint est soumis, pour diffusion comme DIS, au vote comité membre, suite au consensus des membres (P) du comité obtenu.

 on **2012-10-26**
☒ at the meeting of **TC 1 / SC 27 / WG 4**
à la réunion du

 see resolution No. **35** in document **N11941**
voir résolution n° dans le

☐ by postal ballot initiated on
par un vote par correspondance démarré le

P-members in favour: Membres (P) approuvant le projet:	Number 17	Countries Czech Republic, China, Denmark, Ireland, Italy, Kenya, Korea, Republic of, Luxembourg, Mexico, Norway, Romania, Russian Federation, Slovenia, Sweden, Thailand, Ukraine, United States
P-members voting against: Membres (P) désapprouvant:	3	Japan*, Netherlands, United Kingdom*
P-members abstaining: Membres (P) s'abstenant:	16	Australia, Belgium**, Brazil, Canada**, Finland**, Germany**, India, Kazakhstan, Malaysia**, Morocco, New Zealand, Poland, South Africa**, Spain, Switzerland, Uruguay
P-members who did not vote: Membres (P) n'ayant pas voté:	11	Algeria, Austria, Côte d'Ivoire, Cyprus, Estonia, France, Mauritius, Singapore, Slovakia, Sri Lanka, United Arab Emirates

Remarks/Remarques

The 1st CD document was circulated as SC 27 N11012. The summary of voting is presented in SC 27 N11525. Additional National Body comments were circulated as SC 27 N11537 and N11655. The disposition of comments is shown in SC 27 N11992. The text for a 3-month DIS balloting is contained in N11995.

* Negative votes of National Bodies indicated have been satisfactorily resolved and changed to APPROVAL.

** National Bodies indicated changed their votes to APPROVAL.

I hereby confirm that this draft meets the requirements of part 2 of the ISO/IEC Directives
Je confirme que ce projet satisfait aux prescriptions de la partie 2 des Directives ISO/CEI

Date

 Name and signature of the secretary
Nom et signature du secrétaire

2012-11-14
Krystyna Passia

Result of voting

Ballot Information

Ballot reference	ISO/IEC CD 27036-1
Ballot type	CD
Ballot title	Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts
Opening date	2012-06-01
Closing date	2012-09-01
Note	1 st CD Registration and Consideration In accordance with resolution 4 (see SC 27 N11330) of the 24th SC 27 Plenary meeting held in Stockholm, Sweden (14th and 15th May 2012) the attached document has been registered with the ISO Central Secretariat (ITTf) as a 1st Committee Draft (CD) and is hereby circulated for a 1st CD letter ballot closing by 2012-09-01.

Member responses:

Votes cast (35)	Australia (SA) Belgium (NBN) Brazil (ABNT) Canada (SCC) China (SAC) Czech Republic (UNMZ) Denmark (DS) Finland (SFS) India (BIS) Ireland (NSAI) Italy (UNI) Japan (JISC) Kazakhstan (KAZMEMST) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Malaysia (DSM) Mexico (DGN) Morocco (IMANOR) Netherlands (NEN) New Zealand (SNZ)
------------------------	---

	Norway (SN) Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Slovenia (SIST) South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Thailand (TISI) Ukraine (DSSU) United Kingdom (BSI) United States (ANSI) Uruguay (UNIT)
Comments submitted (0)	
Votes not cast (12)	Algeria (IANOR) Austria (ASI) Côte d'Ivoire (CODINORM) Cyprus (CYS) Estonia (EVS) France (AFNOR) Germany (DIN) Mauritius (MSB) Singapore (SPRING SG) Slovakia (SUTN) Sri Lanka (SLSI) United Arab Emirates (ESMA)

Questions:	
Q.1	"Do you agree with approval of the CD text?"
Q.2	"If you approve the CD text with comments, would you please indicate which type ? (General, Technical or Editorial)"
Q.3	"If you disapprove the draft, would you please indicate if you accept to change your vote to Approval if the reasons and appropriate changes will be accepted?"

Votes by members	Q.1	Q.2	Q.3
Australia (SA)	Abstention	Ignore	Ignore
Belgium (NBN)	Abstention	Ignore	Ignore
Brazil (ABNT)	Abstention	Ignore	Ignore
Canada (SCC)	Abstention	Ignore	Ignore
China (SAC)	Approval with comments	All	Ignore
Czech Republic (UNMZ)	Approval as presented	Ignore	Ignore
Denmark (DS)	Approval as presented	Ignore	Ignore
Finland (SFS)	Abstention	Ignore	Ignore
India (BIS)	Abstention	Ignore	Ignore

Ireland (NSAI)	Approval as presented	Ignore	Ignore
Italy (UNI)	Approval as presented	Ignore	Ignore
Japan (JISC)	Disapproval of the draft	Ignore	No
Kazakhstan (KAZMEMST)	Abstention	Ignore	Ignore
Kenya (KEBS)	Approval as presented	Ignore	Ignore
Korea, Republic of (KATS)	Approval as presented	Ignore	Ignore
Luxembourg (ILNAS)	Approval as presented	Ignore	Ignore
Malaysia (DSM)	Abstention	Ignore	Ignore
Mexico (DGN)	Approval with comments	All	Ignore
Morocco (IMANOR)	Abstention	Ignore	Ignore
Netherlands (NEN)	Disapproval of the draft	General	No
New Zealand (SNZ)	Abstention	Ignore	Ignore
Norway (SN)	Approval as presented	Ignore	Ignore
Poland (PKN)	Abstention	Ignore	Ignore
Romania (ASRO)	Approval as presented	Ignore	Ignore
Russian Federation (GOST R)	Approval as presented	Ignore	Ignore
Slovenia (SIST)	Approval as presented	Ignore	Ignore
South Africa (SABS)	Abstention	Ignore	Ignore
Spain (AENOR)	Abstention	Ignore	Ignore
Sweden (SIS)	Approval as presented	Ignore	Ignore
Switzerland (SNV)	Abstention	Ignore	Ignore
Thailand (TISI)	Approval as presented	Ignore	Ignore
Ukraine (DSSU)	Approval as presented	Ignore	Ignore
United Kingdom (BSI)	Disapproval of the draft	All	No
United States (ANSI)	Approval with comments	All	Ignore
Uruguay (UNIT)	Abstention	Ignore	Ignore

Answers to Q.1: "Do you agree with approval of the CD text?"

14 x	Approval as presented	Czech Republic (UNMZ) Denmark (DS) Ireland (NSAI) Italy (UNI) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Norway (SN) Romania (ASRO) Russian Federation (GOST R) Slovenia (SIST) Sweden (SIS) Thailand (TISI) Ukraine (DSSU)
3 x	Approval with comments	China (SAC) Mexico (DGN) United States (ANSI)
3 x	Disapproval of the draft	Japan (JISC) Netherlands (NEN) United Kingdom (BSI)
15 x	Abstention	Australia (SA) Belgium (NBN) Brazil (ABNT) Canada (SCC) Finland (SFS) India (BIS) Kazakhstan (KAZMEMST) Malaysia (DSM) Morocco (IMANOR) New Zealand (SNZ) Poland (PKN) South Africa (SABS) Spain (AENOR) Switzerland (SNV) Uruguay (UNIT)

Answers to Q.2: "If you approve the CD text with comments, would you please indicate which type ? (General, Technical or Editorial)"

1 x	General	Netherlands (NEN)
0 x	Technical	
0 x	Editorial	
4 x	All	China (SAC) Mexico (DGN) United Kingdom (BSI) United States (ANSI)
30 x	Ignore	Australia (SA) Belgium (NBN) Brazil (ABNT) Canada (SCC) Czech Republic (UNMZ) Denmark (DS)

	Finland (SFS) India (BIS) Ireland (NSAI) Italy (UNI) Japan (JISC) Kazakhstan (KAZMEMST) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Malaysia (DSM) Morocco (IMANOR) New Zealand (SNZ) Norway (SN) Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Slovenia (SIST) South Africa (SABS) Spain (AENOR) Sweden (SIS) Switzerland (SNV) Thailand (TISI) Ukraine (DSSU) Uruguay (UNIT)
--	---

Answers to Q.3: "If you disapprove the draft, would you please indicate if you accept to change your vote to Approval if the reasons and appropriate changes will be accepted?"

0 x	Yes	
3 x	No	Japan (JISC) Netherlands (NEN) United Kingdom (BSI)
32 x	Ignore	Australia (SA) Belgium (NBN) Brazil (ABNT) Canada (SCC) China (SAC) Czech Republic (UNMZ) Denmark (DS) Finland (SFS) India (BIS) Ireland (NSAI) Italy (UNI) Kazakhstan (KAZMEMST) Kenya (KEBS) Korea, Republic of (KATS) Luxembourg (ILNAS) Malaysia (DSM) Mexico (DGN) Morocco (IMANOR) New Zealand (SNZ) Norway (SN) Poland (PKN) Romania (ASRO) Russian Federation (GOST R) Slovenia (SIST) South Africa (SABS)

Spain (AENOR) Sweden (SIS) Switzerland (SNV) Thailand (TISI) Ukraine (DSSU) United States (ANSI) Uruguay (UNIT)
--

Comments from Voters		
Member:	Comment:	Date:
China (SAC)	<i>Comment File</i>	2012-08-27 10:00:39
CommentFiles/ISO_IEC_CD_27036-1_SAC.doc		
Japan (JISC)	<i>Comment File</i>	2012-08-29 04:37:14
CommentFiles/ISO_IEC_CD_27036-1_JISC.doc		
Mexico (DGN)	<i>Comment File</i>	2012-08-23 23:24:40
CommentFiles/ISO_IEC_CD_27036-1_DGN.doc		
Netherlands (NEN)	<i>Comment File</i>	2012-08-16 14:07:01
CommentFiles/ISO_IEC_CD_27036-1_NEN.doc		
United Kingdom (BSI)	<i>Comment File</i>	2012-08-28 13:22:12
CommentFiles/ISO_IEC_CD_27036-1_BSI.doc		
United States (ANSI)	<i>Comment File</i>	2012-08-31 16:49:18
CommentFiles/ISO_IEC_CD_27036-1_ANSI.doc		

Comments from Commenters		
Member:	Comment:	Date: