it.sec
security for your information

Der neue Standard ISO/IEC 27036

Information security for supplier relationships

Workshop der GI-FG SECMGT am 11.11.2011

Bernhard C. Witt (it.sec GmbH & Co. KG)

Bernhard C. Witt

- Berater für Datenschutz und Informationssicherheit bei der it.sec GmbH & Co. KG
  verantwortlich für die Geschäftsfelder
  ° Datenschutz
  ° IT Governance, Risk & Compliance Management
- Industriekaufmann, Diplom-Informatiker
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (BSi)
- CRISC (ISACA)
- Lehrbeauftragter an der Universität Ulm (seit 2005)
- Autor der Bücher „IT-Sicherheit kompakt und verständlich“ (2006) und „Datenschutz kompakt und verständlich“ (2008 & 2010)
- verantwortlich zum Thema Compliance der IT-SICHERHEITpraxis (2006 – 2009)
- Sprecher der GI-Fachgruppe Management von Informationssicherheit (seit 2009)
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit (seit 2009)
- Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfahren“ (Normierung zur Informationssicherheit)

it.sec
security for your information

it.sec GmbH & Co. KG

IT-GRCM steht für IT Governance, Risk & Compliance Management.
Hier stehen bei uns Instrumente und Führungsstrukturen des Informationssicherheits-Managements sowie Fragen der tool-gestützten Modellierung von Risikomanagement und Compliance-Anforderungen im Vordergrund, sowie der zielgerichtete Einsatz von technischen und organisatorischen Maßnahmen zur passgenauen Erfüllung identifizierter Anforderungen.

Infrastruktursicherheit & Data Protection
it.sec bietet neben den klassischen Infrastrukturthemen auch umfangreiche Dienstleistungen im Bereich der SCADA Sicherheit an, hierzu zählen neben Sicherheitskonzepten auch Leittechnikverträgliche Methoden für Vulnerability Assessments, Infrastruktur-Mappings oder Protokoll-Analysen. Natürlich gehören auch Industrial Firewalls und AAA Systeme zum Portfolio.

Penetrationstests, IT-Forensik Assessments & Audits
it.sec ist einer der führenden Anbieter von Penetrationstests. Zu unseren Kunden gehören Institutionen aller Branchen, Größen und Sicherheitsstufen, in mehr als einem Dutzend Ländern. Unser Angebot umfasst hierbei **Penetrationstests**, **Sourcecode-Reviews**, **Design-Reviews** sowie **forensische Untersuchungen** und **Beweissicherung. Im Rahmen des PCI DSS Standards führen wir Compliance Penetrationstests durch.**

Datenschutz wird im deutschen Sprachgebrauch leicht verwechselt mit Datensicherheit. Im Englischen spricht man treffender von Privacy ("Privatheit"), geht es doch beim Datenschutz um den Schutz der verfassungsgemäß garantierten Persönlichkeitsrechte beim Umgang mit personenbezogenen Daten. Dazu zählt neben dem sog. Informationellen Selbstbestimmungsrecht auch das Telekommunikationsgeheimnis.

Zur Mitarbeit in dem DIN

- Mitarbeit in Arbeitsgremien des Normenausschusses Informations-technik und Anwendungen (NIA) für jedermann offen
  - ° Jeder NIA-Arbeitsausschuss entscheidet selbst über seine Zusammensetzung (i.d.R. deshalb zuvor Gästestatus)
  - ° Für jedes Gremium sind 980 € pro Jahr (zzgl. MWSt) zu entrichten
- Für IT-Sicherheitsverfahren ist der NIA-01-27 zuständig
  - ° Spiegelgremium des ISO/IEC JTC 1 / SC 27
  - ° Arbeitsausschuss gliedert sich in 5 Arbeitskreise:
    - * AK 01: Information Security Management Systems
    - * AK 02: Cryptography and Security Mechanisms
    - * AK 03: Security Evaluation and Assessment
    - * AK 04: Security Controls and Services
    - * AK 05: Identity Management and Privacy Technologies
  - ° aktive Mitwirkung gefordert (Gäste ohne Zugriff auf Repository)
- Beratungen sind nicht-öffentlich
- Unterlagen sind nur für den Mitarbeiterkreis bestimmt

Vorbemerkungen zum ISO/IEC 27036 (1)

- Sämtliche Teile sind noch auf dem Stand sog. **Working Drafts** (WD), d.h., sie unterliegen noch einer starken Überarbeitung durch Experten (→ selbst Überschriften noch änderbar!)
- Unter Umständen können Entwürfe auf dieser Ebene sogar komplett zurückgezogen oder Scope und Aufteilung massiv verändert werden
- Andererseits ist das ein **guter Zeitpunkt**, um **Einfluss** auf einen derartigen Standard auszuüben ;-)
- Ursprünglich hatte Deutschland (also das DIN) gegen diesen Standard gestimmt (aufgrund der unklaren Zielsetzung des ursprünglichen Scope-Entwurfs)
- Fachlich zuständiger AK 04 innerhalb des DIN erst seit August 2011 mit noch (!) sehr wenig Mitarbeitern gegründet
- Bisher (!) fühlt sich innerhalb des AK 04 keiner für diesen Standard zuständig (→ **Gestaltungsmöglichkeit**!)
- **Die Darstellungen im Folgenden beziehen sich jeweils auf den 1st WD** (2nd WDs gerade in Arbeit!)

Vorbemerkungen zum ISO/IEC 27036 (2)

- Bisherige Entwicklung (1):
  - **2008**: New Work Item Proposal (NWIP) „Security of Outsourcing“ als single International Standard mit folgender **Motivation**:
    „This International Standard will define guidance to organizations on the evaluation of security risks involved in the procurement and use of outsourced services.“
    Die Controls aus den Sections 6.2 (External parties) und 10.2 (Third party service delivery management) der ISO/IEC 27002 reichen hierfür nicht aus.
  - **2009**: NWIP angenommen mit Titel „Guidelines for security of outsourcing“ (als International Standard, kein Technical Report)
    Fokus weiterhin auf die Sichtweise des Acquirer, also des Beziehers eines **outgesourcten Services**, welche wiederum verstanden werden können als
    * Outsourcing zur Informations- und Kommunikationstechnik (ICT)
    * Outsourcing von (kompletten) Geschäftsprozessen, operativen Tätigkeiten oder spezieller ICT-Funktionen

Vorbemerkungen zum ISO/IEC 27036 (3)

- Bisherige Entwicklung (2):
  - **2010**: nach 3rd WD gesplittet in multi-part International Standard „**Information security for supplier relationships**“
    - Part 1: Overview and concepts
    - Part 2: Generic requirements [wird ggf. noch modifiziert]
    - Part 3: Information and communication technology supply chain risk management
    - Part 4: Guidelines for security of outsourcing [bisher ohne WD!]
    - geplanter Part 5 zu Cloud Computing vermutlich zugunsten der ISO/IEC 27017-2 (Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002) hinfällig

    Fokus erweitert sowohl auf Produkte und Services als auch auf die Sicht des Supplier, der Produkte und/oder Services anbietet
    gesamter Prozess des Outsourcings nunmehr im Blick
    International Standard liefert Vorgehensmodell
  - **2011**: **2nd WD** zu Part 1 – 3 wird erstellt (mit starken Änderungen)

Vorbemerkungen zum ISO/IEC 27036 (4)

- Grundsätzlicher Ansatz der ISO/IEC 27036 (1)
  - ° Acquirer möchte Produkt oder Service von Supplier beziehen
  - ° Acquirer verwendet ggf. Produkt oder Service für seine Kunden
  - ° Supplier nutzt ggf. zur Bereitstellung eigene (!) Supplier
  - ° Supplier benötigt für Bereitstellung Informationen / Zugänge des Acquirer
  - ° Acquirer liefert Informationen (inkl. seiner Anforderungen!) / Zugänge, sofern er davon überzeugt ist, dass beim Supplier ein ausreichendes Sicherheitsniveau besteht bzw. sein eigenes Sicherheitsniveau nicht gefährdet ist (risikobasierter Ansatz)
  - ° Supplier liefert erforderliche Daten über sein Sicherheitsniveau
  - ° Acquirer bezieht daraufhin Produkt oder Service von Supplier und gewährt den benötigten Zugang

  → **Acquirer und Supplier haben auszuhandeln**:

  1. Welche Informationen über Sicherheitsniveau sind nötig?
  2. Welche Kontrollrechte sind für Acquirer erforderlich?
  3. Ab wann besteht ein ausreichendes Vertrauen?

Vorbemerkungen zum ISO/IEC 27036 (5)

- Grundsätzlicher Ansatz der ISO/IEC 27036 (2):
  - → Orientierung an der Reihe ISO/IEC 270xx erleichtert das Verständnis über die zu treffenden Vereinbarungen
  - → Der Internationale Standard unterstützt ein Vorgehen nach der ISO/IEC 27002 und konkretisiert hierbei Outsourcing-spezifische Punkte (Ergänzung zur ISO/IEC 27002)
  - → Betrachtung der **Besonderheiten** für ICT Supply Chain Risk Management (also unter Einbeziehung von Unteraufträgen)
  - → Internationaler Standard liefert **Leitfaden** zu Einrichtung, Durchführung, Überwachung und Verbesserung der bestehenden Beziehung und der damit verbundenen Informationssicherheit
  - → Dabei werden alle Phasen / Prozesse, die im Zusammenhang mit Outsourcing relevant sind, behandelt und die im Einzelnen durchzuführenden Aktivitäten benannt
  - → Derzeit (!) liefert der Internationale Standard NICHT eine zertifizierbare Grundlage, die etwaige Audits von Acquirer überflüssig macht

ISO/IEC WD 27036-1 (1)

Reference number of document: **ISO/IEC WD 27036-1**

Committee identification: ISO/IEC JTC 1/SC 27/WG 7

Secretariat: DIN

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

Élément introductif — Élément principal — Partie n: 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.

ISO/IEC WD 27036-1 (2)

Neufassung

Contents

ISO/IEC WD 27036-1 (3)

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

1 Scope

This International Standard gives guidelines for the acquirer and supplier involved in supply chain relationships on the management of information security issues in relation to the implementation of supplier management processes supporting the accomplishment of the acquirer's activities.

Scope wird deutlich geändert (spezifischer!)

ISO/IEC WD 27036-2 (1)

Reference number of document: **ISO/IEC 27036 Part 2**

Committee identification: ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Information technology — Security techniques — Information security for supplier relationships — Part 2: Generic requirements

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.

ISO/IEC WD 27036-2 (2)

Neuer Absatz

Contents

ISO/IEC WD 27036-2 (3)

Information technology — Security techniques — Information security for supplier relationships — Part 2: Generic requirements

Ggf. sowohl „generic“ als auch „requirements“ in Überarbeitung!

1 Scope

ISO/IEC 27036 standard part 2 specifies generic information security requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving supplier relationships from the perspectives of the acquirer and the supplier.

Outsourced products or services in the context of ISO/IEC 27036 standard part 2 cover manufacturing or assembly, business process outsourcing, knowledge process outsourcing or other outsourcing models such as Build-Operate-Transfer and cloud services.

For each of these outsourcing models, there will be generic and particular information security implications that will need to be addressed from the perspectives of the acquirer and the supplier.

The requirements set out in ISO/IEC 27036 standard part 2 are structured following a generic supplier relationships framework. It assumes that the acquirer and the supplier have already implemented a number of foundational processes to support the overall activities, or is actively planning to do so. These foundational processes can include, but are not limited to, the following: governance, business management, operational and human resources management, and information security.

These requirements are intended to be applicable to all organisations, regardless of type, size and nature.

ISO/IEC WD 27036-2 (4)

Beispiel zu Requirements (informativ)

Information security domains	Information security related categories	Information security requirements applied to the supplier
Governance, risk and compliance	Information security framework	Establish, maintain and monitor an information security governance framework
	Information security policy	Develop and distribute a comprehensive, approved information security policy to all individuals with access to the organization's information and systems
	Awareness/education	Establish an information security awareness and behaviour change programme, supported by a range of education/training activities
	Information risk management	Undertake information risk management for key aspects of the service, on a regular basis, in a rigorous and consistent manner, using a structured methodology
	Identification and protection of information that is commercial, sensitive, regulated or personal in nature	Apply an approved method for identifying, maintaining and protecting information such as trade secrets, Intellectual Property, financial, defence-related, food and drug, or personally identifiable information
	Accountability/ownership	Assign ownership and responsibility for particular information and systems to designated individuals who have the required skills, tools and authority
System management	Purchase of hardware and software	Acquire only secure, approved hardware and software (eg purchased from an approved list, subject to a security evaluation and recorded in an inventory)
	Robust resilient design	Design and operate robust, resilient systems that can cope with current and predicted levels of usage, are supported by alternative facilities and incorporate information security requirements
	Separation of primary functions	Deploy servers that implement only one primary function (eg web server, transaction server or database servers should be implemented on separate servers)
	Separation of client databases/ data sets	Separate, both physically and logically, data from one client from that of other clients
	Configuration and security settings	Configure systems in a consistent, accurate manner and apply and monitor approved security settings
	Input/process/output validation	Validate information entered into, processed by and output from business applications and verify that it has not been subject to unauthorised change
	Physical protection	Protect IT facilities equipment and services against malicious attack, accidental damage, natural hazards and unauthorised physical access
	Control of portable storage devices	Restrict the use of unapproved devices and disable the ability to copy data to them
Access management	Segregation of duties	Segregate duties and areas of responsibility to reduce the risk of accidental or deliberate system or application misuse
	Identity and access management	Implement a consistent identity and access management approach that provides effective user administration, identification, authentication and authorisation mechanisms
	Access control	Restrict access to designated information and systems to specified individuals or roles in external suppliers (eg customers, suppliers and business partners) who have been authorised and are subject to agreed security requirements in an approved contract
	Privileged user management	Use strong authentication, force regular password changes and log, monitor and review the activities of privileged users (eg superusers, administrators, DBAs, or people who have access to sensitive or critical information)
Security monitoring and response	Continuous monitoring of systems and networks	Perform continuous monitoring of designated systems and networks, employ intrusion detection systems and record security events
	Malware protection	Deploy comprehensive, up-to-date malware protection software, supported by a user awareness campaign and a process for handling malware infections
	Patch management	Have a documented and measured process for the deployment of system and software patches, including exceptions
	Change management	Implement a comprehensive and approved change management process for information and systems that includes testing/accepting authorised changes and evaluating security implications
	Incident management	Implement a comprehensive and approved incident management process for information and systems that includes identification, response, recovery and post-implementation review of information security incidents
	e-discovery, e-forensic, audit and trail of evidence creation	Collect, store, archive and protect records, logs and other appropriate material
Network connections	Network security	Design and operate robust, resilient networks that can cope with current and predicted levels of traffic, are supported by alternative facilities, incorporate firewalls and restrict network access to authorised individuals
	Control of network access/ connectivity	Restrict connections to the Internet, customers and external suppliers and, where possible, separate those connections
Electronic communications	Protection of electronic communications	Protect electronic communication systems (eg e-mail, instant messaging and VoIP) by setting policy for their use, configuring security settings, performing capacity planning and hardening the supporting infrastructure
	Use of cryptographic solutions	Apply approved, documented cryptographic solutions, supported by effective cryptographic key management
Business control	Sub-contractor management	Restrict access to designated information and systems to sub-contractors and business partners who have been authorised and are subject to agreed security requirements in an approved contract
	Security audit and review	Conduct thorough, independent and regular security audits / reviews and publish the results both internally and for the acquirer
	Business continuity	Have a business continuity plan that is supported by alternative processing facilities and tested regularly using simulations of the live environment
System Development	System Development Life Cycle methodology	Develop systems using a structured and approved system development methodology that ensures information security requirements are considered as part of the process, and consequently defined, documented and met

ISO/IEC WD 27036-3 (1)

ISO/IEC WD 27036-3

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Information technology — Security techniques — Information Security for supplier relationships – Part 3: Information and communication technology supply chain risk management

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.

ISO/IEC WD 27036-3 (2)

Contents

ISO/IEC WD 27036-3 (3)

Information technology — Security techniques — Supplier Relationships — Part 3: Information and communication technology supply chain risk management

1 Scope

This part of international standard ISO/IEC 27036 provides ICT supply chain product and service providers and acquirers with guidance on:

a) gaining visibility into and managing the security risks caused by geographically dispersed ICT supply chains;
b) 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;
c) responding to risks stemming from the global supply chain to IT products and services that may have an impact on the security of organizations using these products and services, including risks related to provided products and services in the ICT supply chain regardless of actors. These risks may be related to organizational as well as technical aspects (e.g., insertion of malicious code or presence of the counterfeit IT products).

This part of ISO/IEC 27036 will not include business continuity management/resiliency-type issues involved with the physical supply chain.

ISO/IEC WD 27036-3 (4)

5.1.2 ICT supply chain risks and associated threats

In supplier relationships, products and services (e.g., hardware, software, integration service, managed security services, IT product development) procured by the acquirer are not necessarily manufactured or operated solely within 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. Or, information processing service can be built on other information processing service as its infrastructure. Thus, supply chains are formed by successive supplier relationships.

In a supply chain, information security management of the supplier in direct relationship is not necessarily sufficient to maintain information security of the products or services. The acquirer's management of the source suppliers, products or services can be essential for information security.

Outsourcing of ICT products and services together with the associated supply chain presents special challenges to acquirers in terms of managing information security throughout the supply chain. These challenges are caused by acquirers having limited (if any) visibility into the processes and practices used by various suppliers upstream or downstream to create ICT products and services within the supply chain. This includes both intentional events (e.g., malicious code insertion and presence of counterfeit electronics in the supply chain) and unintentional events (e.g., sloppy software development practices that result in insecure applications and eventual compromise to acquirer's data and operations).

As global supply chains get more geographically dispersed and traverse multiple international and organizational boundaries, specific security practices applied to individual elements (products, services, and their components) become more difficult to trace including identifying individuals accountable for quality and security of those elements. This creates a general lack of traceability throughout the supply chain which in turn results in higher risk of compromise to acquirers' business operations.

Acquirer concerns associated with ICT supply chain risk management include protection of information and intellectual property, data leakage, malicious code insertion, counterfeit component insertion, reduced functionality of resulting products and services, loss of confidentiality, availability, and integrity which can all result in reduced ability by acquirers to perform their business functions.

ISO/IEC WD 27036-3 (5)

5.6 ICT SCRM-specific requirements

While some of the ICT supply chain risks can be addressed by applying lifecycle processes, establishing an ISMS, and selecting appropriate security controls, additional practices are required to fully address such risks. They include the following:

a) Chain of custody: the confidence that each change and handoff made during the element's lifetime is authorized, transparent and verifiable.

b) Least privilege access: personnel can access critical data with only the privileges needed to do their jobs.

c) Segregation of duties: personnel cannot unilaterally change data, nor unilaterally control the process of creation of elements.

d) Tamper resistance and evidence: attempts to tamper are obstructed, and when they occur they are evident and reversible

e) Persistent protection: critical data is protected in ways that remain effective even if removed from the development location

f) Compliance management: the success of the protections can be continually and independently confirmed

g) Code assessment and verification: methods for code inspection are applied and suspicious code is detected

h) Security training: supplier's ability to effectively train it's developers on secure development practices

i) Vulnerability response: a formal understanding by acquirer of how well their suppliers are equipped with the capability to collect input on vulnerabilities from researchers, customers, or sources, and produce a meaningful impact analysis and appropriate remedies in the short timeframe involved.

j) Defined expectations: clear language regarding the requirements to be met by the element and design/development environment should be set forth in the contractual process. This should include commitment to provide security testing, code fixes and warranties about the development, integration, and delivery processes used.

k) Ownership and responsibilities: intellectual property ownership and responsibilities for protecting the element and development/design environment.

it.sec GmbH & Co. KG
Einsteinstr. 55
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Einsteinstr. 55
D-89077 Ulm