

ISO/IEC 27306 – Summary and Update

Nadya Bartol
November, 2011

Table of Contents

- ▶ Current Status
- ▶ Sample Content
- ▶ Future Plans

Where we are today – ICT SCRM has been accepted as important and adopted by the SC27 community

Timeframe	Impact	Actions and Activities
February 2009 – November 2009	US consensus	<ul style="list-style-type: none"> • Established CS1 ICT SCRM Ad Hoc joint with SC7 TAG with broad industry and government representation • Proposed a new ICT SCRM standard for CS1 to consider which was put forward at the SC27 meeting in Redmond, WA • SC27 established ICT Supply Chain Security Study Period to validate need for a standard
November 2009 – October 2010	ISO consensus	<ul style="list-style-type: none"> • Rapporteur briefed SC27 meeting in April 2010, Study Period was extended to October 2010 • Independently, Information Security Forum (ISF) presented proposal for a joint standard on Information Security for Supplier Relationships • Extensive discussion at the October 2010 resulted in SC27 decision to restructure/expand current draft of ISO/IEC 27036 (Guidelines for Security of Outsourcing) to address “Supplier Relationships” in 3 parts with the potential for further parts • Restructuring was supported by Belgium, Canada, China, France, Japan, Korea, Luxembourg, Malaysia, Russia, Singapore, South Africa, Sweden, Switzerland, United Kingdom, US, US, Information Security Forum (ISF), ISACA
October 2010 – October 2011	First draft	<ul style="list-style-type: none"> • Editors developed preliminary and first working drafts of Parts 1, 2, and 3 • CS1 ICT SCRM Ad Hoc formulated US position • SC27 meetings reviewed and disposed of comments

How does ISO/IEC 27036 fit into the bigger picture

Tools and Techniques

- Common Criteria – ISO/IEC 15408
- OMG KDM BPMN, RIF, XMI, RDF
- OWASP Top 10
- SANS TOP 25
- Secure Content Automation Protocol (SCAP)
- Secure Coding Checklists
- Encryption
- Software Asset Tagging
- Trusted Platform Module (TPM)
-

ICT SCRM and other Context-Specific Requirements

- ISO/IEC 27036 Part 4 – Outsourcing; Part 5 – Cloud; Part 6 – potentially Trusted Technology Framework

ICT SCRM General Requirements

- ISO/IEC 27036 Part 1 – Overview; Part 2: Requirements; Part 3 – ICT SCRM
- NIST IR 7622
- Trusted Technology Framework

Essential Security and Foundational Practices

- **Management Systems:** ISO 9001 - Quality, ISO 27001 – Information Security, ISO 20000 – IT Service Management, ISO 28000 – Supply Chain Resiliency
- **Security Controls:** ISO/IEC 27002, NIST 800-53
- **Lifecycle Processes:** ISO/IEEE 15288 - Systems, ISO/IEEE 12207 - Software
- **Risk Management:** ISO 31000 - overall, ISO/IEC 27005 - security, and ISO/IEC 16085 - systems
- **Industry Best Practices:** CMMI, Assurance Process Reference Model, Resiliency Management Model (RMM), COBIT, ITIL, PMBOK

Processes and Practices

- ISO/IEC 15026 – Software Assurance
- ISO/IEC 27034 – Application Security
- Security Engineering and Design techniques
- NASPO and other Anti -Counterfeiting techniques
- Microsoft Secure Development Lifecycle (SDL)
- SAFECODE
- OWASP
- BSIMM
-

ISO/IEC 27036: Information technology – Security techniques – Information Security for Supplier Relationships

▶ Covers

- Information security in relationships between acquirers and suppliers
- All types of organizations e.g., commercial, public sector, non-profit
- All types of supplier relationships, including outsourcing, product and service acquisition, ICT, and cloud computing, that may have security implications

▶ Multipart standard with Nadya Bartol (US, Booz Allen Hamilton) as Project Editor responsible for success

- Part 1 – Overview and Concepts (Becky Swain, US, EKKO Consulting, CSA, formerly Cisco)
- Part 2 – Common Requirements (Benoit Poletti, Luxemburg, Deloitte)
- Part 3 – Guidelines for ICT Supply Chain Security (Nadya Bartol, US, Booz Allen Hamilton)
- Part 4 – Guidelines for Outsourcing (currently not being worked)
- Part 5 – Cloud Computing (scope is being created by Cisco)
- Part 6 – placeholder for TTF pending further inputs from OTPF

▶ Relies on collaborative relationships

- Information security for supplier relationships – Information Security Forum (ISF)
- Lifecycle processes – SC7 – Software and System Engineering
- Anti-counterfeiting tools – TC246 – Project committee: Anti-counterfeiting tools
- Fraud prevention – TC247 – Fraud countermeasures and controls
- Supply chain – TC8 – Ships and marine technology
- Resiliency – TC223 – Societal Security

October 2011 Comments Summary

- ▶ Who commented
 - National Bodies
 - ISF
 - The Open Group
 - TC8

- ▶ What was in the comments
 - Placement of Definitions
 - Should Part 2 be a requirements standard
 - Restructuring of Part 2 according to Part 3 outline
 - Addressing both Supplier and Acquirer perspectives

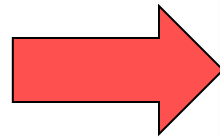
- ▶ TC8 – replace bibliographical reference to ISO 28001 with a normative reference to ISO 28000

- ▶ The Open Group – reserve Part 6 for The Open Group output

ISO/IEC 27036 Part 2 structure provides supplier relationship lifecycle and will also be aligned with ISO/IEC 15288 in the next revision

Supplier Relationship Lifecycle Processes

- 6.2 – Supplier Relationship Planning
- 6.3 – Supplier Selection
- 6.4 – Supplier Relationship Agreement
- 6.5 – Supplier Relationship Management
- 6.6 – Supplier Relationship Termination and Exit



0	Introduction.....	DRAFT
1	Scope.....	6
2	Normative references.....	7
3	Terms and definitions.....	7
4	Symbols and Abbreviated Terms	8
5	Structure of ISO/IEC 27036 standard part 2.....	8
6	Managing information security within the scope of supplier relationships management.....	9
6.1	Introduction.....	9
6.2	Supplier relationships planning	9
6.2.1	Acquirer information security implications	9
6.2.2	Supplier information security implications.....	10
6.3	Supplier selection	11
6.3.1	Acquirer information security implications	11
6.3.2	Supplier information security implications.....	12
6.4	Supplier relationships agreement.....	13
6.4.1	Acquirer information security implications	13
6.4.2	Supplier information security implications.....	14
6.5	Supplier relationships management	14
6.5.1	Acquirer information security implications	14
6.5.2	Supplier information security implications.....	15
6.6	Supplier relationships termination and exit.....	16
6.6.1	Acquirer information security implications	16
6.6.2	Supplier information security implications.....	17
	Annex A (informative) Implementation guidance.....	18
A.1	Supplier relationships strategy	18
A.2	Supplier relationships plan	18
A.3	Information security requirements applied to supplier	19
A.4	Supplier selection criteria.....	22
A.5	Transition plan	22
A.6	Monitoring and enforcing the supplier’s compliance.....	23
	Annex B (informative) Cross-references between ISO/IEC 27002 controls and ISO/IEC 27036 Part 2 clauses	25
	Bibliography	27

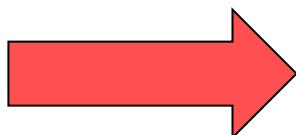
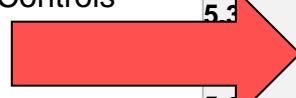
ISO/IEC 27036 Part 3 is aligned with ISO/IEC 15288/12207 as well as ISO/IEC 27001/27002

DRAFT

Foreword.....	
Introduction	v
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
4 Structure of this Standard	4
5 Key concepts	4
5.1 Overview.....	4
5.1.1 Business case for ICT outsourcing.....	4
5.1.2 ICT supply chain risks and associated threats.....	5
5.1.3 Acquirer and supplier characteristics.....	5
5.2 Establishing organizational capability	6
5.3 Using system lifecycle processes.....	6
5.3.1 Using ISMS PDCA processes in relation to system lifecycle processes	7
5.3.2 Using ISMS security controls in relation to SCRM	7
5.6 ICT SCRM-specific requirements	7
6 ICT SCRM in Lifecycle Processes	8
6.1 Agreement Processes.....	8
6.1.1 Acquisition Process.....	8
6.1.2 Supply Process	9
6.2 Organizational Project-Enabling Processes	9
6.2.1 Life Cycle Model Management Process	9
6.2.2 Infrastructure Management Process.....	9
6.2.3 Project Portfolio Management Process	10
6.2.4 Human Resource Management Process.....	10
6.2.5 Quality Management Process.....	10
Annex A Bibliography	18
Annex B Summary of Supply and Acquisition Processes from ISO/IEC 15288 and ISO/IEC 12207	19

Information security

- ISO/IEC 27001 – ISMS
- ISO/IEC 27002 – Security Controls



System and software engineering

- ISO/IEC 15288 – System Lifecycle Processes
- ISO/IEC 12207 – Software Lifecycle Processes Controls

ISO/IEC 27036 – Vision Moving Forward

Timeframe	Expected Outcomes
October 2011-May 2012	<ul style="list-style-type: none"> • Part 1 – Committee Draft
May 2012-October 2012	<ul style="list-style-type: none"> • Part 1 – Final Draft • Part 2 – Committee Draft • Part 3 – Committee Draft
October 2012-May 2013	<ul style="list-style-type: none"> • Part 1 ready for publication • Parts 2 and 3 – Final Draft
May 2013-October 2013	<ul style="list-style-type: none"> • Part 1 published/available for purchase • Parts 2 and 3 ready for publication • 27036 Parts 1-3 available for use
Other pieces that need to be in place	<ul style="list-style-type: none"> • Working with other countries to ensure ISO/IEC 27002, ISO controls catalog, provides appropriate "hooks" for 27036 being used in the context of ISO/IEC 27001 certification • Establishing architectural relationship between ISO/IEC 27036 and other standards for future use cases, e.g. Cloud