ISO/IEC 27306 – Summary and Update

Nadya Bartol
November, 2011

Table of Contents

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**	• **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**	• 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**	• 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

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

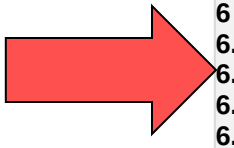
October 2011 Comments Summary

- 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



DRAFT

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

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

DRAFT

ISO/IEC 27036 – Vision Moving Forward

Timeframe	Expected Outcomes
October 2011-May 2012	• Part 1 – **Committee Draft**
May 2012-October 2012	• Part 1 **– Final Draft** • Part 2 **– Committee Draft** • Part 3 **– Committee Draft**
October 2012- May 2013	• Part 1 **ready for publication** • Parts 2 and 3 **– Final Draft**
May 2013-October 2013	• 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	• 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