ISO/IEC 27036 – Information Security for Supplier Relationships
Why Standards?

- Interoperability
- Competitive advantage for countries and companies
- Common language for acquirers and suppliers

*ISO standards: global applicability and acceptance*
ISO has over 90 existing cyber security standards and is currently developing or revising over 45 standards

| Information Security Management System | Sector-Specific Guidance (Telecom, Financial Services) |
| Security Controls                       | Biometric Techniques                                    |
| Information Security Risk Management    | Privacy Technologies                                    |
| Information Security Measurement        | Access control and management                           |
| Disaster Recovery                       | Entity Authentication                                    |
| Vulnerability Management                | Hash Functions                                           |
| Network Security                        | Authenticated Encryption                                 |
| Intrusion Detection System              | Random Bit Generation                                   |
| Incident Management                     | ICT Readiness for Business Continuity                   |
| Application Security                    | Common Criteria                                          |
| Identity Management                     | Security Engineering                                     |
| Authentication Assurance                 | Security Assurance                                       |
| Trusted Platform Module                 | Security of Outsourcing                                  |
|Cryptographic Techniques                 | ICT Supply Chain Security                               |
|Key Management                           | Economics of Information Security                        |
|Authentication Protocols                 | Forensic Investigation                                   |
|Information Security Governance          | Cyber Security                                           |

And Many More…
Why Use ISO/IEC 27001?

- Integrate security governance into business and IT processes
  - Standardize security processes and controls
  - Establish a common approach to risk management
  - Reduce the likelihood, severity, duration and cost of incidents
- Establish risk-based control selection as a standard for risk management
  - Focus resources only on your organization’s risks
  - Facilitate identification and elimination (or minimal retention) of non-critical data
  - Ensure costs reflect the risk’ appetite
- Use ISMS processes to improve overall asset management capabilities
  - Identify and eliminate redundant, duplicate and obsolete assets
  - Enable simplified cost determination for new or revised control deployments
  - Provide risk reference point for both operations and management

Source: Booz Allen Hamilton and DoD
Draft ISO/IEC 27002:2013 Security Controls

- Security Policies
- Organization of information security
- Human resource security
- Asset Management
- Access Control
- Cryptography
- Physical and Environmental Security
- Operations Security
- Communications Security
- System Acquisition, Development, and Maintenance

**Supplier Relationships**

- Information Security Incident Management
- Information Security Aspects of Business Continuity Management
- Compliance

• Addresses Acquirer and Supplier practices
• Applies to all types of organizations e.g., commercial, public sector, non-profit and all types of supplier relationships that may have security implications
• Harmonized with ISO standards for system/software engineering and information security
• Parts 1-3 are currently Draft International Standard, Part 4 is Working Draft
ISO/IEC 27036 Dependencies and Influences

Overview
- ISO/IEC 27036-1 – Overview and Concepts
- ISO/IEC 27000 – Overview and Vocabulary

Requirements

Guidance
- ISO/IEC 15288/12207 – Systems and Software Lifecycle Processes
- ISO/IEC 27036-3 - Information Security for Supplier Relationships – ICT SCRM
- ISO/IEC 27002 – Code of Practice for Information Security Controls

Processes and Techniques
- 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)
- SAFECrde
- OWASP
- BSIMM
- 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)

Source: Booz Allen Hamilton and DoD
Using ISO/IEC 27036 with other SC27 Standards

Certify against ISMS and...

...general requirements for supplier relationships
ISO/IEC 27036-2 – Information Security for Supplier Relationships - Requirements

...ICT SCRM guidance

...Cloud-specific guidance
ISO/IEC 27036-4 - Information Security for Supplier Relationships – Cloud Services

ISO/IEC 27001 – Information Security Management Systems

...27002 controls
ISO/IEC 27002 – Code of Practice for Information Security Controls

...27017 Cloud Controls
ISO/IEC 27017 - ISMS – Code of practice for information security controls for cloud computing services

Source: Booz Allen Hamilton and DoD
# Timeline for Parts 1-3

| Timeframe         | Outcomes                                           |
|-------------------|**************************************************|
| November 2009 – October 2010 | Built consensus through Study Period               |
| October 2010 – May 2012 | Developed Working Drafts                           |
| May 2012          | Progressed to Committee Draft                      |
| October 2012      | Progressed to Draft International Standard          |
| October 2012- April 2013 | Ready for Publication?  |
|                   | Another Draft International Standard?              |
| October 2013      | Ready to publish                                   |
Contact Information

• Nadya Bartol
  Utilities Telecom Council
  202-833-6809
  nadya.bartol@utc.org