ICT SCRM – ISO Standards Update

Nadya Bartol

March 2, 2011

Standards are a common language used to communicate expected levels of performance for products and services

Standards are Essential to Global Economy

- Ensuring interoperability among trade partners
- Facilitating increased efficiencies in the global economy
- Making the development, manufacturing, and supply of products and services more efficient, safer and cleaner
- Providing governments with a technical base for health, safety and environmental legislation
- Safeguarding consumers, and users in general, of products and services - as well as to make their lives simpler

Governments Care

- **US National Technology Transfer and Advancement Act of 1995 (NTTAA)** (Public Law [P.L] 104-113, Sec 12-d-1)

  > *"Federal agencies and departments shall use such technical standards as a means to carry out policy objectives... ."*

- **World Trade Organization Agreement on Technical Barriers to Trade** encourages the use of international standards and conformity assessment systems because of their potential for improving the efficiency of production and facilitating international trade.

Businesses adopt standards when it is clear that they can gain competitive advantage

Countries use international standards compliance as a trade barrier and differentiator for their companies

Most prominent global standards organizations use consensus-driven processes for standards development

- The ***International Organization for Standardization*** (ISO) is the world’s largest developer of standards. ISO is a non-governmental consensus-building network of the national standards institutes of 156 countries. Those institutes do not directly represent the governments of their respective countries, but commonly have close ties to both governments and industries.

- The ***International Electrotechnical Commission*** (IEC) develops international standards and conformity assessments for government, business and society for all electrical, electronic and related technologies. Their standards are relied upon for the creation of national standards, and for international commercial contracts and agreements.

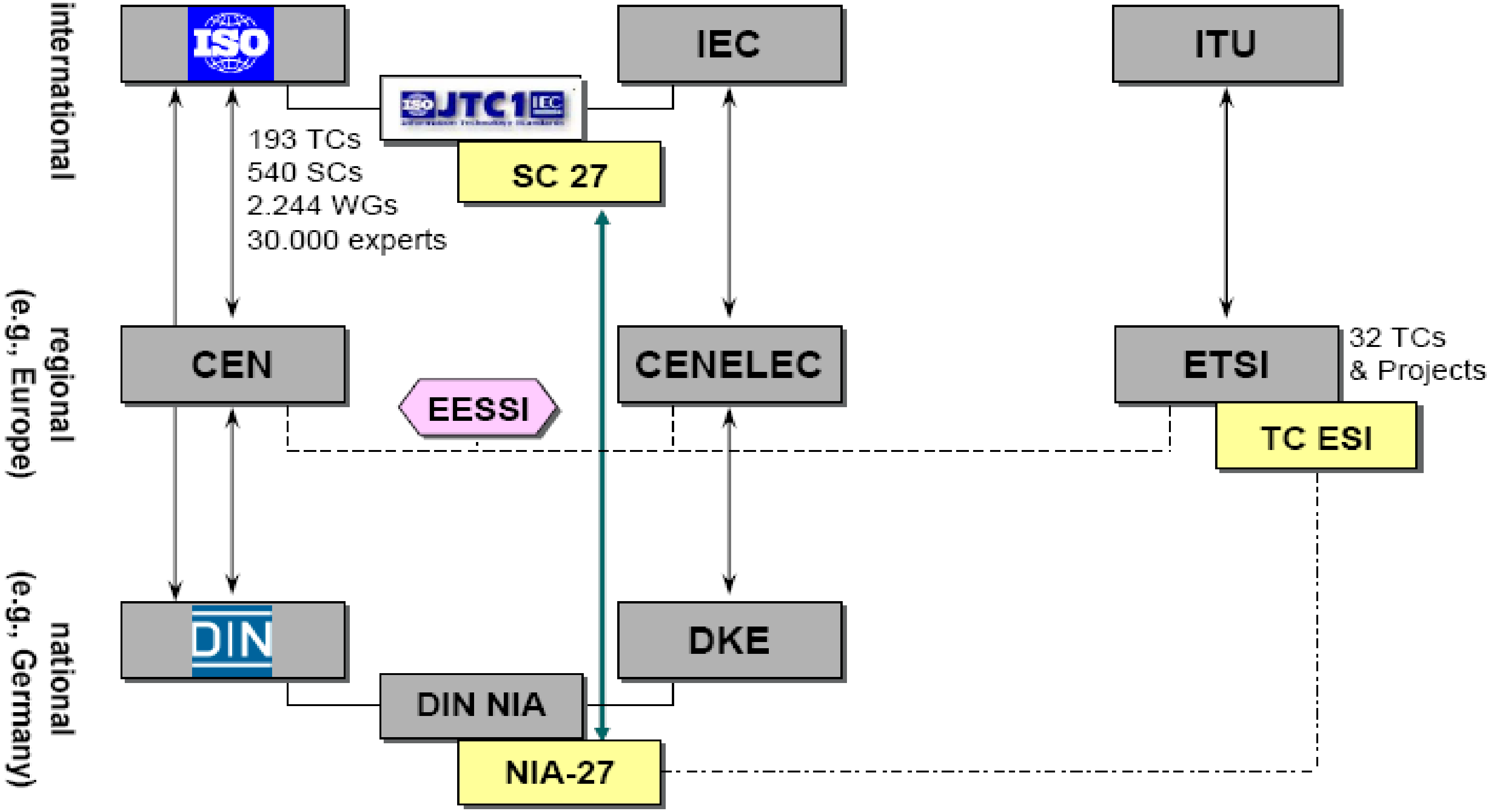
- The ***International Telecommunications Union*** (ITU), with roots in the late 1800s stemming from treaties to address international telegraph interconnections, it is now an international organization within the United Nations system where governments and the private sector coordinate global telecom networks and services.

- ***The Institute of Electrical and Electronics Engineers*** (IEEE), which establishes standards for electro and information technologies and sciences. Like other standards, these support broader commercialization, interoperability, efficient design and implementation, and protection of users and the environment.

- ***The Internet Engineering Task Force*** (IETF), which develops Internet-related standards, especially those relating to the TCP/IP protocol. Its membership is open to the general public, and though it meets three times a year, most of its work is conducted electronically via email.

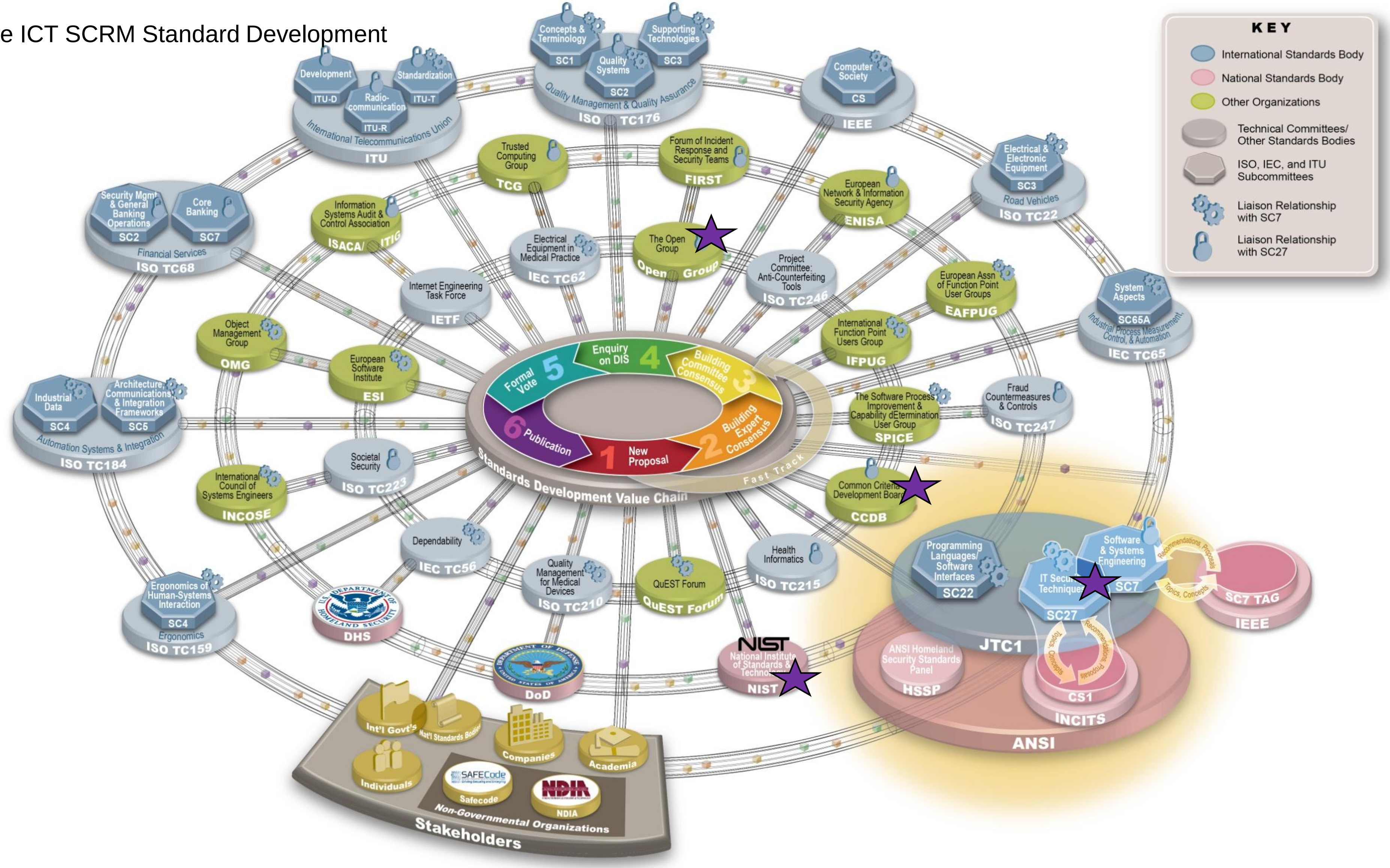
Effective standards incorporate the views of all interested parties from manufacturers, vendors and users to research organizations and governments.

Other players exist and are all connected through higher level organizations or lateral liaisons

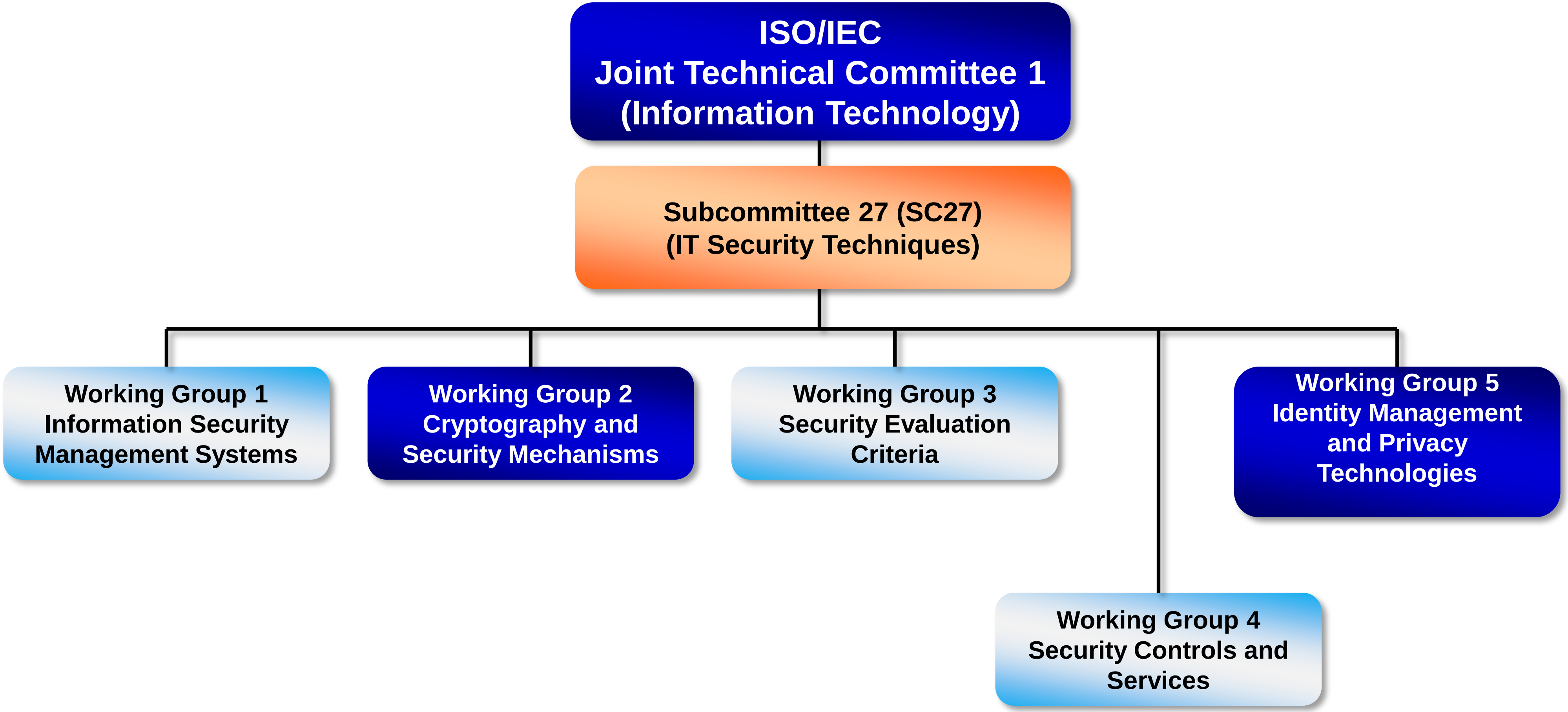


The ICT SCRM Standard Development Organization Landscape

★ Active ICT SCRM Standard Development


KEY
International Standards Body
National Standards Body
Other Organizations
Technical Committees/ Other Standards Bodies
ISO, IEC, and ITU Subcommittees
Liaison Relationship with SC7
Liaison Relationship with SC27
Concepts & Terminology
SC1
Quality Systems
SC2
Supporting Technologies
SC3
Quality Management & Quality Assurance
ISO TC176
Development
ITU-D
Radio-communication
ITU-R
Standardization
ITU-T
International Telecommunications Union
ITU
Computer Society
CS
IEEE
Electrical & Electronic Equipment
SC3
Road Vehicles
ISO TC22
Trusted Computing Group
TCG
Forum of Incident Response and Security Teams
FIRST
European Network & Information Security Agency
ENISA
Security Mgmt & General Banking Operations
SC2
Core Banking
SC7
Financial Services
ISO TC68
Information Systems Audit & Control Association
ISACA/ITIG
Electrical Equipment in Medical Practice
IEC TC62
The Open Group
Open Group
Project Committee: Anti-Counterfeiting Tools
ISO TC246
European Assn of Function Point User Groups
EAFPUG
System Aspects
SC65A
Industrial Process Measurement, Control, & Automation
IEC TC65
Internet Engineering Task Force
IETF
International Function Point Users Group
IFPUG
Object Management Group
OMG
European Software Institute
ESI
Industrial Data
SC4
Architecture, Communications & Integration Frameworks
SC5
Automation Systems & Integration
ISO TC184
Enquiry on DIS
4
Building Committee Consensus
3
Formal Vote
5
Building Expert Consensus
2
Publication
6
New Proposal
1
Fast Track
Standards Development Value Chain
The Software Process Improvement & Capability dEtermination User Group
SPICE
Fraud Countermeasures & Controls
ISO TC247
Societal Security
ISO TC223
International Council of Systems Engineers
INCOSE
Common Criteria Development Board
CCDB
Dependability
IEC TC56
Health Informatics
ISO TC215
Programming Languages/ Software Interfaces
SC22
Software & Systems Engineering
SC7
IT Security Techniques
SC27
JTC1
Recommendations, Proposals
Topics, Concepts
SC7 TAG
IEEE
Ergonomics of Human-Systems Interaction
SC4
Ergonomics
ISO TC159
DHS
Quality Management for Medical Devices
ISO TC210
QuEST Forum
QuEST Forum
NIST
National Institute of Standards & Technology
NIST
ANSI Homeland Security Standards Panel
HSSP
CS1
INCITS
ANSI
DoD
Int'l Govt's
Nat'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
NDIA
Non-Governmental Organizations
Stakeholders

Within the ISO structure, ISO/IEC JTC1 SC27 focuses on cyber security



ISO/IEC
Joint Technical Committee 1
(Information Technology)

Subcommittee 27 (SC27)
(IT Security Techniques)

Working Group 1
Information Security Management Systems

Working Group 2
Cryptography and Security Mechanisms

Working Group 3
Security Evaluation Criteria

Working Group 4
Security Controls and Services

Working Group 5
Identity Management and Privacy Technologies

SC27 portfolio includes over 90 cyber security standards with over 45 currently under development or revision, plus study periods covering a diverse set of subjects

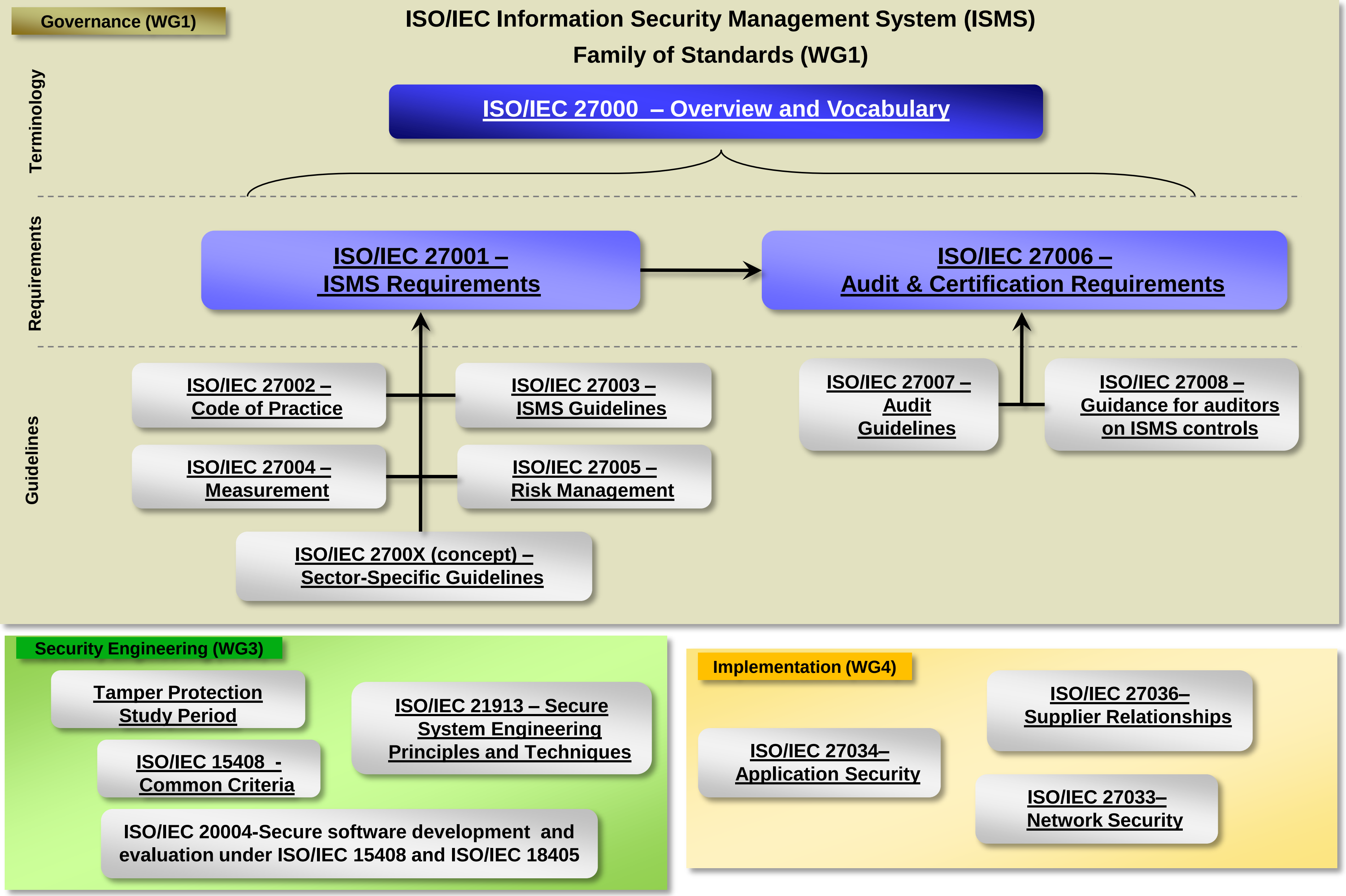
- Information Security Management System
- Security Controls
- Information Security Risk Management
- Information Security Measurement
- Disaster Recovery
- Vulnerability Management
- Network Security
- Intrusion Detection System
- Incident Management
- Application Security
- Identity Management
- Authentication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

And Many More…

CS1 represents US interests within SC27

- Operating under the auspices of InterNational Committee for Information Technology Standards (INCITS), which is the US counterpart to JTC1

- With diverse representation of industry, government, and academia
  - Alcatel Lucent
  - Atsec
  - Boeing
  - Booz Allen
  - CERT
  - Cisco
  - EMC
  - Fidelity
  - Gemalto
  - HP
  - Hitachi Data Systems
  - Intel
  - Kantara Initiative
  - Lexmark
  - Marks
  - Microsoft
  - Mitre
  - NSA
  - NIST
  - Oracle
  - Plum Hall Inc
  - Raytheon
  - Ricoh
  - SAFECode
  - Surety
  - Symantec
  - The Open Group
  - DHS
  - DoD
  - Veridion
  - VHA
  - WB Hamilton
  - Yaana Technologies
  - Zygma Partnership



Governance (WG1)

ISO/IEC Information Security Management System (ISMS) Family of Standards (WG1)

Terminology

ISO/IEC 27000 – Overview and Vocabulary

Requirements

ISO/IEC 27001 – ISMS Requirements

ISO/IEC 27006 – Audit & Certification Requirements

Guidelines

ISO/IEC 27002 – Code of Practice

ISO/IEC 27003 – ISMS Guidelines

ISO/IEC 27004 – Measurement

ISO/IEC 27005 – Risk Management

ISO/IEC 2700X (concept) – Sector-Specific Guidelines

ISO/IEC 27007 – Audit Guidelines

ISO/IEC 27008 – Guidance for auditors on ISMS controls

Security Engineering (WG3)

Tamper Protection Study Period

ISO/IEC 15408 - Common Criteria

ISO/IEC 21913 – Secure System Engineering Principles and Techniques

ISO/IEC 20004-Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405

Implementation (WG4)

ISO/IEC 27036– Supplier Relationships

ISO/IEC 27034– Application Security

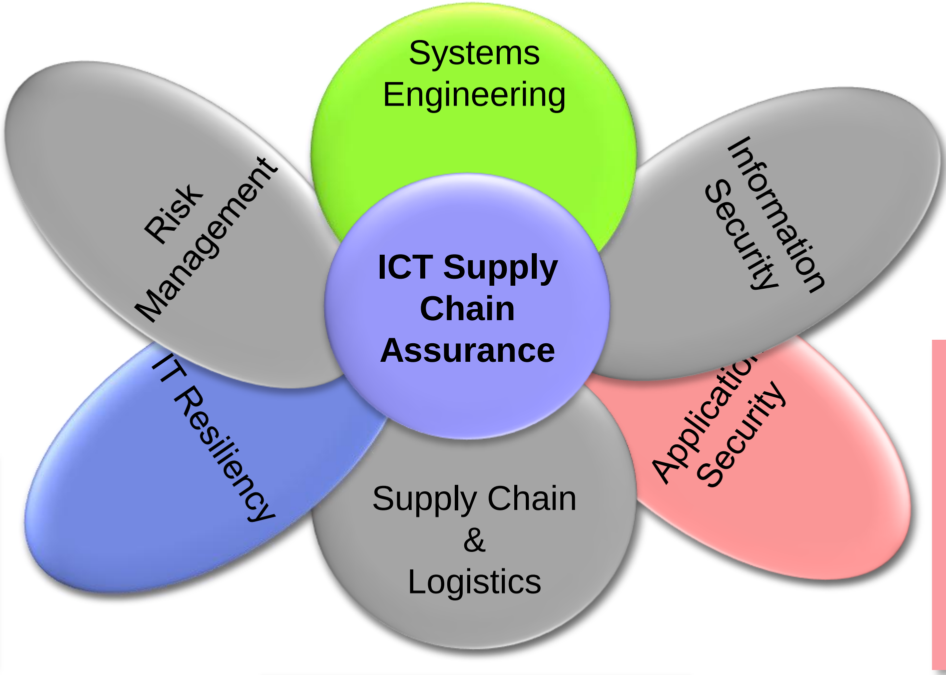
ISO/IEC 27033– Network Security

ICT Supply Chain Risk Management requires contributions and collaboration among many disciplines with recognized standards

- ISO/IEC/IEEE 15288 (Systems)
- *ISO/IEC15026 (Systems Assurance)*
- IEEE 1062 (Software Acquisition)
- Capability Maturity Model Integration (CMMI)

- ISO/IEC 27005 (Risk Management: Information Security)
- ISO/IEC 16085 (Risk Management: Life Cycle Processes)
- ISO/IEC 31000 (Risk Management: Principles and Guidelines)

- *ISO/IEC 27036 (Information Security for Supplier Relationships)*
- ISO/IEC 27000 Family (Information Security Management Systems)
- Common Criteria



- ISO/IEC 20000 (IT Service Management)
- Resiliency Management Model (RMM)

- OSAMM
- BSIMM
- Microsoft Secure Development Lifecycle
- *ISO/IEC 27034 (Guidelines for Application Security)*
- *ISO/IEC TR 24772 (Programming Language Vulnerabilities)*

- ISO/IEC 28000 (Supply Chain Resiliency)

ISO Standards development process takes 2-5 years and requires consensus-building among national standards bodies

- Begins with an established **marketplace requirement** that **is communicated through a national standards body**, which proposes the request to a corresponding subcommittee
- The **subcommittee presents the proposal** for a discussion and a vote, and, if accepted, the subcommittee begins working on the standard
- An **editor is sought and provided**—an expert who leads the standard's development
- The **subcommittee reviews multiple drafts and requests comments** from national standards bodies and liaison organizations to advance drafts to the next formal stage of development
- Advancing the standard from one formal stage to another requires an **international ballot**, voted on by each standards body, one vote per country
- With their votes, the national standards bodies submit **comments on content, suggestions for improvement, and explanations for no votes**
- When a standard successfully advances through all required stages, it is **published** as an international standard

How and when did SC27 decide to develop ICT SCRM standard?

Timeframe	Action
February 2009	• **CS1 ICT SCRM Ad Hoc stood up, chaired by TMSN, driven by commercial input** • Current membership includes Cisco, Microsoft, EMC, Intel, SAFECode, Boeing, Symantec, and others • US SC7 TAG has been an active member in the CS1 ICT SCRM Ad Hoc since the first Ad Hoc meeting expanding commercial and expert involvement to include IEEE and systems integrators (CSC, LMCO, etc)
February 2009 – November 2009	• ICT SCRM Ad Hoc reviewed and commented on ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27034, ISO/IEC 27036 (old draft) • Concluded that ICT SCRM required it's own standard and developed proposal for a new ICT SCRM standard for CS1 to consider
November 2009	• US proposed ICT SCRM Standard at SC27 meeting in Redmond, WA • SC27 established ICT Supply Chain Security Study Period to validate need for a standard • US Delegate (Booz Allen/DoD) is appointed Study Period Rapporteur
November 2009 – October 2010	• CS1 ICT SCRM Ad Hoc consolidated US contribution to the Study Period (contributions from SAFECode, Microsoft, Mitre, and DoD) • Rapporteur briefed SC27 meeting in April 2010 • UK and JP submitted short contributions • Study Period was extended to October 2010
October 2010	• Rapporteur presented Final Study Period report presented at SC27 meeting • Information Security Forum (ISF) presented proposal for a joint standard on Information Security for Supplier Relationships • **SC27 decided to restructure/expand current draft of ISO/IEC 27036 (Guidelines for Security of Outsourcing) to address "Supplier Relationships" in 3 parts** • Rapporteur is nominated Part 3 Project Editor

Restructuring of ISO/IEC 27036 had broad support from the international community

- Technical experts from a number of NBs and liaison organizations agreed that ISO/IEC 27036 needed to be restructured and that ICT SCRM had to be addressed
  - Belgium
  - Canada
  - France
  - Japan
  - Korea
  - Luxembourg
  - Malaysia
  - Russia
  - Singapore
  - South Africa
  - Sweden
  - Switzerland
  - United Kingdom
  - US
  - ISF
  - ISACA

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

- Covers information security in relationships between acquirers and suppliers to provide appropriate information security management for all parties including management of information security risks related to these relationships.
- Applies to all types of organisations (e.g., commercial enterprises, public sector organisations, not-for-profit organisations, and partnerships), specifies the information security requirements and guidance associated with managing a supplier relationship (e.g., identifying and categorizing suppliers; agreeing, monitoring, validating, and changing supplier arrangements; and exiting).
- Covers all types of supplier relationships, including outsourcing, product and service acquisition, and cloud computing including ICT and other types of supplier relationships (e.g. power supply, human resources, facilities management) that have information security implications)
- Consists of four parts:
  - Part 1 – Overview and Concepts (based on ISF proposal and prior ISO/IEC 27036), to introduce the topic
  - Part 2 – Common Requirements (based on ISF proposal, 27036), to provide requirements that acquirers can use in contracts
  - Part 3 – Guidelines for ICT Supply Chain Security (based on study period outcomes), to address ICT SCRM
  - Part 4 – Guidelines for Outsourcing (placeholder for the current text, remain at WD3 to determine future course of action)

Intended to point to other relevant standards and be developed in collaboration with other standards bodies

- Relevant standards:
  - Management Systems: ISO/IEC 27000 family; ISO 28000, Supply Chain Resiliency; ISO/IEC 20000, IT Service Management
  - Risk Management: ISO 31000, ISO/IEC 27005, and ISO/IEC 16085
  - Lifecycle Processes and Practices, software acquisition, and software assurance ISO/IEC/IEEE 15288 (systems), ISO/IEC/IEEE 12207 (software), IEEE 1062 (software acquisition), ISO/IEC15026 (software assurance)
  - ISO TMB NWIP on Outsourcing

- Cooperation and liaison
  - Information Security Forum (ISF)
  - SC7, Software and System Engineering
  - TC246, Project committee: Anti-counterfeiting tools
  - TC247, Fraud countermeasures and controls
  - TC8, Ships and marine technology
  - TC223, Societal Security

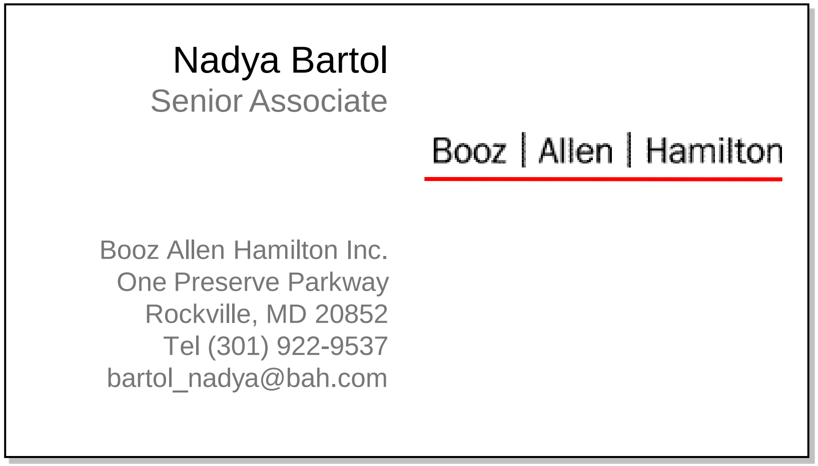
Since restructuring was approved

- ISO/IEC 27036 Parts 1 and 2 editors restructured prior ISO/IEC 27036 text into Parts 1 and 2
- ISO/IEC 27036 Part 3 editor created an outline and preliminary draft based on the ICT SCRM Study Period outputs
- ISF released their document to ISO to serve as a contribution towards the standard
- SC27 distributed Preliminary drafts for Parts 1 and 3 to the National Bodies for review and comment
- CS1 ICT SCRM Ad Hoc reviewed and commented on Parts 1 and 3 and provided these comments to CS1 for inclusion into the US national position for the Spring 2011 meeting

Next Steps

- Before April 2011
  - CS1 will review CS1 ICT SCRM Ad Hoc contributions, revise, and include them in the USNB positions
  - CS1 will send USNB positions to SC27 Secretariat
- Beyond April 2011 meetings
  - CS1 ICT SCRM Ad Hoc will continue contributing to ISO/IEC 27002, ISO/IEC 27036, and other relevant standards
  - ISO/IEC 27036 will go through ISO development process stages with an ambitions goal of finalizing and publishing by May 2013

Stay tuned for further updates



Nadya Bartol
Senior Associate

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
One Preserve Parkway
Rockville, MD 20852
Tel (301) 922-9537
bartol_nadya@bah.com