A Systematic Approach to Influencing System Security Standards

Ken Kepchar ESEP, CISSP
Co-Chair INCOSE Security WG

EagleView Associates LLC
703-346-7706
eagleview2@cox.net

EagleView Associates LLC

The What & Why

Genesis

System Security WG Project 17

- **Initiated to participate in standards development per the SSWG charter**
- **Approved in late 2014 as a formal Technical Project Plan under auspices of INCOSE Standards Director**

Objectives

- **Establish and foster the responsibility for security within Systems Engineering**

  Establish INCOSE as a recognized and respected participant **in the field of system security engineering and align security processes and practices with established System Engineering life cycle processes.**

- **Establish and foster self-sustaining cross- community involvement between systems engineers, security engineers, and system security standards.**

- **Establish and foster systems engineering guidance for enabling effective systems security**

- **Attract an international cadre of engaged participants to broaden the understandings and effectively deal with multi-national interests and differences.**

What Does It Take to Successfully Influence Standards?

***Interaction** (Presence)*

Representation at working and decision making levels

***Input** (Contribution)*

Investment to contribute substantive content

1) Identification of "value" opportunities
2) Expert(s) willing to invest time & energy to review documents and provide **thoughtful** input
3) Organizational support for the experts
4) A channel to submit "expert contributions" *(ISO-speak)* to the standards body
5) Ability (financial, etc) to maintain participation in standards development throughout the document development process

***Impact** (Participation)*

Direct participation in document development (author or editor)

1) Availability of an (recognized?) expert to undertake the commitment involved
2) Organizational support (including resources) of the individual in this role
3) Sponsorship by a standards organization member (National body, etc)
4) Acceptance by the standards organization

ISO Standard Document Development Cycle

Obligatory

Optional

	Description	Process	ISO Level	Input	Decision	Product
Proposal stage (10)	Confirm that a new International Standard in the subject area is needed	Informal	WG (1-5) (SC-27)	Expert	Expert	New Work Item Proposal (NWIP)
Preparation stage (20)	Experts collaborate on the proposed technical content.	Informal / Formal	WG (1-5) (SC-27)	Expert	Expert	Working Draft (WD1-xx)
Committee stage (30)	The draft from the working group is shared with the members of the committee.	Formal	SC-27 Committee	Expert/ Member	SC-27 Member	Committee Drafts (CD1-xx)
Enquiry stage (40)	Committee draft circulated to all ISO members	Formal	ISO	ISO Member	ISO Member	Draft Standard (DIS 1-xx)
Approval stage (50)	Draft standard circulated to all ISO members	Formal	ISO	-----	ISO Member	Final Draft Std (FDIS)
Publication stage (60)	Final document submitted for publication	Formal		-----	-----	International Standard (IS)

Note: Member = National Body (one vote per member country)

Key Principles:

1. ISO standards respond to a need in the market
2. ISO standards are based on global expert opinion
3. ISO standards are developed through a multi-stakeholder process
4. ISO standards are based on a consensus

EagleView Associates LLC

Background - ISO/IEC JTC 1/SC 27
Information technology – Security techniques

ISO Subcommittee responsible for the development of standards for the protection of information and information communications technology (ICT).

Organization - 5 working groups

1: Information security management systems - **Development of ISMS (Information Security Management System) standards and guidelines (see SC 27 N5114) such as ISO/IEC 27000 ISMS standards family.**

2: Cryptography and security mechanisms - **standardization of IT Security techniques and mechanisms, including terminology, general models and standards for these techniques and mechanisms for use in security services.**

3: Security Evaluation, Testing and Specification - **security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products.**

4: Security controls and services - **development and maintenance of standards and guidelines addressing services and applications supporting the implementation of control objectives and controls as defined in ISO/IEC 27001.**

5: Identity management and privacy technologies - **development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data.**

INCOSE and ISO/IEC JTC 1/SC 27

Strategy

Influence the growing body of security related standards to reflect a systems approach rather than allowing the standards develop in a more insular direction.

Approach

Selectively participate in standards developments that further vision guided by INCOSE interests where:

- ***Participation will benefit INCOSE within established priorities:***
  - **System thinking concepts and terms**
  - **"Core"SE process domains (Process, Requirements, Risk, etc)**
  - **Emerging technology applications**
    - ***Connected vehicles***
    - ***Critical Infrastructure***
    - ***"Smart City", "Smart Grid", etc***
- ***INCOSE has the expertise and resources to provide a meaningful input through its chapters, WGs, and members***
- ***Opportunities are presented to further collaboration with other organizations (for example NDIA).***

EagleView Associates LLC

Intersection of SC 27 projects and INCOSE interests (Sample)

INCOSE			ISO SC-27 Meeting 4-8 May - Agenda Items	Kuching, Malaysia
Interest	ISO Document	Version	Title	Status
Strong				
Maybe				
			ISO/IEC JTC 1/SC 27/WG 1 - Information security management systems	
X	**ISO/IEC 27000**		**Information security management systems — Overview and vocabulary**	**Revision**
X	**ISO/IEC 27003**	**rev 1**	**Information security management system – Guidance**	**1st CD**
X	ISO/IEC 27004	rev 1	Information security management systems — Monitoring, measurement, analysis and Evaluation (new title)	1st CD
X	**ISO/IEC 27005**	**Rev (?)**	**ISMS – Information security risk management**	**3rd WD**
	ISO/IEC 27006	rev 1	ISMS – Audit / Certification	2nd CD
	ISO/IEC 27007		Information Security Management Systems - Auditor Guidelines	1st WD
	ISO/IEC 27008		Guidance for Auditors on ISMS controls	1st WD
X	ISO/IEC 27009		Sector-specific application, of ISO/IEC 27001 - Requirements	2nd CD
	ISO/IEC 27010		Information security management for inter-sector and inter-organisational communications	DIS
	ISO/IEC 27011		ISMS – Management guidelines for telecommunications organizations	2nd CD rev 1
	ISO/IEC 27013		ISMS – Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	DIS
	ISO/IEC 27017		ISMS – Code of practice for information security controls for cloud computing services	DIS
X	ISO/IEC 27019		Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry	Revision
X	ISO/IEC 27021		ISMS – Requirements for the Certification of Information Security Management Specialists	1st WD
X	**(ISO/IEC 27000)**		**WG1 Vocabulary Editing Document**	**Study period contributions**
X			Future version development of ISO/IEC 27000	Study period contributions
X			**Cloud Adapted Risk Management Framework (joint with WG4)**	**Study period contributions**

Priorities = Process, Requirements, Risk

Eagle View Associates LLC

Standards Initiatives - ISO/IEC JTC 1/SC 27

Intersection of SC 27 projects and INCOSE interests

INCOSE Interest	ISO Document	Version	ISO SC-27 Meeting 4-8 May - Agenda Items Title	Kuching, Malaysia Status
Strong				
Maybe				
			ISO/IEC JTC 1/SC 27/WG 3 - Security evaluation, testing and specification	
	ISO/IEC 19792		Security evaluation of biometrics	
			ISO/IEC JTC 1/SC 27/WG 5 - Identity management and privacy technologies	
	ISO/IEC 24745		Biometric Information Protection	
	ISO/IEC 24761		Authentication context for biometrics	
	ISO/IEC 24760-1		A Framework For Identity Management – Part 1: Terminology and Concepts	
	ISO/IEC 24760-2		A Framework For Identity Management – Part 2: Reference Architecture and Requirements	
	ISO/IEC 24760-3		A Framework For Identity Management – Part 3: Practice	
	ISO/IEC 29100		Privacy Framework	
	ISO/IEC 29101		Privacy Architecture Framework	
	ISO/IEC 29146		A Framework for Access Management	
	ITU-T X.1085 (X.bhsm) ISO/IEC 17922		Telebiometric authentication framework using biometric hardware security module	
	ISO/IEC 29151		Code of practice for the protection of personally identifiable information	
	ISO/IEC 29115		***Entity Authentication Assurance Framework***	***Study period contributions***
			Guidelines for data pseudonymization and anonymisation processes as privacy enhancing techniques	***Study period contributions***
			Privacy Engineering Framework	***Study period contributions***

Conclusions

- ✓ Security standards concepts and terms need to be internally consistent and compatible with other SE domains
- ✓ INCOSE can add value to the ongoing dialogue around security-focused standards and serve as a bridge between the system engineer and the security community.

Ken Kepchar ESEP, CISSP
Co-Chair INCOSE System Security WG
INCOSE Representative to ISO/IEC JTC1 SC 27
703-346-7706
eagleview2@cox.net