



# ISO SC27 Security Techniques and ISSA Category C Liaison

Eva Kuiper, CISSP-ISSAP, CISA

# What is ISO SC27?

ISO SC27 develops International Standards in IT Security Techniques. Traditionally, these have covered:

- Identification of generic requirements (including requirements methodology) for IT system security services
- Development of security techniques and mechanisms
- Development of security guidelines
- Development of management support documentation and standards (e.g. terminology and security evaluation criteria)
- Standardization of cryptographic algorithms for integrity, authentication, non-repudiation services, and confidentiality services.

# What is a Category C external liaison?

- ISO liaison membership has no power of vote, but has some options to attend meetings and receive documents
- An effective liaison needs to operate in both directions
- Three categories for external organizations
  - A – participates actively in the work of JTC1 or SCs for most of the questions dealt with by the committee
  - B – Organizations that have indicated a wish to be kept informed of the work of JTC1 or any of its SCs
  - C – Organizations which make an effective technical contribution and participate actively at the WG or project level of JTC1 or its SCs

# ISSA and ISO SC27 Liaison

- Category C liaison request from ISSA to SC27 February 2005
  - Submitted by George Mathanool, Vice President, International Relations & Development
  - Balloted in ISO and approved by JTC1 in fall 2005, with George Mathanool appointed liaison from ISSA to SC27
  - Meeting with George in Kuala Lumpur, November 2005
  - Liaison from SC27 to ISSA balloted and appointed by SC27 in May 2006 – Eva Kuiper

## What's been happening in SC27 that ISSA members should care about?

- ISO/IEC 17799 – originally BS7799-1, fast tracked in 2000, revised in 2005
- ISO/IEC 27001 – originally BS7799-2, accelerated review in 2005 leading to publication in late October 2005

# Network Security topics

- New set of standards numbered ISO/IEC 18028-1 to 18028-5 developed on Network Security topics:
- 18028-1:2006 Network Security Management
- 18028-2: 2006 Network Security Architecture
- 18028-3:2005 Securing communications between networks using security gateways
- 18028-4:2005 Securing remote access
- 18028-5 FDIS vote just completed

# Selection of topics recently completed

- ISO/IEC 18043 – Selection deployment and operations of intrusion detection systems (IDS)
- ISO/IEC 18045 – Methodology for IT Security Evaluation
- ISO/IEC 15408-1,2,3 ISO version of Common Criteria
- ISO/IEC TR 15443-1,2,3 A Framework for IT Security Assurance
- ISO/IEC 13335-1 Concepts and models for information and communications technology management

# SC27 has been growing, requiring new WGs to be created



- WG1 has been split and a new WG4 focused on “how-to” types of guidance documents has formed
  - Network security, intrusion detection, and other detailed security guidance will move to WG4
- WG5 has formed to deal with Identity Management and (potentially) Privacy guidance
- WG2 and WG3 remain intact, WG2 still focusing on Cryptography and WG3 on evaluation and assurance

# Newer areas where ISSA experts can add value



- Disaster recovery
- Biometrics
- Measurements
- ISMS implementation guidance
- Identity management

# Disaster Recovery

## ISO/IEC 24762

- Guidelines for information and communications technology disaster recovery services
- Scope – this standard specifies the guidelines for the information & communication technology disaster recovery (ICT DR) services, focusing on the desired disaster recovery (DR) facilities and services capability. It deals with the provision of fallback and recovery support to an organization's information and communication system, including test, implementation and execution aspects of disaster recovery. This standard focuses on ICT DR services and does not include guidelines in other areas of business continuity management
- Achieved 1<sup>st</sup> CD approval at May plenary, request for comments will be coming out this summer. Due date for comments will be due in fall. There is still an opportunity to review during CD comment period

# Authentication context for Biometrics

- ISO/IEC 24761- Authentication context of biometrics
- Interesting area for SC27, few experts with expertise in both biometrics and security
- Scope – This document defines the structure and the data elements of Biometric Authentication Context (BAC). The structure is based on the following two assumptions:
  1. The target biometric verification process consists of five sub processes: data collection, signal processing, storage, matching, and decision.
  2. BAC is generated by each entity, the subject that executes some of these sub processes.

Current status: 1<sup>st</sup> CD as of May Plenary, opportunity to submit comments in time for fall meeting

## Other biometric work

- ISO/IEC 19792 – Security evaluation of biometrics – current status: CD
- ISO/IEC 24745 – Biometric template protection

# ISO/IEC 27000 family of standards

- ISO/IEC 17799 (also known as 27002) and ISO/IEC 27001 are not the end of the story...
- Goal is to have a family of standards on Information Security Management Systems
- Vocabulary, guidance, measurements are ongoing projects
- WG1 has been split into two groups
  - WG1 will focus on ISMS-related topics – 27000 and related documents remain in WG1
  - New WG4 will focus on security technology documents, “how-to” focus (e.g. network security)

# ISO/IEC 27000

- Information security management system fundamentals and vocabulary
- New work item, just initiated, still being defined, lots of room for comment and improvement.

# ISO/IEC 27003

- Information security management system implementation guidance
- Scope – the proposed work item will provide help and guidance in implementing the Information Security Management System (ISMS) requirements for ISO/IEC 27001. The proposed work item will provide further information about using the PDCA model and give guidance addressing the requirements of the different stages of the PDCA process to establish, implement and operate, monitor and improve the ISMS.
- Status
  - this is currently only a WD
  - Lots of opportunity for people familiar with implementing an ISMS within their organizations to contribute

# ISO/IEC 27004

- Information security management measurements
- Scope – this ISO/IEC Standard specifies measurements and provides guidance concerning measurement techniques applicable for determining and describing the efficiency and effectiveness of information security management systems. It includes resources (information security controls), and activities (information security processes and procedures). The measurements mainly support the “Plan” (design) and “Do” components (implement and operate the ISMS) as input to the “Check” (monitor and review) components of an ISMS, with the goal of providing a means for taking decisions at the “Act” (maintain and improve the ISMS) stage, leading to continuous improvement of the ISMS cycle.
- Status
  - Still in WD
  - Hope to go to CD stage in fall
  - Plenty of room for input during the next comment period

# ISO/IEC 27005

- Part 2 (formerly ISO/IEC 13335): Techniques for information and communications technology security risk management
- Scope – ISO/IEC 27005 provides techniques for information security risk management that includes information and communications technology security risk management. The techniques are based on the general concepts, models, and management and planning guidelines laid out in Part 1 of this International Standard. These guidelines are designed to assist the implementation of information security. Familiarity with the concepts and models, and the material concerning the management and planning of information security in ISO/IEC 13335-1, is important for a complete understanding of Part 2.
- Current status:
  - CD
  - Plans to move to FCD in fall with sufficient support
  - Should be reviewed, but major changes are not likely

# Cryptography topics

- Deep dive into Cryptography in WG2
- ISSA could cover these topics under one team leader
- Requires intimate familiarity with cryptography algorithms
- Team should consist of members doing research in cryptography

# ISO/IEC 24760

- A Framework for Identity Management
- Scope – this standard aims to provide a framework for the definition of identity and the secure, reliable, and private management of identity information. This framework should be applicable to individuals as well as organizations of all types and sizes, in any environment and regardless of the nature of the activities they are involved in.
  - Areas to be considered
    - Secure management of identities
    - Identification process leading to authentication
    - Information associated with identification of an entity within a context
    - Identity attributes
    - Policy-based roles
    - Identity management systems
- Status
  - This is a brand new project. Original framework document was proposed by US NB in conjunction with The Open Group. TOG is participating actively in this project through review and submissions
  - This project will probably lead to other documents
  - Identity and Privacy were split off into an new Working Group, WG5, within SC27

# Potential new areas

- ISSA GAISP
  - Still in strawman stage
  - Is there an area within ISO where this could find a home?
  - Precedent set by ISSEA with ISO/IEC 21827 (SSE-CMM)

# ISSA plans for contribution

- Internal ISSA planning on next steps
  - George Mathanool, Hal Tipton, Eva Kuiper
    - Choose a few projects where ISSA can contribute
    - Recruit team leaders for the projects
    - Communicate ISO schedule to team leaders
    - Train team leaders on comment coordination and submission process
    - Collect and package inputs from team leaders
    - Submit comments to ISO for fall meeting
    - Begin the cycle again for spring meeting, etc.
- Expectations from JTC1 for retaining Category C liaison
  - Liaison activity is reviewed on a two-year cycle to assure that the liaison group is, in fact, actively participating
  - ITTF will reaffirm liaison status if there is continued evidence of active participation in the work of a WG or project

# Format of review teams

- Teams should be large enough to achieve a balanced consensus, but small enough to work effectively
- Team members should commit to active participation so that we don't jeopardize our liaison status
- Members should be able to follow a project to completion
- No requirement to attend ISO or NB meetings or deal with letter ballots, but some consensus mechanism should be in place (don't want a single person's opinions...)
- Focus on one SC27 project per team (much more efficient than splitting effort over many projects)
- Choose projects where ISSA can make a contribution (new projects, projects where ISSA members have demonstrated expertise)
- Planning for how to choose projects is currently underway



# Questions?