



# ISO/IEC 17799: 2005

Alice Sturgeon

Enterprise Architecture  
and Standards Division

CIO Branch

**June 2005**



# Outline

---

- Background
- Revision of 17799: 2000
- Current status
- Path Forward
- Q&A



# Too many acronyms!

---

- ISO: International Standardization Organization
- IEC: International Electro-technical Commission
- JTC1: Joint Technical Committee – 1
- CAC-ITS: Canadian Advisory Committee – Information Technology Security
- SCC: Standards Council of Canada
- ISMS: Information Security Management System

...etc.



# What is a “Standard”?

---

A consensus specification resulting from an open, formal development, balloting and review process

- A Standard may be a lengthy document (e.g., ISO/IEC 17799) or it may be a short protocol (e.g., IETF RFC 3874).
- It may be a detailed specification or a high-level management guide.



# Why develop and use standards?

---

- ✓ Facilitate interoperability, common language and understanding
- ✓ Remove barriers to trade
- ✓ Facilitate inter-working in common areas
- ✓ For the user, or buyer, to reduce the risk and eliminate uncertainty – not taking a chance on an unknown.
- ✓ Common foundation for sharing information or services, and provide assurance in security functionality.
- ✓ Enable electronic communication and transactions, by providing authentication, authorization and assurance



# Why Standards? (2)

---

## The 4-Ms:

- Meaningful: for those who use them, understandable and relevant
- Measurable: behaviours that can be observed in action
- Monitorable: recognized processes for compliance
- Manageable: framework for establishing and monitoring the use and effectiveness of standards

## Thought du jour:

- Standards are generally required when excessive diversity creates inefficiencies or impedes effectiveness

Source: Edward W. Hammond and James J. Cimino, *Standards in Medical Informatics* (Springer, 2001)



# Standards Development Bodies

- Governments
  - TBS, CSE, RCMP, U.S. NIST
- National/ Regional
  - CSA, BNQ, CEN, APEC
- International
  - ISO, IEC, ITU, UN
- Professional Associations/ Consortia
  - IETF, W3C, OASIS, BCC
- De facto
  - Microsoft, Linux



# Legislation and Standards

---

## In Canada,

- Privacy Act
- PIPEDA
- Security of Information Act
- Emergency Preparedness Act (rev.)

## In the U.S.A.,

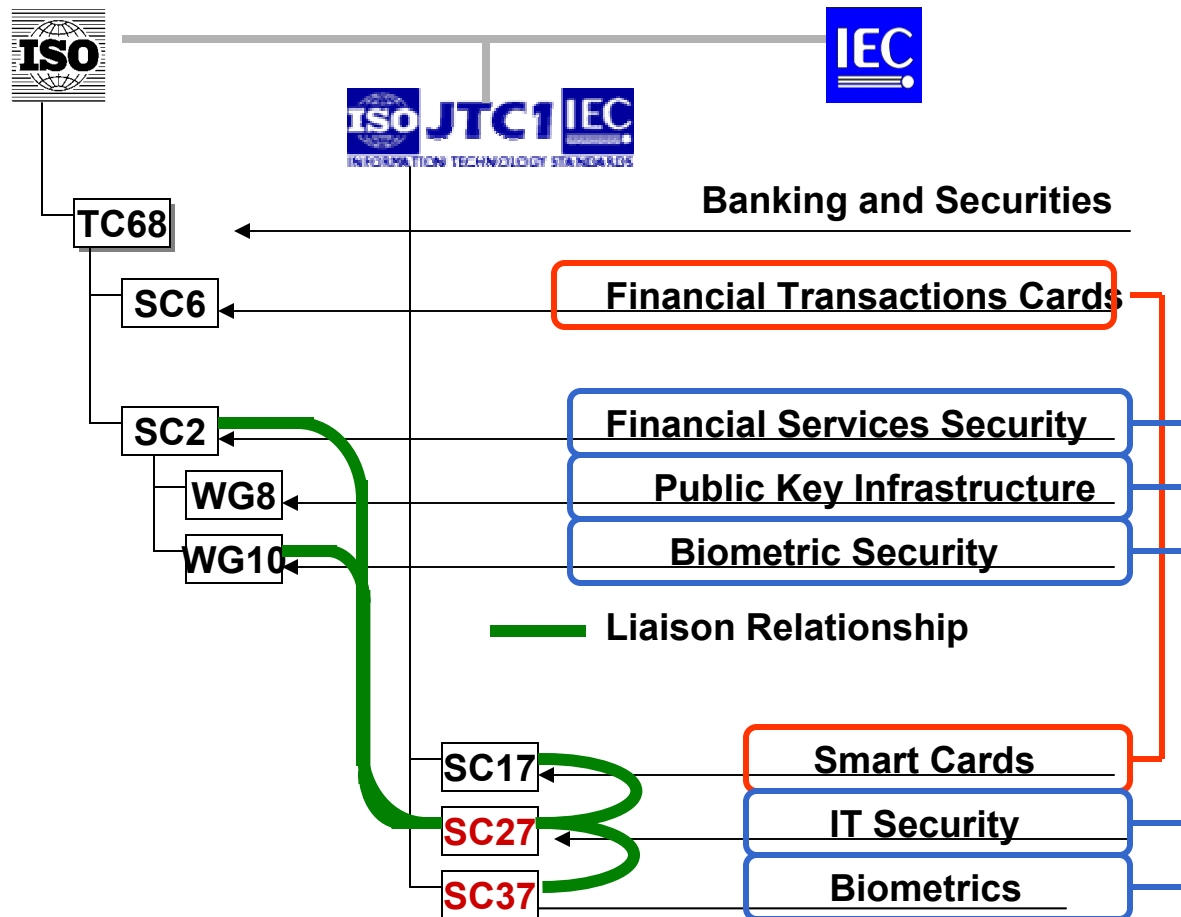
- Sarbanes-Oxley
- Gramm-Leach-Bliley
- Clinger-Cohen Act
- USA Patriot Act



# ISO/IEC

- ISO – International Standardization Organization
  - Established in 1946, more than 200 TCs – and one JTC
  - 14,000 standards, 148 member nations
    - TC 1 – Screw threads
    - TC 121 – Anaesthetic and respiratory equipment
    - TC 147 – Water quality
    - TC 223 – Civil defense
- IEC – International Electro-technical Commission
  - Established in 1944, more than 100 TCs – and one JTC
    - Addressing many disciplines, from marine instrumentation to nuclear power supplies, to lamps
- JTC 1 – Joint Technical Committee # 1 – Information technology
  - And there is only one

# ISO/IEC JTC1



# SC 27 IT security techniques

- 32 P-members
- Semi-annual meetings
- 95 projects, 40 active, 45 publications
- Voluntary participation
- Three Working Groups
- Liaison with other JTC 1 Sub-Committees and other groups,
  - e.g. Common Criteria Development Board, Europay-Mastercard-Visa (EMV) standards body

# SC 27/WG 1 Management guidelines

Recently completed projects include:

- ISO/IEC 13335-1 Management of information and communications technology (ICT) security – Part 1: Concepts and models of information security; Canadian editor
- ISO/IEC 18044 Information security incident management
- ISO/IEC 15816 Security information objects for access control (ITU-T X.841)
- ISO/IEC 15945 Specification of TTP services to support the application of digital signatures (ITU-T X.843)
- ISO/IEC TR 14516 Guidelines on the use and management of Trusted Third Party services (ITU-T X.842); Canadian editor

Current projects include:

- 18028, 5 Parts – Network security
- 18043 Implementation, operation and management of intrusion detection systems (IDS)

# SC 27/WG 2 Cryptographic techniques

Largest number of projects, including:

- 18031 Random bit generation; Canadian editor
- 18032 Prime number generation
- 18033 Encryption algorithms, with four Parts, including asymmetric, block and stream ciphers
- 18014 Time-stamping services, with three Parts
- 15946 Cryptographic techniques based on elliptic curves, with four Parts
- 9796 Digital signature schemes giving message recovery
- 9798 Entity authentication, with six Parts: New Part 6 is based on wireless research
- 11770 Key management, with three Parts
- 19772 Data encapsulation mechanisms ...etc.

# SC 27/WG 3 Assurance

- ISO/IEC 15408 – Common Criteria for IT Security Evaluation
- ISO/IEC 18045 – Common Evaluation Methodology
- ISO/IEC 19790 / U.S. NIST FIPS 140-2 – Security Requirements for Cryptographic Modules; Canadian editor
- ISO/IEC 19791 – Operational Systems Evaluation; Canadian contributor
- ISO/IEC 19792 – Framework for security evaluation and testing of biometric technologies; Canadian contributor
- ISO/IEC TR 15446 Guide on the production of protection profiles and security targets
- ISO/IEC TR 15443 Framework for IT security evaluation, with three parts; two Canadian editors



# Some more WG1 Projects...

---

- Revision of ISO/IEC 17799: 2000
- Revision of ISO/IEC 13335 – Parts 1 and 2
- Information Security Management System
- Roadmap



# Revision of 17799: 2000

---

“Code of practice for information security management”

- Fast-tracked into ISO from BS 7799 Part 1 in 2000
- Canada, and six other NBs, voted against adoption:
  - Revision needed to elevate the content to international level and remove British specificity
  - Outdated overview of security attributes
  - Topics missing that are critical to current electronic environment
  - Split into centralized vs distributed IT approaches



# Content of 17799: 2005

---

- Follow ISO format
- Remove introductory material
- Format for each section and sub-section:
  - Objective
  - Control
  - Implementation guidance
  - Other information
- Version mapping annex



# 2005 Version, continued

---

Example: 2000 Clause 9 Access control =  
2004 version Clause 10 Access control:

## **10.1 Business requirement for access control**

### Objective:

To control access to information – Access to information and business processes should be controlled on the basis of business and security requirements.

This should take into account policies for information dissemination and authorization.

### **10.1.1 Access control policy**

Control – Business requirements for access control should be defined and documented.

Implementation guidance – etc.

Other information – etc.

### **10.2 User access management**

Objective – To prevent unauthorized access to information systems.

Implementation guidance – etc.

Other information – etc.



# ISO/IEC TR 13335

---

## Guidelines on the management of IT security (GMITS) (published 1996-2000)

- Part 1: Concepts and models
- Part 2: Management and planning
- Part 3: Techniques for IT security management
- Part 4: Selection of safeguards
- Part 5: External connections

*Now looking like .....*



# ISO/IEC 13335

## Management of information security (MIS)

- Part 1: Concepts and models
- Part 2: Information security risk management
  - Canadian editor, both parts
- Current Technical Report 13335 – Part 4: merged with new Part 2
- Current TR 13335 – Part 5: revision 2004
  - This will be withdrawn in view of ISO/IEC 18028 Network security



# ISO/IEC 27001 ISMS

---

- Information Security Management System
- ISO Guide 72 similar to ISO 9001 & ISO 14001
- Based on revised 17799 and MICTS, British Standard 7799 Part 2
  - Canadian participation



# ISO/IEC 27001 ISMS - Scope

- This standard covers all types of organizations (e.g., commercial enterprises, government agencies, not-for-profit organizations).
- This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of an organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.
- The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties. (ISO/IEC 17799 provides implementation guidance that can be used when designing controls.)

# ISO/IEC 27001 ISMS - Content

- Normative references:
  - 17799 (2005), ISO Guide 73 Risk terminology
- Definitions, including ISMS:
  - That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
    - ✓ NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.



# ISMS Content – 2

---

1. Scope
2. Normative References
3. Definitions
4. ISMS
  1. General requirements
  2. Establishing and managing the ISMS  
Includes establish, implement, operate, monitor, review, maintain and improve
  3. Documentation requirements
5. Management responsibility



# ISMS Content – 3

---

6. Internal ISMS audit
7. Management review of the ISMS
8. ISMS Improvement

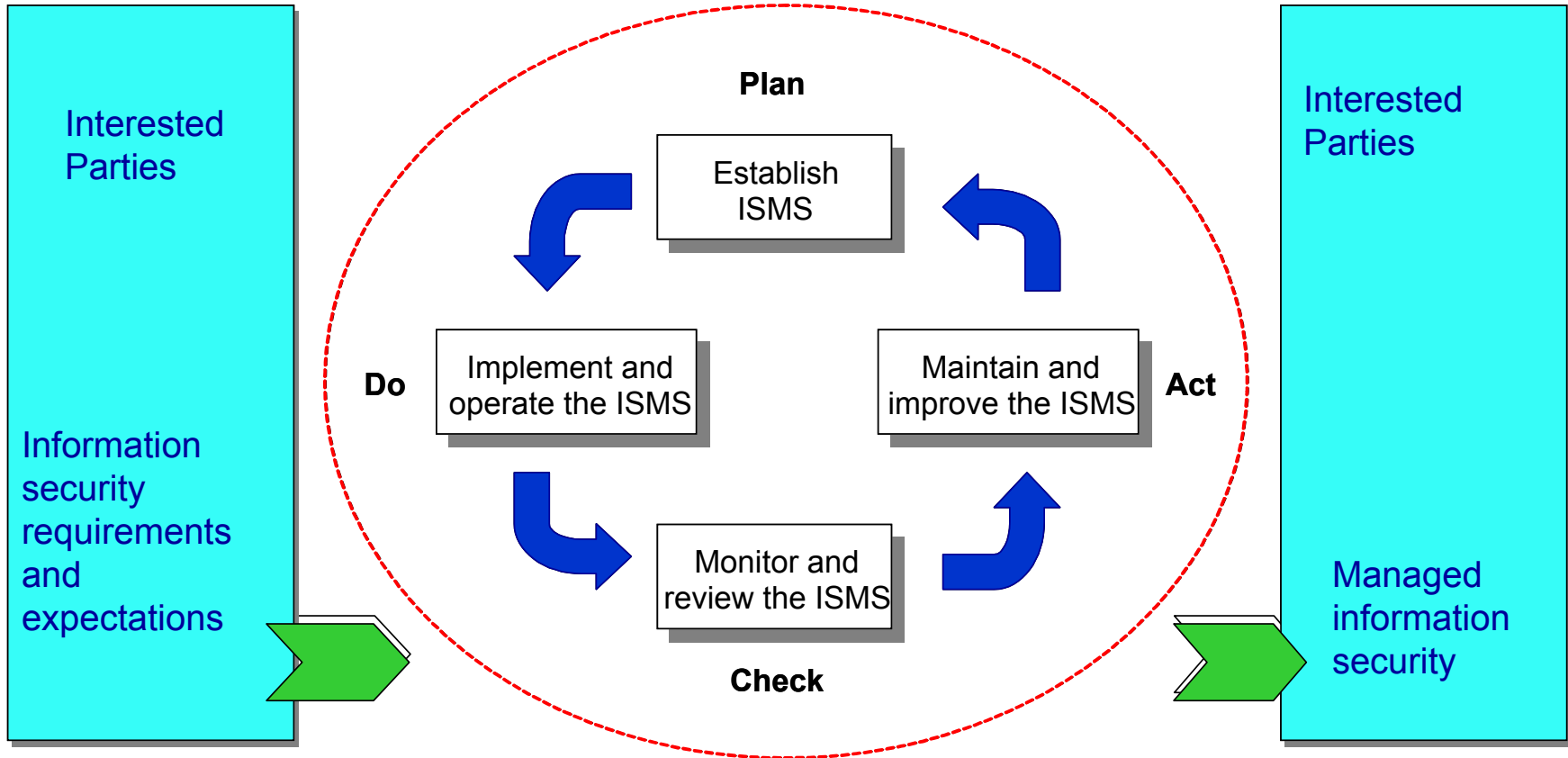
Annex A Control objectives and controls

Annex B OECD principles and this standard

Annex C Correspondence between ISO 9001: 2001, ISO 14001: 1996 and this standard

Bibliography

# PDCA Model



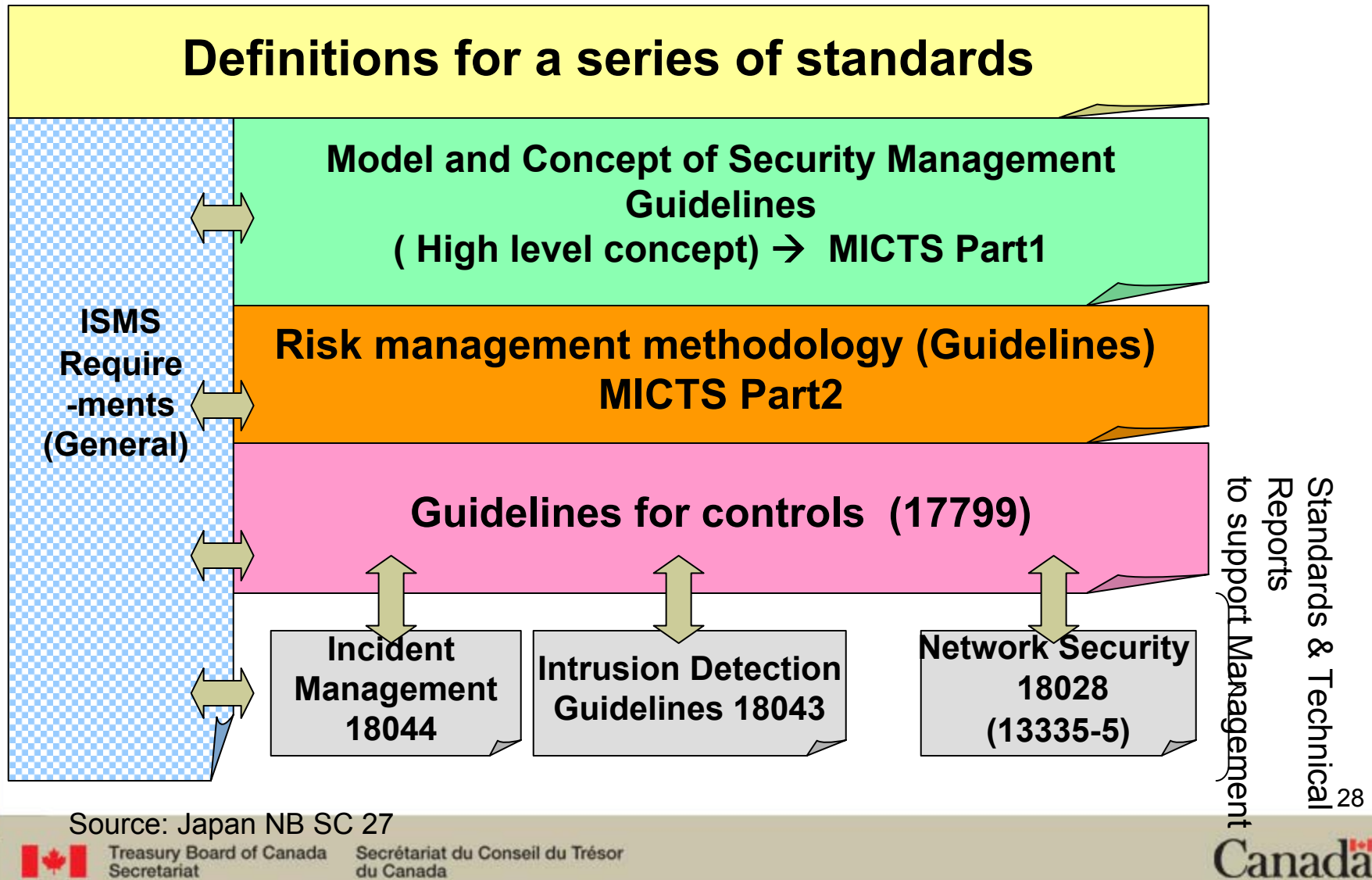


# ISO/IEC 27004 ISMS Metrics

---

- Based partly on NIST SP 800-55 – Security Metrics Guide for IT Systems
- At an early stage still
- Necessary to provide KPIs (Key Performance Indicators) and methodology to address them
  - Canadian participation

# Early SC 27/WG 1 Roadmap





# Current Roadmap

---

## Family of 27000 standards:

- 27000 – Concepts, models, terminology and definitions
  - 27001 – ISMS (changed from 24743)
  - 27002 – ISO/IEC 17799 (2005), by 2007
  - 27003 – Information security risk management
  - 27004 – ISMS Metrics
  - 27005 – ISMS Implementation guidance
  - 27006 – TBD
- Canada leading Study Period on moving 13335 into the 27000 family



# Impact

- SC 27 member nations, and others, are adopting 17799
  - Many had adopted BS 7799-1 as national standard
- Plan to adopt ISMS
  - Many had adopted BS 7799-2 as national standard
- ISMS and 17799 – reborn as 27001 and 27002 – are becoming recognized and accepted global information security standards
- Competition and trade regime
- Emergence of global and national ISMS Users Groups
  - Including Canada

# Potential Information security certifications

- ISO/IEC 27001 ISMS
- ISO/IEC 27002 Code of practice for information security management
  - with*
  - ISO/IEC 27000 Principles, concepts, terminology
  - ISO/IEC 27003 Information security risk management
  - ISO/IEC 27004 ISMS Metrics
    - with*
    - ISO/IEC 15408 – Technical system and product security functionality and assurance
    - ISO/IEC 19790 – Cryptographic modules
      - with*
      - ISO/IEC 19791 – Operational system security
      - ISO/IEC 18045 – Common evaluation methodology
      - ISO/IEC 19792 – Framework for security evaluation and testing of biometric technologies



# Biometric Security Standardization

---

- ISO/IEC JTC 1/SC 27 – IT Security techniques
  - ISO/IEC 19792 Framework for security evaluation and testing of biometric technologies
  - Biometric evaluation methodology (BEM) in CCDB
  - Biometric template protection
  - Biometric authentication context
- ISO/IEC JTC 1/SC 37 – Biometrics
- ISO TC 68/SC 2 – Financial Systems Security:
  - ISO 19092 – Biometric information management & security (based on U.S. ANSI X9.84)

# ISO/IEC JTC1 SC 37 – Biometrics

- Inaugural Plenary December 2002
- Six Working Groups:
  - WG 1 – Harmonized Biometric Vocabulary
  - WG 2 – Biometric Technical Interfaces
  - WG 3 – Biometric Data Interchange Formats
  - WG 4 – Biometric Application Profiles
  - WG 5 – Biometric Testing and Reporting
  - WG 6 – Cross-Jurisdictional and Societal Aspects
    - ✓ 24714 Cross-jurisdiction and societal impacts of implementations of biometrics



# For more information:

---

Alice Sturgeon  
Senior Director, Architecture Domains  
Enterprise Architecture and Standards Division  
CIOB/TBS  
613-948-9475  
[Sturgeon.alice@tbs-sct.gc.ca](mailto:Sturgeon.alice@tbs-sct.gc.ca)