



ISO/IEC 17799 (seventeen seven nine nine) Code of Practice for Information Security Management

Bruce Hunter
Chief Information Officer Branch
Treasury Board Secretariat

Canada



Outline

- Status of ISO revision to 17799
- The GoC IT Security context
- How to apply 17799 within the GoC?



Revision of ISO/IEC 17799 (2000)

- Although several countries, including Canada, voted against 17799 (2000), there is a strong international commitment to revise 17799 to correct major deficiencies
- GOC has been a major contributor to the revision
- International Standards take time.
 - Review of 1st Committee Draft (CD) completed in October 2003 in Paris
 - 2nd CD draft scheduled for Feb 2004
 - **Dec 2004 Earliest date for publication**

3



Revision of ISO/IEC 17799 (2000)

- Major improvements over 17799(2000)
 - but still approximately 1000 comments on latest draft
- Ongoing cooperative effort evident
- Strong commitment to meet origin schedule (Dec 2004), but this could be delayed. While there is high interest in its publication as soon as possible, the dilemma is:
 - extremely high level of interest
 - unprecedented volume of comments
 - desire for a high level of quality

4



Use of ISO/IEC 17799 in Canada

- ISO 17799 seems to be gaining acceptance in Canada.
 - To what extent and how is it used?
- CSO Magazine Survey
 - Using to meet certification 15%
 - As a starting point for security 54%
 - Other standards 12%
 - Not using any standards 19%
- It would be helpful if the user group provided information related to uptake of ISO 17799 in Canada.
 - To be meaningful, it would have to include a description of how 17799 is being applied

5



Use of ISO/IEC 17799 in Canada

Informal Survey: How are you using 17799?

1. Not yet, waiting to see? _____
2. Planning to use it? _____
3. As a reference or guide, along with other standards? _____
4. As the primary foundation for your information security program? _____
5. To obtain formal certification? _____

6



Other relevant standards: NIST

- ***Although 17799 is gaining acceptance, no one standard is widely accepted in North America (yet).***
 - there is a requirement to align with the US
- GoC is closely monitoring promising NIST standards, which closely reflect our needs. In particular they include:
 - Baseline security controls
 - Graduated levels
- Key NIST standards
 - FIPS 199 security categorization (low/med/high)
 - 800-37 certification and accreditation
 - 800-53 baseline security controls

7



Other relevant standards: BS7799-2

- ISO 17799 is a guide: “should” not “shall”
- BS 7799 Part 2 is a **certification** standard
 - Is a specification: uses “shall”
 - Is NOT an international standard
- ISO is studying the need for a **certification** standard for information security management system, similar to BS 7799 Part 2 and ISO 9000
- Canada has not supported this standard
 - Base standards are not yet widely accepted
 - Need to finish revision of 17799 and MICTS
 - Measurement of the effectiveness of security is an immature discipline; Better metrics required
 - Concern about costs and business case

8



Other relevant standards

- Information Security Forum Standard of Good Practise
- ISO Management of Information and Communications Technology Security (MICTS) (formerly ISO 13335 (GMITS))
 - Management processes (i.e. risk management)
- Generally Accepted Information Security Principles (GAISP) - under revision
- Others (COBIT, SSE CMM, OCTAVE ...)

9



Context for GOC IT Security Standards

- GoC security program already well established
- Three part IT Security strategy
 - Policy and Standards
 - Architecture, with focus on Business Transformation
 - Deployment of Secure Solutions (e.g. Secure Channel)
- Business Drivers
 - Government On Line
 - Critical Infrastructure Protection (OCIPEP)
 - Public Security and Anti-Terrorism (PSAT)
- Policy and legal framework
 - Revised Government Security Policy (Feb 2002)
 - Policy for Management of Govt Information (May 2003)



Government Security Policy (GSP)

- Policy Statements:
 - Baseline security requirements: mandatory minimum requirements
 - Continuous risk management
 - Continued delivery of services
- Some specific GSP requirements:
 - Business Continuity Planning
 - Heightened security levels in case of emergency and increased threat
 - Certification and Accreditation
 - Explicit inclusion of the Active Security Cycle
 - *Prevent, Detect, Respond, Recover*

11



GSP Security Standards

- Operational security standards
 - Readiness levels *new*
 - Personnel Security Screening *under revision*
 - Business Continuity Planning *new*
 - Physical Security *under revision*
 - Security in Contracting *future revision*
 - Security Risk Management *new (future)*
 - **Management of IT Security** *new (draft)*
- ITS standards program underway, starting with the Management of IT Security

12



Management of IT Security Standard

- A higher level standard to support the both the GSP and the Policy for Management of Government Information:
 - a capstone document as the starting point for establishing an IT Security program
 - is not a catalogue of controls
 - identifies high level mandatory (baseline) requirements

13



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Canada

Management of IT Security Standard

- Part 1: Context and key concepts:
 - Emphasis on business and service delivery
 - Holistic approach to IT security
- Part 2: Security organization and management
 - Roles of DSO, ITSC, CIO, senior management, program/business managers, IT operations
 - Security management processes (risk management, C&A, awareness, assessment and audit etc)
- Part 3: Technical and operational safeguards
 - Graduated safeguards
 - Enhanced direction on active security: Prevention, Detection, Response and Recovery (PDRR)

14



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Canada

GOC ITS Standards Program

- Other more detailed standards required for the following subject areas:
 - IT Security Zones: network security & perimeter defence
 - Risk Management, Threat and Risk Assessment
 - Certification and Accreditation
 - Self-assessment and audit guide: Self-assessment tool and question set based on maturity levels
 - Intrusion Detection: requirements to perform intrusion detection consistent with legal and policy requirements, including privacy
 - Incident handling
 - Other detailed technical documents and guides (Certificate Policies, Vulnerability Assessments etc)

15



Inter-jurisdictional Standards

- Use of ITS standards across federal, provincial, and municipal governments is being coordinated through National CIO Council Subcommittee for Information Protection (NCSIP)
- Strong support for ISO 17799 in provinces
- Related NCSIP initiatives:
 - Incident response coordination
 - Security classification guide
 - Guide for security agreements
 - **Self-assessment project: based on ISO 17799**

16



Revision of ISO/IEC 17799 (2000)

- The GOC is waiting for the revised standard
- We are just starting to determine how to apply 17799 when it is approved
- No commitment to adopt 17799 as a GoC standard at this time

17



How to apply 17799 in the GOC

- One cannot apply 17799 “as is”
 - Extensive effort is required to apply security within the the GOC legal, policy and business context
 - We are not starting from scratch; many 17799 controls are already well established in the GOC
- Controls by themselves are not enough
 - Must have sound (risk) management processes to select, apply, and review effectiveness of controls.
- Key questions:
 - Which controls are mandatory (baseline requirements)?
 - How robust do they need to be (graduated levels)?

18



How to apply 17799 in the GOC

- As a guide for departments who want to review and update their ITS program
- As a reference checklist as input to:
 - developing policies, standards, and guidelines
 - defining security requirements, C&A
 - assessments/reviews/audit
- As a basis for specifying or assessing security in external organizations:
 - Security in contracting
 - External interfaces and information sharing
 - “Mapping” security policies and practises

19



Conclusions

- 17799 (2000) is unacceptable: wait for the revised version
- GoC is reviewing how to use 17799 within the GOC context; no commitment to adopt it internally yet
- Must first establish an effective IT security program (organization and management processes)
- 17799 best suited as:
 - as a guide or reference document, in combination with other standards such as NIST standards
 - as a reference standard for security relationships with external organizations
- Since 17799 is widely adopted (?) GOC will have to recognize it even if we don't adopt it internally.
 - What does it mean to be “17799 compliant”?

20



Canada

ISO 17799 in Europe and Pacific Rim

- Rapidly becoming the de facto security standard
- Large multinationals have certified their security programs to demonstrate to potential business partners their security proficiency
 - Citibank, KPMG, Sony Electronics, Unisys...
- Taiwan, Singapore and Hong Kong - requiring companies to receive BS 7799 certification to do electronic transactions with the Government
- The foundation for a universal security standard?
- AIG is using ISO 17799 to measure the security of

ISO 17799 adopted as National standard in:

- Australia/New Zealand
- Brazil
- Czech Republic
- Finland
- Iceland
- Ireland
- Israel
- Netherlands (SPE 20003)
- Norway
- Sweden (SS 627799)



CONFIDENTIAL – Copyright Scienton Technologies Inc. © 2004



BS 7799 Certifications Worldwide (Jan 2004)

Japan 225	Norway 8	Iceland 3	Macau 1	UK 118	Australia 7	Brazil 2	Malaysia 1	Korea 20	Ireland 7
Denmark 2	Holland 1	Germany 17	Taiwan 7	Greece 2	Poland 1	India 16	Hungary 6	Mexico 2	Slovenia 1
Hong Kong 15	Argentina 1	Switzerland 2	South Africa 1	Italy 12	USA 5	UAE 2	Spain 1	Singapore 10	Sweden 4
Austria 3	China 5	Finland 8	Egypt 1	Absolute Total 513			Relative Total 517		



CONFIDENTIAL – Copyright Scienton Technologies Inc. © 2004



BS 7799 Certifications USA

Name of Company	Certificate Number	Certification Body
American Society of Quality	IS 60206	BSI
beTRUSTed Holdings Incorporated	0035	KPMG Audit plc
Equifax Secure Ltd	0017	KPMG Audit plc
Symantec Security Services	0005	KPMG Audit plc
The University of Texas	IS 53841	BSI

Projected Future State

- Public companies in NA will need to seriously manage the security of their information assets
 - Tangible and intangible
 - People, process, technology
- ISO 17799 compliance will be necessary to play in many markets for NA information intensive businesses
- ISO 17799 certification will be a discriminator

Enablers

- **ISO adopts BS 7799-2:2002 or equivalent**
 - NA establishes auditor and certification infrastructure
- **Privacy legislation**
 - PIPEDA (Canada)
 - HIPPA (health information)
 - GLBA (financial services)
 - FERPA (education)
 - Others?
- **Corporate governance**
 - Management due diligence
 - Trading partner agreements
- **Government procurements (US, Ontario) citing “best commercial practices” in information security**