

# **Revision of ISMS Standards ISO/IEC 27001 & 27002**

*Presented by: Philip Sy*



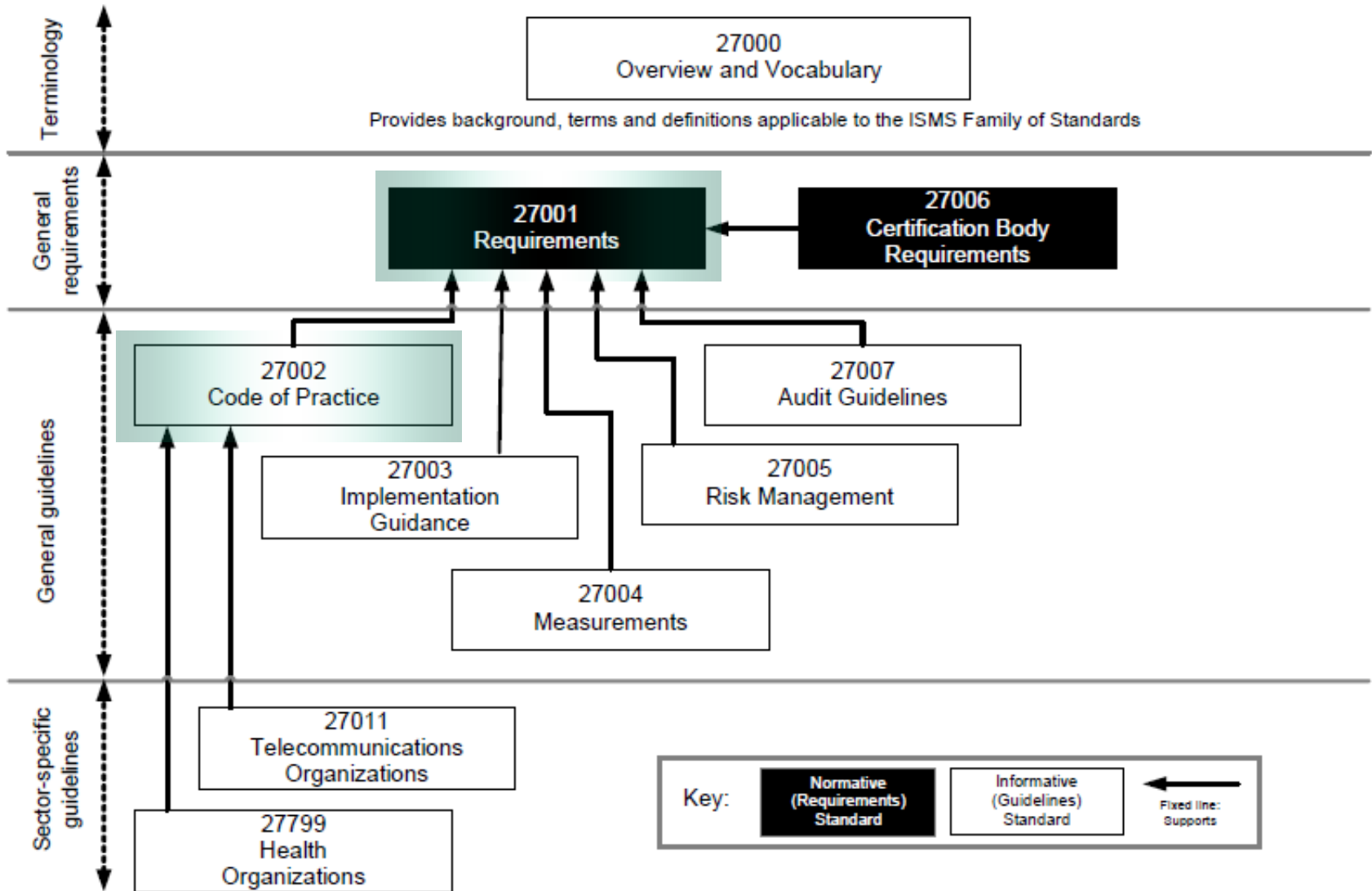
.....  
An industry partnership supported by IDA Singapore and SPRING Singapore

## Topics

- Background
- ISO/IEC 27001 - Direction of changes
- Open issues for 27001 revision
- ISO/IEC 27002 – Possible changes
- What does it mean to you?



## Core Standards of ISMS Series



## ISO/IEC 27001 – the specifications for ISMS

- specifies the requirements for information security management systems (ISMS)
- covers the establishment, implementation, operation, monitoring, review, maintenance and improvement of ISMS
- specifies requirements for the implementation of security controls customized to the needs of individual organization
- includes a set of controls for the control and mitigation of the risks associated with the information assets
- control objectives and controls listed in Annex corresponding to ISO/IEC 27002's best practices
- the only certifiable standard in ISO/IEC 2700x series of standards



## ISO/IEC 27002 – the best practices for information security

- provides a list of commonly accepted control objectives and best practice controls
- Is used as implementation guidance when selecting and implementing controls for achieving information security
- provides specific implementation advice and guidance on best practice in support of the controls specified in annex A of ISO/IEC 27001.

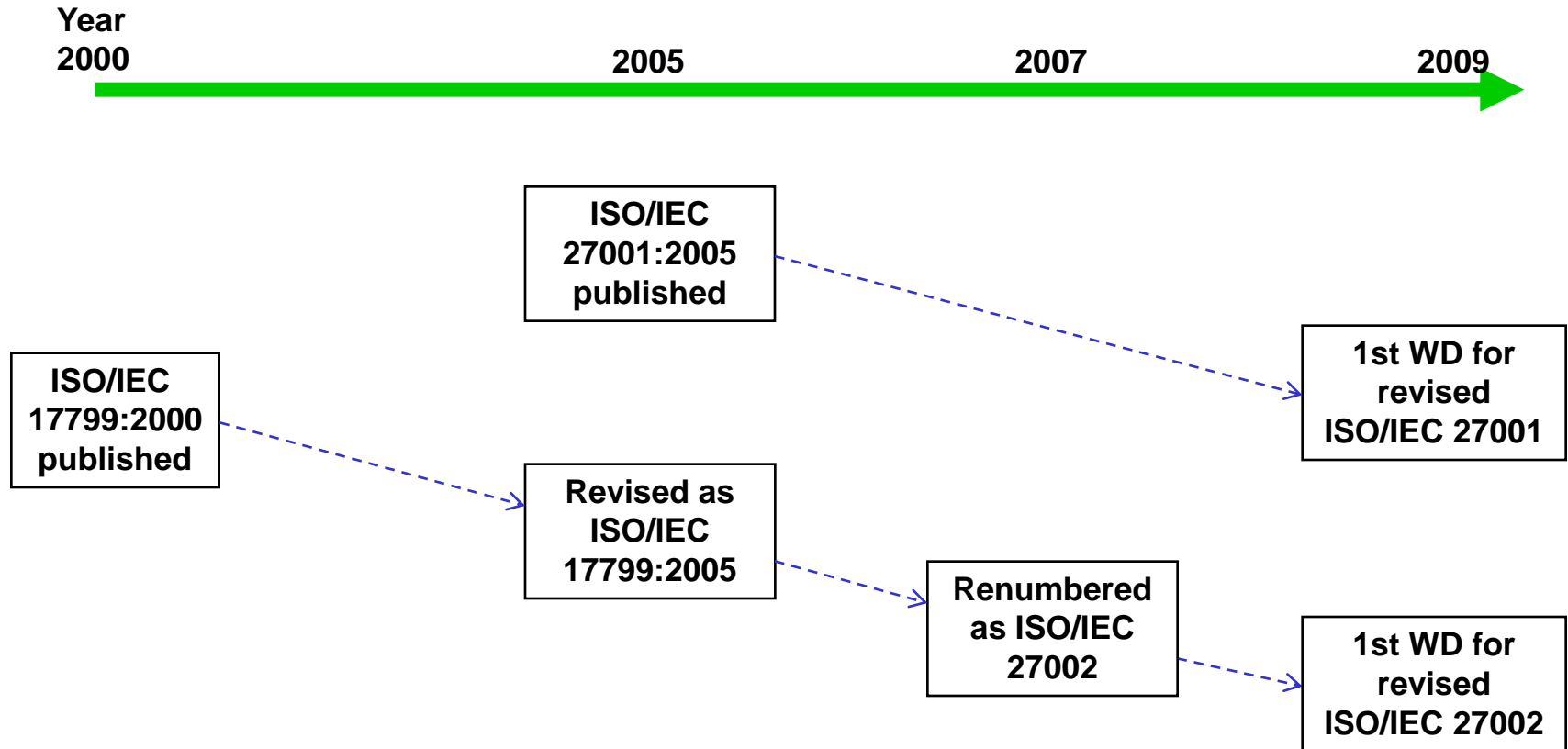


## Adoption of ISO/IEC 27001 and ISO/IEC 27002

- 5,822 accredited ISMS certificates issued worldwide based on ISO/IEC 27001
- Frequent criteria for qualification of suppliers of sensitive information system
- The only globally recognized information security certification for organizations
- Well accepted best practices adopted by most MNC
- Basis for various governments' security policies and/or best practices guidelines
- Popular reference for supplier audit and ICT system audit



## Milestones of ISO/IEC 27001/27002 Standards



## Topics

- Background
- ISO/IEC 27001 - Direction of changes
- Open issues for 27001 revision
- ISO/IEC 27002 – Possible changes
- What does it mean to you?



# Annex A and Relation with ISO/IEC 27002

- A list of control objectives and controls is necessary in ISO/IEC 27001 - there is a need for a unique controls set for comparability.
- Annex A is the basis for the first selection of controls, even if it is possible to use other control sets and add additional controls.
- Guidance for implementation of these controls can be found in ISO/IEC 27002. The link to ISO/IEC 27002 should remain as strong as it currently is. Detailed controls implementation guidance can come from other guides than ISO/IEC 27002.
- The normative reference to ISO 27002 should not be kept, because ISO/IEC 27002 is not indispensable to ISO/IEC 27001 as Annex A states the control objectives and controls.



# terms and definitions

- ISO/IEC 27000 should contain all the definitions of ISO/IEC 2700x standards.



# Relation with other ISO/IEC 2700x standards

- There is a need for clear distinction between the requirements in ISO/IEC 27001, their possible guidance in other documents (eg. ISO 27003, ISO 27005...), and guidance for controls implementation in ISO 27002. The revision process needs to identify what should be a requirement in ISO/IEC 27001 and what should be addressed in other guidance standards
- All guidance documents that have been developed in WG 1 for ISO/IEC 27001 (ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005) are guidance documents to support the implementation of ISO/IEC 27001. Therefore, the guidance documents should be aligned with ISO/IEC 27001, not the other way round.



## ISO/IEC 27001 structure

- It was agreed that the JCTG common structure of management systems standards should be used as the structure of ISO/IEC 27001.
- Comments have been provided to JTCG to make this structure better fitting to ISO/IEC 27001.



# ISMS policy vs information security policy

	"Global" level (full organization or part of it)	Specific / Local levels (single ISMSs)
Intent / Objectives – what is to be done ?	Information security policy ("global")	ISMS Policy / statement / ... (Specific ISMS policies)
Rules - how should it be done?	Information security set of rules ("global")	ISMS set of rules (specific)

- ISMS policy to be addressed in ISO/IEC 27001
- Information security policy and possibly other policies addressed in ISO/IEC 27002 specific controls.



# Information security risk management

- Risk management requirements will be specified in ISO/IEC 27001, keeping the same level of detail that is currently there
- The ISO/IEC 27001 risk management will be aligned with ISO 31000



## Topics

- Background
- ISO/IEC 27001 - Direction of changes
- Open issues for 27001 revision
- ISO/IEC 27002 – Possible changes
- What does it mean to you?



## Outsourcing

- Where an organization chooses to outsource any process that affects conformity to ISMS requirements, there are currently no defined requirements in the current ISO/IEC27001
- As outsourcing situations are becoming increasingly common, this topic should be addressed in ISO/IEC 27001



## Assets

- Currently, ISO/IEC 27001 simply addresses “assets” – it is difficult for users of the standard to understand the concept of what is an ISMS-relevant asset and what not, and what level of detail is suitable for the risk assessment. Should be making this clearer.



## Relationship between controls and assets

- Controls are selected to reduce risks, therefore the controls relate to particular assets. The relationship between controls and assets (e.g. individual ICT systems or groups of systems) should be made clearer.
- The risk assessment at the 'system' level should be integrated with the overall ISMS requirements and processes



## Management vs Top Management

- The text should make clear what type of management is addressed in the different situations, and it should also clarify whether addresses management related to ISMS scope or management of the whole organization.



## Topics

- Background
- ISO/IEC 27001 - Direction of changes
- Open issues for 27001 revision
- ISO/IEC 27002 – Possible changes
- What does it mean to you?



# Canada's suggestion of a brand new approach

## ISMS Taxonomy

Domain: 01 Security Strategy & Governance

Subsection	Title	Reference		Section	Title
		New	ISO27001		
1.1	All security domains integrated strategy	x			
1.1.1	All security domains strategy document	x			
1.1.1.1	Review of all security domains integrated security strategy document	x			
1.1.2	Supporting security philosophy & values	x			
1.1.2.1	Encompasses all domains of security	x			
1.2.2.2	Management commitment to security		x	A.6.1.1	Management commitment to information security
1.1.2.3	Security a business enabler	x			
1.1.2.4	Security integrated across all business functions	x			
1.2	All security domains security program design	x			
1.2.1	All security domains program charter document	x			
1.2.1.1	Security program vision & mission	x			
1.2.2.2	Security program concept of operations	x			
1.2.2.3	Security roles & responsibilities definition		x	A.6.1.2 A.6.1.3 A.6.1.6 A.8.1.1 A.8.2.1 A.13.2.1	Information security coordination Allocation of information security responsibilities Contact with authorities Roles and responsibilities Management responsibilities Roles and procedures
1.2.2.4	Security organisation structure	x			
1.2.2.5	Chief security officer	x			
1.2.2.6	Chief information officer	x			
1.2.2.7	Review of all security domains program charter document	x			
1.3	Organisation policies	x			
1.3.1	Information security policy		x	A.5.1	information security policy
1.3.1.1	Information security policy document		x	A.5.1.1	Information security policy document
1.3.1.2	Review of security policy document		x	A.5.1.2	Review of the information security policy
1.3.2	Access control policy		x	A.11.1.1	Access control policy
1.3.3	Responsibility for assets		x	A.7.1	Responsibility for assets
1.3.3.1	Ownership of assets		x	A.7.1.2	Ownership of assets
1.3.3.2	Acceptable use of assets		x	A.7.1.3	Acceptable use of assets
1.3.4	Information exchange policy		x	A.10.8.1	Information exchange policies and procedures
1.3.5	Other organisation policies	x			
1.3.5.1	Employee code of conduct	x			
1.4	Enterprise architecture	x			
1.4.1	Enterprise reference architecture	x			
1.4.1.1	Enterprise reference architecture document	x			
1.4.1.2	Review of enterprise reference architecture document	x			



# Canada's suggestion of a brand new approach

## ISMS Taxonomy

Domain: 06 IT Security

Subsection	Title	Reference		Section	Title
		New	ISO27001		
<b>Software Security</b>					
6.1	Information technology security standards and guidelines	x			
6.1.1	Information technology security standards and guidelines documentation		x	A.10.8.1	Information exchange policies and procedures
6.1.1.1	Review of IT security standards and guidelines documentation	x		A.11.4.1	Policy on the use of network services
6.2	Technical security architecture	x			
6.2.1	Enterprise architecture governance	x			
6.2.1.1	Architecture control board	x			
6.2.2	Application security architecture	x			
6.2.2.1	Application security architecture document	x			
6.2.3	Data security architecture	x			
6.2.3.1	Data model	x			
6.2.3.2	Data security architecture document	x			
6.2.4	Platform security architecture	x			
6.2.4.1	Platform security architecture document	x			
6.3	Security in the system development lifecycle	x			
6.3.1	Separation of development, test and operational environments		x	A.10.1.4	Separation of development, test and operational facilities
6.3.2	Planning for security in information systems		x	A.10.3	System planning and acceptance
6.3.2.1	Including cost of security in information system projects	x			
6.3.2.2	Consulting with security early in the SDLC	x			
6.3.3	IT security risk management in the SDLC	x			
6.3.3.1	Reviewing IT security risks in each system development phase	x			
6.3.4	Define information system security requirements		x	A.12.1	Security requirements of information systems
6.3.4.1	Information system security requirements analysis and specification		x	A.12.1.1	Security requirements analysis and specification
6.3.4.2	Technical security controls for sensitive systems	x			
6.3.5	Correct processing in applications		x	A.12.2	Correct processing in applications
6.3.5.1	Input data validation		x	A.12.2.1	Input data validation
6.3.5.2	Control of internal processing		x	A.12.2.2	Control of internal processing
6.3.5.3	Message integrity		x	A.12.2.3	Message integrity
6.3.5.4	Output data validation		x	A.12.2.4	Output data validation
6.3.6	Cryptographic controls		x	A.12.3	Cryptographic controls
6.3.6.1	Policy on the use of cryptographic controls		x	A.12.3.1	Policy on the use of cryptographic controls
6.3.6.2	Key management		x	A.12.3.2	Key management
6.3.7	Security of system files		x	A.12.4	Security of system files
6.3.7.1	Control of operational software		x	A.12.4.1	Control of operational software
6.3.7.2	Protection of system test data		x	A.12.4.2	Control of system test data



.....  
 An industry partnership supported by IDA Singapore and SPRING Singapore

## 2 Working Draft for Comments

- **Canada's proposed structure**
  - 300+ controls
- **Based on current 27002**
  - Starting from 133 controls



## Observed responses on Canada model from SC27 member countries

- No country supporting using the new approach
- Due to cost to industry on implementation and conversion
- New approach still not mature
- However, handful of countries suggests to adopt some of the new controls enlisted in the taxonomy



## Other areas with request to review

- More controls on
  - Application security
  - Business continuity
  - Security awareness
  - Roles and responsibilities
- Restructuring of clause 12 “Information system acquisition, development and maintenance” using information system lifecycle model
- Including concept of asset classification in clause 6 “information classification”



## Other areas with request to review

- New clause on “supply chain assurance”
- New clause on “secure receipt of delivery”
- Including concept of asset classification in clause 6 “information classification”



## Topics

- Background
- ISO/IEC 27001 - Direction of changes
- Further consideration for 27001 changes
- ISO/IEC 27002 – Possible changes
- What does it mean to you?



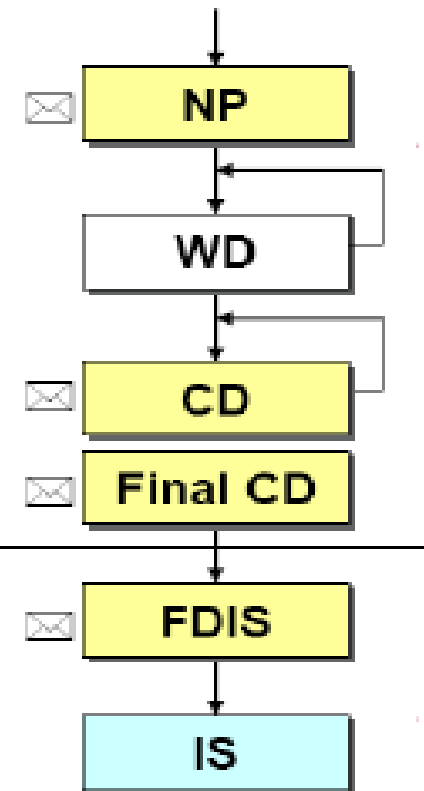
## Timeline for the revision

### *Maturity level / state of standardization*

- **Study Period / New Project (NP)**
  - 2 month NP letter ballot\*)
- **Working Draft (WD)**
- **Committee Draft (CD/FCD)**
  - 3 month CD ballot(s)
  - 4 month FCD ballot
- **Draft International Standard (DIS/FDIS)**

---

  - 2 month FDIS ballot
  - no more comments at this stage
- **International Standard (IS)**
  - review every 5 years
  - or after 'defect report'



\*) one vote per P-member

## Users of the standard are considered

- Completion not earlier than end 2011
- Cost of current ISMS implementation considered
- Target to improve security posture, not increase the cost
- Proceed for ISMS implementation
- Look out for development status and areas of review



Thanks

*(for more information, you can contact Philip Sy at [spstc\\_psy@yahoo.com](mailto:spstc_psy@yahoo.com))*



.....  
An industry partnership supported by IDA Singapore and SPRING Singapore