

# **Measuring Information Security Performance**

## **(An introduction to ISO/IEC 27004)**

*Presented by: Philip Sy*



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

## Topics

- Background
- Status of international standard development
- Principles
- Application
- Significance



## Information Security Management System (ISMS)

- A model for protection of information assets
- To establish, implement, operate, monitor, review, maintain and improve a management system for such protection
- Adopt a risk-based approach

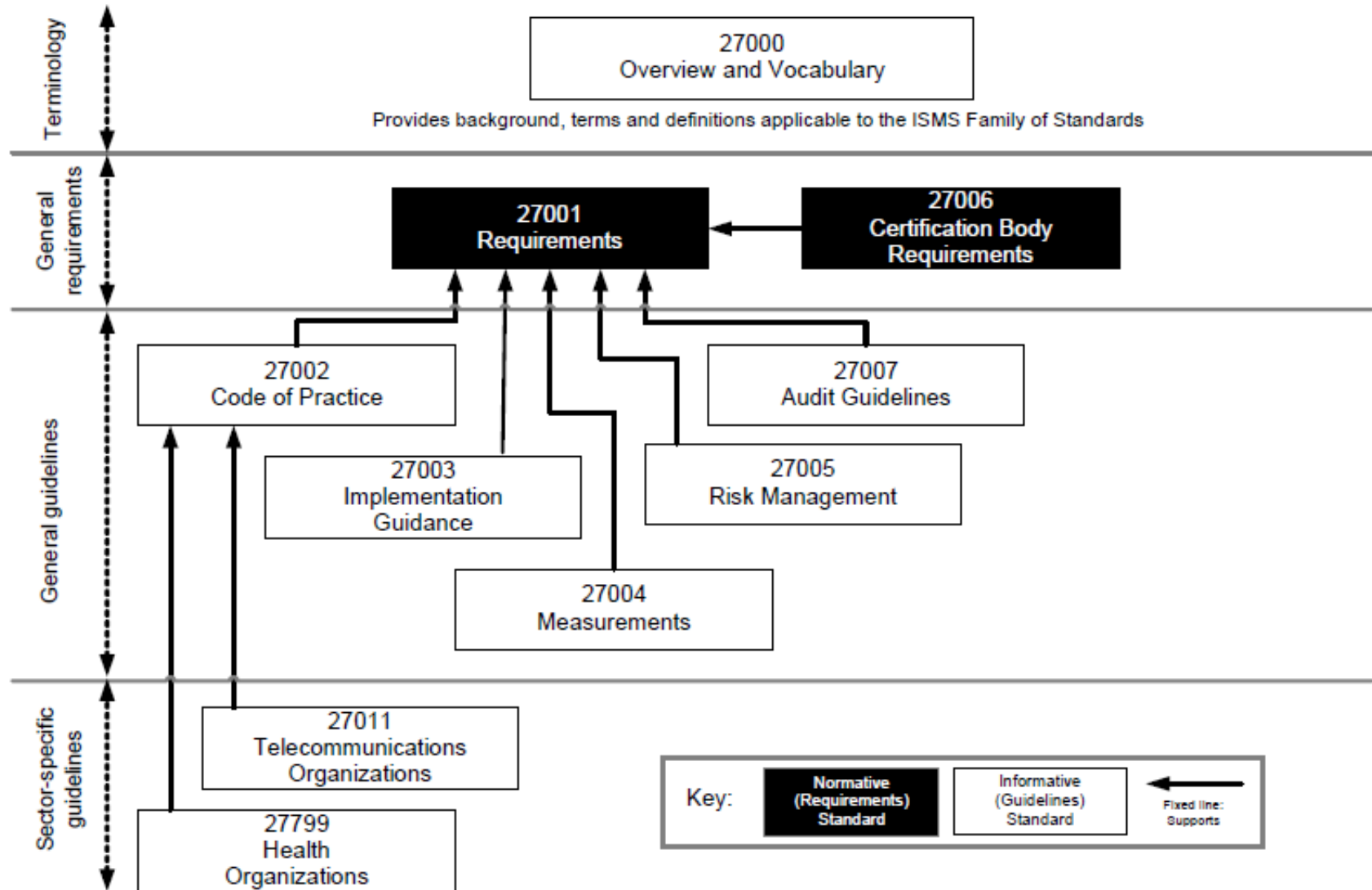


## ISMS critical success factors

- a) information security policy, objectives, and activities aligned with objectives;
- b) an approach and framework for designing, implementing, monitoring, maintaining, and improving information security consistent with the organizational culture;
- c) visible support and commitment from all levels of management, especially top management;
- d) an understanding of information asset protection requirements achieved through the application of information security risk management;
- e) an effective information security awareness, training and education programme, informing all employees and other relevant parties of their information security obligations set forth in the information security policies, standards etc., and motivating them to act accordingly;
- f) an effective information security incident management process;
- g) an effective business continuity management approach; and
- h) **a measurement system used to evaluate performance in information security management and feedback suggestions for improvement.**



# ISMS Family of Standards



## Topics

- Background
- Status of international standard development
- Principles
- Application
- Significance



# Development calendar of ISO/IEC 27004

Apr 2004	New Work Item Proposal (NWIP)
Oct 2004	1 <sup>st</sup> Working Draft (WD)
Nov 2006	1 <sup>st</sup> Committee Draft (CD)
Apr 2008	Final Committee Draft (FCD)
Aug 2009	Final Draft International Standard (FDIS)



# Status of ISO/IEC 27004

- Submitted as FDIS for ballot by JTC1 members
- Closing 27 Oct 09
- Any comments to be resolved
- Any necessary editorial changes
- To be published as International Standard



## Topics

- Background
- Status of international standard development
- Principles
- Application
- Significance



## Objective of the standard

- Provide guidance and advice on the development and use of measurements in order to assess the effectiveness of ISMS, control objectives, and controls used to implement and manage information security, as specified in ISO/IEC 27001.
- Provide a measurement framework allowing an assessment of ISMS effectiveness to be measured in accordance with ISO/IEC 27001.



## Objective of measurement

- a) evaluating the effectiveness of the implemented controls or groups of controls
- b) evaluating the effectiveness of the implemented ISMS
- c) verifying the extent to which identified security requirements have been met
- d) facilitating performance improvement of information security in terms of the organization's overall business risks
- e) providing input for management review to facilitate ISMS-related decision making and justify needed improvements of the implemented

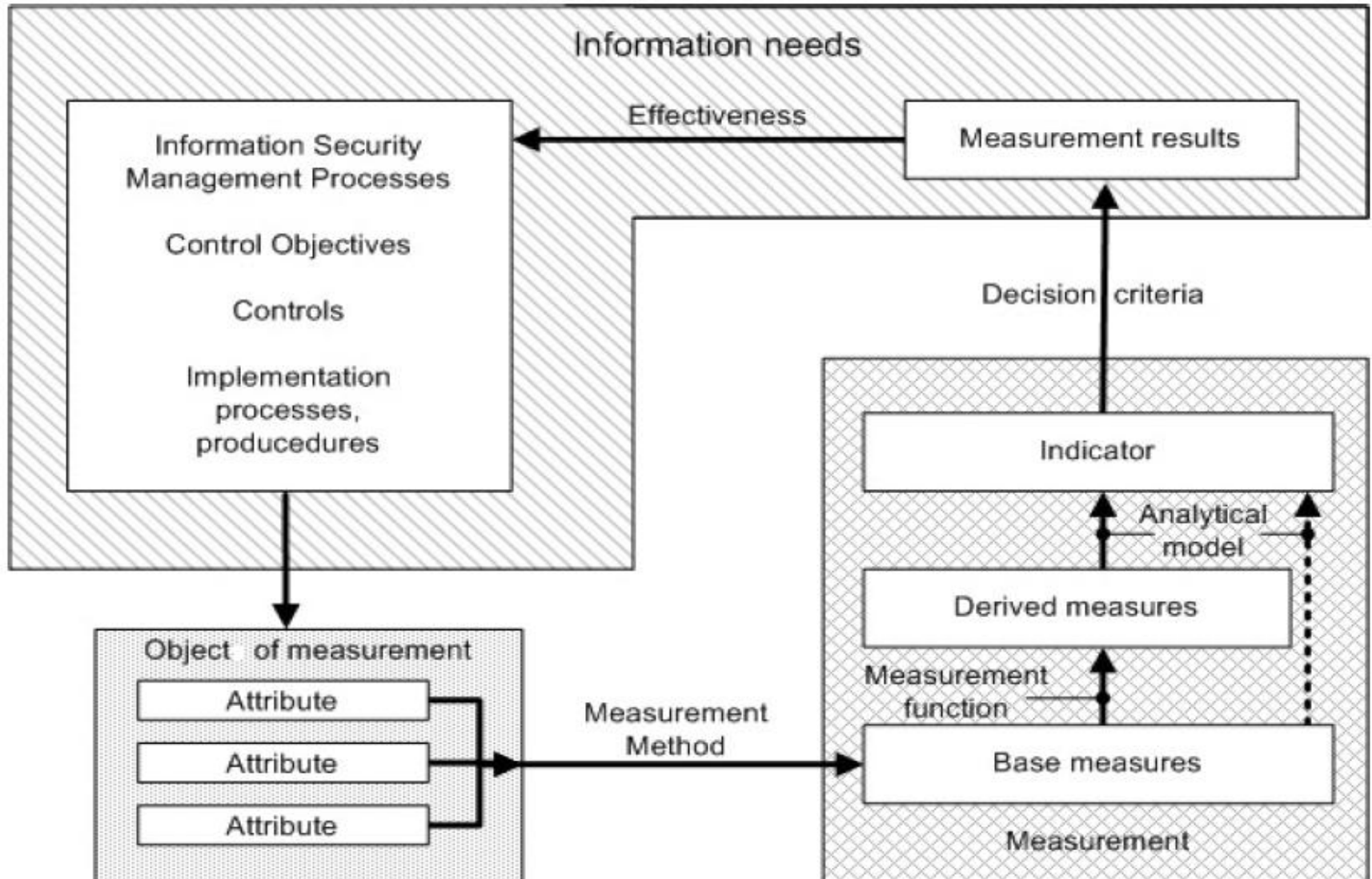


## Process of Information Security Measurement Programme

- a) Measures and measurement development (Clause 7)
- b) Measurement operation (Clause 8)
- c) Data analysis and measurement results reporting (Clause 9)
- d) Information Security Measurement Programme evaluation and improvement (Clause 10)



# Measurement Model

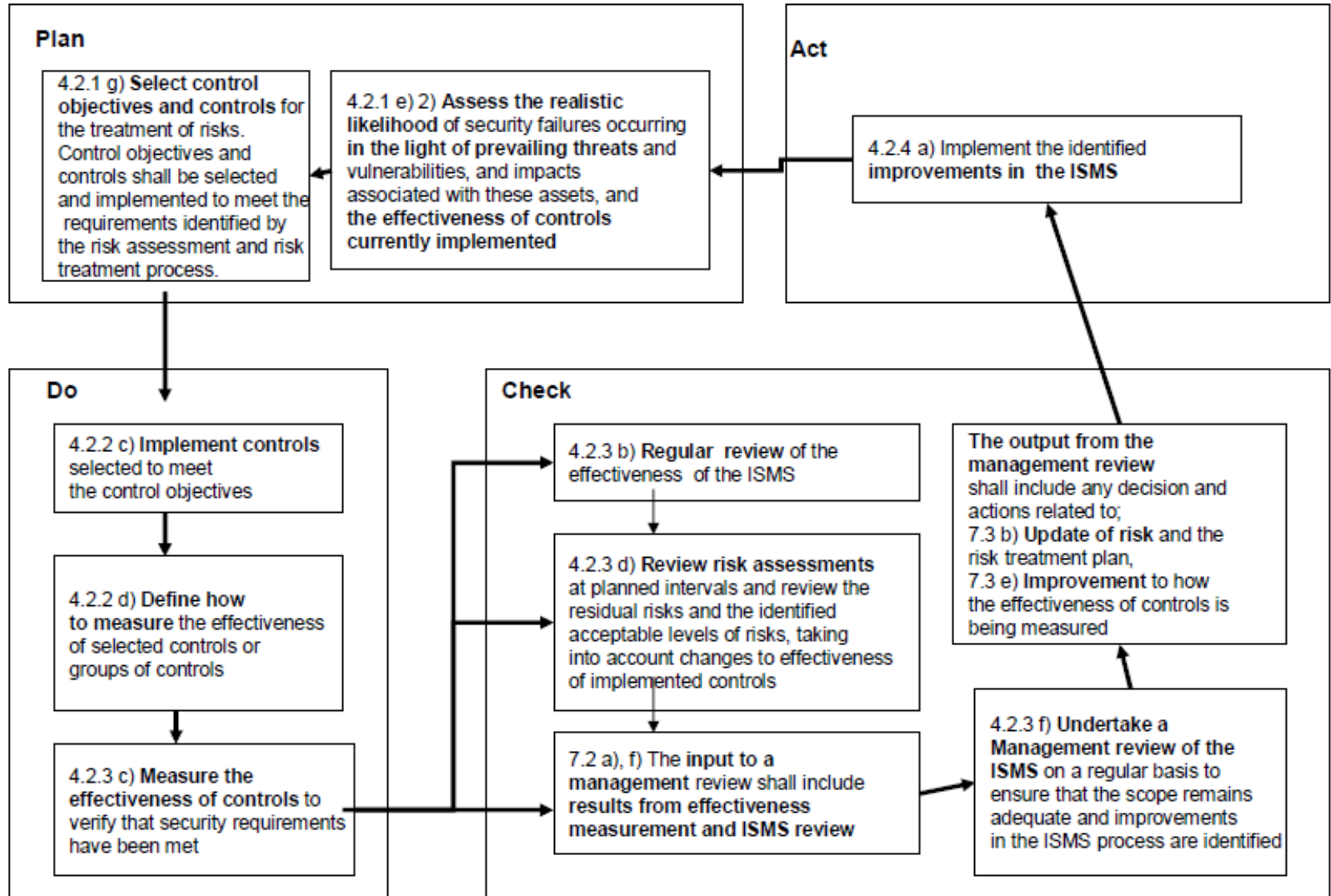


## Topics

- Background
- Status of international standard development
- Principles
- Application
- Significance



# How ISO/IEC 27004 complements PDCA cycle in ISO/IEC27001



## Consideration when selecting measurement objectives

- a) Role of information security in support of business activities and the relevant risks
- b) Applicable legal, regulatory, & contractual requirements
- c) Organizational structure
- d) Costs and benefits
- e) Risk acceptance criteria
- f) Need to compare several ISMSs



## Template for measurement construct

- **Measurement Construct Identification**
  - Name
  - Identifier
  - Control/process objective
  - Control/process
- **Object of Measurement**
  - Object
  - Attribute



## Template for measurement construct

- Base Measure
  - Base Measure
  - Measurement method
  - Type of method
  - Scale
  - Type of scale
  - Unit



## Template for measurement construct

- **Derived Measure**
  - Base Measure
  - Measurement function
- **Indicator**
  - Indicator
  - Analytical Model
- **Decision Criteria**
  - Criteria



## Template for measurement construct

- Measurement results
  - Indicator interpretation
  - Reporting Format
- Stakeholders
  - Client
  - Reviewer
  - Info owner
  - Info collector
  - Info communicator



## Template for measurement construct

- Frequency / Period
  - Freq of data collection
  - Freq of data analysis
  - Freq of reporting
  - Measurement Revision due date
  - Measurement period



## Example of application

Control and implementation	A.8.2.1 “Management Responsibility” implemented by getting all relevant personnel to sign user agreement	
Object of measurement	Plan for signing user agreement	Personnel having signed agreement
Attribute	Personnel identified in plan for signing	Personnel status regards to signing agreement
Measurement method	Count no. of personnel scheduled to have signed	Count no. of personnel having signed
Base Measure	Number of personnel planned to sign to date B1	Number of personnel having signed to date B2
Measurement function	$D1 = B2 / B1$	
Derived Measure	D1	

## Example of application

Control and implementation	A.8.2.1 “Management Responsibility” implemented by getting all relevant personnel to sign user agreement	
Analytical model	$I1 = D1$	Compare I1 with previous year’s result
Indicator	Status of implementation of control for this period - I1	Trend of I1 – I2
Decision criteria	$0.99 < I1$	Trend is upward or stable
Measurement results	Satisfactory or not based on decision criteria	Satisfactory or not based on decision criteria



## Example of application

Control and implementation	A.8.2.2 “Information security awareness, education and training” implemented by getting all relevant personnel to receive awareness training	
Object of measurement	Awareness Training Plan	Personnel completed or in-progress of training
Attribute	Personnel identified in plan	Personnel status regards to training
Measurement method	Count no. of personnel to completed by this date	Ask responsible persons for completeness status of identified personnel
Base Measure	Personnel planned to date B3	Completeness status of individual B4
Measurement function	N/A	Add status for all personnel planned to be complete to date D4 = SUM(B4)
Derived Measure	N/A	Progress to date D4



## Example of application

Control and implementation	A.8.2.2 “Information security awareness, education and training” implemented by getting all relevant personnel to receive awareness training	
Analytical model	$I3 = D4/B3 \times 100$	Compare I3 with previous year’s result
Indicator	Status of implementation of control for this period – I3	I4 = Trend of I3
Decision criteria	$0.9 < I3$	Trend is upward or stable
Measurement results	Satisfactory or not based on decision criteria	Satisfactory or not based on decision criteria



## Topics

- Background
- Status of international standard development
- Principles
- Application
- Significance



## How this standard will affect ISMS implementor?

- Made possible more structured metric definition and measurement process
- Speed up learning curve for information security measurement
- Set expectation for measurement process
- Standardize approach in measurement
- Set basis for industry tool for measurement
- Facilitate greater emphasis on measurement for the feedback on ISMS and security control effectiveness



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