The Issue of Information Security Management

資安管理專題

Course Orientation for Information Security Management

資安管理專題課程介紹

1012ISM01
MI4
Mon 8, 9 (15:10-17:00) (B703)

Min-Yuh Day
戴敏育
Assistant Professor
專任助理教授
Dept. of Information Management, Tamkang University
淡江大學 資訊管理學系

http://mail. tku.edu.tw/myday/

2013-02-18

淡江大學101學年度第2學期
課程教學計畫表
(2013.02 - 2013.06)

- 課程名稱：資安管理專題
  (The Issue of Information Security Management)
- 授課教師：戴敏育 (Min-Yuh Day)
- 開課系級：資管四Ｐ (TLMXB4P)
- 開課資料：選修 單學期 2 學分 (2 Credits, Elective)
- 上課時間：週一 8, 9 (Mon 15:10-17:00)
- 上課教室：B703

課程簡介

- 本課程介紹資訊安全管理基本概念與實務。
- 課程內容包括
  - ISO 27001 資訊安全管理系統，
  - 資訊安全風險，先期規劃，風險評鑑，
  - 資訊安全政策，
  - 資訊安全管理組織，
  - 資產管理，人力資源管理，
  - 實體與環境安全管理，通信與作業管理，
  - 存取控制，資訊系統的取得、開發及維護，
  - 資安事故管理，營運持續管理，
  - 法令、政策、標準、及技術的符合性，
  - 內部稽核，管理審查，持續改進。

Course Introduction

- This course introduces the fundamental concepts and practices of information security management.
- Topics include
  - Introduction to ISO 27001 Information Security Management System (ISMS),
  - Information Security Risk, Risk Assessment,
  - Information Security Policy, Organization of Information Security,
  - Assets Management, Human Resources Management,
  - Physical and Environmental Security,
  - Communications and Operations Management, Access Control,
  - Information Systems Acquisition, Development and Maintenance,
  - Information Security Incident Management,
  - Business Continuity Management,
  - Compliance,
  - Internal Audit, Management Review, Continuous Improvement

課程目標
(Objective)

- 學生將能夠瞭解及應用資訊安全管理基本概念與實務。
- Students will be able to understand and apply the fundamental concepts and practices of information security management.

教學方法與評量方法

- 教學方法
  - 講述、討論、賞析、問題解決
- 評量方法
  - 紙筆測驗、報告、上課表現

課程大綱 (Syllabus)

週次	日期	內容（Subject/Topics）
1	102/02/18	資安管理專題課程介紹 (Course Orientation for Information Security Management)
2	102/02/25	ISO 27001 資訊安全管理系統介紹 (Introduction to ISO 27001 Information Security Management System; ISMS)
3	102/03/04	資訊安全風險 (Information Security Risk); 風險評鑑 (Risk Assessment)
4	102/03/11	資訊安全政策 (Information Security Policy)
5	102/03/18	資訊安全管理組織 (Organization of Information Security); 資產管理 (Assets Management)
6	102/03/25	人力資源管理 (Human Resources Management); 實體與環境安全管理 (Physical and Environmental Security); 通信與作業管理 (Communications and Operations Management); 存取控制 (Access Control)
7	102/04/01	教學行政觀摩日 (Off-campus study)

課程大綱 (Syllabus)

週次	日期	內容（Subject/Topics）
8	102/04/08	資訊系統的取得、開發及維護 (Information Systems Acquisition, Development and Maintenance)
9	102/04/15	期中報告 (Midterm Presentation)
10	102/04/22	期中考試週
11	102/04/29	資安管理專題演講 (Invited Talk on Information Security Management)(Invited Speaker)
12	102/05/06	資安事故管理 (Information Security Incident Management); 營運持續管理 (Business Continuity Management); 法令、政策、標準、及技術的符合性 (Compliance)
13	102/05/13	內部稽核 (Internal Audit); 管理審查 (Management Review); 持續改進 (Continuous Improvement)
14	102/05/20	期末報告 (Final Presentation)
15	102/05/27	畢業考試週

教材課本與參考書籍

- 教材課本 (Textbook)：
  - 講義 (Slides)

- 參考書籍 (References)：
  - 資訊安全管理教材，教育部顧問室資通安全聯盟
  - Alan Calder and Steve Watkins (2012), IT governance: a manager's guide to data security and ISO 27001/ ISO 27002, 5th edition, Kogan Page.

學期成績計算方式

- 期中評量：30.0％
- 期末評量：30.0％
- 其他 (課堂參與及報告討論表現)：40.0％ (3 篇作業)

資訊安全 (information security)

- 資訊安全 (information security)
  - 保存資訊的機密性、完整性及可用性；此外，亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質。
    [CNS 17799]
- information security
  - preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
    [ISO/IEC 17799:2005]

Source: ISO/IEC 27001:2005, CNS 27001

資訊安全管理系統
(Information Security Management System, ISMS)

- 資訊安全管理系統 (Information Security Management System, ISMS)
  - 整體管理系統的一部分， 以營運風險導向(作法)為基礎，用以建立、實作、運作、監視、審查、維持及改進資訊安全。
    - 備考： 管理系統包括組織架構、政策、規劃活動、責任、實務、程序、過程及資源。
- information security management system (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.

Source: ISO/IEC 27001:2005, CNS 27001

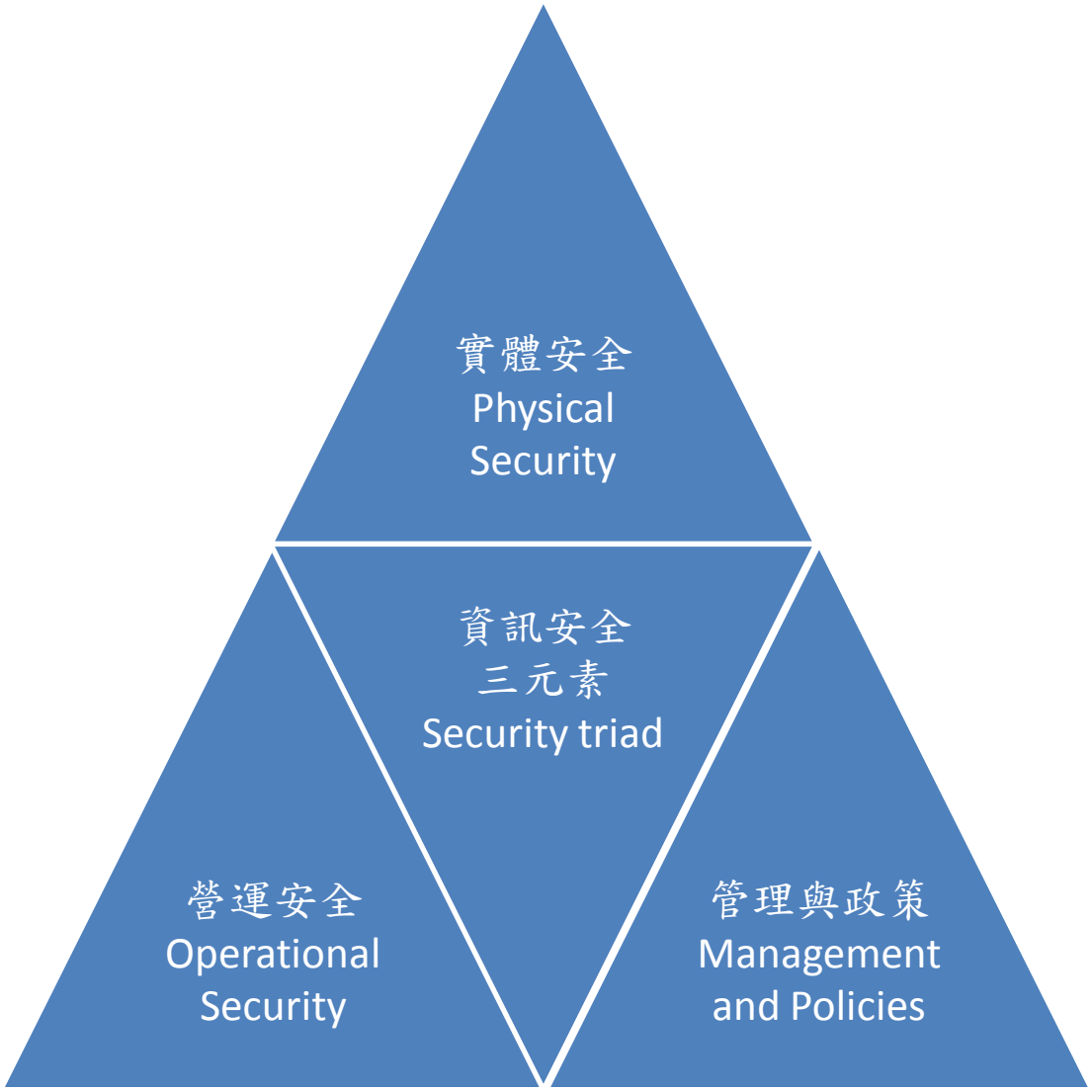
資訊安全是管理議題

- 許多人誤以為資訊安全是個「技術」議題；
  事實上它是一個需要技術輔助的「管理」議題。

【管理疏失案例】在 2003 與 2004 年，世界知名的 Wells Fargo 銀行員工的筆記型電腦有兩次在公司外遭竊。最敏感的客戶交易紀錄及二十萬筆信用卡資料外洩，造成公司嚴重的財務與形象損失。

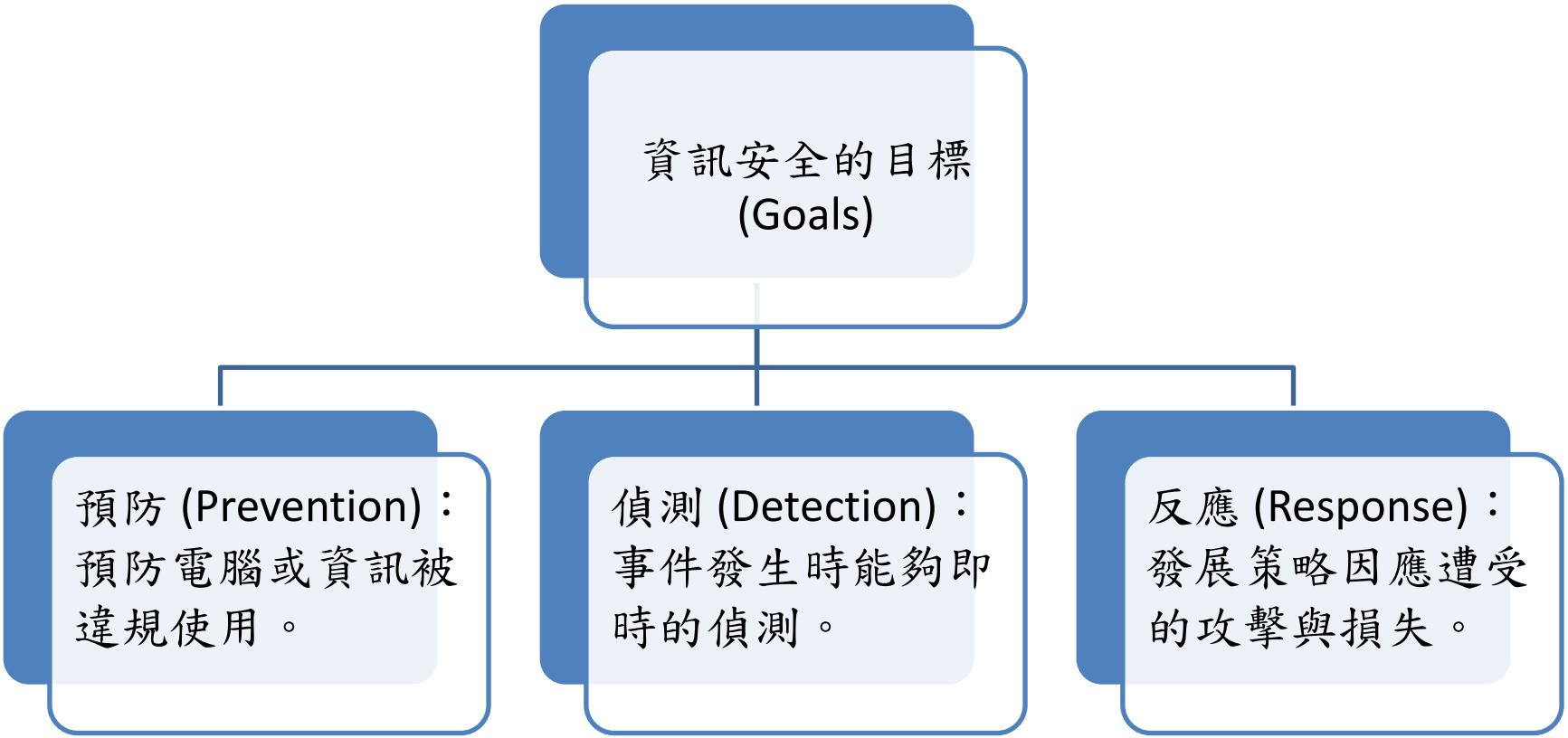
Source:潘天佑 (2011)，資訊安全概論與實務，第二版，碁峰

資訊安全的三元素



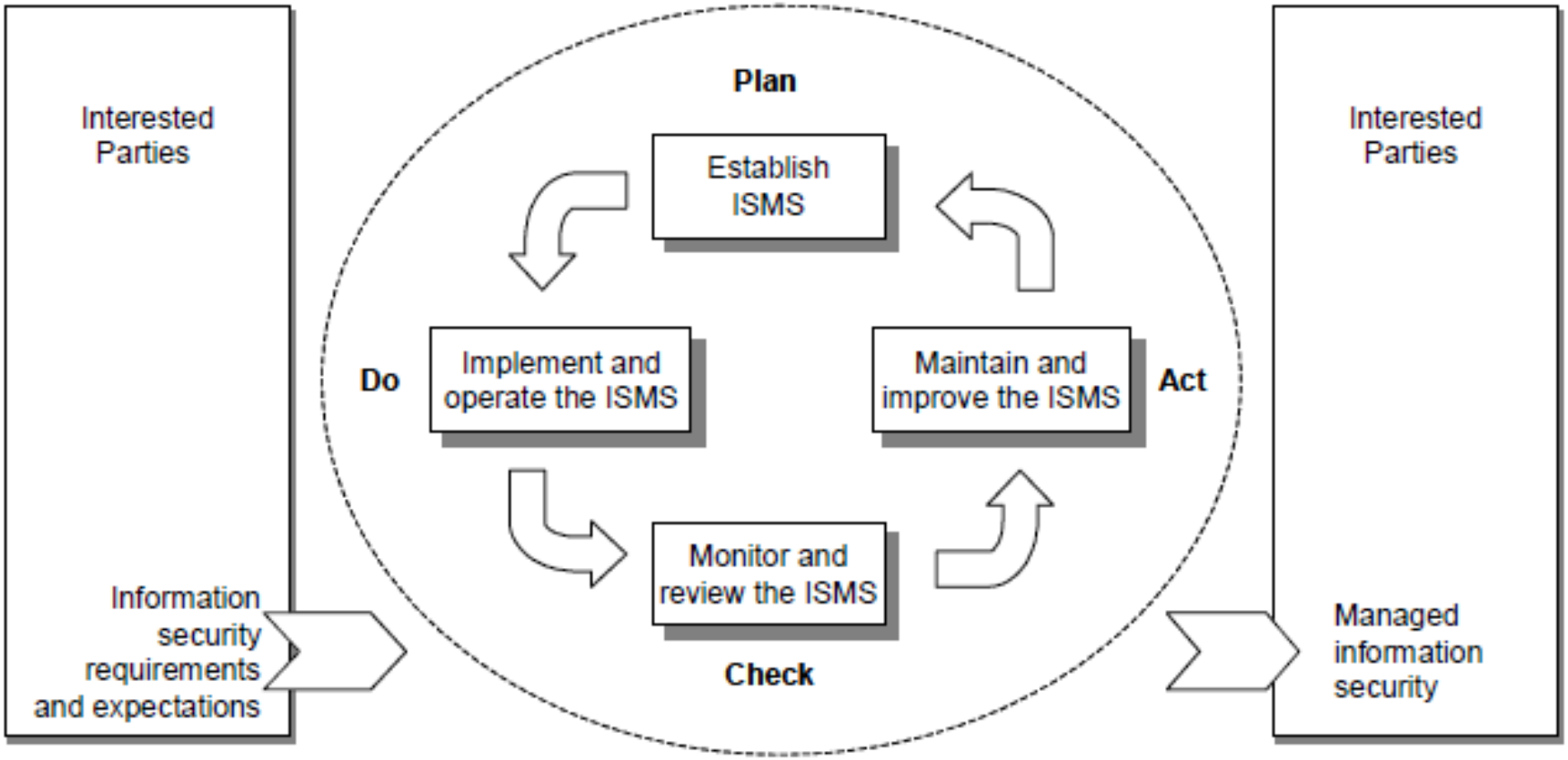
Source:潘天佑 (2011)，資訊安全概論與實務，第二版，碁峰

資訊安全的目標



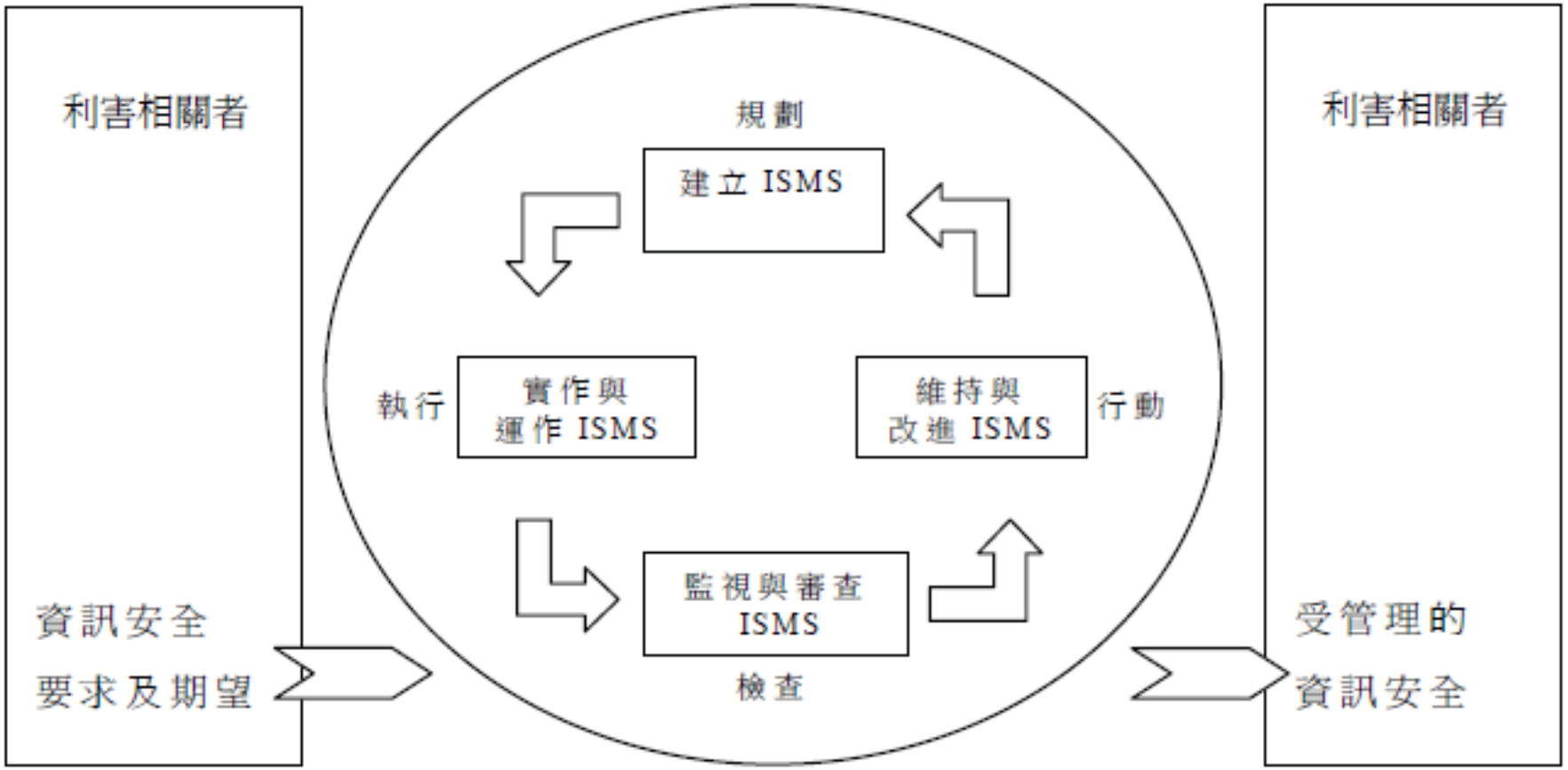
Source:潘天佑 (2011)，資訊安全概論與實務，第二版，碁峰

PDCA model applied to ISMS processes



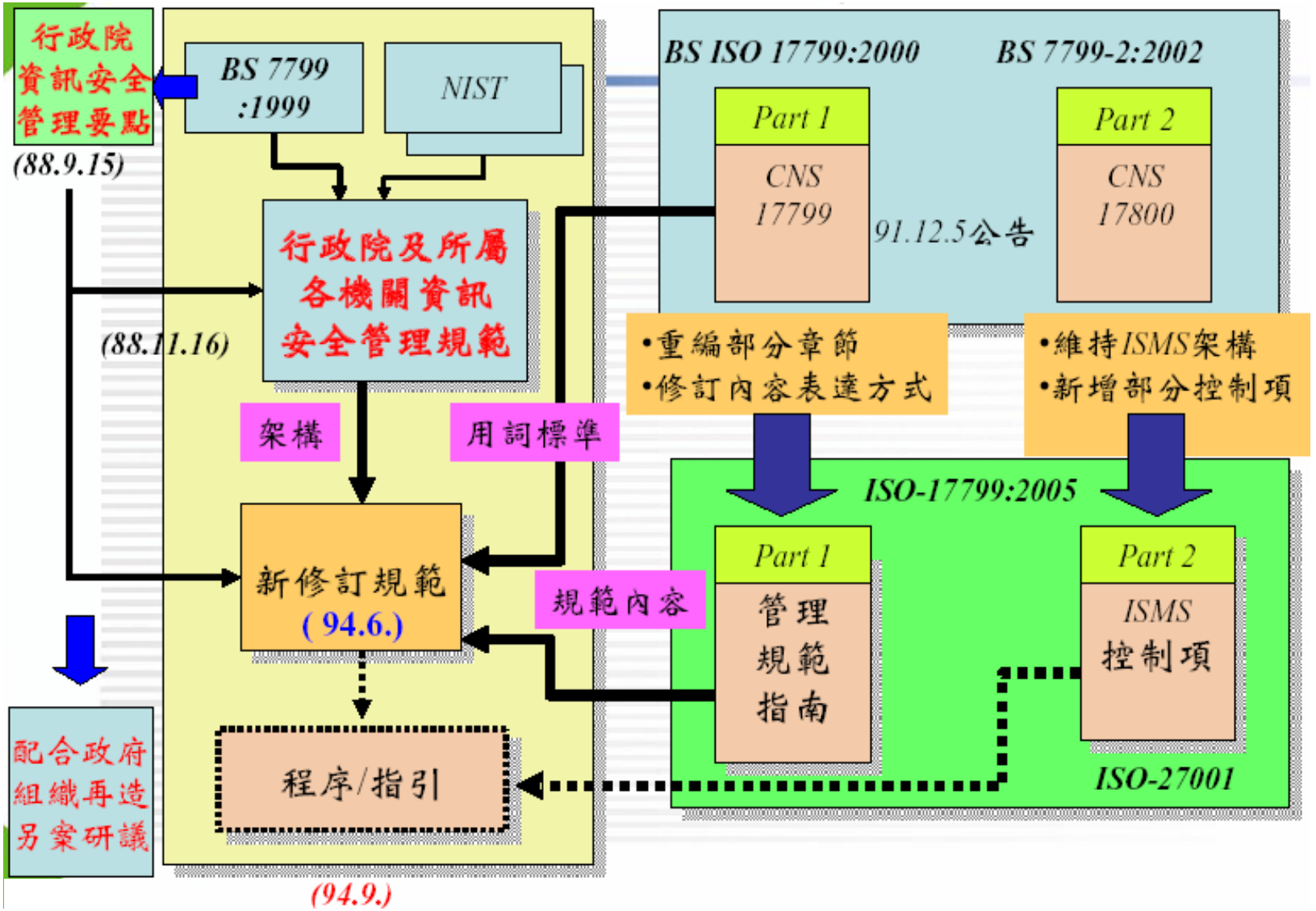
Source: ISO/IEC 27001:2005

適用於 ISMS 過程之PDCA 模型



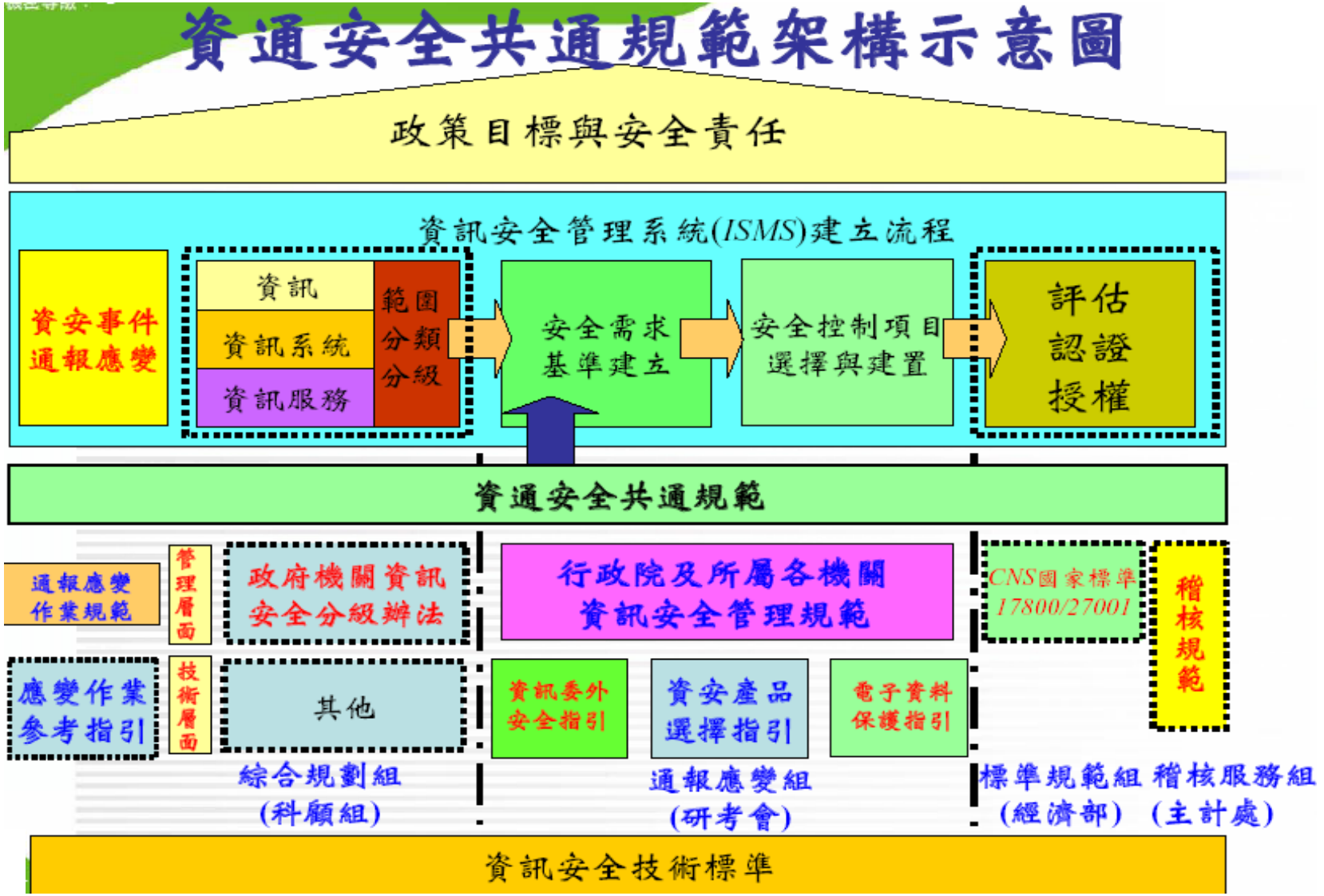
Source: CNS 27001

我國資安管理法源/政策



Source: 教育部顧問室資通安全聯盟，“資訊安全管理”教材

我國資通安全共通規範架構



Source: 教育部顧問室資通安全聯盟，“資訊安全管理”教材

資訊安全管理專業國際證照

- ISO 27001 (ISO 27001 Lead Auditor)
  - BSI: (The British Standards Institution)
- Security+
  - CompTIA
- CISSP (Certified Information Systems Security Professional)
  - $(ISC)^2$：(International Information Systems Security Certification Consortium)
- SSCP (Systems Security Certified Practitioner)
  - $(ISC)^2$：(International Information Systems Security Certification Consortium)
- CEH (Certified Ethical Hacker)
  - EC-Council

Contact Information

戴敏育 博士 (Min-Yuh Day, Ph.D.)

專任助理教授
淡江大學 資訊管理學系

電話：02-26215656 #2347
傳真：02-26209737
研究室：i716 (覺生綜合大樓)
地址： 25137 新北市淡水區英專路151號
Email： myday@mail.tku.edu.tw
網址：http://mail.tku.edu.tw/myday/