資安管理規範之發展

行政院國家資通安全會報

技術服務中心

鍾榮翰顧問

Email: barbet@icst.org.tw

December 4, 2008

課程大綱

一．何謂資訊安全？

二．資安風險管理

三．ISO/IEC/CNS資安標準

四．資訊安全保證(Security Assurance)

五．美國NIST資安文件架構

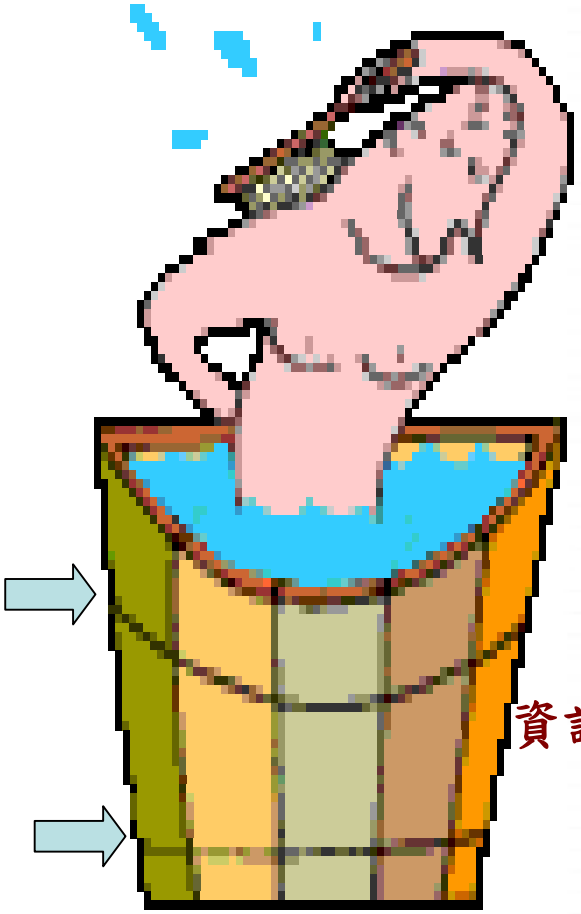
六．我國共通規範藍圖發展

何謂資訊安全？

- 資訊是一種資產，和其他重要的營運資產一樣，對組織營運是不可或缺的，因此需要妥善保護，此在日益互連的營運環境中特別重要。
- 無論資訊的形式為何，以何種方式分享或儲存，均宜加以適當的保護。
- 資訊安全是使資訊不受各種廣泛的威脅之保護，以確保營運持續性、降低營運風險至最低、得到最豐厚的投資報酬率及最大商機。(資料來源：*CNS 27002*)
- 安全是一種過程，而不是產品
- 資訊安全不單是技術問題，更是管理問題

資安理論_木桶理論新解

- 決定木桶儲水量多寡之要件：
  - 堅實的底座
  - 最低高度之木片
  - 上下緊密連結之鐵箍



資安事故通報應變機制

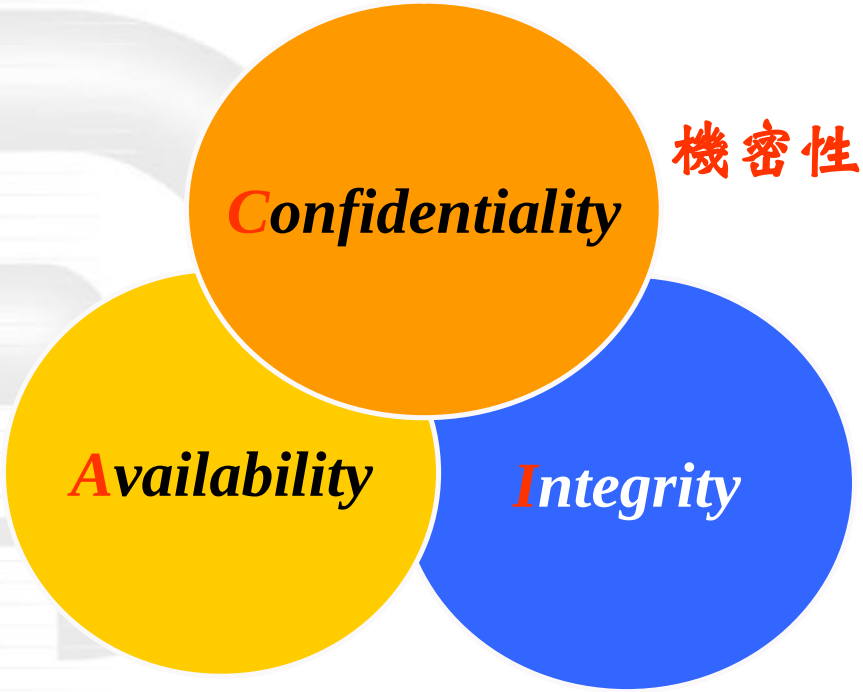
資安管理認、驗證機制

資訊安全領域

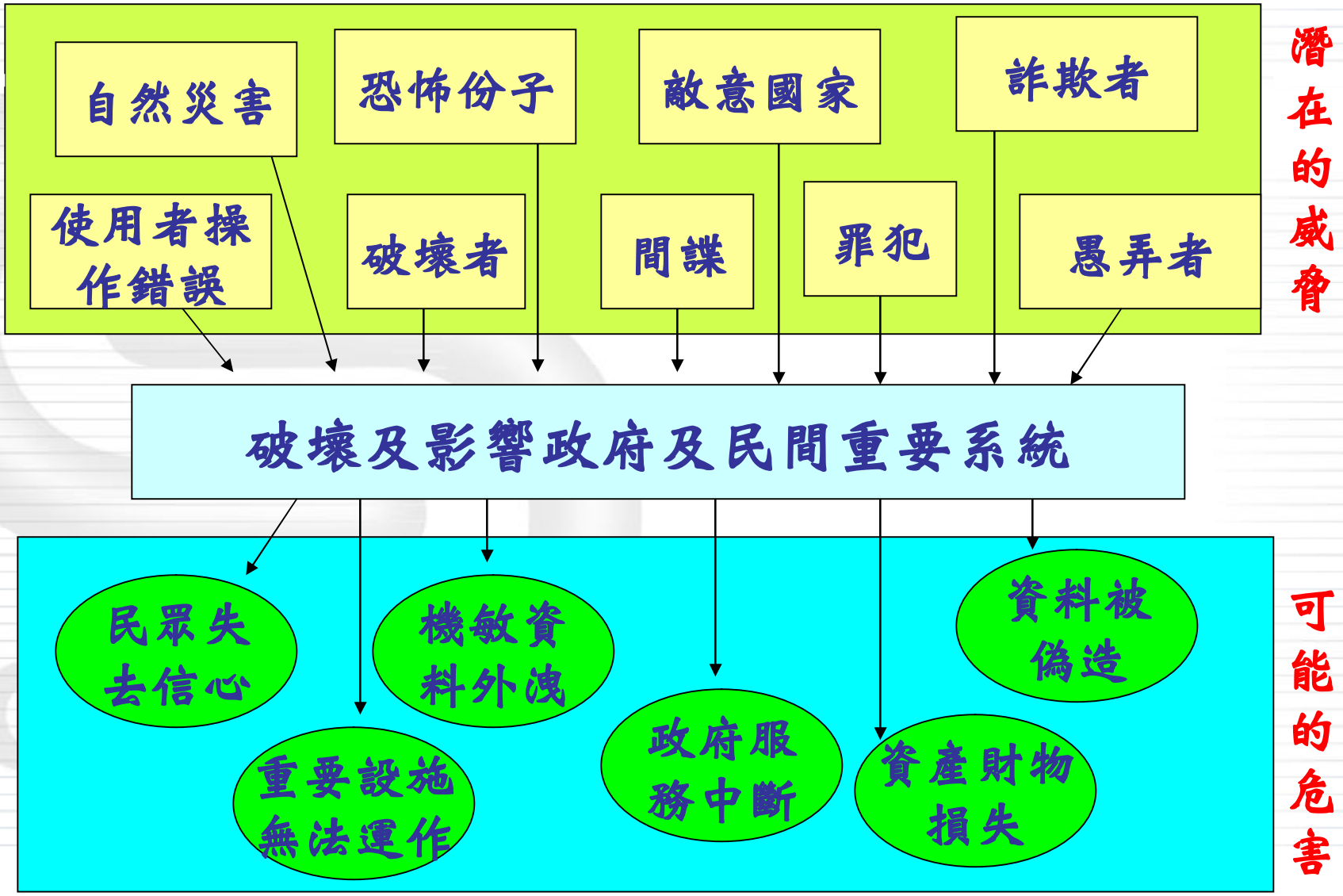
資訊安全管理系統

資訊安全三大目標

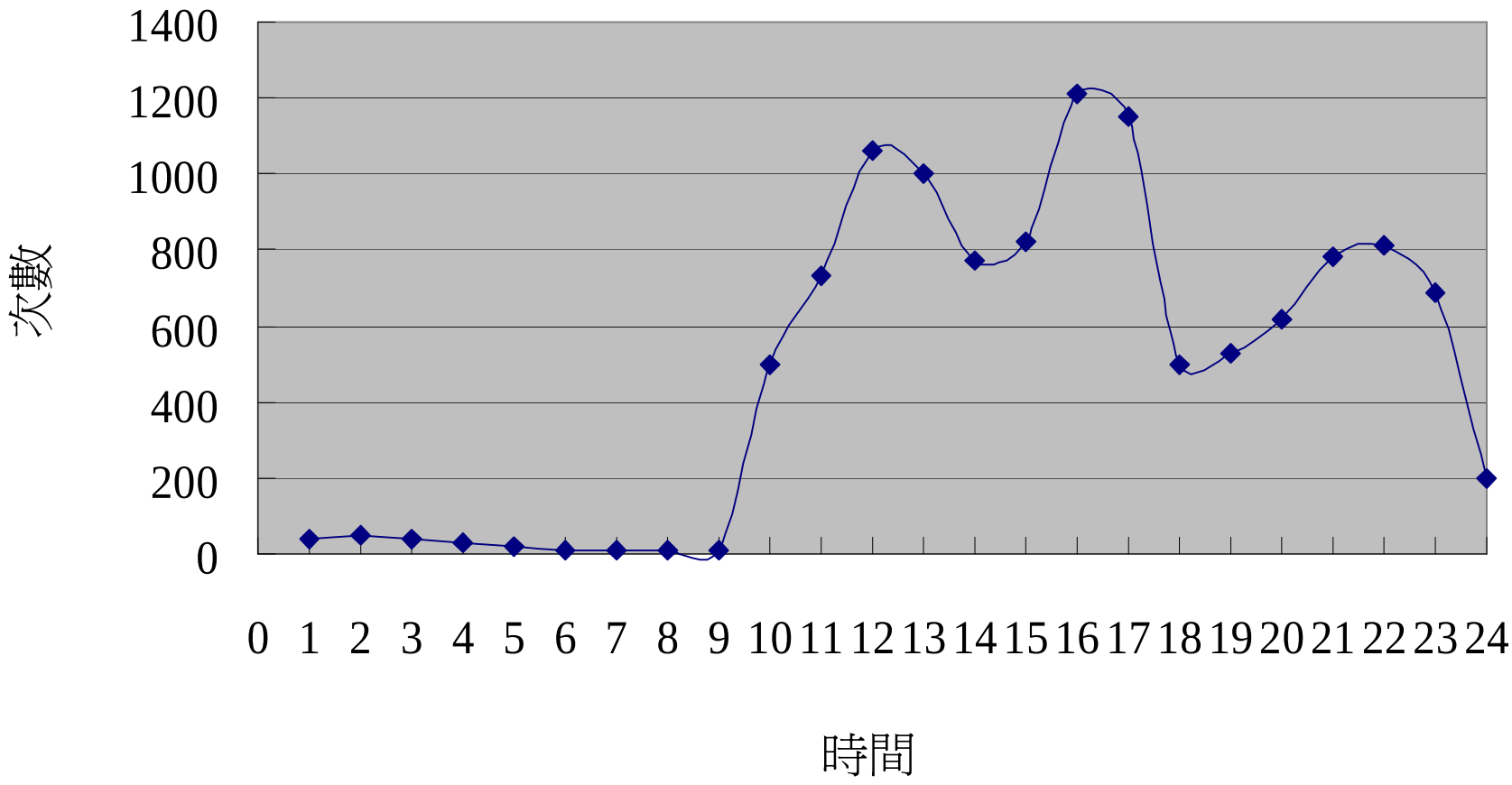
- 資訊安全在保護單位的**資訊資產**，避免遭受各種**威脅**及降低**可能傷害**，以確保單位**永續經營**



資通安全潛在威脅與危害



組織型駭客行為分析


1400
1200
1000
800
600
400
200
0
次數
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
時間

課程大綱

一．何謂資訊安全？

二．資安風險管理 

三．ISO/IEC/CNS資安標準

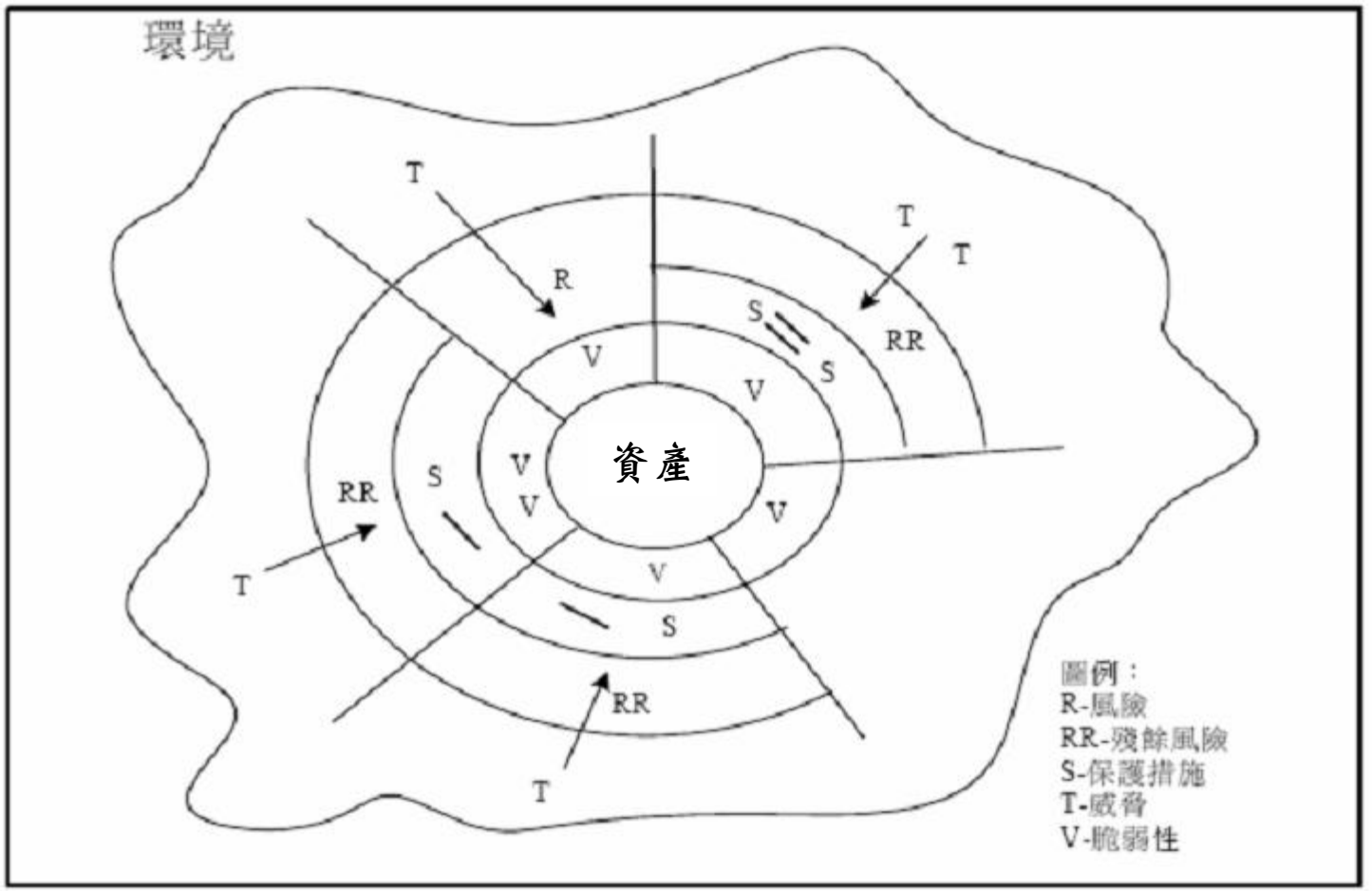
四．資訊安全保證(Security Assurance)

五．美國NIST資安文件架構

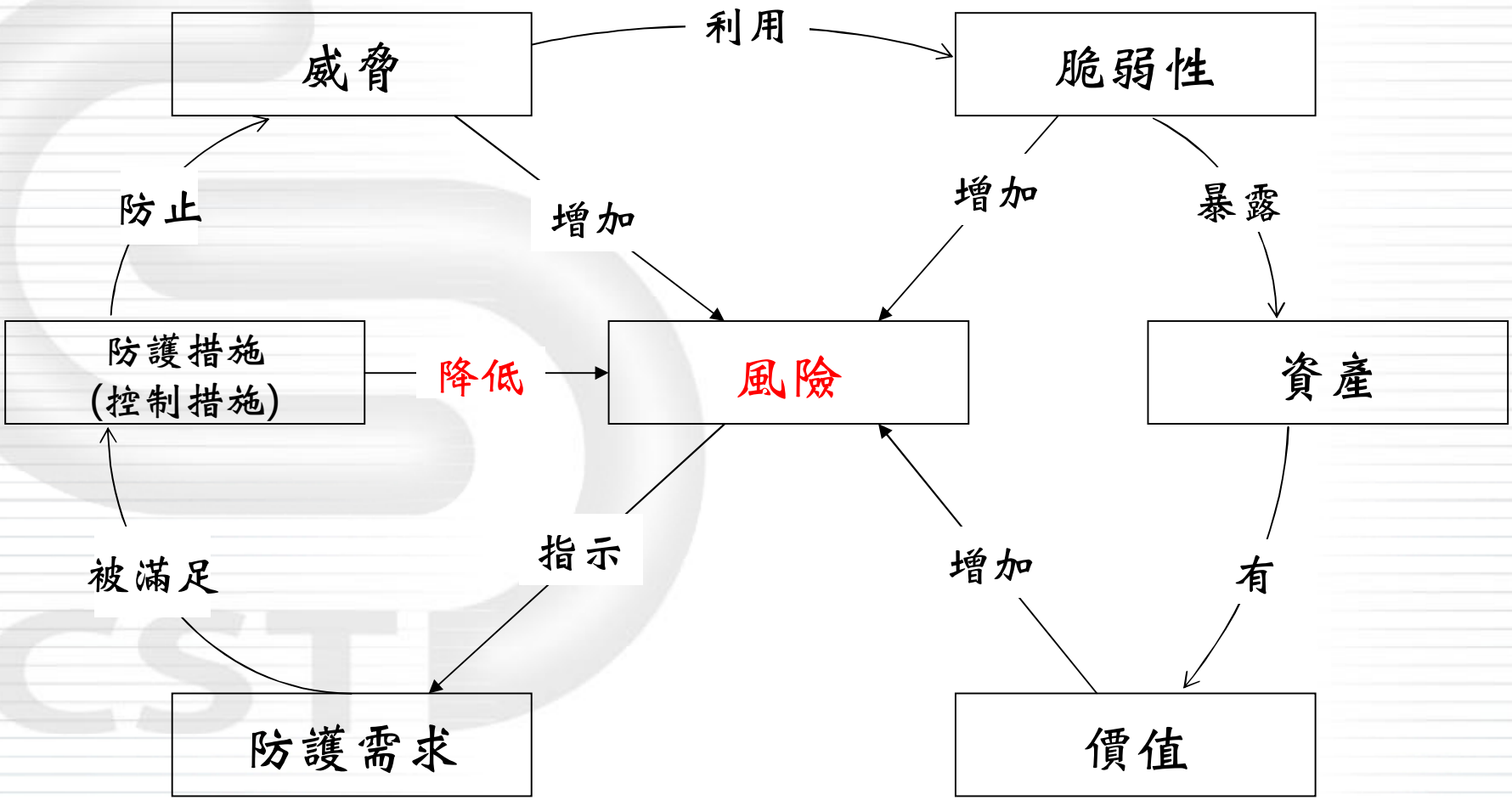
六．我國共通規範藍圖發展

何謂資訊安全風險？

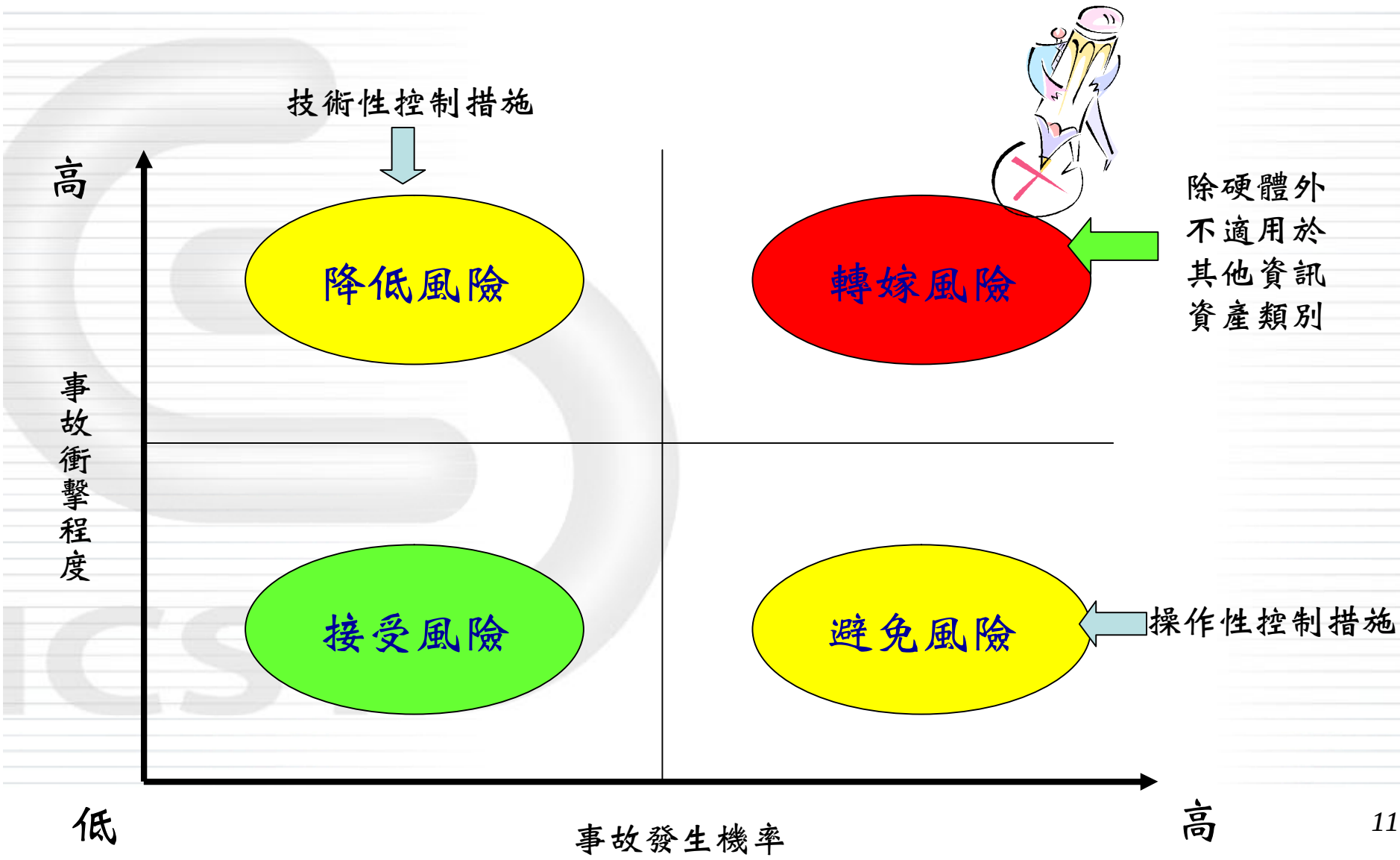
風險(risk)：
已知威脅利用單一或一群資產的脆弱性，造成資產損失或損壞的潛在可能性。



風險管理要素關聯圖



風險處理矩陣圖


技術性控制措施
高
降低風險
轉嫁風險
除硬體外
不適用於
其他資訊
資產類別
事故衝擊程度
接受風險
避免風險
操作性控制措施
低
事故發生機率
高

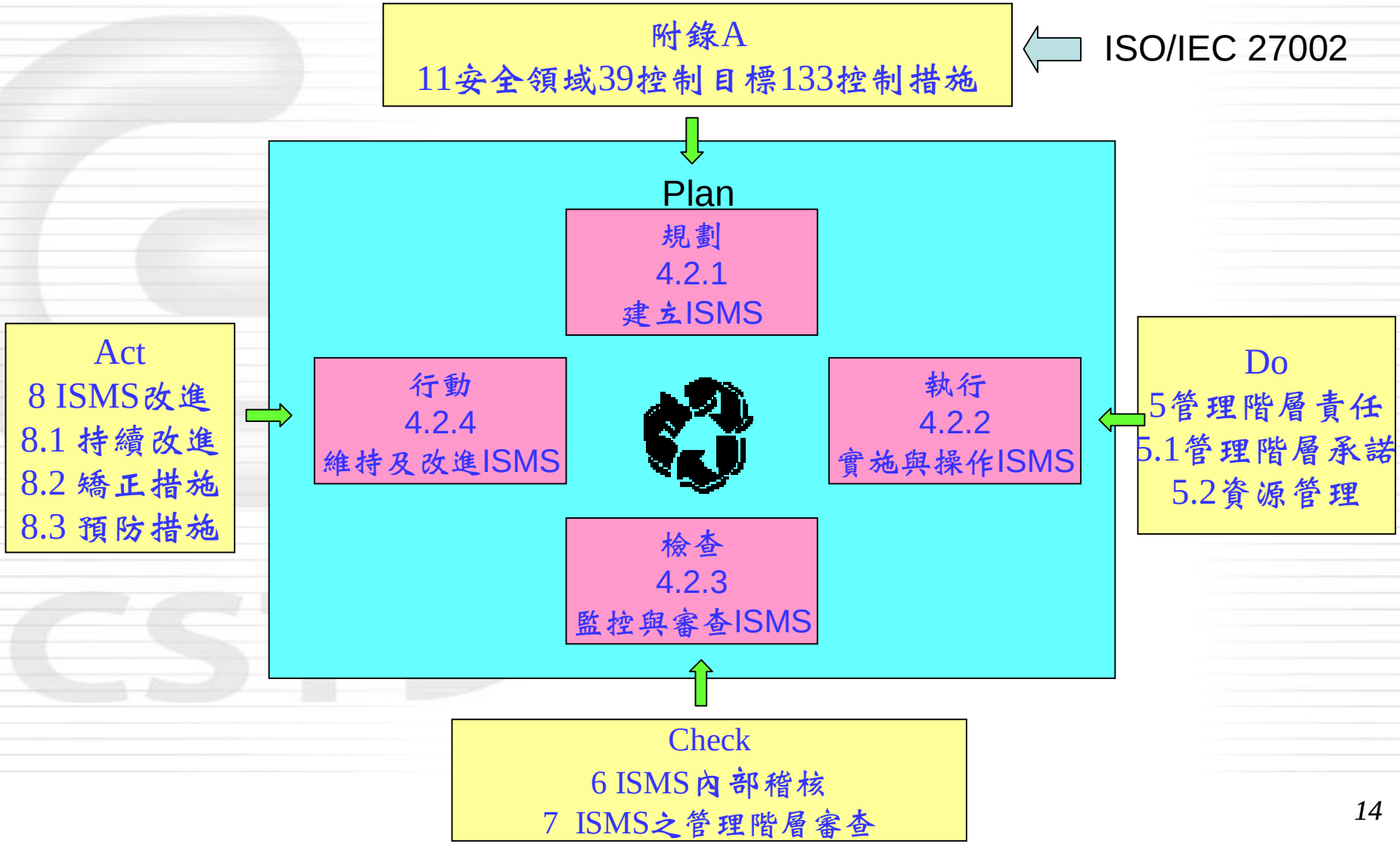
課程大綱

一．何謂資訊安全？
二．資安風險管理
三．ISO/IEC/CNS資安標準 
四．資訊安全保證(Security Assurance)
五．美國NIST資安文件架構
六．我國共通規範藍圖發展

ISO/IEC 27000系列標準簡述

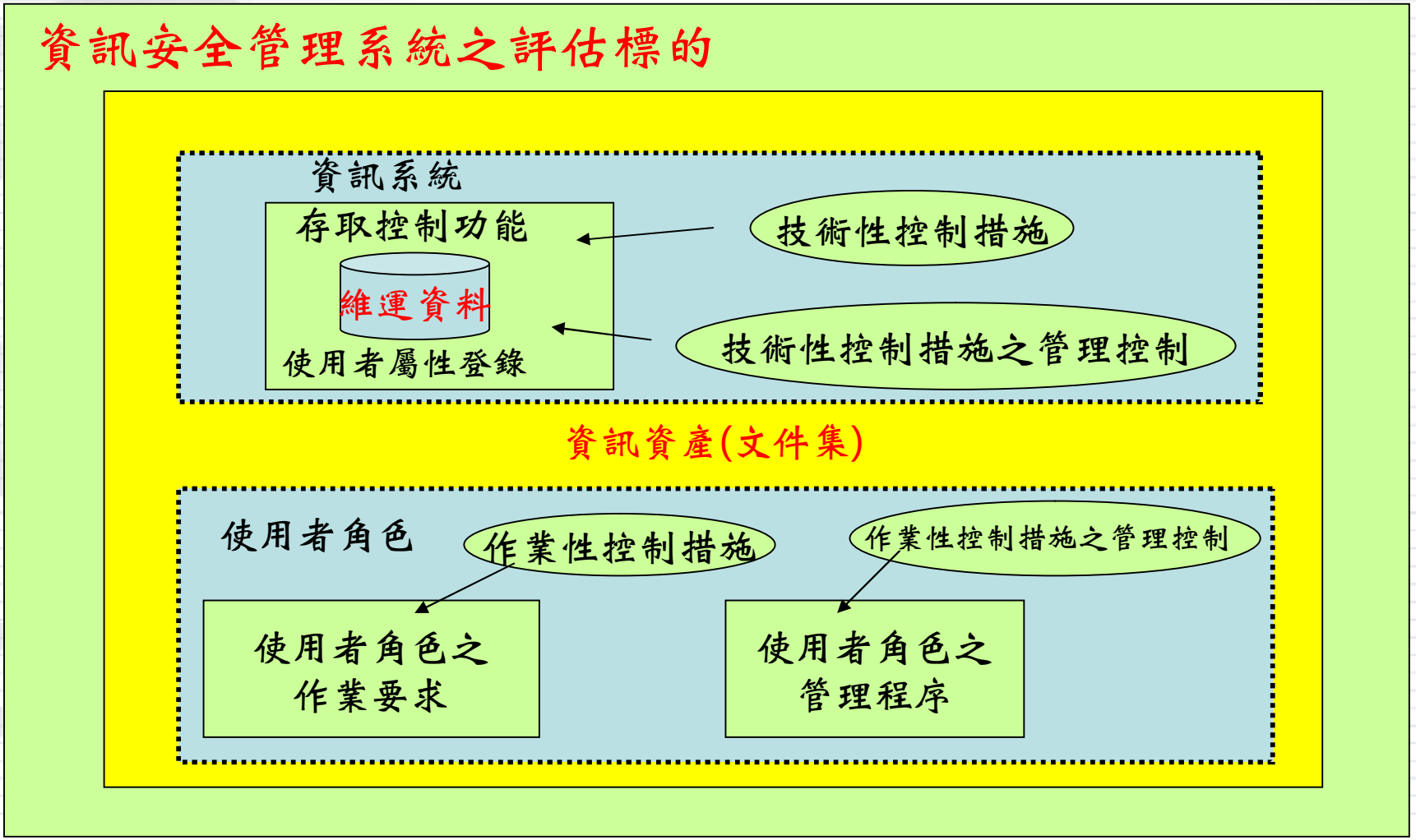
- ISO/IEC 27000：資訊安全管理系統之原則與詞彙
- ISO/IEC 27001：資訊安全管理系統要求(2005/10/15公布)
  CNS-27001已於95/6/15公布
- ISO/IEC 27002：ISO/IEC 17799:2005(E)於公布時說明
  2007/7年改版成為ISO/IEC 27002
  CNS 27002亦於96/10/24公布
- ISO/IEC 27003：資訊安全管理系統實作指引，預訂2008年底至2009年初公布
- ISO/IEC 27004：資訊安全管理測度與測量，
  目前進度：stage 3, working draft level
- ISO/IEC 27005：資訊安全風險管理，已於2008年6月公布
- ISO/IEC 27006：資訊安全管理系統之認驗證機制，已於2007年3月公布

ISO/CNS 27001架構



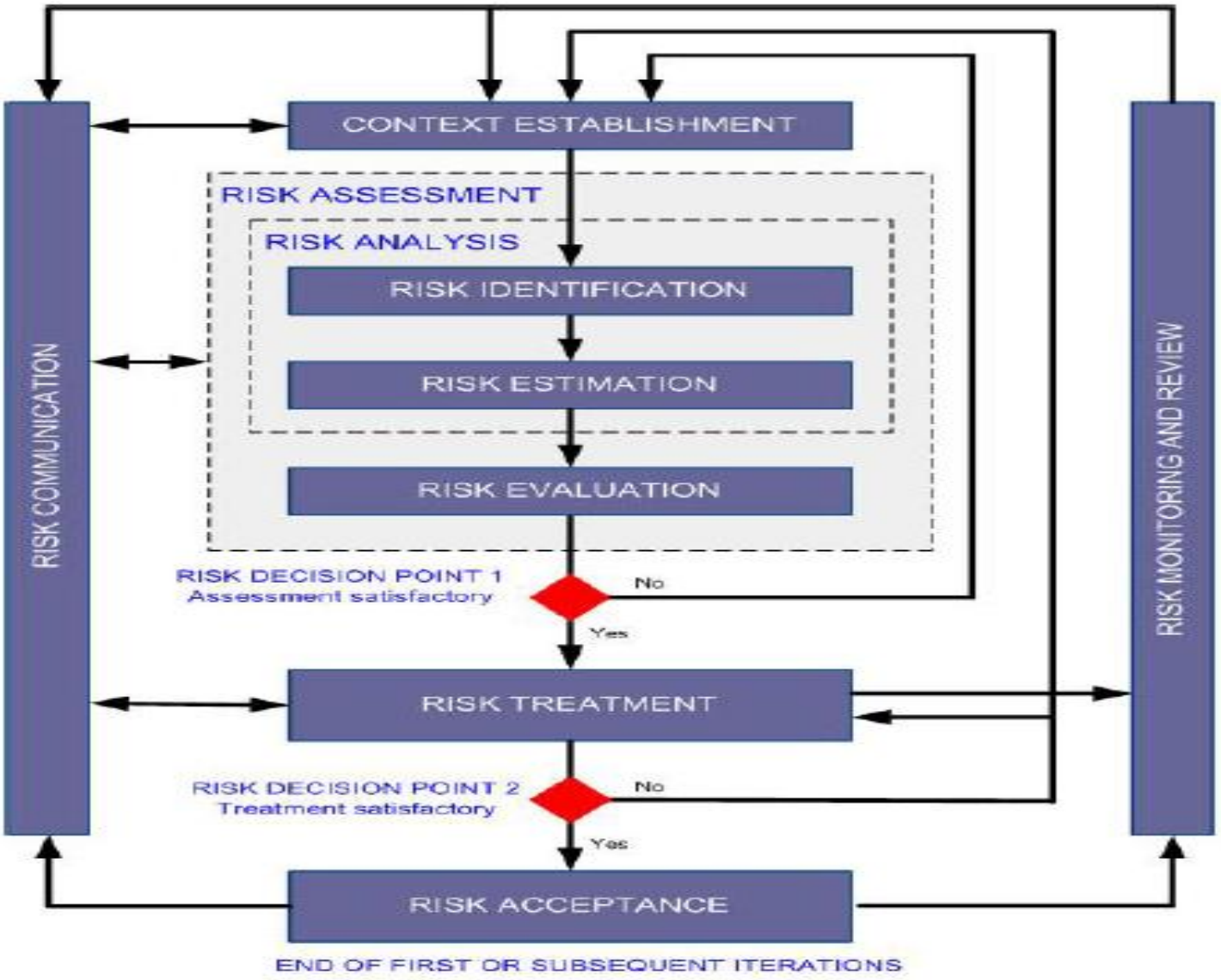
ISO/IEC 27002架構

資訊安全管理系統之控制類別

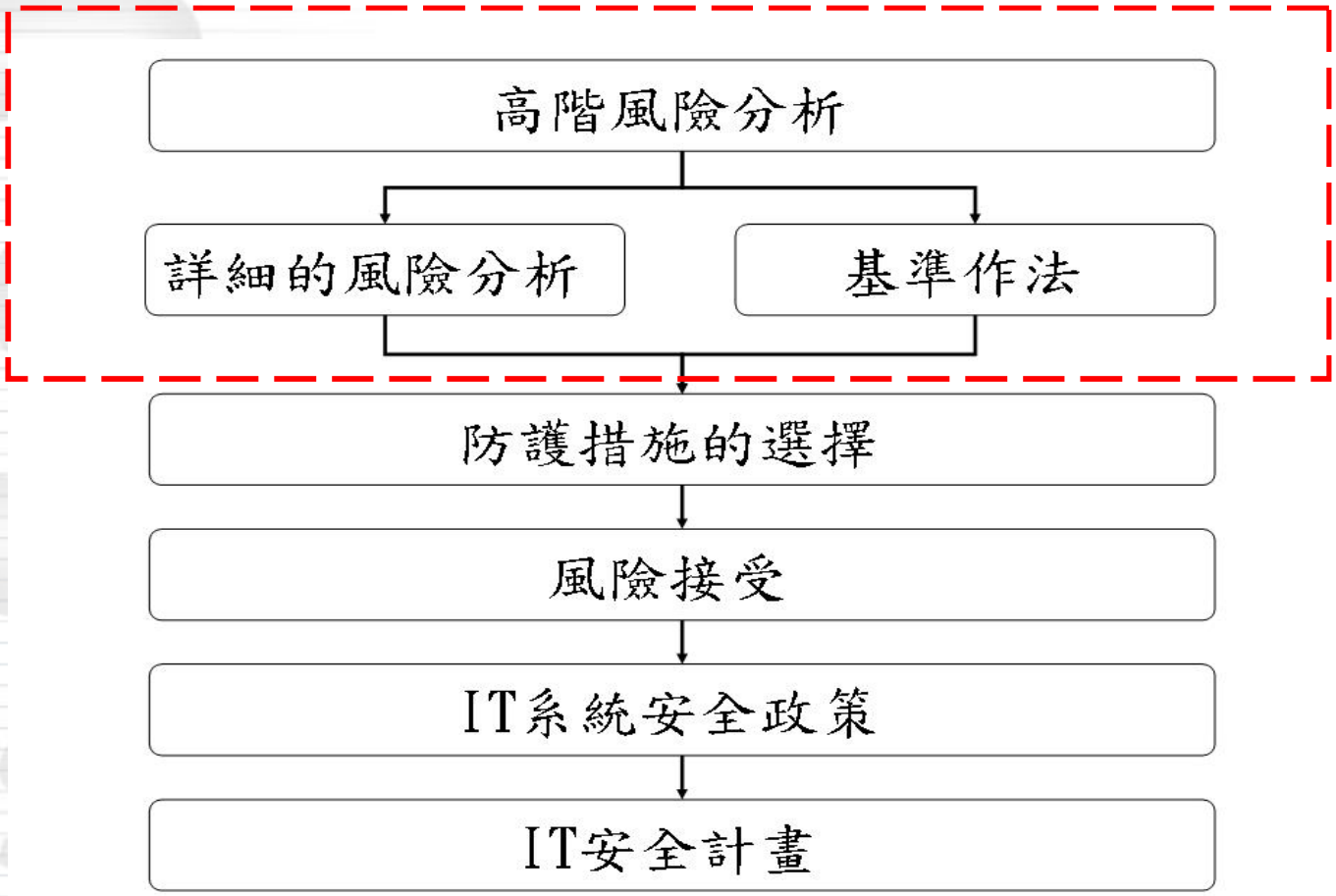


資料來源：ISO/IEC DTR 19791

ISO/IEC 27005資安風險管理程序



ISO/IEC 13335風險評鑑流程



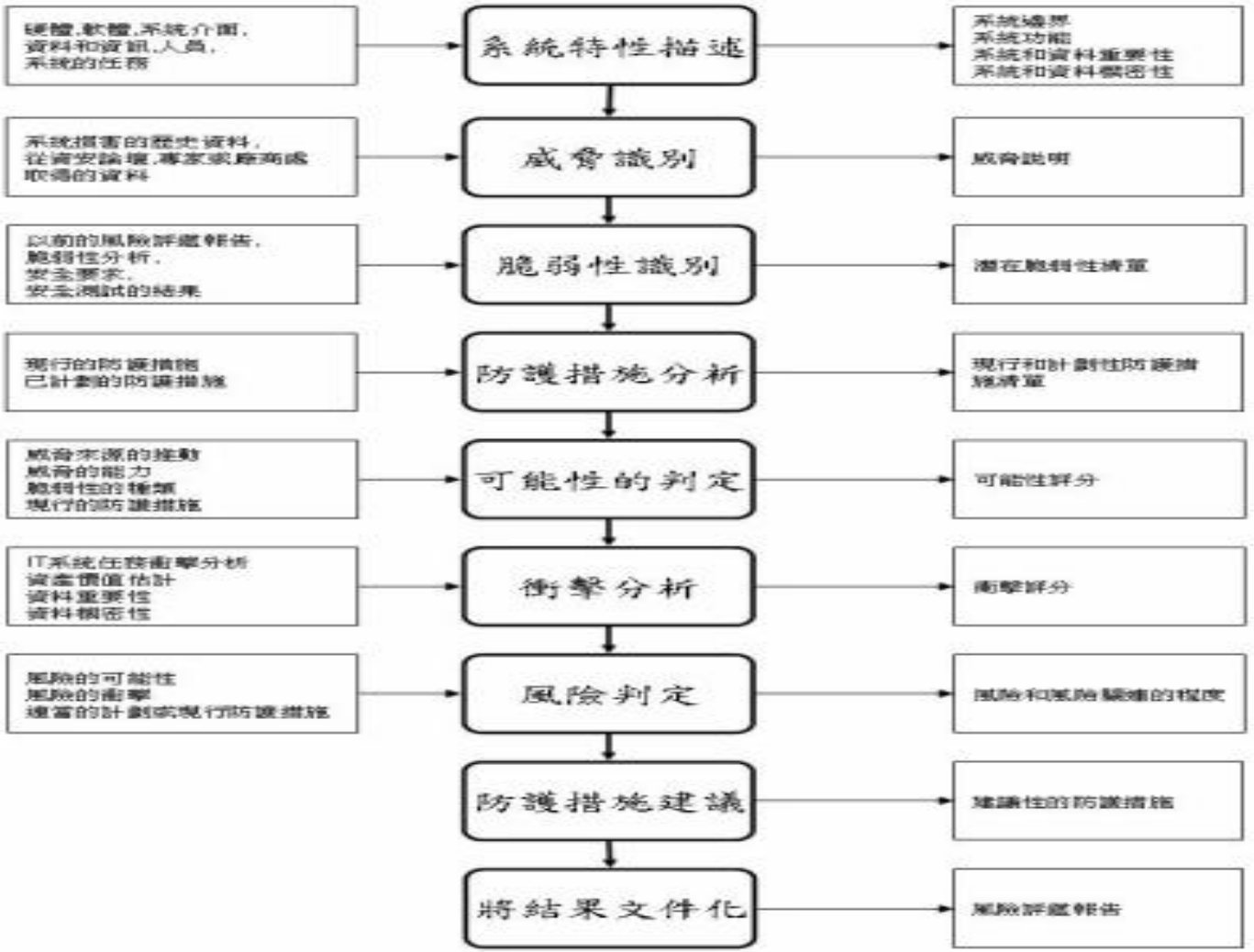
參考：CNS14929[3]

ISO/IEC 13335=CNS 14929

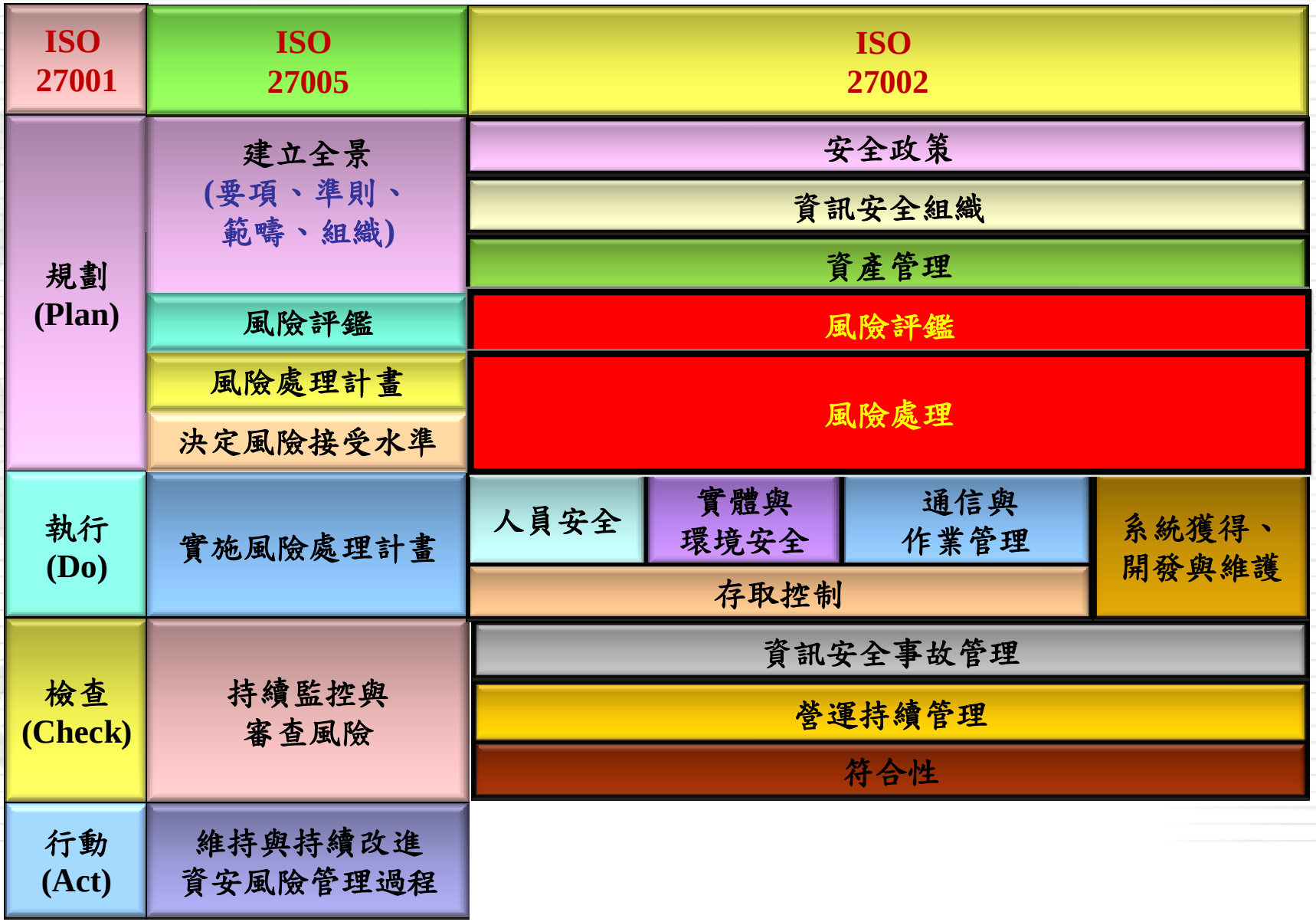
高階風險分析流程


網路圖(network plan)分析
識別相似資產組(grouping)以減小複雜度
彙整IT系統資訊
彙整IT應用程式和相關資訊
IT應用程式防護要求評估
IT系統防護要求評估
IT作業區域防護要求評估
防護要求評估結果解釋

詳細風險分析流程


硬體,軟體,系統介面,
資料和資訊,人員,
系統的任務
系統特性描述
系統邊界
系統功能
系統和資料重要性
系統和資料機密性
系統損害的歷史資料,
從資安論壇,專家或廠商處
取得的資料
威脅識別
威脅說明
以前的風險評鑑報告,
脆弱性分析,
安全要求,
安全測試的結果
脆弱性識別
潛在脆弱性清單
現行的防護措施
已計劃的防護措施
防護措施分析
現行和計劃性防護措施清單
威脅來源的誘動
威脅的能力
脆弱性的種類
現行的防護措施
可能性的判定
可能性評分
IT系統任務衝擊分析
資產價值估計
資料重要性
資料機密性
衝擊分析
衝擊評分
風險的可能性
風險的衝擊
建置的計劃或現行防護措施
風險判定
風險和風險關連的程度
防護措施建議
建議性的防護措施
將結果文件化
風險評鑑報告

ISMS架構對照


ISO 27001
ISO 27005
ISO 27002
規劃 (Plan)
建立全景 (要項、準則、範疇、組織)
風險評鑑
風險處理計畫
決定風險接受水準
執行 (Do)
實施風險處理計畫
檢查 (Check)
持續監控與審查風險
行動 (Act)
維持與持續改進資安風險管理過程
安全政策
資訊安全組織
資產管理
風險評鑑
風險處理
人員安全
實體與環境安全
通信與作業管理
系統獲得、開發與維護
存取控制
資訊安全事故管理
營運持續管理
符合性

課程大綱

一．何謂資訊安全？
二．資安風險管理
三．ISO/IEC/CNS資安標準
四．資訊安全保證(Security Assurance)
五．美國NIST資安文件架構
六．我國共通規範藍圖發展

認證與驗證之定義

- 驗證(*Certification*)：對符合標準之認可
  - 對某一項產品、過程或服務符合規定要求，由第三者出具書面保證之程序
- 認證(*Accreditation*)：對能力之認可
  - 主管機關對某人或某機構給於正式認可，證明其有能力執行某特定工作之程序

- 資料來源：財團法人全國認證基金會

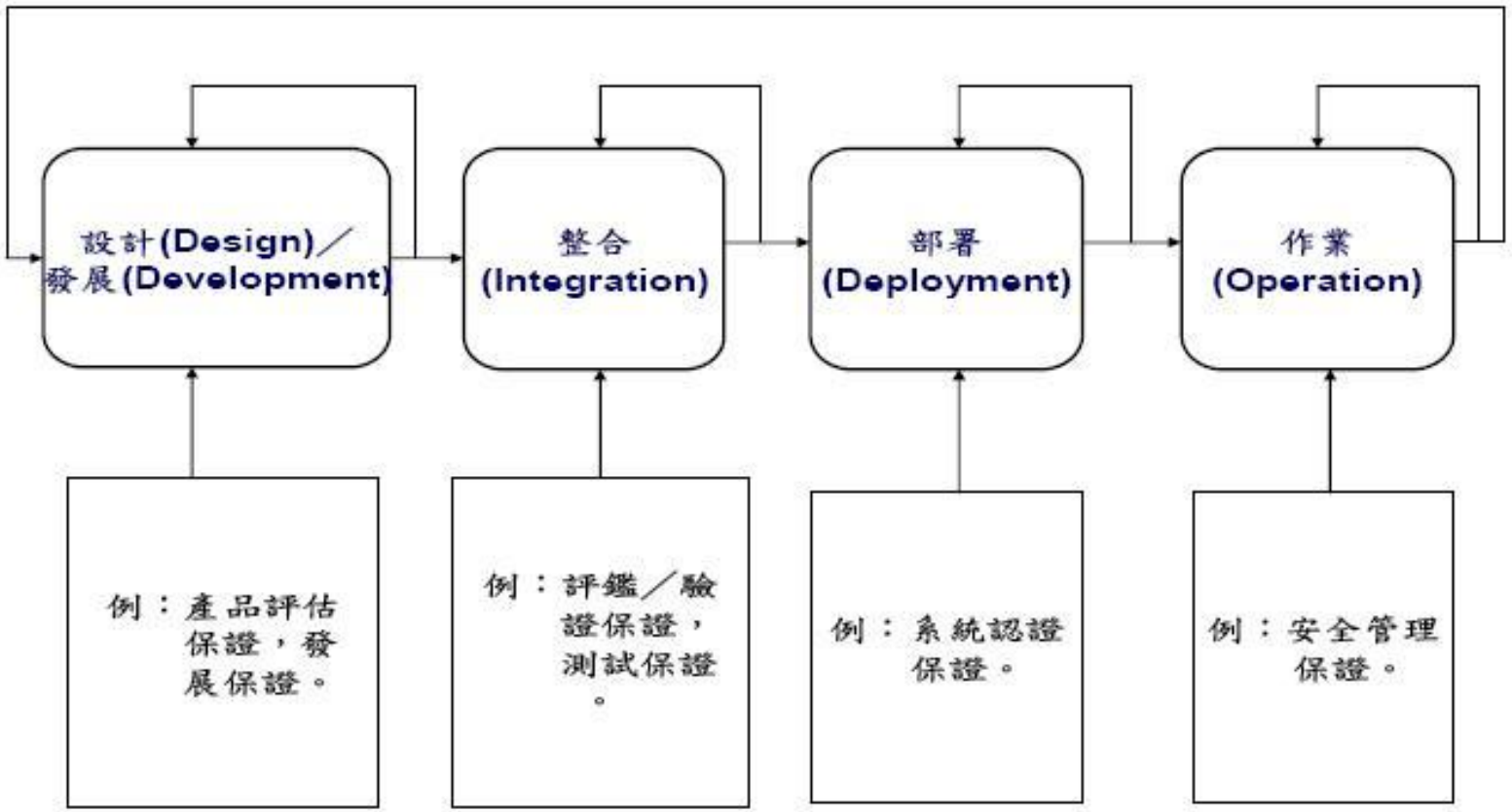
資訊安全保證(*Security Assurance*)

- *Assurance*：完成特定的活動或過程，使交付標的符合安全目標，以逐漸強化信心
- *1994* 年*ISO*開始探討對資訊產品與系統安全保證之資訊安全測試暨評鑑方法
- *1996* 年*ISO*擬提供資安人員，選擇適當之資訊保證的方法(或組合)，以達到資訊產品與系統，對安全保證之要求，開始制定*ISO/IEC 15443*系列標準。

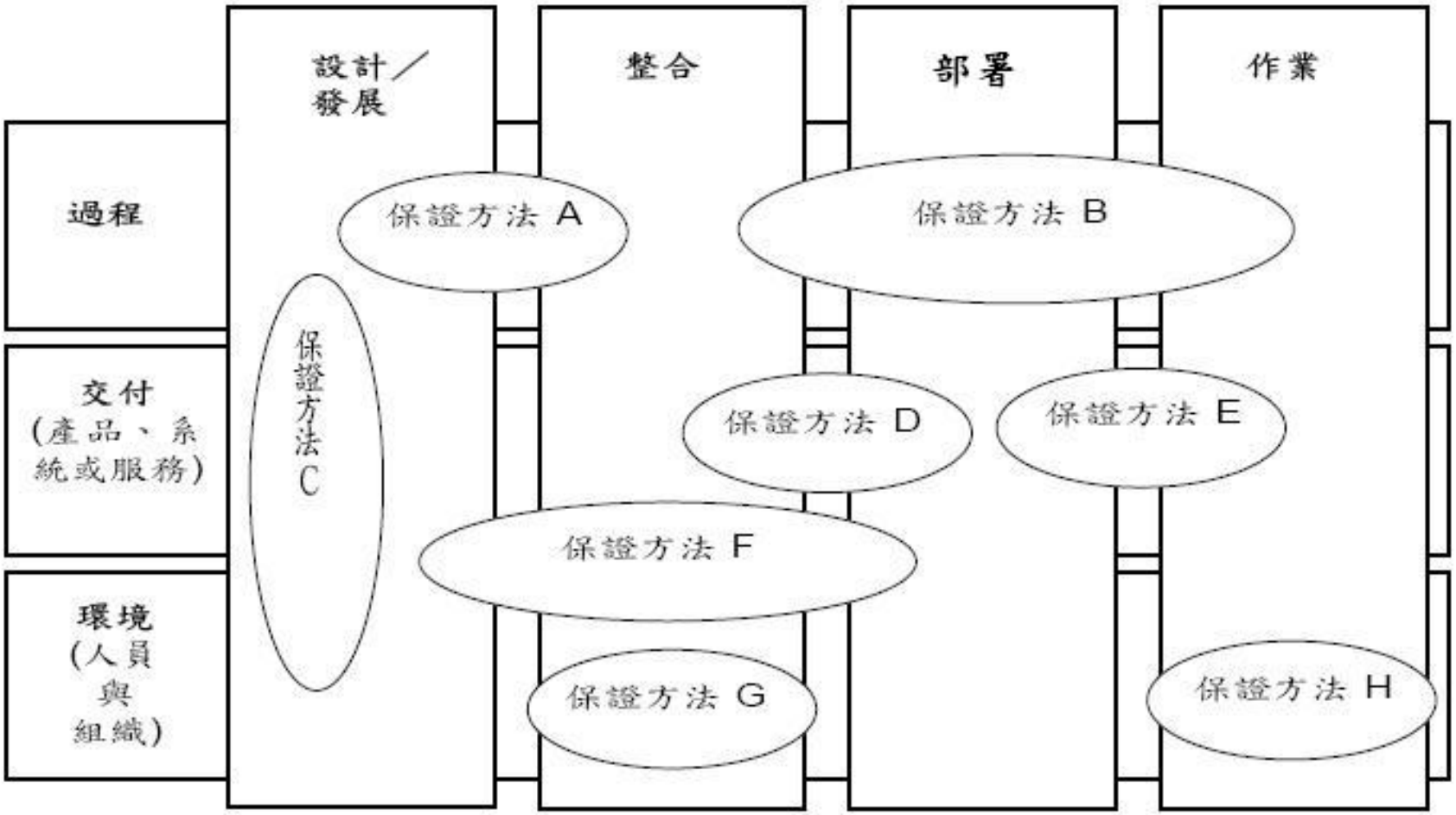
ISO/IEC 15443之發展

- *A framework for IT security assurance*
- *ISO/IEC 15443* 系列標準共有*3*部:
- *ISO/IEC TR 15443-1:2005*提出資訊技術安全保證之概觀與框架
- *ISO/IEC TR 15443-2:2005*就篩選出之*37*種測試暨評鑑，加以說明並提出其適用範圍的建議
- *ISO/IEC TR 15443-3:2007*分析資訊技術安全保證方法之性質，針對選出的下列文件暨其組合加以探討
  - *ISO/IEC 15408*、*ISO/IEC 19790*、*ISO/IEC 21827*、*ISO/IEC 13335*、*ISO/IEC 17799*

資訊安全保證階段劃分


設計(Design)／發展(Development)
整合(Integration)
部署(Deployment)
作業(Operation)
例：產品評估保證，發展保證。
例：評鑑／驗證保證，測試保證。
例：系統認證保證。
例：安全管理保證。

資訊安全保證方法之分類

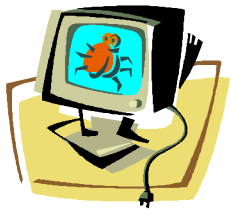


資訊保證相關標準應用範疇

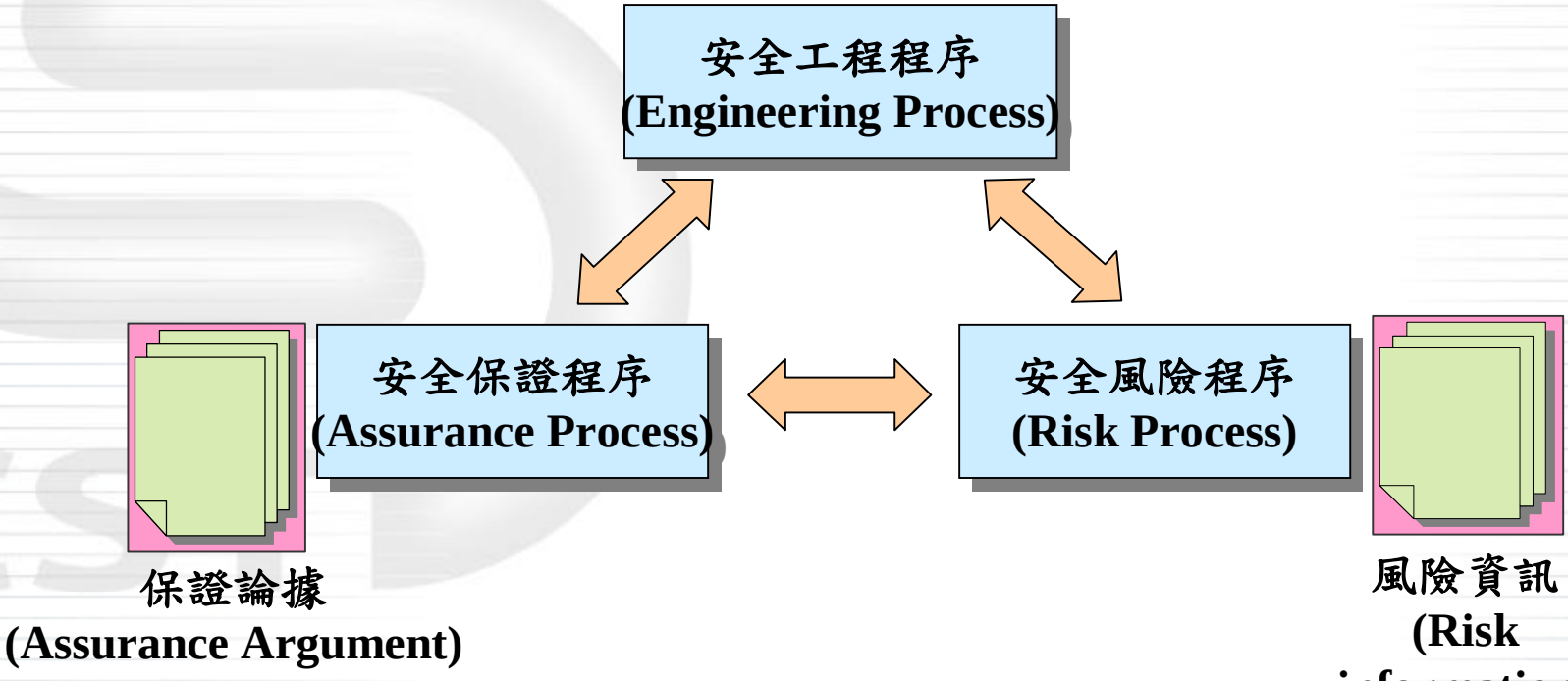
標準/階段/方法	設計/發展	整合	部署	作業
過程 (Process)	ISO/IEC 21827 ISO/IEC TR15504 ISO/IEC 15408	ISO/IEC 21827 ISO/IEC TR15504 ISO/IEC 13335	ISO/IEC 21827 ISO/IEC TR15504 ISO/IEC 13335	ISO/IEC 21827 ISO/IEC TR15504 ISO/IEC 13335 ISO/IEC 17799 ISO/IEC 27001
交付標的 (Deliverable)	ISO/IEC 14598 ISO/IEC 15408	ISO/IEC 14598 ISO/IEC 15408	ISO/IEC 14598 ISO/IEC 15408	ISO/IEC 14598 ISO/IEC 15408
環境 (組織/人員)	ISO/IEC 9000	ISO/IEC 9000 ISO/IEC 27001	ISO/IEC 9000 ISO/IEC 27001 ISO/IEC 17799	ISO/IEC 9000 ISO/IEC 27001 ISO/IEC 17799

ISO/IEC 21827
Security Engineering Process Overview

SSE-CMM：系統安全工程能力成熟度模式
（*Systems Security Engineering Capability Maturity Model*）

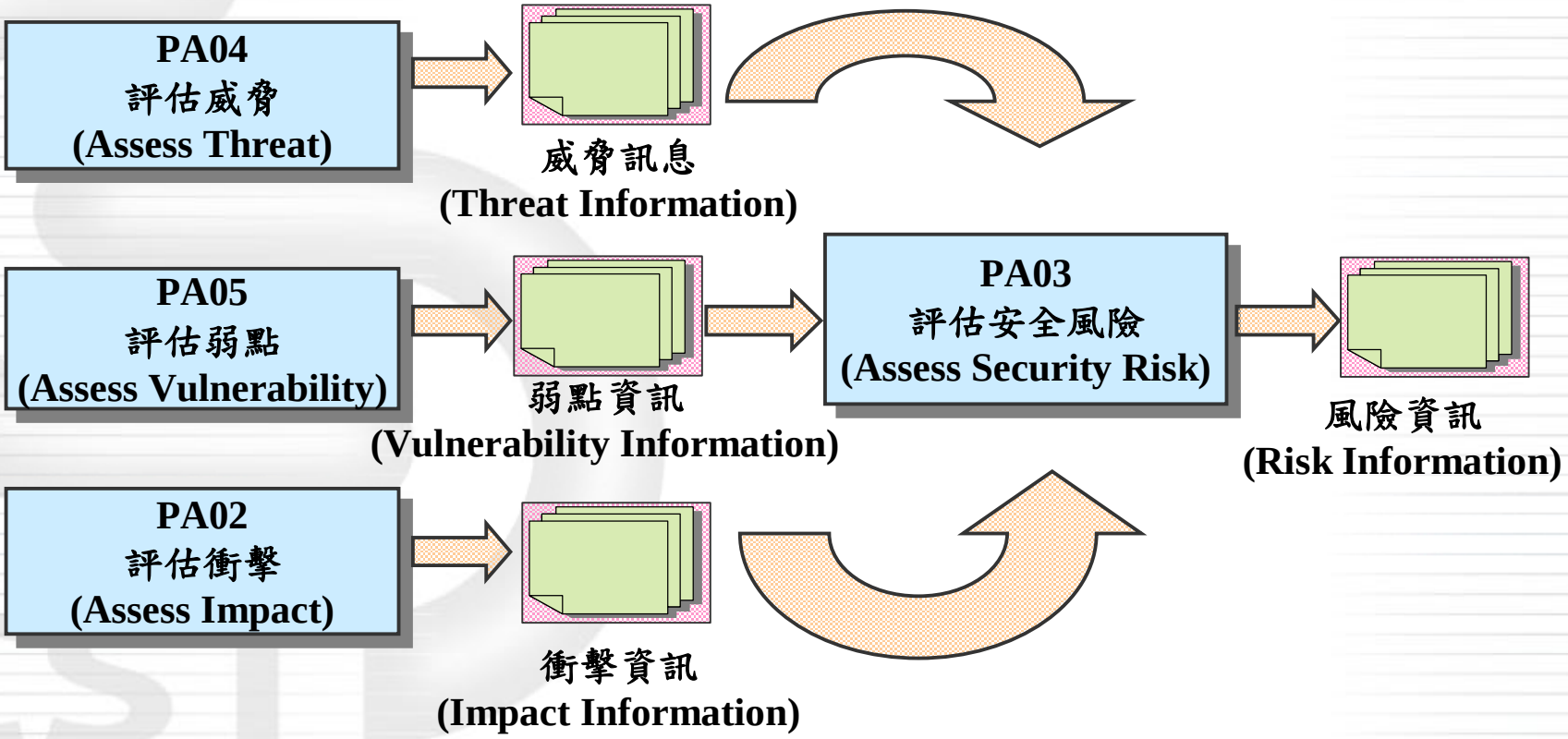


產品、系統、服務
(Product, System or Service)



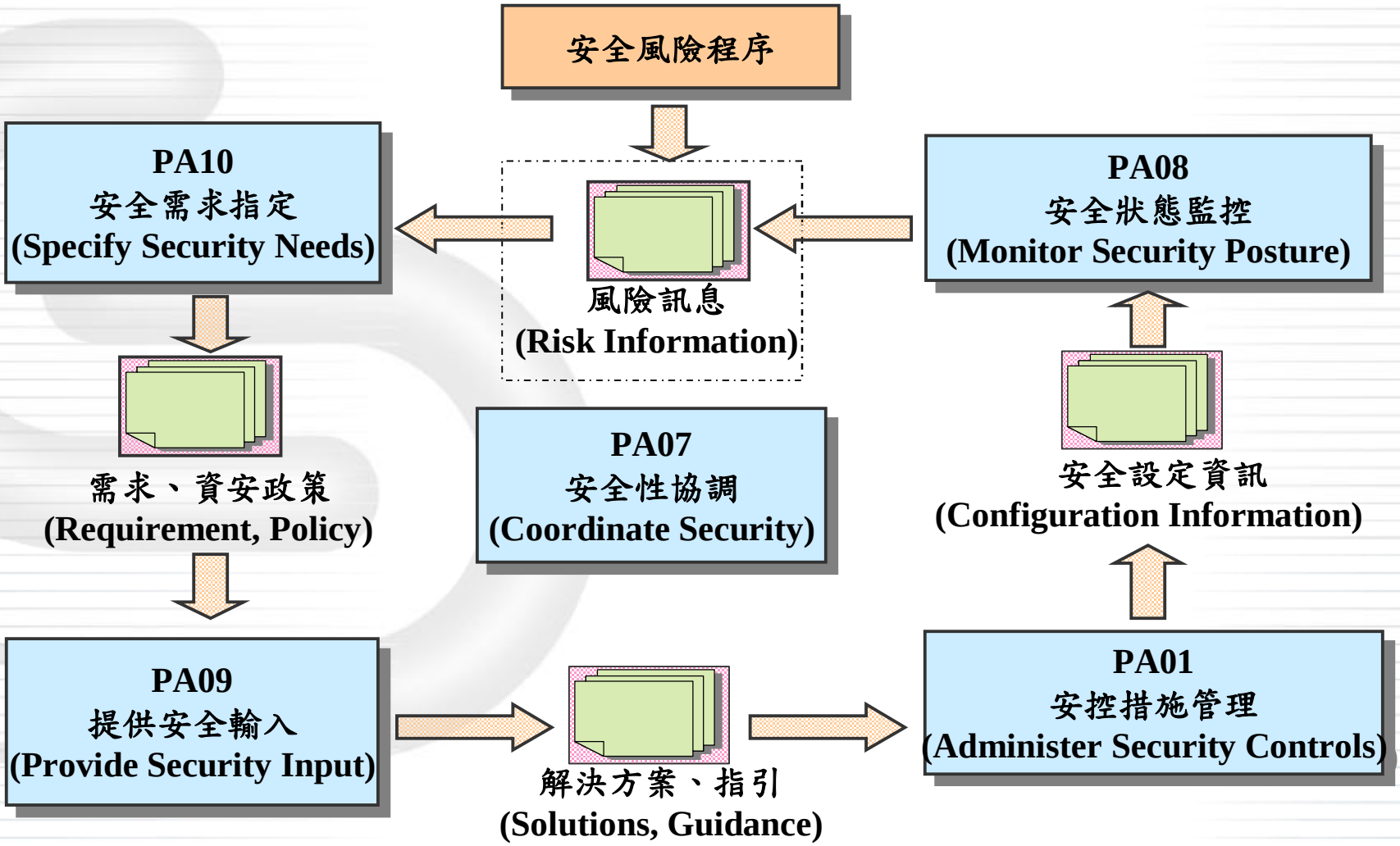
資料來源：ISO/IEC 21827

SSE-CMM 的安全風險程序



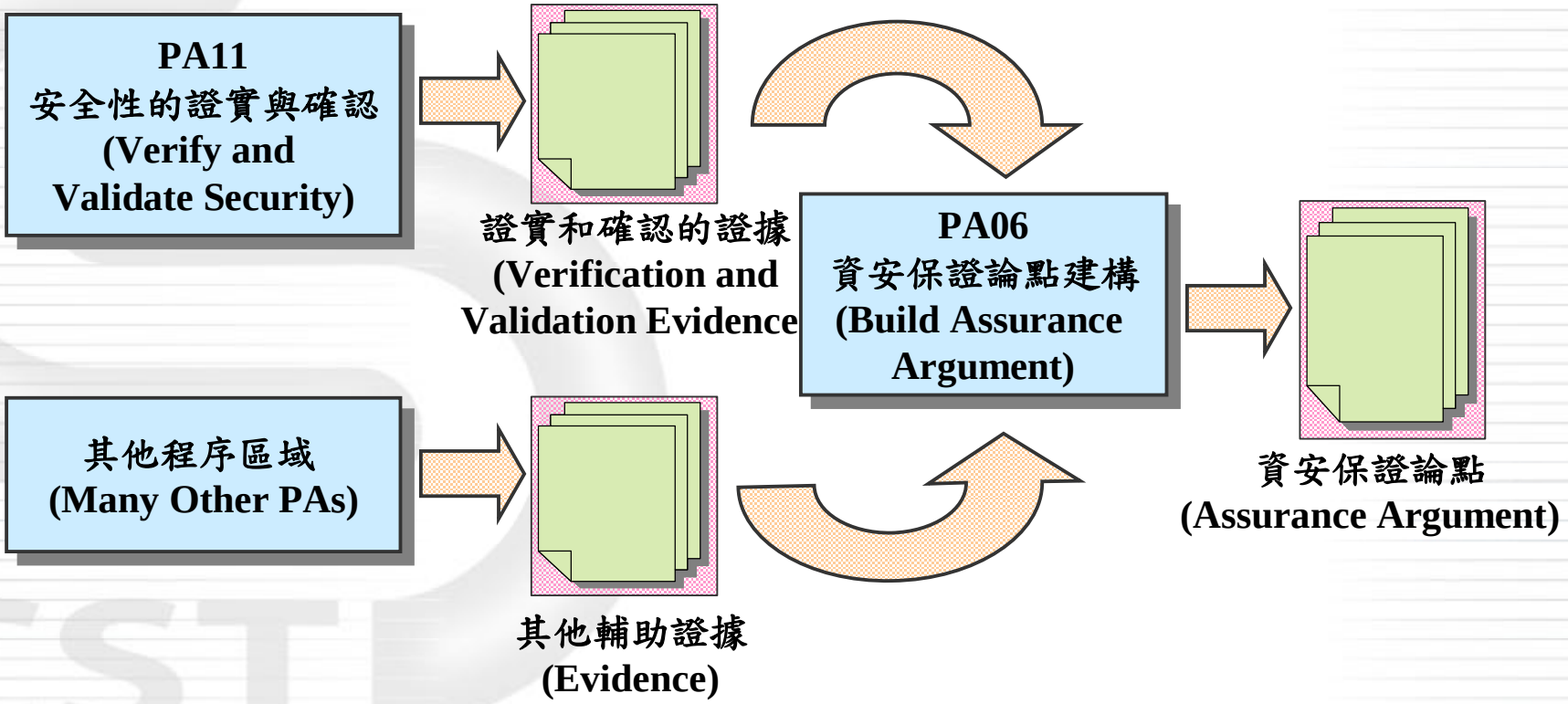
資料來源：SSE-CMM/ISO 21827

SSE-CMM 的安全工程程序



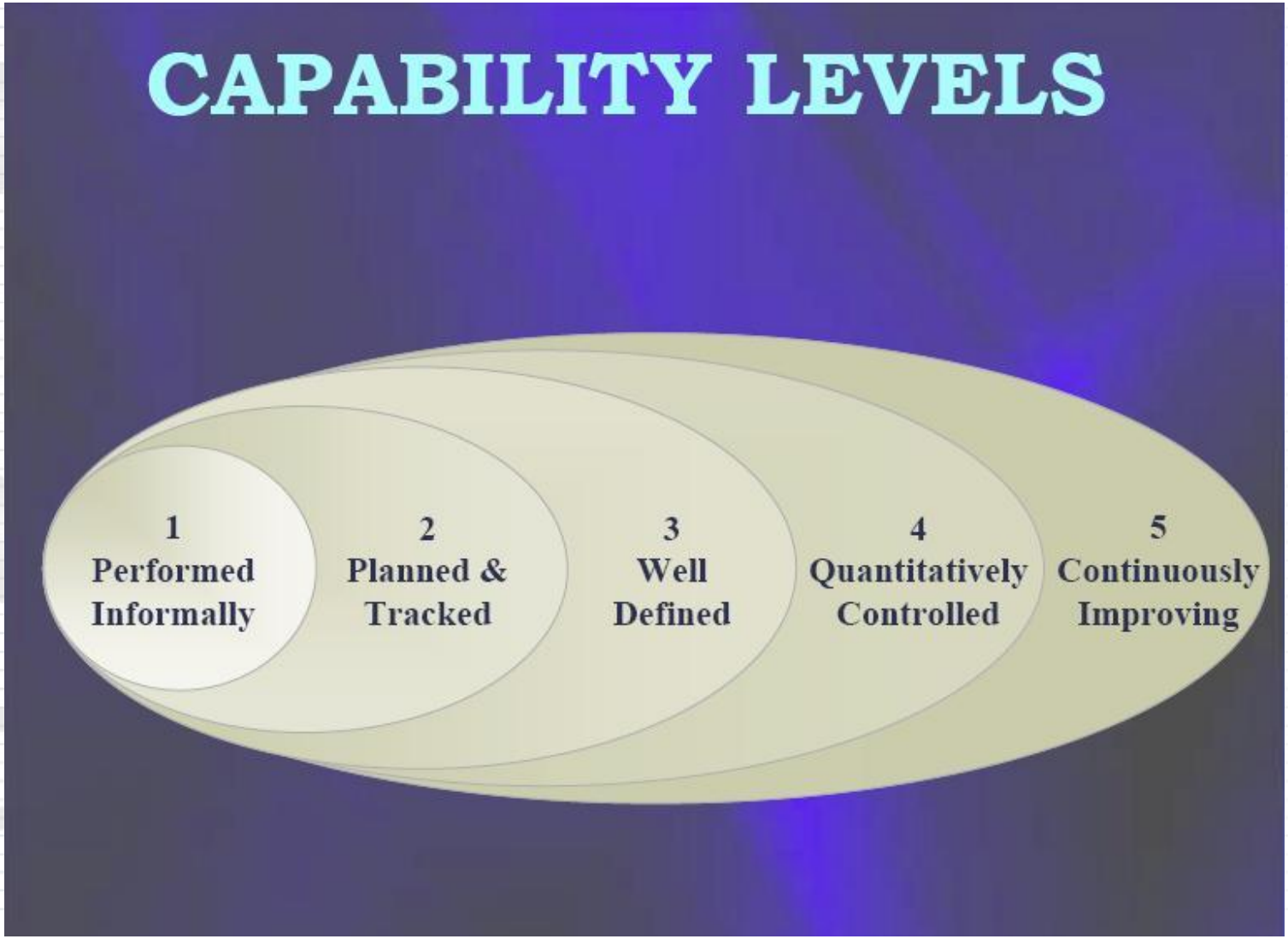
資料來源：SSE-CMM/ISO 21827

SSE-CMM 的安全保證程序



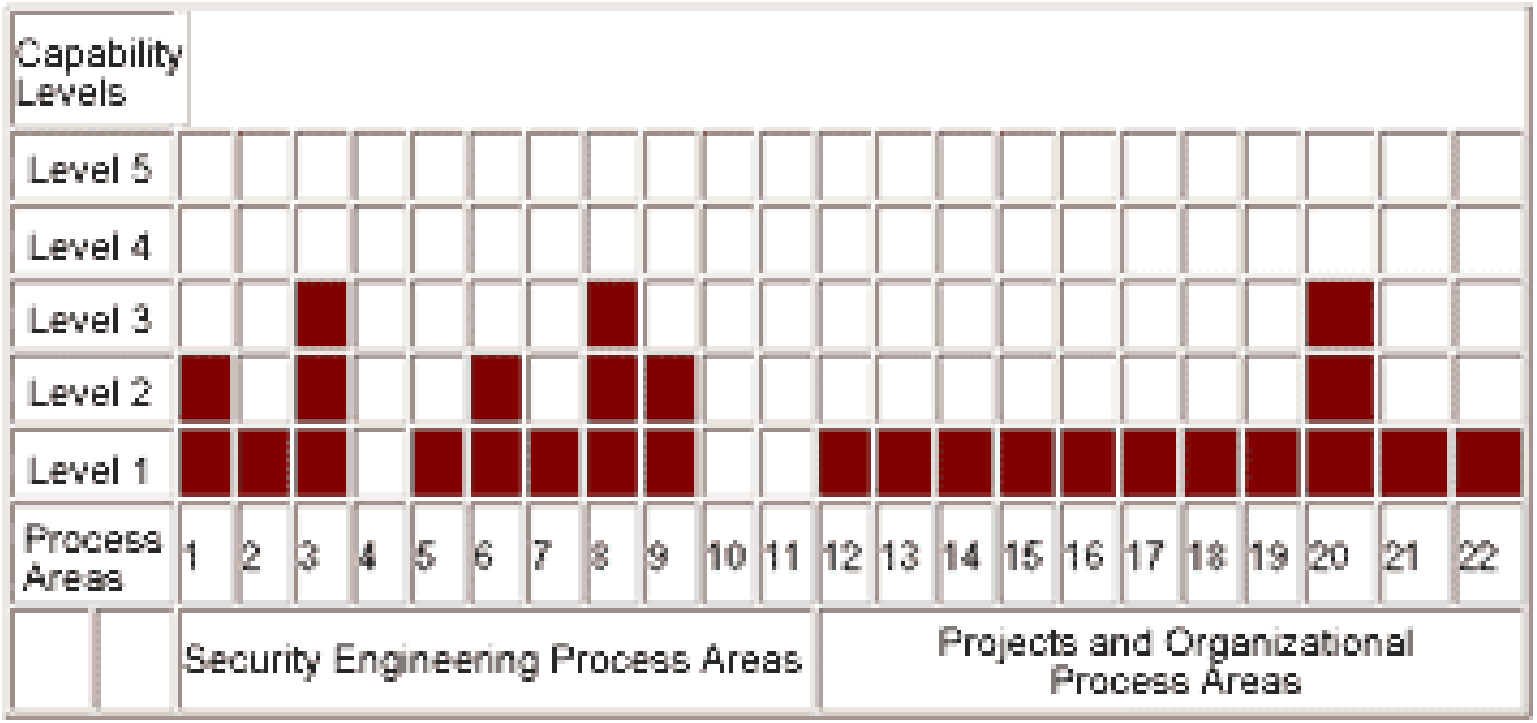
資料來源：SSE-CMM/ISO 21827

Capability Maturity Model (SSE-CMM)



ISO/IEC 21827

Baseline ,Minimum and Target Profile

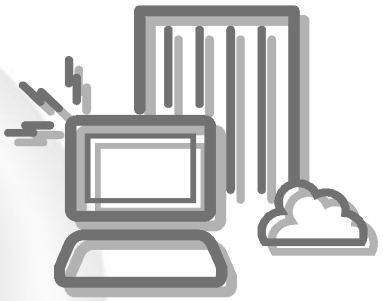


ISO/IEC 21827

課程大綱

一．何謂資訊安全？
二．資安風險管理
三．ISO/IEC/CNS資安標準
四．資訊安全保證(Security Assurance)
五．美國NIST資安文件架構
六．我國共通規範藍圖發展

NIST 風險管理框架(RMF)



1 生命週期起點

FIPS 199/SP800-60

資訊系統分類分級

依據「風險衝擊」損失,定義資訊系統安全「分類分級」

2

FIPS 200/SP800-53

選擇控制措施

在「可接受」的風險等級內選擇「足夠」控制措施,保護資訊系統

3 SP800-70

執行控制措施

在新建資訊系統或原有的資訊系統上「執行」控制措施,進行「安全設定」

4 SP800-53A

評鑑控制措施

根據「資訊系統安全等級」需求,評鑑「控制措施」實施的「有效性」

5 SP800-37

授權資訊系統

確認資訊系統與控制措施「安全保證」後,「授權」該資訊系統上線運作

6 SP800-37/ SP800-53A

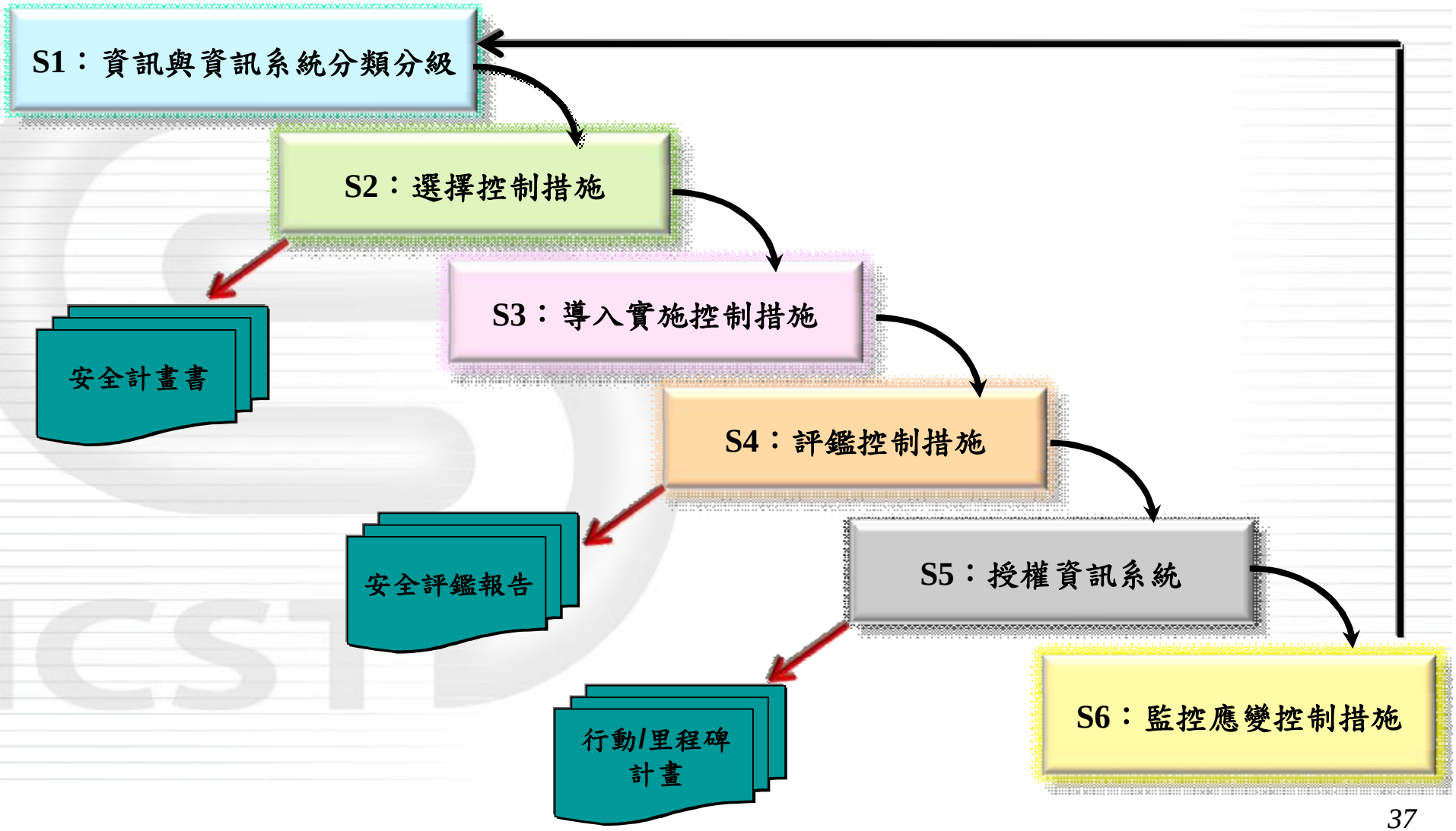
監控控制措施

配合資訊系統的後續變化,「持續調整」控制措施,以確保資訊系統安全等級,落實安全保證

資料來源：NIST SP800-39

36

資訊與資訊系統「風險管理之資安生命週期架構」



S2-選擇控制措施的程序

聯邦政府依據資訊與資訊系統
進行「資安分類分級」作業

選擇
基準控制措施

調整
基準控制措施

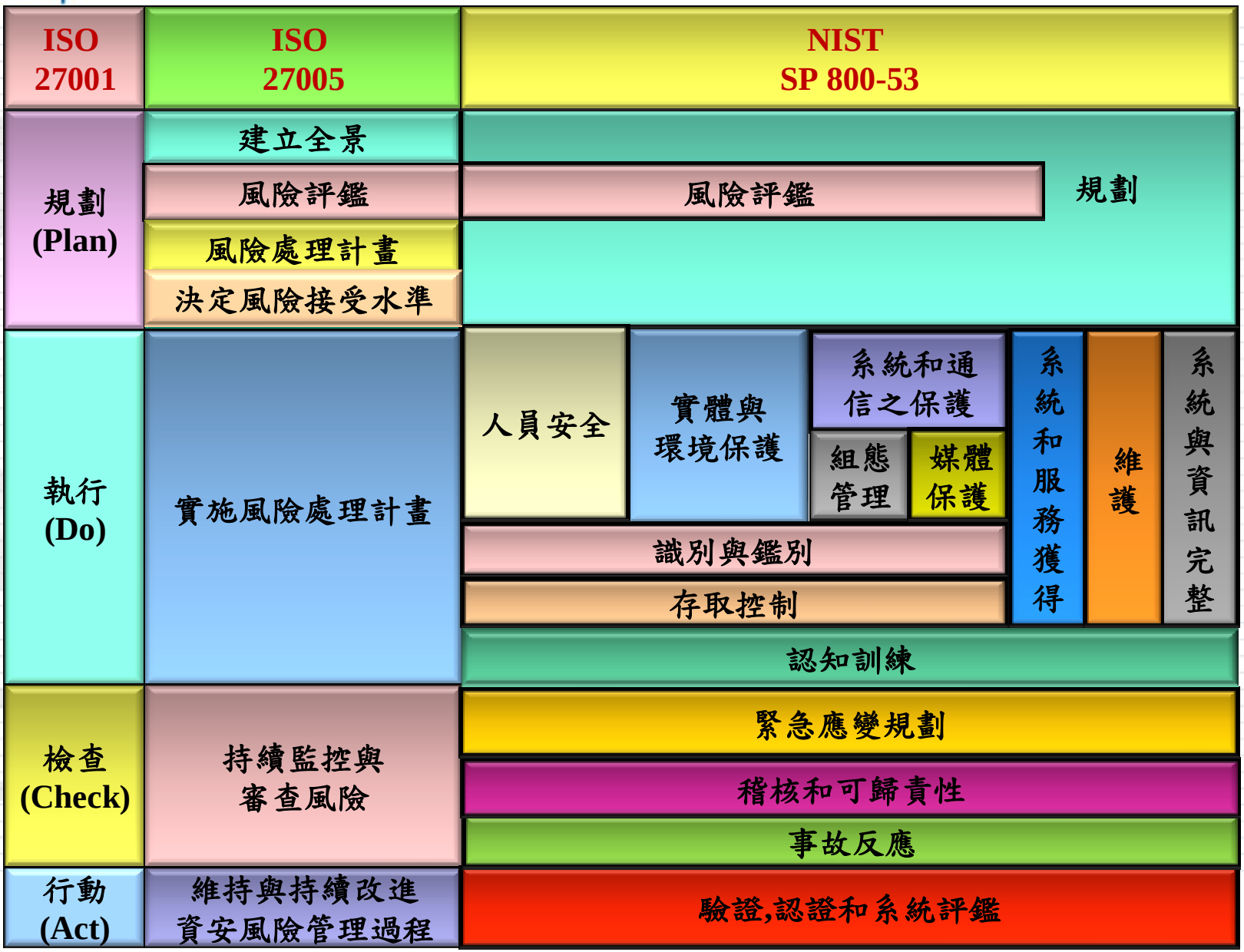
達成共識的
控制措施

修正指引的應用
1.「適用範疇」
2.「替代補償控制措施」
3.「控制措施組態設定」

風險評鑑/特殊需求
1. 額外「強化」控制措施來減輕
未被接受的資安風險

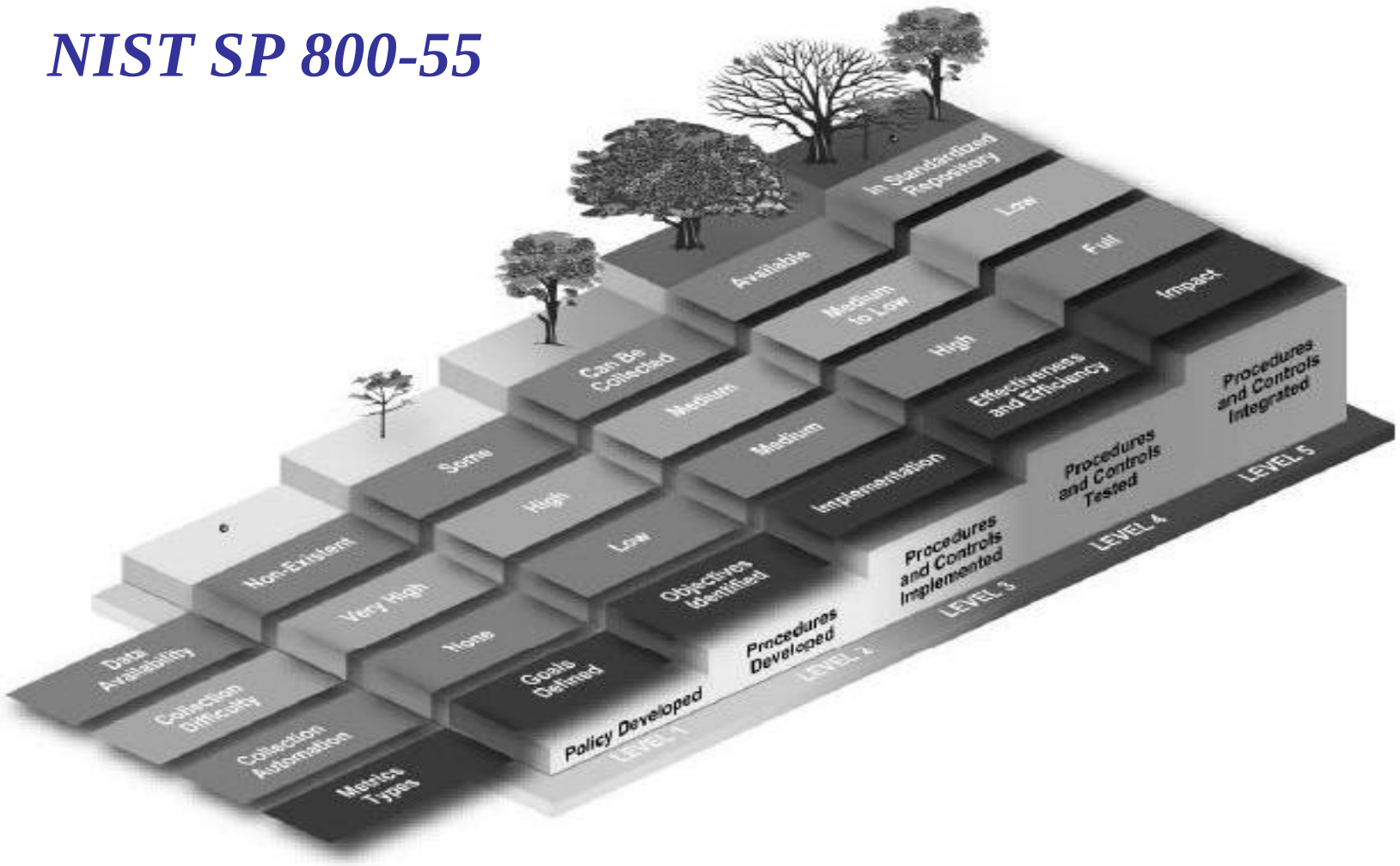
「文件化」控制措施-安全計畫書
解釋整體控制措施選擇、調整與強化過程以及
為何可以確保資安等級的「合理性」

NIST SP 800-53架構對照



Security Program Maturity and Types of Measurement

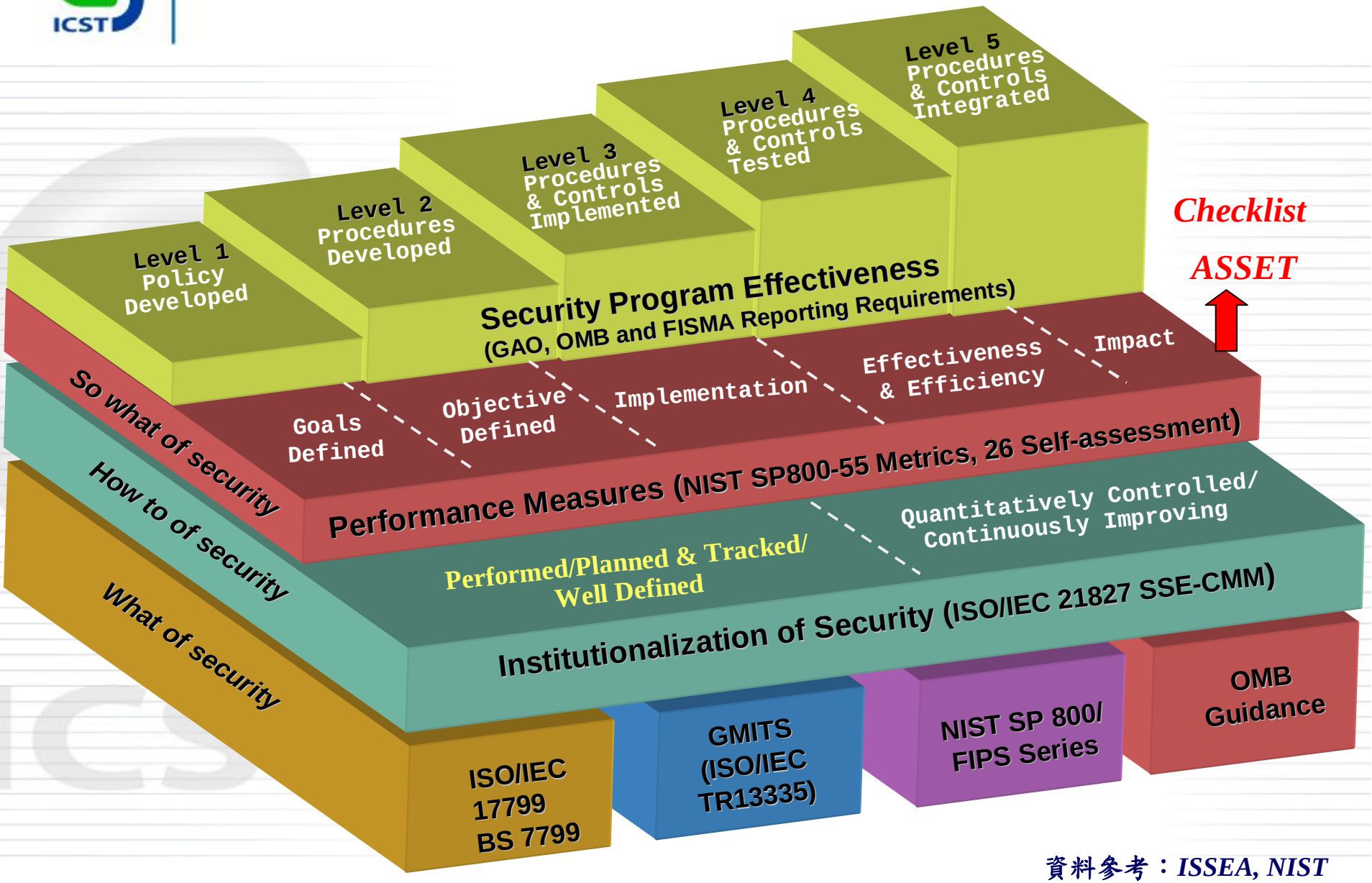
NIST SP 800-55



Metrics Types

Level	Level 1	Level 2	Level 3	Level 4	Level 5
Item	Policy Developed	Procedure Developed	Procedure and Controls Implemented	Procedure and Controls tested	Procedure and Controls Integrated
Metrics Type	Goals Defined	Objectives Identified	Implementation	Effectiveness and Efficiency	Impact
Collection Automation	None	Low	Medium	High	Full
Collection Difficulty	Very High	High	Medium	Medium To Low	Low
Data Availability	Non-existent	Some	Can be Collected	Available	Standardized Repository

美國聯邦政府資安評鑑架構



資料參考：*ISSEA, NIST*

課程大綱

一．何謂資訊安全？

二．資安風險管理

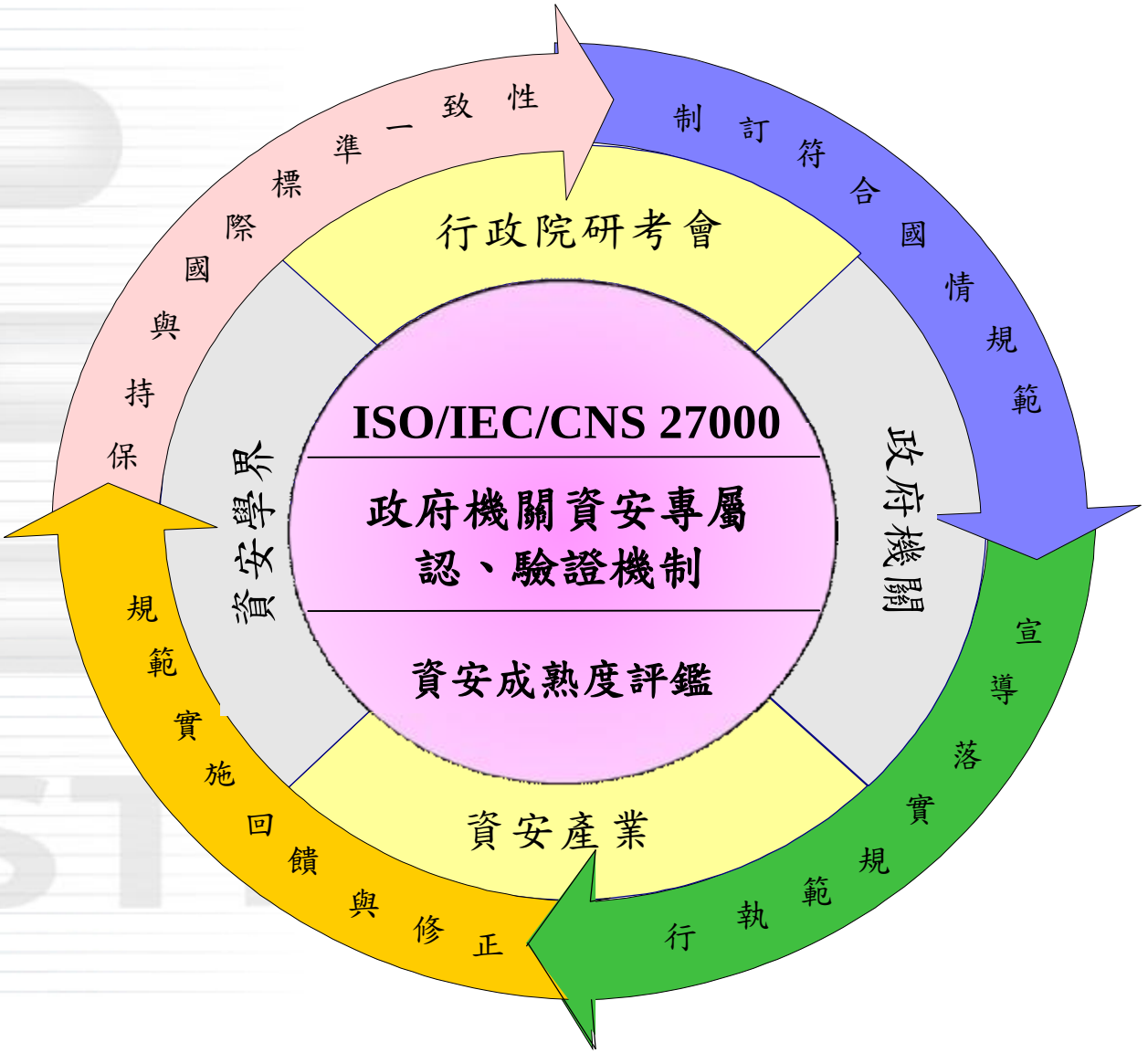
三．ISO/IEC/CNS資安標準

四．資訊安全保證(Security Assurance)

五．美國NIST資安文件架構

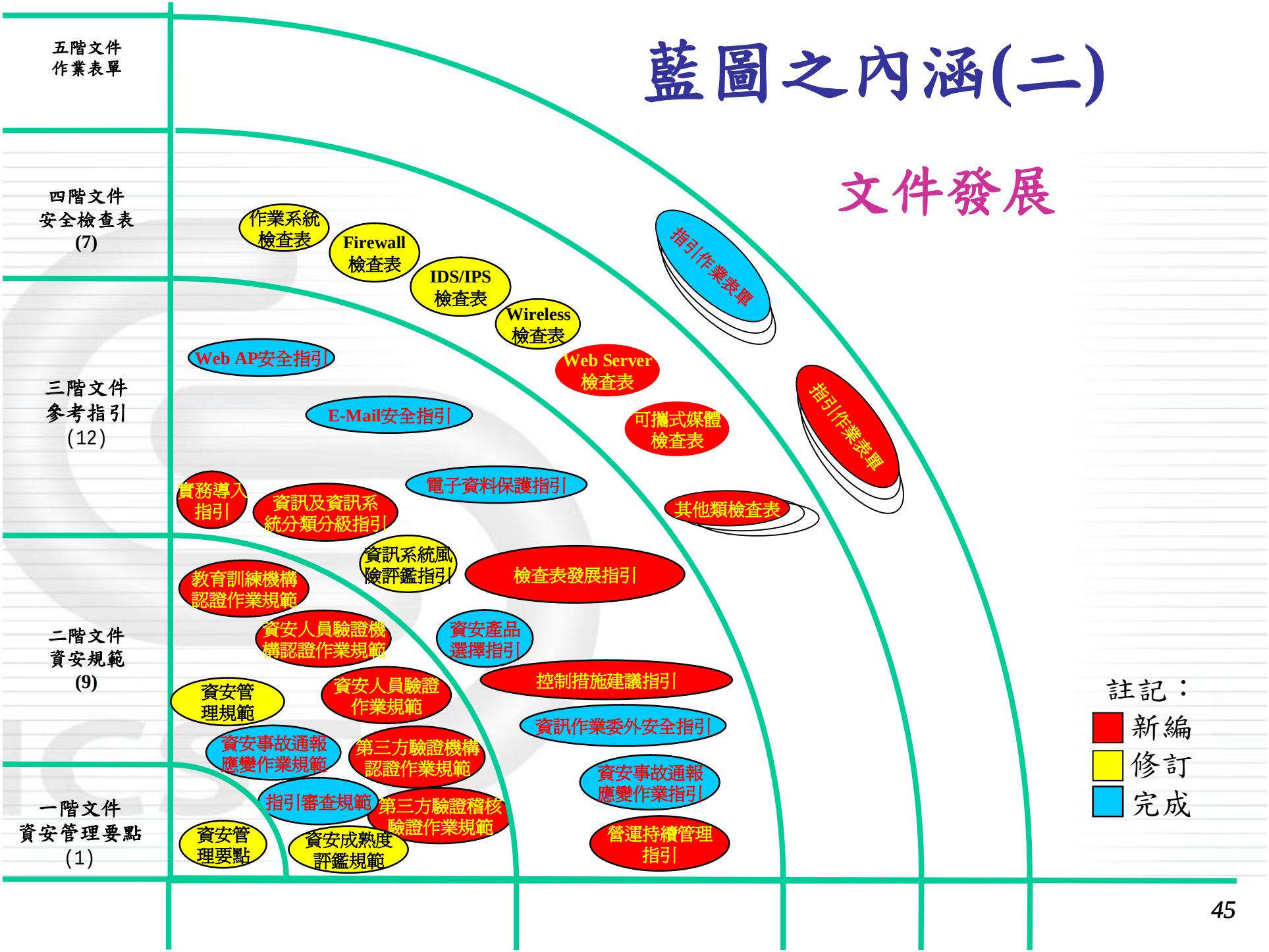
六．我國共通規範藍圖發展

97年度藍圖修訂目的

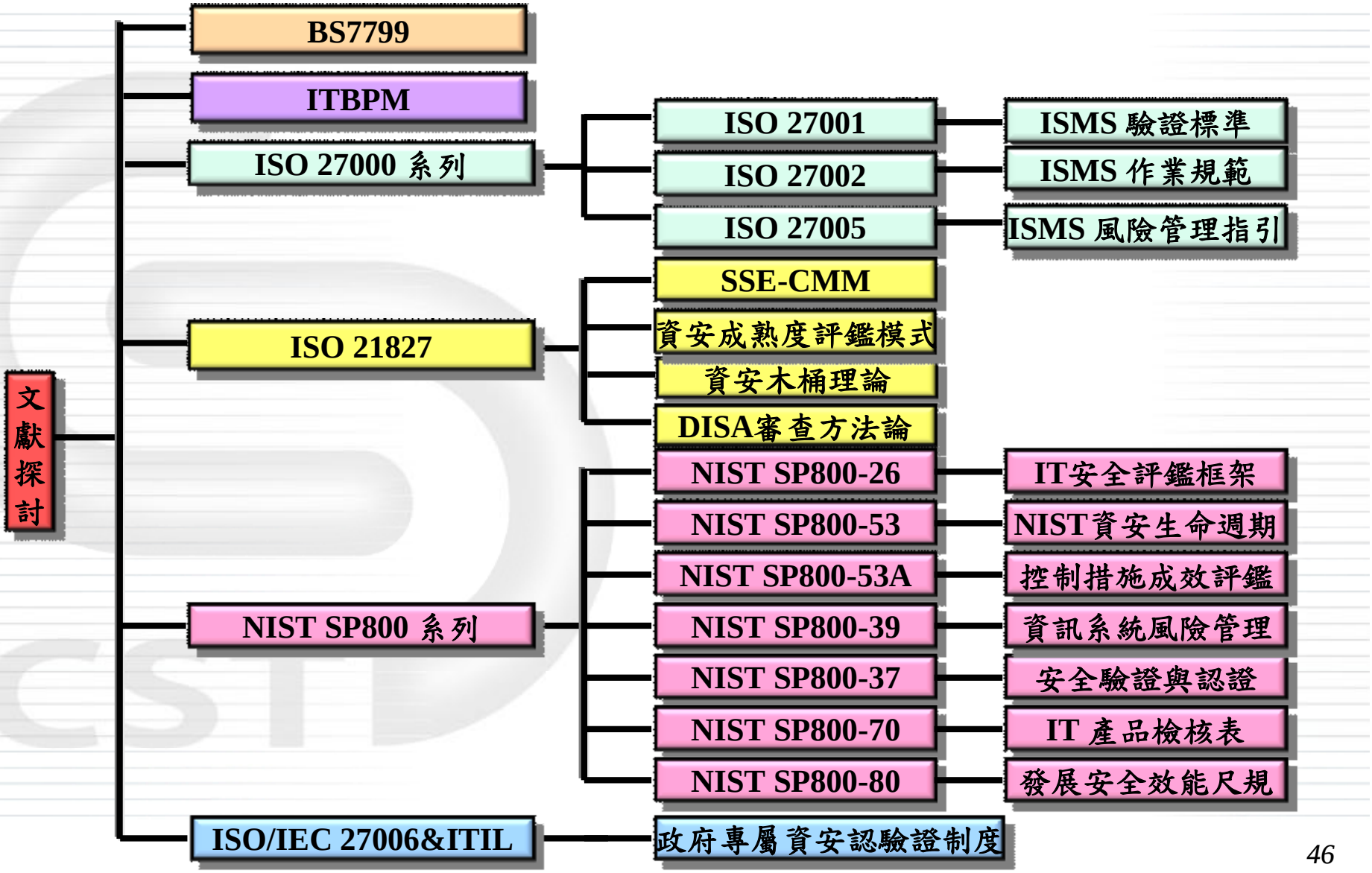

制訂符合國情規範
宣導落實規範執行
規範實施回饋與修正
國際標準一致性與持保
行政院研考會
政府機關
資安產業
資安學界
ISO/IEC/CNS 27000
政府機關資安專屬認、驗證機制
資安成熟度評鑑

藍圖之內涵(二)

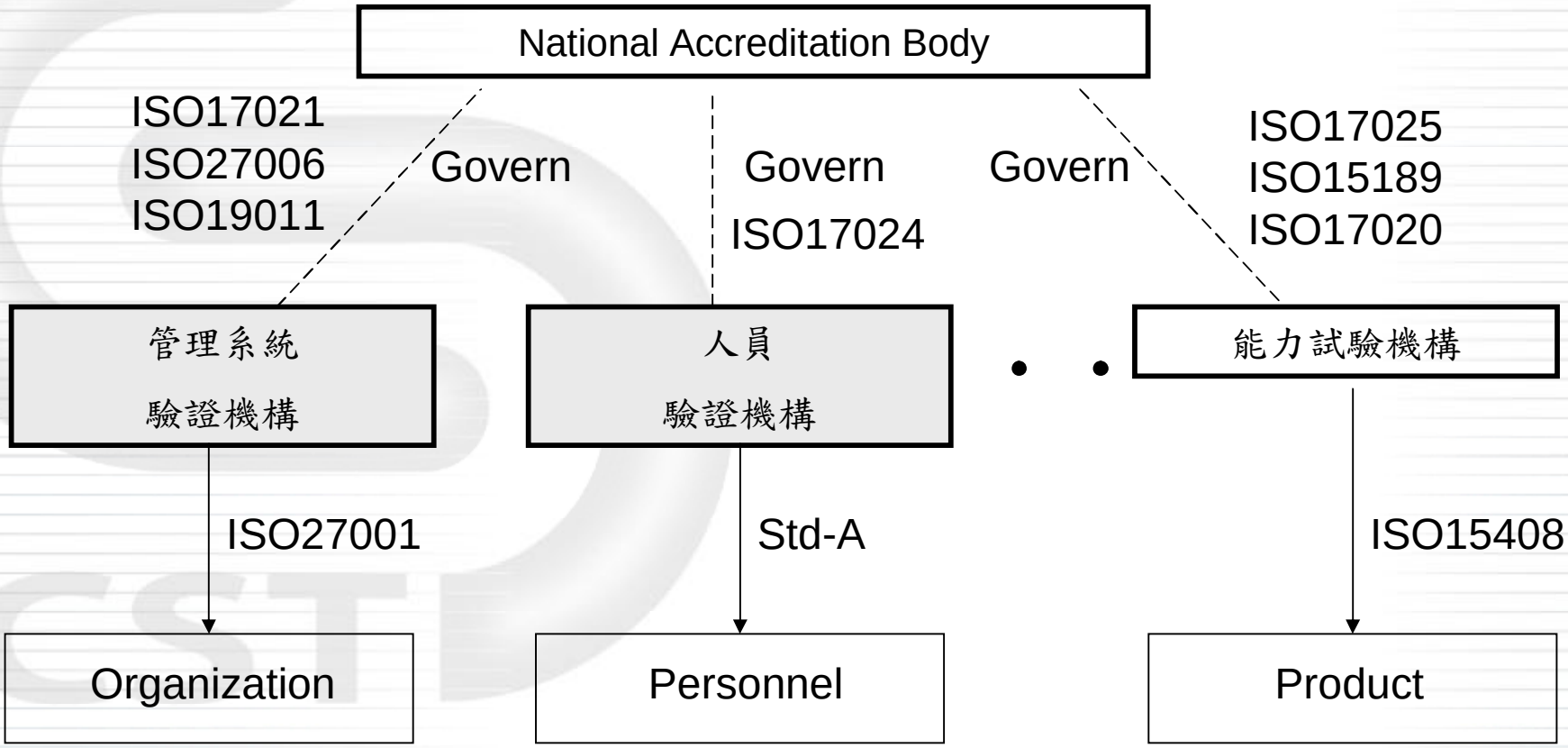
文件發展


五階文件
作業表單
四階文件
安全檢查表
(7)
三階文件
參考指引
(12)
二階文件
資安規範
(9)
一階文件
資安管理要點
(1)
作業系統檢查表
Firewall檢查表
IDS/IPS檢查表
Wireless檢查表
Web Server檢查表
可攜式媒體檢查表
其他類檢查表
指引作業表單
指引作業表單
Web AP安全指引
E-Mail安全指引
實務導入指引
資訊及資訊系統分類分級指引
電子資料保護指引
資訊系統風險評鑑指引
檢查表發展指引
教育訓練機構認證作業規範
資安人員驗證機構認證作業規範
資安產品選擇指引
控制措施建議指引
資安管理規範
資安人員驗證作業規範
資訊作業委外安全指引
資安事故通報應變作業規範
第三方驗證機構認證作業規範
資安事故通報應變作業指引
指引審查規範
第三方驗證稽核驗證作業規範
營運持續管理指引
資安管理要點
資安成熟度評鑑規範
註記：
新編
修訂
完成

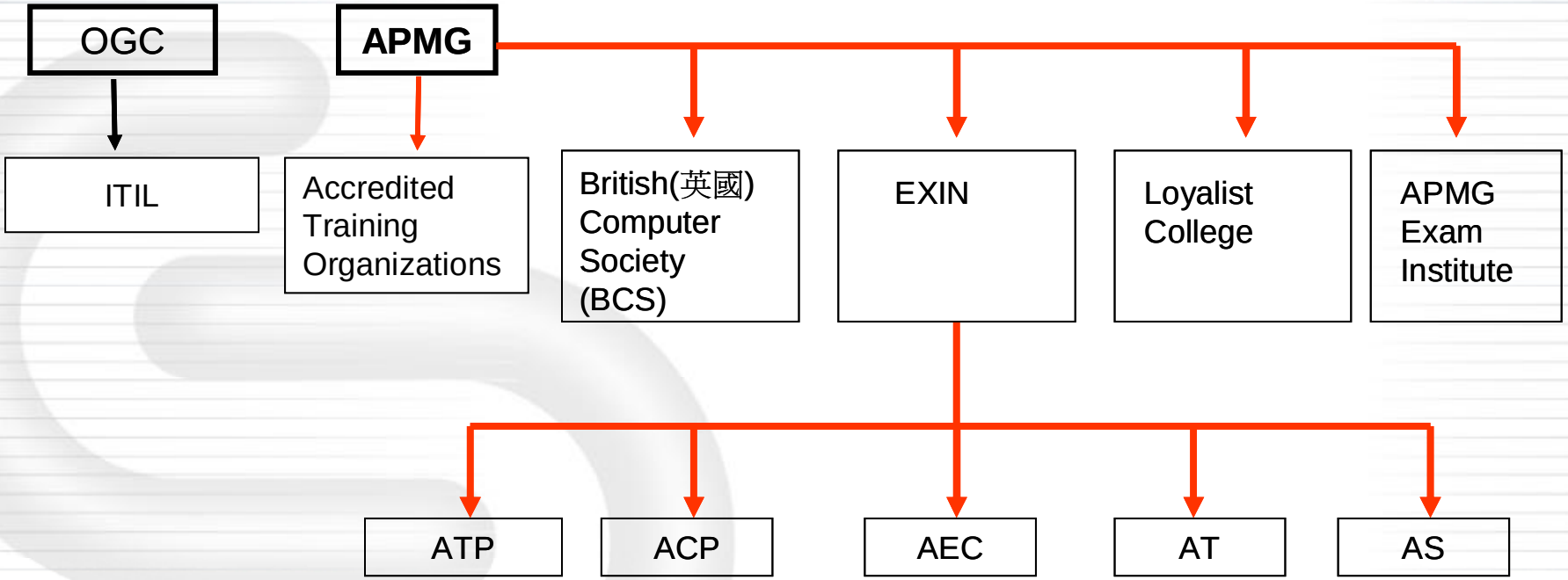
文獻探討之架構


文獻探討
BS7799
ITBPM
ISO 27000 系列
ISO 27001
ISMS 驗證標準
ISO 27002
ISMS 作業規範
ISO 27005
ISMS 風險管理指引
ISO 21827
SSE-CMM
資安成熟度評鑑模式
資安木桶理論
DISA審查方法論
NIST SP800 系列
NIST SP800-26
IT安全評鑑框架
NIST SP800-53
NIST資安生命週期
NIST SP800-53A
控制措施成效評鑑
NIST SP800-39
資訊系統風險管理
NIST SP800-37
安全驗證與認證
NIST SP800-70
IT 產品檢核表
NIST SP800-80
發展安全效能尺規
ISO/IEC 27006&ITIL
政府專屬資安認驗證制度

The ISO National Accreditation Scheme

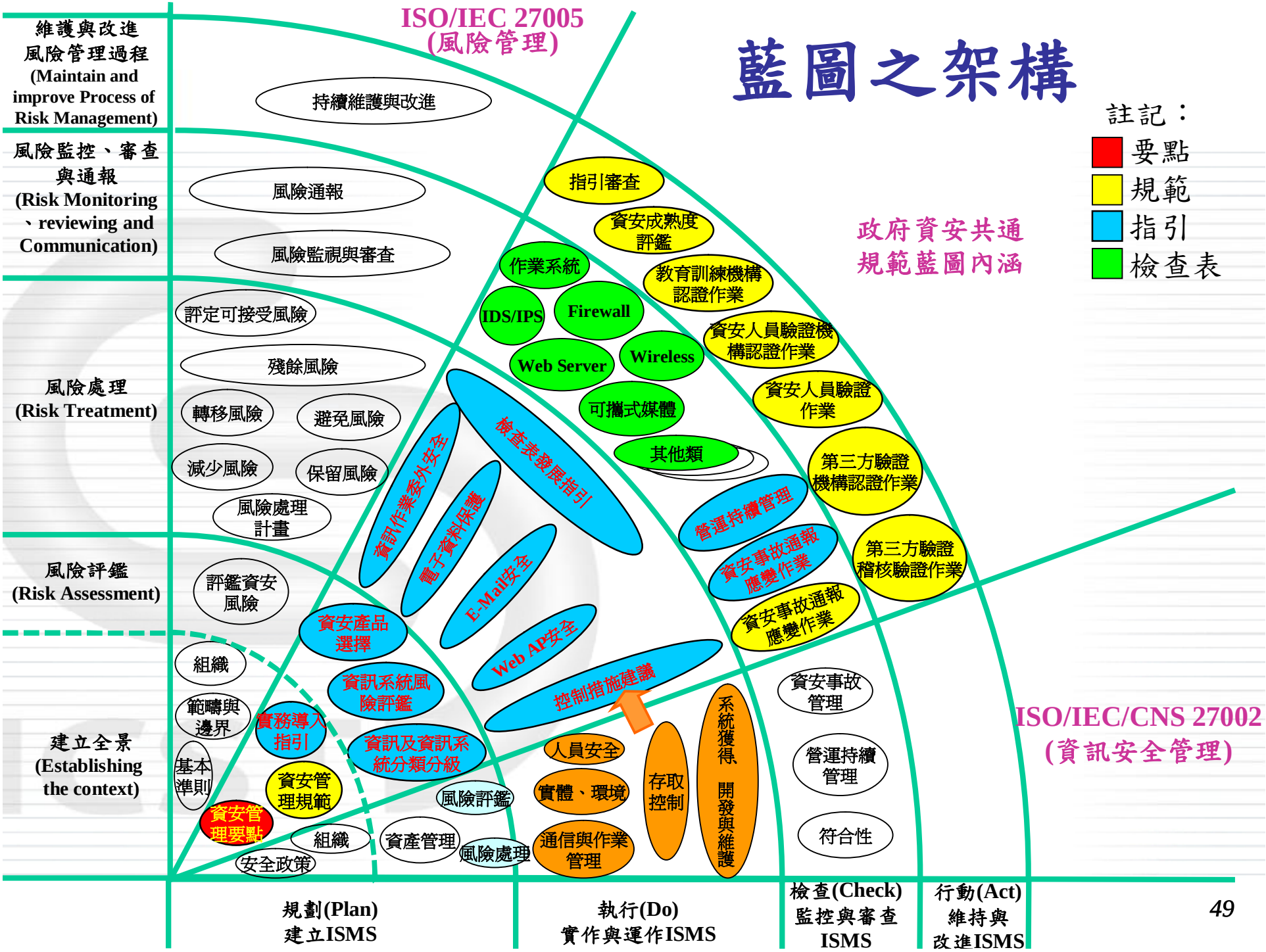


The ITIL Accreditation Scheme



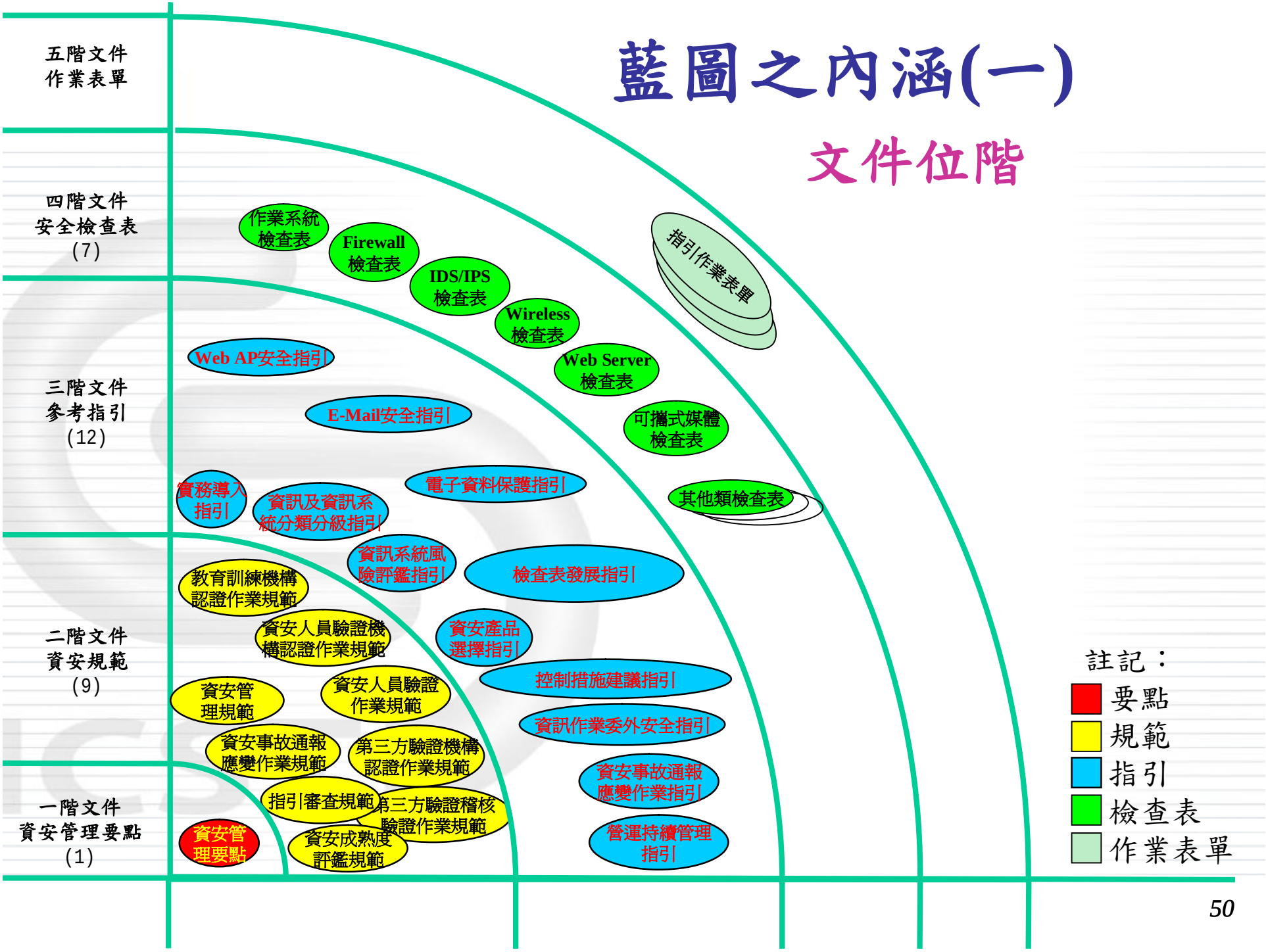
Accredited Training Provider [認證之課程提供商]
Accredited Courseware Provider [認證之教材提供商]
Accredited Examination Center [認證之考試中心]
Accredited Trainer [認證之講師]
Accredited Supervisor [認證之監考人員]
英國政府商務辦公室（ Office of Government Commerce）
APMG [英國的稽核機關]
EXIN is the leading Examination Institute for ITIL® certification
OGC(Open Geospatial Consortium)

藍圖之架構

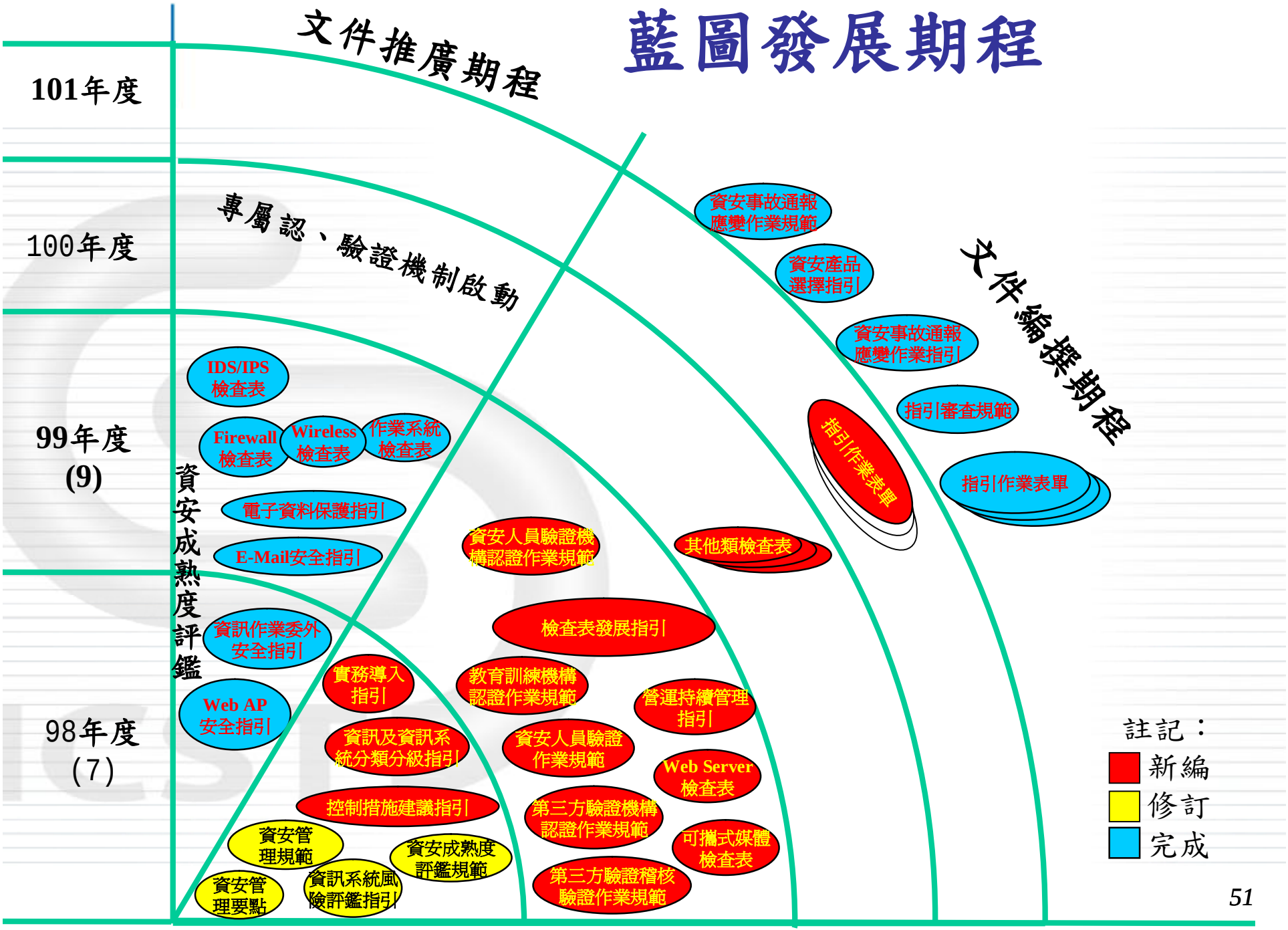

ISO/IEC 27005
(風險管理)
維護與改進
風險管理過程
(Maintain and
improve Process of
Risk Management)
持續維護與改進
風險監控、審查
與通報
(Risk Monitoring
、reviewing and
Communication)
風險通報
風險監視與審查
風險處理
(Risk Treatment)
評定可接受風險
殘餘風險
轉移風險
避免風險
減少風險
保留風險
風險處理
計畫
風險評鑑
(Risk Assessment)
評鑑資安
風險
建立全景
(Establishing
the context)
組織
範疇與
邊界
基本
準則
資務導入
指引
資安管
理規範
資安管
理要點
組織
安全政策
資產管理
風險評鑑
風險處理
資訊及資訊系
統分類分級
資訊系統風
險評鑑
資安產品
選擇
資訊作業委外安全
電子資料保護
E-Mail安全
Web AP安全
檢查表發展指引
控制措施建議
指引審查
資安成熟度
評鑑
作業系統
IDS/IPS
Firewall
Web Server
Wireless
可攜式媒體
其他類
教育訓練機構
認證作業
資安人員驗證機
構認證作業
資安人員驗證
作業
第三方驗證
機構認證作業
第三方驗證
稽核驗證作業
營運持續管理
資安事故通報
應變作業
資安事故通報
應變作業
人員安全
實體、環境
通信與作業
管理
存取
控制
系統獲得、
開發與維護
資安事故
管理
營運持續
管理
符合性
政府資安共通
規範藍圖內涵
註記：
要點
規範
指引
檢查表
ISO/IEC/CNS 27002
(資訊安全管理)
規劃(Plan)
建立ISMS
執行(Do)
實作與運作ISMS
檢查(Check)
監控與審查
ISMS
行動(Act)
維持與
改進ISMS

藍圖之內涵(一)

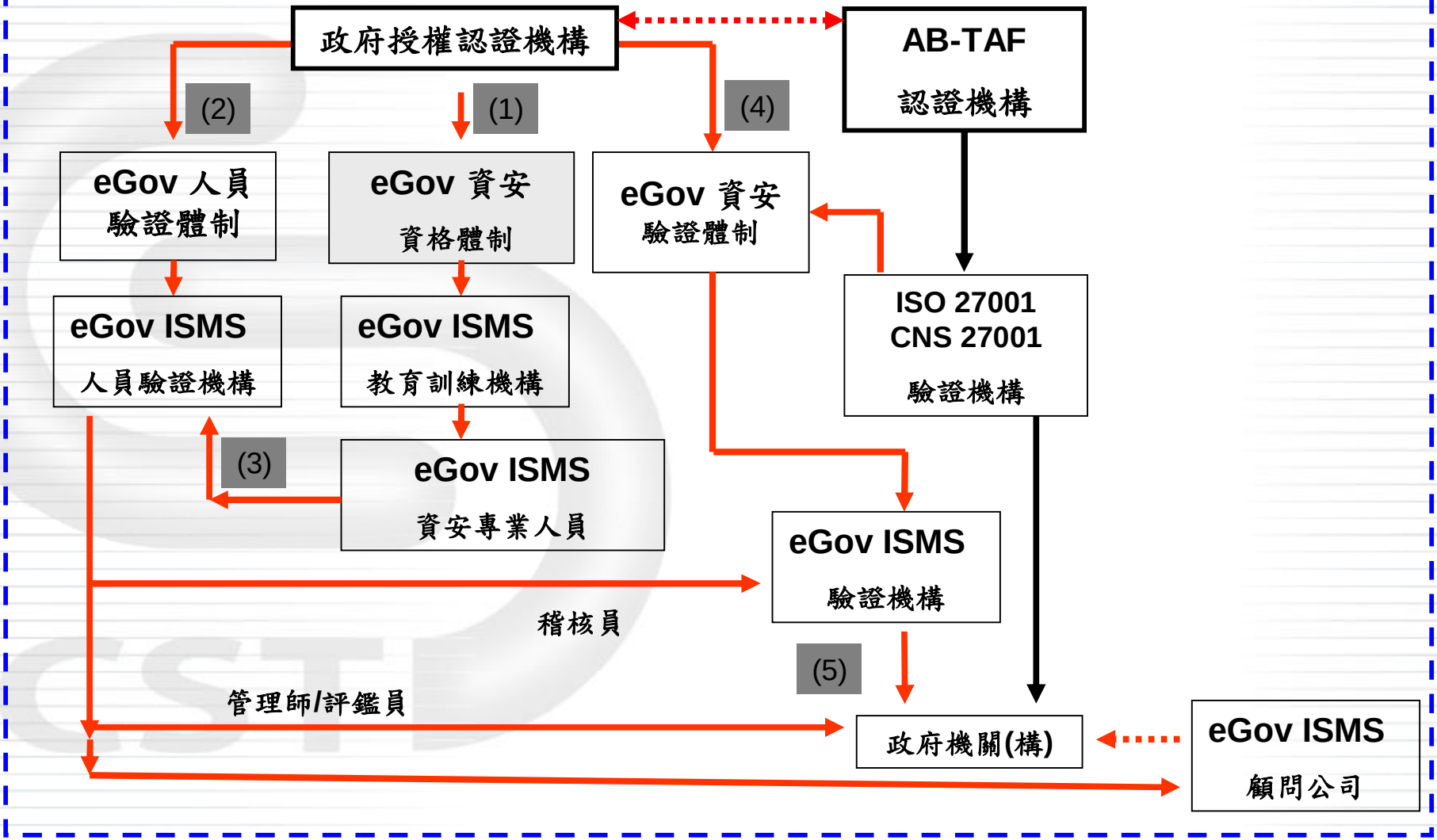
文件位階


五階文件
作業表單
四階文件
安全檢查表
(7)
三階文件
參考指引
(12)
二階文件
資安規範
(9)
一階文件
資安管理要點
(1)
作業系統檢查表
Firewall檢查表
IDS/IPS檢查表
Wireless檢查表
Web Server檢查表
可攜式媒體檢查表
其他類檢查表
指引作業表單
Web AP安全指引
E-Mail安全指引
電子資料保護指引
資務導入指引
資訊及資訊系統分類分級指引
資訊系統風險評鑑指引
檢查表發展指引
教育訓練機構認證作業規範
資安人員驗證機構認證作業規範
資安產品選擇指引
控制措施建議指引
資安管理規範
資安人員驗證作業規範
資訊作業委外安全指引
資安事故通報應變作業規範
第三方驗證機構認證作業規範
資安事故通報應變作業指引
指引審查規範
第三方驗證稽核驗證作業規範
營運持續管理指引
資安管理要點
資安成熟度評鑑規範
註記：
要點
規範
指引
檢查表
作業表單

藍圖發展期程


文件推廣期程
專屬認、驗證機制啟動
文件編撰期程
101年度
100年度
99年度
(9)
98年度
(7)
資安成熟度評鑑
資安事故通報應變作業規範
資安產品選擇指引
資安事故通報應變作業指引
指引審查規範
指引作業表單
指引作業表單
IDS/IPS檢查表
Firewall檢查表
Wireless檢查表
作業系統檢查表
電子資料保護指引
E-Mail安全指引
資安人員驗證機構認證作業規範
其他類檢查表
資訊作業委外安全指引
檢查表發展指引
實務導入指引
教育訓練機構認證作業規範
營運持續管理指引
Web AP安全指引
資訊及資訊系統分類分級指引
資安人員驗證作業規範
Web Server檢查表
控制措施建議指引
第三方驗證機構認證作業規範
資安管理規範
資安成熟度評鑑規範
可攜式媒體檢查表
資安管理要點
資訊系統風險評鑑指引
第三方驗證稽核驗證作業規範
註記：
新編
修訂
完成

政府機關資安專屬認、驗證機制



預期效益

- 資安指引架構之發展
  - 資安風險管理生命週期架構
- 資安作業程序之制訂
  - 根據機關之資安防護等級定義其資安政策及程序
- 資安資源分配之參考
  - 文件發展程序、宣導推廣、教育訓練與修訂維護
- 藍圖發展期程之建議
  - 規劃相關工作的資安工作時程
- 資安成熟等級之評鑑
  - 進行資安成熟度評鑑，符合「資訊安全保證」之要求
- 認、驗證體制之建立
  - 包含教育訓練機構、師資、教材、資訊人員、資安稽核人員及政府機關(構)的認驗證體系

政府資安作業共通規範網站
http://www.giscc.org.tw/giscc/

資安工作的體會

資安最大的威脅？　就是不知道威脅！

資安最大的危機？　也是最大的轉機！

資安最大的績效？　竟是看不到績效！

錢不是資安問題？　問題是不會找錢！

人是最大的資產？　但也是最大挑戰！

認知是最小投資？　然卻是最大回報！

55

問題與討論