議題1. 打造安全信賴的資通訊環境
1.2 安全及信賴的電子化政府服務

行政院研究發展考核委員會

2009年8月18日

內容綱要

壹、施政願景

貳、現況分析

參、發展趨勢

肆、具體策略

伍、行動方案

陸、討論題綱

壹、施政願景

優質網路政府計畫(2008-2011年)

願景：

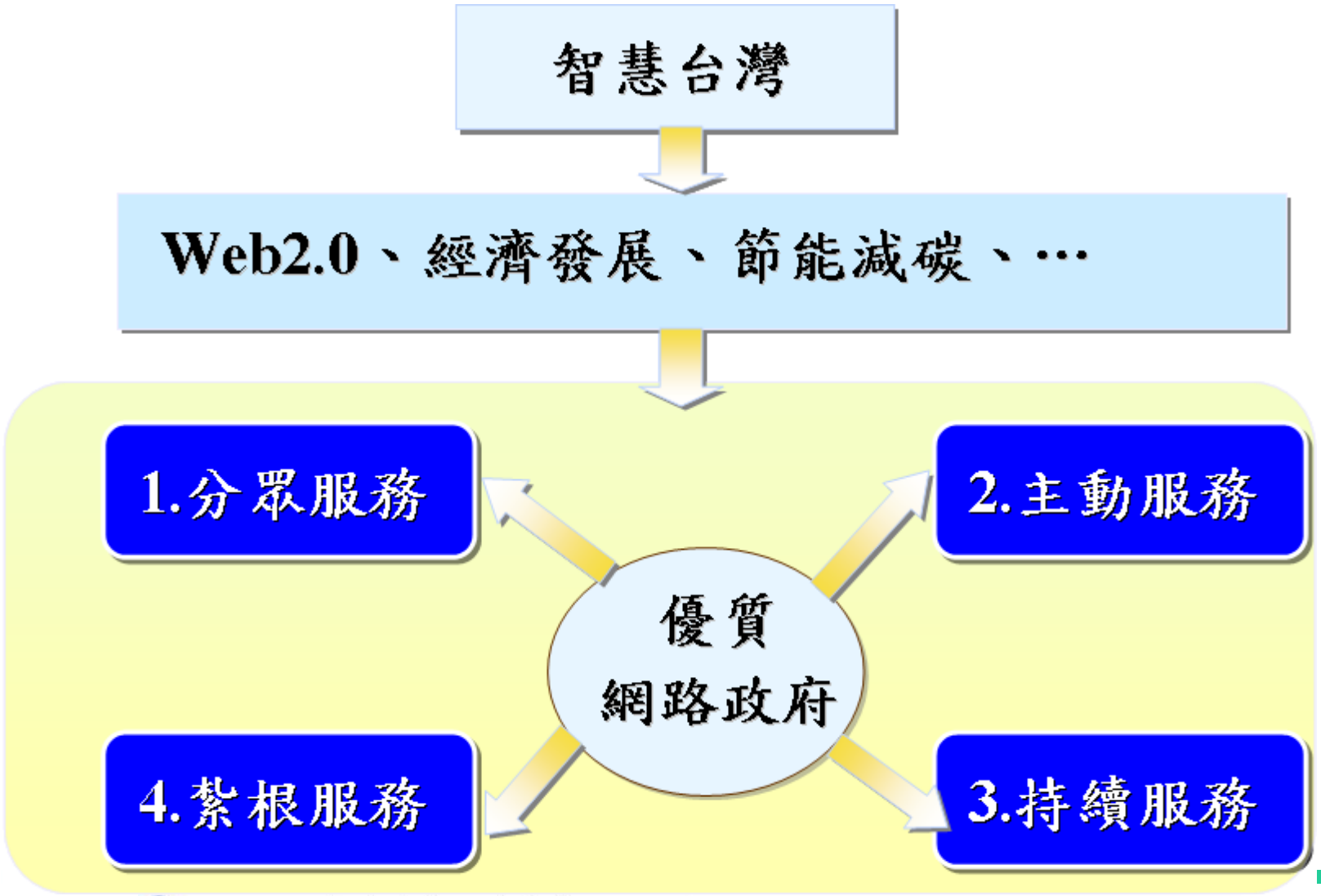
增進公共服務價值，建立社會信賴與聯結

三大目標

1.發展主動服務，創造優質生活	2.普及資訊服務，增進社會關懷	3.強化網路互動，擴大公民參與

五大策略	策略1.推動資訊改造，有效運用資源
	策略2.整合服務流程，展現政府一體
	策略3.革新資訊法制，加速創新應用
	策略4.建立分眾服務，落實需求導向
	策略5.加強應用推廣，提高使用滿意

優質網路政府計畫重點



旗艦計畫架構圖

旗艦 2 國家資通安全技術服務與防護管理精進計畫

旗艦 3 便捷資訊交換整合服務計畫

電子化政府單一入口服務網 / 跨機關共通服務平台

機關服務網 機關服務網 機關服務網

機關整合服務平台 機關整合服務平台 機關整合服務平台

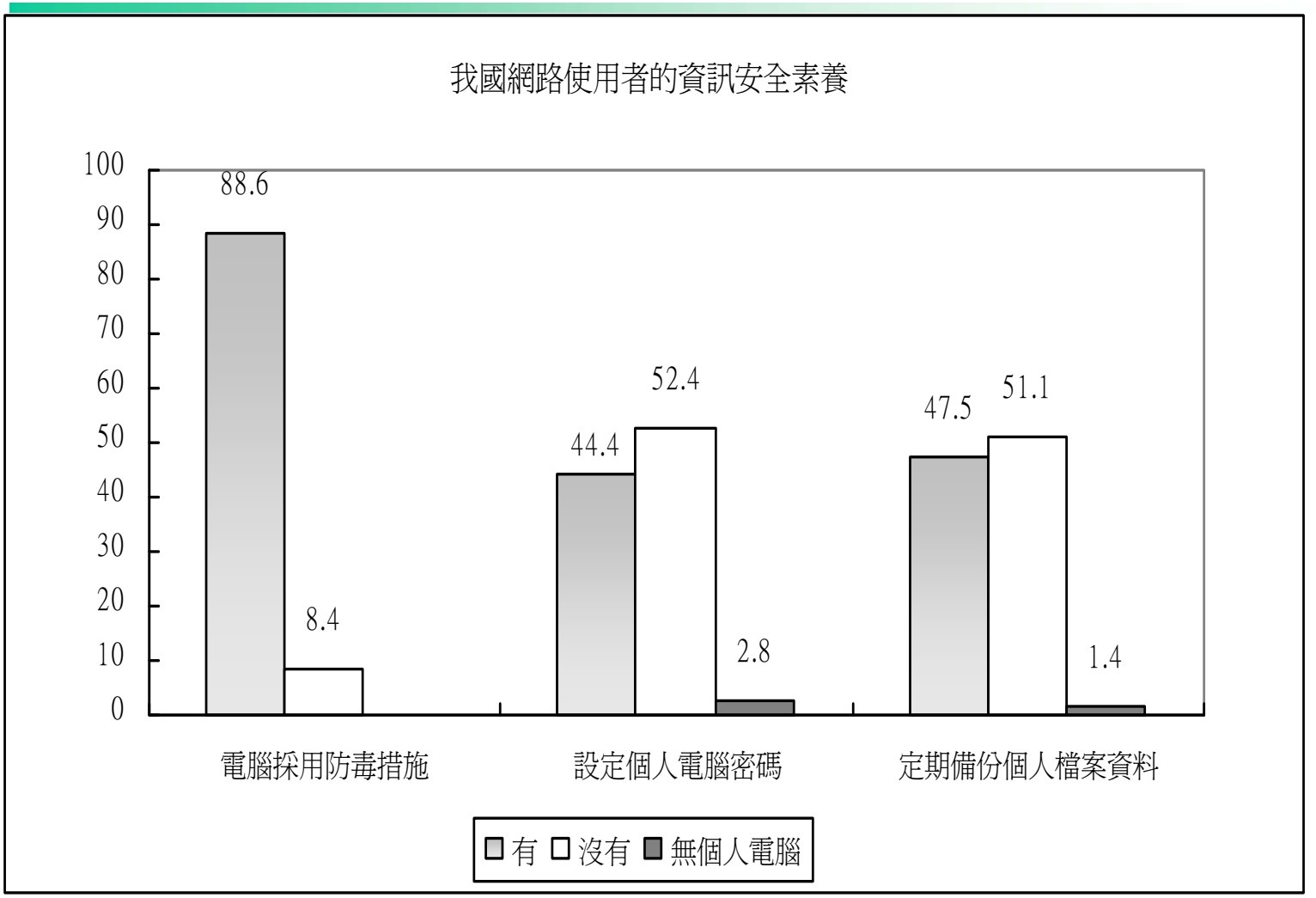
院轄市政府 縣市政府 中央部會

旗艦 1 優質網路政府基礎服務計畫

旗艦 4 中央地方機關e網通資訊服務計畫

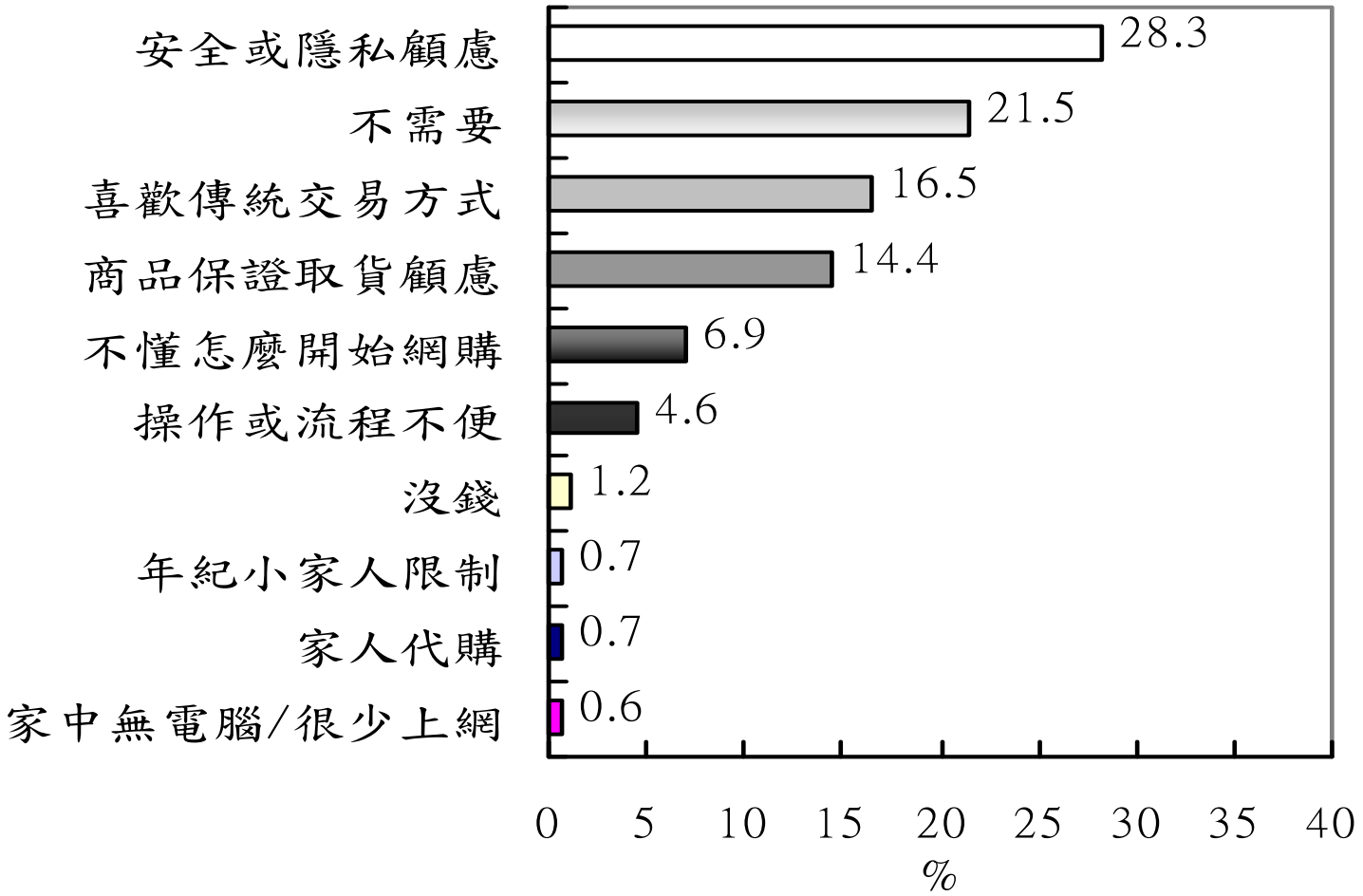
貳、現況分析

我國民眾資安素養



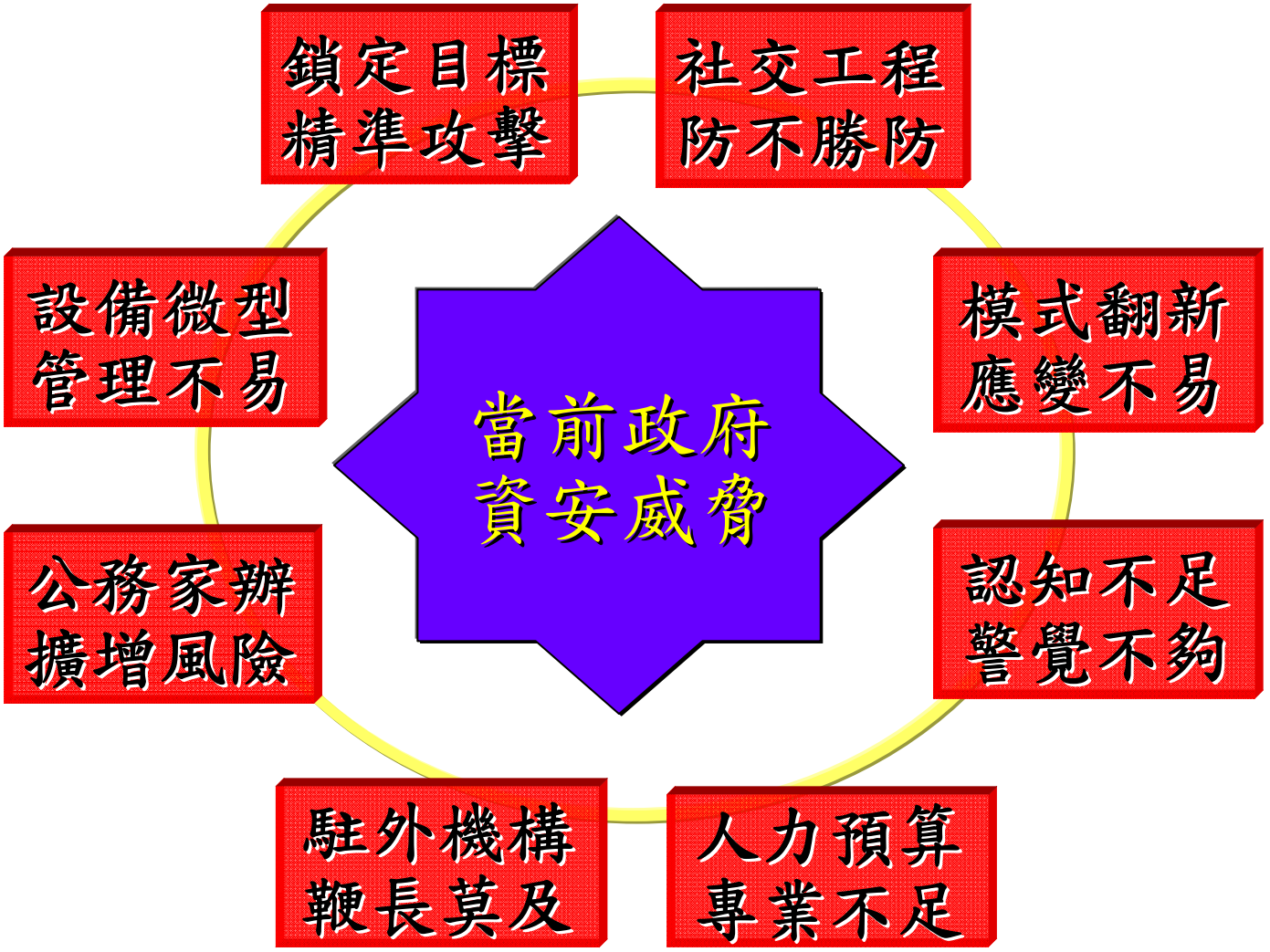
資料來源：2008年數位落差調查報告，行政院研考會2008年10月

網路使用者不曾透過網路從事交易原因



資料來源：2008年數位落差調查報告，行政院研考會 2008年10月

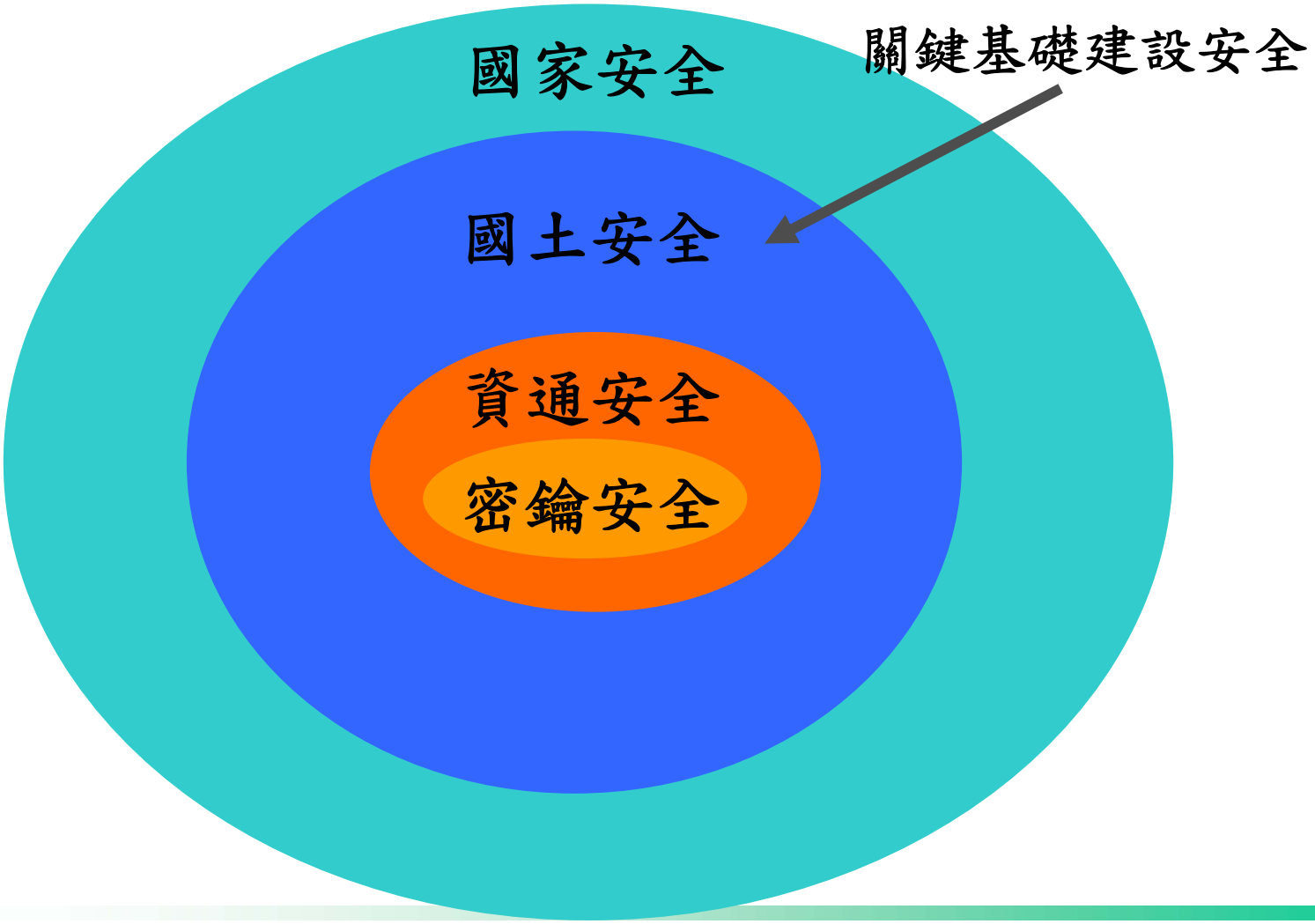
政府資通安全威脅分析


當前政府
資安威脅
鎖定目標
精準攻擊
社交工程
防不勝防
模式翻新
應變不易
認知不足
警覺不夠
人力預算
專業不足
駐外機構
鞭長莫及
公務家辦
擴增風險
設備微型
管理不易

政府資通安全相關問題

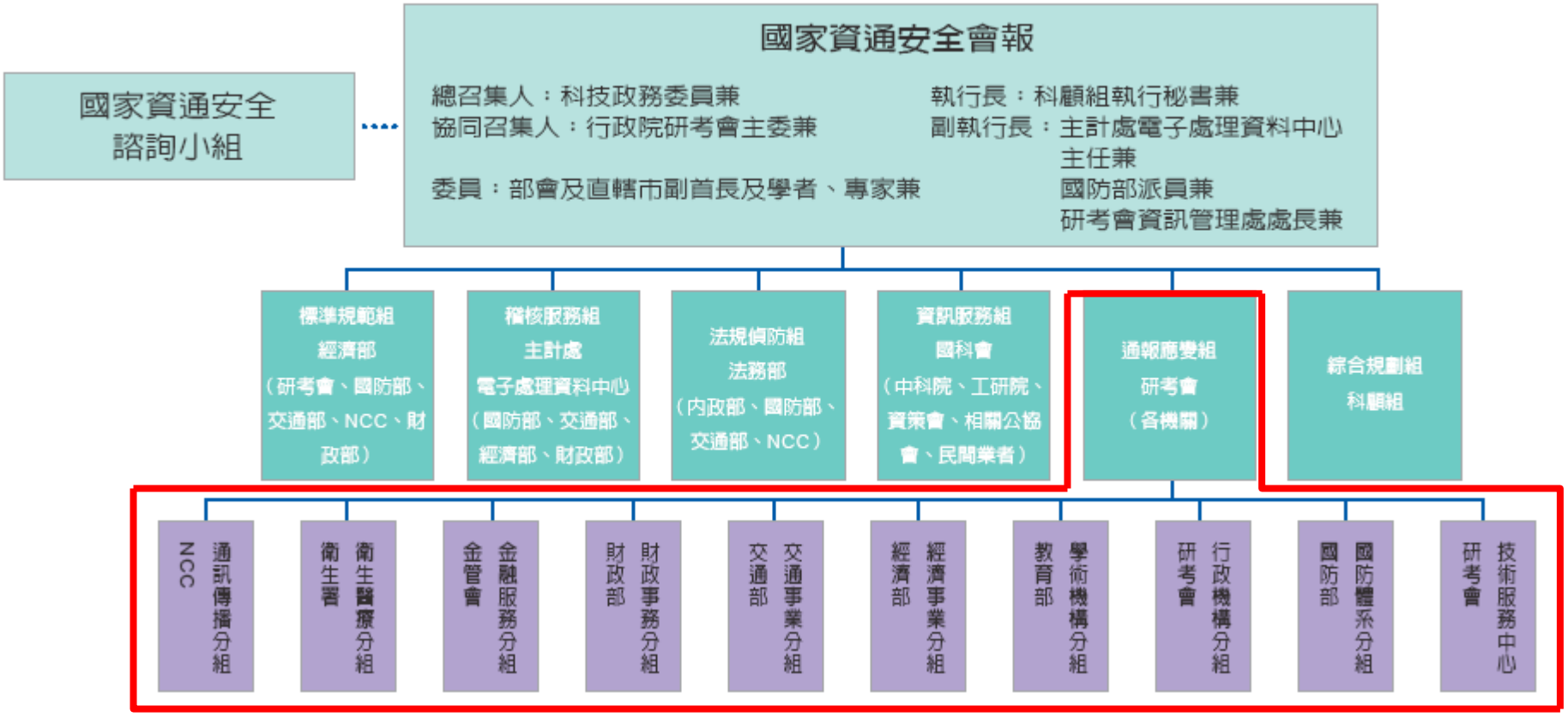
- **外部威脅**
  - ✓組織型駭客針對性攻擊
  - ✓鎖定特定對象或單位
  - ✓攻擊型式變化快速
- **內部問題**
  - ✓政府資安人力、經費及能量相對不足
  - ✓資安事件通報意願不高
  - ✓委外開發軟體及品質管理問題
  - ✓資訊作業委外處理衍生資安管理問題
  - ✓人員資安意識不足
  - ✓各機關橫向聯繫機制尚待建立
  - ✓資安相關法令尚未完備

資通安全是國家安全根基



行政院國家資通安全會報

行政院為積極推動國家資訊通訊安全政策，建構國家資訊通訊安全環境，提升國家競爭力，於2001年1月設立國家資通安全會報，2005年起通報應變組工作由研考會負責執行



通報應變組工作

行政院國家資通安全會報

技術服務中心 ⇔ 行政院研考會（通報應變組）

建立資通安全通報與預警機制

通報、預警、應變、訓練

- 處理資安事件與緊急應變
- 提供事前安全防護
- 提供事中預警應變
- 提供事後復原鑑識
- 提供資安訓練推廣

提供機敏機關7*24資安監看服務

協助政府維護資通安全

約7,500個政府機關(構)、15,000位資安聯絡人

資安事件影響分級判定表

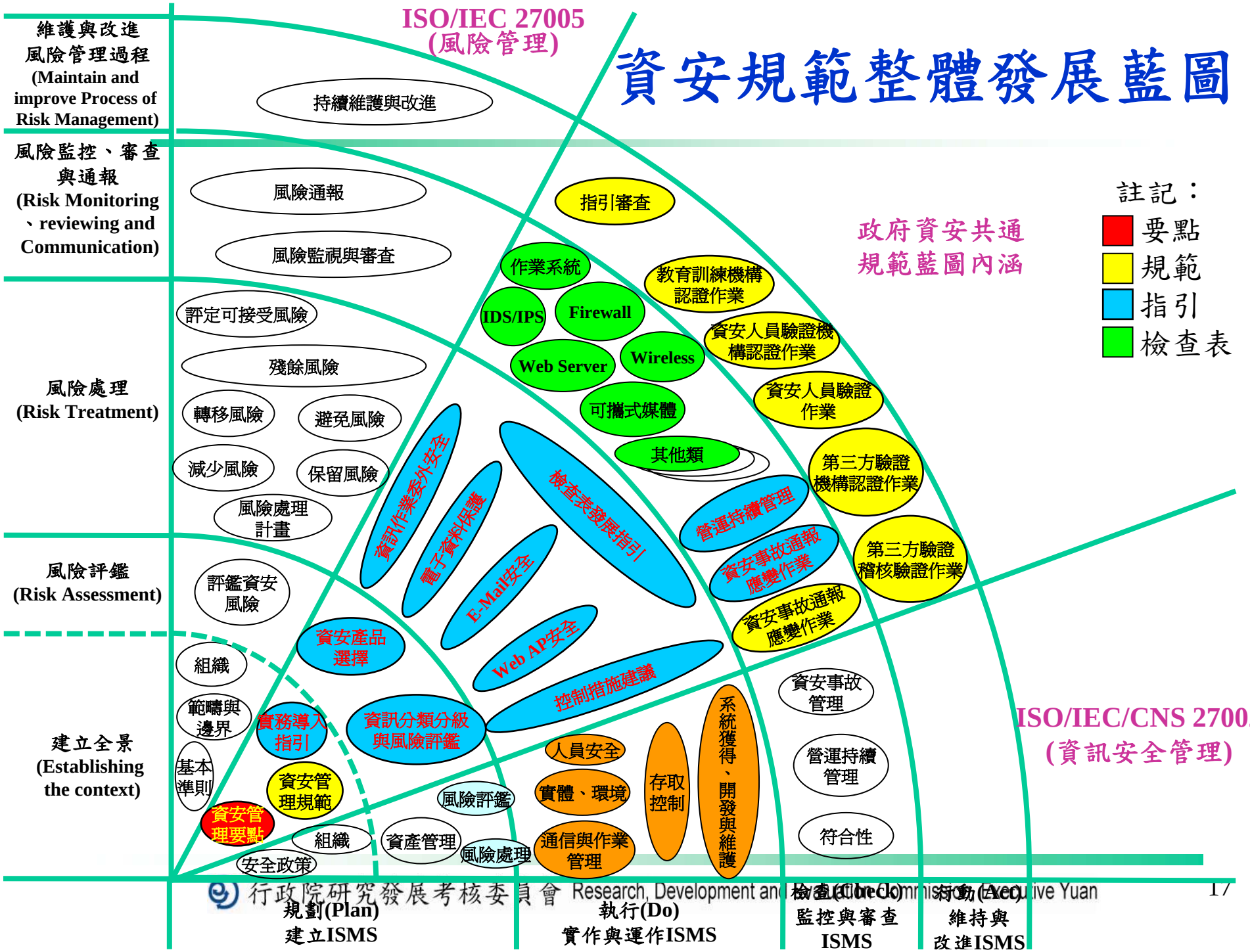
評估類別 / 影響等級		機密性	完整性	可用性
輕微 ↕ 嚴重	1級	非核心業務資料遭洩漏	非核心業務系統或資料遭竄改	非核心業務運作遭影響或短暫停頓
	2級	非屬密級或敏感之核心業務資料遭洩漏	核心業務系統或資料遭輕微竄改	核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作
	3級	密級或敏感公務資料遭洩漏	核心業務系統或資料遭嚴重竄改	核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作
	4級	國家機密資料遭洩漏	國家重要資訊基礎建設系統或資料遭竄改	國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作

電子郵件安全意識逐步改善

演練時間 / 演練項目	2007年	2008年
開啟測試電子郵件人數比	24.17%	22.16%
點閱測試電子郵件連結或附件人數比	16.29%	12.82%
是否事前預警	是	否

註：演練對象為各部會及地方政府

資安規範整體發展藍圖


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
資安產品選擇
資訊分類分級與風險評鑑
風險評鑑
資產管理
風險處理
資訊作業委外安全
電子資料保護
E-Mail安全
Web AP安全
審查表發展指引
控制措施建議
指引審查
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
營運持續管理
資安事故通報應變作業
第三方驗證稽核驗證作業
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

參、發展趨勢

國際資通安全發展趨勢

- 愛沙尼亞爆發史上第一次網路戰，網路安全成為重要議題
- 為提升網路安全，美國全面檢討網路安全整體策略，將任命網路安全總管
- 個人隱私資料被竊與金融詐騙事件頻傳
- 關鍵基礎建設資安風險增加
- 組織型駭客持續竊取政府資料
- 零時差攻擊造成資安防護困難

國安策略大轉型-因應全新的威脅

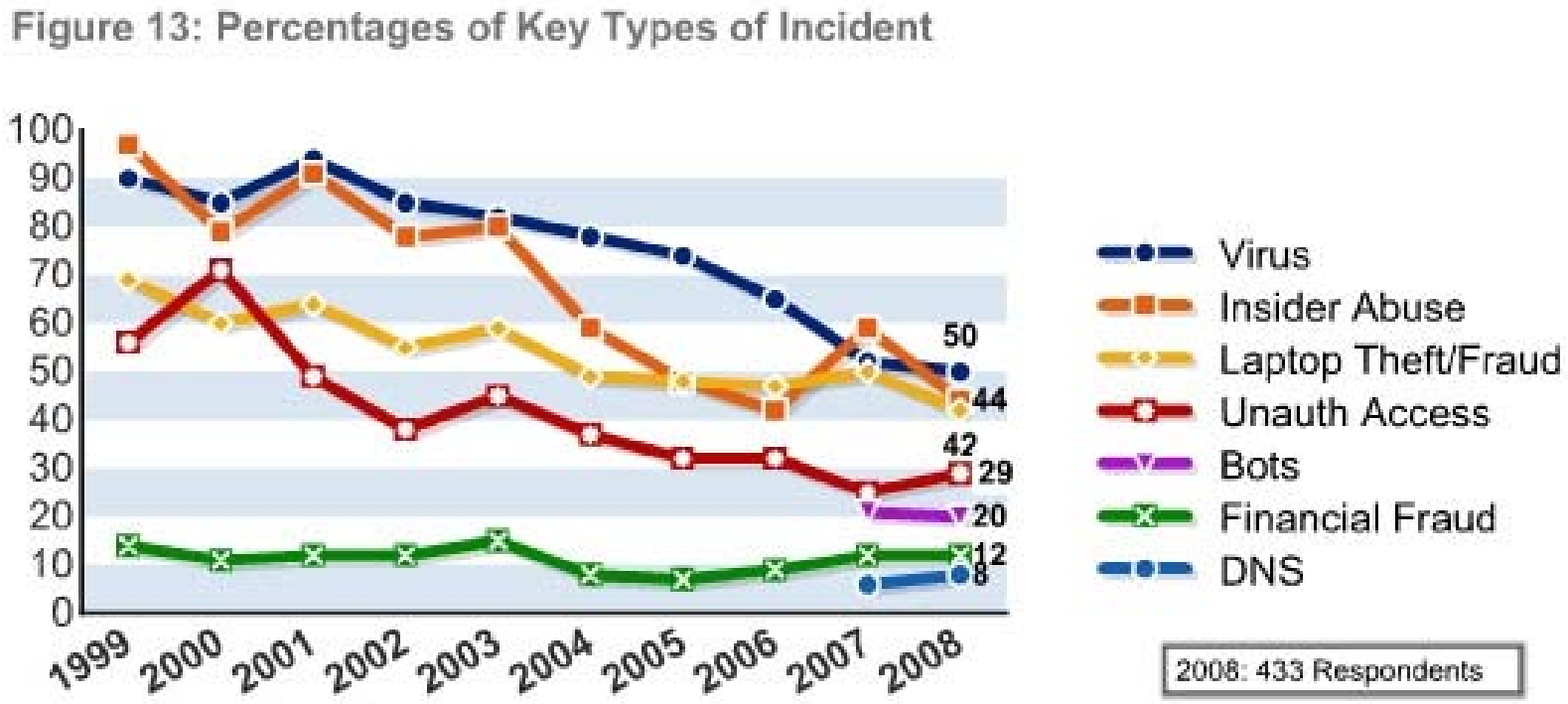
- 例如法國於2008年6月公布國防與安全白皮書
  - ✓ 法國將調整未來15年的國家安全戰略，重返北約組織，與西方盟國尋求戰略合作
  - ✓ 法國提出主要轉型策略包括：
    - ✓ 恐怖主義的威脅
    - ✓ 網路攻擊的威脅
    - ✓ 亞洲崛起的威脅
    - ✓ 能源與環境安全的威脅

給歐巴馬的網路安全報告書

- 美國戰略暨國際事務研究中心(CSIS) 2008年12月8日為歐巴馬發表一份網路安全報告書，指出3項主要發現
  - ✓ 網路安全已經成為美國主要的國家安全問題
  - ✓ 相關的決策與行動都必須尊重隱私與人民自由
  - ✓ 只有同時從國內及國際觀點而建立的完整國家安全策略才能讓美國更加安全

CSI/FBI 2008電腦犯罪與資安調查

➢ 1999~2008年資安事故主要型態比例



CSI/FBI 2008 The 13th Computer Crime and Security Survey

資料來源：*Computer Security Institute*

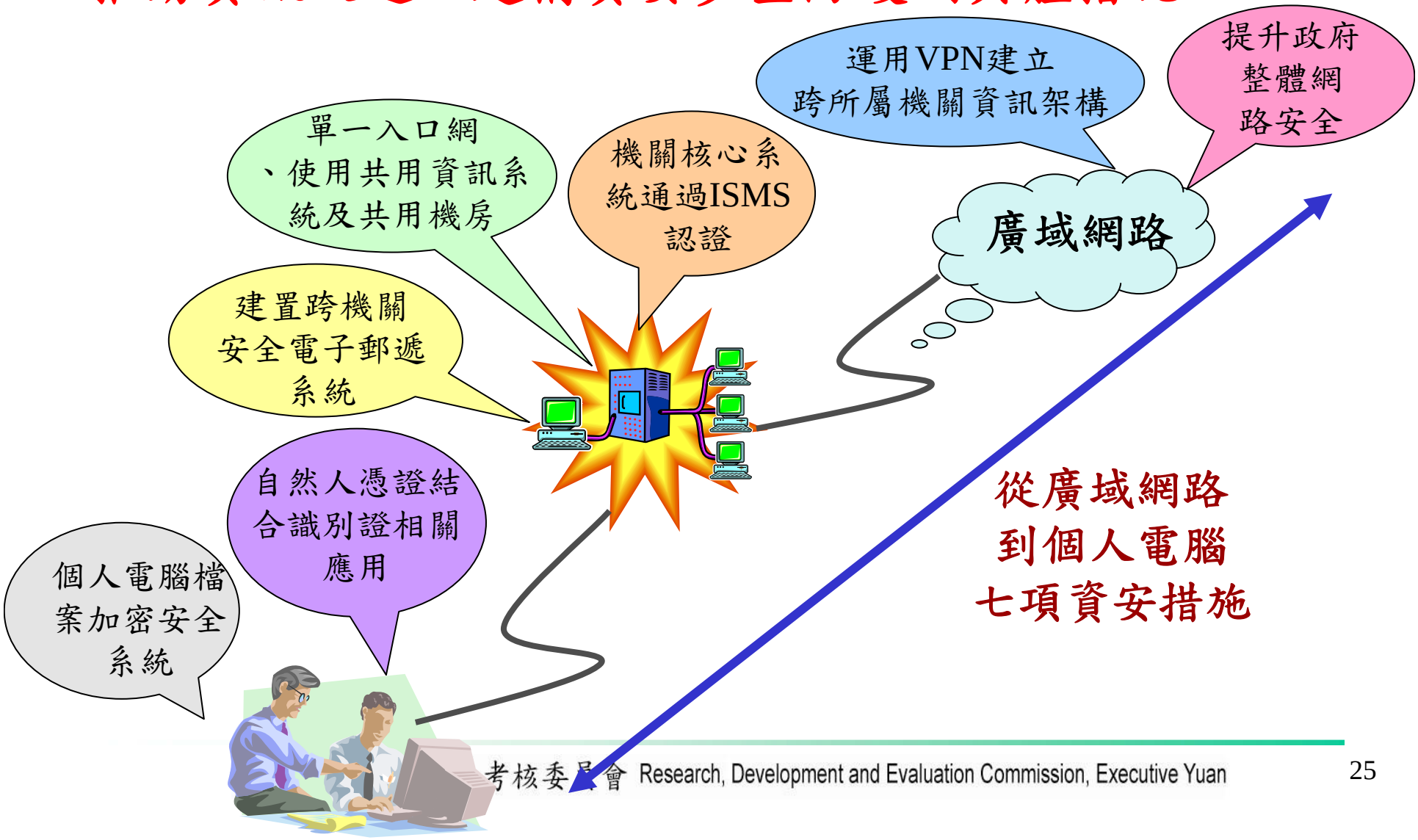
肆、具體策略

政府資通安全推動策略

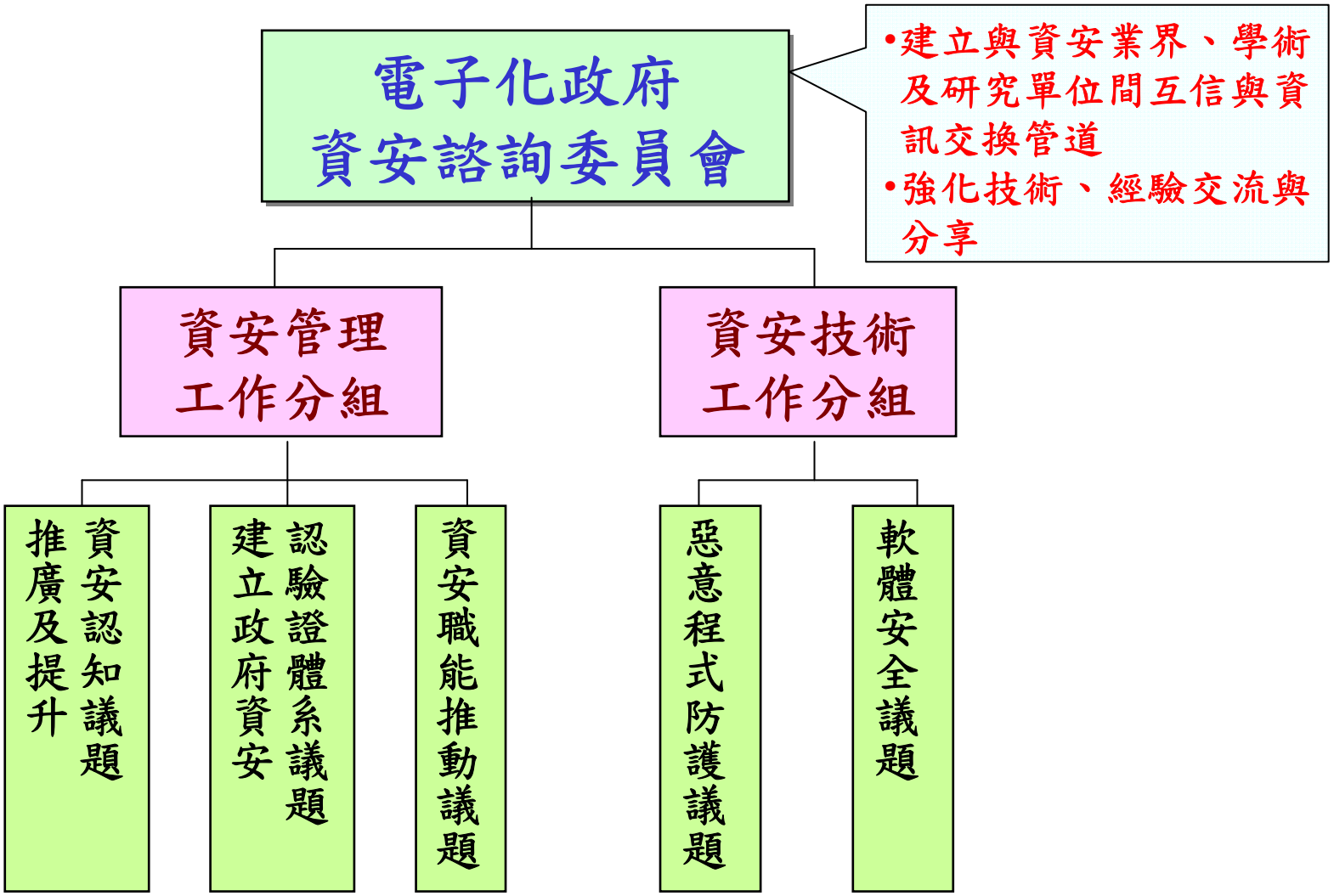
- 以全方位觀念永續推動
- 政府資通安全3E策略
  - ✓ 技術工程(Engineering)：利用防火牆系統、數位簽章、加密技術等建構第一道防線
  - ✓ 執行管理(Enforcement)：資訊安全管理政策、資安事件緊急處理機制、內外部電腦稽核制度、資訊安全標準及規範、產品及系統品質檢驗機制
  - ✓ 教育宣導(Education)：安全警覺訓練、資訊安全宣導、人才培訓、網路使用倫理

具體策略1－技術工程(Engineering)

➢ 推動資訊改造－建構資安多重防護網具體措施

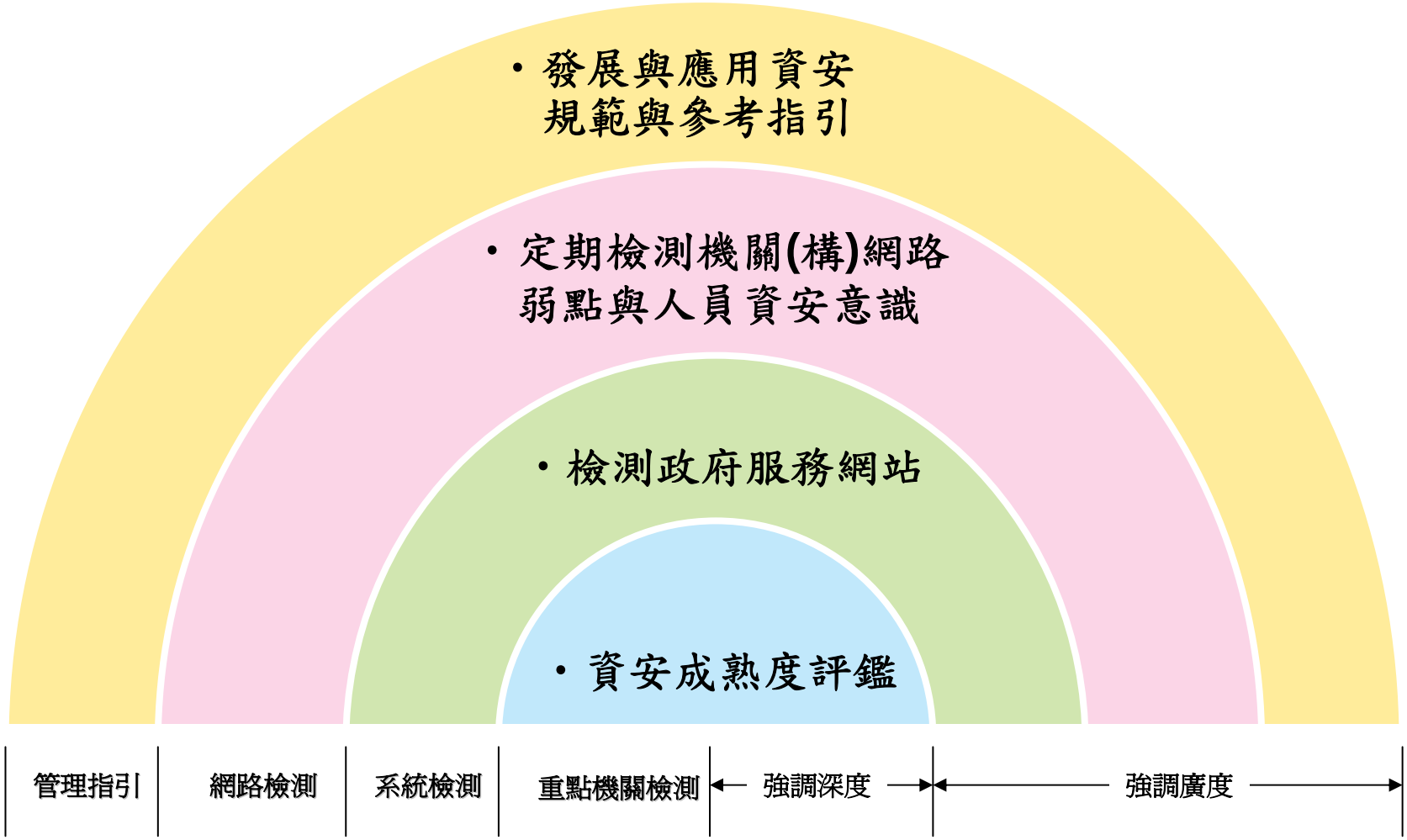


電子化政府資安諮詢委員會



具體策略2－執行管理(Enforcement)

- 提升資安管理與系統安全

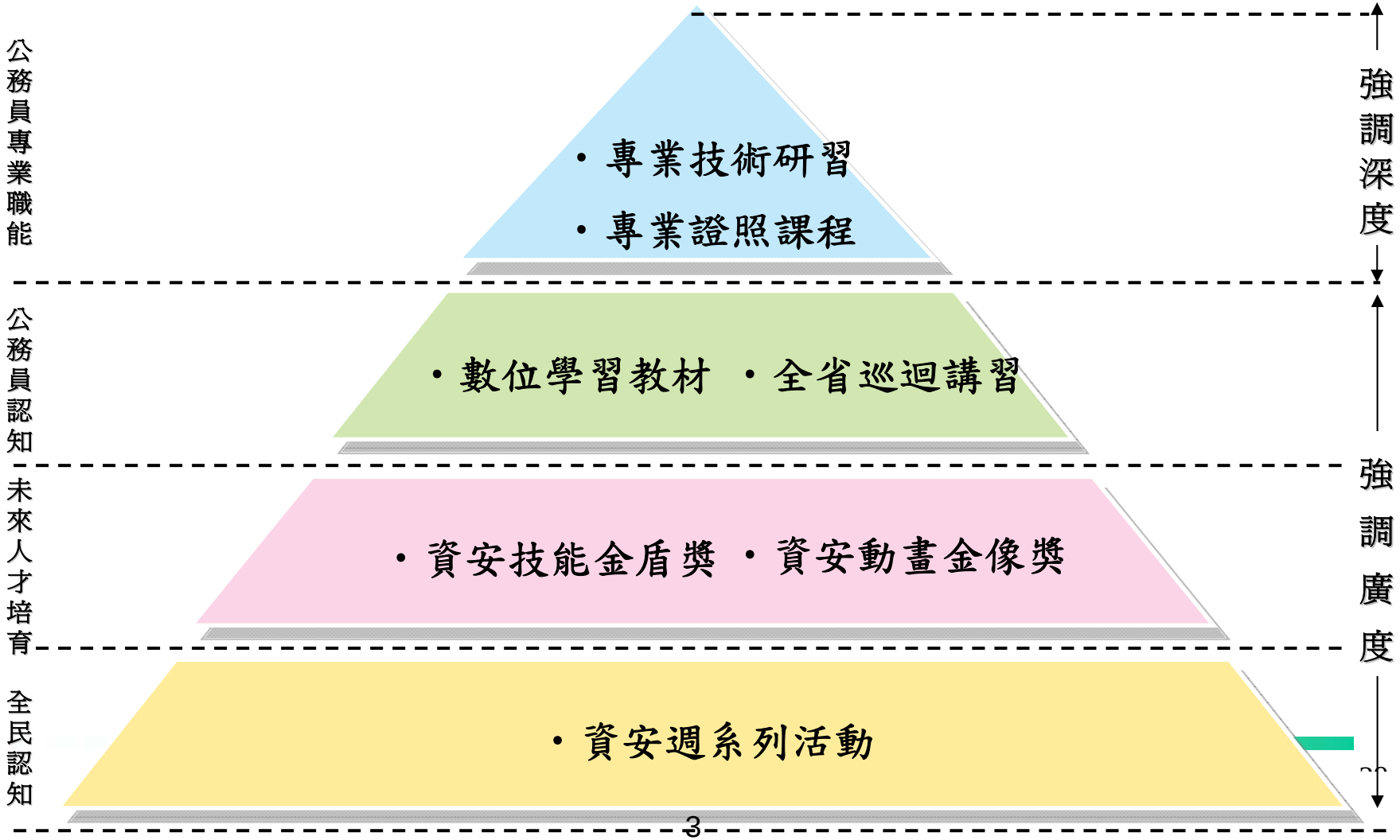


具體策略2－重要措施

- 建立政府機關資安認驗證機制
- 推動重點機關通過資訊安全管理系統(ISMS)驗證
- 逐年增加政府資通安全經費占資訊經費比例，每年提高1%，預計2012年達10%
- 提升政府網站應用程式檢測及修護能力

具體策略3－教育宣導(Education)

➢ 提升公務人員資安知識與能力



推動公務人員資安職能訓練及評量機制

規劃目的

針對公務人員所擔任職務與負責業務，機關應具備之資訊安全知識與技能

人員類別	應具備職能
一般主管	資通安全基本概念及相關資安規定
資訊人員	具備資通安全管理、技術相關知能
一般使用者	資通安全管理基本知能及相關資安規定
資安人員	資通安全管理、技術及稽核相關知能

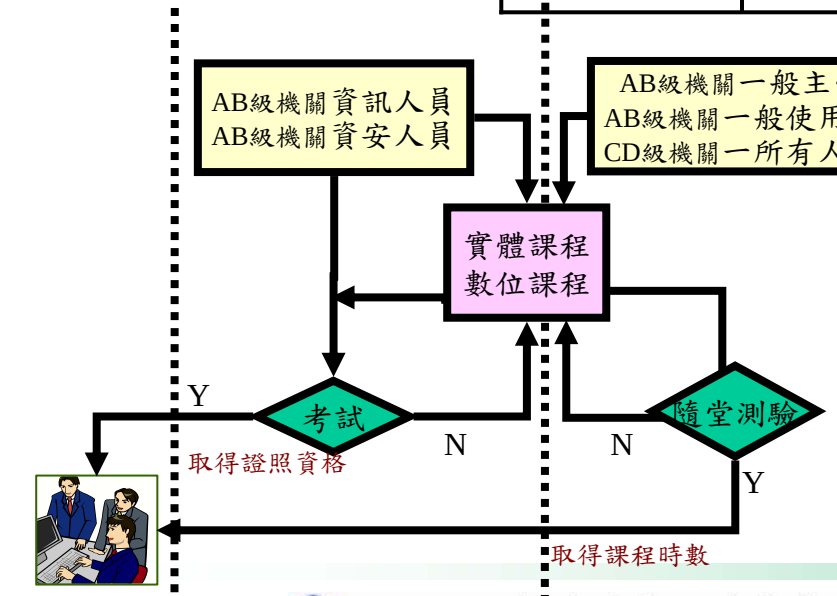
課程設計

課程設計理念以公務人員日常工作所需之資安應用為導向

課程類別
資安入門
資安管理
資安技術
其他

完成課程內容規劃、教材編撰及題庫設計

分類	必修課程
一般主管	➢B09機關資安規定 ➢B12電子郵件安全(參考指引)
資訊人員	➢B01資通安全管理制度 ➢B07政府資訊作業委外安全(參考指引) ➢B10電子資料保護(參考指引) ➢B12電子郵件安全(參考指引) ➢C12 Web應用程式安全(參考指引)
一般使用者	➢B01資通安全管理制度 ➢B09機關資安規定 ➢B10電子資料保護(參考指引) ➢B12電子郵件安全(參考指引)
資安人員	➢B01資通安全管理制度 ➢B03資訊系統風險評鑑(參考指引) ➢B06資通安全稽核 ➢B07政府資訊作業委外安全(參考指引) ➢C12 Web應用程式安全(參考指引)



評量流程

訓練課程

2008年12月首辦資安週活動

國際論壇

資安日

資安金像獎

資安ｅ起學

ICST網站尋寶

資安真言

伍、行動方案

國家資通訊安全發展方案(2009-2012年)

- 行政院研考會主辦項目
  - ✓ 行動方案1：提升通報時效
  - ✓ 行動方案2：建立資安事件管理與回應程序
  - ✓ 行動方案5：發展與維護政府機關資安作業規範與參考指引
  - ✓ 行動方案8：強化電子化政府資通安全，落實公務資料保護
  - ✓ 行動方案12：強化資安素養與能力培訓

優質網路政府計畫(2008-2011年)

- **旗艦2：國家資通安全技術防護與管理精進計畫**
  - ✓ 建立政府資安認驗證體系，發展政府資安作業共通規範，提升政府機關資安管理能力
  - ✓ 落實資料安全防護，提升網站應用系統(Web AP)安全品質
  - ✓ 健全資通安全通報應變機制，提升資通安全通報與應變機制效能，協助政府機關處理重大資安事件，減少資安事件之衝擊與損失
  - ✓ 建立資安事件預警與應變防護技術，強化資安預警能力，提供資安趨勢評估分析資訊，以利早期發現資安威脅，降低資安風險
  - ✓ 提升公務人員資安認知意識，培育政府資安專業人才
  - ✓ 參與國際資通安全聯防機制，建立跨國合作模式，提升整體防護能量

績效指標

績效指標	指標值				說 明
	2008年	2009年	2010年	2011年	
通過資訊安全管理驗證比率	30%	50%	65%	75%	資安等級A、B級機關通過政府資訊安全管理驗證比率
政府資安資訊分享平台訊息分享	2	3	6	9	與政府骨幹網路(GSN、TANET等)、事業主管機關、民間ISP及資安服務業者等建立資安訊息分享管道數
資安偵測規則更新時間	24 小時	12 小時	6 小時	3 小時	中繼站黑名單布建至政府機關監控設備所需時間
自主研發資安監控設備之布建數	80個	90個	100個	120個	自行研發之資安監控設備布建數量(包含SOC、DNS警示系統、使用者端警示系統、內部網路警示系統、Honeynet、Botnet偵測設備等)
資安整體服務滿意度	80分	85分	88分	90分	提供政府機關資安相關服務之整體滿意度(滿分為100分)

諸多挑戰仍待克服

- 整體策略–通盤規劃國家資通安全策略地圖
- 預算經費–相對主要國家，資安資源投入仍不足
- 組織人力–尚待提升資安人員專業能力
- 技術研發–尚待提升自主技術研發及軟體品質
- 科技安全–全球資訊產業分工之科技安全議題
- 法令規章–尚待明確的法令規範企業資安責任
- 國際合作–打擊網路犯罪、區域聯防等
- 全民認知–建立全民資安文化

陸、討論題綱

- 如何結合產、官、學、研資源與能量進一步提升政府整體資通安全防護能量？在技術工程、執行管理及教育宣導等方面之強化措施及優先重點為何？
- 如何加強產、官、學、研資安訊息、技術及經驗交流，建立資安早期預警機制，提升國家整體資安事件應變及防護能力？

報告完畢

敬請指教