資安治理成熟度評估簡介

報告人：王俊凱 協理

日期-106年04月21日

財團法人中華民國國家資訊基本建設產業發展協進會

何謂治理

- 治理或管治（Governance）一詞意思跟「統轄」、「管轄」、「統治」略近。 在政治學領域，通常指國家治理，即政府如何運用治權，來管理國家、人民和領土，以達到延續國祚和讓國家發展的目的。 在商業領域，又延伸到公司治理（corporate governance），指公司等組織中的管理方式和制度等。
- ISACA 的定義，治理可確保”在決定平衡、共同協議的企業目標時，利害關係人的需求、情況與選擇能被納入考量；藉由優先權與決策制訂來設定方向；以及監督協議方向與目標的達成績效和遵循。

何謂治理

- 公司治理是指一種指導及管理企業的機制，以落實企業經營人的責任，並保障股東的合法權益及兼顧其他利害關係人的利益 。良好的公司治理應具有促使董事會與管理階層以符合公司與全體股東最大利益的方式達成營運目標的正當誘因，協助企業管理結構之轉型，以及提供有效的監督機制，以激勵企業善用資源、提升效率，進而提升競爭力，促進全民之社會福祉。
- 為確定組織目標和確保目標實現的績效監控所提供的治理結構

何謂治理

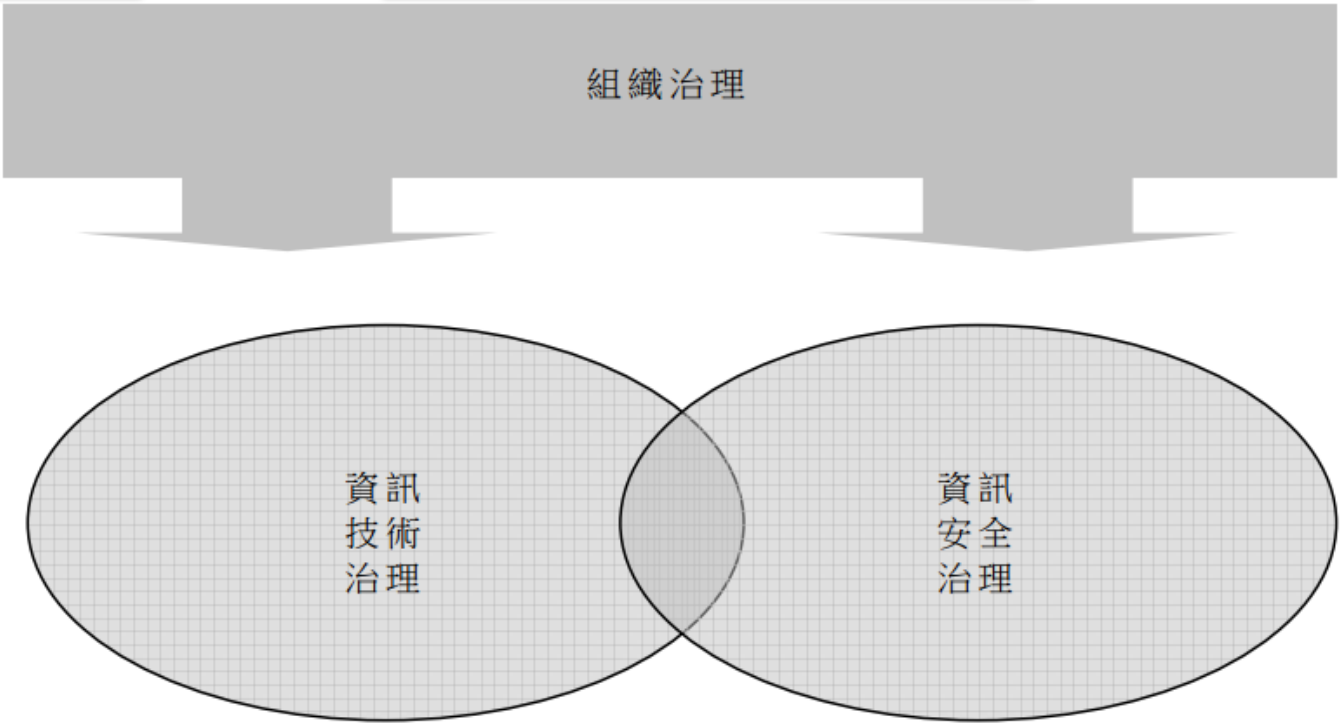
- IT治理是公司治理在信息時代的重要發展，用於描述企業或政府是否採用有效的機制，使得IT的應用能夠完成組織賦予它的使命，同時平衡信息技術與過程的風險、確保實現組織的戰略目標。
- 治理同時也用於表達某機構組織內部的監督與控制。用於此時（譯按：狹義），治理乃成為企業整體治理的子集合。例如，企業整體治理包含了資訊治理－資料擷取、資料儲存與建立、以及資訊分派與使用的監督和控制。資訊治理也包括資料治理。

資安治理架構

- 「105年國家資通安全防護整合服務計畫」經研究與分析資安治理相關國際標準，以及政府機關資安治理相關法規與要求後，採行下述原則，以建立適用於政府機關且涵蓋面完整之資安治理架構。
- 綜合考量各資訊安全與資訊治理相關國際標準，以其最佳實務與建議，設計資安治理模型的基礎框架及構面。
- 承接政府機關資安治理法規、規範、指引或相關要求，以及資安治理現況，對框架與構面進行微調。

資安治理架構基本介紹

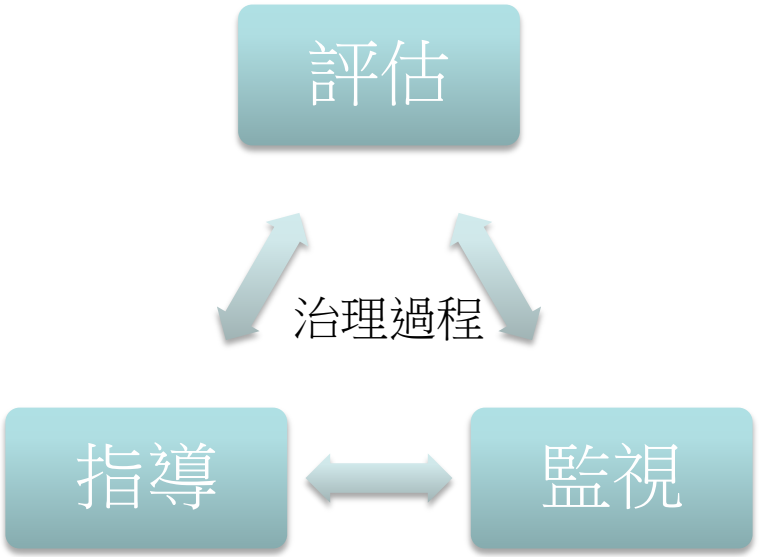
- 參考資訊安全治理國家標準CNS 27014規範，資安治理範圍包含資訊安全治理本身，以及涉及資安治理的資訊技術部分，其上受組織治理的監督、影響。



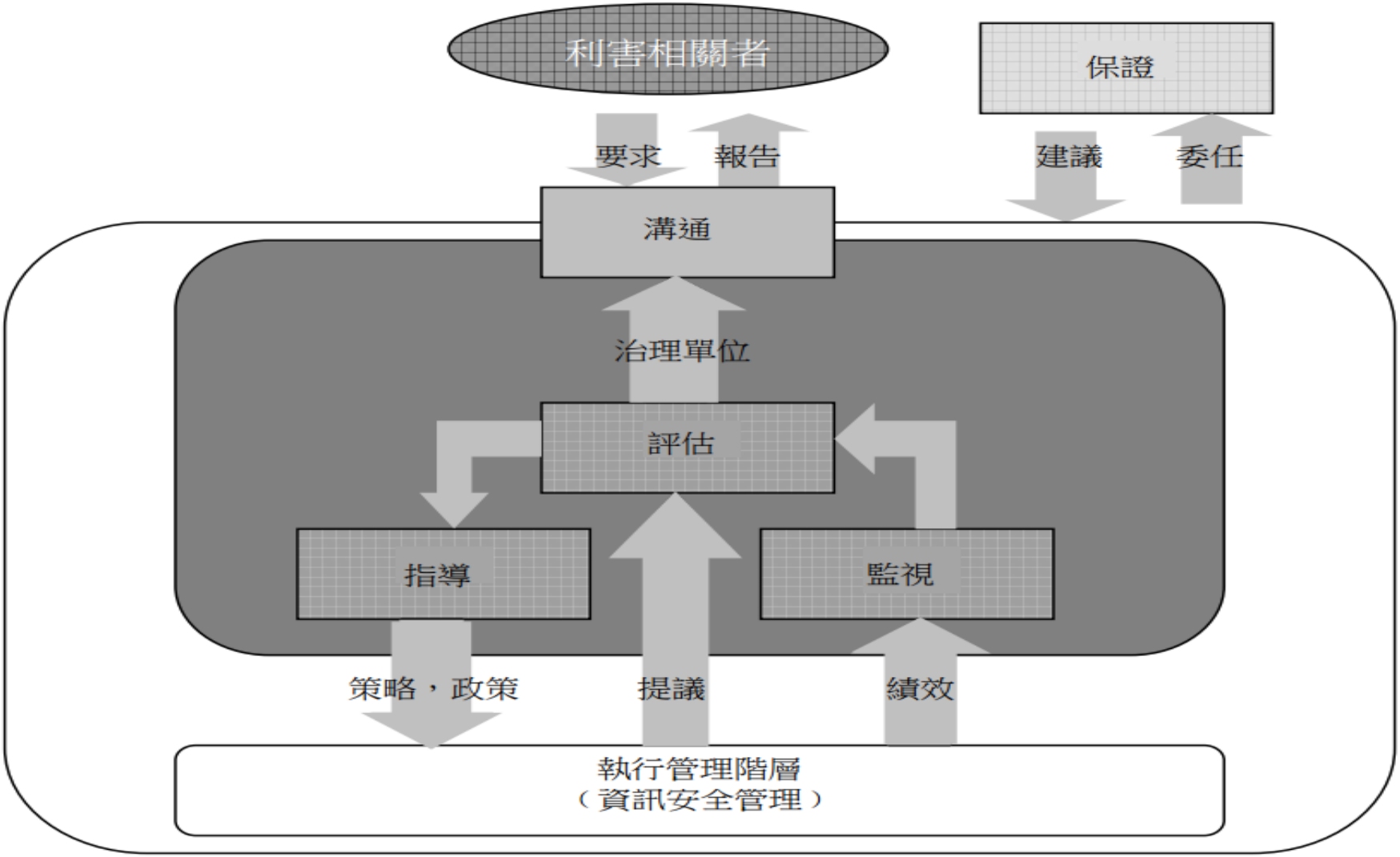
資訊安全治理與資訊技術治理關係

治理過程

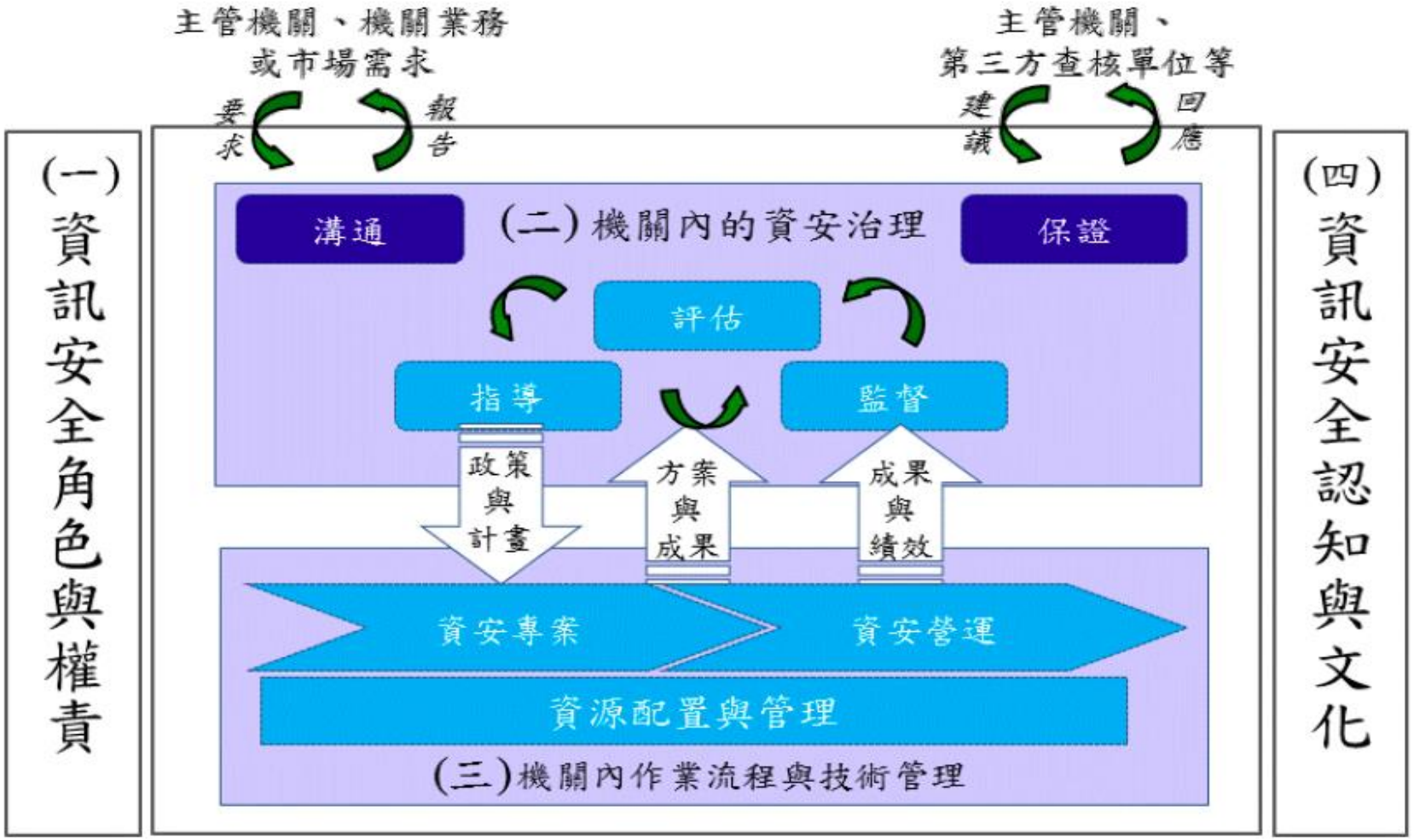
- 資訊安全治理國家標準CNS 27014，治理單位以EDM(評估(Evaluate)、指導(Direct)、監視(Monitor))方式形成治理過程，向下監督、管理資訊安全管理執行單位，並由治理單位向上進行溝通，回應組織利害關係人之要求，且整個運作機制對外可以由獨立機構提供客觀意見。



資安治理模型



我國政府機關資安治理架構



資訊安全角色與權責

- 為機關組織針對資安治理相關之角色與權責設計，角色涵蓋管理層面與操作技術層面之人員等。

機關內的資安治理

- 為資安治理核心，參考來自主管機關等利害關係人要求，透過評估-指導-監督作業，依組織現況評估預期的安全目標級未來策略間之差異，評估最佳化作法後，訂定高階指導原則、政策，機關內資安作業流程與技術管理皆需遵循，並定期監控目標達成率。整個資安治理運作情況與結果，應可受主管機關或第三方機構檢視。

機關內作業流程與技術管理

- 資安治理核心提出資安治理政策與相關計畫，由資安專案及營運進行依循；資安專案內涵為「規劃」、「建立」之管理活動、資安營運內涵為「執行」、「監督」之管理活動，並用以管控資訊資產；管理成效依績效指標衡量與計算，並回應給資安治理核心。

資訊安全認知與文化

- 以資安治理各角色為對象、資安治理架構模型各區塊為範圍，設計相對應之資訊安全認知與教育訓練。

資安治理流程架構

四大面向

組織與人員

E. 1角色與權責

•建立資訊安全治理組織，並區分組織內的各角色權責，確保組織運行順遂。

E.2認知與訓練

- 建立組織內人員定期或不定期之資訊安全教育訓練，藉以強化人員意識

政策與符合性

P.1資安治理架構與政策	• 建立適用於組織的資安治理架構與政策，確保組織內人員之資安意識依循一致。
P.2資安資源確保與監控	• 基於推動資安治理，組織應提供適當且足夠的安全設施經費或維護資源。
P.3資安風險監控	• 監督組織面臨資訊安全風險，並由管理階層參與審查風險評鑑準則與處理結果，確保組織所面臨的風險得以降低。
P.4利害關係人溝通報告	• 識別組織之利害關係人並建立與其溝通與報告機制，以維持與利害關係人之聯繫。
P.5第三方驗證與內稽	• 透過第三方的稽核或審查機制，確保組織資訊安全相關機制運作合宜。

規劃、推動與監督

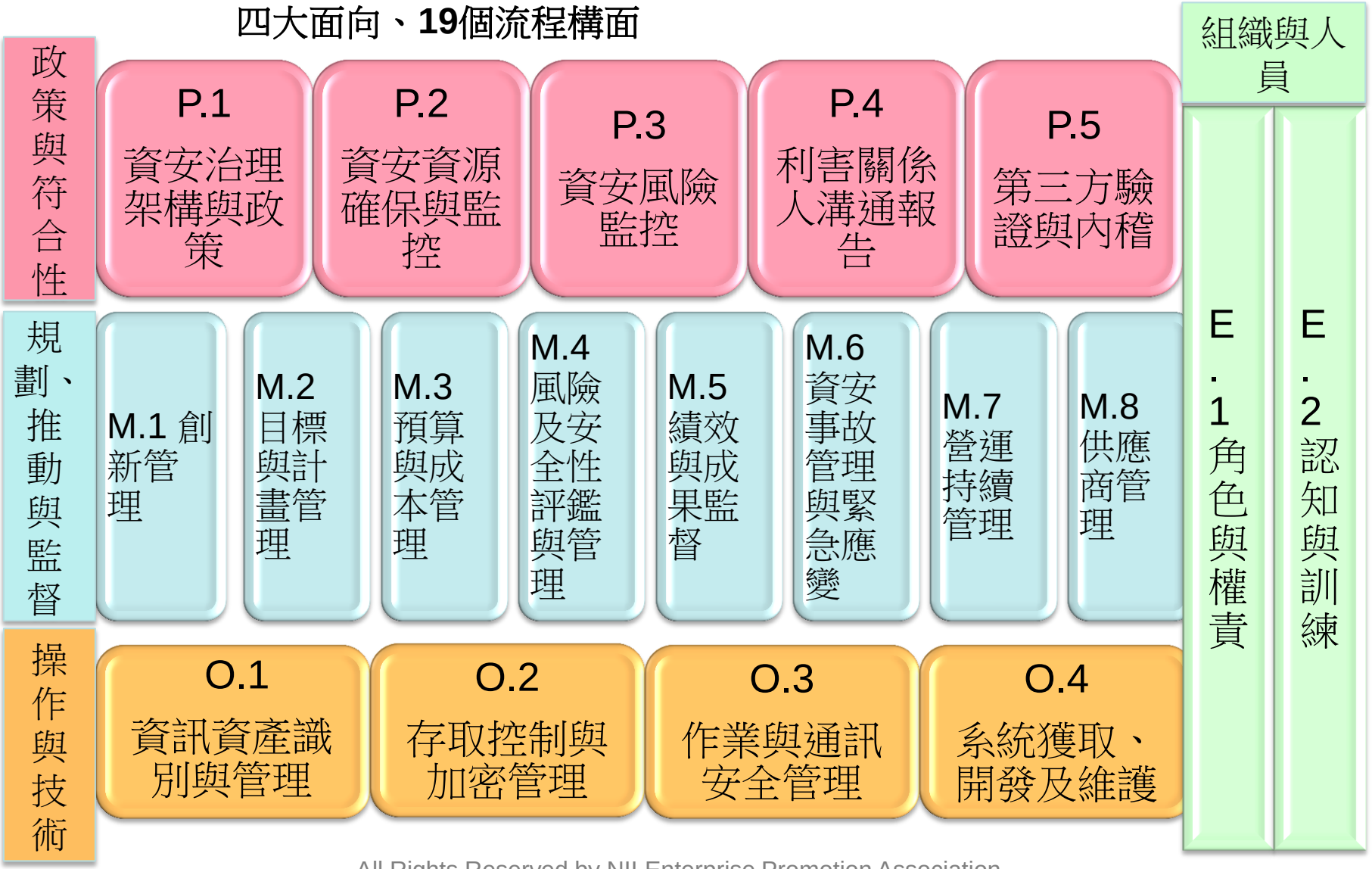
M.1 創新管理	• 組織建立有助於資安創新之環境時，應考量並確保得以因應日益多變的資訊安全衝擊。
M.2目標與計畫管理	• 依資訊安全政策建立組織資訊安全目標與專案管理機制，確保得以面對日益多變的資訊安全議題。
M.3預算與成本管理	• 組織編列預算以及追蹤成本時，應考量資安計畫所需軟硬體項目之經費或資源。
M.4風險及安全性評鑑與管理	• 鑑別與管理組織所面臨的風險，並執行對應的安全性技術測試。
M.5績效與成果監督	• 建立績效量測與監督機制，針對不符合事項進行改善追蹤，並且透過管理審查機制確保管理階層了解現行資安治理運作狀況。
M.6資安事故管理與緊急應變	• 制定資安事故通報程序，包含紀錄、通報、處理以及相關復原措施，確保資安事故發生時，人員了解應如何及時且快速的應變。
M.7營運持續管理	• 建立組織之營運持續運作機制，確保當發生重大事件或災害時，組織所受到的衝擊將得以降低。
M.8供應商管理	• 針對供應商進行資訊安全管控並審查其服務能力，確保供應商的能力符合組織需求。

作業與技術

O.1資訊資產識別與管理	• 識別組織所擁有之資訊資產，並基於組織業務發展的角度定義其關聯性，確保資訊資產被有效的保護與管理。
O.2存取控制與加密管理	• 限制資訊本身與資訊處理設施的存取，並透過適當且有效的加密機制，用以保護資訊的機密性、鑑別性及完整性。
O.3作業與通訊安全管理	• 確保正確與安全地操作資訊處理設施，且資訊及資訊處理設施不受惡意軟體的破壞。
O.4系統獲取、開發及維護	• 確保於資訊系統開發生命週期中落實資訊安全的設計與實施。

資安治理架構流程構面

四大面向、**19**個流程構面



成熟度評審模型之流程構面分級原則

成熟度等級		分級設計考量	資安治理四大面向			
			政策與符合性	規劃推動與監督	作業與技術	組織與人員
Level 5	Extended Process Set (其他流程對應為Extended Process Set)	Extended Process Set強化、優化機關資安治理能力的角度，機關依序滿足的流程構面項目，從Level 2至Level 5分別進行定義		M.1 創新管理		
Level 4			P.3 資安風險監控	M.5 績效與成果監督		
Level 3			P.1 治理架構與政策 P.2 資安資源確保與監控 P.4 利害關係人溝通			
Level 2				M.2 目標與計畫管理 M.3 預算與成本管理 M.6 資安事故管理與緊急應變 M.7 供應商管理	O.1 資訊資產識別與管理 O.2 存取控制與加密管理 O.4 系統取得、開發與維護	
Level 1	Basic Process Set (定義對應成熟度等級為Level 1的Basic Process Set之流程)	依以下原則做為Basic Process Set須滿足之考量 • 角色與認知 • 風險評鑑識別 • 作業與技術安全防護要求相關	P.5 第三方驗證與內稽	M.4風險及安全性評鑑與管理 M.7 營運持續管理	O.3 作業與通訊安全管理	E.1 角色與權責 E.2 認知與訓練

檢核項目設計考量重點、參考來源

- 檢核項目83項
- 考量重點、參考來源

類型	檢核項目主要參考來源
國際標準	COBIT 5
	SP800-100 (2006/10/1版本)
	ISO 27001-2013
	ISO 20000-2011
	CERT-RMM
	NIST Cyber Security Framework
國內要求	行政院及所屬機關資訊安全管理要點
	行政院及所屬各機關資訊安全管理規範
	國家資通安全通報應變作業綱要
	國家資通訊安全發展方案(102-105年)
	政府機關(構)資通安全責任等級分級作業規定
	資訊系統分級與資安防護基準作業規定
	資訊安全業務內部控制制度共通作業

責任等級問項設計重點

A級	B級	C級
❖ 目標、計畫與創新管理有效性 ❖ 資安風險監控與資源提供有效性 ❖ 績效與成果監督有效性 ❖ 資安事故管理與緊急應變有效性 ❖ 應辦事項各作業執行之有效性	❖ 績效與成果監督落實性 ❖ 資安事故管理與緊急應變落實性 ❖ 資安風險監控與資源提供落實性 ❖ 應辦事項各作業執行之有效性	❖ ISMS推動落實性 ❖ 基本防護縱深有效性 ❖ 資安教育訓練有效性

成熟度等級區分


成熟度等級
達成成熟度對應流程構面
成熟度Level 5
M.1 目標、計畫與創新管理
成熟度Level 4
P.3 資安風險監控
M.4 績效與成果監督
標竿值
成熟度Level 3
P.5 第三方驗證
M.6 營運持續管理
基準值
成熟度Level 2
M.5 資安事故管理與緊急應變
M.7 供應商管理...
成熟度Level 1
P.1 治理架構與政策...
M.2 預算與成本管理...
E.1 角色與權責...
O.1 資訊資產識別與管理...

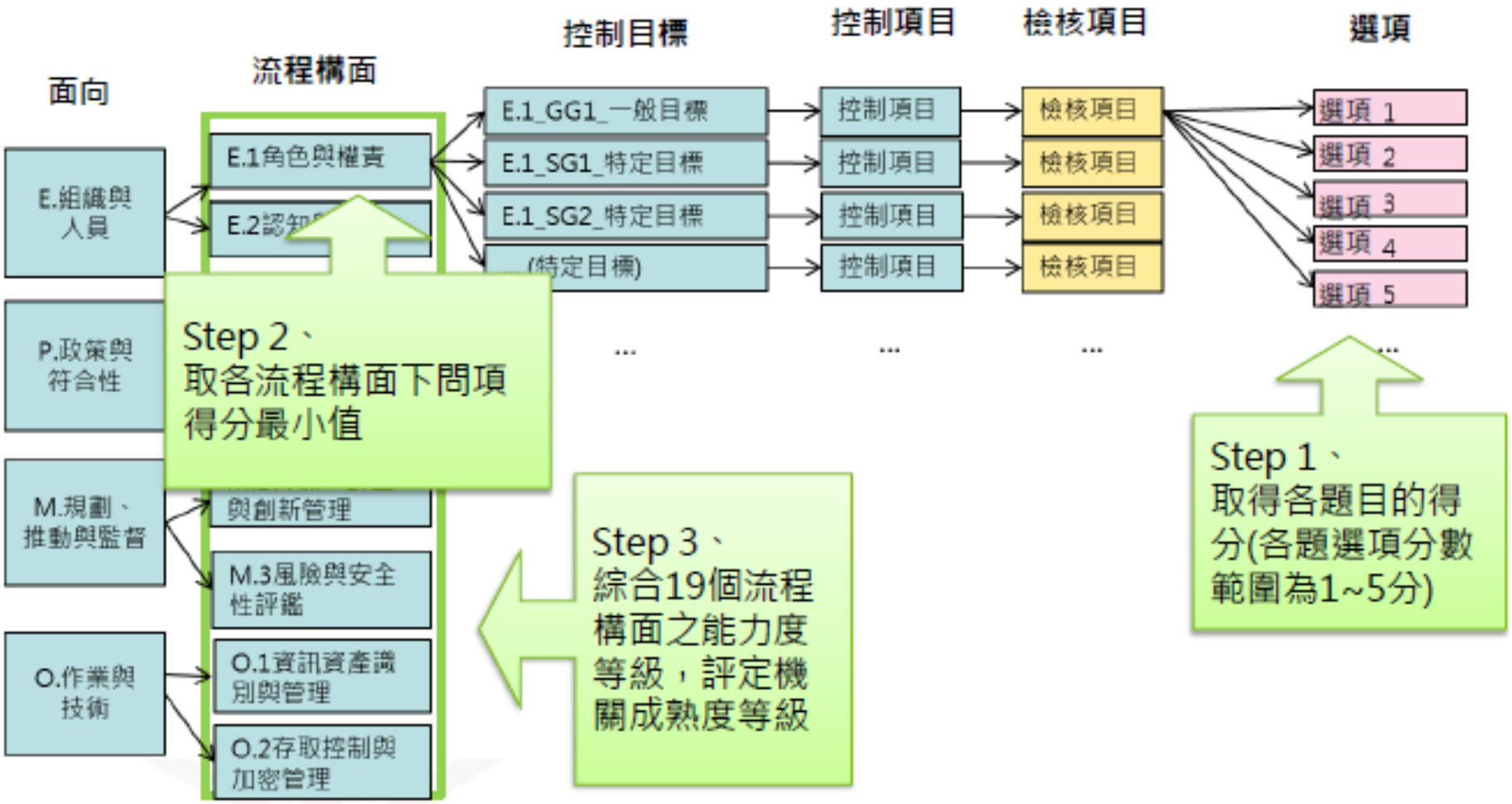
A、B、C級機關專屬問項設計範例

- 參考應辦事項與政府相關規定，設計A、B與C級機關選項
- 選項由Level 1~Level 5逐層堆疊 必須前面Level選項說明已滿足始能進入下一Level選項

面向	流程構面	檢核項目編號	檢核項目	選項編號	A級機關選項	B級機關選項	C級機關選項	選項設計原則
M.規劃推動與監督	M.3風險及安全性評鑑與管理	M.3.2	機關辦理網站安全弱點檢測，是否符合對各級機關要求之頻率?	1	近一年機關已規劃網站安全弱點檢測	近兩年機關已有規劃網站安全弱點檢測	機關已有依據主管機關規定規劃網站安全弱點檢測	該流程已具備部分活動
				2	每年機關已辦理至少2次網站安全弱點檢測	每年機關已辦理至少1次網站安全弱點檢測	前述事項已完成，且機關已有依據主管機關規定辦理網站安全弱點檢測	基準值：該流程已管理且具備工作產出或符合應辦事項要求
				3	前述事項已完成，且針對掃描結果為高風險等級弱點，能於預定時間內改善完成，並執行覆掃作業	前述事項已完成，且針對掃描結果為高風險等級弱點，能於預定時間內改善完成，並執行覆掃作業	前述事項已完成，且針對掃描結果為高風險等級弱點，能於預定時間內改善完成，並執行覆掃作業	標竿值：該流程已被標準化，且確保該流程已被有效實施
				4	前述2~3事項已完成，且已制定衡量指標例如高風險等級弱點數量，且檢測結果能達成衡量目標值	前述2~3事項已完成，且已制定衡量指標例如高風險等級弱點數量，且檢測結果能達成衡量目標值	前述2~3事項已完成，且已制定衡量指標例如高風險等級弱點數量，且檢測結果能達成衡量目標值	該流程可透過衡量結果，了解執行成效
				5	前述2~4事項已完成，且針對掃描結果為中風險與低風險項目進行評估，必要時研擬修補措施或補償性措施	前述2~4事項已完成，且針對掃描結果為中風險與低風險項目進行評估，必要時研擬修補措施或補償性措施	前述2~4事項已完成，且針對掃描結果為中風險與低風險項目進行評估，必要時研擬修補措施或補償性措施	基於過去執行成效分析或其他創新方式強化與優化各流程構面

能力度與成熟度評核(Rating)流程說明

- 計算流程構面下各問項得分最小值，作為該流程構面之能力度依據
- 綜合19個流程構面之能力度，評定機關之成熟度等級



以機關評審後產生之計算結果為例

取各流程構面下問項得分最小值

流程構面分級原則	流程構面成熟度等級	流程構面	流程構面能力度
Extended Process Set	Level 5	M.1 創新管理	3
	Level 4	P.3 資安風險監控	3
		M.5 績效與成果監督	4
	Level 3	P.1 治理架構與政策	4
		P.2 資安資源確保與監控	5
		P.4 利害關係人溝通	3
	Level 2	M.2 目標與計畫管理	3
		M.3 預算與成本管理	3
		M.6 資安事故管理與緊急應變	4
		M.8 供應商管理	4
		O.1 資訊資產識別與管理	3
		O.2 存取控制	3
		O.4 系統獲取、開發及維護	4
Basic Process Set	Level 1	E.1 角色與權責	4
		E.2 認知與訓練	4
		P.5 第三方驗證與內稽	3
		M.4 風險及安全性評鑑與管理	3
		M.7 營運持續管理	3
		O.3 作業與通訊安全管理	3

機關整體成熟度

Level 3

L1~4流程未全數達成能力度4，故成熟度未滿Level 4

L1~3流程皆達成能力度3，故成熟度滿足Level 3

L1~2流程皆達成能力度2，故成熟度滿足Level 2

L1流程皆達成能力度1，故成熟度滿足Level 1

機關資安治理後續配合任務

	資安治理成熟度自我評審-A級機關	資安治理成熟度自我評審-A與B級機關	資安治理成熟度自我評審-A、B與C+級機關
	106年度	107年度	108年度
主要任務	1. 辦理資安治理成熟度主導評審員訓練課程(針對A級與B級機關) 2. A級機關每年使用資安治理評審工具進行自我評估一次 3. 機關檢視與分析評估結果並提出因應措施	1. 辦理資安治理成熟度主導評審員訓練課程(針對A、B與C+級機關) 2. A與B級機關每年使用資安治理評審工具進行自我評估一次 3. 機關檢視與分析評估結果與歷年比較，並提出因應措施	1. 辦理資安治理成熟度自我評審分享會(邀請A、B級機關分享前2年自我評審與改善經驗) 2. A、B與C+級機關每年使用資安治理評審工具進行自我評估一次，C級採自願性質 3. 行政院資安處檢視各級機關成熟度評審結果，調整資安治理推動重點與規劃
相關單位	■ 行政院資安處 ■ 技服中心 ■ 機關自我評審人員 ■ 機關資安治理推動人員	■ 行政院資安處 ■ 技服中心 ■ 機關自我評審人員 ■ 機關資安治理推動人員	■ 行政院資安處 ■ 技服中心 ■ 機關自我評審人員 ■ 機關資安治理推動人員

NII協助規劃與推動B級機關資安治理成熟度評估教育訓練

- 主要針對教育機構B級單位，分北、中、南三區(暫訂臺北、臺中及高雄)規劃及辦理3梯次(每梯次3小時、60位學員)資安治理成熟度檢核項說明教育訓練課程。
- 分區教育訓練之辦理步驟，主要分為前期準備、報名階段，以及課程辦理三個階段，每個階段的細部工作項目如下圖所示。(大約在5月及6月)

資料來源

- 行政院國家資通安全會報技術服務中心-資安治理概論與規劃
- 行政院國家資通安全會報技術服務中心-資安治理成熟度評估機制暨工具說明會

謝謝
聆聽

Question
& Answer ...