政府機關資安治理成熟度評估機制

吳啟文　行政院國家資通安全會報技術服務中心主任
林晶瑩　行政院國家資通安全會報技術服務中心正工程師

壹、緣起

我國政府推動資訊安全管理制度已有一段時間，大多數政府機關業已導入資訊安全管理系統（Information Security Management System, ISMS），並通過公正第三方之驗證，惟在機關內之分工，資安管理工作大多為資訊單位責任，其他單位較少參與。因應資通訊科技發展及資安威脅趨勢，先進國家已將「資安管理」提升至「資安治理」層次，資安風險為組織重要風險之一，資安目標亦為組織重要目標之一，管理高層加強對於資安防護工作之重視，同時亦反映在組織資安相關人力與經費等資源之投入，以降低資安風險。

另配合「資通安全管理法」於 2019 年 1 月 1 日正式施行，其子法「資通安全責任等級分級辦法」之應辦事項規定，資通安全責任等級 A 級與 B 級之公務機關，每年應辦理 1 次資安治理成熟度評估作業。

一、背景

我國於 2001 年 1 月，成立「行政院國家資通安全會報」（以下簡稱資安會報），每 4 年推動 1 期重大資通安全計畫，包含建構資安防護體系之「第一期機制計畫」、健全資安防護能力之「第二期機制計畫」、強化資安整體應變能力之「第三期發展方案」（註 1）及加強資安防護管理之「第四期發展方案」（註 2）。目前刻正推動「國家資通安全發展方案（2017–2020 年）」（以下簡稱第五期發展方案）（註 3），期打造安全可信賴的數位國家，其中「完備資安基礎環境」推動策略之「建立政府資安治理模式」具體措施，將推動政府機關導入資安治理制度，同時於 2019 年推動 30 個 A 級政府機關資安治理成熟度達第 2 級以上，2020 年推動所有 A 級政府機關資安治理成熟度達第 3 級以上，第五期發展方案藍圖詳見圖 1。

「資通安全管理法」已於 2019 年 1 月 1 日正式施行，依其子法「資通安全責任等級分級辦法」之管理面應辦事項，資通安全責任等級 A 級與 B 級之公務機關，每年應辦理 1 次資安治理成熟度評估作業，詳見圖 2。

二、推動歷程

我國自 2014 年起開始推動資安治理制度，首先建立政府資安治理架構，包含四大面向與 18 個流程構面，以及政府機關資安治理成熟度評估機制與自動化評估工具，並遴選 3 個政府機關試行導入。2015 年訂定資安

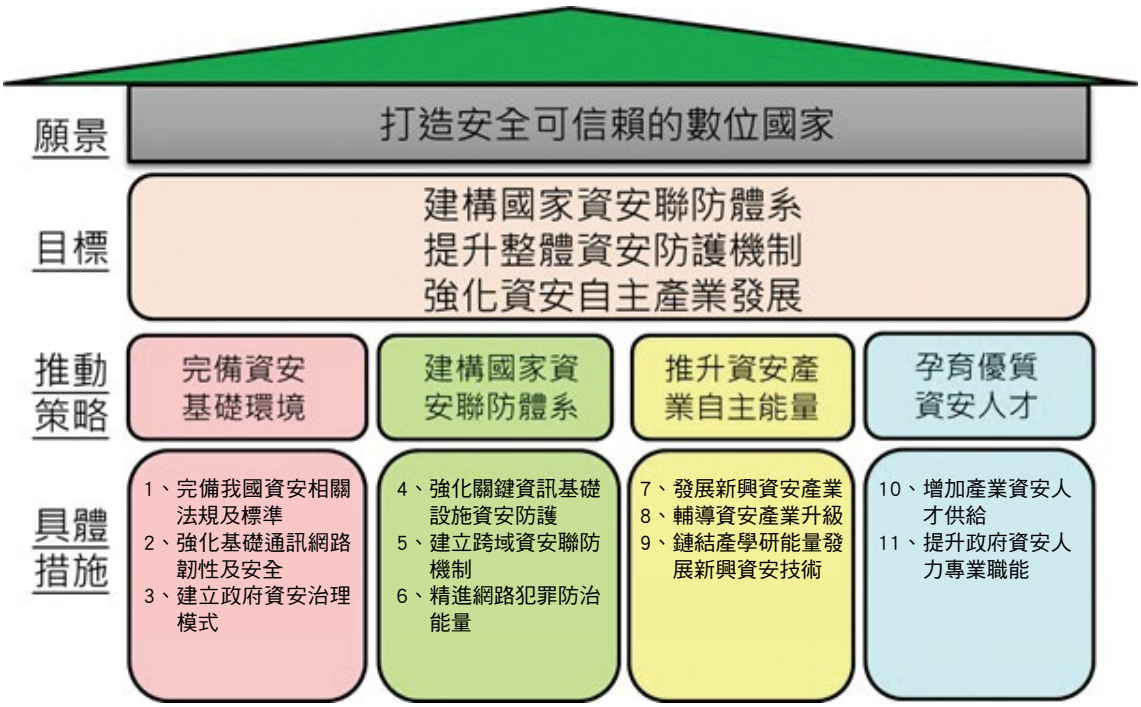

圖 1　第五期發展方案藍圖

資料來源：國家資通安全發展方案（2017–2020 年）

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置四人；須以專職人員配置之。
	內部資通安全稽核		每年辦理二次。
	業務持續運作演練		全部核心資通系統每年辦理一次。
	資安治理成熟度評估		每年辦理一次。

圖 2　資安責任等級分級應辦事項

資料來源：資通安全責任等級分級辦法之應辦事項

防護能力具體指標，並依資通安全責任等級A、B與C級政府機關，發展資安治理評估問項，並遴選A、B與C級機關試行導入。2016年發展資安防護能力指標與分析，包含建立評估使用手冊與評審員受訓機制、規劃評估機制及調整評估工具等。2017年推動資安治理制度成熟度自評作業，精進資安防護能力問項與使用手冊，辦理資安治理自評教育訓練，強化評估工具之效能，並建立常見問題集。2018年檢討與調整資安治理架構，強化資安治理面向、流程構面及問項，並依「資通安全管理法」與其子法規定，更新問項內容與調整評估機制，並辦理政府機關試行導入。另配合「資安服務團」協助機關推動與落實各項政策及措施，辦理資安治理訓練課程與實地輔導作業。

貳、資安治理成熟度評估架構

一、架構設計原則

蒐集資安治理相關國際標準與最佳實務，包含ISACA COBIT 5（註4）、ISO／IEC／CNS 27014（註5）、ISO／IEC／CNS 27001（註6）、ISO／IEC33020（註7）、ISO／IEC33004（註8）及NIST Cyber Security Framework（註9）等，參考其方法論與精神（詳見圖3），並結合我國資安推動之「策略面」、「管理面」及「技術面」3大面向，發展適合我國之資安治理成熟度架構。

同時，亦將我國資安相關法規之要求納入設計原則，包含資通安全管理法、資通安全管理法施行細則（含資通安全維護計畫）、資通安全責任等級分級辦法、資通安全事件通報及應變辦法等。綜整國際標準之方法論、我國法規之要求及政府機關之試行回饋，資安治理成熟度架構包含3大面向、11個流程構面，詳見圖4。

架構之最底層為「技術面」，包含T1存取控制管理、T2通訊與作業安全管理、T3資安事件通報與處理及T4資訊系統開發與維護安全管理。架構之中間層為「管理面」，包含M1資產管理與風險評鑑、M2資訊委外安全管理及M3資安認知與教育訓練。架構之最上層為「策略面」，包含S1資安政策與組織健全、S2資安治理架構、S3資安資源管理及S4資安管理監督。

二、流程構面目標範圍

依據「策略面」、「管理面」及「技術面」3大面向之11個流程構面，建立各流程構面之目標範圍，詳見圖5。

參考CERT RMM（註10）流程模型，設計流程構面之涵蓋要素，包含控制目標、控制項目及佐證資料等，詳見圖6。

三、檢核項目設計重點

參考我國相關法規要求與國際標準，包含資通安全管理法及其子法、第五期發展方案及ISO／IEC／CNS 27014（註5）、ISO／IEC／CNS 27001（註6）、CERT RMM（註10）、ISO／IEC 33020

（註 7）、ISO ／ IEC 33004（註8）、NIST Cyber Security Framework（註 9）及ISACA COBIT 5（註 4），並考量 A 級與 B 級機關之特性，設計對應之檢核項目，包含政策與組織管理有效性、績效與成果監督落實性、資安風險監控與資源提供有效性、績效與成果監督有效性、資安事件管理與緊急應變有效性及應辦事項各作業執行之有效性，並依資安治理成熟度架構之 3 大面向與 11 個流程構面，設計 41 個檢核項目。

國際標準或最佳實務名稱	方法論參考精神	於本案應用領域
ISO/IEC/CNS 27014:2013	資安治理架構六大原則（含建立全組織之資訊安全、採用基於風險的作法、設定投資決策方向、確保符合內部與外部要求、培養安全良好之環境、審查相關營運成果）	•發展資安治理架構，策略與管理面向及對應流程構面
ISO/IEC 38500:2015	資安治理架構中的三項主要活動包含指導、評估、監督	•以組織業務目標、業務需求的角度來監督與評量資訊單位績效
ISACA COBIT 5	資安治理架構中的三項主要活動包含指導、評估、監督	•定義資安治理架構的三大面向
ISO/IEC/CNS 27001:2013	資訊安全管理之控制領域、控制目標與控制項目	•發展資安治理架構之面向與對應流程構面
NIST SP800-100	資訊安全治理、認知與教育訓練、資本規劃與投資控制、認證、保證與安全評估	•發展策略面向之流程構面與評估檢核項目 •發展管理面向之流程構面與評估檢核項目
CERT RMM	一般目標、特定目標、一般執行方法、特定執行方法及對應典型的工作產品	•做為資安治理成熟度評估控制項目發展方式（含控制目標、控制項目以及對應產出）
NIST Cyber Security Framework	資產管理、風險評估、風險管理策略、偵測與告警、回應程序及復原規劃等評估構面	•發展管理面向之流程構面與評估檢核項目 •發展技術面向之流程構面與評估檢核項目
ISO/IEC 33020:2015	流程改善之能力度衡量方式	•能力度等級區分方式
ISO/IEC 33004:2015	流程改善之成熟度等級定義與計算方式	•成熟度等級區分方式 •能力度與成熟度之對應評估方式

圖 3　參考之國際標準與最佳實務

資料來源：技服中心整理

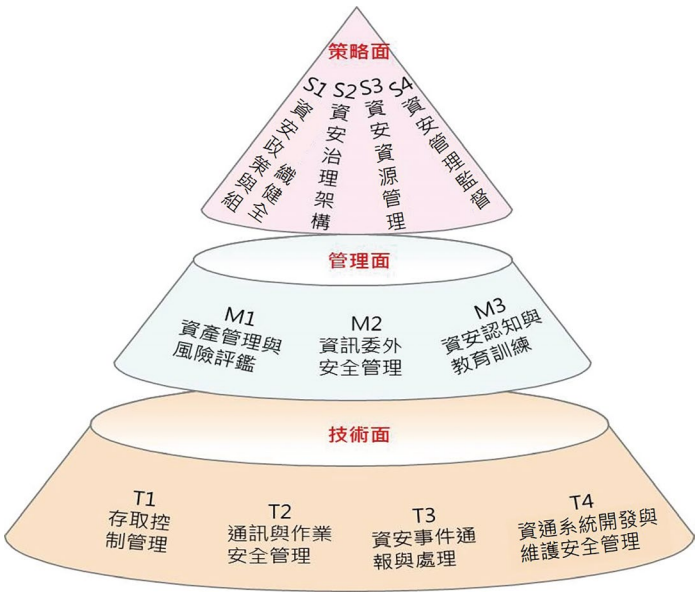

圖 4　資安治理成熟度架構

資料來源：技服中心整理

面向	流程構面	目標範圍	
策略	S1 資安政策與組織健全	• 資安政策建立 • 資安組織與管理審查	• 資安相關法規遵循
	S2 資安治理架構	• 資安新興議題評估	• 利害相關者溝通
	S3 資安資源管理	• 資安資源確保	• 資安專職人員配置
	S4 資安管理監督	• 績效與成果監督	• 業務持續運作管理
管理	M1 資產管理與風險評鑑	• 資安風險管理	• 資通系統分級與防護
	M2 資訊委外安全管理	• 委外廠商資安專業能力	• 委外廠商資安管理 • 委外資安稽核
	M3 資安認知與教育訓練	• 資安認知與教育訓練	
技術	T1 存取控制管理	• 網路安全管理 • 權限管理	• 加密管理
	T2 通訊與作業安全管理	• 惡意軟體管理 • 遠距工作管理 • 電子郵件安全 • 實體環境控制措施 • 資料備份	• 儲存媒體處置 • 資通安全監控 • 資通安全防護 • 安全性檢測
	T3 資安事件通報與處理	• 資安事件通報應變	• 日誌紀錄保存
	T4 資通系統開發與維護安全管理	• 安全系統發展生命週期(SSDLC)落實	

圖 5　流程構面目標範圍

資料來源：技服中心整理

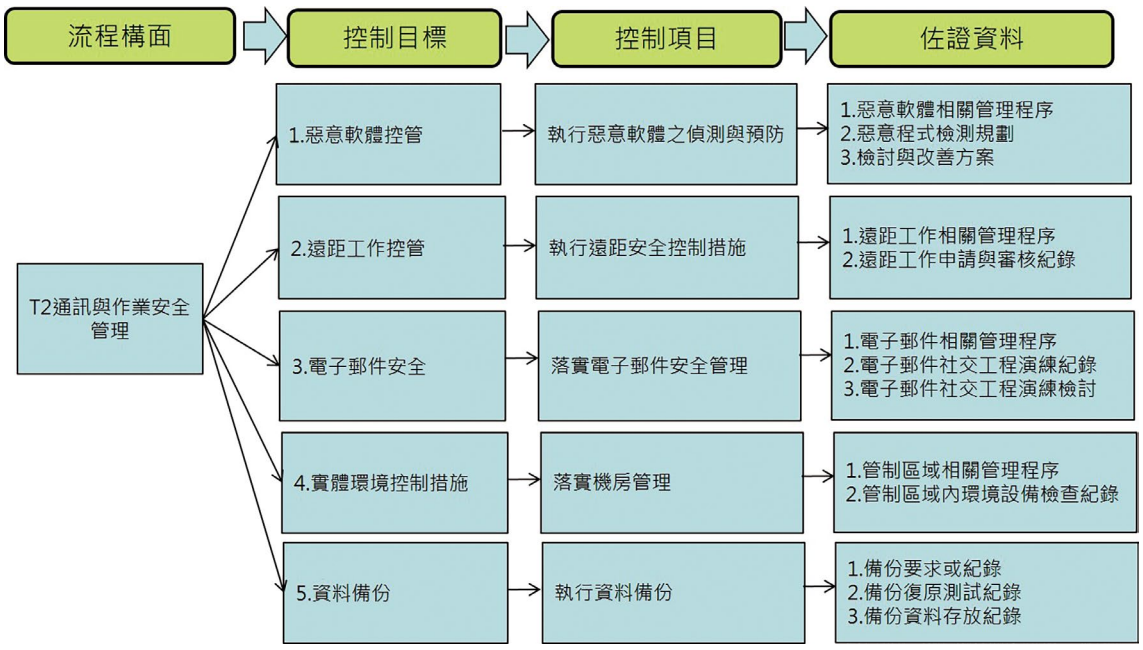

圖 6　流程構面之涵蓋要素

資料來源：技服中心整理

參、能力度、成熟度及評估方法介紹

為確保評估方法之可信度與適用性，參考能力度、成熟度評估相關國際標準，包含 ISO ／ IEC 33004（註 8）與 ISO ／ IEC 33020（註 7）等，詳見圖 7，依據資安治理成熟度架構之運作模式，選定成熟度之評估標的，並建立能力度（Capability）與成熟度（Maturity）分級定義與評估原則，設計完整的資安治理成熟度評估方法，透過量化方式，計算受評單位之資安治理成熟度，並提供評估結果與相關建議。

一、能力度等級定義

在能力度設計上，為有效評估各流程構面之執行程度，使能力度評估結果能與後續之成熟度計算方式結合，參考國際標準 ISO ／ IEC 33020（註 7）設計，將能力度等級由低至高分為 6 級，分別為「Level 0 未執行流程（Incomplete Process）」、「Level 1已執行流程（Performed Process）」、「Level 2已管理流程（Managed Process）」、「Level 3標準化流程（Established Process）」、「Level 4可預測流程（Predictable Process）」及「Level 5最佳化流程（Optimizing Process）」，詳見圖 8。

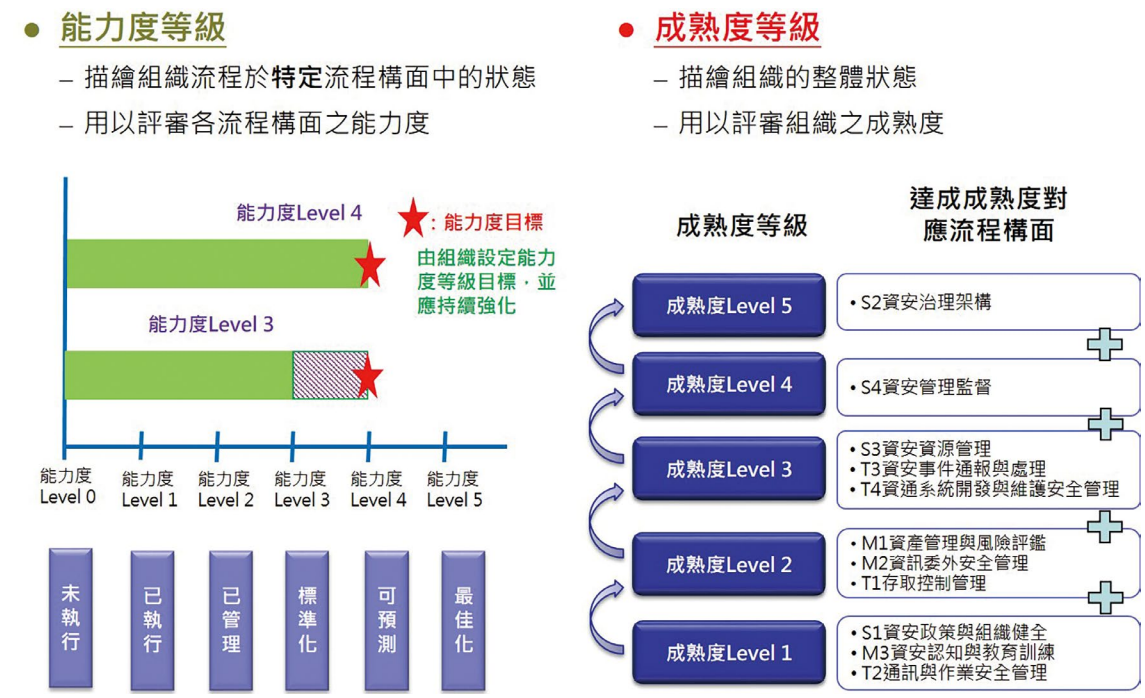

圖 7　能力度與成熟度之評估方法

資料來源：技服中心整理

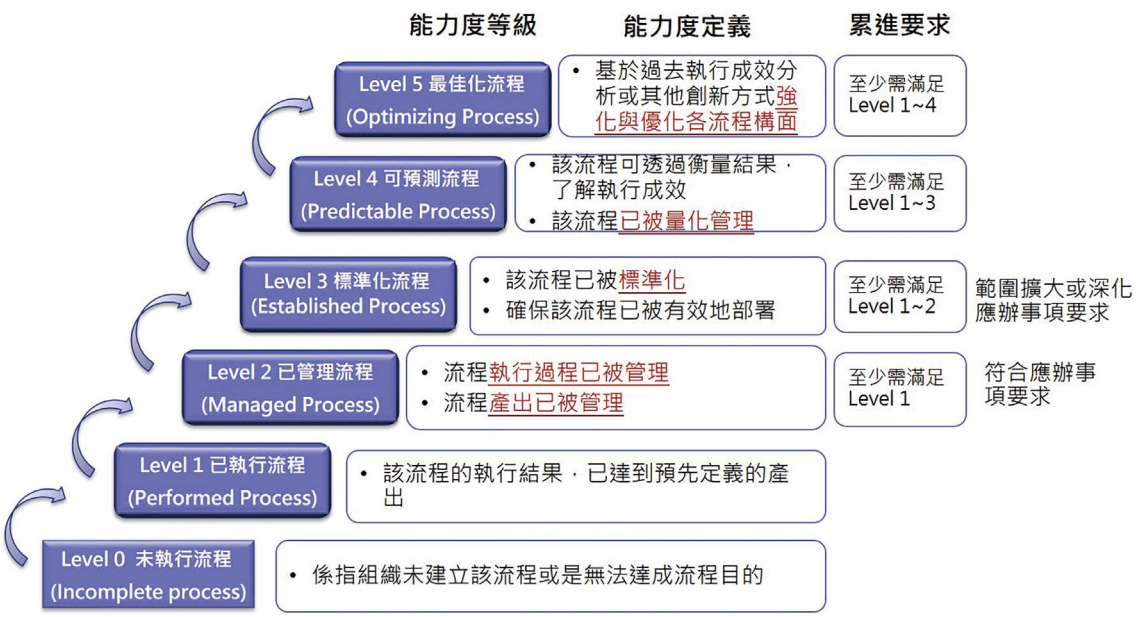

圖 8　能力度等級定義

資料來源：技服中心整理

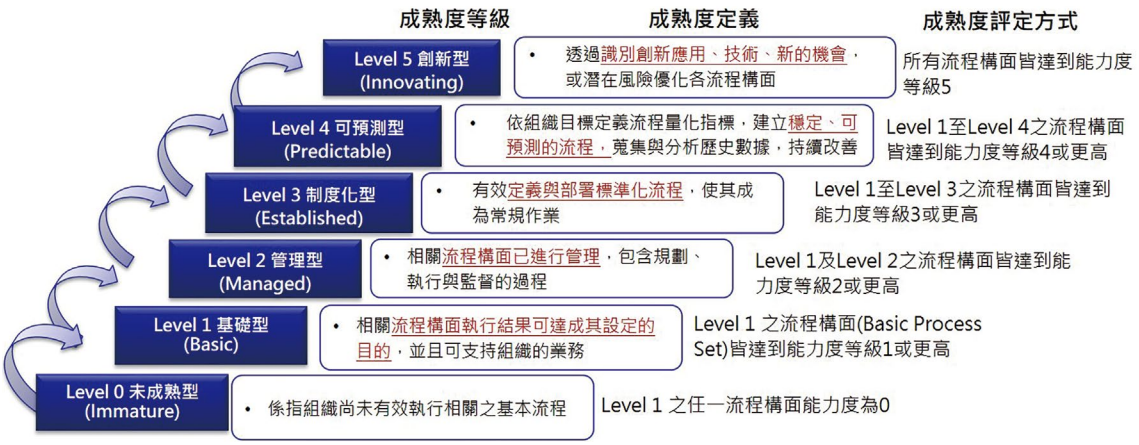

圖 9　成熟度等級定義

資料來源：技服中心整理

二、成熟度等級定義

為有效評估整體資安治理能力成熟度，參考國際標準 ISO ／ IEC 33004（註 8）之成熟度等級定義與計算方式，將成熟度等級由低至高分為 6 級，分別為「Level 0 未成熟型（Immature）」、「Level 1 基礎型（Basic）」、「Level 2 管理型（Managed）」、「Level 3 制度化型（Established）」、「Level 4 可預測型（Predictable）」及「Level 5 創新型（Innovating）」，詳見圖 9。

三、成熟度評估方法

資安治理成熟度評估分為 4 個階段，說明如下。

（一）第 1 階段：確定流程構面與其分級方式

首先，以 11 個流程構面為基礎，進行評估作業。將流程構面對應至成熟度等級 Level 1–Level 5，以定義成熟度評估模型之流程構面分級，做為後續計算成熟度之基礎。成熟度評估模型之流程構面分為 2 類，包含 Basic Process Set 與 Extended Process Set，詳見圖 10。

（二）第 2 階段：確定能力度與成熟度之等級分級

依據國際標準 ISO ／ IEC 33020（註 7）與 ISO ／ IEC 33004（註 8），定義各流程構面之能力度與成熟度之等級分級，以利完成檢核項目填寫後，可將所獲得之評分換算為各流程構面之能力度等級與整體成熟度等級。

（三）第 3 階段：擬定檢核項目

依據受評之流程構面，擬定控制目標與控制項目，並依對應之控制目標與控制項目，擬定檢核項目。

成熟度等級	分級設計考量	資安治理三大面向		
		策略	管理	技術
Level 5	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 3至Level 5分別進行定義	S2資安治理架構		
Level 4		S4資安管理監督		
Level 3		S3資安資源管理		T3資安事件通報與處理 T4資通系統開發與維護安全管理
Level 2	依以下原則做為Basic Process Set從Level 1至Level 2須滿足之考量 • 資安認知與教育訓練 • 作業與技術安全防護要求相關 • 資產管理與風險評鑑 • 資訊委外安全管理 • 存取控制管理		M1資產管理與風險評鑑 M2資訊委外安全管理	T1存取控制管理
Level 1		S1資安政策及組織健全	M3資安認知與教育訓練	T2通訊與作業安全管理

圖 10　成熟度評估模型之流程構面分級

註：Basic Process Set 資安治理之基本流程構面，包含成熟度 Level1 至 Level2 相關流程構面；Extended Process Set 強化資安治理之延伸流程構面，包含成熟度 Level 3 至 Level 5 相關流程構面。

資料來源：技服中心整理

（四）第 4 階段：計算成熟度評估結果

依據檢核項目與選項之配分設計，計算各流程構面之能力度，再依據能力度評估結果與流程構面之等級分級，計算出整體成熟度。

● 步驟 1：各問項得分

依各問項填寫內容 0–5 得分。

● 步驟 2：流程構面之能力度計算方式

依據木桶理論，取流程構面之檢核項目得分最低者，做為該流程構面之能力度。

● 步驟 3：整體成熟度計算方式

依 11 個流程構面之能力度與分級，綜合檢視步驟 2 所計算出之各流程構面能力度，以評定整體成熟度等級。

資安治理成熟度評估機制設計，先以流程構面之檢核項目得分最低者為該流程構面能力度，詳見圖 11，再依流程構面能力度之達成狀況，計算出整體成熟度等級，詳見圖 12。

肆、預期效益

透過資安治理成熟度評估機制之推動，期能掌握政府整體資安防護情形，加強管理階層對於資安管理工作之重視，同時增加資安人力與經費等資源之投入，以降低資安風險加強。以下分不同角色，說明其預期效益。

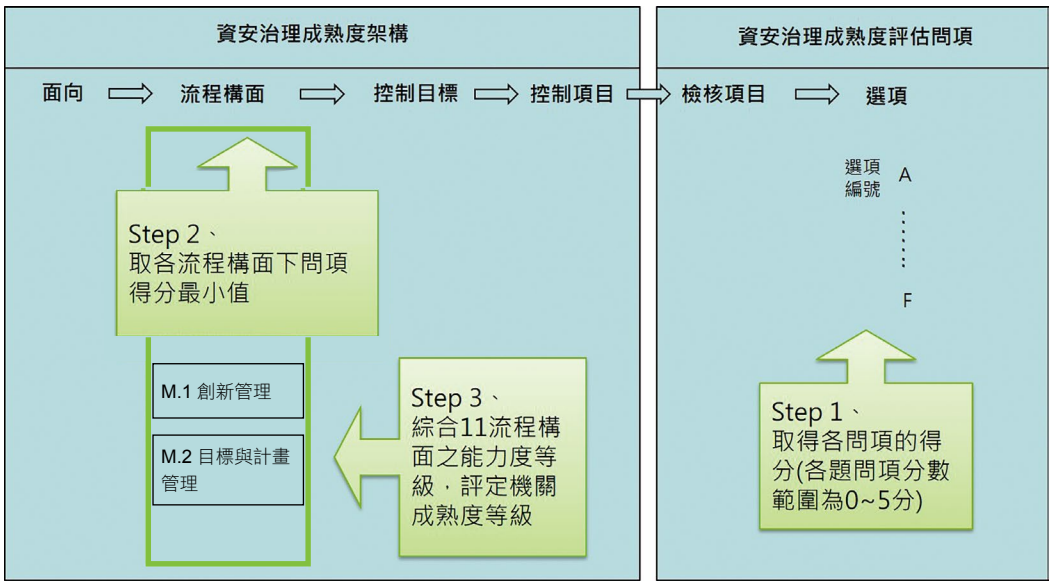

圖 11　能力度評估流程說明

資料來源：技服中心整理

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	S2資安治理架構	3
	Level 4	S4資安管理監督	3
	Level 3	S3資安資源管理	4
		T3資安事件通報與處理	5
		T4資訊系統開發與維護安全管理	3
Basic Process Set	Level 2	M1資產管理與風險評鑑	3
		M2資訊委外安全管理	3
		T1存取控制管理	4
	Level 1	S1資安政策及組織健全	4
		M3資安認知與教育訓練	4
		T2通訊與作業安全管理	3

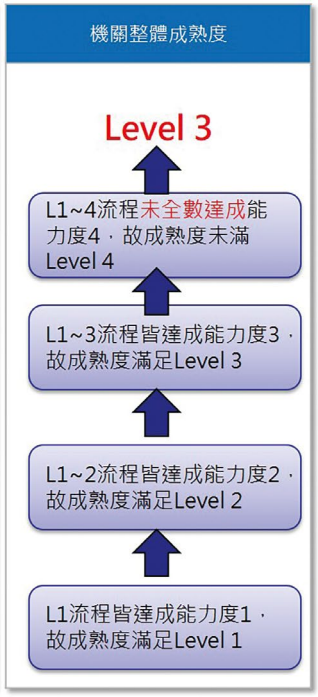

圖 12　成熟度等級計算範例

資料來源：技服中心整理

一、行政院資通安全處

透過資安治理成熟度評估機制，掌握政府機關資安治理落實情形、困難及挑戰，以提供資安政策訂定之參考。另建立資安治理成熟度與防護能力指標之巨量資料分析平台，提升政府機關資安威脅早期預警與應變復原能力。

二、主管機關

藉由所屬機關之流程構面能力度分析，提供擬定資安推動重點之參考。另藉由所屬機關之自評結果彙整分析，提供具體資安防護建議與強化資源之有效運用。

三、政府機關

藉由自評結果分析，強化機關資安防護能量，提升資通系統安全及人員資安能力。另藉由整體改善方案提報，提升機關首長與資安長對於資安防護工作之支持與重視。

伍、結語

政府機關資安治理成熟度評估機制之建立，係因應資通訊科技發展及資安威脅趨勢，將「資安管理」提升至「資安治理」層次，同時配合「資通安全管理法」及其子法相關規定，推動政府機關導入資安治理制度，辦理資安治理成熟度自評作業，以掌握整體資安防護情形。

政府機關資安治理成熟度架構之設計，係參考資安治理相關國際標準與最佳實務之方法論與精神，並結合我國資安推動之「策略面」、「管理面」及「技術面」3 大面向，最後歸納出 11 個流程構面與 41 個檢核項目。

透過政府機關資安治理成熟度評估機制之落實，受評機關可了解本身之各流程構面執行情形，檢討如何強化資安防護措施，以提升整體成熟度。受評機關之主管與資安長，亦可透過各流程構面之能力度分析，掌握需強化之流程構面，以利後續資安改善計畫之訂定。同時，受評機關之主管機關與行政院資通安全處，可掌握政府機關整體資安治理成熟度狀況，分析各流程構面之能力度，以做為後續資安政策推動與資安資源分配之參考依據。

附註

註 1：行政院國家資通安全會報。2009。國家資通訊安全發展方案（98 年 –101 年）。臺北：行政院國家資通安全會報。

註 2：行政院國家資通安全會報。2013。國家資通訊安全發展方案（102 年 –105 年）。臺北：行政院國家資通安全會報。

註 3：行政院國家資通安全會報。2017。國家資通安全發展方案（106 年 –109 年）。臺北：行政院國家資通安全會報。

註 4：ISACA. 2012. COBIT 5. < http：//www.isaca.org/cobit >

註 5：ISO（2009）2nd Working Draft for ISO/IEC 27014 － Information technology － Security techniques － Information security governance framework：2009–12–01, ISO/IEC JTC1/SC7 N8244

註 6：ISO（2009）2nd Working Draft for ISO/IEC 27001 － Information technology － Security techniques － Information security

management systems － Requirements：2009–12–11, ISO/IEC JTC1/SC27 N8232.

註7：ISO（2015）ISO/IEC 33020 － Information technology － Process assessment － Process measurement framework for assessment of process capability.

註8：ISO（2015）ISO/IEC 33004 － Information Technology － process assessment － Requirements for process reference, process assessment and maturity models.

註9：NIST, NIST Releases Version 1.1 of its Popular Cybersecurity Framework, April 2018. ＜ https：//www.nist.gov/news–events/news/2018/04/nist–releases–version–11–its–popular–cybersecurity–framework ＞

註10：Richard A. Caralli, Julia H. Allen, David W. White. 2010. CERT Resilience Management Model （CERT–RMM）：A Maturity Model for Managing Operational Resilience. Upper Saddle River, N.J., Addison–Wesley.

參考文獻

1. 行政院國家資通安全會報。2009。國家資通訊安全發展方案（98 年 –101 年）。臺北：行政院國家資通安全會報。
2. 行政院國家資通安全會報。2013。國家資通訊安全發展方案（102 年 –105 年）。臺北：行政院國家資通安全會報。
3. 行政院國家資通安全會報。2017。國家資通安全發展方案（106 年 –109 年）。臺北：行政院國家資通安全會報。
4. ISACA. 2012. COBIT 5. ＜ http：//www.isaca.org/cobit ＞
5. ISO（2009） 2nd Working Draft for ISO／IEC 27014 － Information technology － Security techniques － Information security governance framework：2009–12–01, ISO／IEC JTC1／SC7 N8244.
6. ISO（2009） 2nd Working Draft for ISO／IEC 27001 － Information technology － Security techniques － Information security management systems － Requirements：2009–12–11, ISO／IEC JTC1／SC27 N8232.
7. ISO（2015） ISO／IEC 33020 － Information technology － Process assessment － Process measurement framework for assessment of process capability.
8. ISO（2015） ISO／IEC 33004 － Information Technology － process assessment － Requirements for process reference, process assessment and maturity models.
9. NIST, NIST Releases Version 1.1 of its Popular Cybersecurity Framework, April 2018. ＜ https：//www.nist.gov/news–events/news/2018/04/nist–releases–version–11–its–popular–cybersecurity–framework ＞
10. Richard A. Caralli, Julia H. Allen, David W. White. 2010. CERT Resilience Management Model （CERT–RMM）：A Maturity Model for Managing Operational Resilience. Upper Saddle River, N.J., Addison–Wesley.