資安治理成熟度評估參考指引
(V1.2)

執行單位：行政院國家資通安全會報技術服務中心
中華民國111年8月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0	109/9/30	新編
2	V1.1	109/11/13	修訂文字
3	V1.2	111/8/29	修訂內文「資通安全處」->「資通安全署」

▪

摘要

報告名稱	資安治理成熟度評估參考指引
資訊等級	☐機密　☐密　☐敏感　☐內部公開　☒普通

內容摘要：

本指引旨在說明資安治理成熟度之評估架構、評估方法及評估系統功能介紹，以協助政府機關了解資安治理成熟度評估作業規範。

本指引針對資安治理成熟度評估機制與檢核項目進行說明，包含各檢核項目之答題標準與注意事項，以強化對資安治理成熟度評估作業之了解與評估結果之一致性。

關鍵詞	資通安全、資安治理、成熟度

目　錄

圖 目 錄

表 目 錄

1. 前言

1.1 目的

本指引旨在說明資安治理成熟度之評估架構、評估方法及評估系統功能介紹，以協助政府機關了解資安治理成熟度評估作業規範。

本指引將針對資安治理成熟度評估之機制與檢核項目進行說明，包含各檢核項目之答題標準與注意事項，以強化對資安治理成熟度評估作業之了解與評估結果之一致性。

1.2 適用對象

本指引主要適用對象為 A 級與 B 級公務機關之人員，特別為資安治理成熟度自評負責人員與機關內部權責主管。

1.3 使用建議

本指引係為協助使用者了解資安治理成熟度評估機制，以執行資安治理成熟度評估作業，如未曾接觸資安治理成熟度評估作業，建議閱讀第 2 章至第 4 章，以整體了解評估作業之運作與重點。若使用者曾進行評估作業，建議閱讀第 3 章至第 4 章，以確認檢核項目與系統操作方式是否正確。

1.4 章節架構

第 1 章前言說明本文之目的、適用對象、使用建議及章節架構。

第 2 章資安治理成熟度評估架構，包含緣起、架構設計原則、流程構面目標範圍、檢核項目設計重點、能力度與成熟度評估方法及預期效益。

第 3 章資安治理成熟度檢核項目，包含策略面檢核項目說明、管理面檢核項目說明及技術面檢核項目說明。

第 4 章資安治理成熟度評估系統，包含資安治理成熟度評估系統自評流程

與資安治理成熟度評估系統功能說明。

第 5 章結論，說明本指引對使用者之幫助

第 6 章參考文獻，詳列本指引所參考之文件與資料。

2. 資安治理成熟度評估架構

本章節說明資安治理成熟度評估架構，包含緣起、架構設計原則、流程構面目標範圍、檢核項目設計重點及能力度與成熟度評估方法。

2.1 緣起

「資通安全管理法」於 108 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 級公務機關每年應辦理 1 次資安治理成熟度評估作業，詳見表 1。

表1　資通安全責任等級分級辦法之應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資安治理成熟度評估		每年辦理一次

資料來源：本計畫整理

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。資安治理屬於高階管理階層之活動，係以評估(Evaluate)、指導(Direct)及監督(Monitor)(以下簡稱EDM)建立治理架構，向下監督資訊安全管理系統執行情形，並透過治理架構向上溝通，回應組織利害相關者之要求；資安管理為遵循治理架構所形成之指導原則，規劃與建立組織適用之管理機制，並透過日常維運執行與監督過程，確保其持續改善，並提供組織得以再次評估之管理回饋。

2.2 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 ISO/IEC/CNS 27014[2]、ISO/IEC/CNS 27001[3]、CERT RMM[4]、、ISO/IEC 21827[5]、ISO/IEC

33004[6]、CMMI[6]、ISO/IEC 33020[8]及 NIST Cyber Security Framework[9]等，參考其方法論與精神，並結合我國資安推動之「策略面」、「管理面」及「技術面」3 大面向，發展適合於我國之資安治理成熟度架構，詳見表 2。

表2　參考之國際標準與最佳實務

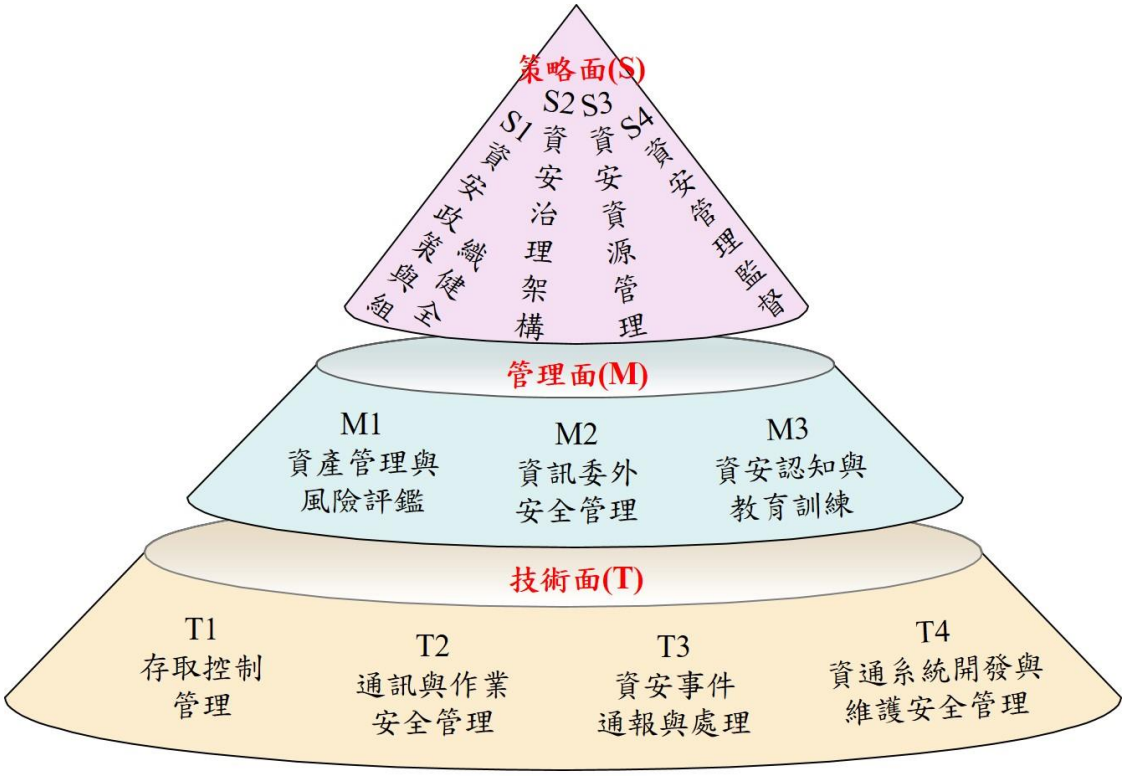
國際標準或最佳實務名稱	方法論參考精神	應用領域
ISO/IEC/CNS 27014：2013	資安治理架構六大原則(含建立全組織之資訊安全、採取以風險為基礎之作法、設定投資決策方向、確保符合內部與外部要求、培養安全良好之環境、審查相關營運成果)	發展資安治理架構，策略面、管理面及對應流程構面
ISO/IEC/CNS 27001：2013	資訊安全管理之控制領域、控制目標及控制項目	發展資安治理架構之面向與對應流程構面
CERT RMM	一般目標、特定目標、一般執行方法、特定執行方法及對應典型之工作產品	資安治理成熟度評估控制項目發展方式(含控制目標、控制項目及對應產出)
ISO/IEC 21827：2008	能力成熟度模型之等級	成熟度等級區分方式
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
CMMI	能力成熟度模型之等級	成熟度等級區分方式
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
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	▪發展管理面之流程構面與檢核項目 ▪發展技術面之流程構面與檢核項目

資料來源：本計畫整理

同時，亦將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 1。

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。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 資通系統開發與維護安全管理。



資料來源：本計畫整理

圖1　資安治理成熟度架構

2.3 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，詳見表 3。

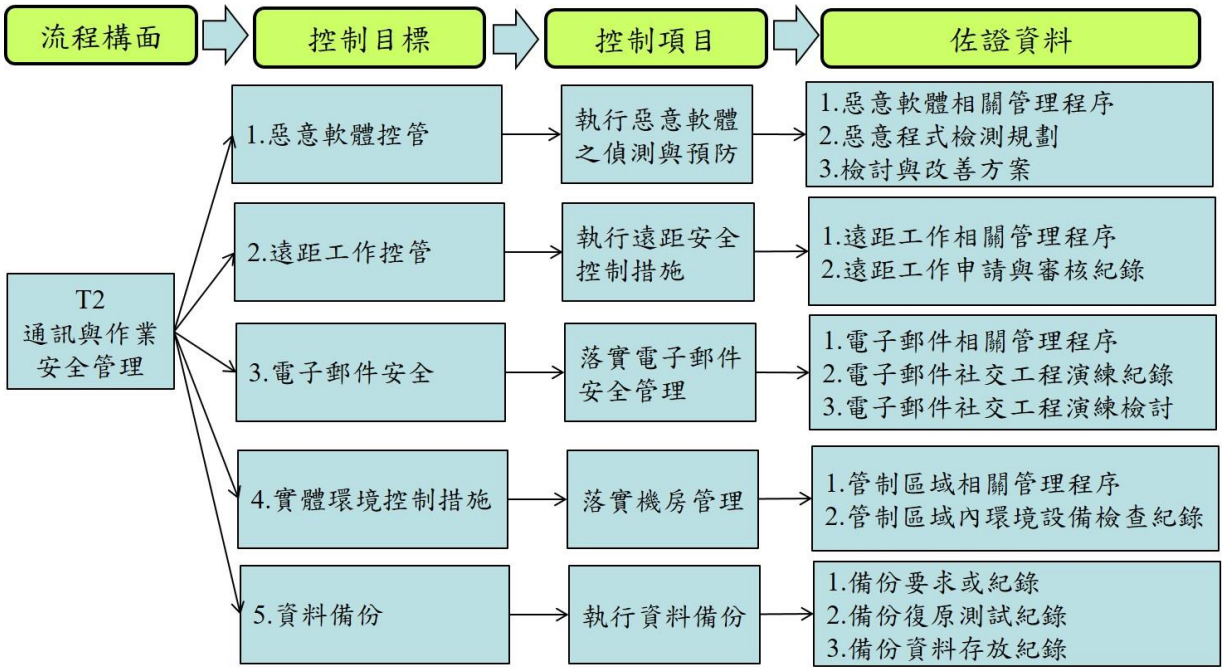
表3　流程構面目標範圍

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 ▪資安相關法規遵循 ▪資安組織與管理審查
	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 ▪委外資安稽核 ▪委外廠商資安管理
	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 ▪加密管理 ▪權限管理
	T2 通訊與作業安全管理	▪惡意軟體管理 ▪儲存媒體處置 ▪遠距工作管理 ▪資通安全監控 ▪電子郵件安全 ▪資通安全防護 ▪實體環境控制措施 ▪安全性檢測 ▪資料備份

面向	流程構面	目標範圍
	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

資料來源：本計畫整理

參考 CERT RMM 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，以 T2 通訊與作業安全管理為例，詳見圖 2。



資料來源：本計畫整理

圖2　流程構面之涵蓋要素

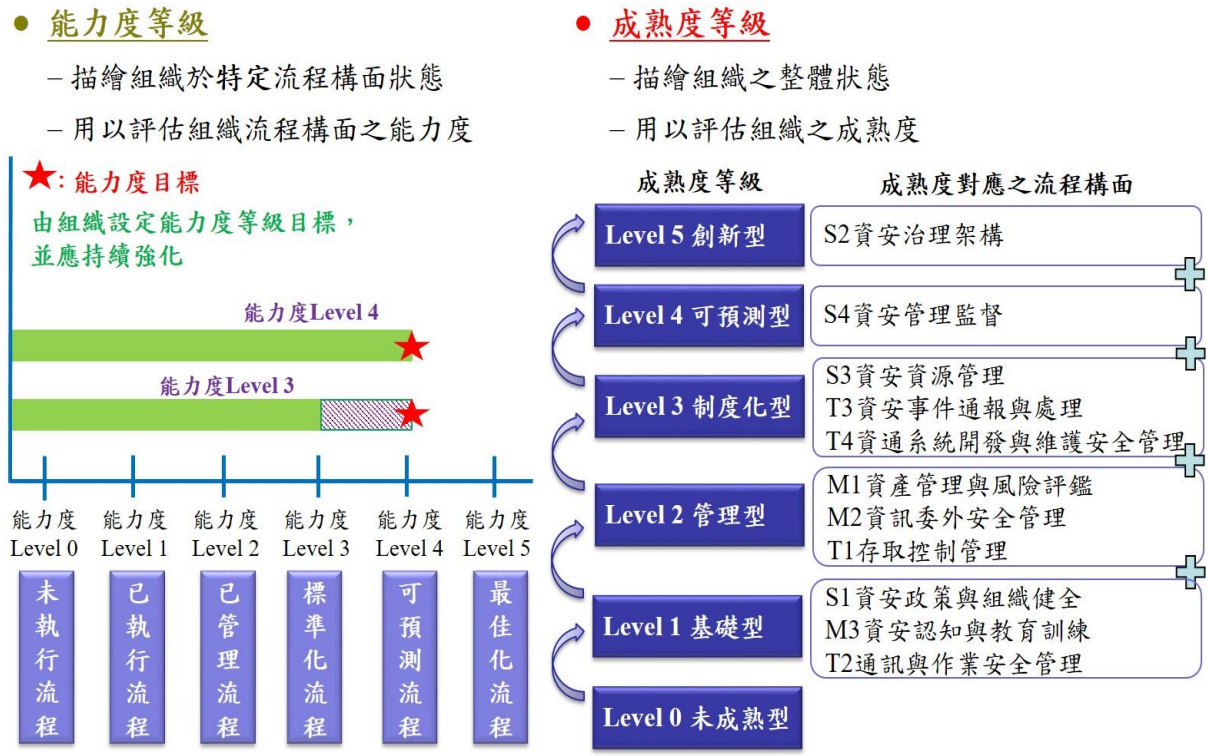
2.4 檢核項目設計重點

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、

ISO/IEC/CNS 27014、ISO/IEC/CNS 27001、CERT RMM、ISO/IEC 33004、ISO/IEC 33020 及 NIST Cyber Security Framework，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。

2.5 能力度與成熟度評估方法

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 與 ISO/IEC 33020 等。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，設計完整之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，詳見圖 3。



資料來源：本計畫整理

圖3　能力度與成熟度等級分級介紹

2.5.1 能力度等級分級定義

在能力度之設計，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 設計，將能力度等級由低至高分為 6 個級別，說明如下：

●Level 0 未執行流程(Unperformed Process)：組織未建立該流程或無法達成該流程。

●Level 1 已執行流程(Performed Process)：該流程之執行結果已達預先設定。

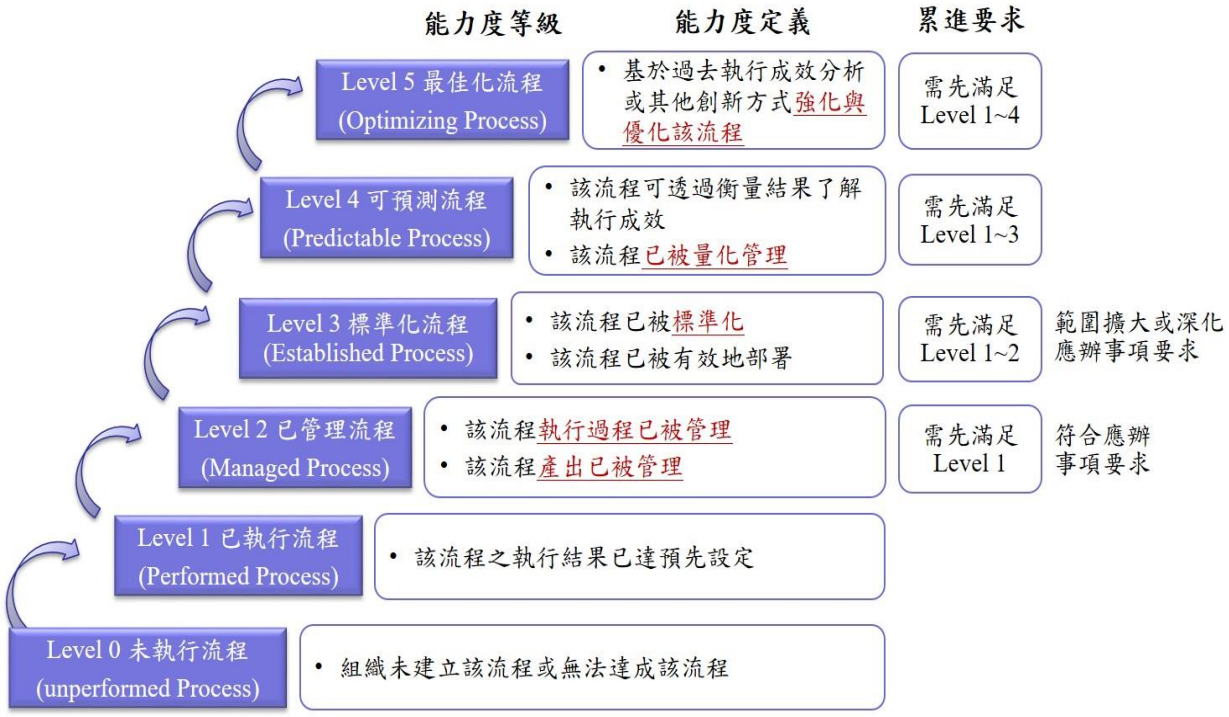
●Level 2 已管理流程(Managed Process)：該流程執行過程已被管理或該流程產出已被管理

●Level 3 標準化流程(Established Process)：該流程已被標準化或該流程已被有效地部署。

●Level 4 可預測流程(Predicatable Process)：該流程可透過衡量結果了解執行成效或該流程已被量化管理。

●Level 5 最佳化流程(Optimizing Process)：基於過去執行成效分析或其他創新方式強化與優化該流程。

能力度等級為累進制，欲達到能力度等級 2 需先滿足能力度等級 1 之要求；欲達到能力度等級 3 需先滿足能力度等級 1 與等級 2 之要求，以此類推。在資安治理成熟度檢核項目，部分檢核項目配分為 2 分之選項內容即為資通安全管理法應辦事項之要求，因此，機關如已完成應辦事項之要求，該檢核項目之能力度即已達等級 2；能力度等級 3 則為範圍擴大或深化應辦事項之要求，詳見圖 4。



資料來源：本計畫整理

圖4　能力度等級分級定義

2.5.2 成熟度等級分級定義

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 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 個級別，說明如下：

- Level 0 未成熟型(Immature)：組織尚未有效執行相關之基本流程。
- Level 1 基礎型(Basic)：相關流程構面執行結果已達成預先設定，且可支持組織之業務。
- Level 2 管理型(Managed)：相關流程構面已進行管理，包含規劃、執行及監督之過程。
- Level 3 制度化型(Established)：有效定義與部署標準化流程，使其成為常規作業。
- Level 4 可預測型(Predictable)：依組織目標定義流程量化指標，建立穩定、可預測之流程，蒐集與分析歷史數據，持續改善。
- Level 5 創新型(Innovating)：透過識別創新應用、技術、新機會或潛在風險優化各流程構面。

成熟度等級亦為累進制，成熟度等級 0 表示成熟度等級 1 之任一流程構面(S1 資安政策與組織健全、M3 資安認知與教育訓練或 T2 通訊與作業安全管理)能力度等級為 0。欲達到成熟度等級 1，需滿足成熟度等級 1 對應之所有流程構面皆為能力度等級 1；欲達到成熟度等級 2，需滿足成熟度等級 1 與等級 2 對應之所有流程構面皆為能力度等級 2，以此類推。成熟度等級、成熟度定義及其累進要求，詳見圖 5。

資料來源：本計畫整理

圖5　成熟度等級分級定義

2.5.3 流程構面分級設計原則

成熟度評估之分級設計考量分為 2 類，包含基礎流程(Basic process set)與擴展流程(Extended process set)。

基礎流程為資安治理之基本流程構面，包含成熟度等級 1 與等級 2。其中，成熟度等級 1 對應 3 個流程構面，分別為 S1 資安政策與組織健全、M3 資安認知與教育訓練及 T2 通訊與作業安全管理；成熟度等級 2 對應 3 個流程構面，分別為 M1 資產管理與風險評鑑、M2 資訊委外安全管理及 T1 存取控制管理。擴展流程為強化、優化資安治理之延伸流程構面，包含成熟度等級 3 至等級 5。其中，成熟度等級 3 對應 3 個流程構面，分別為 S3 資安資源管理、T3 資安事件通報與處理及 T4 資通系統開發與維護安全

管理；成熟度等級 4 對應 1 個流程構面，為 S4 資安管理監督；成熟度等級 5 對應 1 個流程構面，為 S2 資安治理架構。成熟度評估模型之流程構面分級，詳見表 4。

表4　成熟度評估模型之流程構面分級

分級設計考量	成熟度等級	策略面	管理面	技術面
擴展流程	5	S2 資安治理架構		
	4	S4 資安管理監督		
	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
基礎流程	2		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
	1	S1 資安政策與組織健全	M3 資安認知與教育訓練	T2 通訊與作業安全管理

資料來源： 本計畫整理

2.5.4 成熟度等級、流程構面及檢核項目

由上一節得知成熟度等級 1 至等級 3，各包含 3 個流程構面，成熟面等級 4 與等級 5，各為 1 個流程構面。資安治理成熟度評估作業，共包含 41 個檢核項目，本小節介紹 11 個流程構面下，分別對應的檢核項目。

成熟度等級 1 包含 3 個流程構面，分別為 S1 資安政策與組織健全、M3 資安認知與教育訓練及 T2 通訊與作業安全管理。S1 包含 3 個檢核項目，題號為第 1~3 題；M3 包含 4 個檢核項目，題號為第 17~20 題；T2 包含 12 個檢核項目，題號為第 24~35 題。

成熟度等級 2 包含 3 個流程構面，分別為 M1 資產管理與風險評鑑、M2 資訊委外安全管理及 T1 存取控制管理。M1 包含 2 個檢核項目，題號為第 12~13 題；M2 包含 3 個檢核項目，題號為第 14~16 題；T1 包含 3 個檢核項目，題號為第 21~23 題。

成熟度等級 3 包含 3 個流程構面，分別為 S3 資安資源管理、T3 資安事件通報與處理及 T4 資通系統開發與維護安全管理。S3 包含 2 個檢核項目，題號為第 7~8 題；T3 包含 2 個檢核項目，題號為第 36~37 題；T4 包含 4 個檢核項目，題號為第 38~41 題。

成熟度等級 4 僅有 1 個流程構面為 S4 資安管理監督，包含 3 個檢核項目，題號為第 9~11 題。成熟度等級 5 亦僅有 1 個流程構面 S2 資安治理架構，包含 3 個檢核項目，題號為第 4~6 題。資安治理成熟度等級、流程構面及檢核項目之對應，詳如表 5。

表5　成熟度等級、流程構面及檢核項目對應表

成熟度等級	流程構面	檢核項目
5	S2 資安治理架構	4.納入資安新興議題於年度業務項目
		5.落實利害相關者溝通方式
		6.揭露重要資安資訊
4	S4 資安管理監督	9.執行資安內部稽核
		10.落實資安管理制度(ISMS)驗證
		11.訂定業務持續運作計畫與執行演練
3	S3 資安資源管理	7.規劃資安資源
		8.配置資安專職人員
	T3 資安事件通報與處理	36.執行資安事件通報應變
		37.保存資通系統與資安設備日誌紀錄
	T4 資通系統開發與維護安全管理	38. 執行資通系統開發之安全需求設計
		39.執行資通系統開發之安全性測試
		40.執行源碼安全管理
		41.區隔系統開發、測試及實作的環境與設備
2	M1 資產管理與風險評鑑	12.盤點資訊資產與執行風險評鑑
		13.執行資通系統分級與落實資安防護基準
	M2 資訊委外安全管理	14.評估委外廠商資安專業能力
		15.確保委外廠商資安管理
		16.確保委外廠商資安稽核
	T1 存取控制管理	21.落實網路安全管理
		22.管理資通系統權限

成熟度等級	流程構面	檢核項目
		23.落實機敏資訊之加密管理
1	S1 資安政策與組織健全	1.建立資安政策與標準作業程序
		2.具備資安推動組織與執行管理審查
		3.落實資安法令與規範
	M3 資安認知與教育訓練	17.資通安全專職人員應具備資安技能
		18.資訊人員、一般使用者及主管應具備資安認知且資訊人員應具備資安技能
		19.取得資安專業證照
		20.宣導資安政策與相關資安要求
	T2 通訊與作業安全管理	24.執行惡意軟體之偵測與預防
		25.執行遠距工作安全控制措施
		26.落實電子郵件安全管理
		27.落實機房管理
		28.執行資料備份
		29.執行儲存媒體之防護措施
		30.落實資通安全威脅偵測管理機制(SOC)
		31.落實資通安全防護
		32.執行政府組態基準
		33.執行資通安全健診
		34.執行網站安全弱點檢測
		35.執行系統滲透測試

資料來源：本計畫整理

2.5.5 資安治理成熟度等級計算方法

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，計算出整體成熟度等級。資安治理成熟度等級計算之 3 步驟說明如下，詳見圖 6。

●步驟 1：取得各檢核項目之得分

依各檢核項目之填答，取得選項分數 0~5 分或 N/A(不計分)。

●步驟 2：計算流程構面之能力度

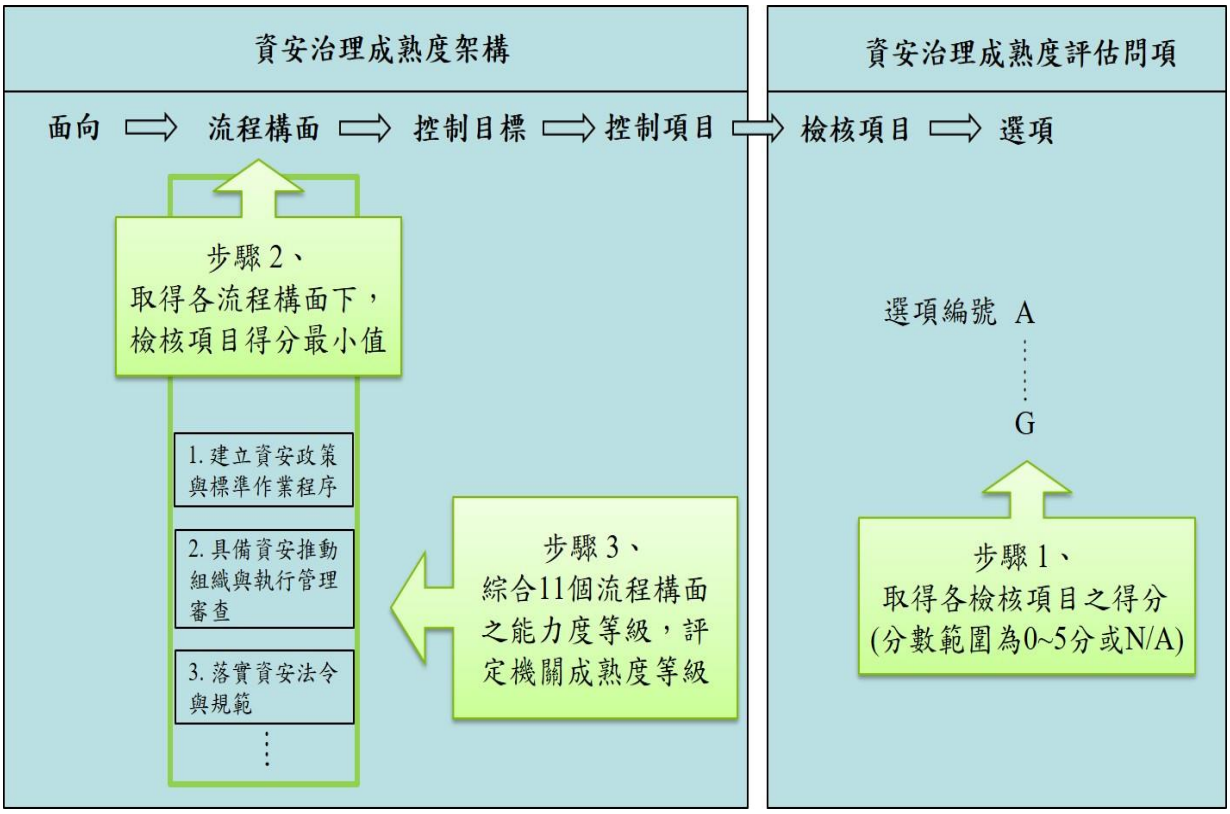
依據木桶理論，取流程構面下，檢核項目得分最小值，做為該流程面之能力度。

(註：木桶理論為一隻木桶盛水之多寡，不取決於桶壁上最長木塊或全部木板之平均長度，而是最短木板。在此意指組織之流程構面能力度，取決於該流程構面中最低分數，而非最高分數或平均分數)

●步驟 3：計算整體成熟度

檢視步驟 2 所計算出之各流程構面能力度，評定機關成熟度等級。

簡言之，資安治理成熟度評估機制之設計，先以各流程構面之檢核項目得分最低者為該流程構面之能力度，再依流程構面能力度之達成狀況，計算出整體成熟度等級。



資料來源：本計畫整理

圖6　資安治理成熟度等級計算方法

2.5.6 資安治理成熟度等級計算範例

為加強使用者對資安治理成熟度等級計算方法之理解，以下舉一範例做為說明，詳見圖 7。

流程構面分級原則	成熟度等級	流程構面名稱	流程構面能力度等級
擴展流程	5	S2資安治理架構	3
	4	S4資安管理監督	3
	3	S3資安資源管理	4
		T3資安事件通報與處理	5
		T4資通系統開發與維護安全管理	3
基礎流程	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
	1	S1資安政策與組織健全	4
		M3資安認知與教育訓練	4
		T2通訊與作業安全管理	3

資料來源：本計畫整理

圖7　資安治理成熟度等級計算範例

2.6 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。以下依不同角色說明其預期效益，詳見圖 8。

●資通安全署

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。

●上級機關

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。

●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陳報，提升機關首長與資安長對於資安防護工作之支持與重視。

資料來源：本計畫整理

圖8　預期效益

3. 資安治理成熟度評估檢核項目

本章節以策略面、管理面及技術面 3 大面向為子章節，在各子章節介紹其流程構面下之檢核項目與選項內容。每題皆為單選題，選項編號為 A 至 G，分別對應選項配分 0 至 5 分與不適用。以下說明各檢核項目選項配分共通性評分基準：

●0 分：完全未執行或未執行完成檢核項目。

●1 分：有執行檢核項目。

●2 分：檢核項目若為應辦事項之要求，完成應辦事項則可評為 2 分。檢核項目若非應辦事項之要求，已對檢核項目進行管理或定期檢視為評分基準。

●3 分：對檢核項目需具備標準作業程序或相關文件化要求，該文件之內容需清楚說明如何完成執行該檢核項目之步驟或流程，並落實執行。任一機關內部人員依據該文件執行檢核項目，皆能得到一致性之結果。該文件亦可列為檢核項目之佐證資料，供資安稽核員審視。請注意每一檢核項目之填寫說明欄位，部分檢核項目之選項配分達 3 分(含)以上，實施範圍應為全面實施。

●4 分：對檢核項目已訂定質化或量化衡量指標於標準作業程序或相關文件化要求，並落實執行。該衡量指標，應由機關內部共同開會討論獲得共識訂定之。

●5 分：對檢核項目之要求，具有優化或最佳化之執行方式。

●不適用：機關不曾發生檢核項目之內容或不允許執行檢核項目之內容。

3.1 策略面檢核項目說明

策略面包含 4 個流程構面，分別為 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，以下介紹 4 個流程構面之檢核項目。

3.1.1 S1 資安政策與組織健全之檢核項目說明

流程構面 S1 包含 3 個檢核項目，題號範圍為第 1 題至第 3 題，分別為「1.建立資安政策與標準作業程序」、「2.具備資安推動組織與執行管理審查」及「3.落實資安法令與規範」。

3.1.1.1 檢核項目第 1 題

第 1 題檢核項目為建立資安政策與標準作業程序，本題旨在期望機關建立資安政策與標準作業程序，以利推動全機關之資安政策。該檢核項目之選項內容與填寫說明，詳見表 6。

表6　1.建立資安政策與標準作業程序

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
1	建立資安政策與標準作業程序	A	未訂定資安政策	0	▪資通安全長：由機關首長指派副首長或適當人員兼任，負責推動與監督機關內資通安全相關事務(資通安全法第十一條) ▪利害相關者：係為會影響機關目標或被機關影響之團體或個人，意同ISO/IEC/CNS27001所述及之 Interested Parties(譯為「關注方」)，可能包含相關權責機關、IT服務供應商、民眾、其他各專家安全論壇或專業公協會等 ▪參考佐證資料 >資安政策等管理制度相關文件 >資安制度推動與維護相關會議紀錄
		B	已訂定資安政策，並經資通安全長或權責主管核准	1	
		C	針對已訂定之資安政策，定期檢討執行情形(如定期於資安專案會議或管審會議管理資安政策執行情形等)	2	
		D	依資安政策要求，已訂定相關標準作業程序或文件化要求，並落實執行	3	
		E	資安政策已具有質化或量化衡量指標(如可分為量化與質化型目標，量化型目標包含降低 10%資安事件發生比例、人員資安防護意識測驗平均達 95 分、減少 10%之社交工程測試點擊率；質化型目標含提升人員資安防護意識、建立全面之資安防護網、有效偵測與預防外部攻擊等)，並檢視執行成效	4	
		F	考量利害相關者需求與資安新興科技發展趨勢，精進資安政策或相關程序	5	

資料來源：本計畫整理

以下為檢核項目第 1 題之提醒事項，供自評人員參考。

- 選項配分為 2 分之佐證資料，可為資安專案會議或管理審查會議之會議紀錄，供資安稽核員審查。
- 選項配分為 3 分之佐證資料，可為機關之資通安全維護計畫或 ISMS 文件。

3.1.1.2 檢核項目第 2 題

第 2 題檢核項目為具備資安推動組織與執行管理審查，本題旨在期望機關具備資安推動組織與執行管理審查，以確保資通安全相關措施支援施政目標。該檢核項目之選項內容與填寫說明，詳見表 7。

表7　2.具備資安推動組織與執行管理審查

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
2	具備資安推動組織與執行管理審查	A	未具備資安推動組織與執行管理審查	0	▪資安推動組織：為推動資通安全功能之組織，訂定相關組織架構及職掌，包含資通安全長、資安通報人員、資安聯絡人員等負責資安業務之人員 ▪評估、指導、監督(EDM)作業：係指組織透過對資訊安全工作推動之成果監測，評估該成果是否足以支持組織目標，並由管理階層審視評估結果、下達決策，以執行資訊安全推動工作應達成之成果及改善方向之循環
		B	已具備資安推動組織與執行管理審查	1	
		C	資安推動組織由資通安全長或指派人員擔任管理階層，定期召開管理審查會議，檢視資通安全推動情形	2	
		D	資安推動組織與執行管理審查會議已訂定標準作業程序或相關文件化要求，並落實執行	3	

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
		E	資安推動組織與管理審查會議已包含各單位主管	4	▪審查議題應至少涵蓋： (a)過往管理審查之議案之處理狀態 (b)與資訊安全管理系統有關之內部及外部議題之變更 (c)資訊安全績效之回饋，包括下列之趨勢： (1)不符合項目及矯正措施 (2)監督及量測結果 (3)稽核結果 (4)資訊安全目標之達成 (d)利害相關者之回饋 (e)風險評鑑結果及風險處理計畫之狀態 (f)持續改善之機會 ▪參考佐證資料 >資安組織圖與職掌說明 >資安管理審查會議相關要求或規定 >管理審查會議紀錄及後續追蹤執行情形
		F	落實評估、指導、監督(EDM)作業，確保資通安全相關措施支援施政目標，指導資安策略與計畫方向，並監控資安目標達成狀況	5	

資料來源：本計畫整理

以下為檢核項目第 2 題之提醒事項，供自評人員參考。

- 選項配分為 1 分之佐證資料，可為資安組織與職掌說明。
- 選項配分為 2 分之佐證資料，可為資安專案會議或管理審查會議之會議紀錄與後續追蹤執行情形，供資安稽核員審查。
- 選項配分為 3 分之佐證資料，可為機關之資通安全維護計畫或 ISMS 文件。

3.1.1.3 檢核項目第 3 題

第 3 題檢核項目為落實資安法令與規範，本題旨在期望機關關注我國資通安全相關政策、法令及規範等，並提出因應措施，以強化機關資安防護能力。若機關已針對我國資通安全相關政策、法令及規範等，提出因應措施，請填選項 B。機關如已針對我國資通安全相關政策、法令及規範我國資通安全相關政策、法令及規範等相關因應措施，定期檢討執行情形(如定期檢討資安法令與規範之盤點、執行及後續規範修正作業等)，則填選項 C。若該因應措施已納入標準作業程序或相關文件化要求，並落實執行，請填選項 D。

機關如已依據我國資通安全相關政策、法令及規範我國資通安全相關政策、法令及規範之因應措施，訂定質化或量化衡量指標(如每年至少檢視 1 次資安相關規範與法令之符合情形、資通安全政策、法令或規範頒布或更新時，於 3 個月內完成相關規範之修正等)，並檢視執行成效，請填選項 E。若機關已針對國內外新興資通安全相關政策、法令及規範，精進資安政策或相關程序，請填選項 F。完整選項內容與填寫說明，詳見表 8。

表8　3.落實資安法令與規範

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
3	落實資安法令與規範	A	未針對我國資通安全相關政策、法令及規範等，提出因應措施	0	▪參考佐證資料 >個人資料保護法相關規範文件 >制度文件審查與修訂紀錄
		B	針對我國資通安全相關政策、法令及規範等，提出因應措施	1	
		C	針對我國資通安全相關政策、法令及規範我國資通安全相關政策、法令及規範等相關因應措施，定期檢討執行情形(如定期檢討資安法令與規範之盤點、執行及後續規範修正作業等)	2	
		D	針對因應措施，已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	依據我國資通安全相關政策、法令及規範我國資通安全相關政策、法令及規範之因應措施，訂定質化或量化衡量指標(如每年至少檢視1次資安相關規範與法令之符合情形、資通安全政策、法令或規範頒布或更新時，於3個月內完成相關規範之修正等)，並檢視執行成效	4	
		F	針對國內外新興資通安全相關政策、法令及規範，精進資安政策或相關程序	5	

資料來源：本計畫整理

3.1.2 S2 資安治理架構之檢核項目說明

流程構面 S2 包含 3 個檢核項目，題號範圍為第 4 題至第 6 題，分別為「4.納入資安新興議題於年度業務項目」、「5.落實利害相關者溝通方式」及「6.揭露重要資安資訊」。

第 4 題檢核項目為納入資安新興議題於年度業務項目，該資安新興議題係指針對機關業務近 3 年所涉及之新興科技應用所衍生資安威脅與風險。本檢核項目之目的為希望於年度開始時，各業務組、資安人員及內部相關權責主管共同開會，討論該年度業務項目是否涉及資安新興議題與規劃其因應措施，若機關之年度業務項目已將資安新興議題納入考量，有納入考量即可填選項 B，其佐證資料可為會議紀錄或足以證明納入考量之文件。

若機關針對納入考量之資安新興議題之年度業務項目，有規劃與執行因應措施，避免遭受資安威脅與風險，請填選項 C，其佐證資料可為執行紀錄或足以證明規劃與已執行因應措施之文件。

機關內部如已將因應措施納入資安標準作業程序或於相關文件記載，使執行結果達一致性並落實執行，請填選項 D，其佐證資料可為標準作業程序或相關文件。如於管審會議或由資安長與機關內部相關權責主管參與之會議，檢視因應措施已符合年度業務項目之要求，請填選項 E，其佐證資料可為會議紀錄或足以證明因應措施已符合年度業務項目要求之文件。機關如已依據國際資安趨勢與內外部資安新興議題，召集內部相關權責主管與人員開會討論，使因應措施有更佳執行方式，請填選項 F，其佐證資料可為會議紀錄或足以證明因應措施已有精進流程之文件。完整選項內容與填寫說明，詳見表 9。

表9　4.納入資安新興議題於年度業務項目

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
4	納入資安新興議題於年度業務項目	A	年度業務項目未將資安新興議題納入考量	0	▪資安新興議題：針對機關業務近3年所涉及之新興科技應用所衍生資安威脅與風險 ▪參考佐證資料 >年度業務項目 >年度業務項目相關檢討會議紀錄
		B	年度業務項目已將資安新興議題納入考量	1	
		C	針對納入考量之資安新興議題之年度業務項目，規劃執行因應措施	2	
		D	因應措施已納入資安標準作業程序或相關文件化要求	3	
		E	檢視因應措施已符合年度業務項目之要求	4	
		F	依據國際資安趨勢與內外部資安議題，精進年度業務項目之資安新興議題	5	

資料來源：本計畫整理

第 5 題檢核項目為落實利害相關者溝通方式，該利害相關者包含機關內部與外部相關權責機關或其他利害相關者(如 IT 服務供應商、民眾、其他各專家)。若機關已規劃利害相關者識別、溝通或報告等相關活動，請填選項 B。機關如已針對利害相關者識別、溝通或報告等相關活動，定期檢討執行情形(如定期檢視利害相關者識別與溝通執行方式等)，請填選項 C。

若機關已對利害相關者溝通訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D，該利害相關者相關文件化要求，包含利害相關者清單、利害相關者溝通與頻率列表。若該標準作業程序或相關文件，已具有質化或量化衡量指標(如利害相關者之溝通與回饋比率等)，並檢視執行成效，請填選項 E。機關如已針對利害相關者溝通，精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 10。

表10 5.落實利害相關者溝通方式

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
5	落實利害相關者溝通方式	A	未規劃利害相關者識別、溝通或報告等相關活動	0	▪利害相關者：包含機關內部與外部相關權責機關或其他利害相關者(如 IT 服務供應商、民眾、其他各專家) ▪利害相關者相關文件化要求：包含利害相關者清單、利害相關者溝通與頻率列表 ▪參考佐證資料 >利害相關者或溝通窗口名單 >利害相關者溝通管理文件
		B	已規劃利害相關者識別、溝通或報告等相關活動	1	
		C	針對利害相關者識別、溝通或報告等相關活動，定期檢討執行情形(如定期檢視利害相關者識別與溝通執行方式等)	2	
		D	利害相關者溝通，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	利害相關者溝通已具有質化或量化衡量指標(如利害相關者之溝通與回饋比率等)，並檢視執行成效	4	
		F	針對利害相關者溝通，精進流程或執行方式	5	

資料來源：本計畫整理

第 6 題檢核項目為揭露重要資安資訊，本題與第 5 題具有關聯性，因主管或上級機關為機關內部相關權責機關。機關如已對主管或上級機關揭露重要資安資訊(至少包含資通安全維護計畫實施情形及三與四級資安事件與改善報告等)，請填選項 B。若機關已針對揭露重要資安資訊，了解主管或上級機關之指示並檢視執行情形，請填選項 C。

機關如已針對揭露重要資安資訊訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已具有質化或量化衡量指標(如主管或上級機關之溝通與回饋比率等)並檢視執行成效，請填選項 E。機關如已針對主管或上級機關溝通或揭露重要資安資訊，精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 11。

表11 6.揭露重要資安資訊

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
6	揭露重要資安資訊	A	未對主管或上級機關揭露重要資安資訊	0	▪重要資安資訊：如 >資通安全維護計畫實施情形 >三與四級資安事件與改善報告 >未遵循資安管理法或個人資料保護法 ▪參考佐證資料 >會議紀錄 >資通安全維護計畫實施情形
		B	已對主管或上級機關揭露重要資安資訊(至少包含資通安全維護計畫實施情形及三與四級資安事件與改善報告等)	1	
		C	針對揭露重要資安資訊，了解主管或上級機關之指示，並檢視執行情形	2	
		D	針對揭露重要資安資訊，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	揭露重要資安資訊已具有質化或量化衡量指標(如主管或上級機關之溝通與回饋比率等)，並檢視執行成效	4	
		F	針對主管或上級機關溝通或揭露重要資安資訊，精進流程或執行方式	5	

資料來源：本計畫整理

3.1.3 S3 資安資源管理之檢核項目說明

流程構面 S3 包含 2 個檢核項目，題號範圍為第 7 題至第 8 題，分別為「7.規劃資安資源」與「8.配置資安專職人員」。

第 7 題檢核項目為規劃資安資源，本題旨在讓機關與其主管或上級機關了解機關資安資源之規劃與運用狀況是否匱乏。機關如已針對資安目標與風險需求，規劃資安所需經費或資源(係指投入於資安之人力、物力及財力)，請填選項 B。若針對資安資源編列，定期檢討執行情形(如定期規劃與審核資安人力與經費需求、資安資源需達到機關對應資安等級所需防護設備資源要求、資安資源提供最少需符合可接受風險等級要求等)，請填選項 C。

若機關已針對資安資源規劃、運用狀況監督與追蹤流程訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已具有質化或量化衡量指標(如資安預算編列為資訊預算 10%等)，並檢視執行成效，請填選項 E。若機關對資安資源規劃，已具有精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 12。

表12 7.規劃資安資源

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
7	規劃資安資源	A	未針對資安目標與風險需求，規劃資安所需經費或資源	0	▪參考佐證資料 >資安需求評估紀錄 >年度預算規劃計畫 >資安預算申請紀錄 >年度預算審核紀錄
		B	已針對資安目標與風險需求，規劃資安所需經費或資源(係指投入於資安之人力、物力及財力)	1	
		C	針對資安資源編列，定期檢討執行情形(如定期規劃與審核資安人力與經費需求、資安資源需達到機關對應資安等級所需防護設備資源要求、資安資源提供最少需符合可接受風險等級要求等)	2	
		D	資安資源規劃、運用狀況監督與追蹤流程已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	資安資源已具有質化或量化衡量指標(如資安預算編列為資訊預算 10%等)，並檢視執行成效	4	
		F	針對資安資源規劃，精進流程或執行方式	5	

資料來源：本計畫整理

第 8 題檢核項目為配置資安專職人員，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關資安專職人員已達該應辦事項項目之要求，並檢討執行情形，請填選項 C。若機關針對資安專職人力投入，已納入標準作業程序或相關文件化要求並落實執行，請填選項 D。

若該標準作業程序或相關文件，已訂定資安專職人員質化或量化衡量指標(如資安專職人員數量、資安專職人員與機關內人員比例或專責資安單位配置等)，且至少指派資安專職人員 2 人，請填選項 E。若機關已具備資安專責單位，由於所有檢核項目之計分方式為累進要求，因此請先確認已完成選項 A 至 E 之要求事項，再填選項 F。完整選項內容與填寫說明，詳見表 13。

表13 8.配置資安專職人員

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
8	配置資安專職人員	A	未投入資安專職人員	0	▪A 級機關：初次受核定或等級變更後之 1 年內，配置 4 人；須以專職人員配置之 ▪B 級機關：初次受核定或等級變更後之 4 年內，配置 2 人；須以專職人員配置之 ▪專職人員：指應全職執行資通安全業務者(資通安全責任等級分級辦法附表一/附表三) ▪參考佐證資料 >資安專(兼)職成員名單(應含成員之所屬單位) >職務說明書
		B	已投入資安專職人員	1	
		C	▪A 級機關：配置資安專職人員 4 人，並檢討執行情形 ▪B 級機關：配置資安專職人員 2 人，並檢討執行情形	2	
		D	針對資安專職人員投入，已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資安專職人員質化或量化衡量指標(如資安專職人員數量、資安專職人員與機關內人員比例或專責資安單位配置等)，且至少指派資安專職人員 2 人	4	
		F	具備資安專責單位	5	

資料來源：本計畫整理

3.1.4 S4 資安管理監督之檢核項目說明

流程構面 S4 包含 3 個檢核項目，題號範圍為第 9 題至第 11 題，分別為「9.執行資安內部稽核」、「10.落實資安管理制度(ISMS)驗證」及「11.訂定業務持續運作計畫與執行演練」。

第 9 題檢核項目為執行資安內部稽核，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已完成該應辦事項項目之要求，並檢討執行情形，請填選項 C。機關如已針對內部稽核相關要求訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已具有質化或量化衡量指標(如每年至少辦理 2 次內稽或於內稽活動結束後 3 個月內完成所有改善措施等)，並檢視執行成效，請填選項 E。若機關已考量資安趨勢、議題與內部稽核發現事項等分析結果，精進資安內稽程序、目標或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 14。

表14 9.執行資安內部稽核

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
9	執行資安內部稽核	A	未執行資安內部稽核	0	▪A 級機關：每年辦理 2 次內部資通安全稽核 ▪B 級機關：每年辦理 1 次內部資通安全稽核 ▪參考佐證資料 >資安內部稽核程序與計畫 >資安內部稽核紀錄
		B	已執行資安內部稽核	1	
		C	A 級機關：每年辦理 2 次資安內稽，並檢討執行情形 B 級機關：每年辦理 1 次資安內稽，並檢討執行情形	2	
		D	內部稽核相關要求，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	資安內稽已具有質化或量化衡量指標(如每年至少辦理 2 次內稽或於內稽活動結束後 3 個月內完成所有改善措施等)，並檢視執行成效	4	
		F	考量資安趨勢、議題與內部稽核發現事項等分析結果，精進資安內稽程序、目標或執行方式	5	

資料來源：本計畫整理

第 10 題檢核項目為落實資安管理制度(ISMS)驗證，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。機關如已規劃或推動 ISMS 導入，請填選項 B。若機關已通過 ISMS 第三方驗證，並維持其有效性，請填選項 C。若機關全部核心資通系統已完成 ISMS 導入，並通過 ISMS 第三方驗證，請填選項 D。機關若已將非核心資通系統或業務與行政單位納入 ISMS 範圍，並通過 ISMS 第三方驗證，請填選項 E。如已全機關導入 ISMS 第三方驗證，請填選項 F。完整選項內容與填寫說明，詳見表 15。

表15 10.落實資安管理制度(ISMS)驗證

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
10	落實資安管理制度(ISMS)驗證	A	未規劃或推動 ISMS 導入	0	▪ A/B 級機關：初次受核定或等級變更後之 2 年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、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 3 年內完成公正第三方驗證，並持續維持其驗證有效性 ▪ 「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構(資通安全責任等級分級辦法) ▪ 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統(資通安全管理法第三條) ▪ 資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核
		B	已規劃或推動 ISMS 導入	1	
		C	通過 ISMS 第三方驗證，並維持其有效性	2	
		D	全部核心資通系統完成 ISMS 導入，並通過 ISMS	3	

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
			第三方驗證		心資通系統(資通安全責任等級分級辦法) ▪核心資通系統：指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者(資通安全管理法施行細則第七條) ▪核心業務：係指公務機關依其組織法規，足認該業務為機關核心權責所在，或各機關維運、提供關鍵基礎設施所必要之業務(資通安全管理法施行細則第七條) ▪參考佐證資料 >ISMS 導入規劃 >ISMS 驗證規劃/計畫 >ISMS 外部稽核報告 >驗證範圍擴大評估報告
		E	將非核心資通系統或業務與行政單位納入 ISMS 範圍，並通過 ISMS 第三方驗證	4	
		F	全機關導入 ISMS 第三方驗證	5	

資料來源：本計畫整理

第 11 題檢核項目為訂定業務持續運作計畫與執行演練，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已完成該應辦事項之要求，並檢討執行情形，請填選項 C。若機關之業務持續運作相關要求，已納入標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已具有質化或量化衡量指標(如每 2 年完成 1 次所有核心系統持續運作演練、每年至少執行 1 次營運衝擊分析、每年至少檢視 1 次系統復原時間目標與資料復原時間點目標、完成緊急應變計畫與業務復原計畫等)，並檢視執行成效，請填選項 E。若機關已針對業務持續運作，精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 16。

表16 11.訂定業務持續運作計畫與執行演練

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
11	訂定業務持續運作計畫與執行演練	A	未執行業務持續運作	0	▪A 級機關：全部核心資通系統每年辦理 1 次業務持續運作演練 ▪B 級機關：全部核心資通系統每 2 年辦理 1 次業務持續運作演練 ▪核心資通系統：指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者(資通安全管理法施行細則第七條) ▪系統復原時間目標(RTO)：資通系統於發生中斷事件後，至恢復運作之目標時間 ▪資料復原時間點目標(RPO)：資通系統發生中斷事件後，資料需恢復之時間點 ▪參考佐證資料 >業務持續運作管理程序、計畫或手冊 >業務持續運作演練紀錄 >核心資通系統備援規劃與紀錄
		B	已執行業務持續運作	1	
		C	A 級機關：全部核心資通系統每年辦理 1 次持續運作演練，並檢討執行情形 B 級機關：全部核心資通系統每 2 年辦理 1 次持續運作演練，並檢討執行情形	2	
		D	業務持續運作相關要求，已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	業務持續運作已具有質化或量化衡量指標(如每 2 年完成 1 次所有核心系統持續運作演練、每年至少執行 1 次營運衝擊分析、每年至少檢視 1 次系統復原時間目標與資料復原時間點目標、完成緊急應變計畫與業務復原計畫等)，並檢視執行成效	4	
		F	針對業務持續運作，精進流程或執行方式	5	

資料來源：本計畫整理

3.2 管理面檢核項目說明

管理面包含 3 個流程構面，分別為 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，以下介紹 3 個流程構面之檢核項目。

3.2.1 M1 資產管理與風險評鑑之檢核項目說明

流程構面 M1 包含 2 個檢核項目，題號範圍為第 12 題至第 13 題，分別為「12.盤點資訊資產與執行風險評鑑」與「13.執行資通系統分級與落實資安防護基準」。

第 12 題檢核項目為盤點資訊資產與執行風險評鑑，機關如已盤點資訊資產，至少包含軟體、硬體(實體設備)及人員等，請填選項 B。若機關已執行資安風險評鑑，並定期檢討執行情形(如定期依據資安風險評鑑結果，執行相關資安防護措施等)，請填選項 C。

機關如已訂定資安風險評鑑相關之標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已具有質化或量化衡量指標(如每年至少檢視 1 次可接受風險準則妥適性等)，並檢視執行成效，請填選項 E。若機關透過新興威脅或弱點分析，重新進行風險評鑑；或針對風險評鑑方式，提出精進作為，請填選項 F。完整選項內容與填寫說明，詳見表 17。

表17 12.盤點資訊資產與執行風險評鑑

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
12	盤點資訊資產與執行風險評鑑	A	未盤點資訊資產	0	▪風險評鑑：風險分析及風險評鑑之整個過程，根據已定之風險準則將預估之風險進行比較，用以決定風險顯著性 ▪參考佐證資料 >資訊資產清冊、更新紀錄 >資訊安全風險列表 >風險管理程序 >風險評鑑紀錄與處理計畫
		B	已盤點資訊資產，至少包含軟體、硬體(實體設備)及人員等	1	
		C	已執行資安風險評鑑，並定期檢討執行情形(如定期依據資安風險評鑑結果，執行相關資安防護措施等)	2	
		D	已訂定資安風險評鑑相關之標準作業程序或相關文件化要求，並落實執行	3	
		E	資安風險評鑑已具有質化或量化衡量指標(如每年至少檢視1次可接受風險準則妥適性等)，並檢視執行成效	4	
		F	透過新興威脅或弱點分析，重新進行風險評鑑；或針對風險評鑑方式，提出精進作為	5	

資料來源：本計畫整理

第 13 題檢核項目為執行資通系統分級與落實資安防護基準，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已盤點資通系統(指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統)，並列出清冊，請填選項 B。若機關已完成應辦事項之要求，並檢討執行情形，請填選項 C。

機關之資通系統資安防護基準如已納入現有之標準作業程序，並落實執行，請填選項 D。若該標準作業程序或相關文件，已具有質化或量化衡量指標(如每年至少檢視 1 次資通系統分級及防護基準，且針對檢視不符情形，執行改善追蹤等)，並檢視執行成效，請填選項 E。若機關針對資通系統分級及防護基準，已具有精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 18。

表18 13.執行資通系統分級與落實資安防護基準

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
13	執行資通系統分級與落實資安防護基準	A	未盤點資通系統	0	▪A/B 級機關：初次受核定或等級變更後 1 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；其後應檢視資通系統分級妥適性 ▪參考佐證資料 >資通系統清冊/分級結果 >防護基準檢視紀錄 >追蹤改善紀錄
		B	已盤點資通系統(指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統)，並列出清冊	1	
		C	完成資通系統分級及防護基準，並檢討執行情形	2	
		D	資通系統資安防護基準已納入現有之標準作業程序，並落實執行	3	
		E	資通系統分級及防護基準已具有質化或量化衡量指標(如每年至少檢視 1 次資通系統分級及防護基準，且針對檢視不符情形，執行改善追蹤等)，並檢視執行成效	4	
		F	針對資通系統分級及防護基準，精進流程或執行方式	5	

資料來源：本計畫整理

3.2.2 M2 資訊委外安全管理之檢核項目說明

流程構面 M2 包含 3 個檢核項目，題號範圍為第 14 題至第 16 題，分別為「14.評估委外廠商資安專業能力」、「15.確保委外廠商資安管理」及「16.確保委外廠商資安稽核」。該流程構面之委外廠商，係指契約期間包含本年度之資安業務相關委外廠商，非限本年度新簽約之資安業務相關委外廠商。

第 14 題檢核項目為評估委外廠商資安專業能力，若機關於委外辦理資通系統之建置、維運或資通服務之提供，已要求委外廠商之資安專業資格或能力，包含服務品質能力(如專案價格、交付品質與時效、履約能力等)、資安專業技術能力(如鑑識能力、SOC 監控能力、弱點掃描能力等)、專案管理能力(如專案人力、專業證照、國際認證、具備 SOP 等)、廠商本身能力(如專案實績等)，請填選項 B。若機關針對委外廠商之資安專業資格或能力、資安專業技術能力、專案管理能力、廠商本身能力有管理做法或機制，並檢討執行情形，請填選項 C。

機關如已訂定委外作業程序包含資安要求並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定委外廠商之資安專業資格或能力質化或量化衡量指標(如委外廠商需具備執行資安專案經驗，執行專案成員需具備資安專業證照及委外廠商執行之滿意度調查需達 80%等)，並檢視執行成效，請填選項 E。若機關針對委外廠商之資安專業資格或能力之評估，已具精進流程或執行方式，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含所有委外廠商。完整選項內容與填寫說明，詳見表 19。

表19 14.評估委外廠商資安專業能力

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
14	評估委外廠商資安專業能力	A	於委外辦理資通系統之建置、維運或資通服務之提供，未要求委外廠商之資安專業資格或能力	0	▪選項配分達3分(含)以上者，實施範圍應包含所有委外廠商 ▪參考佐證資料 >委外服務建議書 >委外廠商評鑑結果 >委外廠商改善與追蹤紀錄
		B	已要求委外廠商之資安專業資格或能力，包含服務品質能力(專案價格、交付品質與時效、履約能力等)、資安專業技術能力(如：鑑識能力、SOC監控能力、弱點掃描能力等)、專案管理能力(如：專案人力、專業證照、國際認證、具備SOP等)、廠商本身能力(如：專案實績等)	1	
		C	針對委外廠商之資安專業資格或能力、資安專業技術能力、專案管理能力、廠商本身能力有管理做法或機制，並檢討執行情形	2	
		D	已訂定委外作業程序包含資安要求，並落實執行	3	
		E	已訂定委外廠商之資安專業資格或能力質化或量化衡量指標(如委外廠商需具備執行資安專案經驗，執行專案成員需具備資安專業證照及委外廠商執行之滿意度調查需達80%等)，並檢視執行成效	4	
		F	針對委外廠商之資安專業資格或能力之評估，精進流程或執行方式	5	

資料來源：本計畫整理

第 15 題檢核項目為確保委外廠商資安管理，若機關已於委外文件納入資安防護要求(如保密協議、設備攜出/入規定、契約履約或終止後要求廠商刪除或返還資料、要求廠商於發生資安事件時，必須通報機關並執行相關配合辦理，軟體交付前必須完成資安檢測作業、實施供應商資訊安全教育訓練、個人資料處理保護要求等)，請填選項 B。若機關針對委外資安防護要求(如於委外專案會議，檢視資安管理要求達成情形，並執行後續改善追蹤事宜等)有管理做法或機制，並檢討執行情形，請填選項 C。

機關如已將委外資安管理要求訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定委外資安管理質化或量化衡量指標(如委外廠商需提出書面資料，確認委外管理要求已落實等)，並檢視執行成效，請填選項 E。若機關針對委外資安控管，已具精進流程或執行方式，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含所有委外項目。完整選項內容與填寫說明，詳見表 20。

表20 15.確保委外廠商資安管理

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
15	確保委外廠商資安管理	A	未於委外文件納入資安防護要求	0	▪委外文件：包含委外服務建議書、委外契約及委外作業程序等 ▪選項配分達3分(含)以上者，實施範圍應包含所有委外項目 ▪參考佐證資料 >委外廠商之資安管理要求 >事件通報紀錄 >刪除或返還資料紀錄
		B	已於委外文件納入資安防護要求(如保密協議、設備攜出/入規定、契約履約或終止後要求廠商刪除或返還資料、要求廠商於發生資安事件時，必須通報機關並執行相關配合辦理，軟體交付前必須完成資安檢測作業、實施供應商資訊安全教育訓練、個人資料處理保護要求等)	1	
		C	針對委外資安防護要求(如於委外專案會議，檢視資安管理要求達成情形，並執行後續改善追蹤事宜等)有管理做法或機制，並檢討執行情形	2	
		D	委外資安管理要求，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定委外資安管理質化或量化衡量指標(如委外廠商需提出書面資料，確認委外管理要求已落實等)，並檢視執行成效	4	
		F	針對委外資安控管，精進流程或執行方式	5	

資料來源：本計畫整理

第 16 題檢核項目為確保委外廠商資安稽核，若機關已進行委外廠商之資安稽核(至少包含書面或實地稽核等)，請填選項 B。機關如已針對委外資安稽核作業(如已規劃委外資安稽核時程、項目並執行後續改善追蹤事宜等)有管理做法或機制，並檢討執行情形，請填選項 C。

若機關已將委外資安稽核要求訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定委外資安稽核質化或量化衡量指標(如每年至少執行 1 次委外廠商稽核作業、委外查核未符合事項，需於 3 個月內完成改善作業等)，並檢視執行成效，請填選項 E。機關如針對委外資安稽核，已具精進流程或執行方式，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含所有委外項目。完整選項內容與填寫說明，詳見表 21。

表21 16.確保委外廠商資安稽核

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
16	確保委外廠商資安稽核	A	未進行委外廠商之資安稽核	0	▪選項配分達3分(含)以上者，實施範圍應包含所有委外項目 ▪參考佐證資料 >委外廠商稽核計畫 >委外廠商資安稽核結果 >委外廠商改善與追蹤紀錄
		B	已進行委外廠商之資安稽核(至少包含書面或實地稽核等)	1	
		C	針對委外資安稽核作業(如已規劃委外資安稽核時程、項目並執行後續改善追蹤事宜等)有管理做法或機制，並檢討執行情形	2	
		D	委外資安稽核要求，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定委外資安稽核質化或量化衡量指標(如每年至少執行1次委外廠商稽核作業、委外查核未符合事項，需於3個月內完成改善作業等)，並檢視執行成效	4	
		F	針對委外資安稽核，精進流程或執行方式	5	

資料來源：本計畫整理

3.2.3 M3 資安認知與教育訓練之檢核項目說明

流程構面 M3 包含 4 個檢核項目，題號範圍為第 17 題至第 20 題，分別為「17.資通安全專職人員應具備資安技能」、「18.資訊人員、一般使用者及主管應具備資安認知且資訊人員應具備資安技能」、「19.取得資安專業證照」及「20.宣導資安政策與相關資安要求」。

第 17 題檢核項目為使資通安全專職人員應具備資安技能，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已完成該應辦事項之要求，請填選項 C。若機關之資通安全專職人員訓練要求已納入標準作業程序或相關文件化要求，並落實執行，請填選項 D。機關如已於標準作業程序或相關文件，訂定資通安全專職人員訓練質化或量化衡量指標(如教育訓練評量結果整體通過率、教育訓練出席率等)，並檢視執行成效，請填選項 E。若機關有定期評估資安威脅、新興科技與業務適切性，規劃資通安全專職人員接受相關專業課程訓練，請填選項 F。完整選項內容與填寫說明，詳見表 22。

表22 17.資通安全專職人員應具備資安技能

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
17	資通安全專職人員應具備資安技能	A	資通安全專職人員未接受資安專業課程訓練	0	▪A/B 級機關：資通安全專職人員，每人每年至少接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練 ▪參考佐證資料 >教育訓練執行計畫 >教育訓練執行結果
		B	資通安全專職人員已接受資安專業課程訓練	1	
		C	資通安全專職人員，每人每年至少接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練，並檢討執行情形	2	
		D	資通安全專職人員之訓練要求，已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資通安全專職人員訓練質化或量化衡量指標(如教育訓練評量結果整體通過率、教育訓練出席率等)，並檢視執行成效	4	
		F	定期評估資安威脅、新興科技與業務適切性，規劃資通安全專職人員接受相關專業課程訓練	5	

資料來源：本計畫整理

第 18 題檢核項目為資訊人員、一般使用者及主管應具備資安認知，且資訊人員應具備資安技能，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已完成該應辦事項之要求，請填選項 C。機關如已將資訊人員、一般使用者及主管之資通安全通識教育訓練，與資訊人員之資通安全訓練要求，已納入標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已設定資訊人員、一般使用者及主管之資通安全通識教育訓練，與資訊人員之資通安全訓練成效質化或量化衡量指標(如教育訓練評量結果整體通過率、教育訓練出席率等)，並檢視執行成效，請填選項 E。若機關有定期評估資安威脅、新興科技與業務適切性，規劃資訊人員、一般使用者及主管接受相關能力課程訓練，請填選項 F。完整選項內容與填寫說明，詳見表 23。

表23 18.資訊人員、一般使用者及主管應具備資安認知且資訊人員應具備資安技能

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
18	資訊人員、一般使用者及主管應具備資安認知且資訊人員應具備資安技能	A	資訊人員、一般使用者及主管未接受資通安全通識教育訓練，且資訊人員未接受資通安全專業課程訓練或資通安全職能訓練	0	▪A/B 級機關：資通安全專職人員以外之資訊人員，每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教育訓練 ▪A/B 級機關：一般使用者與主管，每人每年接受 3 小時以上之資通安全通識教育訓練 ▪參考佐證資料 >教育訓練執行計畫 >教育訓練執行結果
		B	資訊人員、一般使用者與主管已接受資通安全通識教育訓練，且資訊人員已接受資通安全專業課程訓練或資通安全職能訓練	1	
		C	資訊人員、一般使用者及主管每人每年接受 3 小時以上之資通安全通識教育訓練，且資訊人員每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，並檢討執行情形	2	
		D	資訊人員、一般使用者及主管之資通安全通識教育訓練，與資訊人員之資通安全訓練要求，已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已設定資訊人員、一般使用者及主管之資通安全通識教育訓練，與資訊人員之資通安全訓練成效質化或量化衡量指標(如教育訓練評量結果整體通過率、教育訓練出席率等)，並檢視執行成效	4	
		F	定期評估資安威脅、新興科技與業務適切性，規劃資訊人員、一般使用者及主管接受相關能力課程訓練	5	

資料來源：本計畫整理

第 19 題檢核項目為取得資安專業證照，其資安專業證照係指由主管機關認可之國內外發證機關(構)所核發之資通安全證照。本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已完成該應辦事項之要求，請填選項 C。機關如已將資安專業證照要求納入標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定資通安全專業證照與資通安全職能所需專業證照質化或量化衡量指標(如人員於預定期間內取得證照比率等)，並檢視執行成效，請填選項 E。若機關有定期評估資安威脅、新興科技與業務適切性，規劃取得資通安全專業證照與資通安全職能課程訓練，請填選項 F。完整選項內容與填寫說明，詳見表 24。

表24 19.取得資安專業證照

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
19	取得資安專業證照	A	未具備資通安全專業證照或資通安全職能訓練證書	0	▪A 級機關：初次受核定或等級變更後之 1 年內，資通安全專職人員總計應持有 4 張以上資通安全專業證照與 4 張以上資通安全職能評量證書，並持續維持證照之有效性 ▪B 級機關：初次受核定或等級變更後之 1 年內，資通安全專職人員總計應持有 2 張以上資通安全專業證照與 2 張以上資通安全職能評量證書，並持續維持證照之有效性 ▪資通安全專業證照，指由主管機關認可之國內外發證機關(構)所核發之資通安全證照(資通安全責任等級分級辦法) ▪參考佐證資料 >資安專業證照 >資安職能證書
		B	已具備資通安全專業證照或資通安全職能訓練證書	1	
		C	A 級機關：資通安全專職人員總計應持有 4 張以上資通安全專業證照與 4 張以上資通安全職能評量證書，並檢討執行情形 B 級機關：資通安全專職人員總計應持有 2 張以上資通安全專業證照與 2 張以上資通安全職能評量證書，並檢討執行情形	2	
		D	資安專業證照要求，已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資通安全專業證照與資通安全職能所需專業證照質化或量化衡量指標(如人員於預定期間內取得證照比率等)，並檢視執行成效	4	
		F	定期評估資安威脅、新興科技與業務適切性，規劃取得資通安全專業證照與資通安全職能課程訓練	5	

資料來源：本計畫整理

第 20 題檢核項目為宣導資安政策與相關資安要求，若機關已針對全體人員執行資安政策與相關資安要求宣導(如透過教育訓練、內部會議、公文、張貼公告等)，請填選項 B。機關如已針對資安政策與相關資安要求宣導，定期檢討執行情形(如檢討資安政策與相關資安要求宣導活動之規劃與執行作業等)，請填選項 C。

若機關已訂定資安政策與相關資安要求宣導之標準作業程序或相關文件化要求，並落實執行，請填選項 D。若機關之資安政策與相關資安要求宣導，已具有質化或量化衡量指標，如辦理 2 場次資安宣導課程、宣導課程測試成績達 70 分以上或增加多元性宣導方式(實體課程、數位課程及政策重點宣導海報等)或每年至少向全體人員宣導 1 次資安政策等，並檢視執行成效，請填選項 E。機關如已依據資安政策與相關資安要求宣導作業執行成果，精進資安政策宣導方式，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含全機關。完整選項內容與填寫說明，詳見表 25。

表25 20.宣導資安政策與相關資安要求

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
20	宣導資安政策與相關資安要求	A	未針對全體人員執行資安政策與相關資安要求宣導	0	▪全體人員包含：正式人員、臨時人員、派遣人員 ▪選項配分達3分(含)以上者，實施範圍應包含全機關 ▪參考佐證資料 >資安宣導規劃 >公告資安相關管理制度 >資安宣導紀錄
		B	已針對全體人員執行資安政策與相關資安要求宣導(如透過教育訓練、內部會議、公文、張貼公告等)	1	
		C	針對資安政策與相關資安要求宣導，定期檢討執行情形(如檢討資安政策與相關資安要求宣導活動之規劃與執行作業等)	2	
		D	已訂定資安政策與相關資安要求宣導之標準作業程序或相關文件化要求，並落實執行	3	
		E	資安政策與相關資安要求宣導已具有質化或量化衡量指標，如辦理2場次資安宣導課程、宣導課程測試成績達70分以上或增加多元性宣導方式(實體課程、數位課程及政策重點宣導海報等)或每年至少向全體人員宣導1次資安政策等，並檢視執行成效	4	
		F	依據資安政策與相關資安要求宣導作業執行成果，精進資安政策宣導方式	5	

資料來源：本計畫整理

3.3 技術面檢核項目說明

技術面包含 4 個流程構面，分別為 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 資通系統開發與維護安全管理，以下介紹 4 個流程構面之檢核項目。

3.3.1 T1 存取控制管理之檢核項目說明

流程構面 T1 包含 3 個檢核項目，題號範圍為第 21 題至第 23 題，分別為「21.落實網路安全管理」、「22.管理資通系統權限」及「23.落實機敏資訊之加密管理」。

第 21 題檢核項目為落實網路安全管理，若機關已執行網路安全相關作業，至少包含網路區隔，依據網路服務需要區隔出獨立之邏輯網域(內部網路、外部網路及 DMZ)及防火牆設定檢視等，請填選項 B。機關如已針對網路安全相關作業(如定期檢視網路安全相關設備設定規則與其日誌紀錄等)有管理做法或機制，並檢討執行情形，請填選項 C。

機關若對於網路安全管理已訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定網路安全管理質化或量化衡量指標(如每年至少檢視 1 次網路安全政策或檢視網路設備設定符合實際架構等)，並檢視執行成效，請填選項 E。機關若針對網路安全相關管理措施，已具精進流程或執行方式，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含全機關。完整選項內容與填寫說明，詳見表 26。

表26 21.落實網路安全管理

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
21	落實網路安全管理	A	未執行網路安全相關作業	0	▪選項配分達 3 分(含)以上者，實施範圍應包含全機關 ▪參考佐證資料 >網路安全管理程序 >網路拓樸圖 >網路設備清單 >檢視紀錄
		B	已執行網路安全相關作業，至少包含網路區隔，依據網路服務需要區隔出獨立之邏輯網域(內部網路、外部網路及 DMZ)及防火牆設定檢視等	1	
		C	針對網路安全相關作業(如定期檢視網路安全相關設備設定規則與其日誌紀錄等)有管理做法或機制，並檢討執行情形	2	
		D	網路安全管理已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定網路安全管理質化或量化衡量指標(如每年至少檢視 1 次網路安全政策或檢視網路設備設定符合實際架構等)，並檢視執行成效	4	
		F	針對網路安全相關管理措施，精進流程或執行方式	5	

資料來源：本計畫整理

第 22 題檢核項目為管理資通系統權限，若機關已針對資通系統設置一般權限與特殊權限要求(至少包含存取控制政策、角色權責區分及權限申請與變更作業等)，請填選項 B。本題之特殊權限係指如作業系統最高權限、資料庫管理系統最高權限、機敏性系統資料存取權限等。

機關如已針對資通系統設置一般權限與特殊權限要求(如管理資通系統權限之申請、變更與刪除作業等)有管理做法或機制，並檢討執行情形，請填選項 C。若機關對於資通系統一般權限與特殊權限要求，已訂定標準作業程序或相關文件化要求並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定資通系統一般權限與特殊權限要求質化或量化衡量指標(如定期審查與執行權限管控等)，並檢視執行成效，請填選項 E。若機關針對資通系統設置一般權限與特殊權限相關管理措施，已具精進流程或執行方式，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含全部資通系統。完整選項內容與填寫說明，詳見表 27。

表27 22.管理資通系統權限

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
22	管理資通系統權限	A	未針對資通系統設置一般權限與特殊權限要求	0	▪特殊權限：如作業系統最高權限、資料庫管理系統最高權限、機敏性系統資料存取權限等 ▪選項配分達3分(含)以上者，實施範圍應包含全部資通系統 ▪參考佐證資料 >密碼管理程序 >系統存取管理程序 >資通系統權限管理程序或規範 >使用稽核軌跡/行為分析/審查
		B	已針對資通系統設置一般權限與特殊權限要求(至少包含存取控制政策、角色權責區分及權限申請與變更作業等)	1	
		C	針對資通系統設置一般權限與特殊權限要求(如管理資通系統權限之申請、變更與刪除作業等)有管理做法或機制，並檢討執行情形	2	
		D	資通系統一般權限與特殊權限要求，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資通系統一般權限與特殊權限要求質化或量化衡量指標(如定期審查與執行權限管控等)，並檢視執行成效	4	
		F	針對資通系統設置一般權限與特殊權限相關管理措施，精進流程或執行方式	5	

資料來源：本計畫整理

第 23 題檢核項目為落實機敏資訊之加密管理，該機敏資訊係指為「文書處理手冊」之一般公務機密文書與涉及機關(構)內部資料，如業務程序、紀錄(日誌)、個人資料等敏感資料。

若機關已針對機敏資訊於儲存或傳輸時，進行加密措施(如壓縮檔+密碼加密亦可)，請填選項 B。機關如針對機敏資訊於儲存或傳輸時之加密措施(如採購加密設備及記錄使用者安裝時程、通知與落實使用者更新加密裝置並進行金鑰管理等)已有管理做法或機制，並檢討執行情形，請填選項 C。自評人員請留意，機關若無採購加密設備，只要有針對現行加密措施進行管理，並定期檢討執行情形(如定期檢視個人資料或密件於郵件傳輸或儲存於內網硬碟空間是否進行加密)，亦可填選項 C，佐證資料可為檢視紀錄。

機關內部有針對機敏資訊之加密措施與做法訂定標準作業程序或在相關文件記載，使執行結果具一致性，並落實執行，請填選項 D，佐證資料為標準作業程序或相關文件。若該標準作業程序或相關文件，已訂定機敏資訊之加密質化或量化衡量指標(如每年檢視 1 次機密資料加密措施之符合性，每年檢視 1 次作業程序之符合性等)，並定期檢視執行成效，請填選項 E，佐證資料可為檢視紀錄或會議紀錄。機關針對機敏資訊儲存或傳輸之加密措施，有更優化之執行方式(如規劃採購加密設備之時程、改善機關內部對機敏資訊加密作業程序等)，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含全機關。完整選項內容與填寫說明，詳見表 28。

表28 23.落實機敏資訊之加密管理

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
23	落實機敏資訊之加密管理	A	未針對機敏資訊於儲存或傳輸時，進行加密措施	0	▪機敏資訊：為「文書處理手冊」之一般公務機密文書與涉及機關(構)內部資料，如業務程序、紀錄(日誌)、個人資料等敏感資料 ▪選項配分達3分(含)以上者，實施範圍應包含全機關 ▪參考佐證資料 >加密機制相關程序 >加密技術證明(採用技術之程序紀錄/委外合約)
		B	已針對機敏資訊於儲存或傳輸時，進行加密措施	1	
		C	針對機敏資訊於儲存或傳輸時之加密措施(如採購加密設備及記錄使用者安裝時程、通知與落實使用者更新加密裝置並進行金鑰管理等)有管理做法或機制，並檢討執行情形	2	
		D	機敏資訊之加密，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定機敏資訊之加密質化或量化衡量指標(如每年檢視1次機密資料加密措施之符合性，每年檢視1次作業程序之符合性等)，並檢視執行成效	4	
		F	針對機敏資訊儲存或傳輸之加密措施，精進流程或執行方式	5	

資料來源：本計畫整理

3.3.2 T2 通訊與作業安全管理之檢核項目說明

流程構面 T2 包含 12 個檢核項目，題號範圍為第 24 題至第 35 題，分別為「24.執行惡意軟體之偵測與預防」、「25.執行遠距工作安全控制措施」、「26.落實電子郵件安全管理」、「27.落實機房管理」、「28.執行資料備份」、「29.執行儲存媒體之防護措施」、「30.落實資通安全威脅偵測管理機制」、「31.落實資通安全防護」、「32.執行政府組態基準」、「33.執行資通安全健診」、「34.執行網站安全弱點檢測」及「35.執行系統滲透測試」。

第 24 題檢核項目為執行惡意軟體之偵測與預防，若機關已執行惡意軟體偵測與預防措施(至少包含限制未授權軟體與安裝防毒軟體等)，請填選項 B。若機關針對惡意軟體偵測與預防措施(如採購軟硬體惡意軟體偵測與預防設備等)有管理做法或機制，並檢討執行情形，請填選項 C。

機關如已針對惡意軟體偵測與預防措施，訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定惡意軟體偵測與預防質化或量化衡量指標(如每年至少檢視 1 次惡意軟體防護或未授權軟體之符合情形等)，並檢視執行成效，請填選項 E。機關如針對惡意軟體偵測與預防措施，已具精進流程或執行方式，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含全機關。完整選項內容與填寫說明，詳見表 29。

表29 24.執行惡意軟體之偵測與預防

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
24	執行惡意軟體之偵測與預防	A	未執行惡意軟體偵測與預防措施	0	▪選項配分達 3 分(含)以上者，實施範圍應包含全機關 ▪參考佐證資料 >惡意軟體相關管理程序 >惡意程式檢測規劃 >檢討與改善方案
		B	已執行惡意軟體偵測與預防措施(至少包含限制未授權軟體與安裝防毒軟體等)	1	
		C	針對惡意軟體偵測與預防措施(如採購軟硬體惡意軟體偵測與預防設備等)有管理做法或機制，並檢討執行情形	2	
		D	惡意軟體偵測與預防措施，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定惡意軟體偵測與預防質化或量化衡量指標(如每年至少檢視 1 次惡意軟體防護或未授權軟體之符合情形等)，並檢視執行成效	4	
		F	針對惡意軟體偵測與預防措施，精進流程或執行方式	5	

資料來源：本計畫整理

第 25 題檢核項目為執行遠距工作安全控制措施，若機關規定禁止遠距工作，請填選項 G 不適用。若機關未禁止遠距工作，請選擇下列選項之一。若機關未執行遠距工作之安全措施，請填選項 A。機關如已執行遠距工作之安全措施(至少包含對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，並採用伺服端之集中過濾機制檢查使用者之授權等)，請填選項 B。針對遠距工作之安全措施(如管理遠距工作之申請與授權作業等)，機關已有管理做法或機制，並檢討執行情形，請填選項 C。

對於遠距工作安全控制措施，機關如已訂定標準作業程序或相關文件化要求並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定遠距工作安全控制措施質化或量化衡量指標(如每年至少檢視 1 次遠距工作之安全措施等)，並檢視執行成效，請填選項 E。針對遠距工作之安全管理措施，機關已具備精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 30。

表30 25.執行遠距工作安全控制措施

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
25	執行遠距工作安全控制措施	A	未執行遠距工作之安全措施	0	▪遠距工作之安全措施：如 >對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，並採用伺服端之集中過濾機制檢查使用者之授權 >應監控資通系統遠端連線 >資通系統應採用加密機制 >資通系統遠端存取來源應為機關已預先定義及管理之存取控制點 >依維運需求，授權透過遠端執行特定之功能及存取相關資訊 ▪若規定禁止遠距工作，則填寫「不適用」選項 ▪參考佐證資料 >遠距工作相關管理程序 >遠距工作申請與審核紀錄
		B	已執行遠距工作之安全措施(至少包含對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，並採用伺服端之集中過濾機制檢查使用者之授權等)	1	
		C	針對遠距工作之安全措施(如管理遠距工作之申請與授權作業等)有管理做法或機制，並檢討執行情形	2	
		D	遠距工作安全控制措施，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定遠距工作安全控制措施質化或量化衡量指標(如每年至少檢視1次遠距工作之安全措施等)，並檢視執行成效	4	
		F	針對遠距工作之安全管理措施，精進流程或執行方式	5	
		G	不適用	N/A	

資料來源：本計畫整理

第 26 題檢核項目為落實電子郵件安全管理，若機關已執行電子郵件之安全防護措施(至少包含建置電子郵件之垃圾郵件過濾與電子郵件社交工程演練等)，請填選項 B。若針對電子郵件之安全防護措施(如管理垃圾郵件過濾或內容過濾偵測結果等)已有管理做法或機制，並檢討執行情形，請填選項 C。

對於電子郵件之安全防護措施，已訂定標準作業程序或相關文件化要求並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定電子郵件之安全防護措施質化或量化衡量指標(如每年至少執行 1 次社交工程演練，每年至少檢視 1 次郵件管理措施等)，並檢視執行成效，請填選項 E。若針對電子郵件之安全防護措施，已具有精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 31。

表31 26.落實電子郵件安全管理

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
26	落實電子郵件安全管理	A	未執行電子郵件之安全防護措施	0	▪電子郵件之安全防護措施：如 >電子郵件加簽以避免發送匿名或偽造電子郵件 >不得利用機關所提供電子郵件，侵害他人權益、違法之行為 >依郵件內容之機密性、敏感性規範傳送限制，例如密等以上之公文不得以電子郵件傳送、含有個人資料之信件必須加密傳送 >建置電子郵件之垃圾郵件過濾、防毒牆及內容過濾及防止資料外洩之技術 >定期執行電子郵件社交工程宣導、教育訓練及演練 ▪參考佐證資料 >電子郵件相關管理程序 >電子郵件社交工程演練紀錄 >電子郵件社交工程演練檢討
		B	已執行電子郵件之安全防護措施(至少包含建置電子郵件之垃圾郵件過濾與電子郵件社交工程演練等)	1	
		C	針對電子郵件之安全防護措施(如管理垃圾郵件過濾或內容過濾偵測結果等)有管理做法或機制，並檢討執行情形	2	
		D	電子郵件之安全防護措施，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定電子郵件之安全防護措施質化或量化衡量指標(如每年至少執行 1 次社交工程演練，每年至少檢視 1 次郵件管理措施等)，並檢視執行成效	4	
		F	針對電子郵件之安全防護措施，精進流程或執行方式	5	

資料來源：本計畫整理

第 27 題之檢核項目為落實機房管理，若機關已執行電腦機房之安全防護措施(至少包含電腦機房進出管制與電腦機房溫濕度控制等)，請填選項 B。針對電腦機房之安全防護措施(如檢視機房門禁授權名單與設備、管理機房溫濕度等)已有管理做法或機制，並檢討執行情形，請填選項 C。

對於電腦機房之安全防護措施已訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定電腦機房安全管理質化或量化衡量指標(如每週檢視 1 次人員與設備進出紀錄、每月檢視 1 次環境管控紀錄或定期檢視機房進出之授權名單等)，並檢視執行成效，請填選項 E。若針對電腦機房之安全管理措施，已有精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 32。

表32 27.落實機房管理

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
27	落實機房管理	A	未執行電腦機房之安全防護措施	0	▪電腦機房：包含機關內部機房與對外服務之機房 ▪參考佐證資料 >管制區域相關管理程序 >管制區域內環境設備檢查紀錄
		B	已執行電腦機房之安全防護措施(至少包含電腦機房進出管制與電腦機房溫濕度控制等)	1	
		C	針對電腦機房之安全防護措施(如檢視機房門禁授權名單與設備、管理機房溫濕度等)有管理做法或機制，並檢討執行情形	2	
		D	電腦機房之安全防護措施，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定電腦機房安全管理質化或量化衡量指標(如每週檢視1次人員與設備進出紀錄、每月檢視1次環境管控紀錄或定期檢視機房進出之授權名單等)，並檢視執行成效	4	
		F	針對電腦機房之安全管理措施，精進流程或執行方式	5	

資料來源：本計畫整理

第 28 題檢核項目為執行資料備份，若機關已對資料進行備份(至少包含重要資料備份與異地存放等)，請填選項 B。針對資料之備份作業(如定期透過復原測試以確認備份之有效性等)，機關已有管理做法或機制，並檢討執行情形，請填選項 C。

若機關之資料備份作業，已訂定標準作業程序或相關文件化要求並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定資料備份作業質化或量化衡量指標(如每週至少執行 1 次資料備份，資料備份需保留 3 代等)，並檢視執行成效，請填選項 E。針對資料備份作業，機關已有精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 33。

表33 28.執行資料備份

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
28	執行資料備份	A	未對資料進行備份	0	▪資料備份作業：如 >依資料等級、重要性，規劃備份方式與頻率 >重要資料備份保存至少 3 代 >執行安全距離之異地備份 >針對具機敏性的資料進行加密保護 ▪磁帶保留代數：保留 1 份完整備份(全備份)之磁帶，為保留 1 代；保留全備份磁帶 3 份，則為保留 3 代 ▪參考佐證資料 >備份要求或紀錄 >備份復原測試紀錄 >備份資料存放紀錄
		B	已對資料進行備份(至少包含重要資料備份與異地存放等)	1	
		C	針對資料之備份作業(如定期透過復原測試以確認備份之有效性等)有管理做法或機制，並檢討執行情形	2	
		D	資料備份作業，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資料備份作業質化或量化衡量指標(如每週至少執行 1 次資料備份，資料備份需保留 3 代等)，並檢視執行成效	4	
		F	針對資料備份作業，精進流程或執行方式	5	

資料來源：本計畫整理

第 29 題之檢核項目為執行儲存媒體之防護措施，若機關已針對機密與敏感性資料之儲存媒體實施防護措施(至少包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙等)，請填選項 B。針對機密與敏感性資料之儲存媒體防護措施(如檢視儲存媒體防護措施之妥適性等)，機關已有管理做法或機制，並檢討執行情形，請填選項 C。

對於儲存媒體之防護措施，機關已訂定標準作業程序或相關文件化要求並落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定儲存媒體之防護措施質化或量化衡量指標(如每年至少檢視 1 次含機密與敏感資料儲存媒體之管理，且針對查核不符者持續審視與改善追蹤等)，並檢視執行成效，請填選項 E。針對儲存媒體之防護措施，機關已有精進流程或執行方式，請填選項 F。

自評人員請留意，本題選項配分達 3 分(含)以上者，實施範圍應包含全部儲存媒體。完整選項內容與填寫說明，詳見表 34。

表34 29.執行儲存媒體之防護措施

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
29	執行儲存媒體之防護措施	A	未針對機密與敏感性資料之儲存媒體實施防護措施	0	▪選項配分達 3 分(含)以上者，實施範圍應包含全部儲存媒體 ▪參考佐證資料 >儲存媒體管理相關規範 >儲存媒體管理檢核紀錄 >改善紀錄
		B	已針對機密與敏感性資料之儲存媒體實施防護措施(至少包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙等)	1	
		C	針對機密與敏感性資料之儲存媒體防護措施(如檢視儲存媒體防護措施之妥適性等)有管理做法或機制，並檢討執行情形	2	
		D	儲存媒體之防護措施，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定儲存媒體之防護措施質化或量化衡量指標(如每年至少檢視 1 次含機密與敏感資料儲存媒體之管理，且針對查核不符者持續審視與改善追蹤等)，並檢視執行成效	4	
		F	針對儲存媒體之防護措施，精進流程或執行方式	5	

資料來源：本計畫整理

第 30 題檢核項目為落實資通安全威脅偵測管理機制，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已完成該應辦事項之要求，請填選項 C。若資通安全威脅偵測管理機制作業由委外廠商承包，可將委外廠商之服務建議書、執行規劃或實施紀錄等，列為標準作業程序或相關文件化要求。若機關同時具備文件與落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定資通安全威脅偵測管理機制質化或量化衡量指標(如每月檢視監控之成效、高風險弱點應即時修復、資安事件達 1 或 2 級時，應立即通報與處理等)，並檢視執行成效，請填選項 E。針對資通安全監控，若機關已有精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 35。

表35 30.落實資通安全威脅偵測管理機制(SOC)

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
30	落實資通安全威脅偵測管理機制(SOC)	A	未規劃資通安全威脅偵測管理機制	0	▪A/B 級機關：初次受核定或等級變更後之 1 年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料 ▪參考佐證資料 >資通安全執行規劃 >資通安全實施紀錄 >監控管理資料 >改善方案
		B	已規劃資通安全威脅偵測管理機制	1	
		C	完成資通安全威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料，且檢討執行情形	2	
		D	資通安全威脅偵測管理機制已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資通安全威脅偵測管理機制質化或量化衡量指標(如每月檢視監控之成效、高風險弱點應即時修復、資安事件達 1 或 2 級時，應立即通報與處理等)，並檢視執行成效	4	
		F	針對資通安全威脅偵測管理機制，精進流程或執行方式	5	

資料來源：本計畫整理

第 31 題檢核項目為落實資通安全防護，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已完成該應辦事項之要求，請填選項 C。若資通安全防護作業由委外廠商承包，可將委外廠商之服務建議書或執行計畫書，列為標準作業程序或相關文件化要求。若機關同時具備文件與落實執行，請填選項 D。若該標準作業程序或相關文件，已訂定資通安全防護質化或量化衡量指標(如每年至少檢視 1 次應辦事項之資通安全防護要求，且針對不符情形，執行改善追蹤等)，並檢視執行成效，請填選項 E。若針對資通安全防護要求，機關已有精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 36。

表36 31.落實資通安全防護

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
31	落實資通安全防護	A	未執行資通安全防護	0	▪A/B 級機關：初次受核定或等級變更後之 1 年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級 ▪參考佐證資料
		B	已執行資通安全防護(至少包含防毒軟體、網路防火牆及具有郵件伺服器者，應備電子郵件過濾機制等)	1	
		C	▪A 級機關已建置以下措施，並檢討執行情形： -防毒軟體 -網路防火牆 -具有郵件伺服器者，應備電子郵件過濾機制 -入侵偵測及防禦機制 -具有對外服務之核心資通系統者，應備應用程式防火牆 -進階持續性威脅攻擊防禦措施	2	

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
			▪B 級機關已建置以下措施，並檢討執行情形： -防毒軟體 -網路防火牆 -具有郵件伺服器者，應備電子郵件過濾機制 -入侵偵測及防禦機制 -具有對外服務之核心資通系統者，應備應用程式防火牆		>資通安全防護要求之相關作業程序 >執行與查核紀錄 >改善紀錄
		D	資通安全防護要求，已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資通安全防護質化或量化衡量指標(如每年至少檢視 1 次應辦事項之資通安全防護要求，且針對不符情形，執行改善追蹤等)，並檢視執行成效	4	
		F	針對資通安全防護要求，精進流程或執行方式	5	

資料來源：本計畫整理

第 32 題檢核項目為執行政府組態基準，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已導入與持續維運政府組態基準，並檢討例外管理項目與執行情形，請填選項 B。若政府組態基準導入作業與持續維運作業由委外廠商承包，可將委外廠商之服務建議書或執計畫書，列為標準作業程序或相關文件化要求。若機關同時具備文件與落實執行，請填選項 D。若該標準作業程序或相關文件，已制定政府組態基準質化或量化衡量指標(如每年至少檢視 1 次政府組態基準例外管理項目，且針對政府組態基準要求查核不符情形，執行改善追蹤等)，並檢視執行成效，請填選項 E。若針對應辦事項之政府組態基準要求，機關已有精進流程或執行方式，請填選項 F。

自評人員請留意，本題之選項配分達 3 分(含)以上者，實施範圍應包含政府組態基準全部項目(排除已核定之政府組態基準例外管理項目)。完整選項內容與填寫說明，詳見表 37。

表37 32.執行政府組態基準

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
32	執行政府組態基準	A	未導入政府組態基準	0	▪A/B 級機關：初次受核定或等級變更後之 1 年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運 ▪選項配分達 3 分(含)以上者，實施範圍應包含政府組態基準全部項目(排除已核定之政府組態基準例外管理項目) ▪參考佐證資料 >政府組態基準導入與維護資料
		B	已導入政府組態基準	1	
		C	已導入與持續維運政府組態基準，並檢討例外管理項目與執行情形	2	
		D	政府組態基準已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已制定政府組態基準質化或量化衡量指標(如每年至少檢視 1 次政府組態基準例外管理項目，且針對政府組態基準要求查核不符情形，執行改善追蹤等)，並檢視執行成效	4	
		F	針對應辦事項之政府組態基準要求，精進流程或執行方式	5	

資料來源：本計畫整理

第 33 題之檢核項目為執行資通安全健診，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項。若機關已完成應辦事項之要求，請填選項 C。若資通安全健診作業由委外廠商承包，可將委外廠商之服務建議書、檢測/複測報告及改善計畫等文件，列為標準作業程序或相關文件化要求。若機關同時具備文件與落實執行，請填選項 D。若該標準作業程序或相關文件，已制定資通安全健診質化或量化衡量指標(如改善比率、不符合事項比率、範圍或次數擴大等)，並檢視執行成效，請填選項 E。機關若針對資通安全健診結果進行分析，提出預防措施，並於預定時間內完成，請填選項 F。

自評人員請留意，公務機關辦理資通安全責任等級分級辦法附表一/附表三「資通安全健診」時，除依附表一/附表三所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。完整選項內容與填寫說明，詳見表 38。

表38 33.執行資通安全健診

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
33	執行資通安全健診	A	未執行資通安全健診	0	▪A 級機關：每年辦理 1 次資通安全健診 ▪B 級機關：每 2 年辦理 1 次資通安全健診 ▪公務機關辦理資通安全責任等級分級辦法附表一/附表三「資通安全健診」時，除依附表一/附表三所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施(資通安全責任等級分級辦法) ▪參考佐證資料 >檢測/複測報告 >改善計畫 >追蹤改善紀錄
		B	已執行資通安全健診(至少包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視等)	1	
		C	A 級機關：每年辦理 1 次資通安全健診，並檢討執行情形 B 級機關：每 2 年辦理 1 次資通安全健診，並檢討執行情形	2	
		D	資通安全健診已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已制定資通安全健診質化或量化衡量指標(如改善比率、不符合事項比率、範圍或次數擴大等)，並檢視執行成效	4	
		F	針對資通安全健診結果進行分析，提出預防措施，並於預定時間內完成	5	

資料來源：本計畫整理

第 34 題檢核項目為執行網站安全弱點檢測，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項。若機關已完成應辦事項之要求，請填選項 C。若網站安全弱點檢測作業由委外廠商承包，可將委外廠商之服務建議書、檢測/複測報告及改善計畫等文件，列為標準作業程序或相關文件化要求。若機關同時具有文件與落實執行，請填選項 D。

若該標準作業程序或相關文件，已訂定網站安全弱點檢測質化或量化衡量指標(如弱點改善比率、SQL injection 數量等)，並檢視執行成效，請填選項 E。機關若針對網站安全弱點檢測結果進行分析，提出預防措施，並於預定時間內完成，請填選項 F。完整選項內容與填寫說明，詳見表 39。

表39 34.執行網站安全弱點檢測

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
34	執行網站安全弱點檢測	A	未執行網站安全弱點檢測	0	▪A 級機關：全部核心資通系統每年辦理 2 次網站安全弱點檢測 ▪B 級機關：全部核心資通系統每年辦理 1 次網站安全弱點檢測 ▪參考佐證資料 >檢測/複測報告 >改善計畫 >追蹤改善紀錄
		B	已執行網站安全弱點檢測	1	
		C	A 級機關：全部核心資通系統每年辦理 2 次網站安全弱點檢測，並檢討執行情形 B 級機關：全部核心資通系統每年辦理 1 次網站安全弱點檢測，並檢討執行情形	2	
		D	網站安全弱點檢測已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定網站安全弱點檢測質化或量化衡量指標(如弱點改善比率、SQL injection 數量等)，並檢視執行成效	4	
		F	針對網站安全弱點檢測結果進行分析，提出預防措施，並於預定時間內完成	5	

資料來源：本計畫整理

第 35 題檢核項目為執行系統滲透測試，本題亦為資通安全責任等級 A 級與 B 級之公務機關應辦事項項目之一。若機關已完成該應辦事項之要求，請填選項 C。若系統滲透測試作業由委外廠商承包，可將委外廠商之服務建議書、檢測/複測報告及改善計畫等文件，列為標準作業程序或相關文件化。若機關同時具有文件與落實執行，請填選項 D。

若該標準作業程序或相關文件，已訂定系統滲透測試質化或量化衡量指標(如高/中/低風險發現事項數量等)，並檢視執行成效，請填選項 E。若機關針對系統滲透測試結果進行分析，提出預防措施，並於預定時間內完成，請填選項 F。完整選項內容與填寫說明，詳見表 40。

表40 35.執行系統滲透測試

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
35	執行系統滲透測試	A	未辦理系統滲透測試	0	▪A 級機關：全部核心資通系統每年辦理 1 次系統滲透測試 ▪B 級機關：全部核心資通系統每 2 年辦理 1 次系統滲透測試 ▪參考佐證資料 >檢測/複測報告 >改善計畫 >追蹤改善紀錄
		B	已辦理系統滲透測試	1	
		C	A 級機關：全部核心資通系統每年辦理 1 次系統滲透測試，並檢討執行情形 B 級機關：全部核心資通系統每 2 年辦理 1 次系統滲透測試，並檢討執行情形	2	
		D	系統滲透測試已納入標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定系統滲透測試質化或量化衡量指標(如高/中/低風險發現事項數量等)，並檢視執行成效	4	
		F	針對系統滲透測試結果進行分析，提出預防措施，並於預定時間內完成	5	

資料來源：本計畫整理

3.3.3 T3 資安事件通報與處理之檢核項目說明

流程構面 T3 包含 2 個檢核項目，題號範圍為第 36 題至第 37 題，分別為「36.執行資安事件通報應變」與「37.保存資通系統與資安設備日誌紀錄」。

第 36 題旨在檢核機關是否執行資安事件通報與處理。若機關前一年度無發生資安事件，請填選項 G 不適用；若機關前一年度曾發生資安事件，請根據實際執行情形，選擇 A 至 F 任一選項答案。機關如未執行資安事件通報與處理，請填選項 A。機關如已執行資安事件通報與處理，請填選項 B。機關若針對資安事件通報與處理(如召開會議檢討事件執行情形等)已有管理做法或機制，並檢討執行情形，請填選項 C。

對於資安事件通報處理，機關已訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若機關已於標準作業程序或相關文件訂定資安事件通報與處理質化或量化衡量指標(如發現第 1 或 2 級資安事件時，於 72 小時內完成損害控制或復原作業；發現第 3 或 4 級資安事件時，於 36 小時內完成損害控制或復原作業或每年辦理 1 次資安事件通報應變演練等)，並檢視執行成效，請填選項 E。若機關針對資安事件通報與處理，已有精進流程或執行數位證據保全與鑑識作業，請填選項 F。完整選項內容與填寫說明，詳見表 41。

表41 36.執行資安事件通報應變

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
36	執行資安事件通報應變	A	未執行資安事件通報與處理	0	▪數位證據：指經解釋後得為事實佐證之數位資料 ▪數位鑑識：(有時又被稱作數位鑑識科學)乃是鑑識科學之其中一個分支，主要在針對數位裝置之內容進行調查與復原，這常常是與電腦犯罪有所相關 ▪若無發生資安事件，則填寫「不適用」選項 ▪參考佐證資料 >資安事件通報程序、資通安全緊急應變程序 >資安事件紀錄 >改善方案
		B	已執行資安事件通報與處理	1	
		C	針對資安事件通報與處理有管理做法或機制，並檢討執行情形(如召開會議檢討事件執行情形等)	2	
		D	資安事件通報處理，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資安事件通報與處理質化或量化衡量指標(如發現第 1 或 2 級資安事件時，於 72 小時內完成損害控制或復原作業；發現第 3 或 4 級資安事件時，於 36 小時內完成損害控制或復原作業或每年辦理 1 次資安事件通報應變演練等)，並檢視執行成效	4	
		F	針對資安事件通報與處理，精進流程或執行數位證據保全與鑑識作業	5	
		G	不適用	N/A	

資料來源：本計畫整理

第 37 題亦為流程構面 T3 資安事件通報與處理之相關檢項項目，旨在檢核機關是否保存資通系統與資安設備日誌紀錄，尤其當資安件事發生時。若機關已針對核心資通系統與資安設備，保存日誌紀錄，請填選項 B。針對核心資通系統與資安設備之日誌紀錄(如檢視資通系統與資安設備之日誌紀錄，並由主管覆核執行成果等)，機關已有管理做法或機制，並檢討執行情形，請填選項 C。

若針對日誌紀錄保存，機關已訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。機關如已訂定日誌紀錄保存質化或量化衡量指標(如每年至少檢視 1 次核心資通系統與資安設備日誌紀錄保存是否符合程序要求，且針對不符項目執行改善追蹤等)，並檢視執行成效，請填選項 E。若針對日誌紀錄保存，機關已有精進流程或執行方式，請填選項 F。完整選項內容與填寫說明，詳見表 42。

表42 37.保存資通系統與資安設備日誌紀錄

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
37	保存資通系統與資安設備日誌紀錄	A	未針對核心資通系統與資安設備，保存日誌紀錄	0	▪核心資通系統：指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則，判定其防護需求等級為高者(資通安全管理法施行細則第七條) ▪參考佐證資料 >日誌紀錄保存要求 >日誌紀錄 >日誌紀錄檢視紀錄
		B	已針對核心資通系統與資安設備，保存日誌紀錄	1	
		C	針對核心資通系統與資安設備之日誌紀錄(如檢視資通系統與資安設備之日誌紀錄，並由主管覆核執行成果等)有管理做法或機制，並檢討執行情形	2	
		D	針對日誌紀錄保存，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定日誌紀錄保存質化或量化衡量指標(如每年至少檢視1次核心資通系統與資安設備日誌紀錄保存是否符合程序要求，且針對不符項目執行改善追蹤等)，並檢視執行成效	4	
		F	針對日誌紀錄保存，精進流程或執行方式	5	

資料來源：本計畫整理

3.3.4 T4 資通系統開發與維護安全管理之檢核項目說明

流程構面 T4 包含 4 個檢核項目，題號範圍為第 38 題至第 41 題，分別為「38.執行資通系統開發之安全需求設計」、「39.執行資通系統開發之安全性測試」、「40.執行源碼安全管理」及「41.區隔系統開發、測試、實作的環境與設備」。

第 38 題檢核項目為安全的系統發展生命週期(SSDLC)之相關檢核項目，旨在檢核機關是否於資通系統開發前設計安全性要求。本檢核項目之資通系統係指新系統或有影響安全性之系統改版，若無新系統或有影響安全性之系統改版，請填選項 G 不適用。

若機關已於資通系統開發前，設計安全性要求(至少包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等)，請填選項 B。若機關針對資通系統開發前之安全性要求(如檢視系統開發安全性要求之妥適性等)，已有管理做法或機制，並檢討執行情形，請填選項 C。

機關如已針對資通系統開發之資安相關措施，訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。機關若已訂定資通系統開發之資安相關措施質化或量化衡量指標(如系統上線前不得有高風險項目、系統開發與測試需由不同人員負責執行等)，並檢視執行成效，請填選項 E。針對資通系統開發資安相關措施，機關如已有精進流程或執行方式，請填選項 F。

自評人員請留意，此檢核項目之填答選項配分若達 3 分(含)以上，實施範圍應包含全部資通系統。完整選項內容與填寫說明，詳見表 43。

表43 38.執行資通系統開發之安全需求設計

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
38	執行資通系統開發之安全需求設計	A	未於資通系統開發前，設計安全性要求	0	▪本檢核項目之資通系統，指新系統或有影響安全性之系統改版 ▪選項配分達3分(含)以上者，實施範圍應包含全部資通系統 ▪若無新系統或有影響安全性之系統改版，則填寫「不適用」選項 ▪參考佐證資料 >系統開發管理程序 >需求說明書
		B	已於資通系統開發前，設計安全性要求(至少包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等)	1	
		C	針對資通系統開發前之安全性要求(如檢視系統開發安全性要求之妥適性等)有管理做法或機制，並檢討執行情形	2	
		D	針對資通系統開發之資安相關措施，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定資通系統開發之資安相關措施質化或量化衡量指標(如系統上線前不得有高風險項目、系統開發與測試需由不同人員負責執行等)，並檢視執行成效	4	
		F	針對資通系統開發資安相關措施，精進流程或執行方式	5	
		G	不適用	N/A	

資料來源：本計畫整理

第 39 題亦為安全的系統發展生命週期(SSDLC)之相關檢核項目，旨在檢核機關是否於資通系統上線前執行安全性測試。本檢核項目之資通系統係指新系統或有影響安全性之系統改版，若無新系統或有影響安全性之系統改版，請填選項 G 不適用。

若機關已於上線前執行安全性測試(至少包含弱點掃描，若為高等級之資通系統則需執行源碼掃描與滲透測試等)，並檢討執行情形，請填選項 B。針對上線前之安全性測試(如檢視系統測試方式，經主管覆核測試結果等)，機關已有管理做法或機制，並檢討執行情形，請填選項 C。

若機關針對系統開發之安全性測試，已訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。機關如已訂定上線前安全性測試質化或量化衡量指標(如系統開發之安全性測試通過率需達 100%等)，並檢視執行成效，請填選項 E。若機關針對系統開發之測試，已有檢討與精進流程或執行方式，請填選項 F。

自評人員請留意，此檢核項目之填答選項配分若達 3 分(含)以上，實施範圍應包含全部資通系統。完整選項內容與填寫說明，詳見表 44。

表44 39.執行資通系統開發之安全性測試

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
39	執行資通系統開發之安全性測試	A	未於上線前執行安全性測試	0	▪本檢核項目之資通系統，指新系統或有影響安全性之系統改版 ▪選項配分達 3 分(含)以上者，實施範圍應包含全部資通系統 ▪若無新系統或有影響安全性之系統改版，則填寫「不適用」選項 ▪參考佐證資料 >系統測試管理程序 >系統測試計畫 >審查紀錄
		B	已於上線前執行安全性測試(至少包含弱點掃描，若為高等級之資通系統則需執行源碼掃描與滲透測試等)，並檢討執行情形	1	
		C	針對上線前之安全性測試(如檢視系統測試方式，經主管覆核測試結果等)有管理做法或機制，並檢討執行情形	2	
		D	針對系統開發之安全性測試，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定上線前安全性測試質化或量化衡量指標(如系統開發之安全性測試通過率需達 100%等)，並檢視執行成效	4	
		F	針對系統開發之測試，檢討與精進流程或執行方式	5	
		G	不適用	N/A	

資料來源：本計畫整理

第 40 題檢核項目為執行源碼安全管理，旨在確認機關是否執行資通系統源碼安全管理措施。若機關已執行資通系統源碼安全措施(至少包含源碼存取控制與版本控管等)，請填選項 B。針對資通系統源碼安全措施(如定期檢視版本控管情形與管理資通系統源碼存取權限等)，機關已有管理做法或機制，並檢討執行情形，請填選項 C。

針對資通系統源碼安全措施，機關已訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若機關已訂定源碼安全措施質化或量化衡量指標(如每年至少檢視 1 次源碼存取權限等)，並檢視執行成效，請填選項 E。針對源碼安全措施，機關已有精進流程或執行方式，請填選項 F。

自評人員請留意，此檢核項目之填答選項配分若達 3 分(含)以上，實施範圍應包含全部資通系統。完整選項內容與填寫說明，詳見表 45。

表45 40.執行源碼安全管理

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
40	執行源碼安全管理	A	未執行資通系統源碼安全措施	0	▪選項配分達 3 分(含)以上者，實施範圍應包含全部資通系統 ▪參考佐證資料 >資通系統源碼存取之相關管理程序 >存取控制與管理相關紀錄
		B	已執行資通系統源碼安全措施(至少包含源碼存取控制與版本控管等)	1	
		C	針對資通系統源碼安全措施(如定期檢視版本控管情形與管理資通系統源碼存取權限等)有管理做法或機制，並檢討執行情形	2	
		D	針對資通系統源碼安全措施，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定源碼安全措施質化或量化衡量指標(如每年至少檢視 1 次源碼存取權限等)，並檢視執行成效	4	
		F	針對源碼安全措施，精進流程或執行方式	5	

資料來源：本計畫整理

第 41 題檢核項目為區隔系統開發、測試、實作的環境與設備，旨在確認機關在系統開發、測試或實作階段，其環境與設備皆能與正式作業環境進行區隔與管理，以確保機關之系統環境與設備皆能在安全穩定之狀態下正常運作或對外提供服務。

若機關之正式作業環境已與其他環境(如辦公室、開發、測試環境等)進行邏輯或實體區隔，請填選項 B，其邏輯區隔如放置於不同目錄、網域；實體區隔如放置於不同主機。若機關除正式作業環境已區隔外，開發、測試環境亦已進行部分邏輯或實體區隔，請填選項 C。

針對系統開發、測試、實作的環境與設備區隔，機關已訂定標準作業程序或相關文件化要求，並落實執行，請填選項 D。若機關已於標準作業程序或相關文件訂定系統開發、測試、實作的環境與設備區隔質化或量化衡量指標(如每年至少檢視 1 次系統開發、測試、實作的環境與設備區隔等)，並檢視執行成效，請填選項 E。針對系統開發、測試、實作的環境與設備區隔，機關已有精進流程或執行方式，請填選項 F。

自評人員請留意，本檢核項目之填答選項配分若達 3 分(含)以上，實施範圍應包含全機關。完整選項內容與填寫說明，詳見表 46。

表46 41.區隔系統開發、測試、實作的環境與設備

題號	檢核項目	選項編號	選項內容	選項配分	填寫說明
41	區隔系統開發、測試、實作的環境與設備	A	正式作業環境未與其他環境進行邏輯或實體區隔	0	▪邏輯區隔：如放置於不同目錄、網域 ▪實體區隔：如放置於不同主機 ▪選項配分達3分(含)以上者，實施範圍應包含全機關 ▪參考佐證資料 >系統開發、測試、實作的環境與設備區隔相關管理程序 >系統開發、測試、實作的環境與設備區隔檢視紀錄
		B	正式作業環境已與其他環境(如辦公室、開發、測試環境等)進行邏輯或實體區隔	1	
		C	除正式作業環境已區隔外，開發、測試環境亦已進行部分邏輯或實體區隔	2	
		D	針對系統開發、測試、實作的環境與設備區隔，已訂定標準作業程序或相關文件化要求，並落實執行	3	
		E	已訂定系統開發、測試、實作的環境與設備區隔質化或量化衡量指標(如每年至少檢視1次系統開發、測試、實作的環境與設備區隔等)，並檢視執行成效	4	
		F	針對系統開發、測試、實作的環境與設備區隔，精進流程或執行方式	5	

資料來源：本計畫整理

4. 資安治理成熟度評估系統

資安治理成熟度評估系統提供 A 級與 B 級公務機關每年上網填寫資安治理成熟度評估表，該系統開放時間為全年度(每年 1 月 1 日至 12 月 31 日)。

建議機關自評人員應具備以下其一先備知識，確保得以真實呈現機關之資安治理成熟度現況，如：

- 了解政府機關資安治理與資安管理概況。
- 具有基礎資通安全認知，或曾接受資通安全管理相關之培訓，如 ISO 27001 認知課程。
- 具有資通安全相關驗證資格人員，如 ISO 27001 主導稽核員。

4.1 資安治理成熟度評估系統自評流程

資安治理成熟度評估系統自評流程分為 3 階段，自評作業啟動、自評結果審核及自評作業完成(詳見圖 9)。以下介紹各階段之步驟：

- 步驟一、自評作業啟動

自評人員於資安治理成熟度評估系統首頁使用個人帳號登入，有關個人帳號註冊與登入方式，詳見附錄 1 資安聯絡人身分驗證機制操作手冊。

登入系統後，「未填寫」頁籤顯示一份當年度自評表，點選管理欄下方「填寫」鍵即可進行檢核項目填答。每一檢核項目皆有「填寫說明」鍵與「備忘錄」鍵。填寫說明提供自評人員於填寫選項答案時應注意之事項(如選項配分達 3 分(含)以上者，實施範圍應包含全機關等)；備忘錄提供自評人員記錄有關該檢核項目之相關資料或佐證資料。

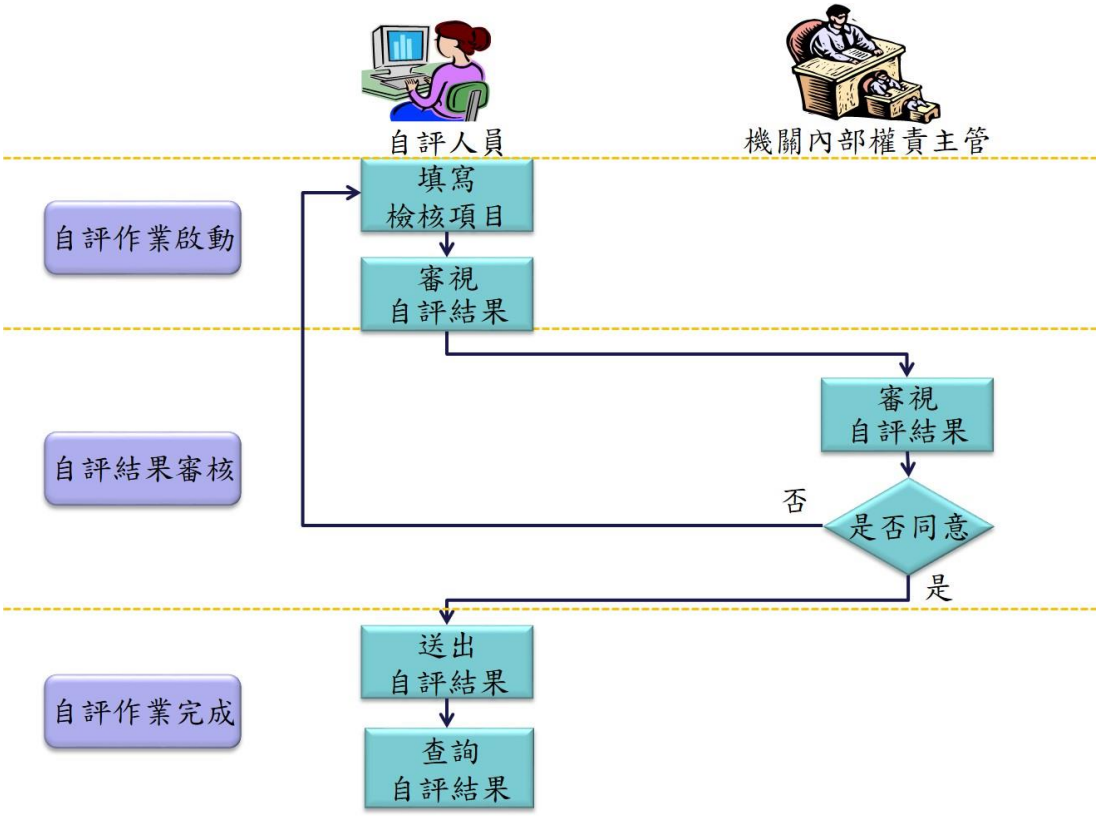
完成所有檢核項目填寫後，將網頁進行重新整理(F5)，未填寫頁籤之管理欄將會增加「檢視」鍵。點選該鍵後，自評人員可先檢視機關成熟度等級與確認各檢核項目之選項答案是否填寫正確。

●步驟二、自評結果審核

資安治理成熟度評估表需經機關內部權責主管核可，才能進行提交。為方便機關內部討論或呈核，自評人員可於資安治理成熟度評估系統\未填寫頁籤下之「檢視」鍵，下載「評估項目清單」與「評估結果清單」，以呈核機關內部權責主管。俟機關內部權責主管核可，自評人員再登入系統提交自評表。

●步驟三、自評作業完成

當年度之自評表提交後，該自評表將儲存至「已填寫」頁籤。若需修改自評表內容或選項答案，請來信或來電告知本中心該業務承辦人。承辦人將會將自評表退回，供機關自評人員進行調修。自評表修改完成後，先經機關內部權責主管核可，再由自評人員進行提交。



資料來源：本計畫整理

圖9　資安治理成熟度評估系統自評流程

4.2 資安治理成熟度評估系統功能說明

資安治理成熟度評估系統登入後，一般機關提供 5 個功能頁籤，包含未填寫、已填寫、常見問題集、下載專區及歷年資料；主管機關提供 8 個功能頁籤，包含未填寫、已填寫、常見問題集、下載專區、歷年資料、所屬機關未填寫、所屬機關未填寫及所屬機關統計。以下介紹各頁籤之功能，詳細內容詳見附錄 2 資安治理成熟度系統操作手冊。

●未填寫

本頁籤存放當年度自評表，尚未填完檢核項目時，管理欄僅顯示「填寫」與「下載」功能鍵。點選「填寫」鍵，瀏覽器將自動開啟另一網頁，供自評人員填寫自評表。如無法一次填完全部檢核項目，請於關閉網頁前進行存檔，以確保已填寫之檢核項目答案存入資料庫。點選「下載」鍵，可下載自評表電子檔，方便機關進行內部討論或呈核相關權責主管。全部檢核項目填寫完成，將網頁進行重新整理後，管理欄將顯示「檢視」功能鍵。該功能鍵供自評人員於正式提交自評表前，先檢視機關成熟度等級與確認各檢核項目之答案是否填寫正確。點選「檢視」鍵，瀏覽器將自動開啟另一網頁，該網頁顯示 4 個頁籤，分別為「評估項目清單」、「評估結果清單」、「評估結果分析圖」及「評估結果比較圖」。「評估項目清單」顯示整份自評表之題目、填寫結果及備忘錄內容，亦提供「下載評估項目清單」鍵，方便機關列印自評表進行討論與審核。「評估結果清單」呈現機關資安治理成熟度等級與各流程構面能力度等級，亦提供下載功能讓機關儲存與列印。「評估結果分析圖」以圖形化呈現各流程構面能力度等級，分別有長條圖與雷達圖，亦提供下載鍵供機關儲存與列印。「評估結果比較圖」提供機關查詢年度評估結果比較圖，機關自設比較之年度，以了解機關各流程構面是否逐年精進。

●已填寫

自評人員提交自評表後，當年度之自評表將放置在「已填寫」頁籤，管理欄存在「檢視」鍵，該鍵之功能與自評表未提交時於「未填寫」頁籤之檢視鍵相同。點選檢視鍵後，瀏覽器將自動開啟另一網頁，顯示「評估項目清單」、「評估結果清單」、「評估結果分析圖」及「評估結果比較圖」等 4 個頁籤。該 4 個頁籤之功能，請參閱上方「未填寫」頁籤之說明。

●常見問題集

提供使用者較為常見之問題與回答，常見問題分為三類：權限說明、使用說明及其他說明，使用者可依問題之方向，尋找是否存在相關答覆。

●下載專區

提供資安治理成熟度評估作業相關文件之下載，如資安治理成熟度機制說明、資安治理成熟度系統操作手冊、資安治理成熟度評估表及資安治理成熟度評估說明會簡報等。

●歷年資料

存放歷年已提交之自評表，該頁籤提供自評人員於每年填寫新年度自評長時，可參考歷年自評表，做為答題方向或依據。

若機關為主管機關，則會多顯示 3 個頁籤如下：

●所屬機關未填寫

若機關本身為主管機關身分，登入系統後將會看到該頁籤。主管機關可在此查詢所屬機關各年度未提交自評表之名單，以便追蹤所屬機關資安治理成熟度自評表填寫情形。

●所屬機關已填寫

若機關本身為主管機關身分，登入系統後將會看到該頁籤。主管機關可在此查詢所屬機關各年度提交自評表之情況，以利管理所屬機關資安治理成熟度評估之執行情形。

●所屬機關統計

若機關本身為主管機關身分，登入系統後將會看到該頁籤。主管機關可在此查詢所屬機關各年度成熟度等級與其機關數量之統計數據，以利了解所屬機關資安治理之落實程度。

5. 結論

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評估作業，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作業之落實，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通安全長，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，受評機關之上級管機關與資通安全署，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。

6. 參考文獻

[1]行政院資通安全處(109 年 4 月)。「109 年數位國家資通安全跨域聯防整合計畫委外辦理案」需求說明書。未出版。

[2]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.

[3]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.

[4]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.

[5]ISO(2008) ISO/IEC 21827－Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model.

[6]ISO(2015) ISO/IEC 33004－Information Technology－process assessment－Requirements for process reference, process assessment and maturity models.

[7]SEI(2002)CMMI－Capability Maturity Model Integration.

[8]ISO(2015) ISO/IEC 33020－Information technology－Process assessment－Process measurement framework for assessment of process capability.

[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.

7. 附件

附件 1 資安治理成熟度評估系統帳號申請操作手冊

附件 2 資安治理成熟度評估系統操作手冊