資訊系統分級與資安防護基準作業規定

行政院國家資通安全會報

中華民國 104 年 7 月修正

目錄

一、 目的

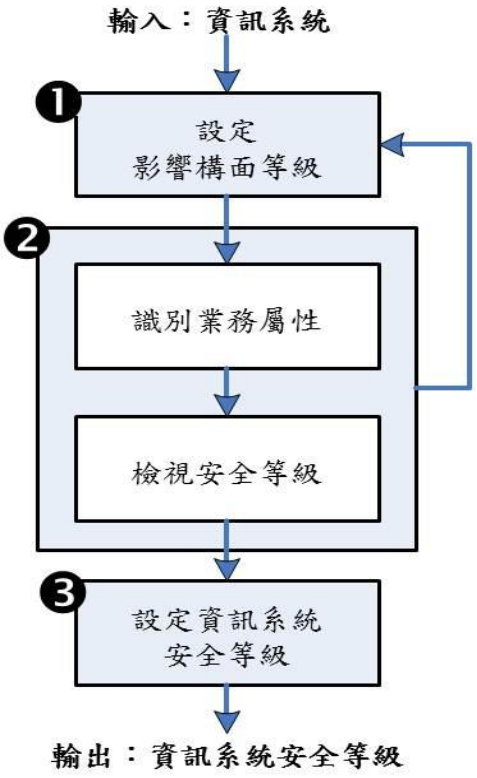
資訊系統分級與資安防護基準作業規定(以下簡稱本規定)旨在鑑別資訊系統安全等級，協助機關掌握重點保護標的，並促使機關進行風險評鑑、有效運用資源，採行適當安全控制措施，以確保資訊系統之安全防護水準。

二、 適用範圍

本規定適用於「政府機關（構）資通安全責任等級分級作業規定」應辦事項所律定對象之資訊系統。

三、 處理程序

處理程序如圖 1 所示，包含❶設定影響構面等級、❷識別業務屬性並檢視安全等級、❸設定資訊系統安全等級等三個處理步驟。



❶：由業務承辦人依機密性、完整性、可用性及法律遵循性四大影響構面，分別評估對各資訊系統之影響衝擊，並據以設定影響構面等級。

❷：識別資訊系統所支援之業務屬性，並由承辦單位主管檢視業務承辦人所設定安全等級之合理性。

❸：資訊系統安全等級經承辦單位主管、資訊主管確認後，最後由資訊安全長核定。

圖 1：資訊系統分級處理程序

各項資訊系統均須依循上述處理程序填寫「安全等級評估表」(參考範本如附件 1)，並由資訊單位彙整「資訊系統清冊」(參考範本如附件 2)。為確保系統分級符合機關安全需求，本處理程序須由業務承辦人、承辦單位主管、資安人員、資訊主管等相關人員會辦，最後由資訊安全長核定資訊系統安全等級。機關使用附件 1、2 參考範本時，宜依機關本身實際簽核流程調整簽核欄位。

本處理程序主要在協助機關設定資訊系統安全等級、掌握重點保護標的，以利機關辦理風險評鑑及執行防護基準。因此，機關每年度應至少檢視 1 次各項資訊系統分級妥適性。

另外，已通過資訊安全管理驗證（例如：ISO/IEC 27001、CNS 27001 等）機關，準用已採行之風險評鑑方法，須將資訊系統衝擊評估結果轉換為本規定之【普】、【中】、【高】三個安全等級。

四、 處理步驟說明

處理步驟說明如下表，請相關人員依處理步驟逐項填寫「安全等級評估表」，以設定資訊系統安全等級。附件 3 提供安全等級評估表參考範例，各機關可視實際情形參考使用。需要進行分級之資訊系統，以自行或委外開發之資訊系統為主。

套裝軟體、作業系統或防毒系統、防火牆系統、入侵偵測/防禦系統、弱點掃瞄系統、網頁/郵件內容過濾系統等屬資安防護處理相關控制措施，均不需進行資訊系統分級。

處理程序	工作項目	相關人員
輸入： 資訊系統	• 輸入資訊系統。	承辦單位主管（或其授權人員）
步驟❶：	• 由業務承辦人評估當發生資安事件時，對機密	業務承辦

處理程序	工作項目	相關人員
設定影響構面等級	性、完整性、可用性及法律遵循性四大影響構面之衝擊程度，並參照「五、安全等級設定原則」填寫影響構面安全等級，安全等級區分為【普】、【中】、【高】三級，對於不適用之影響構面，安全等級以 NA (Not Applicable)表示。 ● 資訊系統之安全等級，取其四大影響構面安全等級最高者。	人
步驟❷： 1.識別業務屬性 2.檢視安全等級	● 識別資訊系統之業務屬性，並由承辦單位主管檢視設定安全等級之合理性。 ● 資訊系統依其支援之單位及業務屬性，分為行政與業務二類，說明如下： ◇ **行政類：** 指機關內部輔助單位之業務（如：人事、薪資等），惟若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別。 ◇ **業務類：**指機關內部業務單位之業務（如：交通監理、便民服務等）。 ● 本步驟所進行各項異動均須記錄異動原因。	承辦單位主管（或其授權人員）
步驟❸： 核定資訊系統安全等級	● 由資訊單位綜整各資訊系統「安全等級評估表」中資訊，併同**共同性系統**(不需填安全等級)，彙整至「資訊系統清冊」，資訊系統安全等級經相關主管確認後，最後由資訊安全長核定。**共同性系統之分級，統一由開發管理之機關進行評估與鑑別**。 ● 本步驟所指之**共同性系統**，包含共用性系統與共通性系統，共用性系統指單一機關主責系統開發與資料管理，其餘機關僅涉及使用操作，如國稅系統。共通性系統指單一機關主責系統開發與規格制訂，其餘機關除使用操作外，資	資訊安全長、相關主管、資訊人員

處理程序	工作項目	相關人員
	料主要儲存於使用機關，如公文電子交換系統。	
輸出： 資訊系統安全等級	• 本程序所設定之資訊系統安全等級，將作為後續執行防護基準之依據。 • 資訊系統安全等級列【高】者，可考量進一步實施詳細風險評鑑，俾利進行風險管理。	

五、 安全等級設定原則

安全等級分為【普】、【中】、【高】三級，由機關依機密性、完整性、可用性及法律遵循性四大影響構面，分別考量資訊系統於發生資安事件時可能造成之衝擊，即衡量資訊系統資料外洩、資料遭竄改、系統故障等情事時可能造成的後果嚴重程度，並據以評估、設定安全等級。

資訊系統於發生資安事件時，通常會同時衝擊多個影響構面。當資訊系統發生資料外洩時，可能衝擊「機密性」、「完整性」、「法律遵循性」等影響構面；當資訊系統發生資料遭竄改情形時，可能衝擊「機密性」、「完整性」、「法律遵循性」影響構面；而當資訊系統發生系統故障情形時，則可能衝擊「可用性」、「法律遵循性」等影響構面。此外，若系統發生資安事件時，對於某個影響構面不造成任何危害，則該影響構面安全等級以 NA 表示不適用。

各影響構面安全等級設定原則說明如下：

(一) 影響構面「機密性」

資訊系統發生資安事件時，可能造成系統資料外洩或遭竄改等情事，導致資料機密性受到損害。

「機密性」影響構面安全等級設定原則如下：

安全等級	說　明

安全等級	說　明
普	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： ● 一般性資料；資料外洩不致影響機關權益或僅導致機關權益輕微受損。
中	未經授權的資訊揭露，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： ● 敏感性資料；資料外洩將導致機關權益嚴重受損。 ▫ 涉及區域性或地區性個人資料，包含出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。
高	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： ● 機密性資料；資料外洩將危及國家安全、導致機關權益非常嚴重受損。 ▫ 凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療等重要機敏系統。 ▫ 特殊屬性之個人資料（如：臥底警員、受保護證人、被害人等資料），資料外洩可能會使相關個人身心受到危害、社會地位受到損害、或衍生財物損失等情形。 ▫ 涉及個人之醫療、基因、性生活、健康檢查、犯罪前科等資料，資料外洩將使個人權益非常嚴重受損。例如：醫療資訊系統、刑案

安全等級	說　明
	資訊整合系統等。 ▫ 涉及全國性個人資料，包含出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。例如：戶役政資訊系統、護照管理系統等。

(二) 影響構面「完整性」

資訊系統委外開發與營運時，若未有效執行資安防護作為，可能會造成系統完整性遭受破壞。

「完整性」影響構面安全等級設定原則如下：

安全等級	說　明
普	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： ● 資料遭竄改不致影響機關權益或僅導致機關權益輕微受損。
中	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： ● 資料遭竄改將導致機關權益嚴重受損。
高	未經授權之資訊修改或破壞，在機關、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： ● 資料遭竄改將危及國家安全、導致機關權益非常嚴重受損。

(三) 影響構面「可用性」

資訊系統目的在輔助機關提升業務效能與服務品質，已成為機關業務運作不可或缺的一環，因此，系統故障（包含無法使用、異常運作等情形）可能導致業務執行效能降低，甚至業務中斷。

機關評估本影響構面安全等級時，應考量資訊系統可容許中斷時間、服務受影響程度等。一般而言，行政類系統（例如：人事管理系統、會計系統等）等，於系統故障時通常不致造成機關業務執行效能嚴重降低或業務中斷。

「可用性」影響構面安全等級設定原則如下：

安全等級	說　明
普	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： ● 系統容許中斷時間較長（如：72 小時）。 ● 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響。 ● 系統故障造成機關業務執行效能輕微降低。
中	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： ● 系統容許中斷時間短。 ● 系統故障對社會秩序、民生體系運作將造成嚴重影響。 ● 系統故障造成機關業務執行效能嚴重降低。
高	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如：

安全等級	說　明
	● 系統容許中斷時間非常短（如：30 分鐘）。 ● 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全。 ● 系統故障造成機關業務執行效能非常嚴重降低，甚至業務停頓。

(四) 影響構面「法律遵循性」

本影響構面之危害程度評估係基於機關負有遵守法律規章之責任與義務下，如發生違法情事時，機關將面臨之衝擊，本影響構面衝擊後果之嚴重程度係取決於法令規定。

政府機關依法行事，資訊使用原則上應至少符合智慧財產權相關法令，資訊於網路揭露也應遵循「兒童及少年福利與權益保障法」及其相關規定。

「影響法律規章遵循」影響構面安全等級設定原則如下：

安全等級	說　明
普	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之有限負面影響，如： ● **全球資訊網：**必須符合智慧財產權相關法令尊重他人智慧財產，並遵守兒童及少年福利與權益保障法進行資訊內容管理，否則將涉及違反法律之遵循性。
中	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之嚴重負面影響，如： ● **政府電子採購網：**依「政府採購法」第 27 條

安全等級	說　明
	規定，機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化。
高	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之非常嚴重或災難性負面影響，如： • **機密性資料**：依「國家機密保護法施行細則」第 28 條第 4 款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。 • **醫療機構醫囑暨電子病歷系統**：依「醫療機構電子病歷製作及管理辦法」第 3 條、第 4 條規定，電子病歷資訊系統之建置、電子病歷之製作及儲存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。

六、 防護基準選取

機關完成資訊系統分級後，應依資訊系統【高】、【中】、【普】等級，執行相對應之防護基準。即【高】等級資訊系統執行高等級防護措施，【中】、【普】等級資訊系統，則執行【中】、【普】等級防護措施。機關可依其資源，調整控制措施之優先順序。

詳細防護基準，說明如下：

控制措施	安全等級			參考文件
	普	中	高	
存取控制(Access Control)(3)				
帳號管理 (Account Management)	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	1. 執行等級「普」之所有控制措施。 2. 資訊系統已逾期之臨時或緊急帳號應刪除或禁用。 3. 應禁用資訊系統閒置帳號。 4. 應定期審核資訊系統帳號之建立、修改、啟用、禁用及刪除動作。	1. 執行等級「中」之所有控制措施。 2. 當超過機關所規定之預期閒置時間或可使用期限時，系統應自動將使用者登出。 3. 資訊系統應依照機關所規定之情況及條件(如上班時間或指定 IP 來源)，使用資訊系統。 4. 監控資訊系統帳號以發現違常使用，並於發現帳號違常使用時回報管理者。	安全控制措施參考指引附件 4 AC-2
最小權限 (Least Privilege)		1. 採用最小權限原則，只允許使用者(或代表使	執行等級「中」之所有控	安全控制措施參考指引附件

控制措施	安全等級			參考文件
	普	中	高	
		用者行為的程序)依據機關任務和業務功能，完成指派任務所需之授權存取。 2. 應稽核資訊系統管理者帳號所執行之各項功能。	制措施。	4 AC-6
遠端存取 (Remote Access)	對於每一種允許之遠端存取類型，都應先取得授權，建立使用限制、組態需求、連線需求及文件化。	1. 執行等級「普」之所有控制措施。 2. 應監控資訊系統遠端連線。 3. 資訊系統應實作加密機制來保護遠端存取連線的機密性。 4. 資訊系統遠端存取之來源應為機關已預先定義及管理之存取控制點。	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 4 AC-17

控制措施	安全等級			參考文件
	普	中	高	
		5. 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。		
稽核與可歸責性(Audit and Accountability)(6)				
稽核事件 (Audit Events)	1. 依律定之時間週期及紀錄留存政策，保留稽核紀錄，並滿足法規要求。 2. 確保資訊系統有稽核特定事件(如更改密碼、登錄失敗、資訊系統存取失敗)之能力，並決定有哪些特定事件在資訊系統中應該被稽核。	1. 執行等級「普」之所有控制措施。 2. 應定期審查稽核事件。	執行等級「中」之所有控制措施。	安全控制措施參考指引附件6 AU-2
稽核紀錄內容 (Content of Audit Records)	資訊系統產生之稽核紀錄至少應包含以下資訊：事件類型、何時發生、何處	1. 執行等級「普」之所有控制措施。 2. 資訊系統產生的稽核紀	執行等級「中」之所有控制措施。	安全控制措施參考指引附件6 AU-3

控制措施	安全等級			參考文件
	普	中	高	
	發生及任何與事件相關之使用者之身分識別。	錄，應依需求納入額外的資訊。		
稽核儲存容量 (Audit Storage Capacity)	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。	執行等級「普」之所有控制措施。	執行等級「普」之所有控制措施。	安全控制措施參考指引附件 6 AU-4
稽核處理失效之回應 (Response to Audit Processing Failures)	資訊系統應在稽核處理失效(如儲存容量不足)之情況下，採取適當之行動，例如：關閉資訊系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等。	執行等級「普」之所有控制措施。	1. 執行等級「普」之所有控制措施。 2. 當機關規定需要即時通報的稽核失效事件發生時，資訊系統應在機關規定之時效內，對機關特定之人員、角色提出告警。	安全控制措施參考指引附件 6 AU-5
時戳 (Time Stamps)	資訊系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對映到世界協	1. 執行等級「普」之所有控制措施。 2. 系統內部時鐘對基準時	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 6 AU-8

控制措施	安全等級			參考文件
	普	中	高	
	調時間(UTC)或格林威治標準時間(GMT)。	間源的時間差大於機關規定之時間週期時應予同步。		
稽核資訊之保護 (Protection of Audit Information)	對稽核紀錄之存取管理，僅限於有權限之使用者。	執行等級「普」之所有控制措施。	1. 執行等級「中」之所有控制措施。 2. 定期備份稽核紀錄到與原稽核系統不同之實體系統 (如 Log 伺服器)。 3. 運用加密機制，以保護稽核資訊之完整性。	安全控制措施參考指引附件 6 AU-9
營運持續計畫(Contingency Planning)(2)				
資訊系統備份 (Information System Backup)	1. 訂定系統可容忍資料損失之時間要求 2. 執行系統源碼與資料備份。	1. 執行等級「普」之所有控制措施。 2. 應定期測試備份資訊來驗證備份媒體之可靠性及資訊之完整性。	1. 執行等級「中」之所有控制措施。 2. 應將備份還原，做為營運持續計畫測試之一部分。	安全控制措施參考指引附件 9 CP-9 電腦機房異地備援機制參考指引

控制措施	安全等級			參考文件
	普	中	高	
			3. 應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資訊系統軟體與其他安全相關資訊之備份拷貝。	
資訊系統備援 (Redundancy of Information Systems)		1. 訂定資訊系統從中斷後至重新恢復服務之可容忍時間要求 2. 當原服務中斷，由備援設備取代提供服務。	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 9 CP-9 電腦機房異地備援機制參考指引
識別與鑑別(Identification and Authentication)(5)				
使用者之識別與鑑別 (Identification and Authentication)	資訊系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)，不應有共用帳號之行為。	執行等級「普」之所有控制措施。	1. 執行等級「普」之所有控制措施。 2. 對帳號之網路或本機存取採取多重認證技術(如鎖 IP)。	安全控制措施參考指引附件 10 IA-2

控制措施	安全等級			參考文件
	普	中	高	
裝置之識別與鑑別 (Device Identification and Authentication)			資訊系統在建立連線前，應識別允許存取之特定來源(如 IP)。	安全控制措施參考指引附件 10 IA-3
鑑別資訊管理 (Authenticator Management)	使用預設密碼登入系統時，應於登入後要求立即變更。	1. 執行等級「普」之所有控制措施。 2. 基於通行碼之鑑別資訊系統應強制最低通行碼複雜度；強制新的通行碼最少變更之字元數；強制通行碼最短及最長之效期限制。	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 10 IA-5
鑑別資訊回饋 (Authenticator Feedback)	資訊系統應遮蔽在鑑別過程中之資訊(如通行碼)，以防止未授權之使用者可能之窺探/使用。	執行等級「普」之所有控制措施。	執行等級「普」之所有控制措施。	安全控制措施參考指引附件 10 IA-6
加密模組鑑別 (Cryptographic Module		資訊系統若以通行碼進行鑑別時，該通行碼應加密儲存與處理。	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 10 IA-7

控制措施	安全等級			參考文件
	普	中	高	
Authentication)				
系統與服務獲得(System and Services Acquisition)(8)				
系統發展生命週期需求階段 (System Development Life Cycle-Requirement)	針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認。	執行等級「普」之所有控制措施。	執行等級「普」之所有控制措施。	安全控制措施參考指引附件 18 SA 安全軟體發展流程參考指引 3.1 安全軟體需求
系統發展生命週期設計階段 (System Development Life Cycle-Design)		1. 應根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估。 2. 將風險評估結果回饋需求階段的檢核項目，並	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 18 SA 安全軟體發展流程參考指引 3.2 安全軟體設計

控制措施	安全等級			參考文件
	普	中	高	
		提出安全需求修正。		
系統發展生命週期開發階段 (System Development Life Cycle-Develop)	1.應針對安全需求實作必要控制措施。 2.應注意避免軟體常見漏洞(如 OWASP TOP 10)及實作必要控制措施。	執行等級「普」之所有控制措施。	1.執行等級「普」之所有控制措施。 2.執行「源碼掃描」安全檢測。	安全控制措施參考指引附件 18 SA 安全軟體發展流程參考指引 3.3 安全軟體開發
系統發展生命週期測試階段 (System Development Life Cycle-Test)	執行「弱點掃描」安全檢測。	執行等級「普」之所有控制措施。	1.執行等級「普」之所有控制措施。 2.執行「滲透測試」安全檢測。	安全控制措施參考指引附件 18 SA 安全軟體發展流程參考指引

控制措施	安全等級			參考文件
	普	中	高	
				3.4 安全軟體測試
系統發展生命週期部署與維運階段 (System Development Life Cycle-Deployment and Maintenance)	在部署環境中應針對相關資安威脅，進行更新與修補。	1. 執行等級「普」之所有控制措施。 2. 在系統發展生命週期之維運階段需要注重版本控制與變更管理。	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 18 SA 安全軟體發展流程參考指引 3.5 安全軟體部署與維運
系統發展生命週期委外階段 (System Development Life Cycle-Outsourcing)	資訊系統開發若委外服務應將系統發展生命週期各階段依安全等級將安全需求(含機密性、可用性、完整性)納入委外合約。	執行等級「普」之所有控制措施。	執行等級「普」之所有控制措施。	安全控制措施參考指引附件 18 SA 安全軟體發展流程參考指引 3.6 安全軟體委外開發管理

控制措施	安全等級			參考文件
	普	中	高	
獲得程序 (Acquisition Process)		開發、測試以及正式作業環境應作區隔。	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 18 SA 安全軟體發展流程參考指引 3.3.3 安全開發環境
資訊系統文件 (Information System Documentation)	應儲存與管理系統發展生命週期之相關文件。	執行等級「普」之所有控制措施。	執行等級「普」之所有控制措施。	安全控制措施參考指引附件 18 SA 安全軟體發展流程參考指引
系統與通訊保護(System and Communications Protection)(2)				
傳輸之機密性與完整性 (Transmission Confidentiality and Integrity)			1. 傳輸過程中除非有其他替代之實體保護措施，否則資訊系統應實作加密機制以防止未授權之資訊揭露或偵測資訊之	安全控制措施參考指引附件 19 SC-8

控制措施	安全等級			參考文件
	普	中	高	
			變更。	
資料儲存之安全 (Protection of Information at Rest)			機密資訊應加密儲存	安全控制措施參考指引附件 19 SC-28
系統與資訊完整性(System and Information Integrity)(3)				
漏洞修復 (Flaw Remediation)	系統的漏洞修復應測試有效性及潛在影響，並依律定之時間週期更新。	1. 執行等級「普」之所有控制措施。 2. 定期確認資訊系統相關漏洞修復之狀態。	執行等級「中」之所有控制措施。	安全控制措施參考指引附件 20 SI-2
資訊系統監控 (Information System Monitoring)	發現資訊系統有被入侵跡象時，應通報機關特定人員。	1. 執行等級「普」之所有控制措施。 2. 監控資訊系統，以偵測攻擊和未授權之連線，並識別資訊系統之未授權使用。	1. 執行等級「中」之所有控制措施。 2. 資訊系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時針對該事件進行分析。	安全控制措施參考指引附件 20 SI-4

控制措施	安全等級			參考文件
	普	中	高	
軟體及資訊完整性 (Software, Firmware, and Information Integrity)		1. 使用完整性驗證工具以偵測未授權變更特定軟體及資訊。 2. 當發現違反完整性時，資訊系統應實施機關指定之安全保護措施。	1. 執行等級「中」之所有控制措施。 2. 應定期執行軟體和資訊完整性檢查。	安全控制措施參考指引附件 20 SI-7

附件 1：安全等級評估表

表單編號：

「ＯＯＯ資訊系統」安全等級評估表

功能說明：

業務屬性：　□行政類□業務類　　日期：___年___月___日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
		資訊系統安全等級：		

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估		
	異動		
2. 完整性	初估		
	異動		
3. 可用性	初估		
	異動		
4. 法律遵循性	初估		
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估		
	異動		

備註	

承辦人	複核人員(1)	複核人員(2)	複核人員(3)	承辦單位主管

註：請各機關依本身實際陳核流程調整簽核欄位。

附件 2：資訊系統清冊

表單編號：

資訊系統清冊

彙整日期：　　年　　月　　日

編號	資訊系統名稱	業務屬性	資訊系統安全等級	共同性系統(Y/N)	承辦(管理)單位	備註
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

承辦(填報)單位	審核	決行

註：請各機關依本身實際陳核流程調整簽核欄位。

附件 3：安全等級評估表參考範例

(一) 停車管理系統

「停車管理系統(參考範例)」安全等級評估表

功能說明：提供停車場所查詢，以及汽機車未繳費資料查詢線上服務。

業務屬性：□行政類■業務類 **日期：__年__月__日**

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	高	普	中	高
		資訊系統安全等級：		高

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	本系統資料屬敏感性資料，資料保護不當，將遭受一定程度之影響
	異動		
2. 完整性	初估	高	本系統目的在提供車輛未繳費資料查詢服務，若資料未妥適保存或發生資安事件造成資料外洩，可能造成資料完整性受損
	異動		
3. 可用性	初估	普	本系統容許中斷時間較長(超過 24 小時)，且服務中斷不致影響業務運作
	異動		
4. 法律遵循性	初估	中	本系統資料包含車號與未繳費資料明細等，應依「個人資料保護法」規定辦理
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	業務類	本系統提供汽機車未繳費資料查詢等對外資訊服務，屬機關業務類系統
	異動		

備註	

(二) 全球資訊網

「全球資訊網(參考範例)」安全等級評估表

功能說明：機關官方網站，提供機關簡介及政策措施介紹，並無提供線上申辦等服務。

業務屬性：□行政類■業務類　　日期：__年__月__日

影響構面				資訊系統安全等級
1.機密性	2.完整性	3.可用性	4.法律遵循性	
普	普	普	普	普
		資訊系統安全等級：		普

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1.機密性	初估	普	網站資訊均為可公開之一般性資料
	異動		
2.完整性	初估	普	本網站主要提供資訊公告
	異動		
3.可用性	初估	普	本網站提供一般性資料瀏覽
	異動		
4.法律遵循性	初估	普	本網站必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及其相關規定，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	業務類	本系統提供機關簡介、政策措施介紹等對外資訊服務，無涉及機關業務線上申辦等其他服務，屬機關業務類系統
	異動		

備註	

(三) 人事管理系統

「人事管理系統(參考範例)」安全等級評估表

功能說明：提供機關同仁進行差勤線上申請，以及人事單位進行相關人事差勤管理。

業務屬性：■行政類□業務類　　日期：__年__月__日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	普	普	普	中
		資訊系統安全等級：		中

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	本系統資料屬敏感性資料，資料保護不當，將遭受一定程度之影響
	異動		
2. 完整性	初估	普	本系統目的在提供人事管理服務，不對外提供服務，若個人資料未妥適保存或發生資安事件造成資料外洩，可能造成資料完整性受損
	異動		
3. 可用性	初估	普	本系統容許中斷時間較長(超過 24 小時)，且服務中斷不致影響業務運作
	異動		
4. 法律遵循性	初估	普	本系統包含同仁基本個人資料，應依「個人資料保護法」規定辦理；惟資料筆數不多，且多屬個人基本資料，評估若未完成遵循個人資料保護法辦理資料保護，可能伴隨輕微不良後果
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	行政類	本系統支援機關內部人事管理屬行政類資訊系統
	異動		

備註	

(四) 會計管理系統

「會計管理系統(參考範例)」安全等級評估表

功能說明：提供機關會計人員進行會計帳務作業及管理。

業務屬性：■行政類□業務類 **日期：__年__月__日**

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	普	普	中	中
		資訊系統安全等級：		中

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	系統包含本機關收入、支出明細資料，屬敏感資料
	異動		
2. 完整性	初估	普	本系統目的在提供會計帳務管理，本系統不對外提供服務，惟會計帳務屬敏感性資料，若遭入侵完整性可能會有影響
	異動		
3. 可用性	初估	普	本系統容許中斷時間較長(超過 24 小時)，且服務中斷不致影響業務運作
	異動		
4. 法律遵循性	初估	中	會計系統資料包含受款人資料(包含姓名、戶籍地址、身分證字號、金融帳號等)及帳務往來明細等，應依「個人資料保護法」規定辦理
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	行政類	本系統支援機關內部會計管理屬行政類資訊系統
	異動		

備註	