「資訊系統分級與資安防護基準作業規定」介紹

國家資通安全會報 技術服務中心

大綱

- 推動歷程
- 修訂重點說明
- 執行作業
- 處理程序
- 設定影響構面
- 識別業務屬性與檢視安全等級
- 核定資訊系統安全等級
- 防護基準選取
- 注意事項

推動歷程

- 99年訂定「資訊系統分類分級與鑑別機制參考手冊」，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
- 因應資訊科技發展及資通安全威脅趨勢，檢討修訂政府機關資安責任等級、資訊系統分級作業及其防護基準，完善國家整體資安防護體系

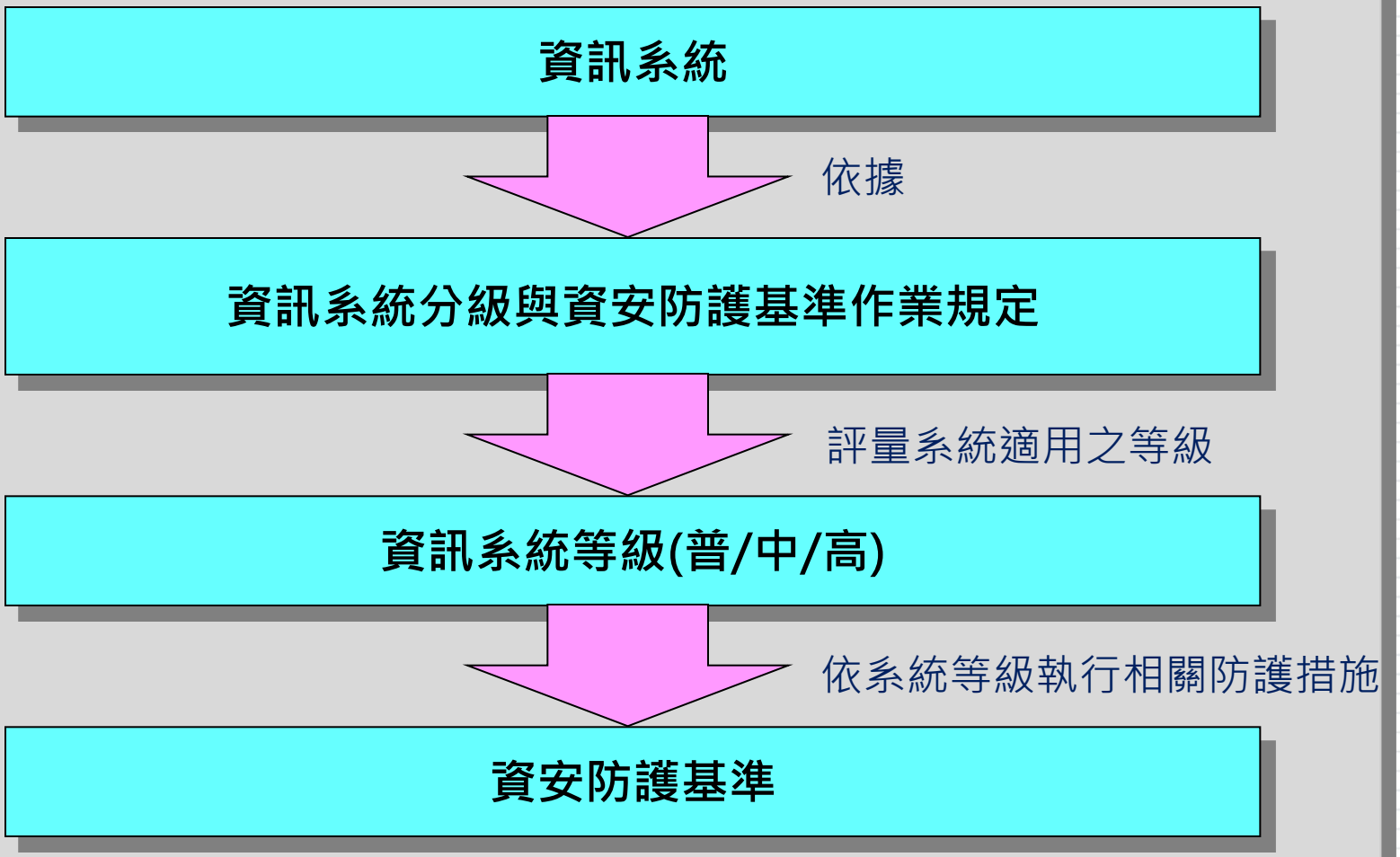
修訂重點說明(1/2)

名稱 / 差異性	原計畫名稱或內容	修訂建議
調整名稱	資訊系統分類分級與鑑別機制參考手冊	依行政規則名稱訂定原則，修訂為「資訊系統分級與資安防護基準作業規定」
簡化資訊系統分級處理程序	資訊系統先參照「行政院施政分類架構」之施政分類，識別資訊類別，再針對所選擇之各項資訊類別進行系統安全等級評估 評估程序包含識別資訊類別、設定影響構面等級、識別業務屬性與檢視安全等級及核定資訊系統安全等級	因資訊分類與系統安全等級無直接關聯性，因此簡化分級處理程序，資訊系統不分類，直接進行系統安全等級評估 評估程序包含設定影響構面等級、識別業務屬性與檢視安全等級及核定資訊系統安全等級

修訂重點說明(2/2)

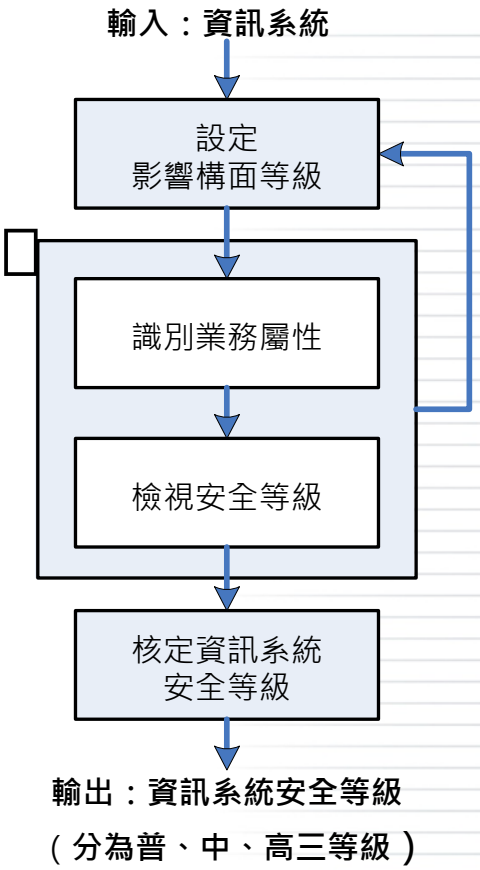
名稱 差異性	原計畫名稱或內容	修訂建議
簡化影響構面	影響構面包含資料保護受到損害、影響業務運作、影響法律規章遵循、人員傷亡、損害組織信譽及其他等六大構面	原影響構面均可歸納為資訊安全管理要件(機密性、完整性、可用性)與法律遵循性。因此簡化影響構面，調整為機密性、完整性、可用性及法律遵循性等四大構面
調整資訊系統之業務屬性	資訊系統依其服務之業務屬性分為行政性業務、關鍵性業務、支援性業務等三類	資訊系統依其業務屬性，分為行政與業務二類
增訂資訊系統資安防護基準	未規劃	參考「安全控制措施參考指引」之控制措施執行優先順序，以及美國NIST “Framework for Improving Critical Infrastructure Cybersecurity”，增訂資訊系統資安防護基準

執行作業


資訊系統
依據
資訊系統分級與資安防護基準作業規定
評量系統適用之等級
資訊系統等級(普/中/高)
依系統等級執行相關防護措施
資安防護基準

處理程序

- 各資訊系統均須依循處理程序填寫「安全等級評估表」
- **步驟❶**：依**機密性、完整性、可用性及法律遵循性**四大構面，分別評估對各資訊系統(不含共同性系統)之影響衝擊，並設定影響構面等級，依資訊系統填寫「安全等級評估表」
- **步驟❷**：依據資訊系統支援之業務屬性（分為**行政與業務**二類），檢視安全等級之合理性
- **步驟❸**：由資訊單位將各資訊系統「安全等級評估表」中資訊，併同**共同性系統**，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，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。



1. 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，資料主要儲存於使用機關，如電子公文交換系統。
2. 行政類：指機關內部輔助單位之業務(如：人事、薪資等)，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
3. 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）

影響構面(1/3)

構面 \ 等級	普級	中級	高級
1.機密性	未經授權的資訊揭露，在機關營運、資產或信譽等方面造成輕微之負面影響，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。	未經授權的資訊揭露，在機關營運、資產或信譽等方面，造成嚴重之負面影響，如： 敏感性資料；資料外洩將導致機關權益嚴重受損。 涉及個人出生年月日、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。	未經授權的資訊揭露，在機關營運、資產或信譽等方面，造成非常嚴重或災難性之負面影響，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。 極大規模（如：全國性）之涉及識別個人之資料。例如：戶役政資訊系統、護照管理系統等。

影響構面(2/3)

構面 \ 等級	普級	中級	高級
2.完整性	未經授權的資訊修改或破壞，在機關營運、資產或信譽等方面，造成輕微之負面影響，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。	未經授權的資訊修改或破壞，在機關營運、資產或信譽等方面，造成嚴重之負面影響，如：資料遭竄改將導致機關權益嚴重受損。	未經授權的資訊修改或破壞，在機關、資產或信譽等方面，造成非常嚴重或災難性之負面影響，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。
3.可用性	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，造成輕微之負面影響，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。	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，造成嚴重之負面影響，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。	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，造成非常嚴重或災難性之負面影響，如： 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。

影響構面(3/3)

構面＼等級	普級	中級	高級
4.法律遵循性	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，造成輕微之負面影響，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結晶，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。	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，造成嚴重之負面影響，如： 政府電子採購網：依「政府採購法」第27條規定，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。	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，造成非常嚴重或災難性之負面影響，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。

步驟❶ ：設定影響構面等級

「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：■業務　□行政性業務　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

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、電腦網路內容分級處理辦法，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 ：識別業務屬性與檢視安全等級(1/2)

- 檢視安全等級合理性之範例：
  - 於步驟❷，識別業務屬性為業務類，惟於步驟❶設定資訊系統安全等級為「普」級
  - 於步驟❷，識別業務屬性為行政類，惟於步驟❶設定資訊系統安全等級為「高」級
- 如有前述情形發生，則建議機關就其合理性進一步討論，如經討論確有該情形，則宜備註說明原因

步驟❷ ：識別業務屬性與檢視安全等級(2/2)

「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：■核心業務　□行政性業務　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

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

步驟❸ ：核定資訊系統安全等級

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)	承辦單位	備註
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						

設定完成資訊系統安全等級後，由資訊單位綜整各項資訊系統「安全等級評估表」，並製作「資訊系統清冊」，經簽核程序由資訊安全長核定安全等級

資訊單位	複核主管	資訊安全長

註：請各機關依本身實際陳核流程調整簽核欄位，如：複核主管調整為主任秘書等

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
存取控制Access Control				
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

資安防護基準選取

- 機關完成資訊系統分級後，依照資訊系統【高】、【中】、【普】等級，執行相對應之資安防護基準。

控制措施	安全等級			
	普	中	高	參考文件
存取控制Access Control				
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

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
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	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-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 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	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

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
稽核與可歸責性(Audit and Accountability)				
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、何處發生及任何與事件相關之使用者之身分識別	1. 執行等級「普」之所有控制措施 2. 資訊系統產生的稽核紀錄，應依需求納入額外的資訊	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
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

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
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調時間(UTC)或格林威治標準時間(GMT)	1. 執行等級「普」之所有控制措施 2. 系統內部時鐘對基準時間源的時間差大於機關規定之時間週期時應予同步	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
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)				
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

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
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)				
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
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

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
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 Authentication)		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
系統與服務獲得(System and Services Acquisition)				
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

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
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，並提出安全需求修正	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
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 3.4安全軟體測試

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
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
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

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
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)				
傳輸之機密性與完整性(Transmission Confidentiality and Integrity)			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變更	安全控制措施參考指引 附件19 SC-8
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

資安防護基準選取

控制措施	安全等級			
	普	中	高	參考文件
系統與資訊完整性(System and Information Integrity)				
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
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

注意事項(1/2)

- 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
- 已通過資訊安全管理驗證（例如：ISO/IEC 27001、CNS 27001等）之機關，準用已採行之風險評鑑方法，轉換為【普】、【中】、【高】三個安全等級
- 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

注意事項(2/2)

- 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
- 作業規定之附件已提供安全等級評估表參考範例，各機關仍應依實際情形，評估資訊系統等級

報告完畢
敬請指教