資安法資訊系統分級分類及防護基準說明

八月 2021

pwc 資誠

前言

資通安全管理法（資安法）

105/8/31
完成草案修訂

資通安全管理法草案

辦理座談會

刪除爭議條文

105/10/13公布

個人資料保護法調修版

辦理子法草案座談會

107/5/11
立法院三讀通過

資通安全管理法

107/6/6
總統府正式公布

資通安全管理法

108/1/1
行政院公告
正式實施

資通安全管理法及相關子法

107/11/21 行政院訂定發布相關子法

《資通安全管理法施行細則》
《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》
《特定非公務機關資通安全維護計畫實施情形稽核辦法》
《資通安全情資分享辦法》
《公務機關所屬人員資通安全事項獎懲辦法》

資通安全管理法

資通安全管理法

資通安全管理法施行細則

- 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
- 特定非公務機關資通安全維護計畫實施情形稽核辦法
- 資通安全情資分享辦法
- 公務機關所屬人員資通安全事項獎懲辦法
- 資安維護計畫範本
- 公務機關資通安全事件通報應變程序範本
- 特定非公務機關資通安全事件通報應變程序範本

納管對象

公務機關	非 公 務 機 關	
• 中央與地方機關 • 行政法人	關鍵基礎設施提供者	• 非關鍵基礎設施之公營事業 • 政府捐助達一定比例之財團法人

對人民生活、經濟活動及公眾或國家安全有重大影響者

資通安全責任等級分級原則

A級

全國性

- 全國性民眾或公務員個人資料檔案
- 外交、國防或國土安全事項
- 公務機關涉全國性之能源、水、通訊傳播、交通、銀行與金融、緊急救援
- 關鍵基礎設施提供者
- 全國性民眾服務資通系統之維運
- 全國性跨公務機關共用性資通系統之維運
- 公立醫學中心

區域或地區性

- 區域性或地區性民眾個人資料檔案
- 公務機關所捐助或研發之敏感科學
- 技術資訊安全維護管理
- 公務機關涉及區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項
- 關鍵基礎設施提供者
- 區域性或地區性民眾服務資通系統維運
- 區域性或地區性跨公務機關共用性資通系統維運
- 公立區域醫院

B級

資通安全責任等級分級原則

C級

自行或委外發資訊系統，並設置伺服器者

D級

未自行或委外開發資訊系統，未設置伺服器

E級

全部資訊業務由其他機關兼辦或代辦

國立大專院校資安責任等級

- 資通安全責任等級分級辦法第三條
- 行政院直屬機關應每二年提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，報主管機關核定。
- 教育部來函將國立大專院校資安責任等級列為B級。

資通安全責任等級B級之公務機關應辦事項-管理面

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，配置二人；須以專職人員配置之
	內部資通安全稽核		每年辦理一次
	業務持續運作演練		全部核心資通系統每二年辦理一次。
	資安治理成熟度評估		每年辦理一次。

資通安全責任等級B級之公務機關應辦事項-管理面

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	限制使用危害國家資通安全產品		一、 除因業務需求且無其他替代方案外，不得採購及使用主管機關核定之廠商生產、研發、製造或提供之危害國家資通安全產品。 二、 必須採購或使用危害國家資通安全產品時，應具體敘明理由，經主管機關核可後，以專案方式購置。 三、 對本辦法修正施行前已使用或因業務需求且無其他替代方案經主管機關核可採購之危害國家資通安全產品，應列冊管理，且不得與公務網路環境介接。

資通安全責任等級B級之公務機關應辦事項-技術面(1/2)

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次
		系統滲透測試	全部核心資通系統每二年辦理一次
	資通安全健診	網路架構檢視	每二年辦理一次
		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	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，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。
	政府組態基準		初次受核定或等級變更後之一年內，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。

資通安全責任等級B級之公務機關應辦事項-認知與訓練

制度面向	辦理項目	辦理項目細項	辦理內容
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及 職能訓練證書	資通安全專業證照	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有二張以上，並持續維持證照之有效性。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有二張以上，並持續維持證書之有效性。

資通安全責任等級B級之公務機關應辦事項-技術面(2/2)

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，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。
		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	

資通系統防護需求分級原則

防護需求等級 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能**造成未經授權之資訊揭露**，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能**造成未經授權之資訊揭露**，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能**造成未經授權之資訊揭露**，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能**造成資訊錯誤或遭竄改等情事**，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能**造成資訊錯誤或遭竄改等情事**，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能**造成資訊錯誤或遭竄改等情事**，對機關之營運、資產或信譽等方面將產生有限之影響。

資通系統防護需求分級原則

防護需求等級 構面	高	中	普
可用性	發生資通安全事件致資通系統受影響時，可能**造成對資訊、資通系統之存取或使用之中斷**，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能**造成對資訊、資通系統之存取或使用之中斷**，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能**造成對資訊、資通系統之存取或使用之中斷**，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

資通系統防護基準構面

存取控制 01

稽核與可歸責性 02

營運持續計畫 03

識別與鑑別 04

系統與服務獲得 05

系統與通訊保護 06

系統與資訊完整性 07

資通系統防護基準控制措施 —— 帳號管理（1/9）

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	普	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。

資通系統防護基準控制措施 —— 帳號管理 (2/9)

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	中	一、**已逾期**之**臨時或緊急**帳號應刪除或禁用。

資通系統防護基準控制措施 —— 帳號管理 (3/9)

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	中	二、資通系統**閒置帳號**應禁用。

資通系統防護基準控制措施 —— 帳號管理（4/9）

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	中	三、**定期審核**資通系統帳號之建立修改、啟用、禁用及刪除。

資通系統防護基準控制措施 —— 帳號管理 (5/9)

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	中	四、等級「普」之所有控制措施。

資通系統防護基準控制措施 —— 帳號管理 (6/9)

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	高	一、逾越機關所定預期**閒置時間**或**可使用期限時**，系統應自動將使用者登出。

資通系統防護基準控制措施 —— 帳號管理（7/9）

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	高	二、應依**機關規定之情況及條件**，使用資通系統。

資通系統防護基準控制措施 —— 帳號管理 (8/9)

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	高	三、**監控資通系統帳號**，如發現帳號**違常使用**時回報管理者。

資通系統防護基準控制措施 —— 帳號管理（9/9）

構面	措施內容	防護需求分級	控制措施說明
存取控制	帳號管理	高	四、等級「中」之所有控制措施。

資通系統防護基準控制措施 —— 最小權限（1/3）

構面	措施內容	防護需求分級	控制措施說明
存取控制	最小權限	普	無要求。

資通系統防護基準控制措施 —— 最小權限（2/3）

構面	措施內容	防護需求分級	控制措施說明
存取控制	最小權限	中	採**最小權限**原則，僅允許使用者（或代表使用者行為之程序）依**機關任務及業務功能**，完成指派任務所需之授權存取。

資通系統防護基準控制措施 —— 最小權限（3/3）

構面	措施內容	防護需求分級	控制措施說明
存取控制	最小權限	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 遠端存取（1/6）

構面	措施內容	防護需求分級	控制措施說明
存取控制	遠端存取	普	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**，使用者之權限檢查作業應**於伺服器端完成**。

資通系統防護基準控制措施 —— 遠端存取（2/6）

構面	措施內容	防護需求分級	控制措施說明
存取控制	遠端存取	中	一、應**監控**資通系統遠端連線 。

資通系統防護基準控制措施 —— 遠端存取（3/6）

構面	措施內容	防護需求分級	控制措施說明
存取控制	遠端存取	中	二、資通系統應採用**加密機制**。

資通系統防護基準控制措施 —— 遠端存取（4/6）

構面	措施內容	防護需求分級	控制措施說明
存取控制	遠端存取	中	三、資通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 。

資通系統防護基準控制措施 —— 遠端存取（5/6）

構面	措施內容	防護需求分級	控制措施說明
存取控制	遠端存取	中	四、等級「普」之所有控制措施。

資通系統防護基準控制措施 —— 遠端存取（6/6）

構面	措施內容	防護需求分級	控制措施說明
存取控制	遠端存取	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 稽核事件（1/6）

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核事件	普	一、依**規定時間週期**及**紀錄留存政策**，保留稽核紀錄。

資通系統防護基準控制措施 —— 稽核事件（2/6）

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核事件	普	二、 確保資通系統有**稽核特定事件之功能**，並決定應稽核之特定資通系統事件。

資通系統防護基準控制措施 —— 稽核事件（3/6）

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核事件	普	三、 應稽核資通系統**管理者帳號**所執行之**各項功能**。

資通系統防護基準控制措施 —— 稽核事件（4/6）

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核事件	中	一、應**定期審查**稽核事件 。

資通系統防護基準控制措施 —— 稽核事件（5/6）

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核事件	中	二、等級「普」之所有控制措施。

資通系統防護基準控制措施 —— 稽核事件（6/6）

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核事件	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 稽核紀錄內容 (1/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核紀錄內容	普	資通系統產生之稽核紀錄應包含**事件類型、發生時間、發生位置**及任何與事件相關之**使用者身分識別**等資訊，並採用**單一日誌紀錄機制**，確保**輸出格式之一致性**。

資通系統防護基準控制措施 —— 稽核紀錄內容 (2/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核紀錄內容	中	一、資通系統產生之稽核紀錄，應**依需求**納入其他相關資訊。

資通系統防護基準控制措施 —— 稽核紀錄內容 (3/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核紀錄內容	中	二、等級「普」之所有控制措施。

資通系統防護基準控制措施 —— 稽核紀錄內容 (4/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核紀錄內容	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 稽核紀錄容量 (1/3)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核紀錄容量	普	依據稽核紀錄儲存需求，配置稽核紀錄所需之**儲存容量**。

資通系統防護基準控制措施 —— 稽核紀錄容量 (2/3)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核紀錄容量	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 稽核紀錄容量 (3/3)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核紀錄容量	高	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 ——稽核處理失效之回應(1/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核處理失效之回應	普	資通系統於**稽核處理失效**時，應**採取適當之行動**。

資通系統防護基準控制措施 ——稽核處理失效之回應(2/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核處理失效之回應	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 ——稽核處理失效之回應(3/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核處理失效之回應	高	一、機關規定需要**即時通報之稽核失效事件**發生時，資通系統應於機關**規定之時效內**，對特定人員提出警告。

資通系統防護基準控制措施 ——稽核處理失效之回應(4/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核處理失效之回應	高	二、等級「中」及「普」之所有控制措施。

資通系統防護基準控制措施 —— 時戳及校時（1/4）

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	時戳及校時	普	資通系統應使用系統內部時鐘產生稽核紀錄所需**時戳**，並可以對應到**世界協調時間(UTC)或格林威治標準時間(GMT)**。

資通系統防護基準控制措施 —— 時戳及校時 (2/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	時戳及校時	中	一、系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。

資通系統防護基準控制措施 —— 時戳及校時 (3/4)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	時戳及校時	中	二、等級「普」之所有控制措施 。

資通系統防護基準控制措施 —— 時戳及校時（4/4）

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	時戳及校時	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 ——稽核資訊之保護 (1/5)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核資訊之保護	普	對稽核紀錄之存取管理，僅限於**有權限之使用者**。

資通系統防護基準控制措施 ——稽核資訊之保護 (2/5)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核資訊之保護	中	一、應運用**雜湊**或**其他適當方式**之完整性確保機制。

資通系統防護基準控制措施 ——稽核資訊之保護 (3/5)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核資訊之保護	中	二、等級「普」之所有控制措施 。

資通系統防護基準控制措施 ——稽核資訊之保護 (4/5)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核資訊之保護	高	一、**定期備份**稽核紀錄至與原稽核系統**不同之實體系統**。

資通系統防護基準控制措施 ——稽核資訊之保護 (5/5)

構面	措施內容	防護需求分級	控制措施說明
稽核與可歸責性	稽核資訊之保護	高	二、等級「中」之所有控制措施 。

資通系統防護基準控制措施 —— 系統備份（1/7）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備份	普	一、訂定系統**可容忍資料損失之時間**要求 。

資通系統防護基準控制措施 —— 系統備份（2/7）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備份	普	二、 執行系統**源碼與資料**備份 。

資通系統防護基準控制措施 —— 系統備份（3/7）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備份	中	一、應**定期測試備份資訊**，以驗證備份媒體之**可靠性**及資訊之**完整性**。

資通系統防護基準控制措施 —— 系統備份（4/7）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備份	中	二、等級「普」之所有控制措施 。

資通系統防護基準控制措施 —— 系統備份（5/7）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備份	高	一、應將備份還原，**作為營運持續計畫測試之一部分**。

資通系統防護基準控制措施 —— 系統備份（6/7）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備份	高	二、應在與運作系統**不同處之獨立設施或防火櫃**中，儲存重要資通系統軟體與其他安全相關資訊之備份 。

資通系統防護基準控制措施 —— 系統備份（7/7）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備份	高	三、等級「中」之所有控制措施 。

資通系統防護基準控制措施 —— 系統備援（1/4）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備援	普	無要求。

資通系統防護基準控制措施 —— 系統備援 (2/4)

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備援	中	一、訂定資通系統**從中斷後至重新恢復服務之可容忍時間**要求 。

資通系統防護基準控制措施 —— 系統備援 (3/4)

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備援	中	二、原服務中斷時，於**可容忍時間內**，由**備援設備**取代提供服務 。

資通系統防護基準控制措施 —— 系統備援（4/4）

構面	措施內容	防護需求分級	控制措施說明
營運持續計畫	系統備援	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 內部使用者之識別與鑑別（1/4）

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	內部使用者之識別與鑑別	普	資通系統應具備**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)之功能，**禁止使用共用帳號**。

資通系統防護基準控制措施 — 內部使用者之識別與鑑別 (2/4)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	內部使用者之識別與鑑別	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 內部使用者之識別與鑑別（3/4）

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	內部使用者之識別與鑑別	高	一、對帳號之網路或本機存取採取**多重認證技術**。

資通系統防護基準控制措施 —— 內部使用者之識別與鑑別（4/4）

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	內部使用者之識別與鑑別	高	二、等級「中」及「普」之所有控制措施。

資通系統防護基準控制措施 —— 身分驗證管理 (1/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	普	一、使用預設密碼登入系統時，應於**登入後要求立即變更**。

資通系統防護基準控制措施 —— 身分驗證管理 (2/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	普	二、**身分驗證相關**資訊**不以明文傳輸**。

資通系統防護基準控制措施 —— 身分驗證管理 (3/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	普	三、具備**帳戶鎖定機制**，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或**使用機關自建之失敗驗證機制**。

資通系統防護基準控制措施 —— 身分驗證管理 (4/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	普	四、基於密碼之鑑別資通系統應強制**最低密碼複雜度**；強制密碼**最短及最長之效期限制**。

資通系統防護基準控制措施 —— 身分驗證管理 (5/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	普	五、使用者更換密碼時，至少**不可以與前三次使用過之密碼相同**。

資通系統防護基準控制措施 —— 身分驗證管理 (6/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	普	六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。

資通系統防護基準控制措施 —— 身分驗證管理 (7/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	中	一、身分驗證機制應防範**自動化程式**之登入或密碼更換嘗試。

資通系統防護基準控制措施 —— 身分驗證管理 (8/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	中	二、密碼重設機制對使用者重新身分確認後，發送**一次性及具有時效性**符記。

資通系統防護基準控制措施 —— 身分驗證管理 (9/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	中	三、等級「普」之所有控制措施。

資通系統防護基準控制措施 —— 身分驗證管理 (10/10)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	身分驗證管理	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 — 鑑別資訊回饋 (1/3)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	鑑別資訊回饋	普	資通系統應**遮蔽鑑別過程中之資訊**。

資通系統防護基準控制措施 —— 鑑別資訊回饋 (2/3)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	鑑別資訊回饋	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 鑑別資訊回饋 (3/3)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	鑑別資訊回饋	高	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 加密模組鑑別 (1/3)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	加密模組鑑別	普	無要求。

資通系統防護基準控制措施 —— 加密模組鑑別 (2/3)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	加密模組鑑別	中	資通系統如以密碼進行鑑別時，該密碼應**加密或經雜湊處理後儲存**。

資通系統防護基準控制措施 —— 加密模組鑑別 (3/3)

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	加密模組鑑別	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 非內部使用者之識別與鑑別（1/3）

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	非內部使用者之識別與鑑別	普	資通系統應識別及鑑別**非機關使用者**(或代表機關使用者行為之程序)

資通系統防護基準控制措施 —— 非內部使用者之識別與鑑別（2/3）

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	非內部使用者之識別與鑑別	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 非內部使用者之識別與鑑別（3/3）

構面	措施內容	防護需求分級	控制措施說明
識別與鑑別	非內部使用者之識別與鑑別	高	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期需求階段（1/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期需求階段	普	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。

資通系統防護基準控制措施 —— 系統發展生命週期需求階段（2/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期需求階段	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期需求階段（3/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期需求階段	高	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期設計階段（1/4）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期設計階段	普	無要求。

資通系統防護基準控制措施 —— 系統發展生命週期設計階段（2/4）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期設計階段	中	一、根據系統功能與要求，**識別**可能影響系統之**威脅**，進行**風險分析及評估**。

資通系統防護基準控制措施 —— 系統發展生命週期設計階段（3/4）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期設計階段	中	二、將**風險評估結果回饋**需求階段之檢核項目，並提出**安全需求修正**

資通系統防護基準控制措施 —— 系統發展生命週期設計階段（4/4）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期設計階段	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期開發階段（1/7）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期開發階段	普	一、應針對安全需求實作**必要控制措施**。

資通系統防護基準控制措施 —— 系統發展生命週期開發階段（2/7）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期開發階段	普	二、應注意避免軟體**常見漏洞**及實作**必要控制措施**。

資通系統防護基準控制措施 —— 系統發展生命週期開發階段（3/7）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期開發階段	普	三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。

資通系統防護基準控制措施 —— 系統發展生命週期開發階段（4/7）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期開發階段	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期開發階段（5/7）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期開發階段	高	一、執行「**源碼掃描**」安全檢測。

資通系統防護基準控制措施 —— 系統發展生命週期開發階段（6/7）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期開發階段	高	二、具備系統**嚴重錯誤**之通知機制

資通系統防護基準控制措施 —— 系統發展生命週期開發階段（7/7）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期開發階段	高	三、等級「中」及「普」之所有控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期測試階段（1/4）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期測試階段	普	執行「**弱點掃描**」安全檢測。

資通系統防護基準控制措施 —— 系統發展生命週期測試階段（2/4）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期測試階段	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期測試階段（3/4）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期測試階段	高	一、執行「**滲透測試**」安全檢測。

資通系統防護基準控制措施 —— 系統發展生命週期測試階段（4/4）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期測試階段	高	二、等級「中」及「普」之所有控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期部署與維運階段（1/5）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期部署與維運階段	普	一、於部署環境中應針對相關**資通安全威脅**，進行更新與修補，並**關閉不必要服務及埠口**。

資通系統防護基準控制措施 —— 系統發展生命週期部署與維運階段（2/5）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期部署與維運階段	普	二、資通系統**相關軟體**，**不使用預設密碼**。

資通系統防護基準控制措施 —— 系統發展生命週期部署與維運階段（3/5）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期部署與維運階段	中	一、於系統發展生命週期之維運階段，須注意**版本控制**與**變更管理**。

資通系統防護基準控制措施 —— 系統發展生命週期部署與維運階段（4/5）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期部署與維運階段	中	二、等級「普」之所有控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期部署與維運階段（5/5）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期部署與維運階段	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期委外階段（1/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期委外階段	普	資通系統開發如委外辦理，應將**系統發展生命週期各階段**依**等級**將**安全需求**（含機密性、可用性、完整性）納入**委外契約**。

資通系統防護基準控制措施 —— 系統發展生命週期委外階段（2/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期委外階段	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 系統發展生命週期委外階段（3/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統發展生命週期委外階段	高	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 獲得程序（1/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	獲得程序	普	無要求。

資通系統防護基準控制措施 —— 獲得程序 (2/3)

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	獲得程序	中	**開發、測試及正式**作業環境應為**區隔**。

資通系統防護基準控制措施 —— 獲得程序 (3/3)

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	獲得程序	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 系統文件（1/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統文件	普	應儲存與**管理系統發展生命週期之相關文件**。

資通系統防護基準控制措施 —— 系統文件 (2/3)

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統文件	中	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 系統文件（3/3）

構面	措施內容	防護需求分級	控制措施說明
系統與服務獲得	系統文件	高	同「防護需求分級」為普的控制措施。

資通系統防護基準控制措施 —— 傳輸之機密性與完整性（1/7）

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	傳輸之機密性與完整性	普	無要求。

資通系統防護基準控制措施 —— 傳輸之機密性與完整性（2/7）

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	傳輸之機密性與完整性	中	無要求。

資通系統防護基準控制措施 —— 傳輸之機密性與完整性（3/7）

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	傳輸之機密性與完整性	高	一、資通系統應採用**加密機制**，以**防止未授權之資訊揭露或偵測資訊之變更**。但傳輸**過程中有替代之實體保護措施者**，不在此限。

資通系統防護基準控制措施 —— 傳輸之機密性與完整性（4/7）

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	傳輸之機密性與完整性	高	二、使用**公開、國際機構驗證**且**未遭破解**之演算法。

資通系統防護基準控制措施 —— 傳輸之機密性與完整性（5/7）

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	傳輸之機密性與完整性	高	三、支援演算法**最大長度金鑰**。

資通系統防護基準控制措施 —— 傳輸之機密性與完整性（6/7）

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	傳輸之機密性與完整性	高	四、**加密金鑰**或**憑證**週期性更換。

資通系統防護基準控制措施 —— 傳輸之機密性與完整性（7/7）

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	傳輸之機密性與完整性	高	五、伺服器端之**金鑰保管**應訂定**管理規範**及實施應有之**安全防護措施**

資通系統防護基準控制措施 —— 資料儲存之安全 (1/3)

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	資料儲存之安全	普	無要求。

資通系統防護基準控制措施 —— 資料儲存之安全 (2/3)

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	資料儲存之安全	中	無要求。

資通系統防護基準控制措施 —— 資料儲存之安全 (3/3)

構面	措施內容	防護需求分級	控制措施說明
系統與通訊保護	資料儲存之安全	高	**靜置資訊**及相關**具保護需求之機密資訊**應加密儲存。

資通系統防護基準控制措施 —— 漏洞修復（1/4）

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	漏洞修復	普	系統之**漏洞修復**應**測試有效性及潛在影響**，並**定期更新**。

資通系統防護基準控制措施 —— 漏洞修復 (2/4)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	漏洞修復	中	一、**定期確認資通系統相關漏洞修復之狀態**。

資通系統防護基準控制措施 —— 漏洞修復 (3/4)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	漏洞修復	中	二、等級「普」之所有控制措施。

資通系統防護基準控制措施 —— 漏洞修復（4/4）

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	漏洞修復	高	同「防護需求分級」為中的控制措施。

資通系統防護基準控制措施 —— 資通系統監控 (1/5)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	資通系統監控	普	發現資通系統有被入侵跡象時，應通報**機關特定人員**。

資通系統防護基準控制措施 —— 資通系統監控 (2/5)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	資通系統監控	中	一、監控資通系統，以偵測**攻擊**與**未授權之連線**，並識別資通系統之**未授權使用**。

資通系統防護基準控制措施 —— 資通系統監控 (3/5)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	資通系統監控	中	二、等級「普」之所有控制措施。

資通系統防護基準控制措施 —— 資通系統監控 (4/5)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	資通系統監控	高	一、資通系統應採用**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**。

資通系統防護基準控制措施 —— 資通系統監控 (5/5)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	資通系統監控	高	二、等級「中」之所有控制措施。

資通系統防護基準控制措施 —— 軟體及資訊完整性 (1/6)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	軟體及資訊完整性	普	無要求。

資通系統防護基準控制措施 —— 軟體及資訊完整性 (2/6)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	軟體及資訊完整性	中	一、使用**完整性驗證工具**，以偵測**未授權變更**特定軟體及資訊。

資通系統防護基準控制措施 —— 軟體及資訊完整性 (3/6)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	軟體及資訊完整性	中	二、使用者**輸入資料合法性檢查**應置放於**應用系統伺服器端**。

資通系統防護基準控制措施 —— 軟體及資訊完整性 (4/6)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	軟體及資訊完整性	中	三、發現違反**完整性**時，資通系統應實施**機關指定之安全保護措施**。

資通系統防護基準控制措施 —— 軟體及資訊完整性 (5/6)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	軟體及資訊完整性	高	一、應**定期**執行**軟體與資訊完整性檢查**。

資通系統防護基準控制措施 —— 軟體及資訊完整性 (6/6)

構面	措施內容	防護需求分級	控制措施說明
系統與資訊完整性	軟體及資訊完整性	高	二、等級「中」之所有控制措施。

註：因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯有困難者，得經第3條第2項至第4項所定其等級提交機關或同條第5項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施。

Thank you

pwc.tw

© 2021 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.