聯準科技
股份有限公司
Security Standard Service

資通系統盤點、安全等級評估暨防護基準作業實務

本次課程將說明依據「資通安全管理法」及相關子法規定，從單位業務界定、資通系統盤點、核心系統確認、安全等級評估、防護基準檢視等步驟，協助各單位完成作業並符合法遵規範。

法源依據

- **資通安全管理法施行細則第6條**：資通安全維護計畫應包含資通系統及資訊之盤點，並標示核心資通系統及相關資產。
- **資通安全責任等級分級辦法**：依據機關的資通安全責任等級，規範應辦事項，包括資通系統分級、防護基準、資產盤點及風險評估等。

資通系統定義

法定定義

依據《資通安全管理法》第3條的規定，資通系統是指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊進行其他處理、使用或分享的系統。這些系統的主要目的是輔助政府機關及其他組織的業務運作，確保資訊的有效管理和安全性。

案例宣導

多數政府機關單位仍未落實盤點核心業務相關資通系統

內容摘要：

- 依據數位發展部公布的《111年度公務機關資安稽核概況報告》指出，多數政府機關尚未有效界定並落實盤點其核心業務及相關資通系統。這一缺失使得許多機關在面對資安風險時，無法及時識別和應對潛在的威脅。
- 報告中還提到，許多機關在執行資通系統防護基準控制措施方面存在困難，尤其是在核心資通系統的安全檢測和網路架構檢測上，顯示出明顯的改進空間。這些問題包括未落實資訊資產盤點、委外服務契約未納入資通安全管理法相關要求等，這些都可能導致資安事件的發生。

資通系統盤點步驟

步驟一：界定組織業務

明確業務範疇

首先必須明確界定單位內的各項業務，這些業務是單位運作的基礎，為後續系統盤點工作奠定重要基礎。

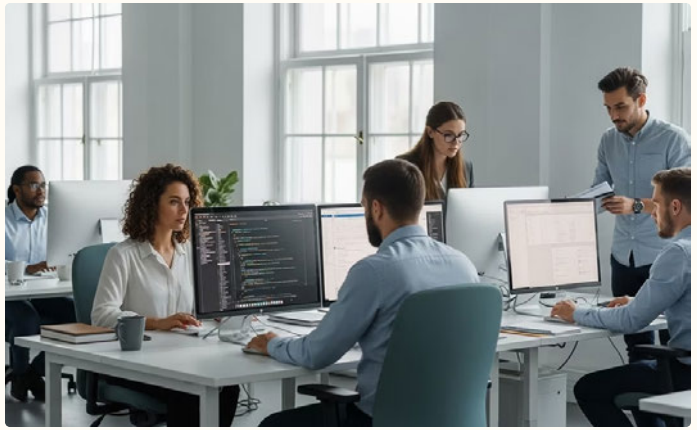
業務流程分析

詳細分析各項業務的執行流程，了解每個環節所需的資訊支援，確保不遺漏任何關鍵業務活動。

系統關聯性

所有相關的資通系統都應該支持這些業務的持續運作，建立業務與系統間的對應關係。

步驟二：盤點資通系統

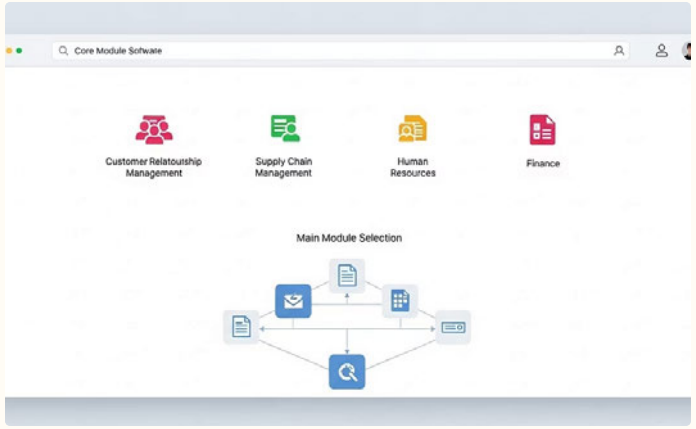


自行或委外建置系統

各單位盤點必須包括所有自行開發或委外開發的資通系統。這些系統的安全管理和防護需求必須依據《資通安全管理法》中的相關規定進行評估和控制。

共用系統

由其他單位（包括上級機關）提供的共用系統也必須納入盤點範圍。共用系統的安全需求和防護等級由主責機關進行判斷，並應納入整體的資通系統盤點。



套裝系統

套裝系統同樣需要納入盤點。這些系統通常涉及多個機關的業務運作，因而其安全性和合規性也必須受到重視，需進行全面的安全評估。

※各單位系統重複盤點問題：如該系統涉及多個單位使用，且無法確認其主責(管理)單位、使用單位性質，建議統一先列表紀錄，後續再召集會議確認權責。

步驟三：確認核心資通系統

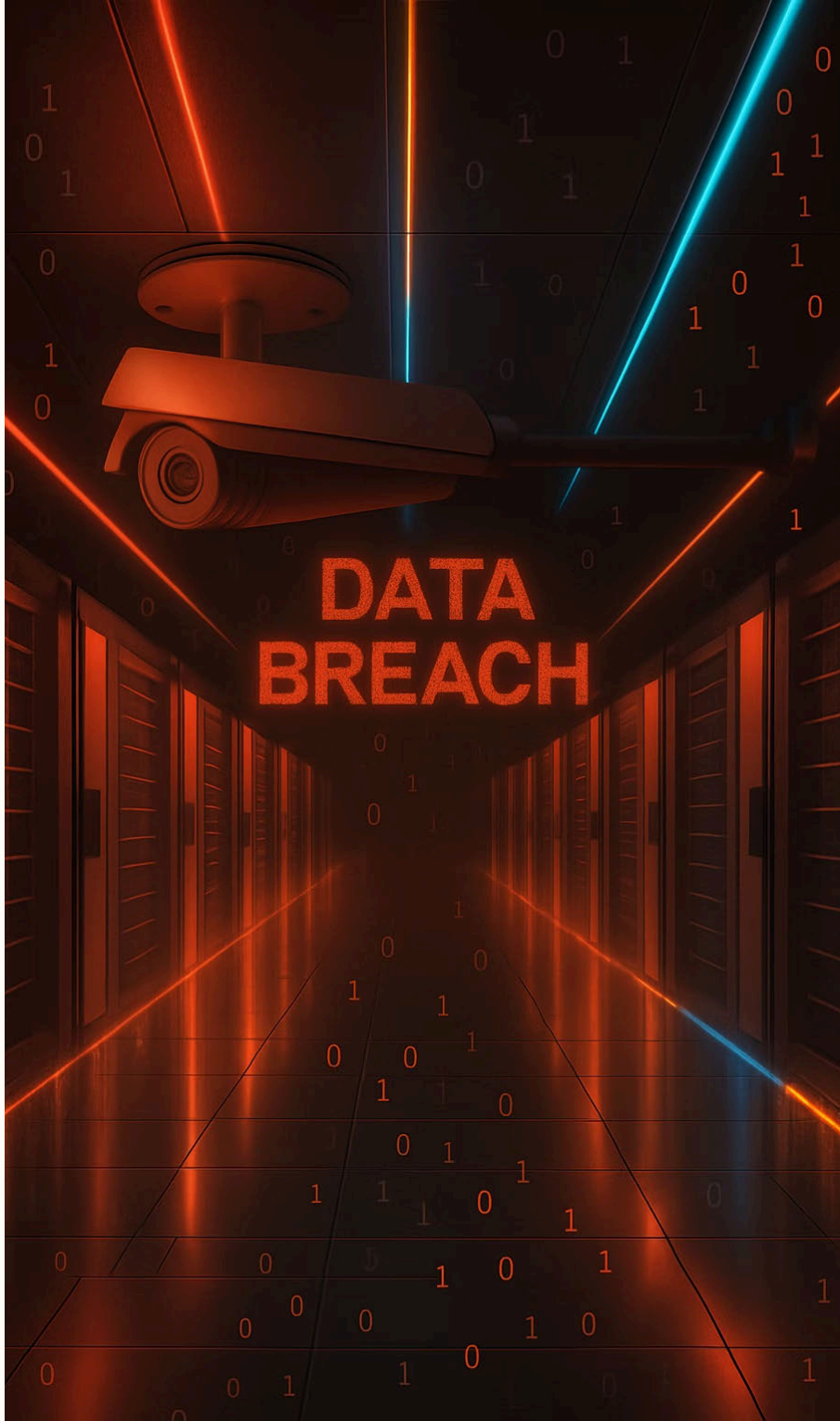
- 依據《資通安全管理法施行細則》第7條2項，核心資通系統指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者。
- 需要特別注意的是，核心系統不等於防護需求等級「高」系統，但防護需求等級「高」系統等於核心系統。
- 由計資中心識別各單位核心(關鍵)業務，分別完成"核心系統"及"非核心系統"統計

步驟四：資通系統防護需求分級評估

根據《資通安全責任等級分級辦法》第11條規定，機關應針對所有自行或委外開發之資通系統，應依據「資通安全責任等級分級辦法」附表九所定「資通系統防護需求分級原則」進行評估。

ⓘ 分級評估是針對個別資通系統之機密性、完整性、可用性及法律遵循性等構面，分別考量資通系統於發生資通安全事件時可能造成的衝擊(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)並據以評估各構面之「普」、「中」及「高」等級(附表詳次頁)

ⓘ 對於非自行或委外開發的系統，如上級機關提供的共用系統、套裝軟體等，法規並未強制要求填寫「系統安全等級評估表」。然而，若這些系統如對單位業務運作具有關鍵性，或涉及敏感資訊，各單位得依實需進行風險評估，以確保整體資通安全。



附表九 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。
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。

備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

步驟五：資通系統防護基準檢視

依據《資通安全責任等級分級辦法》第11條的規定，針對自行或委外開發的資通系統，依據其防護需求等級(普、中、高)，所需達成的安全控制措施進行自我檢核。

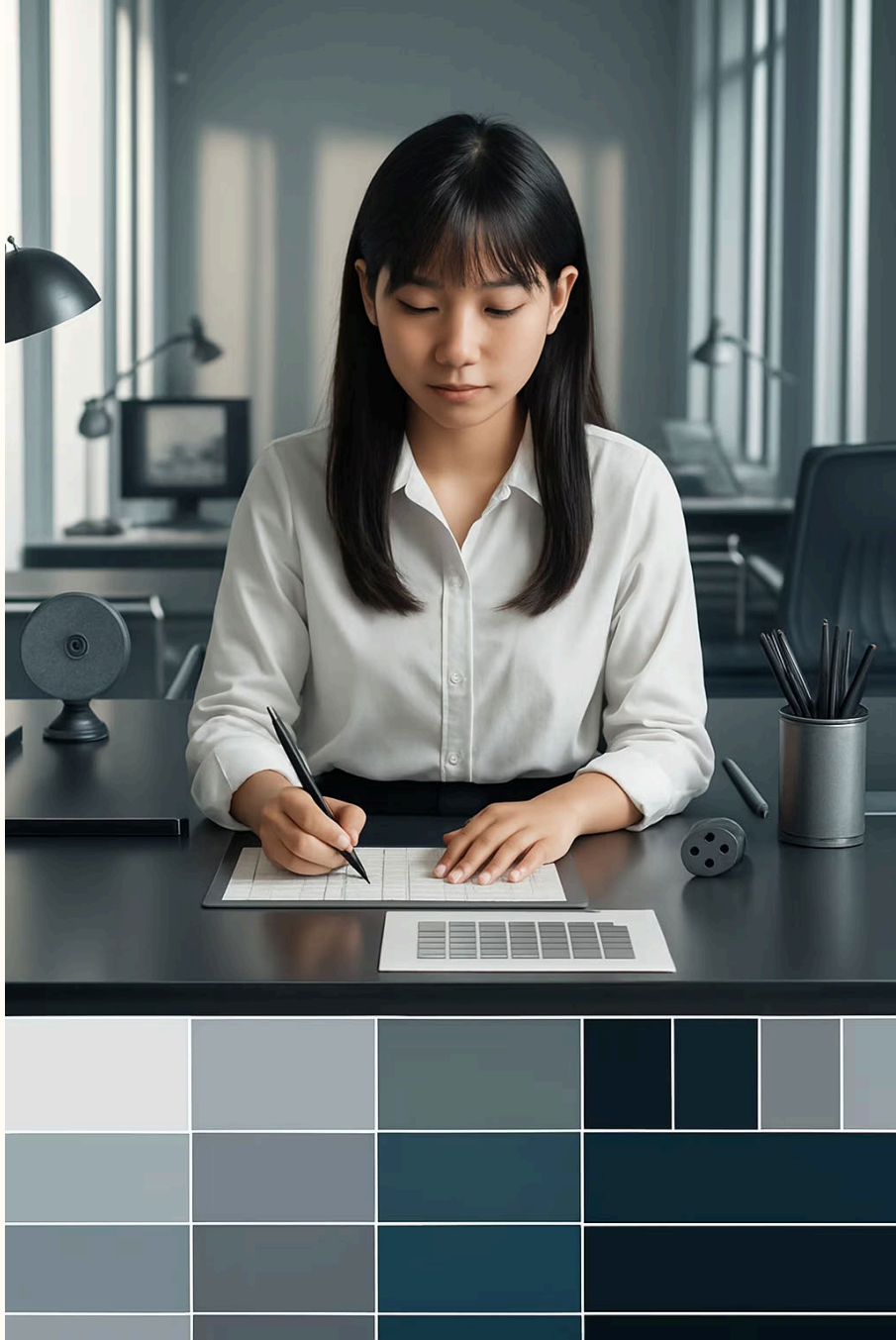
制定防護基準的目的

- 確保系統安全： 防護基準表的主要目的是為了確保資通系統的安全性，通過明確的控制措施來降低潛在的安全風險。
- 標準化管理： 透過防護基準表，各機關可以標準化其資通系統的安全管理流程，確保所有系統都遵循相同的安全標準

資通系統防護基準填寫說明

35	58	78
普級控制措施	中級控制措施	高級控制措施
基礎防護要求項目數量	包含普級的累加性要求	最高等級的完整防護要求

- 根據《資通安全責任等級分級辦法》附表十「資通系統防護基準」的規定，資通系統的防護需求分為「普」、「中」與「高」三個等級。
- 控制措施涵蓋存取控制、事件日誌與可歸責性、營運持續計畫、識別與鑑別、系統與服務獲得、系統與通訊保護、系統與資訊完整性等構面。每個等級的控制措施具有累加性。
- 原則上由各單位之系統負責人自評，亦得請系統開發廠商協助提供相關資訊。



資通系統防護基準一覽表		
構面	措施內容	控制措施
存取控制(3)	帳號管理	8
	最小權限	1
	遠端存取	5
稽核與可歸責性(6)	記錄事件	4
	日誌紀錄內容	1
	日誌儲存容量	1
	日誌處理失效之回應	2
	時戳及校時	2
	日誌資訊之保護	3
營運持續計畫(2)	系統備份	5
	系統備援	2
識別與鑑別(5)	內部使用者之識別與鑑別	2
	身分驗證管理	8
	鑑別資訊回饋	1
	加密模組鑑別	1
	非內部使用者之識別與鑑別	1
系統與服務獲得 (8)	系統發展生命週期需求階段	1
	系統發展生命週期設計階段	2
	系統發展生命週期開發階段	5
	系統發展生命週期測試階段	2
	系統發展生命週期部署與維運階段	3
	系統發展生命週期委外階段	1
	獲得程序	1
	系統文件	1
系統與通訊保護(2)	傳輸之機密性與完整性	5
	資料儲存之安全	1
系統與資訊完整性(3)	漏洞修復	2
	資通系統監控	3
	軟體及資訊完整性	4

區分7個構面

29項措施內容

78項控制措施

A040030000002700-20190826-11000-010.pdf

資通系統防護基準驗證實務
(V1.1)

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9月

2. 資通系統防護基準驗證

本章節針對資通系統防護基準，說明 7 個構面、29 項控制措施類別之各項控制措施，逐項說明其控制措施、使用等級、內容說明及驗證實務等，並提供可能之佐證資料作為驗證之參考依據，參考文獻則為該項控制措施之原始出處及補充說明，以提供實作與驗證之參考。

2.1 存取控制

2.1.1 帳號管理

2.1.1.1 建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序

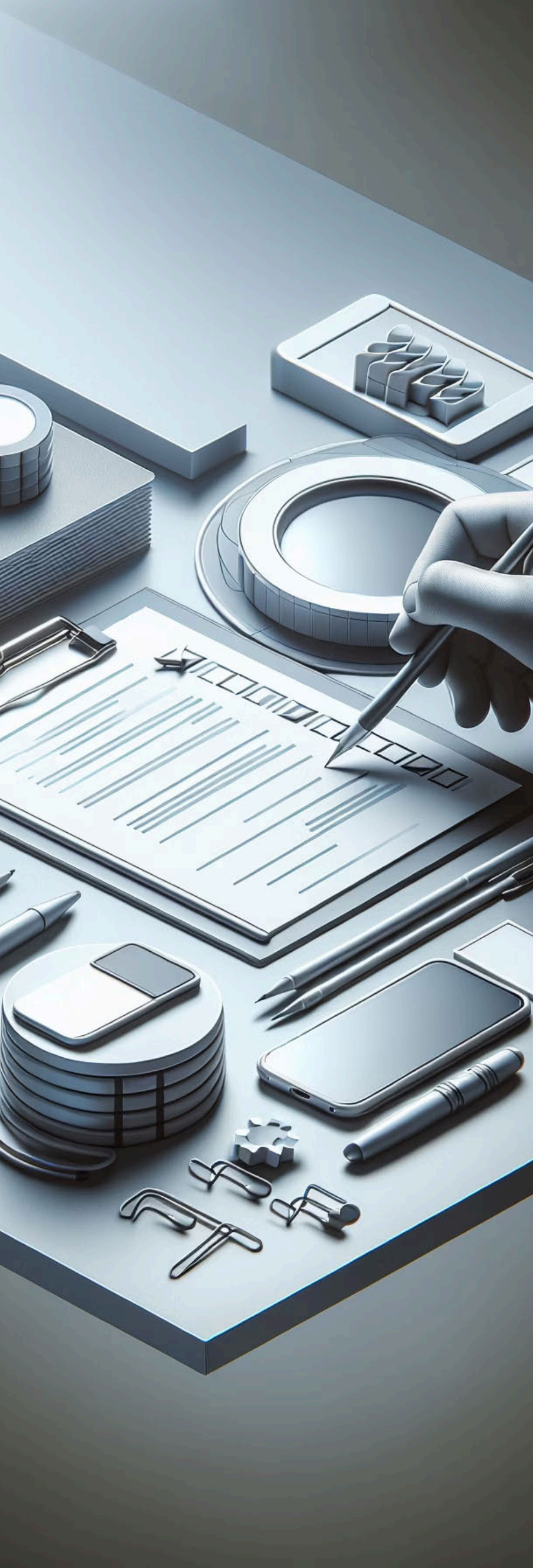
表2 帳號管理控制措施 1

控制措施	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序
適用等級	普、中、高
內容說明	▪須建立資通系統帳號管理機制，以適切管理資通系統使用者帳號、後臺主機作業系統帳號及資料庫管理者帳號等。 ▪內部使用者使用資通系統應符合機關訂定之帳號管理程序，包含帳號之申請、建立、修改、啟用、停用及刪除等作業規範並落實執行。除因緊急需求外，原則上所有帳號異動不可由系統管理者任意調整異動，宜由相關權責人員提出異動申請，並通過審核程序後始可進行異動作業。而帳號異動流程，一般可透過紙本或電子化系統完成，填寫相關表單(如系統帳號/權限異動申請單等)。系統帳號權限異動申請單範例，詳見圖 1。

控制措施	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序
	 資料來源：本計畫整理 圖1 系統帳號權限異動申請單範例
驗證實務	▪如未建立帳號管理機制，或是雖訂定帳號管理規範卻未落實執行，則未符合此項控制措施。 ▪驗證人員宜檢視機關實作之帳號管理機制，如使用電子化或紙本流程，並可檢閱機關訂定之帳號管理文件化規範，檢查是否在現有帳號管理機制中，已包含帳號申請、建立、修改、啟用、停用及刪除等各種帳號異動程序相關要求，以提供系統管理者與一般使用者進行帳號申請及異動之作業依據。 ▪驗證人員宜檢視機關帳號管理規範之落實情形，此時可抽查既有帳號之申請、建立、修改、啟用、停用及刪除等帳號異動相關紀錄(可能透過電子化系統或是紙本表單等形式)，從中查找帳號違規使用情形。 ▪驗證情境如驗證人員抽查資通系統中近期新建之內部使用者帳號(如系統管理者等)，檢閱其申請與審核相關紀錄，以確認是否為未經核可卻私自建立或啟用之帳號。同時，驗證人員亦可抽查系統是否仍留存應依程序完成停用或刪除作業卻仍繼續使用之帳號，如已逾期之臨時帳號、緊急帳號及開置帳號等。

控制措施	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序
佐證資料	▪機關訂定之資通系統帳號管理規範 ▪資通系統帳號申請異動單(如帳號權限申請表、使用者帳號異動申請單等) ▪系統線上帳號權限申請或異動紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 4-存取控制 Access Control (控制措施編號 AC-2 帳號管理)[2]

資料來源：本計畫整理



防護基準不符合控制措施處理方式

作法1：

- 根據《資通安全責任等級分級辦法》第11條規定，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，得報請主管機關備查後，免執行該事項或控制措施。

作法2：

1. 記錄不符合項目：在防護基準表中明確標示不符合的控制措施，並簡要說明不符合的原因。
2. 風險評估：評估該不符合項目對資通系統的機密性、完整性、可用性及法律遵循性的影響程度。
3. 擬定改善計畫：根據風險評估結果，制定具體的改善措施，明確改善內容、負責人及預定完成時間。
4. 持續追蹤與檢討：定期檢視改善計畫的執行情形，確保不符合項目已獲得有效改善。

風險處理的方式

- **風險避免（Avoidance）**
  避免進行會產生風險的活動。
  例：不使用某不安全的技術。
- **風險移轉（Transference）**
  將風險轉嫁給第三方。
  例：委外服務。
- **風險降低（Mitigation）**
  採取控制措施來減少風險的發生機率或影響程度。
  例：導入防火牆、定期備份。
- **風險接受（Acceptance）**
  認知風險存在並選擇接受，不採取行動。
  例：風險成本低於控制成本。

步驟六：定期檢視與持續改進

定期檢視

單位應每年至少檢視一次資通系統分級的妥適性，確保其與實際風險狀況相符

二年期限

防護需求等級為「高」的系統，應於初次受核定或等級變更後二年內完成所有防護基準控制措施

改進優化

根據檢視結果持續改進資通系統的安全防護能力，提升整體安全水準

持續監控

建立持續監控機制，確保防護措施的有效性並適時調整安全策略

根據《資通安全責任等級分級辦法》規定，單位針對自行或委外開發的資通系統，應依附表九完成系統分級，並依附表十完成相應的防護基準控制措施。

透過定期檢視機制，確保資通系統的安全防護措施能夠持續有效運作，並適應不斷變化的資安威脅環境。建立完善的檢視制度是維護資通安全的重要環節，也是法規遵循的必要要求。

執行紀錄建立：計資中心「資通盤點系統」填報

新增盤點項目—1

新增盤點項目—2


國立臺灣大學 National Taiwan University 資通盤點系統
盤點專區
其他服務
登出
個人區
送彙整
/ 資通系統盤點
資通系統盤點
※防護需求等級出現【高】有紅點警示的話，送出彙整前建議先找我們諮詢，專業團隊協助你診斷系統藥到病除。
新增
新增中英文網站平台填報範本
全部送彙整
編輯
序號
單位名稱
資通系統名稱
系統屬性
核心系統
防護需求等級
填報時間
送彙整
1131
計算機及資訊網路中心程式設計組
test
行政
是
普
2025-01-07
如為使用「中英文網站」平台製作之網站，
新增好後，點此進入編輯頁面。
※點選「新增」者，則會直接進入編輯頁面。

資通系統盤點平台欄位說明—1

資通系統盤點平台欄位說明—2

欄位名稱	欄位說明
填報單位	請選擇資通系統所屬的單位
系統名稱	1. 機關運用計畫經費所籌獲之資通系統亦應納入盤點 2. 若為委外雲端服務，請填寫該雲端系統之名稱 3. 有關系統盤點如係不同廠商所建置、維運，應盤出不同系統；另如機關係將各系統以群組命名，則一律納為高防護等級之系統，群組內各系統一律適用。
系統屬性	限填「行政」、「業務」、「兼具行政/業務」
建置方式	限填「本機關委外開發」、「本機關租用服務」、「本機關購置套裝軟體」、「本機關自行開發」、或「其他」
建置方式補充說明	「系統建置方式」為「其他」者必填

資通系統盤點平台欄位說明—3

欄位名稱	欄位說明
建置廠商	1. 系統建置方式為「套裝軟體」者請填「套裝軟體」 2. 若為機關自行開發者，請填寫該機關名
建置廠商之統一編號	1. 若廠商無統一編號請填寫「0」 2. 系統建置方式為「套裝軟體」者請填「2」 3. 若為機關建置，請填寫該機關之OID
維運廠商	1. 系統建置方式為「套裝軟體」者請填「套裝軟體」 2. 若為機關自行維運者，請填寫該機關名
維運廠商之統一編號	1. 若廠商無統一編號請填寫「0」 2. 系統建置方式為「套裝軟體」者請填「2」 3. 若為機關建置，請填寫該機關之OID

欄位說明
【系統名稱】

xxx官網、xxx系統

欄位說明
【建置方式】

建置方式是指在執行項目或計畫時所採用的方法或策略。它涉及到將設計或計畫轉化為實際的操作或系統的過程。

欄位說明
【系統屬性】

【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】【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）】＊範例某某網站：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

欄位說明
【建置廠商】

建置廠商（Implementing Vendor）是指在專案或計畫中負責實際執行和實施工作的供應商或承包商。

欄位說明
【建置廠商之統一編號】

統一編號，也稱為統一編號碼（Uniform Invoice Number），是一個用於識別企業和機構的唯一識別號碼。

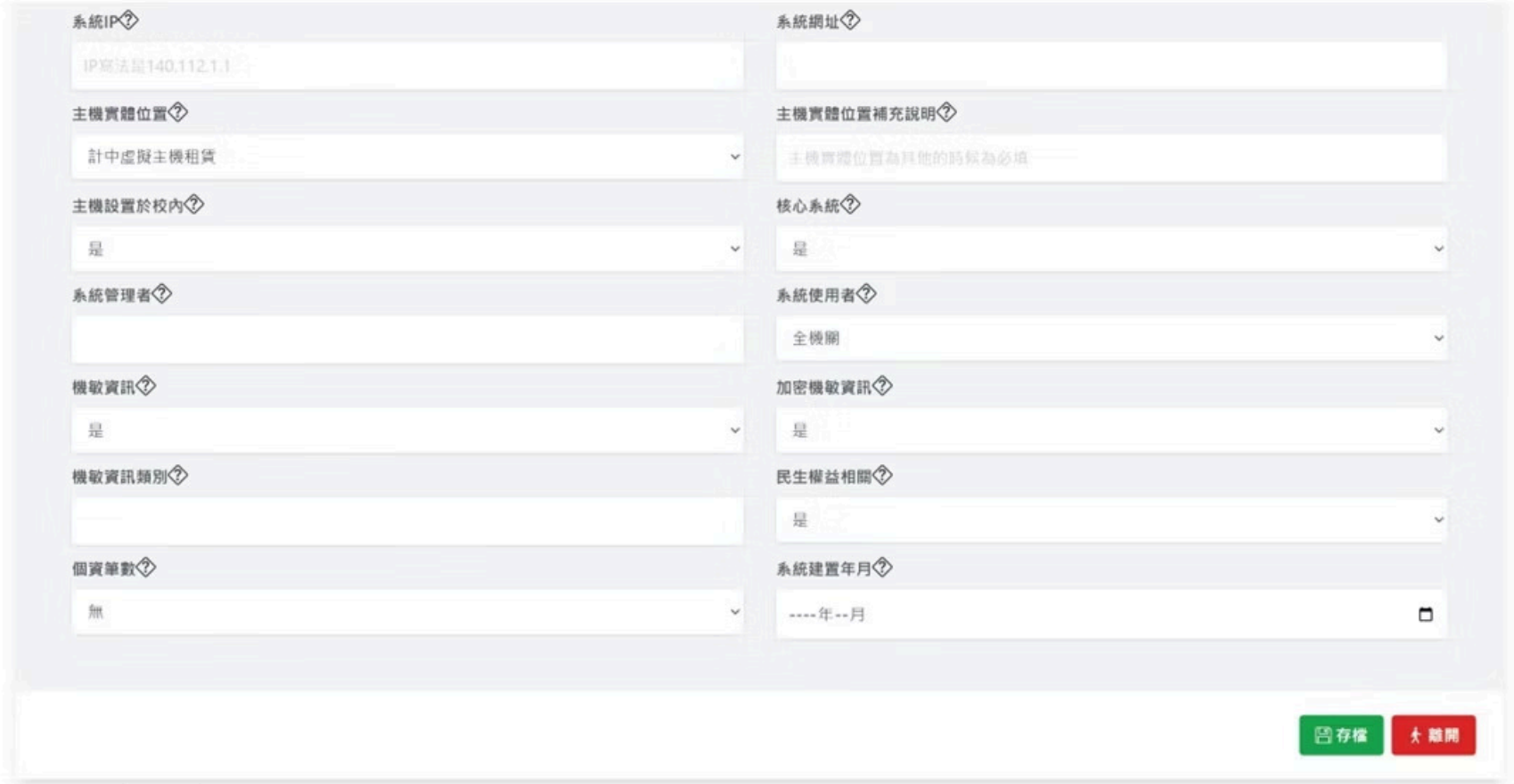
欄位說明
【維運廠商】

維運廠商（Maintenance and Operations Vendor）是指負責維護和營運特定設施、設備或系統的供應商或承包商。他們通常與組織或機構簽訂合約，負責提供持續的維護、保養、修理和操作服務，以確保這些設施或系統的正常運作和功能。

欄位說明
【維運廠商之統一編號】

統一編號，也稱為統一編號碼（Uniform Invoice Number），是一個用於識別企業和機構的唯一識別號碼。

資通系統盤點平台欄位說明—4



資通系統盤點平台欄位說明—5

欄位名稱	欄位說明
系統IP	系統IP（Internet Protocol）指的是在網際網路或區域網路中，用於識別和定位電腦或網路設備的唯一識別碼。IP地址由一串數字組成，通常表現為四組由句點分隔的數字（例如：192.168.0.1）。
系統網址	系統網址是指一個網站、應用程式或服務的網路地址，也稱為網站URL（Uniform Resource Locator）。 系統網址通常由幾個部分組成。 例如，一個標準的URL可能包含協議（例如http://或https://）、域名（例如www.example.com）和路徑（例如/path/to/page）等元素。這些部分組合在一起提供了一個完整的網址。
主機實體位置	主機實體位置是指電腦系統中主機（通常是伺服器）的物理位置或放置位置。這是指主機所在的地理位置或具體的建築物、機房或機櫃等實體位置。
主機實體位置補充說明	主機非放置校內請填寫補充說明。
主機設置於校內	限填「是」或「否」
核心系統	1. 限填「是」或「否」 2. 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 註：機關之核心系統以應用系統為主

資通系統盤點平台欄位說明—6

欄位名稱	欄位說明
系統管理者	請填寫擁有系統管理權限功能者之所在部門/單位
系統使用者	1. 請填寫主要使用該系統的單位(可為多個單位)，如為機關全單位都有使用，則填寫全機關 2. 若系統為跨機關使用，亦請填寫使用該系統之機關，例如：直轄市、縣市政府 3. 若該系統亦提供民眾使用，請加註「…處，且供民眾使用」
機敏資訊	限填「是」、「否」
加密機敏資訊	限填「是」、「否」、「無機敏資訊」
民生權益相關	限填「是」、「否」
機敏資訊類別	1. 「無機敏資訊」者免填 2. 機敏資訊：例如身分證字號、特種個資、稅務資料等
個資筆數	單位擁有個資的數量。
系統建置年月	請填系統上線日期，並以數字表示，例如於2023年3月上線之系統，本項應填「2023/3」

欄位說明
【校內主機】

伺服器或VM虛擬機建置於臺灣大學內。

欄位說明
【核心系統】

核心系統（Core System）是指一個組織或企業中最關鍵、最重要的系統。它通常涉及到支持組織的核心產業業務功能和關鍵流程，對於組織的運轉和業務成功至關重要。

欄位說明
【系統管理者】

系統管理員是負責管理和維護伺服器、網路和資訊技術基礎設施的專業人員。

欄位說明
【系統使用者】

使用系統、軟體應用或其他資訊技術工具來完成特定任務或目標的個人或群體系統用戶可以包括各種職務和角色的人員，從一般員工到高階管理人員，都可以是系統的最終用戶。開放全校使用之系統可填「全機關」。

欄位說明
【機敏資訊】

機敏資訊（Sensitive Information）指的是對個人、組織或其他實體具有高度機密性或隱私性的資訊。這些資訊如果落入錯誤的人手中或被不當使用，可能導致負面後果，包括金融損失、身份盜竊、個人隱私侵犯、商業競爭優勢喪失等。因此，保護機敏資訊是非常重要的。

欄位說明
【機敏資訊類別】

個人身份資訊：包括姓名、地址、社會安全號碼、護照號碼、駕照號碼等。 金融資訊：包括信用卡號碼、銀行帳戶號碼、交易記錄、金融投資資訊等。 醫療資訊：包括病歷記錄、處方藥物、疾病診斷、醫療保險資訊等。 企業機密：包括商業計劃、市場策略、專利、客戶名單、供應商資訊等。 政府機密：包括國家安全資訊、機密政府文件、情報報告等。

欄位說明
【加密機敏資訊】

使用加密技術對機敏資訊進行加密，以防止非授權人員訪問或截取資訊。

欄位說明
【民生權益相關】

民生權益（Livelihood Rights）是指人們基本的生活需求和福祉所應享有的權益。這些權益涉及到人們的生存、糧食、住所、教育、醫療、就業、社會保障和文化等方面的需求。

欄位說明
【個資筆數】

單位擁有個資的數量。

資通系統盤點平台欄位說明—7

資通系統盤點平台欄位說明—8

欄位名稱	欄位說明
系統是否對外	1. 限填「是」、「否」 2. 「系統對外」係指以網際網路即可連線檢視或使用之系統
系統日誌保存時間超過6個月	限填「是」、「否」
開放遠端連線維護	限填「有」、「無」 註：系統建置方式為「主管/上級/其他機關」者請填「其他機關維運」
禁用弱密碼	限填「是」、「否」、「不適用」
包含於ISMS導入範圍	限填「是」、「否」
系統有備份	系統備份是指將計算機系統中的數據、應用程式、配置和設定等重要資訊複製並保存到另一個儲存媒介或位置的過程。

資通系統盤點平台欄位說明—9

欄位名稱	欄位說明
有流量清洗機制	非為對外之系統，本項請填「非對外系統」
有CDN啟用作業程序	非為對外之系統，本項請填「非對外系統」
備妥靜態網頁	非為對外之系統，本項請填「非對外系統」
可10分鐘內切換至靜態網頁	非為對外之系統，本項請填「非對外系統」
每天尖峰使用人數	系統每日於熱門使用時段的使用人數。
使用頻率	系統的使用頻率。

欄位說明
【系統是否對外】

「系統對外」係指以網際網路即可連線檢視或使用之系統。

欄位說明
【系統日誌保存時間是否超過6個月】

系統日誌（System Log）是電腦系統或應用程式生成和記錄事件、錯誤和活動的檔案或記錄。它包含系統的運行狀態、錯誤訊息、警告、事件記錄、使用者活動等資訊，並用於故障排除、監控系統運作和安全審計等目的。

欄位說明
【有無開放遠端連線維護】

遠端連線維護（Remote Connection Maintenance）是指通過網路或遠程(遠端)連線技術，遠端訪問和管理遠端電腦系統或設備，進行維護和支援工作，而無需實際接觸到被維護對象的物理位置。

欄位說明
【是否禁用弱密碼】

弱密碼是指容易被猜測、破解或猜出的不安全密碼。它通常由簡單、常見的字詞、數字或模式組成，缺乏足夠的複雜性和隨機性。弱密碼容易受到惡意攻擊者的破解或入侵，從而危及帳戶、系統或敏感資料的安全性。 以下是一些常見的弱密碼特徵： 簡單字詞：弱密碼可能是簡單的常見單詞或詞組，如"password"、"123456"、"qwerty"等。這些容易被猜測和破解。 數字序列：弱密碼可能是連續的數字序列，如"123456"、"987654"等。這些容易被猜測和猜出。 個人資訊：弱密碼可能包含個人資訊，如姓名、生日、電話號碼等。這些容易被猜測和從社交媒體或其他途徑獲取。 簡單模式：弱密碼可能是簡單的模式，如重複字符、連續鍵盤上的字符、簡單的替換或反轉等。這些模式容易被猜測和破解。 過於短小：弱密碼可能太短，不足以提供足夠的組合和隨機性。一般而言，長度較短的密碼更容易被破解。

欄位說明
【是否包含於ISMS導入範圍】

ISMS（Information Security Management System）導入範圍指的是在組織中實施資訊安全管理體系的範圍和範圍界定。ISMS是一套組織內部制定、實施、監控和持續改進資訊安全控制的框架，旨在保護組織的資訊資產免受潛在的威脅和風險。

欄位說明
【系統有備份】

系統備份是指將電腦系統中的數據、應用程式、配置和設定等重要資訊複製並保存到另一個儲存媒介或位置的過程。

欄位說明
【有流量清洗機制】

使用臺灣大學網路或各大雲端服務廠商都會有流量清洗機制。

欄位說明
【有CDN啟用作業程序】

CDN代表內容傳遞網路（Content Delivery Network）。它是一種分散式網路架構，用於提供高效的內容傳遞和分發服務。CDN的目標是提供快速、可靠的網路內容交付，減少網路延遲和提高用戶體驗。

欄位說明
【備妥靜態網頁】

靜態網頁（Static Web Page）是指在網頁請求時，其內容在伺服器端事先被建立好並固定不變的網頁。靜態網頁的內容通常以HTML、CSS和JavaScript等靜態檔案的形式存在，它們直接被瀏覽器下載並呈現給用戶。

欄位說明
【可10分鐘內切換至靜態網頁】

網頁備援機制。

資通系統盤點平台欄位說明—10

機密性 (連動防護需求等級)

普

完整性 (連動防護需求等級)

普

可用性 (連動防護需求等級)

普

法律遵循性 (連動防護需求等級)

普

資通系統防護需求等級

普

系統回復時間目標(RTO)

3天以內

資料回復目標點(RPO)

30天

最大可容忍中斷時間(MTPD)

4天

備註

存檔

離開

資通系統盤點平台欄位說明—11

欄位名稱	欄位說明
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、資產或信譽等方面產生影響。
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、資產或信譽等方面產生影響。
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、資產或信譽等方面產生影響。
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。
資通系統防護需求等級	限填「普」、「中」、「高」、「套裝軟體」

資通系統之防護需求等級之四大構面

01
機密性

- 防止非授權人員存取資訊，確保資訊秘密性。

02
完整性

- 防止非授權人員竄改資訊，確保資訊資產及其處理過程的準確度（accuracy）和完全性（completeness）。

資通系統之防護需求等級

03
可用性

- 防止系統故障或人為惡意阻斷服務，確保資訊與資訊處理的可獲得性

04
法律遵循性

- 組織必須遵守的法律、規定、與合約義務。

資通系統防護需求分級原則—機密性

分級原則說明	分級
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。	高
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。	中
1. 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。 2. 儲存特種個資或大量個資者，不得評為普。	普

資通系統防護需求分級原則—完整性

分級原則說明	分級
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。	高
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。	中
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。	普

資通系統防護需求分級原則—可用性

分級原則說明	分級
1. 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。 2. 最大可容忍中斷時間（MTPD）低於8小時者，應評為高。	高
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。	中
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。	普

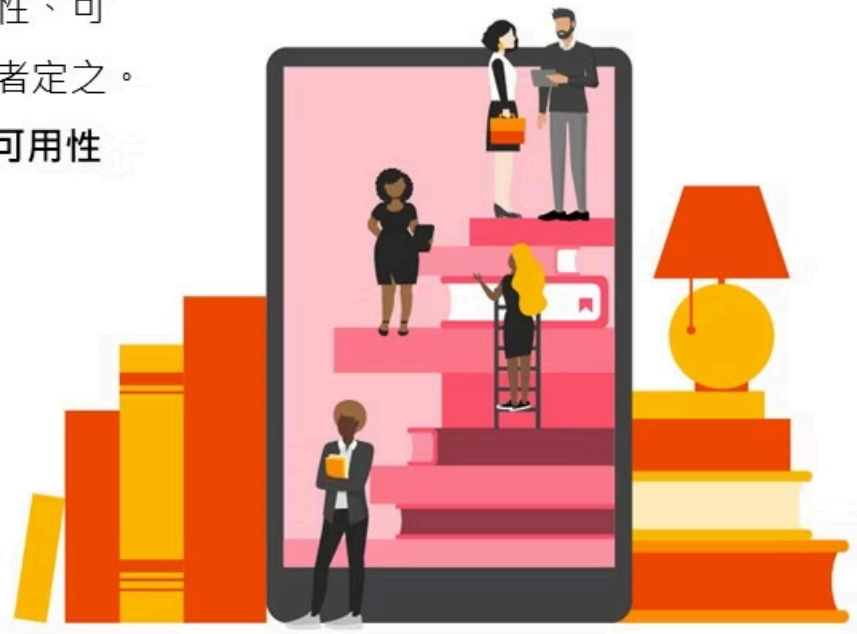
資通系統防護需求分級原則—法律遵循性

分級原則說明	分級
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。	高
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。	中
其他資通系統設置或運作於法令有相關規範之情形。	普

資通系統之防護需求等級之判斷

- 資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。**資通系統之防護需求等級=Max(機密性分級，完整性分級，可用性分級，法律遵循性分級)**
- 判斷是否為核心系統

防護需求等級	高	中	低
	核心系統	核心系統/非核心系統	非核心系統



資通系統盤點平台欄位說明—12

欄位名稱	欄位說明
最大可容忍中斷時間(MTPD)	最大可容忍中斷時間（Maximum Tolerable Period of Disruption, MTPD）關鍵業務發生中斷後，恢復至最低運作水準，所能容許的中斷時間。
系統回復時間目標(RTO)	系統回復時間目標（Recovery Time Objective，簡稱RTO）即業務中斷可容忍回復時間，於基礎設施正常供應下，核心業務從資通安全事件或災難發生到業務復原的目標時間。
資料回復目標點(RPO)	資料回復目標點（Recovery Point Objective，簡稱RPO）是指於基礎設施正常供應下，核心業務從資通安全事件或災難發生到復原期間資料所能回復的時間點。

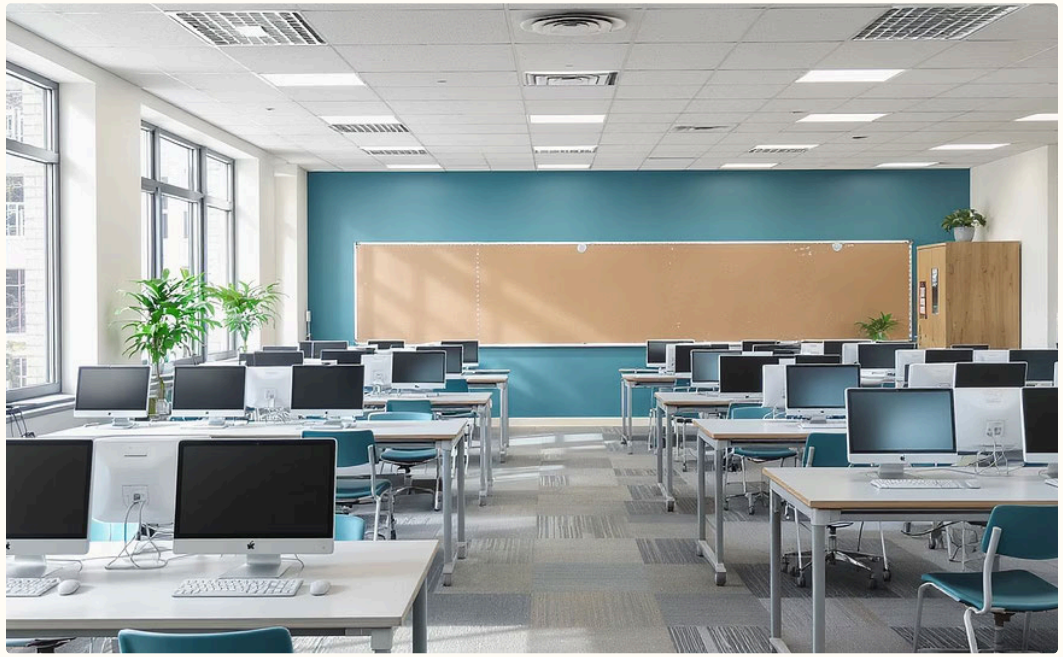
資通訊設備盤點

盤點範圍

資通訊設備盤點需涵蓋以下範圍：

網路連接設備

可透過連接網路提供服務的各類設備



校園公務設備

學校採購與公務使用的資通訊設備

資通訊設備盤點

基本資料

填報單位

資訊網路組

資通訊設備名稱

資通訊設備名稱，ex.計中1樓事務機

設備類別

網路印表機/多功能事務機

資通訊設備IP

IP寫法是140.112.1.1

資通訊設備網址/DOMAIN

沒有的話請填無

資通訊設備廠牌型號

範例:NTU牌 E316-9

資通訊設備版本號/作業系統版本號

如無則填無

資通訊設備存放建築物

資通訊設備存放位置

搜尋

是否修改預設密碼

是

是否使用遠端維護

是

使用者/管理者

備註

資通訊設備盤點欄位

資通訊設備名稱

- 請填寫可以識別此資通訊設備的名稱或者電腦名稱。
  - NTU牌事務機
  - DESKTOP-5A1234S

設備類別(可連網之設備)

- 請選擇資通訊設備的類別，如果超過這些類別請聯繫諮詢專線(65013、65012)。
- 伺服器及測試機請填資通訊系統。

- 網路印表機/多功能事務機
- 使用者電腦
- 智慧家電
- DNS Server
- 網路攝影機
- 自設門禁設備
- 環控系統
- 自設無線網路基地台(AP)/路由器
- 連網電子看板
- 能源管理系統(EMS)
- 網路磁碟NAS
- 智慧電表

資通訊設備盤點欄位

是否修改預設密碼

- 使用手冊、操作手冊
- Google搜尋設備型號

是否使用遠端維護

- 查詢設備防火牆設定
- 遠端維護的連線如下範例:
  - Microsoft RDP遠端桌面(3389)
  - TeamViewer(5938)
  - telnet(23)、SSH(22)
  - 設備管理介面(80、443、8443)

應用場景：IT人員維修伺服器、廠商維護工控設備、協助用戶解決電腦問題，須注意僅在必要時啟用連線。

大陸廠牌盤點

大陸廠牌資通訊產品盤點

基本資料

填報單位

資訊網路組

資通訊產品名稱

如有英文名稱，以括號加註於後

廠牌名稱(中文及英文)

如有英文名稱，以括號加註於後

產品型號或版本

如無則填N/A

分類

軟體

軟體及服務細項分類

作業系統

產品是否具供不特定人士直接收視或收聽之功能

是

委外調查

是否屬委外案廠商(含分包商)使用之產品

不是

大陸廠牌資通訊產品盤點

汰換調查

仍未汰換原因(請敘明原因)

範例:無使用需求，但未達保存年限。行政院已核定同意使用。

預訂汰換時間

2024/12/31

汰換前配套措施或相應作為

停用(封存)

汰換產品之經費估算(無則填0)

0

汰換產品之經費缺口(無則填0)

0

提報調查

111年已提報且經本署核定屬盤點範圍

是

111年未提報但本次提報原因

如經雙資安長同意，數位部核定(請填數位部核定文號)

財產調查

資通訊產品購置年份

109年以前

資通訊產品財產編號

請填臺大產編，如無則填N/A

禁止使用及採購「大陸廠牌資通訊產品(危害國家資通安全產品)」相關規定

一、公務機關⚠️全面禁止採購與使用

1. **行政命令禁令**：
   - 依行政院秘書長109年12月18日院臺護長字第1090201804A號函，公務機關全面禁止使用及採購大陸廠牌資通訊產品（含硬體、軟體及服務）。
   - 大陸廠牌：係指大陸地區廠商所提供之產品，至大陸地區廠商之定義係依行政院公共工程委員會107年12月20日工程企字第1070050131號函所稱「大陸地區廠商」，包含大陸地區法律設立登記之公司、合夥或獨資之工商行號、法人、機構或團體；此外，各機關於辦理採購案時，如屬經濟部投資審議委員會公告「具敏感性或國安含資安疑慮之業務範疇」，應確實於招標文件中載明不允許陸資資訊服務業者參與。
2. **範圍**：涵蓋資通安全管理法定義的軟體、硬體與資通訊服務（如伺服器、網通設備、無人機、雲端服務等）
3. **大陸廠牌認定方式：**由填報機關「從嚴認定」，所有屬大陸廠牌者，無論其原產地於我國、大陸地區或第三地區等，渠等產品均須納入。
4. **採購相關規定**：
   - 招標文件需明訂不得使用大陸廠牌、不得由陸資或陸籍人員參與。
   - 雲端服務若使用大陸存儲、備份、傳輸，即可終止契約且不賠償。

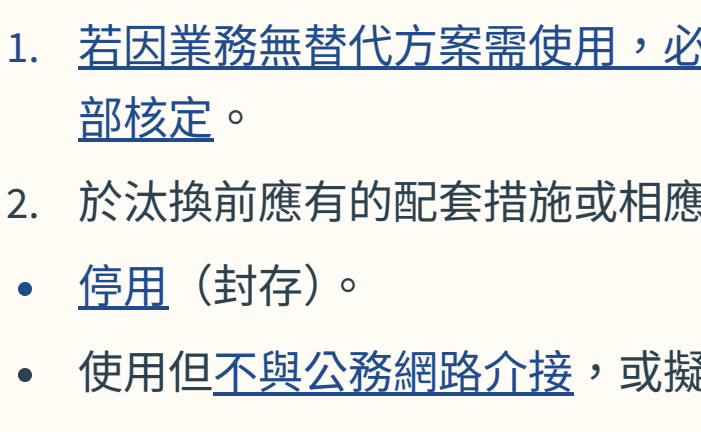
二、處理流程

1. 若因業務無替代方案需使用，必須提出正當理由，經機關資安長→上級資安長逐級核可，並函報數位發展部核定。
2. 於汰換前應有的配套措施或相應作為：

- 停用（封存）。
- 使用但不與公務網路介接，或擬訂其他適當配套管制措施。
- 將使用情形列入年度稽核時之檢視項目。
- 產品使用屆期後不得再購買危害國家資通安全產品。

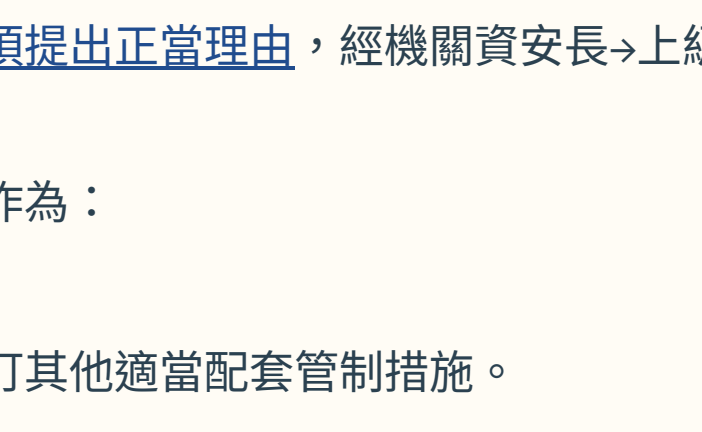
備註：考量實務執行問題，現行僅限制其最終資通訊產品不可為大陸廠牌，暫未限制大陸廠牌零組件。

以下大陸廠牌僅供參考，包括但不限於以下清單：



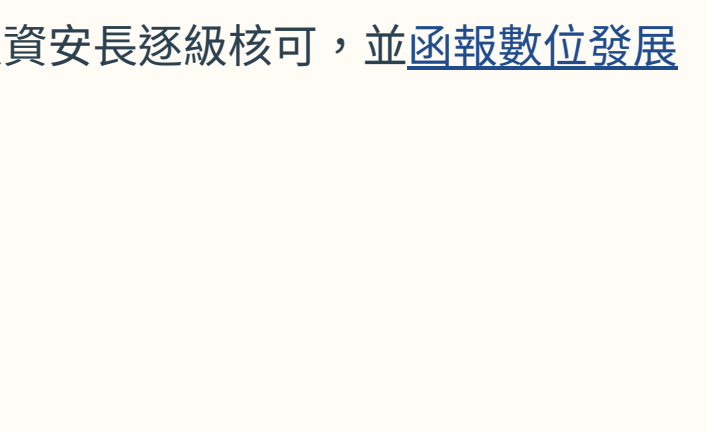
通訊設備製造商

Huawei(華為)、中興通訊、OPPO(廣東歐加)、vivo、MEIZU(魅族)、MI(小米集團)、REALME(真我)、Nubia(努比亞)



監控與安全設備

Hikvision(海康威視)、Dahua(浙江大華技術公司)、Foscam、RisingCam



航拍與影像設備

DJI(深圳大疆創新科技公司)、Insta360、OBSBOT、FOXTECH、Livox

網路設備製造商

TP Link(普聯技術)、Tenda、TOTOLINK、Mercusys(水星)、騰達

電腦與資訊設備

聯想、ZOTAC(索泰)、INNO3D、Snapmaker、QTS、映眾、CREALITY(創想)、CZUR

消費電子產品

Apabi、Hisense(海信)、TLC、HARMAN KARDON、Sugar、Boox、Royal(賓利皇家)、SEGWAY、Hiwonder（幻爾科技）

此清單持續更新中，採購前請確認產品不屬於禁止使用之大陸廠牌。

參考來源：經濟部投資審議司 陸資投資資訊產業事業清冊、來臺陸資名錄
https://www.moea.gov.tw/Mns/dir/Investment/ApprovedInvestment.aspx?menu_id=42802
https://www.moea.gov.tw/Mns/dir/Investment/InvestmentList.aspx?menu_id=42804

結語

通過本次課程的學習,相信您已經全面掌握了資通系統盤點、安全等級評估與防護基準的實務作業流程。從明確組織業務需求、盤點校內資通系統,到確認關鍵系統、評估防護需求,再到檢視與持續改進,這些都是確保校園網路安全、保護師生隱私的重要步驟。希望您能將所學應用於日常工作中,為校園資安建設貢獻一份力量,為學校創造更大的價值。讓我們一起攜手,共同守護校園的數位安全,為學校的長遠發展保駕護航。