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

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	V1.0	110/9/1	新編
2	V1.1	111/9/28	1.修正系統日誌留存類型之說明 2.酌作文字修正 3.參考文獻修正
備註			

資料來源：本計畫整理

報告摘要

報告名稱	資通系統防護基準驗證實務
資訊等級	☐機密　☐密　☐敏感　☐內部公開　☒普通
閱讀對象	☒行政院 ☒數發部資安署 ☒政府機關 ☐其他(_____)
文件屬性	☐研究報告 ☐調查統計報告 ☐系統開發報告 ☐業務執行報告 ☒參考規範/指引 ☐技術報告 ☐其他(_____)

內容摘要：

本文件適用對象為「一般主管」、「資訊人員」及「資安人員」。

本文件旨在協助政府機關依據「資通安全責任等級分級辦法」之資通系統防護基準之規範內容進行驗證，爰針對各項安全控制措施內容，提供解釋說明與驗證實務參考，惟此原則並非一體適用所有類型資通系統，實務上仍有許多應注意事項，建議以整體資安風險為考量，評估所施行安全控制措施之有效性與適切性。

本文件內容包含第 1 章「前言」，說明本文件之目的、適用對象及章節架構介紹；第 2 章「資通系統防護基準驗證」，說明資通系統防護基準 7 個構面各項安全控制措施要求與驗證實務；第 3 章「結論」，總結各章節摘要；第 4 章「參考文獻」，詳列本文件相關參考資料。附件為資通系統防護基準檢核表，提供機關自評之參考。

關鍵詞	資通安全管理法、資通安全責任等級分級辦法、資通系統防護基準、安全系統發展生命週期、SSDLC、稽核、驗證

目　次

圖 目 次

表 目 次

1. 前言

「資通安全管理法」(以下簡稱資安法)已於 108 年 1 月 1 日施行，政府機關應依據「資通安全責任等級分級辦法」(以下簡稱分級辦法)[1]之附表九「資通系統防護需求分級原則」，依系統之機密性、完整性、可用性及法律遵循性等構面，任一構面之防護需求等級之最高者，訂定資通系統之防護需求等級(普、中、高)，並依據其安全等級，執行附表十「資通系統防護基準」所規定之安全控制措施。資通系統防護基準分為 7 個構面，共計 29 項控制措施類別，詳見表 1。

表1　資通系統防護基準類別

項次	構面	控制措施
1	存取控制	▪帳號管理 ▪最小權限 ▪遠端存取
2	事件日誌與可歸責性	▪記錄事件 ▪日誌紀錄內容 ▪日誌儲存容量 ▪日誌處理失效之回應 ▪時戳及校時 ▪日誌資訊之保護
3	營運持續計畫	▪系統備份 ▪系統備援
4	識別與鑑別	▪內部使用者之識別與鑑別 ▪身分驗證管理 ▪鑑別資訊回饋 ▪加密模組鑑別 ▪非內部使用者之識別與鑑別

本文件之智慧財產權屬數位發展部資通安全署擁有。

項次	構面	控制措施
5	系統與服務獲得	▪系統發展生命週期需求階段 ▪系統發展生命週期設計階段 ▪系統發展生命週期開發階段 ▪系統發展生命週期測試階段 ▪系統發展生命週期部署與維運階段 ▪系統發展生命週期委外階段 ▪獲得程序 ▪系統文件
6	系統與通訊保護	▪傳輸之機密性與完整性 ▪資料儲存之安全
7	系統與資訊完整性	▪漏洞修復 ▪資通系統監控 ▪軟體及資訊完整性

資料來源：本計畫整理

1.1 目的

本文件旨在協助政府機關依據分級辦法之附表十資通系統防護基準修正規定內容進行驗證，爰針對各項安全控制措施內容，提供解釋說明與驗證實務參考。

1.2 章節架構

本文件分為前言、資通系統防護基準驗證、結論及參考文獻共 4 部分，重點摘錄如下：

第 1 章「前言」，說明本文件之目的、適用對象及章節架構介紹。

第 2 章「資通系統防護基準驗證」，為本文件重點內容，逐項說明各安全

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施要求與驗證實務。

第 3 章「結論」，總結各章節摘要。

第 4 章「參考文獻」，詳列本文件所參考文獻資料。

附件為資通系統防護基準檢核表，提供機關自評之參考。

1.3 使用建議

本文件旨在協助政府機關確認資通系統防護措施，是否符合資通系統防護基準之規定，提供驗證實務參考，惟此原則並非一體適用所有類型資通系統，實務上仍有許多應注意事項，建議以整體資安風險為考量，評估所施行安全控制措施之有效性與適切性。

本文件之智慧財產權屬數位發展部資通安全署擁有。

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。

本文件之智慧財產權屬數位發展部資通安全署擁有。

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、緊急帳號及閒置帳號等。

本文件之智慧財產權屬數位發展部資通安全署擁有。

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

2.1.1.2 已逾期之臨時或緊急帳號應刪除或禁用

表3 帳號管理控制措施 2

控制措施	已逾期之臨時或緊急帳號應刪除或禁用
適用等級	中、高
內容說明	▪基於實際作業需要，得建立短期性與臨時性使用者帳號，如為提供廠商或安全測試人員短期使用、代理工作等需求，或因應突發情況而需要迅速建立並啟用帳號，惟使用完畢後應盡速取消其使用權限。 ▪應定義臨時帳號與緊急帳號之使用期限，如資通系統允許使用者申請臨時帳號，使用效期 30 天，或者由系統管理者開立緊急帳號並設定使用截止日期。緊急帳號申請單設定使用期限範例，詳見圖 2。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	已逾期之臨時或緊急帳號應刪除或禁用
	 資料來源：本計畫整理 圖2　緊急帳號申請單範例 ▪ 應具備帳號檢查機制，將逾期之臨時或緊急帳號刪除或禁用，例如可人工定期進行帳號清查，或於資通系統實作自動管理逾時帳號之功能，如系統自動刪除自建立日起已達 30 天之臨時帳號。
驗證實務	▪ 如未管理臨時或緊急帳號，或是雖訂定相關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是否允許使用臨時或緊急帳號，並檢視機關對於臨時或緊急帳號之管理方式，包含帳號逾期之判定及帳號刪除或禁用之實作方式。 ▪ 驗證人員宜抽查資通系統帳號使用現況，從中查找違規之臨時或緊急帳號，例如已超過機關規定使用期限之帳號或帳號，原始使用目的已消失卻仍未刪除或禁用。 ▪ 如以資通系統實作帳號自動禁用或刪除功能，驗證人員可發展測試案例，以確認系統功能之有效性。例如，先建立一組測試用臨時帳號，調整系統日期以模擬超出臨時或緊急帳號使用期限，再檢視帳號是否已確實被刪除或禁用。
佐證資料	▪ 機關訂定之資通系統帳號管理程序 ▪ 資通系統帳號申請異動單

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	已逾期之臨時或緊急帳號應刪除或禁用
	▪ 資通系統帳號管理功能之測試紀錄 ▪ 資通系統帳號清查紀錄
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)

資料來源：本計畫整理

2.1.1.3 資通系統閒置帳號應禁用

表4 帳號管理控制措施 3

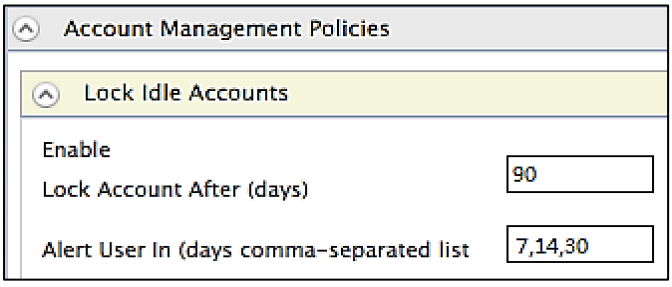
控制措施	資通系統閒置帳號應禁用
適用等級	中、高
內容說明	▪ 閒置帳號係指久未登入(如 90 天等)使用系統服務之帳號，常見原因如未移除已調、離(退)職人員之帳號權限等。 ▪ 應具備帳號檢查機制，將閒置帳號禁用，拒絕其登入行為，使用者需申請重新啟用後始可登入。常見作法為帳號接近逾期前(如 7 天等)，先寄發警示信件以提醒使用者進行登入。 ▪ 實務上可針對不同類型之資通系統與帳號，個別評估其使用需求與資安風險，定義其帳號之閒置期限。機關可定期以人工完成帳號審查作業，或是評估於系統上實作相關功能，如依機關設定之期限自動禁用逾期之閒置帳號。閒置帳號禁用範例，詳見圖 3。  資料來源：本計畫整理

圖3 閒置帳號禁用範例

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統閒置帳號應禁用
驗證實務	▪如未管理閒置帳號，或是雖訂定相關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對於閒置帳號之定義，包含其使用限制與期限，並檢視閒置帳號管理機制，包含判定帳號逾期與禁用帳號之實作方式。 ▪驗證人員宜抽查資通系統帳號使用現況，從中查找違規之閒置帳號。 ▪如以資通系統實作帳號自動禁用功能，驗證人員可發展測試案例以確認系統功能之有效性。例如，先建立一組測試用帳號，調整系統日期以模擬超出閒置帳號使用期限，再檢視帳號是否已確實被禁用。
佐證資料	▪機關訂定之資通系統帳號管理程序 ▪資通系統帳號申請異動單 ▪資通系統帳號管理功能之測試紀錄 ▪資通系統帳號清查紀錄
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)

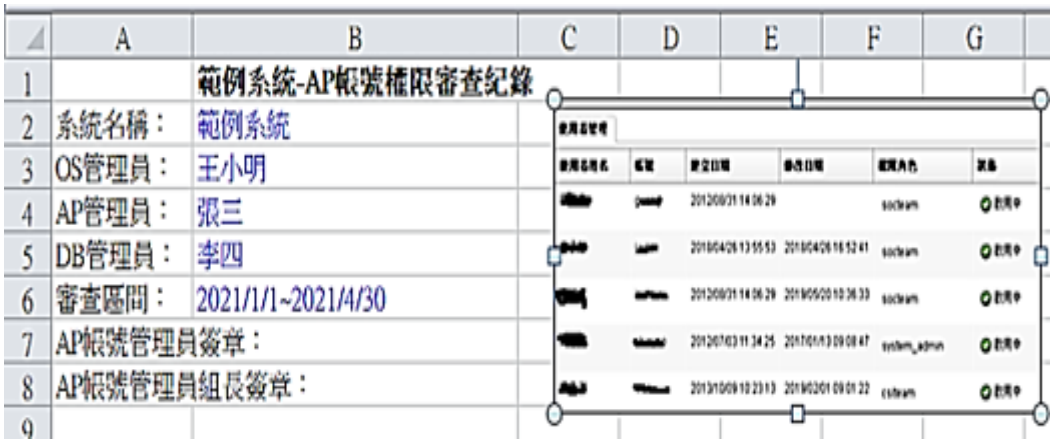
資料來源：本計畫整理

2.1.1.4 定期審核資通系統帳號之系統帳號之申請、建立、修改、啟用、停用及刪除

表5 帳號管理控制措施 4

控制措施	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除
適用等級	中、高
內容說明	▪應定期(如每季等)透過系統帳號清查活動，以審核帳號之申請、建立、修改、啟用、停用及刪除等相關紀錄，以發現未經授權之帳號變更行為。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除
	▪帳號審核範圍，宜包含系統管理者帳號、後臺主機作業系統帳號及資料庫管理者帳號等，亦可評估實際執行需求，納入機關內部及外部一般使用者帳號，並應依機關規定清查應禁用或刪除之帳號，如臨時帳號、緊急帳號及閒置帳號等。系統帳號清查紀錄範例，詳見圖 4。  資料來源：本計畫整理 圖4　系統帳號清查紀錄範例
驗證實務	▪如未定期進行帳號審查活動，則未符合此項控制措施。 ▪驗證人員宜檢視機關規範或訪談相關權責人員，從中了解現行之帳號審查機制，含審核週期與方式等。 ▪驗證人員宜抽查資通系統現有帳號之使用情況，並與帳號異動紀錄比對，以驗證機關帳號審核之有效性。
佐證資料	▪機關訂定之資通系統帳號管理程序 ▪資通系統帳號申請異動單 ▪資通系統帳號清查紀錄
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)

2.1.1.5 機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件

本文件之智慧財產權屬數位發展部資通安全署擁有。

表6　帳號管理控制措施 5

控制措施	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件
適用等級	高

內容說明	▪閒置時間係指使用者久未操作資通系統之閒置行為，當閒置過久，可能是使用者已離開系統操作環境卻未自行登出帳號，此時容易造成帳號被他人惡意盜用之風險；可使用期限如每次登入帳號後能進行系統操作時間限制(如 1 小時等)或時段限制(如 18:00 前等)。資通系統之使用情況及條件係指資通系統帳號之使用限制，如帳號類型與功能限制、操作時段限制、來源位址、連線數量及存取資源等。
	▪實務上因各資通系統使用需求之差異，系統管理者可設定不同之閒置時間或可使用期間，並限制各種使用情況及條件以確保安全性。這些條件限制，可能描述於機關相關管理規範內，亦可能是未明文規定之使用慣例要求，惟系統管理者及相關權責人員應熟知這些使用限制，並應確保資通系統已啟用相關設定，例如會談(Session)機制常被利用來管理使用者與伺服器之間之連線狀態，多數開發框架皆會內建會談管理功能，並設定使用者操作之閒置期限。以.NET 開發框架為例，設定會談逾期時間預設值為 20 分鐘，當使用者操作閒置達 20 分鐘時即自動登出。系統管理者也可利用 Web.config 組態設定檔案變更設定值，範例詳見圖 5。
	`<configuration>`
	`  <system.web>`
	`  <sessionState mode="InProc" cookieless="true" timeout="20" />`
	`  </system.web>`
	`</configuration>`
	資料來源：本計畫整理
	
	圖5　帳號操作閒置期限設定範例

驗證實務	▪除因系統使用需求不得設定限制帳號閒置時間外，原則上系統應設定閒置時間以防止帳號被盜用。驗證人員宜以資安風險角度，評估機關所定義閒置時間或可使用期限設定值之有效性，若違反合理操作範圍或完全未進行設定，亦未限制任何使用情況及條件，造成資

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件
	安風險顯著提升者，原則上應視為未符合此項控制措施。 ▪驗證人員宜檢視機關訂定之資通系統閒置時間或可使用期限之設定值，可透過人員訪談、檢視機關相關管理規範，以及檢視應用程式原始碼或設定檔等方式。
佐證資料	▪機關訂定之資通系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統應用程式原始碼或組態設定檔等與會談相關之設定值
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) ▪安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-14 非持續性)

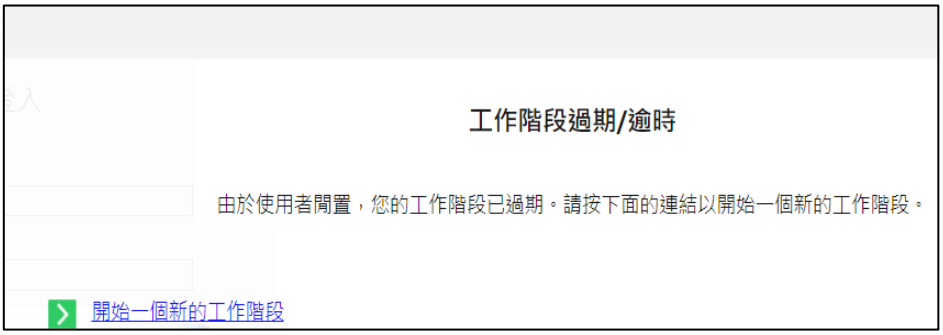
資料來源：本計畫整理

2.1.1.6 逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出

表7　帳號管理控制措施 6

控制措施	逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出
適用等級	高
內容說明	▪將系統設定為機關所定義之操作閒置期限以自動登出帳號，可減少帳戶被盜用之風險。建議使用開發框架內建會談管理機制，通常已經過嚴謹測試，不僅方便使用，亦能提供足夠安全保護。 ▪若由開發人員自行設計帳號登出機制，應確保進行帳號登出時已確實將會談資料作廢。一種常見系統設計缺失是在逾期後僅將操作頁面導向登入畫面，卻仍然繼續留存著舊有會談資料，此時惡意使用者可能會利用瀏覽器網頁瀏覽紀錄或「回上一頁」功能，取得帳號

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出
	原始登入狀態。
驗證實務	▪如系統未在逾期時自動將使用者登出，則未符合此項控制措施。 ▪驗證人員可評估發展測試案例，如建立測試帳號並登入資通系統，閒置超過許可之期限後，再嘗試操作資通系統功能，此時資通系統應自動將使用者登出或要求重新登入始可操作資通系統功能。使用者閒置登出系統畫面示意圖，詳見圖 6。測試步驟可納入使用瀏覽器「回上一頁」功能，測試無法切換回到已登入狀態，以確保帳戶登出機制之有效性。  資料來源：本計畫整理
佐證資料	▪機關訂定之資通系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統應用程式原始碼或組態設定檔等與會談相關之設定值 ▪資通系統閒置自動登出功能之測試紀錄
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) ▪安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-14 非持續性)

資料來源：本計畫整理

圖6　使用者閒置自動登出

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.1.1.7 應依機關規定之情況及條件，使用資通系統

表8　帳號管理控制措施 7

控制措施	應依機關規定之情況及條件，使用資通系統
適用等級	高

內容說明	▪為強化資通系統安全性，系統管理者可限制各種不同使用情況及條件，使用者應符合所規定之使用規範。
	▪舉例說明：機關內部系統僅允許機關同仁利用 AD 目錄服務帳號登入，並限制帳號來源 IP 位址: 10.0.2.1~10.0.2.250，而資通系統後臺僅限管理者帳號利用本機位址(127.0.0.1)存取管理頁面，禁止從遠端登入管理者帳號。以 Apache Tomcat 9 為例，可透過組態設定檔案 manager.xml 內新增 RemoteAddrValve 參數，允許或拒絕特定來源位址之連線，設定 Apache Tomcat 僅開放本機存取設定範例，詳見圖 7。
	`<Context privileged="true">`
	`  <Valve className="org.apache.catalina.valves.RemoteAddrValve"`
	`  allow="127\.0\.0\.1"/>`
	`</Context>`
	資料來源：本計畫整理
	圖7　Apache Tomcat 僅限本機存取設定範例

驗證實務	▪如抽查發現帳號違規使用行為，則未符合此項控制措施。 ▪驗證人員宜檢視機關所訂定之資通系統使用規範，或訪談相關權責人員及檢視系統設定等方式，以了解機關許可之使用情況與條件。 ▪驗證人員可評估發展測試案例，以驗證這些條件限制是否確實有效。例如，若資通系統僅允許機關內部網路進行存取，驗證人員可測試使用外部網路能否連線登入系統。或可從系統日誌中檢視使用行為紀錄，查找違規使用行為，包含登入未經申請核可之帳號、從非許可網路來源或時段登入，以及違規之遠端存取行為等。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應依機關規定之情況及條件，使用資通系統
佐證資料	▪機關訂定之資通系統發展維護辦法 ▪資通系統帳號清查紀錄 ▪系統日誌
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)

資料來源：本計畫整理

2.1.1.8 監控資通系統帳號，如發現帳號違常使用時回報管理者

表9 帳號管理控制措施 8

控制措施	監控資通系統帳號，如發現帳號違常使用時回報管理者
適用等級	高
內容說明	▪帳號違常使用係指與使用者日常工作使用模式不相符之行為，例如於異常時間登入資通系統、於非業務期間存取重要系統服務、存取機敏資訊出現不正常瀏覽流量，或是頻繁觸發帳號身分驗證失敗等情況。 ▪資通系統帳號之監控，如部署各式資安監控防護產品，包含但不限於安全資訊事件管理(Security Information and Event Management, SIEM)、入侵偵測系統(Intrusion Detection System, IDS)、入侵預防系統(Intrusion Prevention System, IPS)、網站應用程式防火牆(Web Application Firewall, WAF)、身分識別與存取管理(Identity and Access Management, IAM)以及特權帳號管理(Privileged Account Manager, PAM)等，亦可評估導入 SOC 服務，或於資通系統設計異常警示功能，如實作系統例外處理(Exception Handling)機制，當發生帳號疑似惡意破解、越權存取及違規使用行為時提出警告。 ▪向管理者回報方式，如人工回報、於系統操作頁面顯示警告畫面，以及寄送警示信件或簡訊等各種通知方式。WAF 警示信件範例，詳見圖 8。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	監控資通系統帳號，如發現帳號違常使用時回報管理者
	 資料來源：本計畫整理 圖8　WAF 警示信件範例
驗證實務	▪ 如未具備資通系統帳號之異常行為監控及通報能力，則未符合此項控制措施。 ▪ 驗證人員宜檢視機關訂定之資通系統使用規範，或訪談相關權責人員及檢視系統設定等方式，了解系統帳號之監控及回報機制。 ▪ 驗證人員宜調閱系統監控紀錄，如 IDS/IPS 與 WAF 等資安設備或資通系統自建之系統日誌，檢視近期是否曾出現帳號違常行為，並追蹤後續處理紀錄及負責人員。 ▪ 驗證人員宜評估發展測試案例，以驗證確實具備發現帳號違常使用能力。例如，若欲驗證機關可發現帳號越權存取機敏資訊之行為，驗證人員宜利用測試帳號試圖存取未被授權之機敏資訊或系統功能頁面，觀察是否被監控機制所察覺並提出警示。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	監控資通系統帳號，如發現帳號違常使用時回報管理者
佐證資料	▪機關訂定之資通系統發展維護辦法 ▪監控防護相關紀錄，如 SOC 維運紀錄、WAF 日誌等 ▪資通系統日誌
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)

資料來源：本計畫整理

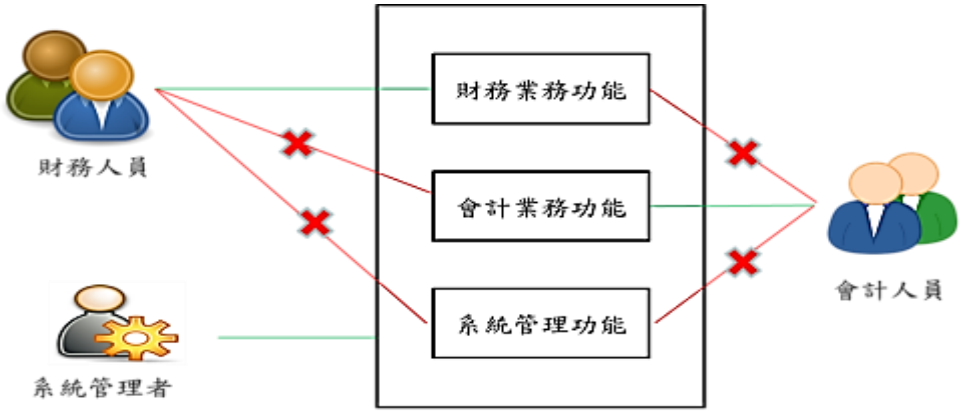
2.1.2 最小權限

2.1.2.1 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

表10 最小權限控制措施

控制措施	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
適用等級	中、高
內容說明	▪應依資通系統使用需求，賦予各級人員必要之系統存取權限。機關員工之系統存取權限，應以執行法定任務所必要者為限，例如不同業務單位因使用需求差異，所賦予資通系統存取權限亦會有所區別，應針對使用者及角色，僅賦予所需要之最低權限。軟體程序(process)及伺服器服務之執行權限，亦應符合最小權限原則，例如以一般使用者權限啟動執行，儘量避免使用系統管理者或最高權限。 ▪配發系統最高管理權限之人員及掌理重要技術與作業控制之特定人員帳號時，應經過審慎之評估與限制，防範非業務必要所需之機關人員與非機關使用者執行特權功能，如創建帳號、管理加密金鑰或變更系統重要組態設定等。機關亦可透過定期帳號權限清查，審核帳號使用者與其權限是否符合其業務所需之最小權限。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	▪ 資通系統應具備存取控制安全機制，採用最小權限之設計原則，機關可以考慮增設程序、使用者角色及系統帳號，並透過服務組態參數與存取控制列表等方式設定授權存取以實現最小權限。最小權限原則設計示意圖，詳見圖 9。圖中財務人員僅可存取財務業務相關系統功能，禁止存取會計業務功能與系統管理功能。  資料來源：本計畫整理 圖9　系統設計採用最小權限原則示意圖 ▪ 市面上亦發展多種帳號管理解決方案，可協助管理一般使用者與特權使用者帳號並控制其存取權限，如身分識別與存取管理(Identity and Access Management, IAM)與特權帳號管理(Privileged Account Manager, PAM)等。這些解決方案可快速建立一致性存取控制政策、部署存取規則及提供儀錶板操作檢視等，依產品類型不同，管理範圍包含系統、網路與主機之單一登入、使用者資料管理與認證及目錄服務(AD)等。
驗證實務	▪ 如抽查發現明確違反最小權限原則之使用行為，則未符合此項控制措施，如使用者所配發之帳號權限，明顯超出其業務存取範圍、浮濫發放特權帳號等。 ▪ 驗證人員宜檢視機關訂定之資通系統相關使用規範，或訪談相關權責人員及檢視系統設定等方式，檢視系統權限設定及特權帳號發放狀況。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	▪資通系統原則上應區分一般業務使用之權限與系統管理維護之權限，僅允許特權帳號存取系統管理維護相關功能頁面。驗證人員可評估發展測試案例，如利用一般業務使用之測試帳號，試圖存取系統管理維護網址及功能，系統應禁止存取該功能頁面。
佐證資料	▪機關訂定之資通系統發展維護辦法 ▪資通系統存取控制功能之測試紀錄
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-6 最小權限)

資料來源：本計畫整理

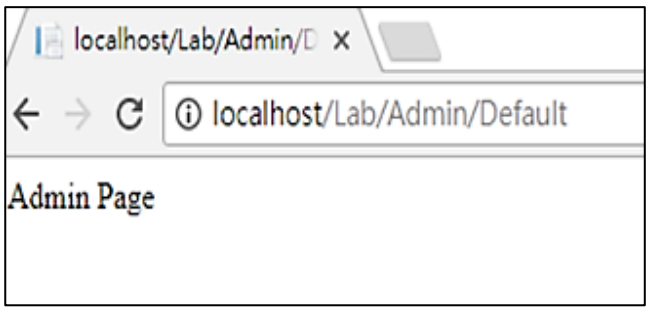
2.1.3 遠端存取

2.1.3.1 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

表11 遠端存取控制措施 1

控制措施	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
適用等級	普、中、高
內容說明	▪遠端存取係指使用者(或代表使用者行為程序)透過非本地端網路(如網際網路等)通信存取機關資通系統之連線行為，常用網路協定包含但不限於 HTTP(S)、SSH、遠端桌面(RDP)及 VPN 等。 ▪應控管資通系統所有允許之遠端連線行為，其中包含對於應用程式及作業系統資源之存取控制，應通過授權檢查後始可放行。例如，機關官方網站常會公開授權所有民眾存取，惟進階操作或後臺管理功能，則只開放給具有相應權限之使用者帳號使用，須完成身分驗證及授權檢查後，始可存取相關功能資源。為有效進行存取控制，資通系統應建立相關使用限制、組態需求及連線需求，其中包含使

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	用者身分類型、來源位址、連線人數上限、網路連線類型、開放時段、允許存取之功能資源及任何先備條件等限制。 ▪使用情境如資通系統為因應遠距辦公之需求而開放 VPN 連線存取，但限制使用者須為機關同仁透過 AD 帳號登入，並使用機關配發之 OA 電腦，檢測已安裝及更新防毒軟體後始可連線，連線後僅允許存取特定系統功能。 ▪將資通系統存取控制資訊文件化，有助於日常維運遵循與日後稽核查檢作業，如可將相關使用規範描述於資通系統開發維護文件或是統一規範於機關相關管理辦法。
驗證實務	▪如抽查發現資通系統未限制遠端存取行為或授權檢查機制無效，則未符合此項控制措施。 ▪驗證人員可評估發展測試案例；測試情境例如除系統公開頁面外，其餘功能頁面一律需通過帳號登入並取得系統授權後始能存取。參考測試步驟例如： 1.先使用測試帳號登入系統並存取功能頁面，操作畫面示意圖詳見圖 10。  資料來源：本計畫整理 圖10 測試系統授權機制範例 2.將頁面網址記錄下來(如範例 http://localhost/Lab/Admin/Default) 3.登出帳號。 4.在未登入帳號情況下，直接存取所記錄之頁面網址。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	5.此時系統應拒絕未經授權之存取行為，如要求使用者登入帳號或顯示錯誤訊息頁面。 ▪驗證人員宜檢視機關訂定之資通系統相關使用規範或訪談相關權責人員，並檢視機關所實作之安全控制措施；例如限制連線時段或系統功能、強制使用安全加密通道、建立黑(白)名單限制來源 IP 位址、主機及帳號等。 ▪機關所產出之文件化結果，包含相關管理辦法(如系統功能規格書、VPN 網路使用規定、委外廠商網路使用規範等)，以及組態設定或實行紀錄，如帳號或防火牆規則申請及開通紀錄等。
佐證資料	▪機關訂定之網路管理規範 ▪防火牆規則、存取控制列表(ACL) ▪資通系統存取控制功能之測試紀錄 ▪系統連線日誌
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-17 遠端存取) ▪安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication(控制措施編號 IA-2 內部使用者之識別與鑑別)

資料來源：本計畫整理

2.1.3.2 使用者之權限檢查作業應於伺服器端完成

表12 遠端存取控制措施 2

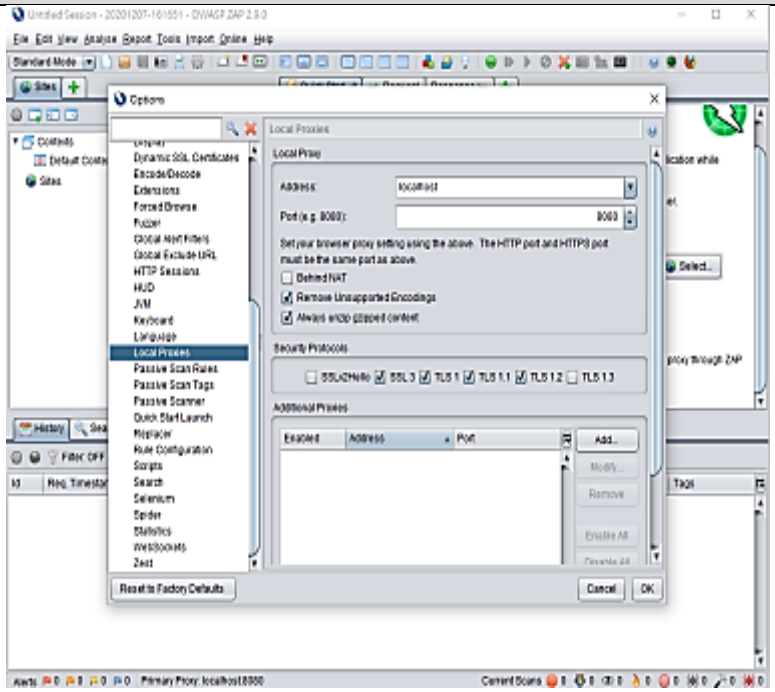
控制措施	使用者之權限檢查作業應於伺服器端完成
適用等級	普、中、高
內容說明	▪資通系統應檢查使用者存取權限，禁止未經系統授權存取行為；惟若系統將權限檢查作業實作於使用者端(如 JavaScript、Mobile App

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用者之權限檢查作業應於伺服器端完成
	等)則可視為無效，因其可能被惡意使用者利用竄改網站 Cookies 內容或網路封包內容等手法繞過檢查機制，故資通系統應於伺服器端實作授權檢查。
驗證實務	▪使用者進行遠端存取時，如系統未於伺服器端實作授權檢查作業，則未符合此項控制措施。 ▪驗證人員宜檢視資通系統之授權檢查實作方式，是否於伺服器端完成。因授權檢查機制通常較為複雜，驗證人員可先行檢視相關系統開發文件(如系統功能規格書等)，或由系統開發人員說明系統授權檢查實作方式，並提供應用程式原始碼或系統功能測試紀錄等相關佐證資料。 ▪欲驗證授權檢查之實作方式，驗證人員亦可評估發展測試案例，建置 OWASP Zed Attack Proxy (ZAP)或 Burp Suite 等代理伺服器(Proxy)，模擬惡意攻擊者攻擊手法以繞過客戶端之授權檢查。測試情境示意圖，詳見圖 11。  資料來源：本計畫整理 圖11 提權測試示意圖 ▪使用 ZAP 之測試參考步驟如下： 1.安裝並啟用 ZAP，選擇 Tools 功能頁簽 >> Options >> Local Proxies，詳見圖 12。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用者之權限檢查作業應於伺服器端完成



資料來源：本計畫整理

圖12 ZAP Proxy 畫面範例

2.調整電腦主機 Proxy 設定，讓其攔截所有流經瀏覽器之網路流量，詳見圖 13。

資料來源：本計畫整理

圖13 調整電腦主機 Proxy 設定範例

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用者之權限檢查作業應於伺服器端完成
	3. 利用一般業務使用之測試帳號，試圖存取系統管理功能頁面。 4.透過 Proxy 竄改網路封包內所攔截之授權資訊，對伺服器進行提權攻擊。常用手法如檢視是否存在「role」、「user」及「admin」等常用來記錄使用者身分之參數，例如將「role=user」竄改為「role=admin」，以將一般使用者權限提升至系統管理者權限。若成功竄改後系統允許存取特權功能，表示已順利繞過使用者端授權檢查，這也代表系統未於伺服器端有效檢查使用者授權。
佐證資料	▪機關訂定之網路管理規範 ▪資通系統存取控制功能測試紀錄
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-17 遠端存取) ▪安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication(控制措施編號 IA-2 內部使用者之識別與鑑別)

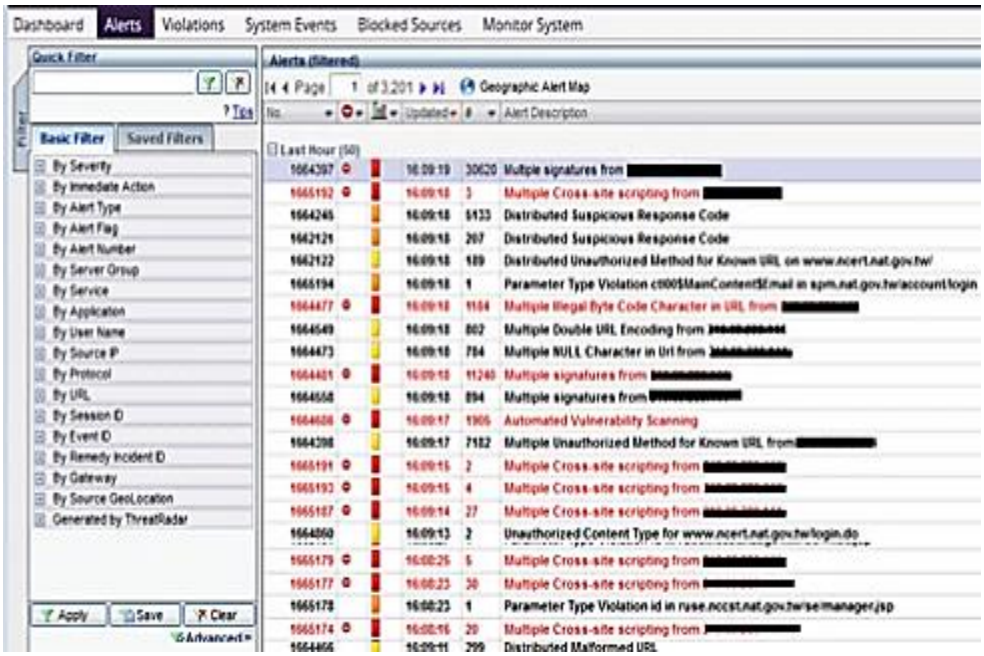
資料來源：本計畫整理

2.1.3.3 應監控遠端存取機關內部網段或資通系統後臺之連線

表13 遠端存取控制措施 3

控制措施	應監控遠端存取機關內部網段或資通系統後臺之連線
適用等級	普、中、高
內容說明	機關可能因使用需求，而允許機關內部使用者(如外點單位、居家辦公等)或廠商自遠端來源存取機關內部網段或資通系統後臺，以進行系統管理維護作業。實務上常透過 VPN 建立安全通道，以保護連線過程之機密性與完整性，惟此種遠端連線行為因具備高度資安風險，很可能被惡意攻擊者利用作為系統入侵管道，故機關宜使用網路安全監控設備(如 Firewall、WAF 及 IPS/IDS 等)或服務(如 SOC 監控等)，監控遠端存取機關內部網段或資通系統後臺之連線，以及時發現異常連線或惡意攻擊行為。WAF 監控資通系統後

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應監控遠端存取機關內部網段或資通系統後臺之連線
	臺範例，詳見圖 14。  資料來源：本計畫整理 圖14 WAF 監控資通系統後臺範例
驗證實務	▪ 如未監控遠端存取機關內部網段或資通系統後臺之連線，則未符合此項控制措施。 ▪ 驗證人員宜訪談相關權責人員(如網路管理者、監控人員等)，並檢視機關相關規定，以了解如何監控資通系統遠端連線。
佐證資料	▪ 機關訂定之系統監控程序 ▪ 系統監控紀錄
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-17 遠端存取)

資料來源：本計畫整理

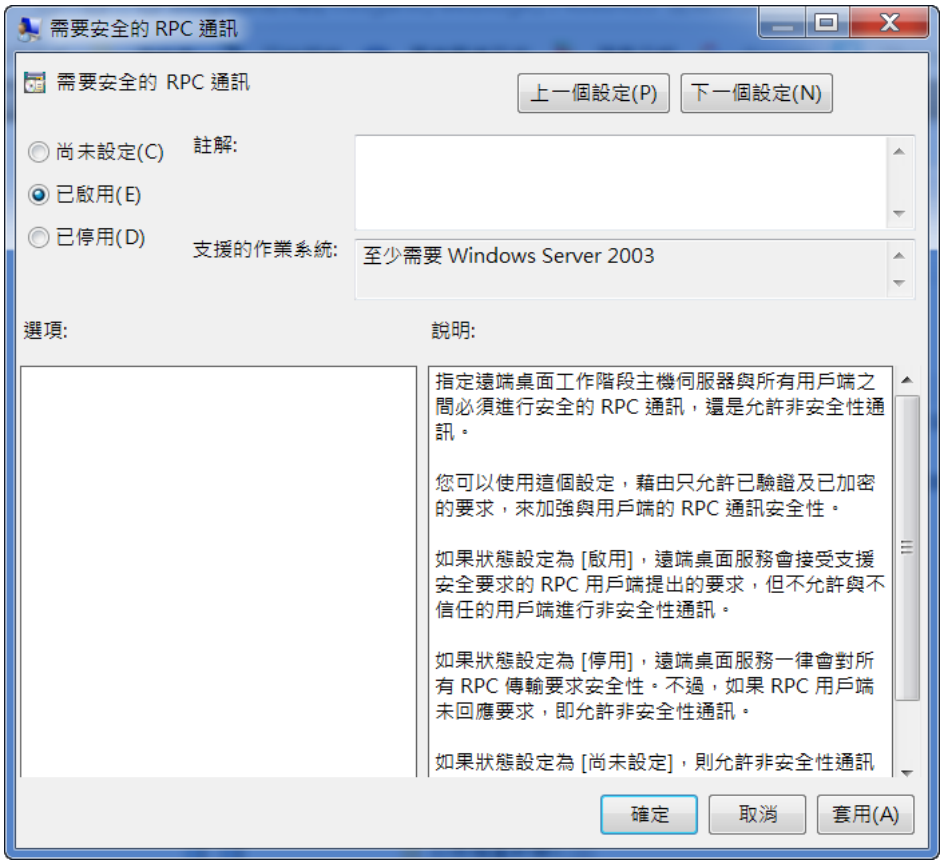
2.1.3.4 應採用加密機制

本文件之智慧財產權屬數位發展部資通安全署擁有。

表14 遠端存取控制措施 4

控制措施	應採用加密機制
適用等級	普、中、高
內容說明	▪為保護遠端存取連線之機密性與完整性，資通系統應採用加密機制以建立安全通道，最常見應用如啟用 HTTPS TLS 1.2 加密傳輸協定等。實務上機關可能因居家辦公等使用需求，而允許同仁或系統維護人員遠端存取內部網段之服務或資通系統後臺，此時常會建立 VPN 安全通道，並可限制遠端來源以降低存取風險，VPN 遠端存取資通系統服務範例，詳見圖 15。  資料來源：本計畫整理 圖15 VPN 遠端存取資通系統服務範例 ▪如資通系統允許管理人員透過遠端桌面服務登入伺服器進行維護操作，為降低被駭客利用遠端桌面服務入侵之機率，亦應強化伺服器本機資安防護設定，啟用加密連線機制。如參照政府組態基準之建議，於 Windows Server 環境啟用「需要安全的 RPC 通訊」組態設定，RPC 介面是用於管理及設定遠端桌面服務，啟用安全的 RPC 通訊後，遠端桌面服務只會接受支援安全要求的 RPC 用戶端提出要求，禁止與未受信任用戶端進行非安全性通訊，以此加強與用戶端遠端桌面服務連線安全性。組態設定路徑為「電腦設定\系統管理範本\Windows 元件\遠端桌面服務\遠端桌面工作階段主機\安全性\需要安全的 RPC 通訊」，設定畫面範例詳見圖 16。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應採用加密機制
	 資料來源：本計畫整理 圖16 設定遠端桌面加密連線範例
驗證實務	▪如所允許之任何資通系統遠端存取連線未採用加密保護，則未符合此項控制措施。 ▪驗證人員宜檢視機關訂定之資通系統相關規範，並訪談相關權責人員(如網路管理者者、系統管理者等)或檢視系統設定，以確認資通系統所使用之遠端存取連線加密機制。 ▪驗證人員宜評估發展測試案例，模擬遠端連線之行為，以驗證加密機制之有效性。測試情境例如使用 HTTP 進行未加密之網頁存取，或在未建立 VPN 連線情況下遠端存取系統功能頁面，系統應拒絕連線或強制導向至 HTTPS 加密頁面。
佐證資料	▪機關訂定之網路管理規範

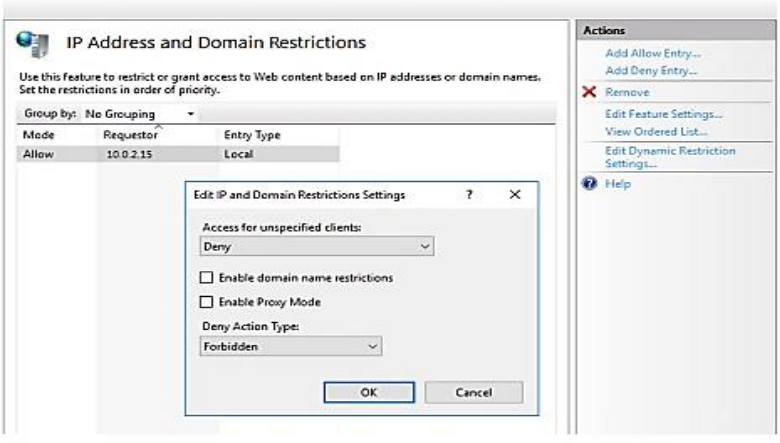
本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應採用加密機制
	▪ 資通系統加密連線之測試紀錄
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-17 遠端存取)

資料來源：本計畫整理

2.1.3.5 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

表15 遠端存取控制措施 5

控制措施	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
適用等級	中、高
內容說明	▪ 遠端存取行為應通過授權後始可放行，若有必要允許外部遠端存取之系統功能時，應限制遠端存取控制點以降低遭受攻擊機會，如識別來源主機、來源端 IP 位址、目的端 IP 位址、埠口及通訊協定等連線限制，避免全面性開放存取。 ▪ 以 Winows IIS 伺服器為例，可利用「IP Address and Domain Restrictions」功能，設定來源網址黑(白)名單，設定範例詳見圖 17。  資料來源：本計畫整理 圖17 IIS 限制連線來源操作範例

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
驗證實務	▪如未定義及管理之資通系統遠端存取來源或是管理過濾機制無效，則未符合此項控制措施。例如，若允許外點單位、同仁遠距辦公或系統維運廠商等進行遠端連線存取資通系統，此時應建立白名單連線清單，如部署防火牆連線規則或調整系統組態設定，以過濾未經授權之連線來源。 ▪驗證人員宜檢視機關訂定之資通系統相關使用規範，並訪談相關權責人員(如網路管理者、系統管理者等)或檢視系統設定，以確認機關所定義之存取控制點。 ▪驗證人員宜評估發展測試案例，模擬未授權之遠端連線之行為，如使用未預先定義之來源 IP，系統應拒絕存取。
佐證資料	▪機關訂定之網路管理規範 ▪機關部署之防火牆規則、ACL ▪資通系統存取控制功能測試紀錄 ▪系統連線日誌
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-17 遠端存取)

資料來源：本計畫整理

2.2 事件日誌與可歸責性

2.2.1 記錄事件

2.2.1.1 訂定日誌之記錄時間週期及留存政策，並保留日誌至少 6 個月

表16 記錄事件控制措施 1

控制措施	訂定日誌之記錄時間週期及留存政策，並保留日誌至少 6 個月
適用等級	普、中、高
內容說明	▪應訂定相關管理辦法以妥善留存資通系統日誌，如作業系統日誌(OS event log)、網站日誌(Web log)、應用程式日誌(AP log)及登入

本文件之智慧財產權屬數位發展部資通安全署擁有。

<table>
<tr><td>控制措施</td><td>訂定日誌之記錄時間週期及留存政策，並保留日誌至少 6 個月</td></tr>
<tr><td></td><td>
日誌(logon log)等，以符合程式除錯、行為歸責、稽核取證及法律規範等用途。資通系統日誌留存期限應至少保留 6 個月。
▪ 日誌留存管理規範範例，詳見圖 18。
(一)作業系統及應用系統之日誌(帳號登入、帳號登出、存取成功、存取失敗、管理者行為、系統組態變更等資訊) 至少需留存六個月，並應視其重要性進行必要備份及保護，避免竄改及未經授權之存取。
資料來源：本計畫整理
圖18 日誌留存管理規範範例
▪ 依據「各機關資通安全事件通報及應變處理作業程序」之規定，各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌，並定期備份於外部設備，其保存範圍及項目詳見圖 19。
<table>
<tr><th>資通安全責任等級</th><th>保存範圍</th><th>保存項目</th></tr>
<tr><td>A</td><td>機關應保存全部資通系統與各項資通及防護設備最近六個月之日誌紀錄。</td><td rowspan="3">1. 作業系統日誌(OS event log)
2. 網站日誌(web log)
3. 應用程式日誌(AP log)
4. 登入日誌(logon log)</td></tr>
<tr><td>B</td><td>機關應保存全部核心資通系統與相連之資通及防護設備最近六個月之日誌紀錄。</td></tr>
<tr><td>C</td><td>機關應保存全部核心資通系統最近六個月之日誌紀錄。</td></tr>
</table>
資料來源：本計畫整理
圖19 資通系統日誌保存範圍及項目
</td></tr>
</table>

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	訂定日誌之記錄時間週期及留存政策，並保留日誌至少 6 個月
驗證實務	▪如未訂定日誌之記錄時間週期及留存政策，或實際留存日誌未達 6 個月，則未符合此項控制措施。 ▪驗證人員宜檢視機關訂定之系統日誌留存規範，並訪談相關權責人員(如系統管理者等)，以確認機關所規定紀錄留存時間週期與政策。 ▪驗證人員宜抽查資通系統日誌，如作業系統日誌(OS event log)、網站日誌(Web log)、應用程式日誌(AP log)及登入日誌(logon log)等，確認已包含 6 個月日誌內容。
佐證資料	▪機關訂定之日誌相關管理辦法 ▪資通系統日誌
參考文獻	▪各機關資通安全事件通報及應變處理作業程序 ▪安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-11 日誌之保存)

資料來源：本計畫整理

2.2.1.2 確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件

表17 記錄事件控制措施 2

控制措施	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件
適用等級	普、中、高
內容說明	資通系統事件係指任何發生在機關資通系統中可觀察到行為之結果，當具備資安風險之特定系統事件發生時，資通系統應觸發記錄系統日誌功能，以描述事發時系統狀態。為使日誌分析可有效發揮作用，機關應仔細評估系統使用需求與資安風險後，定義哪些系統事件需要留下日誌，避免記錄功能流於形式，惟亦應避免留存不必要之系統事件日誌，過於冗雜之內容對日誌分析活動沒有幫助，反

本文件之智慧財產權屬數位發展部資通安全署擁有。

<table>
<tr><td>控制措施</td><td>確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件</td></tr>
<tr><td></td><td>而可能危害系統效能及儲存空間。記錄一般帳號帳號登入之系統事件日誌範例，詳見圖 20。
Data Output Explain Messages Notifications Scratch Pad
<table><tr><th></th><th>id
[PK] integer</th><th>action_type
text</th><th>action_descr
text</th><th>user_id
integer</th><th>log_time
timestamp without time zone</th></tr><tr><td>1</td><td>25608</td><td>登入</td><td>一般帳號登入</td><td>365</td><td>2020-08-24 08:57:59.568</td></tr><tr><td>2</td><td>25581</td><td>登入</td><td>一般帳號登入</td><td>364</td><td>2020-08-18 14:49:49.372</td></tr><tr><td>3</td><td>25578</td><td>登入</td><td>一般帳號登入</td><td>364</td><td>2020-08-18 14:38:03.659</td></tr><tr><td>4</td><td>25576</td><td>登入</td><td>一般帳號登入</td><td>365</td><td>2020-08-18 14:37:23.165</td></tr></table>
資料來源：本計畫整理

圖20 記錄一般帳號登入事件範例

實務上建議可包含(但不限於)以下系統事件：
▪管理者行為(如調整系統組態、異動系統帳號等)
▪身分驗證失敗(如帳號登入失敗、觸發帳戶鎖定等)
▪存取資源失敗(如頁面失效、資料庫連線失敗等)
▪功能錯誤(如系統功能無法使用、帳戶無法登入等)
▪重要資料異動(如存取個人資料或機敏資訊等)
▪重要操作行為(如變更個人密碼、金融轉帳交易等)</td></tr>
<tr><td>驗證實務</td><td>▪如資通系統未能於特定資通系統事件發生時產生相關日誌，則未符合此項控制措施。
▪驗證人員宜檢視機關訂定之資通系統相關使用規範，並訪談相關權責人員(如系統管理者等)，以了解機關所決定應記錄之資通系統事件，並可抽查資通系統日誌，檢視其中已留存之資通系統事件，或評估委由相關權責人員(如系統管理者等)提供程式原始碼或其他佐證資料，以確認系統已具備記錄特定事件之功能。</td></tr>
<tr><td>佐證資料</td><td>▪機關訂定之日誌相關管理辦法
▪資通系統日誌</td></tr>
</table>

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-2 記錄事件)

資料來源：本計畫整理

2.2.1.3 應記錄資通系統管理者帳號所執行之各項功能

表18 記錄事件控制措施 3

控制措施	應記錄資通系統管理者帳號所執行之各項功能
適用等級	普、中、高
內容說明	資通系統管理者帳號具有最高系統操作權限，無論是故意或非故意操作行為，都具有高度操作風險，可能對機關產生重大且不利影響，而駭客入侵時，亦常試圖取得系統管理者帳號權限，以進行更進一步攻擊行為，故記錄管理者帳號執行各項功能，不僅有助於強化內部控制與稽核，亦有助於追蹤資安事件行為軌跡。記錄管理者帳號帳號登入之系統事件日誌範例，詳見圖 21。
驗證實務	▪ 如資通系統未記錄系統管理者帳號所執行之各項功能，則未符合此項控制措施。

Data Output | Explain | Messages | Notifications | Scratch Pad

	id [PK] integer	action_type text	action_descr text	user_id integer	log_time timestamp without time zone
1	25607	登入	機關管理者帳號登入	258	2020-08-24 08:56:28.994
2	25605	登入	機關管理者帳號登入	258	2020-08-20 14:36:56.266
3	25604	登入	機關管理者帳號登入	258	2020-08-20 14:32:32.808
4	25602	登入	機關管理者帳號登入	258	2020-08-20 13:50:21.884
5	25600	登入	機關管理者帳號登入	258	2020-08-20 11:58:05.661
6	25598	登入	機關管理者帳號登入	258	2020-08-20 11:54:57.422
7	25596	登入	機關管理者帳號登入	258	2020-08-20 11:51:12.689

資料來源：本計畫整理

圖21 記錄管理者帳號登入事件範例

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應記錄資通系統管理者帳號所執行之各項功能
	▪驗證人員宜檢視機關訂定之資通系統相關使用規範，並訪談相關權責人員(如系統管理者等)，以了解機關如何記錄資通系統管理者帳號行為。 ▪驗證人員宜抽查資通系統日誌，其中已留存之管理者帳號功能執行紀錄，建議至少可抽查以下項目： – 管理者帳號登入與登出 – 管理者帳號密碼變更 – 異動使用者帳號密碼、鎖定狀態及存取權限等 – 異動系統重要功能組態 – 存取機敏資訊，如使用者個人資料、帳戶資訊等
佐證資料	▪機關訂定之日誌相關管理辦法 ▪資通系統日誌
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-2 記錄事件)

資料來源：本計畫整理

2.2.1.4 應定期審查機關所保留資通系統產生之日誌

表19 記錄事件控制措施 4

控制措施	應定期審查機關所保留資通系統產生之日誌
適用等級	中、高
內容說明	▪應定期審查分析資通系統產生之日誌內容，以掌握是否在期間內曾發生重要資安事件，如異常存取行為、重大系統錯誤等。日誌審查規範範例，詳見圖 22。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應定期審查機關所保留資通系統產生之日誌
	(1) 應用系統屬於中風險等級以上者，應每季審查稽核事件(帳號異動、密碼異動、登入失敗)，檢視已稽核的事件集合仍有必要且已滿足稽核需求。 資料來源：本計畫整理 圖22 日誌審查規範範例 ▪市面上有多款日誌管理(Log Management)或資安事件管理(Security Information Event Management，SIEM)解決方案，其功能為自動化收集各種系統元件或設備所產生日誌，並在符合資通安全政策及相關法規要求下，進行日誌收容、事件分類、日誌關聯分析、日誌監看、觸發警告及建立報表等功能，可協助相關權責人員進行日誌分析與管理審查活動，減輕管理人員負擔。 ▪應參考所訂定之日誌留存政策並決定日誌審查之週期。例如，若機關規定日誌留存期限為 6 個月，則至少應每 6 個月內完成 1 次以上之審查活動。
驗證實務	▪如未定期審查資通系統日誌，則未符合此項控制措施。 ▪驗證人員宜檢視機關訂定之資通系統相關使用規範，並訪談相關權責人員(如系統管理者等)，以了解審查記錄事件之執行方式與週期。 ▪驗證人員宜檢視所留存之記錄事件審查紀錄，以驗證機關已確實完成定期審查。
佐證資料	▪機關訂定之日誌相關管理辦法 ▪日誌審查紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-2 記錄事件)

資料來源：本計畫整理

2.2.2 日誌紀錄內容

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.2.2.1 資通系統產生之日誌應包含事件類型、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，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊

表20 日誌紀錄內容控制措施

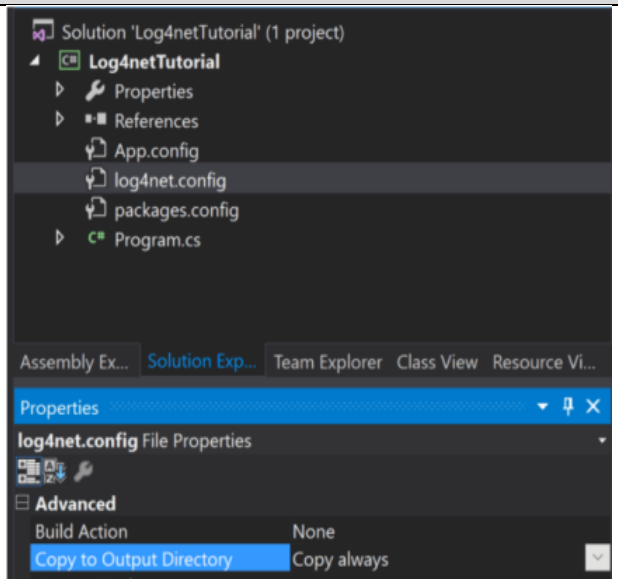
控制措施	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊
適用等級	普、中、高
內容說明	▪ 日誌應詳細描述所觸發事件，包含人、事、時、地、物等關鍵資訊，如使用者帳號、時間、執行之功能或存取之資源名稱、事件類型或優先等級、執行結果或事件描述、事件發生當下相關物件資訊、網路來源與目的位址，以及錯誤代碼等。惟須注意應避免在日誌內留下個人資料及涉及隱私內容，以符合我國個人資料保護法相關規定。 ▪ 日誌輸出格式可讀性對日誌關聯分析效率影響甚鉅，尤其資通系統開發人員常會利用開發框架內建或第三方所提供日誌記錄工具或函式庫留存客製化日誌內容，此時若因各程式功能模組實作差異或是多位開發人員不同程式撰寫習慣，就很容易產生不同格式日誌，不利於進行日誌分析。例如，使用.NET 開發框架資通系統，開發人員可能選擇使用.NET Logger、Apache Log4NET 及 NLog 等元件產生日誌，而 Java 資通系統則可能選擇 Java Util Logging 或 Apache Log4j 等元件。資通系統日誌格式上混雜，如功能模組 1 日期格式採用 MM-DD-YYYY，而功能模組 2 卻採用 YYYY/MM/DD。為減少這種日誌格式混雜現象，宜要求委外廠商或內部開發人員遵照一致性程式撰寫標準(Coding Standard)，避免同時混用多種日誌框架與不同格式，以確保日誌內容品質。 ▪ 應確保日誌已納入所有必要資訊。日誌需求包含系統維運或業務使用需求等，同時也要考慮法律規章、行政命令、政策、產業標準及合約等要求。適用情境，例如「電子支付機構資訊系統標準

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統產生之日誌應包含事件類型、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，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊
	及安全控管作業基準辦法」第 13 條第五款規定：「電子支付作業環境之個人資料保護應建置留存個人資料使用軌跡(如登入帳號、系統功能、時間、系統名稱、查詢指令或結果)或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況，包括檔案、螢幕畫面、列表。」，資通系統如涉及電子支付作業，為符合此項規範就應依規定將登入帳號、系統功能、時間、系統名稱、查詢指令或結果等資訊納入系統日誌內。
驗證實務	▪如資通系統在特定事件發生時，所留存之日誌未提供足夠之人、事、時、地、物等關鍵資訊，造成難以進行分析活動，該筆日誌內容實際上並無效用，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之資通系統相關規範，並訪談相關權責人員(如系統管理者等)，以了解資通系統使用之日誌機制與格式。 ▪驗證人員宜抽查日誌內容，確認記錄事件之描述已充分表達該事件之關鍵訊息，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。 ▪驗證人員宜檢視資通系統原始碼或設定檔，從中找尋違規之混用情況，如同時使用 Java Util Logging 與 Apache Log4j，或是同時混用 NET Logger、Apache Log4NET 及 NLog 等多種日誌框架。例如，若發現.NET 站台程式目錄內，同時存在 log4net.config 與 NLog.config 兩個組態設定檔案，則可能是因為同時混用 Apache Log4NET 及 NLog 日誌機制，此時宜從程式碼中進一步確認其使用情況。log4net.config 檔案範例詳見圖 23。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統產生之日誌應包含事件類型、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，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊



資料來源：本計畫整理

圖23 log4net.config 檔案範例

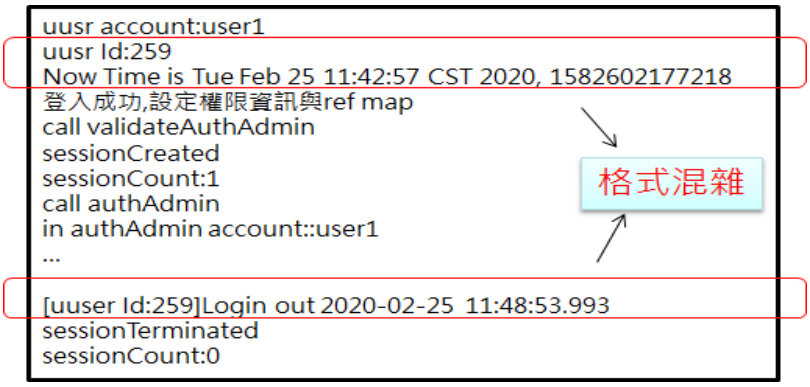
- 驗證人員宜抽查日誌，檢視格式是否混雜而難以分析，則未符合此項控制措施要求。實務上若將資通系統日誌留存於資料庫內，通常因資料庫欄位型別限制，所以格式容易統一並具較高可讀性，範例詳見圖 24。若留存於檔案內之日誌，則因開發人員可自行設計日誌格式，而較易產生雜亂內容，範例詳見圖 25。

	id [PK] integer	action_type text	action_descr text	user_id integer	log_time timestamp without time zone
1	25608	登入	一般帳號登入	365	2020-08-24 08:57:59.568
2	25607	登入	機關管理者帳號登入	258	2020-08-24 08:56:28.994
3	25605	登入	機關管理者帳號登入	258	2020-08-20 14:36:56.266
4	25604	登入	機關管理者帳號登入	258	2020-08-20 14:32:32.808
5	25587	登入	機關管理者帳號登入	258	2020-08-19 16:33:58.833
6	25583	登入	機關管理者帳號登入	400	2020-08-19 14:17:18.19
7	25582	登入	一般帳號登入	366	2020-08-19 09:00:03.971

資料來源：本計畫整理

圖24 日誌輸出格式具一致性範例

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統產生之日誌應包含事件類型、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，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊
	 資料來源：本計畫整理 圖25 日誌輸出格式未具一致性範例 ▪ 如資通系統產生之日誌未依需求充分納入必要資訊，則未符合此控制措施。驗證人員宜檢視機關訂定之資通系統相關規範，並訪談相關權責人員(如系統管理者等)，以了解資通系統之日誌需求，包含資通系統適用之法律規章、行政命令、政策、產業標準及合約等，並可抽查日誌，以檢視是否已留存必要資訊。
佐證資料	▪ 機關訂定之日誌相關管理辦法 ▪ 資通系統 RFP ▪ 資通系統日誌
參考文獻	▪ 安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-12 稽核的產生) ▪ 安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-3)

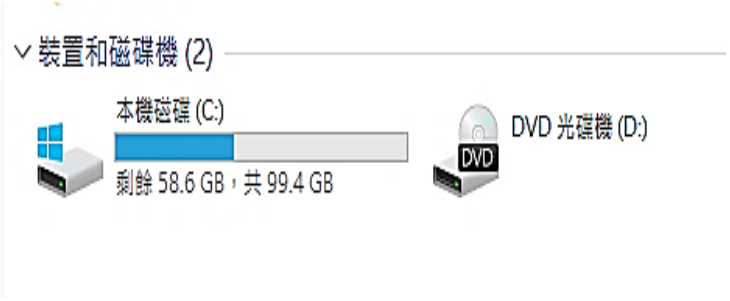
資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.2.3 日誌儲存容量

2.2.3.1 依據日誌儲存需求，配置所需之儲存容量

表21 日誌儲存容量控制措施

控制措施	依據日誌儲存需求，配置所需之儲存容量
適用等級	普、中、高
內容說明	資通系統應配置足夠之日誌儲存容量，如硬碟或資料庫空間，以避免因容量不足造成日誌損失或是降低記錄能力，此時可透過檢查剩餘容量即可推算是否符合日誌儲存需求，如系統若將日誌檔案留存於本機磁碟(C)內，檢查硬碟剩餘空間範例詳見圖 26。  資料來源：本計畫整理 圖26 檢查硬碟剩餘空間範例 亦可實作其他控制措施以維持可用之儲存空間，例如： ▪ 定期檢查剩餘容量 ▪ 超過容量警戒值時通知相關人員 ▪ 定期壓縮或歸檔日誌 ▪ 定期刪除超過保存期限之日誌
驗證實務	▪ 如資通系統未規劃足夠之日誌儲存容量，使得儲存空間滿載而危害日誌處理機制，或未有其他有效配套措施足以符合日誌儲存需求，則未符合此控制措施。 ▪ 驗證人員宜檢視機關訂定之資通系統相關規範，並訪談相關權責人員(如系統管理者與資料庫管理者等)，以了解日誌儲存方式

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	依據日誌儲存需求，配置所需之儲存容量
	及容量規劃，或使用其他可有效維持儲存空間之機制。 ▪驗證人員宜確認所配置之日誌儲存空間，可有效應付日誌成長速度，如機關規定日誌須至少保存 6 個月，而資通系統平均每個月可產生之 1GB 日誌量，若規劃之儲存空間少於 6GB 則容易發生容量不足情況，原則上應規劃更充足之儲存空間。
佐證資料	▪機關訂定之日誌相關管理辦法 ▪資通系統日誌主機或資料庫容量資訊
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-4 日誌儲存容量)

資料來源：本計畫整理

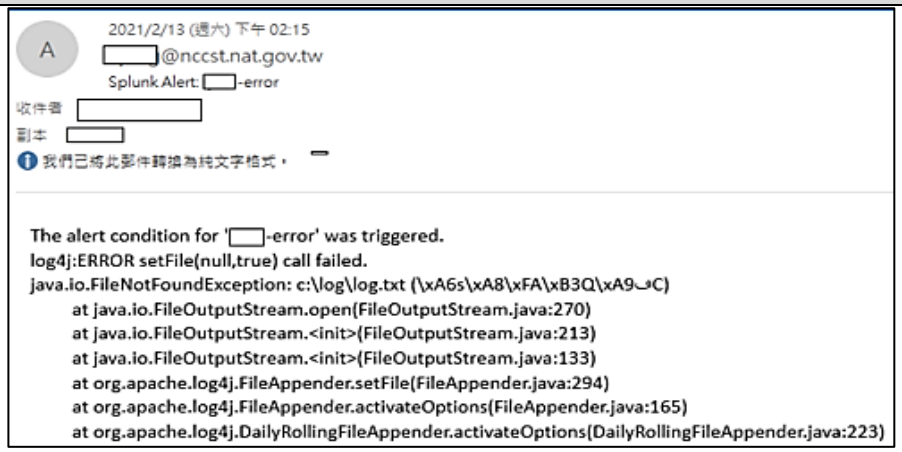
2.2.4 日誌處理失效之回應

2.2.4.1 資通系統於日誌處理失效時，應採取適當之行動

表22 日誌處理失效之回應控制措施 1

控制措施	資通系統於日誌處理失效時，應採取適當之行動
適用等級	普、中、高
內容說明	應識別任何可能造成資通系統引發日誌處理失效狀況，並評估可能對資通系統造成之危害。日誌處理失效狀況，如軟/硬體錯誤、無法順利產生或留存日誌，以及日誌儲存容量飽和或超過等。可評估為不同日誌處理失效選擇定義額外動作(如依類型、依地理位置、依嚴重程度，或這些因素組合)，因應資通系統日誌處理失效之處理行動須符合機關資安規範與系統使用需求，如於系統畫面顯示警示訊息、覆寫最舊之日誌(惟仍須確保符合日誌保留 6 個月以上之規定)、或以信件、簡訊或其他方式警示特定人員或角色等各種適當方式，警示信件範例詳見圖 27。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統於日誌處理失效時，應採取適當之行動
	 資料來源：本計畫整理 圖27 紀錄處理失效警示信件範例
驗證實務	▪ 如未分析評估任何可能造成資通系統日誌處理失效原因，或未規劃日誌處理失效因應措施，則未符合此控制措施。 ▪ 驗證人員宜檢視機關訂定之資通系統相關規範，並訪談相關權責人員(如系統管理者與資料庫管理者等)，以了解資通系統發生日誌處理失效時會採用之處理行動，該行動之適當性應以符合機關營運目標及資安政策為判定原則。 ▪ 驗證人員可評估發展測試案例，模擬日誌處理失效狀況，如關閉日誌伺服器(Log Server)服務、關閉資料庫服務、網路斷線，以及填滿日誌儲存空間(如硬碟)等方式，並檢視資通系統應變方式。若測試結果引發非預期錯誤行為或與先前規劃有大幅落差，則未符合此項控制措施要求。
佐證資料	▪ 機關訂定之日誌相關管理辦法 ▪ 資通系統日誌處理失效之測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-5)

資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.2.4.2 機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告

表23 日誌處理失效之回應控制措施 2

控制措施	機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告
適用等級	高
內容說明	▪應依照資安政策或相關規定,定義需要即時通報之特定記錄失效事件、時效及特定通知對象。 ▪資通系統應依定義實作相關通知機制,以利及早釐清事件發生原因並進行故障排除。例如，當日誌伺服器無法連線造成日誌寫入失敗時，即時以信件或簡訊通知系統管理者。 ▪如機關未另外訂定管理辦法，仍須遵循我國相關法規進行通報作業，如「資通安全事件通報及應變辦法」等。
驗證實務	▪如需要即時通報之日誌處理失效事件發生時,未於規定之時效內對特定人員提出警告，則未符合此項控制措施。 ▪驗證人員宜檢視機關訂定之資通系統相關規範,並訪談相關權責人員(如系統管理者與資安人員等)，確認機關規定需要即時通報之記錄失效事件，並進一步確認規定之時效與通知對象。
佐證資料	▪機關訂定之日誌相關管理辦法或通報應變作業程序 ▪資通系統日誌處理失效之測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-5)

資料來源：本計畫整理

2.2.5 時戳及校時

2.2.5.1 資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)

本文件之智慧財產權屬數位發展部資通安全署擁有。

表24 時戳及校時控制措施 1

控制措施	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)
適用等級	普、中、高
內容說明	系統日誌所留存時戳在日誌分析活動中扮演相當重要的角色，應確保其記錄時間之正確性與可讀性，以助於建立系統事件時間軸。資通系統管理者應確認作業系統內部時鐘設定為正確時間，並避免使用過於特殊之時戳格式，通常可使用世界協調時間(UTC)、格林威治標準時間(GMT)或本地時間與 UTC 偏移時間來表示。日誌時戳使用範例詳見圖 28。  資料來源：本計畫整理 圖28 日誌時戳範例
驗證實務	▪如資通系統日誌內未留存時戳，或時戳非由系統內部時鐘所產生而無法對應到 UTC 或 GMT 時間格式，造成日誌分析活動難以進行，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之資通系統相關規範，並訪談相關權責人員(如系統管理者等)，以了解資通系統日誌時戳產生方式與格式。 ▪驗證人員宜確認資通系統日誌內時戳是否與作業系統時鐘一致，並檢視日誌所產生之時戳格式，應足以辨識並可方便轉換至 UTC 或 GMT 時間格式。
佐證資料	▪機關訂定之日誌相關管理辦法 ▪資通系統日誌

	id [PK] integer	action_type text	action_descr text	user_id integer	log_time timestamp without time zone
1	25608	登入	一般帳號登入	365	2020-08-24 08:57:59.568
2	25607	登入	機關管理者帳號登入	258	2020-08-24 08:56:28.994
3	25605	登入	機關管理者帳號登入	258	2020-08-20 14:36:56.266
4	25604	登入	機關管理者帳號登入	258	2020-08-20 14:32:32.808
5	25587	登入	機關管理者帳號登入	258	2020-08-19 16:33:58.833
6	25583	登入	機關管理者帳號登入	400	2020-08-19 14:17:18.19
7	25582	登入	一般帳號登入	366	2020-08-19 09:00:03.971

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)
參考文獻	▪ 安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-8 時戳) ▪ 安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-12 稽核的產生)

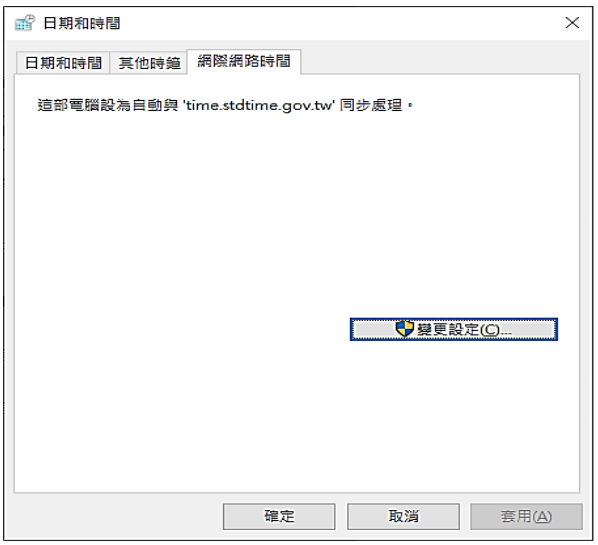
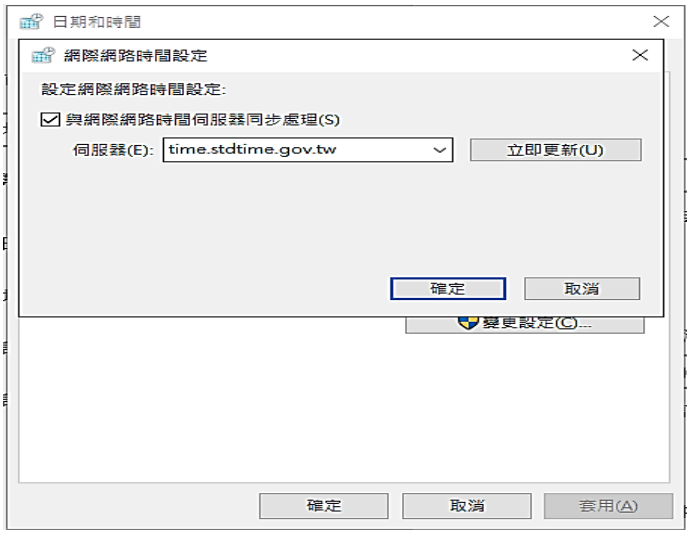
資料來源：本計畫整理

2.2.5.2 系統內部時鐘應定期與基準時間源進行同步

表25 時戳及校時控制措施 2

控制措施	系統內部時鐘應定期與基準時間源進行同步
適用等級	中、高
內容說明	資通系統應使用系統內部時鐘產生日誌所需時戳，而內部時鐘亦應定期進行同步以確保時間正確性。若以人工定期校正時間雖仍可保持時間正確性，但效率不佳且容易疏漏，故實務上常使用網際網路時間伺服器(NTP Server)或由機關自建之伺服器，並設定由系統依排程自動同步處理。使用情境如 AD 成員主機向 AD 伺服器同步時間，而 AD 伺服器則與網際網路伺服器(如 time.stdtime.gov.tw 等)進行同步。
驗證實務	▪ 如系統內部時鐘未定期成功與基準時間源進行同步，則未符合此項控制措施。 ▪ 驗證人員宜檢視機關訂定之資通系統相關規範，並訪談相關權責人員(如系統管理者、AD 或 NTP 伺服器管理者等)，以了解資通系統時間同步機制之規定。 ▪ 驗證人員可初步檢視資通系統內部時鐘所顯示時間是否與真實時間存在明顯落差，並可進一步發展測試案例，驗證資通系統內部時鐘之同步機制。例如，若資通系統係採用 Windows 作業系統，可檢視系統控制台，「時鐘和區域」項目之「日期和時間」設定，點選「網際網路時間」設定頁簽，範例詳見圖 29，

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	系統內部時鐘應定期與基準時間源進行同步
	如範例中顯示已設定為依排程自動同步處理。  資料來源：本計畫整理 圖29 Windows 主機日期與時間設定 ▪ 驗證人員宜進一步確認設定值正確有效，可點選「變更設定」後，確認「與網際網路時間伺服器同步處理」已確實勾選，並按下「立即更新」，範例詳見圖 30。  資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	系統內部時鐘應定期與基準時間源進行同步
	圖30 手動執行網際網路時間同步操作範例 ▪檢視網際網路時間同步執行結果，確認顯示成功完成同步處理，成功完成同步訊息範例詳見圖 31。若顯示同步失敗錯誤訊息，代表可能因伺服器位址設定錯誤或被防火牆阻擋等原因而無法成功進行同步，則仍未符合此項控制措施。  資料來源：本計畫整理 圖31 成功完成同步處理畫面範例
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統時間同步之測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-8 時戳)

資料來源：本計畫整理

2.2.6 日誌資訊之保護

2.2.6.1 對日誌之存取管理，僅限於有權限之使用者

表26 日誌資訊之保護控制措施 1

控制措施	對日誌之存取管理，僅限於有權限之使用者
適用等級	普、中、高
內容說明	日誌應妥善留存，以符合程式除錯、行為歸責、稽核取證及法律

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	對日誌之存取管理，僅限於有權限之使用者
	規範等使用需求，且其中可能存在機敏資訊，故應禁止未授權之存取、刪除及修改。應施行日誌(及其備份)之存取控管，僅限有權限之特定人員(如系統或資料庫管理者等)存取日誌(如日誌檔案或日誌主機等)，以保護機密性、完整性及可用性，此存取控制可能利用實體安全、系統功能實作帳號與權限管理或其他適用之管控機制來達成。
驗證實務	▪如未針對資通系統日誌進行存取管理，或允許非權責人員任意調閱，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之日誌相關管理辦法，並訪談相關權責人員(如系統管理者與資料庫管理者等)，以了解機關如何針對日誌進行存取管理。 ▪驗證人員宜發展測試案例以驗證存取控制之有效性，如嘗試利用未授權存取之使用者帳號存取日誌，應能有效禁止其存取行為。例如，若機關規定僅限資料庫管理者存取留存於資料庫之日誌內，則驗證人員可驗證系統管理者或一般使用者帳號無法存取日誌。
佐證資料	▪機關訂定之日誌管理辦法 ▪日誌存取控制權限申請/審核紀錄 ▪存取日誌之測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-9 日誌資訊之保護)

資料來源：本計畫整理

2.2.6.2 應運用雜湊或其他適當方式之完整性確保機制

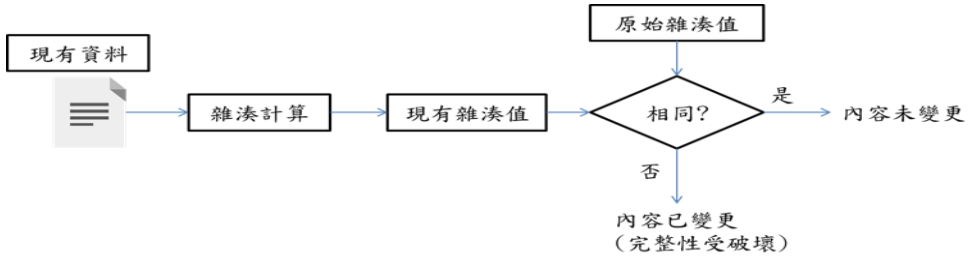
表27 日誌資訊之保護控制措施 2

控制措施	應運用雜湊或其他適當方式之完整性確保機制
適用等級	中、高

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應運用雜湊或其他適當方式之完整性確保機制
內容說明	▪資通系統日誌可作為資安事件追蹤、行為歸責與資料佐證等用途，而惡意攻擊者也可能試圖竄改或破壞日誌內容以湮滅攻擊軌跡，因此除實作日誌存取管理外，亦須實作相關控制措施以確保在日誌內容正確可靠，在日誌保存期間不會受到未經授權之竄改。 ▪從日誌完整性防護又分為事前預防、事中監視及事後驗證等三種面向，包含防止日誌內容被惡意竄改、當發生竄改行為時可即時察覺提出示警，以及在懷疑資料內容真實性時可驗證日誌內容是否曾經過異動等。可評估實際使用需求及資安風險，並以縱深防禦思維實作相關安全控制措施，以下舉例說明。 ▪(事前預防)將日誌以 CD-ROM / DVD-ROM 或其他具唯讀(Read Only)特性之儲存媒體進行保存，因可禁止其內容再次變更，故可保護日誌內容之完整性；惟須注意儲存媒體使用壽命，避免因保存不當而無法使用。 ▪(事前預防)將日誌經過加密處理後保存或備份，因未經授權使用者難以解密而無法閱讀與修改其中內容，故同時具有維持機密性與完整性之優點；惟此時加密金鑰之存取保護變為安全管理重點。使用情境如資通系統產生日誌檔案經過工具壓縮及加密處理後，儲存至日誌伺服器或其他儲存媒體進行保存或備份。 ▪(事中監視)目前市面上推出多款針對檔案、目錄或資料庫專用之監控工具，其功能特性為可即時偵測檔案、目錄或資料庫欄位異動，並提出警示通知。可評估針對系統日誌檔案進行監控，使用情境如應用程式設定為每日新產生一個日誌檔案，理論上昨日之日誌檔案不會再被異動，因此若監控工具偵測到過往檔案之異動行為，即應進一步釐清是否遭人惡意竄改。 ▪(事後驗證)雜湊為一種常用且簡單之完整性驗證機制，可利用 SHA-256 或 HMAC-SHA-256 等雜湊演算法(Hash algorithms)對資料或檔案計算出雜湊值。雜湊值是一種資料指紋之概念，經常用來識別檔案與資料是否有被竄改。[3]雜湊原理為不同資料即使只存在細微差異亦會產生大不相同之雜湊值，故若要驗證原始內容是否經過異動，只要比對前後兩者所產生之雜湊值即

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應運用雜湊或其他適當方式之完整性確保機制
	可，若相異則表示資料內容已受到竄改，示意圖詳見圖 32。雜湊值需適當保護與管理，如將雜湊值與日誌分開存放等，避免惡意攻擊者一併竄改原始內容與雜湊值。使用情境如將每日產生並不再異動之日誌檔案進行雜湊計算後留存雜湊值，未來需要驗證完整性時，再把現有資料重新計算產生新雜湊值，比對兩份雜湊值應相同，表示完整性未受到破壞。  資料來源：本計畫整理 圖32 以雜湊驗證完整性 ▪ (事後驗證)將日誌備份至原日誌系統不同之實體系統，亦可用來驗證資料完整性，如比對原始資料與備份資料兩者內容或雜湊值是否相同，即可察覺資料內容是否受到竄改，惟備份資料亦應具備適當之存取管理，避免惡意攻擊者同時竄改原始資料與備份資料。
驗證實務	▪如未實作任何日誌完整性確保機制，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之日誌相關管理辦法，並訪談相關權責人員(如系統管理者與資料庫管理者等)，了解機關如何確保日誌之完整性，並評估整體資安風險及安全控制措施之有效性。 ▪驗證人員可評估發展測試案例，如模擬非授權之竄改行為，以驗證能有效保護或發覺完整性受到破壞之情形。
佐證資料	▪機關訂定之日誌相關管理辦法 ▪機關導入之完整性確保機制，如提供雜湊值等
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-9 日誌資訊之保護)

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應運用雜湊或其他適當方式之完整性確保機制
	▪ NIST Special Publication 800-92, Guide to Computer Security Log Management ▪ 使用雜湊程式碼確定資料完整性。微軟。https://docs.microsoft.com/

資料來源：本計畫整理

2.2.6.3 定期備份日誌至與原系統外之其他實體系統

表28 日誌資訊之保護控制措施 3

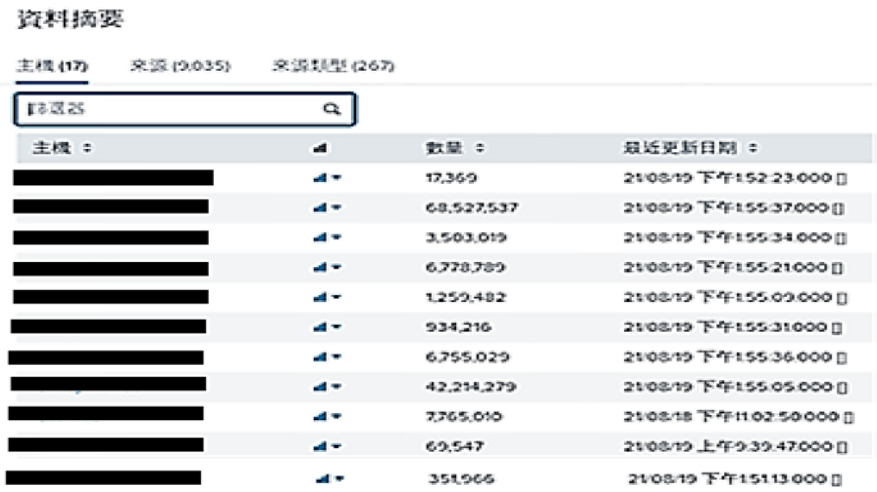
控制措施	定期備份日誌至與原系統外之其他實體系統
適用等級	高
內容說明	應定期執行日誌備份，且不可存放在同一個系統內，以避免因實體主機損毀而造成原始資料與備份資料一併丟失。常見方式如建置日誌伺服器、NAS 及雲端空間等，或是利用磁碟與磁帶等儲存媒體存放備份資料。以日誌伺服器備份系統日誌範例詳見圖 33。  資料來源：本計畫整理

圖33 以日誌伺服器備份系統日誌範例

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	定期備份日誌至與原系統外之其他實體系統
驗證實務	▪如未定期執行日誌備份，或是將備份留存於原系統內，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之日誌管理辦法，並訪談相關權責人員(如系統管理者與資料庫管理者等)，以了解日誌備份方式。 ▪驗證人員宜抽查備份執行紀錄並檢視備份結果，不得因產生日誌之實體系統損毀而造成備份資料一併丟失。例如，若將備份資料存放於同一台實體主機不同磁碟，仍具有丟失資料之高度風險。
佐證資料	▪機關訂定之日誌管理辦法 ▪日誌備份紀錄與結果
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 6-稽核和可歸責性 Audit And Accountability (控制措施編號 AU-9 日誌資訊之保護)

資料來源：本計畫整理

2.3 營運持續計畫

2.3.1 系統備份

2.3.1.1 訂定系統可容忍資料損失之時間要求

表29 系統備份控制措施 1

控制措施	訂定系統可容忍資料損失之時間要求
適用等級	普、中、高
內容說明	▪應訂定可容忍資料損失之時間要求，若資安事件發生造成資料損失時，需使用最接近之備份資料進行復原。資料損失與備份資料之間之時間間隔，亦稱為復原點目標(Recovery Point Objective, RPO)。RPO 一旦訂定完成，則可協助系統維護人員選擇適合之備份機制及週期。如訂定為 1 小時，則至少每小時必須進行 1 次資料備份，所選擇儲存媒體可能為磁碟；但若 RPO 訂定為 1 週，則

本文件之智慧財產權屬數位發展部資通安全署擁有。

<table>
<tr><td>控制措施</td><td>訂定系統可容忍資料損失之時間要求</td></tr>
<tr><td></td><td>至少每週進行 1 次資料備份，使用磁帶或光碟片等媒體即可符合備份需求。RPO 示意圖詳見圖 34。
 

資料來源：本計畫整理
圖34 復原點目標示意圖</td></tr>
<tr><td>驗證實務</td><td>▪ 如未訂定系統可容忍資料損失之時間要求，或未落實執行，則未符合此控制措施。
▪ 驗證人員宜檢視機關訂定之營運持續計畫相關辦法，並訪談相關權責人員(如系統管理者、資料庫管理者及網路管理者等)，以了解該資通系統所適用之可容忍資料損失時間要求。各系統訂定 RPO 範例詳見圖 35。
 
資料來源：本計畫整理
圖35 定義系統復原點目標範例
▪ 宜抽查備份資料，檢視其備份週期是否符合機關訂定之備份目標。</td></tr>
<tr><td>佐證資料</td><td>機關訂定之營運持續計畫</td></tr>
<tr><td>參考文獻</td><td>安全控制措施參考指引(修訂)(V2.0)_附件 9-營運持續計畫
Contingency Planning(控制措施編號 CP-2 營運持續計畫)</td></tr>
</table>

	A	B	C	D	E	F	G	H	I
1	#	計畫組織	計畫	資產類別	資產名稱	可容許資料損失最長時間(RPO)	最大容忍中斷時間(RTO)	系統Owner	盤點者
2	1	軟體安全科	資安服務系統維運	系統類	範例系統1	24H	24H	張三	李四
3	2	軟體安全科	資安服務系統維運	系統類	範例系統2	24H	24H	張三	李四
4	3	軟體安全科	資安服務系統維運	系統類	範例系統3	48H	48H	張三	李四
5	4	軟體安全科	資安服務系統維運	系統類	範例系統4	N/A	N/A	張三	李四
6									

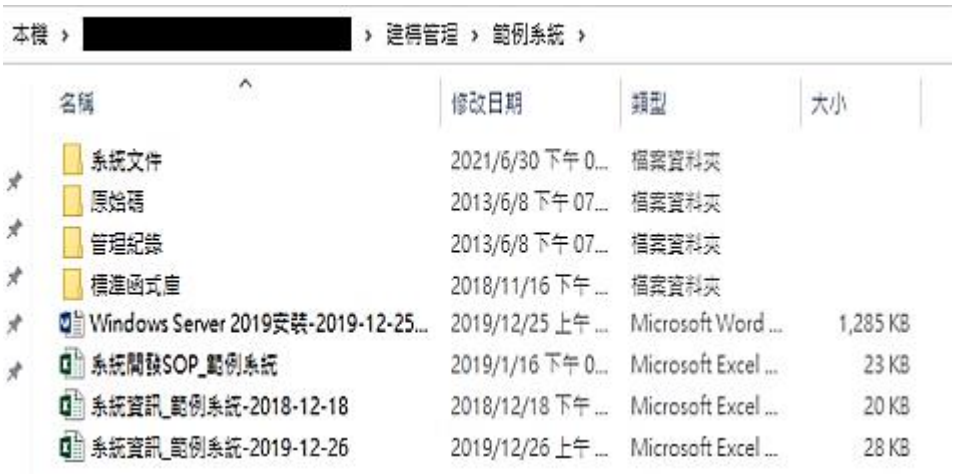
本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	訂定系統可容忍資料損失之時間要求

資料來源：本計畫整理

2.3.1.2 執行系統源碼與資料備份

表30 系統備份控制措施 2

控制措施	執行系統源碼與資料備份
適用等級	普、中、高
內容說明	▪ 資通系統應依機關資安政策及規範進行系統源碼(含原始程式碼、目的程式(Object Code)等)或資料(如系統業務資料等)備份作業。套裝軟體、租賃系統，或因合約特別規定允許委外廠商可不提供系統源碼者，不在此限。可建立集中式存放空間，以方便管理保存，備份實作範例詳見圖 36。  資料來源：本計畫整理 圖36 系統源碼與資料備份範例 ▪ 當廠商交付驗收或是程式更版時，皆應透過有效之儲存管理機制進行備份，以有效掌控版本實際狀況。 ▪ 實務上如建置版本控制系統，或利用(虛擬)主機備份與資料庫備份等方式達成備份效果。 ▪ 系統源碼之版本控制與變更管理，以機關自行維護為原則，不

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	執行系統源碼與資料備份
	宜全委由廠商負責變更管理作業。機關至少應留存系統源碼備份，避免委外廠商因故倒閉或更換後，無法再行還原系統源碼之情形。 ▪應針對資通系統重要資料進行備份，重要資料如為維持關鍵系統服務所必須，或考量機密性、完整性及可用性而具有較高資安風險等資料。
驗證實務	▪如未執行系統源碼與相關重要資料備份，可能造成資通系統難以進行災後重建者，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之營運持續計畫相關辦法，並訪談相關權責人員(如系統管理者與資料庫管理者等)，了解系統源碼與資料備份執行方式。 ▪驗證人員宜檢視資通系統源碼備份結果，至少應留存 1 份最新之系統源碼備份，不可全數交由廠商管理保存。 ▪驗證人員宜檢視資通系統資料備份結果，如依機關訂定之復原點目標(RPO)要求，定期執行備份作業。
佐證資料	▪機關訂定之營運持續計畫 ▪源碼備份執行紀錄 ▪資料備份執行紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 9-營運持續計畫 Contingency Planning(控制措施編號 CP-9 資訊系統備份)

資料來源：本計畫整理

2.3.1.3 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

表31 系統備份控制措施 3

控制措施	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
適用等級	中、高

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
內容說明	常見之資料儲存媒體如磁碟、光碟及磁帶等，因使用方式及保存環境之差異，可能影響儲存媒體壽命而造成備份資料損毀，故應定期檢查儲存媒體仍可正常使用，並測試其中資料仍正確完整。管理規範範例詳見圖 37。 備份資料應至少每半年執行資料回復測試，以確認備份媒體與資料之可用性，並將備份可用性測試之狀況應紀錄於「備份回復測試紀錄表」。 資料來源：本計畫整理 圖37 備份測試管理規範範例
驗證實務	▪ 如未曾執行過備份測試，亦無明確之執行時程規劃或明文規範，則未符合此控制措施。 ▪ 驗證人員宜檢視機關訂定之營運持續計畫相關辦法，並訪談相關權責人員(如系統管理者與資料庫管理者等)，以了解執行備份之方式與儲存媒體，以及執行備份資訊測試之週期。 ▪ 驗證人員宜檢視機關針對備份媒體與備份資訊所執行之測試結果，測試週期應符合機關規定，測試內容需包含查檢備份資料正確可用，如進行備份資料讀取測試等。
佐證資料	▪ 機關訂定之營運持續計畫 ▪ 營運持續計畫測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 9-營運持續計畫 Contingency Planning(控制措施編號 CP-9 資訊系統備份)

資料來源：本計畫整理

2.3.1.4 應將備份還原，作為營運持續計畫測試之一部分

本文件之智慧財產權屬數位發展部資通安全署擁有。

表32 系統備份控制措施 4

<table>
<tr><td>控制措施</td><td>應將備份還原，作為營運持續計畫測試之一部分</td></tr>
<tr><td>適用等級</td><td>高</td></tr>
<tr><td>內容說明</td><td>▪ 災害復原是營運持續計畫中相當重要之環節，其目的是為在發生天災、人為疏失或惡意破壞造成資通系統損害時，能快速回復至正常或可接受之營運水準。
▪ 營運持續計畫應定期完整測試、演練，以驗證計畫之適切性及有效性，在災害復原過程中應使用備份資料，以驗證備份機制是否正確可靠。備份還原測試步驟範例詳見圖 38。
表1 演練時程規劃表
<table><tr><th rowspan="2">NO</th><th rowspan="2">演練項目</th><th colspan="3">預計完成時間</th><th rowspan="2">負責人</th><th rowspan="2">演練方式</th></tr><tr><th>開始</th><th>結束</th><th>總計</th></tr><tr><td>1</td><td>通報並於臨時指揮中心集合</td><td>09：00</td><td>09：30</td><td>30m</td><td>管理代表</td><td>☒模擬
☐實際</td></tr><tr><td>2</td><td>成立緊急應變小組進行任務分派</td><td>09：31</td><td>09：40</td><td>10m</td><td>管理代表</td><td>☒模擬
☐實際</td></tr><tr><td>3</td><td>中心長官聯繫</td><td>09：41</td><td>09：50</td><td>10m</td><td>中心 PO</td><td>☒模擬
☐實際</td></tr><tr><td>4</td><td>系統維護人員進行檢查和處理，無法救回</td><td>09:50</td><td>10:00</td><td>10m</td><td>系統維護人員</td><td>☒模擬
☐實際</td></tr><tr><td>5</td><td>請網管人員進行 VM 備份還原</td><td>10:00</td><td>16:50</td><td>6h50m</td><td>網管人員</td><td>☐模擬
☒實際</td></tr><tr><td>6</td><td>系統維護人員進行測試，確認系統復原正常運作</td><td>16:50</td><td>17:00</td><td>10m</td><td>系統維護人員</td><td>☐模擬
☒實際</td></tr></table>資料來源：本計畫整理
圖38 備份還原測試步驟範例</td></tr>
<tr><td>驗證實務</td><td>▪ 如資通系統營運持續計畫測試內容未曾包含備份還原測試，則未</td></tr>
</table>

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應將備份還原，作為營運持續計畫測試之一部分
	符合此控制措施。 ▪驗證人員宜檢視機關訂定之營運持續計畫相關辦法，並訪談相關權責人員(如系統管理者與資料庫管理者等)，以了解機關擬定之營運持續計畫與相關測試活動。 ▪驗證人員宜檢視營運持續計畫測試項目，需納入備份還原測試，如於測試環境中利用備份之源碼與資料還原資通系統，測試服務是否仍可正常運作。
佐證資料	▪機關訂定之營運持續計畫 ▪營運持續計畫測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 9-營運持續計畫 Contingency Planning(控制措施編號 CP-9 資訊系統備份)

資料來源：本計畫整理

2.3.1.5 應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份

表33 系統備份控制措施 5

控制措施	應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份
適用等級	高
內容說明	▪應評估資安風險，決定應備份之重要資通系統軟體(如程式執行檔、安裝檔等)與安全相關資訊(如機關硬體、軟體及韌體元件清單等)。 ▪應使用適當實體(如防火櫃等)及環境保護備份資料儲存媒體，需將備份資料與原始資料分開存放，切不得置放於同一運作系統中，以避免系統損毀造成原始與備份資料一併丟失。例如，使用 DVD 光碟儲存資通系統軟體備份，並置於防火櫃中妥善保管。資料備份保存規範範例詳見圖 39。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份
	8.1 已開封或已有儲存資料的磁帶應存放於防潮櫃中，並且貼上標籤妥善編號。 8.2 存放資料的光碟(CD/DVD)，應編號裝在 CD 保存盒中，存放於防潮櫃中。 8.3 防潮櫃或是磁帶櫃的開關，備份媒體的存放與取用，須由備份管理員執行與管制。 資料來源：本計畫整理 圖39 資料備份保存規範範例
驗證實務	▪如重要資通系統軟體與其他安全相關資訊之備份與運作系統儲存於相同地點，且未利用獨立設施或防火櫃加以保護，使得備份資料與原始資料容易一併丟失者，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之營運持續計畫相關辦法，並訪談相關權責人員(如系統管理者與資料庫管理者等)，了解如何存放備份媒體。 ▪驗證人員宜檢視執行資通系統軟體與其他安全相關資訊備份之成果，至少不可存放於同一個主機或機櫃內。
佐證資料	機關訂定之營運持續計畫
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 9-營運持續計畫 Contingency Planning(控制措施編號 CP-9 資訊系統備份)

資料來源：本計畫整理

2.3.2 系統備援

2.3.2.1 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

表34 系統備援控制措施 1

控制措施	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
適用等級	中、高

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
內容說明	應考量服務需求、使用現況、相關資源項目，以及資安事件發生之風險，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，亦可稱為復原時間目標(Recovery Time Objective, RTO)。RTO 示意圖詳見圖 40。  資料來源：本計畫整理 圖40 復原時間目標示意圖
驗證實務	▪ 如未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，或未落實執行，則未符合此控制措施。 ▪ 驗證人員宜檢視機關訂定之營運持續計畫相關辦法，並訪談相關權責人員(如系統管理者等)，確認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。RTO 之訂定，應與資通系統安全等級評估表、資訊資產風險評鑑表，以及委外契約等相關文件中要求之服務水準協議(SLA)一致。 ▪ 各系統訂定 RTO 範例詳見圖 41。 資料來源：本計畫整理 圖41 定義系統復原時間目標範例

	A	B	C	D	E	F	G	H	I
1	#	計畫組織	計畫	資產類別	資產名稱	可容許資料損失最長時間(RPO)	最大容忍中斷時間(RTO)	系統Owner	盤點者
2	1	軟體安全科	資安服務系統維運	系統類	範例系統1	24H	24H	張三	李四
3	2	軟體安全科	資安服務系統維運	系統類	範例系統2	24H	24H	張三	李四
4	3	軟體安全科	資安服務系統維運	系統類	範例系統3	48H	48H	張三	李四
5	4	軟體安全科	資安服務系統維運	系統類	範例系統4	N/A	N/A	張三	李四
6									

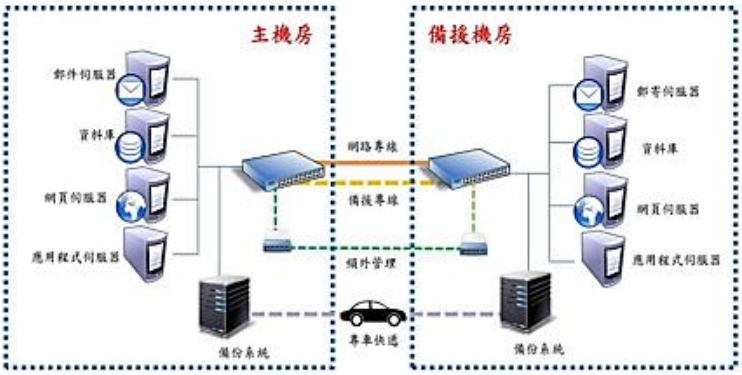
本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	▪驗證人員可檢視曾執行之營運持續計畫測試紀錄，是否包含災害復原演練或測試，以驗證是否符合復原時間目標(RTO)要求。
佐證資料	▪機關訂定之營運持續計畫 ▪營運持續計畫測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 9-營運持續計畫 Contingency Planning(控制措施編號 CP-2 營運持續計畫)

資料來源：本計畫整理

2.3.2.2 原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務

表35 系統備援控制措施 2

控制措施	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務
適用等級	中、高
內容說明	應規劃適當備援機制，以便在發生災害時，可於所訂定之容忍時間內讓服務回復正常運作。準備足夠之備援設備可提高服務運作之可用性，實務上常以異地備援或雲端服務方式提高系統可用性，可避免因火災、水災、遭竊等災難，造成重要軟硬體資源損毀而中斷服務。異地備援系統架構示意圖詳見圖 42。  資料來源：電腦機房異地備援機制參考指引[4]

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務
	圖42 異地備援系統架構示意圖
驗證實務	▪如未準備備援設備或其他方式取代並提供服務，使得無法符合復原時間目標(RTO)之要求，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之營運持續計畫相關辦法，並訪談相關權責人員(如系統管理者等)，以了解實作之備援機制。 ▪驗證人員可檢視曾執行之營運持續計畫測試紀錄，是否包含災害復原演練或測試，確保已提供足夠備援設備或其他可維持服務運作之方式(如雲端服務等)，並可符合復原時間目標(RTO)之要求。
佐證資料	▪機關訂定之營運持續計畫 ▪營運持續計畫測試紀錄
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 9-營運持續計畫 Contingency Planning(控制措施編號 CP-9 資訊系統備份) ▪電腦機房異地備援機制參考指引[4]

資料來源：本計畫整理

2.4 識別與鑑別

2.4.1 內部使用者之識別與鑑別

2.4.1.1 資通系統應具備唯一識別及鑑別使用者(或代表使用者行為之程序)之功能，禁止使用共用帳號

表36 內部使用者之識別與鑑別控制措施 1

控制措施	資通系統應具備唯一識別及鑑別使用者(或代表使用者行為之程序)之功能，禁止使用共用帳號
適用等級	普、中、高

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統應具備唯一識別及鑑別使用者(或代表使用者行為之程序)之功能，禁止使用共用帳號
內容說明	▪ 資通系統應具有身分驗證機制，內部使用者如系統管理人者與其他雇員，亦包含臨時人員、駐點廠商及工讀人員等所有可能之資通系統使用者。除允許匿名存取之功能頁面外，資通系統應利用身分驗證(如帳號密碼或自然人憑證等)機制識別內部使用者(或代表使用者行為之程序)。 ▪ 共用帳號行為可能出現在系統特權帳號或業務使用帳號，為提高可歸責性，應避免使用共用帳號。資通系統帳號僅提供已取得授權人員使用，並以開立個人帳號為原則，除非有特殊使用需求另行規定外，不應製發匿名或多人共用帳號。以國家資通安全通報應變網站為例，機關進行通報作業時仍需以個人帳號登入使用，目的即在避免共用帳號問題，使用範例詳見圖 43。  資料來源：本計畫整理 圖43 以個人帳號登入範例
驗證實務	▪ 除允許匿名存取功能頁面外，如資通系統未實作身分驗證功能，或未限制內部使用者使用共用帳號，則未符合此控制措施。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統應具備唯一識別及鑑別使用者(或代表使用者行為之程序)之功能，禁止使用共用帳號
	▪驗證人員宜檢視資通系統是否已實作身分驗證功能，如帳號密碼等，並可評估發展測試案例，以測試身分驗證功能之有效性。例如，在未登入之帳號情況下，測試存取系統非公開功能頁面，系統應導向帳號登入頁面或禁止存取。 ▪驗證人員宜檢視資通系統日誌，查找是否存在共用帳號之行為。例如，若日誌顯示某使用者帳號登入來源包含 3 個網路位址，而這 3 個位址卻分別屬於 3 位不同業務使用者所擁有，故可能存在共用帳號行為，惟驗證人員仍須進一步透過訪談等方式進行確認。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄 ▪資通系統日誌
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication(控制措施編號 IA-2 內部使用者之識別與鑑別)

資料來源：本計畫整理

2.4.1.2 對資通系統之存取採取多重認證技術

表37 內部使用者之識別與鑑別控制措施 2

控制措施	對資通系統之存取採取多重認證技術
適用等級	高
內容說明	▪內部使用者存取高等級資通系統應用服務時應採取多重認證技術，使用情境如系統管理者登入系統後臺管理功能頁面進行系統維護。多重認證技術係指採用兩種以上不同身分驗證因子，意即使用 MFA (Multi-Factor Authentication)。身分驗證因子依類型，可分為所知之事、所持之物及所具之形等；所知之事係指利用僅

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	對資通系統之存取採取多重認證技術
	限使用者所知內容進行身分驗證，如密碼、PIN 碼及安全問答等；所持之物則利用使用者擁有之實體或非實體物品，如憑證、晶片卡、SMS 簡訊驗證碼、符記(Token)及一次性密碼(OTP)等；而所具之形為使用者具有之生物特徵辨識技術，如臉部、聲紋、指紋及虹膜等。 ▪ 多重認證技術使用範例，如自然人憑證或健保卡，使用時需具備晶片卡(所有之物)與 PIN 碼(所知之事)正確組合，才能完成驗證。以綜合所得稅申報系統為例，可使用自然人憑證進行身分驗證，此時需準備讀卡機，並輸入身分證統一編號及卡片 PIN 碼進行登入，操作畫面範例詳見圖 44。  資料來源：本計畫整理 圖44 以自然人憑證登入系統範例
驗證實務	▪ 如內部使用者存取高等級資通系統時未採取多重認證技術，則未符合此控制措施。 ▪ 驗證人員宜檢視資通系統身分驗證功能，當內部使用者存取資通系統時，需經過兩種以上不同類型之身分驗證因子。惟若同時多次使用同一種類型之身分驗證因子，如同時使用密碼與安全問答作為驗證關卡，並不符合多重認證技術之精神。另外需注意的是，Captcha 圖形驗證碼作用僅為辨別人為或自動化程式之操作行

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	對資通系統之存取採取多重認證技術
	為，不可視為身分驗證因子之一。 ▪驗證人員宜檢視資通系統多重認證技術是否為全面性適用，包含所有內部使用者或登入方式。例如，若資通系統允許使用者利用自然人憑證或是帳號密碼擇一方式進行登入，雖自然人憑證符合多重認證技術，惟若允許使用者僅以帳號密碼即完成登入，則仍未完全符合此項控制措施要求。 ▪資通系統如將網路位址(如 IP 或 MAC 等)作為身分驗證因子之一，則應可識別其為特定使用者之專屬設備，始符合「所有之物」之定義，惟建議仍需仔細評估偽冒網路位址之風險。 ▪驗證人員宜發展測試案例，如以代表內部使用者之測試帳號，僅使用帳號密碼嘗試登入，若系統允許登入，則表示符合此項控制措施要求。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication(控制措施編號 IA-2 內部使用者之識別與鑑別)

資料來源：本計畫整理

2.4.2 身分驗證管理

2.4.2.1 使用預設密碼登入系統時，應於登入後要求立即變更

表38 身分驗證管理控制措施 1

控制措施	使用預設密碼登入系統時，應於登入後要求立即變更
適用等級	普、中、高
內容說明	▪預設密碼係指由資通系統自動產生或由系統管理者協助建立之個人使用者密碼，可能於使用者初次註冊或密碼重設時產生，供

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用預設密碼登入系統時，應於登入後要求立即變更
	使用者登入系統。 ▪預設密碼變更之要求，原則上應具備一定程度之強制力，而非僅作警示用途，避免使用者選擇視而不見。例如，當使用者未完成預設密碼變更時，限制使用者之系統功能操作權限，以促使用戶變更預設密碼。變更預設密碼系統操作範例詳見圖 45。  資料來源：本計畫整理 圖45 變更預設密碼範例
驗證實務	▪如資通系統以預設密碼登入時未出現變更密碼提示畫面，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員(如系統管理者等)，以了解資通系統是否允許使用預設密碼，如系統禁止使用預設密碼登入，則不適用此規範。 ▪驗證人員宜發展測試案例，如申請測試帳號與預設密碼，初次登入資通系統時，檢視是否要求立即變更。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄

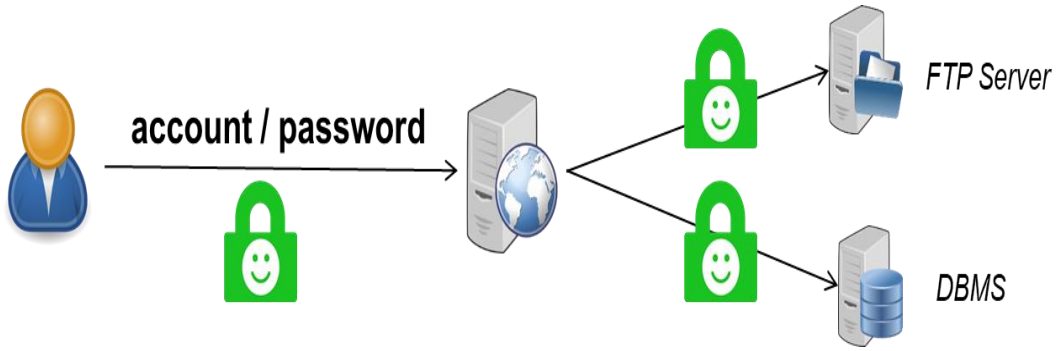
本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用預設密碼登入系統時，應於登入後要求立即變更
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理)

資料來源：本計畫整理

2.4.2.2 身分驗證相關資訊不以明文傳輸

表39 身分驗證管理控制措施 2

控制措施	身分驗證相關資訊不以明文傳輸
適用等級	普、中、高
內容說明	▪ 身分驗證相關資訊如密碼等具有機敏性，一旦外洩即可能造成帳戶被惡意盜用，切不可以未經保護之明文形式進行網路傳輸，避免攻擊者試圖攔截網路封包進而竊取其中密碼資訊。資通系統傳輸身分驗證資訊之行為，包含機關內外部使用者透過網際網路或機關內部網路登入資通系統帳戶、資通系統與其他資通系統介接時傳遞之身分驗證資訊等，皆應避免明文傳輸。加密傳輸示意圖詳見圖 46。  資料來源：本計畫整理 圖46 加密傳輸示意圖 ▪ 實務上常建立已加密之安全通道(如 HTTPS 與 VPN 等)保護傳輸資料之機密性。站台啟用 HTTPS 保護使用者身分驗證資訊範例詳見

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	身分驗證相關資訊不以明文傳輸
	圖 47。  資料來源：本計畫整理 圖47 站台啟用 HTTPS ▪ 當無法使用加密連線時，另一種替代方案如將機敏資訊先以應用程式或其他軟硬體實作加密或編碼保護後，再進行網路傳輸。
驗證實務	▪ 如資通系統以明文傳輸密碼，不論是在網際網路或內部網路傳輸過程中可能具有密碼外洩之風險者，則未符合此控制措施。 ▪ 驗證人員宜訪談相關權責人員(如系統管理者等)，以了解資通系統所有可能傳輸身分驗證資訊之管道，並檢視資通系統網路傳輸協定，確認是否經過加密保護，如使用 HTTPS、SSH 及 SFTP 等加密傳輸協定。 ▪ 惟若觀察到資通系統僅使用 HTTP 等未加密之傳輸協定，仍可能存在其他方式保護身分驗證資訊，如以應用程式加密等方式，故可評估委請系統管理者或開發人員進一步說明其實作方式，並提供系統功能規格書或原始碼等相關佐證資料。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	身分驗證相關資訊不以明文傳輸
	▪驗證人員可評估發展測試案例，如使用 Wireshark[5]等網路封包分析軟體，檢視身分驗證過程之網路封包內容，從中找尋明文密碼等身分驗證機敏資訊。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理) ▪www.wireshark.org[5]

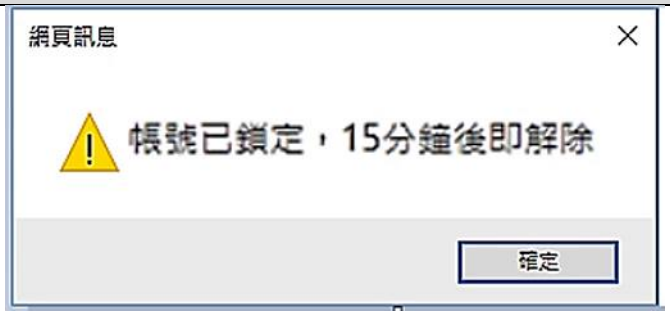
資料來源：本計畫整理

2.4.2.3 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 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

表40 身分驗證管理控制措施 3

控制措施	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 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
適用等級	普、中、高
內容說明	系統應實作帳戶鎖定機制以防範密碼破解攻擊，於鎖定期間禁止該帳號所有登入嘗試，超過鎖定時間則重新計次。機關得視系統使用需求，自建之失敗驗證機制，如訂定不同之鎖定觸發條件與閉鎖期，實作帳戶永久鎖定以人工解鎖，或是其他身分驗證強化機制等。帳戶鎖定畫面提示畫面範例詳見圖 48。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 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
	 資料來源：本計畫整理 圖48 帳戶鎖定範例
驗證實務	▪驗證人員宜訪談相關權責人員(如系統管理者等)，以了解系統帳戶鎖定機制之設計及觸發條件。 ▪驗證人員宜發展測試案例，需包含測試鎖定機制觸發條件，以及測試鎖定期間禁止完成登入行為。 測試步驟，例如： 1.以測試帳號連續登入失敗達 5 次，檢視系統是否觸發帳戶鎖定，或觸發其他強化驗證強度之行為(如 CAPTCHA 或簡訊驗證碼等) 2.於帳戶鎖定期間，嘗試以正確帳號密碼進行登入，系統應予以拒絕
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理)

資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.4.2.4 使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。

表41 身分驗證管理控制措施 4

控制措施	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制
適用等級	普、中、高
內容說明	▪應依資安政策及系統使用需求，訂定適用之密碼複雜度、最短及最長效期等使用限制。 ▪最低密碼複雜度目的在確保產生數量足夠之密碼組合，如密碼長度或組成字元種類基本要求等。 ▪密碼最短效期則在避免使用者為規避密碼歷程限制，而於短時間內頻繁變更密碼。 ▪強制密碼最長效期，可避免使用者長期使用同一個密碼而提高被破解之風險，建議以不超過 6 個月為原則。 ▪對非內部使用者，如資通系統服務係提供給一般民眾存取使用，可依機關自行規範辦理。
驗證實務	▪如資通系統未強制最低密碼複雜度，使得可利用簡易密碼即可登入者，則未符合此控制措施。如資通系統未強制密碼最短及最長之效期限制者，則未符合此控制措施。除機關另行規範外，內部使用者與非內部使用者身分驗證皆應強制密碼複雜度及效期限制。 ▪驗證人員宜訪談相關權責人員(如系統管理者等)或檢視系統功能頁面，以了解資通系統密碼複雜度、密碼最短效期及最長效期限制。 ▪驗證人員宜發展測試案例，偵測密碼複雜度及最短與最長效期是否符合機關規定。測試方式參考如下： 1.如資通系統要求密碼字元需達 12 個字元以上，則嘗試使用少於 12 個字元之簡短字串進行密碼變更，此時系統應拒絕變更。此時測試目的為密碼長度限制，故可在符合密碼複雜度要求情況

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制
	下使用較簡短之字串進行測試。例如，變更密碼時輸入未滿 12 個字元要求之密碼字串「P@ss1234」，檢視系統是否仍允許變更，操作範例詳見圖 49。  資料來源：本計畫整理 圖49 簡短密碼字串變更測試範例 2.如資通系統要求密碼組成需包含英文大寫、小寫字元與數字，則嘗試使用英文大寫與小寫字元組成之字串進行密碼變更，系統應拒絕變更。以此類推，逐一測試其他違反密碼要求之字串組合。 3.如資通系統要求最短效期為 30 分鐘，則嘗試在 30 分鐘內執行兩次密碼變更，系統應拒絕變更。 4.如資通系統要求最長效期為 90 天，則評估模擬 90 天後使用情境之可行性，測試方式如調整系統內部時鐘或是資料庫內紀錄時戳等，系統應偵測過期密碼並要求變更。
佐證資料	▪機關訂定之系統發展維護辦法

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制
	▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理)

資料來源：本計畫整理

2.4.2.5 密碼變更時，至少不可以與前 3 次使用過之密碼相同。對非內部使用者，可依機關自行規範辦理

表42 身分驗證管理控制措施 5

控制措施	密碼變更時，至少不可以與前 3 次使用過之密碼相同
適用等級	普、中、高
內容說明	▪資通系統密碼歷程紀錄至少須保留 3 代，不可重覆使用。 ▪對非內部使用者，可依機關自行規範辦理。
驗證實務	▪驗證人員宜訪談相關權責人員(如系統管理者等)或檢視系統功能頁面，以了解資通系統密碼歷程限制。 驗證人員宜發展測試案例，測試案例參考如下： 1.原始密碼假設為「P@ssword111」。 2.測試人員將密碼變更為「P@ssword222」。 3.測試人員再將密碼變更為「P@ssword333」。 4.測試人員嘗試將密碼變更回「P@ssword111」，此時由於與前 3 次使用過之密碼相同，故系統應拒絕變更。操作範例詳見圖 50。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	密碼變更時，至少不可以與前 3 次使用過之密碼相同
	 資料來源：本計畫整理 圖50 密碼歷程測試範例
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理)

資料來源：本計畫整理

2.4.2.6 第 4 點及第 5 點所定措施，對非內部使用者，可依機關自行規範辦理

本文件之智慧財產權屬數位發展部資通安全署擁有。

表43 身分驗證管理控制措施 6

控制措施	第 4 點及第 5 點所定措施，對非內部使用者，可依機關自行規範辦理
適用等級	普、中、高
內容說明	▪非內部使用者包含所有未明確涵蓋於機關內部使用者之資通系統使用者，如一般民眾等。 ▪針對非內部使用者之身分驗證，可自行規範資通系統密碼複雜度、最短效期、最長效期，以及密碼歷程等限制。
驗證實務	驗證人員宜訪談相關權責人員(如系統管理者等)，以了解資通系統密碼複雜度、效期以及密碼歷程等限制。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理)

資料來源：本計畫整理

2.4.2.7 身分驗證機制應防範自動化程式之登入或密碼更換嘗試

表44 身分驗證管理控制措施 7

控制措施	身分驗證機制應防範自動化程式之登入或密碼更換嘗試
適用等級	中、高
內容說明	系統若採用帳號密碼進行身分驗證，往往可能遭受到自動化程式以暴力破解方式嘗試登入。防範方式如實作圖形驗證碼(CAPTCHA)，透過將驗證碼以圖形方式呈現於頁面上，並要求使用者辨別該圖形中文字之方式，或以其他足以辨識人為動作之方式(如勾選特定選項等)，防堵自動化程式之嘗試行為；實作密碼鎖定機制亦可有效防範密碼暴力破解攻擊。於帳號登入頁面實作圖形驗證碼範例詳見圖 51。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	身分驗證機制應防範自動化程式之登入或密碼更換嘗試
	 資料來源：本計畫整理 圖51 圖形驗證碼範例
驗證實務	▪驗證人員宜訪談相關權責人員(如系統管理者等)或檢視系統功能頁面，以確認是否啟用圖形驗證碼或使用密碼鎖定等，足以有效降低自動化程式攻擊資安風險之防護機制。 ▪驗證人員宜發展測試案例，確認防護機制之正確性及有效性。例如，當驗證圖形驗證碼，當未輸入答案或錯誤時，系統應予以拒絕，待輸入正確答案後始允許放行。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理)

資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

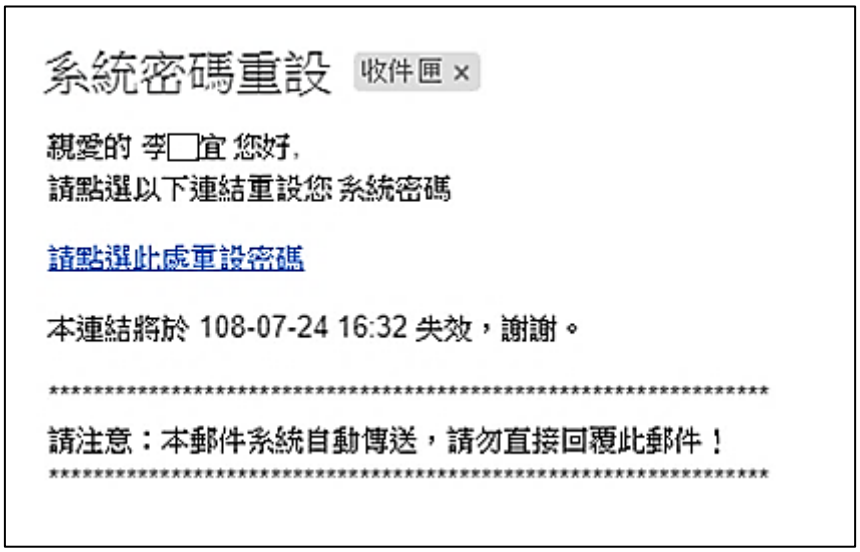
2.4.2.8 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記

表45 身分驗證管理控制措施 8

控制措施	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
適用等級	中、高
內容說明	▪ 當使用者忘記密碼時，常需使用密碼重設功能以設定新密碼，但密碼重設機制若設計不當，則容易被惡意攻擊者利用，偽冒成他人進行密碼重設，進而盜取帳戶使用權。 ▪ 如資通系統提供使用者線上進行密碼重設，此時應有效確認使用者真實身分，常用方式如利用與帳號綁定之電子郵件或手機等僅限真實使用者存取裝置，作為密碼重設符記(Token)之載體。當進行密碼重設時，可要求使用者輸入當初註冊時所留存之電子郵件或手機號碼，比對無誤後則發送一次性及時效性之密碼重設符記，如簡訊驗證碼或 Email 認證連結等，必須設定有效期限(如 30 分鐘等)，且一旦使用過則立即作廢，不得重複使用。簡訊驗證碼操作範例詳見圖 52，Email 認證連結操作範例詳見圖 53。  資料來源：本計畫整理

圖52 使用簡訊驗證碼進行密碼重設操作範例

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	 資料來源：本計畫整理 圖53 使用 Email 連結進行密碼重設操作範例 ▪如資通系統實作密碼重設機制，設計為由系統重新產生配發一組預設密碼，寄送給使用者後登入使用，原則上亦可視為一種形式符記；惟此時仍需實作一次性及時效性之特徵始符合此控制措施要求，如使用者以預設密碼初次登入後須強制立即變更密碼，且該預設密碼自產生後僅維持有效期限(如 1 小時等)，若逾期則無法登入，須申請重新產生。 ▪如資通系統係透過 AD 服務進行身分驗證，因 AD 服務架構設計上限制，當使用者忘記密碼時，實務上需聯繫 AD 管理員協助進行密碼重設，系統並不會發送一次性及具有時效性符記，故原則上並不適用此控制措施。
驗證實務	▪如資通系統允許使用者自行重設密碼，卻未嚴謹確認使用者身分或未發送一次性及具有時效性符記，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員(如系統管理者等)或檢視系統功能頁面，以確定資通系統如何處理使用者忘記密碼之重設申

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	請。 ▪驗證人員宜評估發展測試案例，測試符記可順利產生及發送，並符合一次性及時效性之要求。測試案例，例如： 1.操作密碼重設功能，檢視是否確實收到符記。 2.測試符記符合具時效性要求，收到符記後，等待超過有效期限後才使用，此時系統應拒絕。 3.測試符記符合具一次性要求，若符記已過期，重新申請新符記並於有效期限內使用，此時應成功完成密碼重設。 4.成功完成密碼重設後，再次使用同一符記進行密碼重設，系統應拒絕。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理)

資料來源：本計畫整理

2.4.3 鑑別資訊回饋

2.4.3.1 資通系統應遮蔽鑑別過程中之資訊

表46 鑑別資訊回饋控制措施

控制措施	資通系統應遮蔽鑑別過程中之資訊
適用等級	普、中、高
內容說明	▪實務上常會將密碼字元顯示為星號「*」，以避免有心人士在使用者輸入密碼時從後方窺視。。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統應遮蔽鑑別過程中之資訊
	▪如系統欲讓使用者檢視所輸入之密碼字元，可在遮蔽前以非常短時間顯示，或設計顯示密碼功能，惟預設應遮蔽字元，讓使用者手動勾選啟用。
驗證實務	▪如資通系統預設未遮蔽密碼字元，則未符合此控制措施。 ▪驗證人員可檢視任何需要輸入使用者密碼之頁面，除非使用者另行設定(如勾選「顯示密碼」)，否則不得長時間顯示密碼或 PIN 碼等輸入字元，示意圖詳見圖 54。  資料來源：本計畫整理 圖54 遮蔽鑑別過程中之資訊
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統身分驗證功能測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-6 鑑別符回饋)

資料來源：本計畫整理

2.4.4 加密模組鑑別

2.4.4.1 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

本文件之智慧財產權屬數位發展部資通安全署擁有。

表47 加密模組鑑別控制措施

控制措施	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
適用等級	中、高
內容說明	密碼儲存時應經過加密或雜湊(Hashing)保護，實務上建議實作雜湊加鹽(Salted Hashing)技術，可有效對抗彩虹表(Rainbow Table)等密碼破解攻擊手法。
驗證實務	▪如資通系統以明文儲存密碼，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員(如系統管理者與資料庫管理者等)以了解資通系統實作之密碼儲存方式，實務上常將密碼儲存於資料庫內，驗證人員可評估檢視資料庫內密碼儲存欄位，不應直接呈現明文字串。資料庫密碼欄位以雜湊值儲存範例詳見圖 55。 資料來源：本計畫整理 圖55 資料庫密碼欄位範例
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統密碼儲存結果
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-5 身分驗證管理)

ID	ACCOUNT	PWD	NAME
123	user1	6eb2b2c576lac38aca47d04e3f3af81allc01b4	陳小名
144	user2	e55969620728e8cla26999dc4ce45e7ba89e6f7	葉大熊
143	user3	51235962728e8cla26995dc4e456eb27bc571ac	李阿福

資料來源：本計畫整理

2.4.5 非內部使用者之識別與鑑別

2.4.5.1 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)

本文件之智慧財產權屬數位發展部資通安全署擁有。

表48 非內部使用者之識別與鑑別控制措施

控制措施	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)
適用等級	普、中、高
內容說明	▪非機關使用者包含所有未明確涵蓋於機關內部使用者之資通系統使用者，如一般民眾等。 ▪除公開頁面外，資通系統應利用身分驗證機制進行使用者識別及鑑別以強化可歸責性，如利用使用者帳號及密碼登入方式實作，範例詳見圖 56。  資料來源：本計畫整理 圖56 識別及鑑別非機關使用者
驗證實務	▪除公開頁面外，資通系統如未實作身分驗證機制，則未符合此控制措施。 ▪驗證人員宜檢視資通系統是否已實作身分驗證功能，如使用帳號密碼登入等，並可評估發展測試案例，以測試身分驗證功能之有效性。例如，在未登入之帳號情況下，測試存取系統非公開功能頁面，系統應導向帳號登入頁面或禁止存取。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統功能規格書 ▪資通系統密碼儲存結果

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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)
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 10-識別與鑑別 Identification and Authentication (控制措施編號 IA-8 識別與鑑別非內部使用者)

資料來源：本計畫整理

2.5 系統與服務獲得

2.5.1 系統發展生命週期需求階段

2.5.1.1 針對系統安全需求(含機密性、可用性、完整性)進行確認

表49 系統發展生命週期需求階段控制措施

控制措施	針對系統安全需求(含機密性、可用性、完整性)進行確認
適用等級	普、中、高
內容說明	▪ 自行開發或委外發展之系統，應在系統生命週期之初始階段，即將安全需求納入考量，如系統發展初期或系統重大改版時所進行之需求規劃活動，除考量功能相關需求外，亦應完成安全需求確認活動。資通系統安全需求項目至少應符合資通系統防護基準之規範，讓系統可依照其評定之普、中、高安全等級實作必要之安全控制措施。 ▪ 建議使用檢核表進行安全需求確認，好處為可提供基本必要之安全控制項目，避免有所缺漏。實務上可自行設計發展系統安全需求檢核表，亦可參考技服中心「資通系統委外開發 RFP 資安需求範本(V3.0)-附件 1 資通系統資安需求項目查檢表」，提供相關權責人員在發展系統安全需求時參考依據，惟建議機關仍須自行調修其中項目，以符合資通系統開發專案之特性以及最新資安法規要求，範例詳見圖 57。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	針對系統安全需求(含機密性、可用性、完整性)進行確認
	附件1　資通系統資安需求項目查檢表 技術面資安需求 分類 / 安全需求項目 / 說明 / 適用分級：普 / 中 / 高 / 評量結果(是/否/不適用) 存取控制 / 3.2.1.1.1 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。 / 資通系統之帳號應透過正式的帳號申請程序所建立，完成開通審核程序始能使用，因此系統應具備帳號管理機制，可對系統帳號進行申請、開通、停用或刪除之行為。 / V / V / V 3.2.1.1.2 已逾期之臨時或緊急帳號應刪除或禁用。 / 若具有臨時帳號或緊急帳號時，應實作已逾期之系統帳號檢查機制，於帳號逾期時自動停用或刪除，以避免帳號遭有心人士盜用。 / V / V 3.2.1.1.3 資通系統閒置帳號應禁用。 / 宜記錄系統帳號最後登入時間，可透過工作排程，檢查是否有持續一段時間(如半年等)未登入系統之帳號，並實作自動停用該帳號之功能。 / V / V 資料來源：本計畫整理 圖57 資通系統資安需求項目查檢表範例 ▪如部分所使用之資通系統開發完成並上線服務已久，可能當初在進行系統設計開發時並未充分考量或條列安全需求，惟現為符合資通系統防護基準之規範，建議仍應針對系統所實作之安全控制措施進行盤點並盡速補強缺漏項目，並留存相關檢核紀錄，以作為安全需求確認活動之稽核證據。
驗證實務	▪如資通系統未於發展初期確認系統安全需求項目而僅考量業務功能面需求，致使系統功能規格書未描述安全需求，亦無實作相關檢核確認活動，則未符合此控制措施。 ▪驗證人員宜進行人員訪談或檢視資通系統功能規格書與安全需求檢核表等文件紀錄，以了解機關已將必要之安全需求納入系統實作範圍。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	針對系統安全需求(含機密性、可用性、完整性)進行確認
佐證資料	▪資通系統功能規格書 ▪資通系統安全需求檢核表 ▪安全需求確認相關紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-4 獲得程序)

資料來源：本計畫整理

2.5.2 系統發展生命週期設計階段

2.5.2.1 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

表50 系統發展生命週期設計階段控制措施 1

控制措施	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
適用等級	中、高
內容說明	▪應識別資通系統所面臨之各種資安威脅，包含偽冒、竄改、否認行為、機敏資訊外洩、拒絕存取服務及權限提升等，足以危害系統機密性、完整性及可用性之系統存取行為。 ▪威脅識別與風險分析相關方法論，可參考包含誤用模型(Misuse case) [7]，以及威脅建模(Threat Modeling)、STRIDE 威脅類別及 DREAD 風險計算方法[8]等。 ▪以威脅模型分析方法論為例，觀察系統架構設計時所產生之資料流程圖(Data Flow Diagram, DFD)，將系統分解成相關元件，分析每個元件容易遭受威脅程度，有助於識別及分析系統潛在之安全威脅，以進一步擬定威脅處理之安全控制措施。DFD 係由外部實體、資料流程、處理程序及資料存放區等元件所繪製而成，DFD 各元件代表符號詳見圖 58。

本文件之智慧財產權屬數位發展部資通安全署擁有。

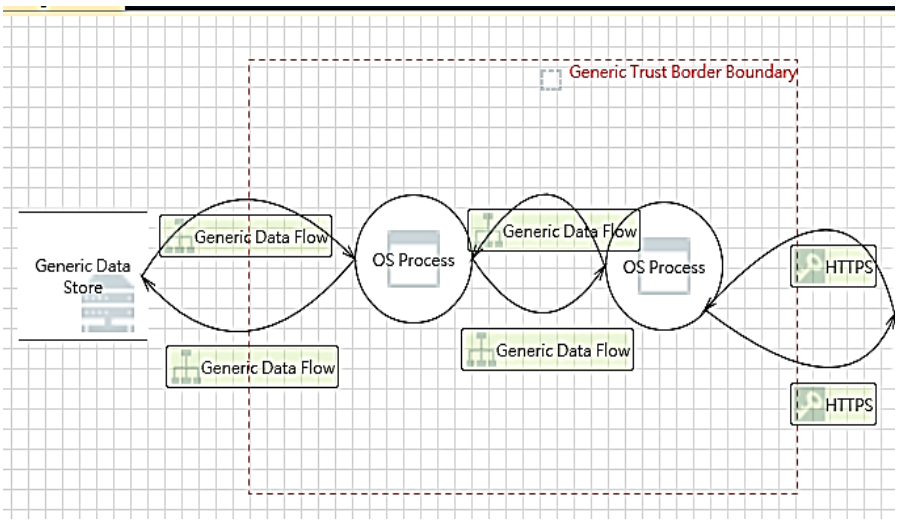
控制措施	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估

組成元素	符號	定義
外部實體	External Entity	驅動軟體的某人或某物，且為軟體本身無法控制者
程序	Process	處理輸入資料的工作或行為，並輸出資料者
資料流	Data Flow	資料於軟體或系統中移動的方法
資料儲存庫	Data Store	軟體中資料暫時或持續的儲存區
信任邊界		變更信任水準的界線

資料來源：本計畫整理

圖58 DFD 元件組成

- 繪製 DFD 為完成威脅建模活動必要之前置作業，建議可使用微軟 Threat Modeling Tool[8]，除方便繪製 DFD 外，亦可自動進行 STRIDE 威脅類別分析。Threat Modeling Tool 內建之 DFD 範例詳見圖 59。



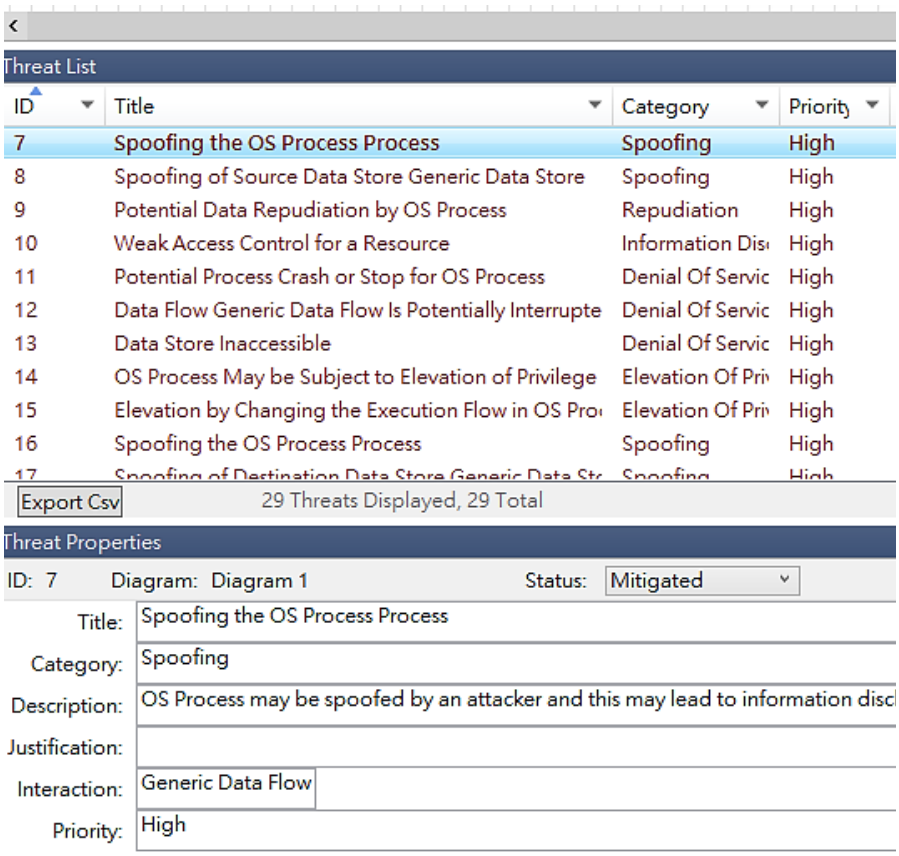
資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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

圖59 DFD 範例

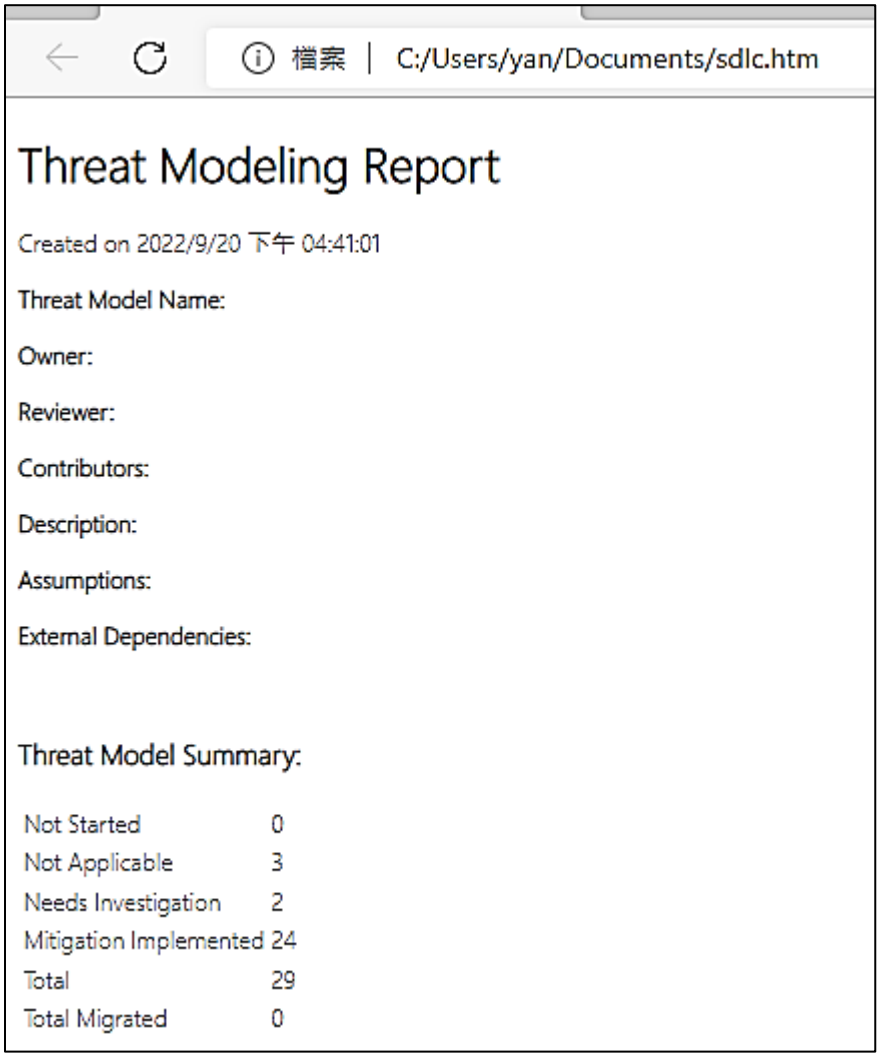
- STRIDE 威脅分析則是透過攻擊者角度，將把威脅劃分成 6 個類別，分別為偽冒身分(Spooling)、竄改(Tampering) 、否認行為(Repudiation)、資訊洩露(Information Disclosure)、阻斷服務(DOS)及權限提升(Elevation of Privilege)等。藉由分析現有系統設計是否潛藏此 6 種資安威脅，並評比各項資安威脅之風險高低，進而發展相對應安全控制措施。Threat Modeling Tool 可分析 DFD 並產生威脅分析清單，範例詳見圖 60。



資料來源：本計畫整理

圖60 以 Threat Modeling Tool 產生威脅分析清單

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	▪針對威脅分析清單完成人工確認後，可使用 Threat Modeling Tool 內建之報告功能，建立 HTML 格式之威脅建模分析報告，範例詳見圖 61。  資料來源：本計畫整理 圖61 以 Threat Modeling Tool 產生威脅建模分析報告
驗證實務	▪如未進行資通系統威脅識別與風險分析評估活動，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之系統發展管理辦法，並訪談相關權責人員(如系統管理者等)，了解資通系統如何進行威脅識別與風險

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	分析及評估等活動。 ▪驗證人員宜檢視資通系統威脅識別活動相關執行紀錄與分析報告，應包含可能危害資通系統機密性、完整性及可用性等各種資安威脅之識別。例如，若使用威脅建模方法論，則應檢附 DFD 資料流程圖及相應之威脅分析結果報告。
佐證資料	▪資通系統威脅識別執行紀錄或報告 ▪資通系統風險評估執行紀錄或報告
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 17-風險評鑑 Risk Assessment (控制措施編號 RA-3 風險評鑑) ▪安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-11 開發人員安全測試及評估) ▪Capturing Security Requirements through Misuse Cases, Sindre and Opdahl [7] ▪Threat Modeling, www.microsoft.com [8]

資料來源：本計畫整理

2.5.2.2 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

表51 系統發展生命週期設計階段控制措施 2

控制措施	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
適用等級	中、高
內容說明	應依規定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，所完成之風險評估結果應與既有之安全需求比對，以找出其中缺漏之處，其目的在強化安全需求內容，並修正安全需求檢核項目，以降低資安風險。例如，當系統風險等級變化(如中安全等級提升為高安全等級)時，應補強尚未實作之安全控制措施，此時有必要修正相關安全需求，並調整對應之需求檢

本文件之智慧財產權屬數位發展部資通安全署擁有。

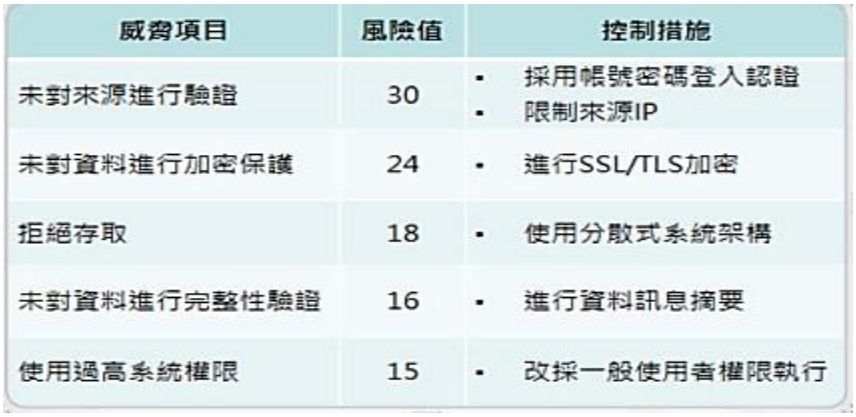
<table>
<tr><td>控制措施</td><td>將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正</td></tr>
<tr><td></td><td>核項目。例如，利用 DREAD 威脅風險分析結果，發展相對應安全控制措施後，納入系統安全需求修正項目，範例詳見圖 62。
 
<table><tr><th>威脅項目</th><th>風險值</th><th>控制措施</th></tr><tr><td>未對來源進行驗證</td><td>30</td><td>• 採用帳號密碼登入認證
• 限制來源IP</td></tr><tr><td>未對資料進行加密保護</td><td>24</td><td>• 進行SSL/TLS加密</td></tr><tr><td>拒絕存取</td><td>18</td><td>• 使用分散式系統架構</td></tr><tr><td>未對資料進行完整性驗證</td><td>16</td><td>• 進行資料訊息摘要</td></tr><tr><td>使用過高系統權限</td><td>15</td><td>• 改採一般使用者權限執行</td></tr></table>
資料來源：本計畫整理

圖62 安全需求修正</td></tr>
<tr><td>驗證實務</td><td>▪ 如進行風險評估活動後，有修正安全需求之必要，卻未落實修正，使得安全需求有所疏漏或未符合資通系統防護基準規定項目，則未符合此控制措施。
▪ 驗證人員宜訪談相關權責人員(如系統管理者等)，並檢視威脅識別及風險評估活動等結果，當識別出新興資安威脅或是系統風險等級變化時，應確認已進行安全需求變更作業(如提出系統功能變更申請等)，並修正安全需求檢核項目。</td></tr>
<tr><td>佐證資料</td><td>▪ 資通系統風險評估執行紀錄或報告
▪ 資通系統安全需求修正紀錄
▪ 機關訂定之安全需求檢核表</td></tr>
<tr><td>參考文獻</td><td>安全控制措施參考指引(修訂)(V2.0)_附件 17-風險評鑑 Risk Assessment (控制措施編號 RA-3 風險評鑑)</td></tr>
</table>

資料來源：本計畫整理

2.5.3 系統發展生命週期開發階段

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.5.3.1 應針對安全需求實作必要控制措施

表52 系統發展生命週期開發階段控制措施 1

控制措施	應針對安全需求實作必要控制措施
適用等級	普、中、高
內容說明	資通系統應依照需求規格文件內容，實作相關功能或機制。安全需求可能包含機關規定之組態設定，以明確說明允許之功能、埠口、協定及服務等，或是提供必要資安防護能力，如密碼強度要求、加密強度要求、實作存取控制、身分驗證及授權機制等資安功能實作。於專案管理實務上可使用資通系統安全需求追蹤矩陣(Secure Requirement Traceability Matrix, SRTM)，將安全需求、功能實作及後續測試驗證等活動串聯起來，以便於追蹤管理，範例詳見圖 63。

網頁部落格安全需求追溯矩陣範例

專案名稱	網頁部落格		專案經理	○○○	專案期程	YY/MM/DD		
專案說明	網頁部落格							
編號	功能 ID	高階需求	功能需求	狀態	設計/技術規格	實作模組/元件	測試案例編號	測試時間	測試結果
1	B-S-01	導入使用者權限控機制	透過URL Authorization 功能攔截所有使用者請求進行使用者權限管制	開啟	網頁部落格系統設計規格書 P.31	實作於使用者認證權限控管模組	T-S-01	N/A	N/A
2	B-S-02	驗證所有使用者輸入	透過Talidtion 控制元件進行所有使用者輸入過濾	開啟	網頁部落格系統設計規格書 P.31	實作於安全驗證模組	T-S-02	N/A	N/A

資料來源：本計畫整理

圖63 安全需求追蹤矩陣範例

驗證實務	▪ 如資通系統未依其需求規格文件訂定之安全需求進行實作，或未符合資通系統防護基準之安全規範項目，則未符合此控制措施。 ▪ 驗證人員宜檢視系統需求規格文件、安全需求檢核表等相關資料，以了解系統所訂定之安全需求清單。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應針對安全需求實作必要控制措施
	▪驗證人員宜訪談相關權責人員(如系統管理者等)，並檢視驗收測試報告等相關佐證資料，確認各項安全需求全數實作完畢。例如，若系統 RFP 要求資通系統須符合資通系統防護基準之規定，則驗證人員宜依系統安全等級，逐項驗證各安全控制措施實作之有效性與正確性。
佐證資料	▪資通系統安全需求 RFP 與功能規格書 ▪資通系統安全需求追蹤矩陣(Secure Requirement Traceability Matrix, SRTM) ▪資通系統驗收測試報告
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-4 獲得程序)

資料來源：本計畫整理

2.5.3.2 應注意避免軟體常見漏洞及實作必要控制措施

表53 系統發展生命週期開發階段控制措施 2

控制措施	應注意避免軟體常見漏洞及實作必要控制措施
適用等級	普、中、高
內容說明	常見漏洞如 OWASP Top 10、CWE Top25 等實作上容易產生之安全弱點及程式設計缺陷，系統開發時應避免產生具安全弱點之程式碼，如防範注入攻擊(Injection)與跨站腳本攻擊(XSS)等，並實作必要之安全控制措施，如強化身分驗證、存取控制及加密等。OWASP Top 10:2021 漏洞列表詳見圖 64。

本文件之智慧財產權屬數位發展部資通安全署擁有。

<table>
<tr><td>控制措施</td><td>應注意避免軟體常見漏洞及實作必要控制措施</td></tr>
<tr><td></td><td>
<table>
<tr><th>項次</th><th>中文</th><th>英文</th></tr>
<tr><td>A01:2021</td><td>權限控制失效</td><td>Broken Access Control</td></tr>
<tr><td>A02:2021</td><td>加密機制失效</td><td>Cryptographic Failures</td></tr>
<tr><td>A03:2021</td><td>注入式攻擊</td><td>Injection</td></tr>
<tr><td>A04:2021</td><td>不安全設計</td><td>Insecure Design</td></tr>
<tr><td>A05:2021</td><td>安全設定缺陷</td><td>Security Misconfiguration</td></tr>
<tr><td>A06:2021</td><td>危險或過舊的元件</td><td>Vulnerable and Outdated Components</td></tr>
<tr><td>A07:2021</td><td>認證及驗證機制失效</td><td>Identification and Authentication Failures</td></tr>
<tr><td>A08:2021</td><td>軟體及資料完整性失效</td><td>Software and Data Integrity Failures</td></tr>
<tr><td>A09:2021</td><td>資安記錄及監控失效</td><td>Security Logging and Monitoring Failures</td></tr>
<tr><td>A010:2021</td><td>伺服端請求偽造</td><td>Server-Side Request Forgery (SSRF)</td></tr>
</table>
資料來源：本計畫整理

圖64 OWASP Top 10:2021 常見漏洞</td></tr>
<tr><td>驗證實務</td><td>如在自行或委外開發資通系統時，未要求防範軟體常見漏洞，則未符合此控制措施。驗證人員可訪談相關權責人員(如系統管理者、資安人員等)，並檢視相關佐證資料，確認系統已防範 OWASP Top 10 等安全漏洞，常見控制措施包含(但不限於)：
▪ 系統安全開發教育訓練
▪ 訂定安全程式碼撰寫原則
▪ 執行源碼審查(Code Review)活動
▪ 執行弱點掃描，並確實修補安全漏洞
▪ 執行源碼掃描，並確實修補安全漏洞
▪ 執行滲透測試，並確實修補安全漏洞</td></tr>
<tr><td>佐證資料</td><td>▪ 教育訓練紀錄
▪ 安全程式碼撰寫規範
▪ 源碼掃描、弱點掃描、滲透測試執行紀錄與修補紀錄</td></tr>
<tr><td>參考文獻</td><td>安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-4 獲得程序)</td></tr>
</table>

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應注意避免軟體常見漏洞及實作必要控制措施

資料來源：本計畫整理

2.5.3.3 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

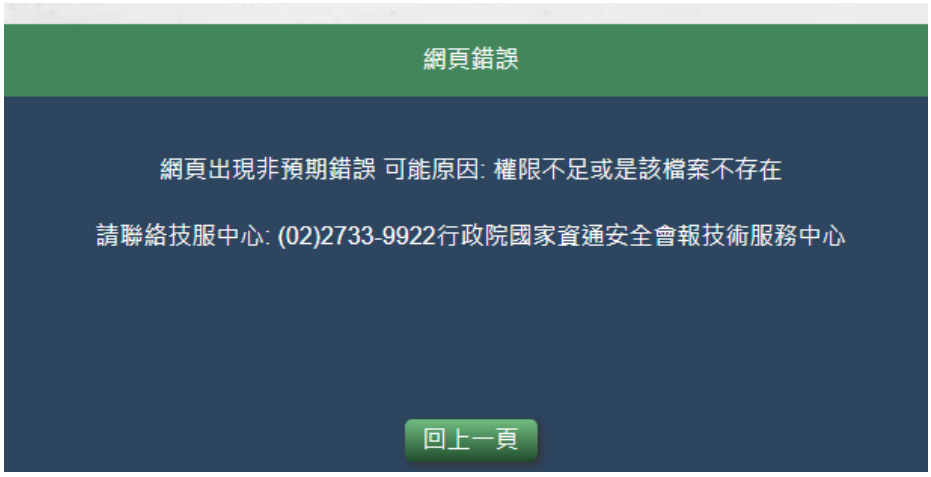
表54 系統發展生命週期開發階段控制措施 3

控制措施	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
適用等級	普、中、高
內容說明	系統錯誤頁面若揭露過於詳細之錯誤訊息，可能會被當成攻擊提示資訊而被人惡意利用，如密碼輸入錯誤之錯誤登錄嘗試、資料庫連線資訊、程式碼錯誤位置及 SQL 執行語法等。此類錯誤訊息應該留存於系統日誌內，讓系統管理者進行程式除錯或故障排除，而不應直接呈現於使用者操作頁面上。使用者頁面呈現過於詳細之錯誤訊息頁面範例詳見圖 65，範例中不僅洩露原始程式檔案位置，亦揭露程式碼實作細節，應避免顯示。 

資料來源：本計畫整理

圖65 使用者頁面呈現過於詳細之錯誤訊息

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	實務上常客製化錯誤頁面，僅顯示聯絡相關資訊與簡短錯誤代碼(如 404 錯誤等)，以提供使用者與客服人員或系統管理者溝通聯繫。使用客製化頁面範例詳見圖 66。  資料來源：本計畫整理 圖66 客製化頁面範例
驗證實務	▪ 如系統發生錯誤時，於使用者頁面上直接呈現詳細錯誤訊息，如洩露原始程式檔案位置或揭露程式碼實作細節等，而足以讓惡意攻擊者取得攻擊提示資訊，則未符合此控制措施。 ▪ 驗證人員宜發展測試案例，嘗試引發系統錯誤並觀察顯示結果，不得出現詳細錯誤訊息，如程式碼堆疊追蹤(stack trace)等。引發系統錯誤之步驟可能包含例如但不限於： 1.存取不存在或未經授權之網址頁面 2.輸入錯誤格式資料、超過範圍之數值及空白資料等 3.輸入特殊符號，如「’」、「”」、「;」、「>」及「#」等可能引發程式解析異常之字元
佐證資料	▪ 資通系統功能規格書 ▪ 資通系統測試紀錄

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
參考文獻	▪ 安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-11 錯誤處理) ▪ OWASP Web Security Testing Guide[9]

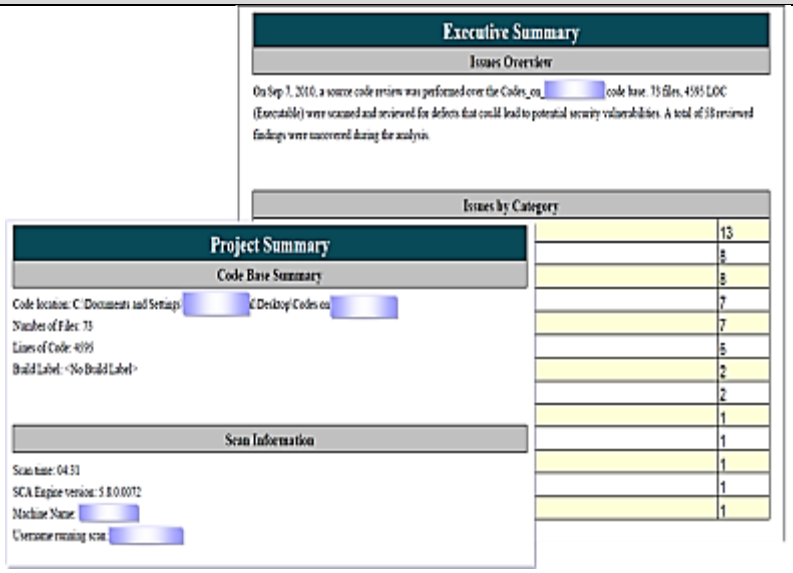
資料來源：本計畫整理

2.5.3.4 執行「源碼掃描」安全檢測

表55 系統發展生命週期開發階段控制措施 4

控制措施	執行「源碼掃描」安全檢測
適用等級	高
內容說明	▪ 源碼掃描係指使用靜態分析掃描工具，識別原始碼內安全弱點，其優點為提供快速、高覆蓋率檢測結果，惟掃描工具不可避免仍會存在漏報與誤報現象，故通常仍需經由專業人員進一步分析檢測結果，且為避免檢測活動流於形式，應確實進行源碼弱點修補作業，並追蹤修復狀況。 ▪ 要求廠商交付源碼檢測報告時，建議以市場主流且國際知名工具所檢測產出報告為優先考量，並確認其安全檢測能力是否充足，可參考 OWASP 組織所整理之檢測工具列表[11]。
驗證實務	▪ 如未檢附源碼掃描報告及修補紀錄，則未符合此控制措施。 ▪ 驗證人員宜檢視源碼掃描報告或相關執行紀錄，應注意所採用之源碼檢測工具需具備安全弱點(如 OWASP Top 10、跨站腳本攻擊及注入攻擊等)檢測能力，而非僅檢查程式碼不良寫法或臭蟲。源碼掃描報告畫面範例詳見圖 67。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	執行「源碼掃描」安全檢測
	 資料來源：本計畫整理 圖67 源碼掃描報告畫面範例
佐證資料	▪ 源碼掃描檢測報告 ▪ 源碼掃描檢測複測報告 ▪ 弱點修補紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-11 開發人員安全測試及評估)

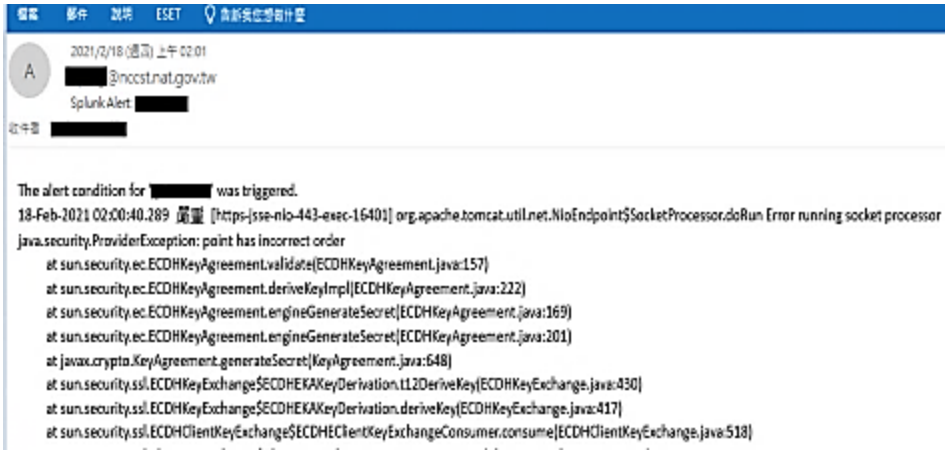
資料來源：本計畫整理

2.5.3.5 系統應具備發生嚴重錯誤時之通知機制

表56 系統發展生命週期開發階段控制措施 5

控制措施	系統應具備發生嚴重錯誤時之通知機制
適用等級	高
內容說明	▪ 系統應避免產生安靜無聲之錯誤，從而錯失及時處理黃金時間，所以當偵測到資通系統發生嚴重錯誤(如局部或全部系統功能停

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	系統應具備發生嚴重錯誤時之通知機制
	擺等)，應啟動警示機制以通知相關人員進行後續處理。通知機制如呈現於系統執行畫面、寄發 Email 或簡訊通知、以電話或當面告知等。嚴重錯誤通知信件範例詳見圖 68。  檔案 郵件 說明 ESET 告訴我您想做什麼 2021/2/18 (週四) 上午 02:01 [redacted]@nccst.nat.gov.tw Splunk Alert [redacted] 收件者 [redacted] The alert condition for [redacted] was triggered. 18-Feb-2021 02:00:40.289 嚴重 [https-jsse-nio-443-exec-16401] org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun Error running socket processor java.security.ProviderException: point has incorrect order at sun.security.ec.ECDHKeyAgreement.validate(ECDHKeyAgreement.java:157) at sun.security.ec.ECDHKeyAgreement.deriveKeyImpl(ECDHKeyAgreement.java:222) at sun.security.ec.ECDHKeyAgreement.engineGenerateSecret(ECDHKeyAgreement.java:169) at sun.security.ec.ECDHKeyAgreement.engineGenerateSecret(ECDHKeyAgreement.java:201) at javax.crypto.KeyAgreement.generateSecret(KeyAgreement.java:648) at sun.security.ssl.ECDHKeyExchange$ECDHEKAKeyDerivation.t12DeriveKey(ECDHKeyExchange.java:430) at sun.security.ssl.ECDHKeyExchange$ECDHEKAKeyDerivation.deriveKey(ECDHKeyExchange.java:417) at sun.security.ssl.ECDHClientKeyExchange$ECDHEClientKeyExchangeConsumer.consume(ECDHClientKeyExchange.java:518) 資料來源：本計畫整理 圖68 嚴重錯誤通知信件範例 ▪偵測管道如系統實作例外捕捉(try-catch)機制、利用 SOC 監控服務或自動化監控程式等事先規劃之發現機制，而非僅被動接收系統使用者抱怨客訴或通知。
驗證實務	▪如系統在發生嚴重錯誤時未具備有效可靠之通知機制，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員(如系統管理者、資安人員等)，以了解資通系統實作之錯誤偵測與通知機制。 ▪驗證人員宜發展測試案例，如模擬觸發嚴重錯誤情境，以確認系統會使用常態且可靠通知機制警示相關人員，如系統主動發出警示或導入監控工具等。
佐證資料	▪機關訂定之系統發展維護辦法 ▪機關訂定之監控作業程序 ▪資通系統錯誤處理功能測試紀錄
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	系統應具備發生嚴重錯誤時之通知機制
	System and Services Acquisition (控制措施編號 SA-11 開發人員安全測試及評估) ▪ 安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-13 可預測之故障預防)

資料來源：本計畫整理

2.5.4 系統發展生命週期測試階段

2.5.4.1 執行「弱點掃描」安全檢測

表57 系統發展生命週期測試階段控制措施 1

控制措施	執行「弱點掃描」安全檢測
適用等級	普、中、高
內容說明	▪ 資通系統應執行弱點掃描，如主機安全性弱點掃描與網頁應用程式安全性弱點掃描等，並提供檢測結果報告或執行紀錄。 ▪ 檢測活動之執行週期應符合資安法(如應辦事項等)與機關資安政策之規範。為避免檢測活動流於形式，應確實進行弱點修補作業，並追蹤修復狀況。弱點掃描執行範例詳見圖 69。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	執行「弱點掃描」安全檢測
	110 年第 2 季弱掃之弱點修補說明表 一、基本資料 系統負責人：張三、 組別：系統安全組、 科別：開發一科、 系統名稱：範例系統、 系統 IP：10.20.30.40、 系統網址：https://10.20.30.40/Demo/、 檢測結果 弱點掃描 網站應用程式安全檢測：嚴重(CRITICAL) 0、高(HIGH) 1、中(MEDIUM) 3、 檢測結果 弱點掃描 主機安全檢測：嚴重(CRITICAL) 1、高(HIGH) 0、中(MEDIUM) 8、 備註： •中心資安防護管理目標：「對外服務系統弱點掃描/滲透測試，以及資安健診之執行結果，判斷為中風險以上之弱點，應於 7 個工作天內完成矯正」、 •無法於規定期限內完成矯正，系統負責人經組內審查同意後，應於規定期限內 2 天前提報管理代表同意、 •本次弱點通知日期為：2021/6/1，依規定應於 2021/6/10 內完成弱點修補；若無法完成者，於 2021/6/8 前提報管理代表同意、 二、修復說明 NO、風險等級、弱點類別、是否修復、完成日期、修補處理方式或修補困難簡述，(如可修復，請填入預估修復時間)、 1、中、Vulnerable JavaScript libraries、是、110/6/2、已於6/2針對已知弱點版本JQuery 進行升級修補與系統調整、 2、中、Application error messages、是、110/6/2、已於 6/2 針對已知弱點進行修補，隱藏詳細錯誤訊息、 3、中、147164 - Apache Tomcat 9.0.0.M1 < 9.0.43 Multiple、是、110/6/2、已於 6/2 針對已知弱點版本 Apache Tomcat 進行升級修補與系統調整、 資料來源：本計畫整理 圖69 弱點掃描執行範例
驗證實務	▪如未檢附弱點掃描報告與修補紀錄，則未符合此控制措施。 ▪驗證人員宜檢視弱點掃描報告或相關執行紀錄，應注意所採用之弱點掃描工具需具備基本之安全弱點(包含但不限於 OWASP Top 10、軟體元件版本弱點、通訊協定弱點等)檢測能力。
佐證資料	▪弱點掃描檢測報告 ▪弱點掃描複測報告 ▪弱點修補紀錄
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 17-風險評鑑 Risk

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	執行「弱點掃描」安全檢測
	Assessment (控制措施編號 RA-5 弱點掃描) ▪ 安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-11 開發人員安全測試及評估)

資料來源：本計畫整理

2.5.4.2 執行「滲透測試」安全檢測

表58 系統發展生命週期測試階段控制措施 2

控制措施	執行「滲透測試」安全檢測
適用等級	高
內容說明	▪ 滲透測試是一種特殊類型評鑑，由技術熟練之資安專家模擬敵人行動，執行之白、灰、黑箱測試及分析等各種檢測活動，對資通系統或個別系統元件辨識可能被敵人利用之弱點。這種測試可用於驗證弱點，或驗證資通系統防護程度已達某種特定限制條件下(如時間、資源或技能等)能力。開始測試前，各方應協調及同意滲透測試場景與規則，宜將滲透測試規則與預期敵人進行攻擊所採用工具、技術及程序相互關聯，並依風險評鑑結果與等級需求進行滲透測試，並在定義之廣度/深度及限制因素下執行滲透測試。 ▪ 滲透測試與弱點掃描執行目的不相同，弱點掃描僅作為滲透測試活動其中之一個環節。弱點掃描係利用自動化工具，檢查系統潛藏弱點，產生弱點風險分析報告，並不會利用該弱點入侵破壞系統；而滲透測試則會試圖模仿敵人，從安全相關弱點或漏洞深度分析並加以利用，對系統進行入侵攻擊，執行過程中也會需要使用檢測工具輔助，但滲透測試成效更取決於檢測人員實務經驗與入侵技巧，而非僅仰賴自動化掃描工具。 ▪ 自行或委外開發之高風險等級資通系統，不分內網或外網，皆應執行滲透測試安全性檢測活動，並提供檢測結果報告或執行

本文件之智慧財產權屬數位發展部資通安全署擁有。

<table>
<tr><th>控制措施</th><th>執行「滲透測試」安全檢測</th></tr>
<tr><td></td><td>
紀錄以供查檢，檢測活動之執行週期應符合資安法(如應辦事項等)與機關資安政策之規範。為避免檢測活動流於形式，應確實進行弱點修補作業，並追蹤修復狀況。滲透測試執行範例詳見圖 70。
110 年第 2 季滲透測試之弱點修補說明表
一、基本資料
<table>
<tr><td>系統負責人</td><td>張三</td><td>組別</td><td>系統安全組</td><td>科別</td><td>開發一科</td></tr>
<tr><td>系統名稱</td><td colspan="5">範例系統</td></tr>
<tr><td>系統IP</td><td colspan="5">10.20.30.40</td></tr>
<tr><td>系統網址</td><td colspan="5">https://10.20.30.40/Demo/</td></tr>
<tr><td rowspan="2">滲透測試報告風險</td><td colspan="2">嚴重(CRITICAL)</td><td colspan="2">高(HIGH)</td><td>中(MEDIUM)</td></tr>
<tr><td colspan="2">0</td><td colspan="2">0</td><td>1</td></tr>
<tr><td>備註</td><td colspan="5">•中心資安防護管理目標：「對外服務系統弱點掃描/滲透測試，以及資安健診之執行結果，判斷為中風險以上之弱點，應於7個工作天內完成矯正」
•無法於規定期限內完成矯正，系統負責人經組內審查同意後，應於規定期限內2天前提報管理代表同意
•本次弱點通知日期為：2021/6/1，依規定應於2021/6/10內完成弱點修補；若無法完成者，於2021/6/8前提報管理代表同意</td></tr>
</table>
二、修復說明
<table>
<tr><th>NO.</th><th>風險等級</th><th>弱點類別</th><th>是否修復</th><th>完成日期</th><th>修補處理方式或修補困難簡述，(如可修復，請填入預估修復時間)</th></tr>
<tr><td>1</td><td>中</td><td>SQL Injection</td><td>是</td><td>110/6/2</td><td>已於6/2前完成將SQL語法改用PrepareStatement參數化查詢</td></tr>
</table>
資料來源：本計畫整理
圖70 滲透測試執行範例
</td></tr>
<tr><td>驗證實務</td><td>
▪ 如未檢附滲透測試報告及修補紀錄，則未符合此控制措施。
▪ 驗證人員宜檢視滲透測試報告或相關執行紀錄，並判斷檢測報告內容適切性，滲透測試實務上會有較多人工檢測行為軌跡，而非僅執行弱點掃描工具卻宣稱已完成滲透測試活動。
</td></tr>
<tr><td>佐證資料</td><td>
▪ 滲透測試檢測報告
▪ 滲透測試複測報告
▪ 弱點修補紀錄
</td></tr>
</table>

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	執行「滲透測試」安全檢測
參考文獻	▪ 安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-11 開發人員安全測試及評估) ▪ 安全控制措施參考指引(修訂)(V2.0)_附件 7-安全評鑑和授權 Security Assessment And Authorization (控制措施編號 CA-8 滲透測試) ▪ 政府機關滲透測試服務委外服務案建議書徵求文件 (V4.0)。https://www.nccst.nat.gov.tw/SecurityRFP [12]

資料來源：本計畫整理

2.5.5 系統發展生命週期部署與維運階段

2.5.5.1 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

表59 系統發展生命週期部署與維運階段控制措施 1

控制措施	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
適用等級	普、中、高
內容說明	▪ 資通系統部署環境各個軟體元件皆可能面臨資通安全威脅，包含作業系統、網頁伺服器、執行環境(如 Java Runtime Environment, JRE 等)及函式庫(Library)等，因此執行版本更新與安全弱點修補相當重要，資通系統軟體元件示意圖詳見圖 71。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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

資料來源：本計畫整理

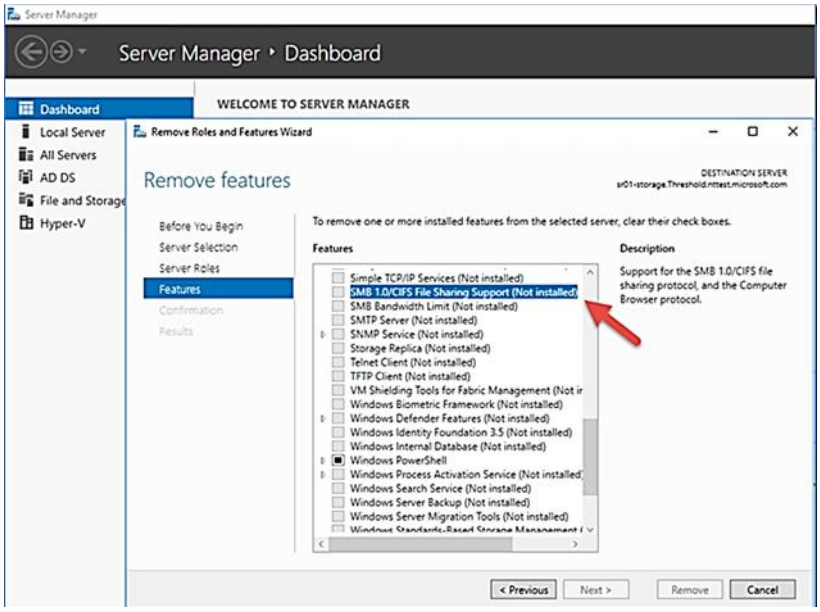
圖71 資通系統軟體元件示意圖

- 作業系統應定期安裝更新檔案(如 Windows Patch 等)，當接獲資安弱點通報或相關資安訊息時，宜確認資通系統是否在威脅範圍內，利用弱點掃描等安全性檢測發現安全漏洞時，亦應進行元件更新與弱點修補。
- 政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資安法之資產盤點與風險評估應辦事項。VANS 機制實作範例詳見圖 72。

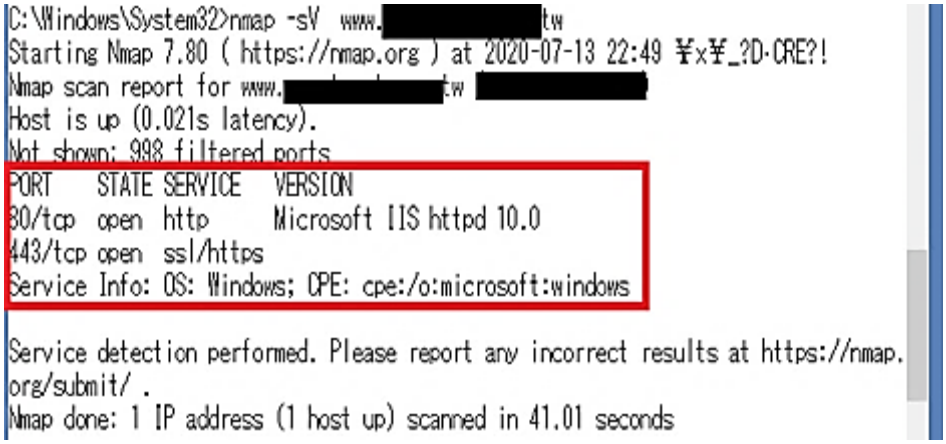
資料來源：本計畫整理

圖72 VANS 機制實作範例

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	▪系統管理者應盤點並保留業務運作必要開放之服務與埠口，以防止非授權連線、非授權資訊傳送或非授權通道建立。伺服器通常可同時提供廣泛多元之功能與服務，以 Windows 作業系統為例，不同服務具有不同預設啟動原則，如預設自動啟動、在需要時啟動及預設停用等。預設啟用功能服務可能在機關業務運作上並非必要，若繼續開放這些服務及埠口連線易增加外部連線攻擊之資安風險，應限制資通系統所提供服務及埠口，以達到安全強化目的。例如，Windows 作業系統透過 TCP 445 埠口提供 Server Message Block (SMBv1)服務，而著名之WannaCry勒索軟體亦利用此埠口進行攻擊，原則上建議停用 SMBv1 服務，並確認關閉 445 埠口以降低資安風險。Windows Server 移除系統服務操作範例詳見圖 73。  資料來源：本計畫整理 圖73 Windows Server 移除系統服務操作範例
驗證實務	▪如資通系統未更新與修補部署環境中之軟體元件，包含作業系統、資通系統伺服器、執行環境以及函式庫等，造成存留重大安全漏洞，或仍允許使用者透過網路連接至非必要系統服務及

本文件之智慧財產權屬數位發展部資通安全署擁有。

<table>
<tr><td>控制措施</td><td>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</td></tr>
<tr><td></td><td>埠口，則未符合此控制措施。
▪驗證人員宜檢視機關訂定之資通系統相關規範，或訪談相關權責人員(如系統管理者與資安人員等)，以及檢視系統設定等方式，了解如何進行資通系統元件修補更新作業。
▪驗證人員宜檢視部署環境之更新修補狀況，以避免使用具安全漏洞之元件為原則，如依機關規定時程安裝作業系統更新(Windows Update)，並修補與更新資通系統伺服器、執行環境及函式庫等版本。
▪驗證人員宜使用 nmap[13]等網路檢測工具，掃描資通系統部署環境所開放之服務與埠口，檢視掃描結果，請相關人員說明服務及埠口使用目的，若非為資通系統業務運作必要，原則上應設定組態檔案或防火牆規則以禁止使用。
▪以下為使用 nmap 檢測範例：nmap -sV 網站位址。
檢測結果詳見圖 74。
 

資料來源：本計畫整理
圖74 Nmap 檢測埠口服務範例</td></tr>
<tr><td>佐證資料</td><td>▪機關訂定之系統發展維護辦法
▪資通系統部署之防火牆規則
▪資通系統連線檢測紀錄</td></tr>
</table>

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
參考文獻	▪ 安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-4 獲得程序) ▪ 安全控制措施參考指引(修訂)(V2.0)_附件 8-組態管理 Configuration Management (控制措施編號 CM-7 最基本功能) ▪ https://www.nccst.nat.gov.tw/Vans ▪ Nmap, https://nmap.org/ [13]

資料來源：本計畫整理

2.5.5.2 資通系統不使用預設密碼

表60 系統發展生命週期部署與維運階段控制措施 2

控制措施	資通系統不使用預設密碼
適用等級	普、中、高
內容說明	▪ 資通系統相關軟體(如資料庫與資通系統伺服器等軟體元件)若內建並啟用預設帳號密碼，很可能被惡意攻擊者透過搜尋引擎而輕易取得並加以利用，故應停用預設帳號與密碼，在預設帳號無法停用條件下，則應儘速變更密碼。 ▪ 目前多數軟體元件會基於故障安全(Fail-Safe)原則，預設未啟用內建帳號密碼，但仍可能因系統管理者操作上失誤，在不經意啟用預設密碼而不自知，尤其若使用較舊版本之元件，操作風險又更高。以 Apache Tomcat 為例，新版本如 Apache Tomcat 9 已從組態設定檔案內移除預設帳號密碼，管理人員必須自行新增帳號密碼，故可降低操作失誤之風險；但若系統仍然使用舊版 Apache Tomcat 7(官方已不再維護，建議更新版本)，此版本之組態設定檔 tomcat-users.xml 仍內建帳號密碼，雖預設為已註解之未啟用狀態，但管理人員仍可因為操作不當而啟用預設帳密，故風險較高，Tomcat 預設帳密設定範例詳見圖 75。

本文件之智慧財產權屬數位發展部資通安全署擁有。

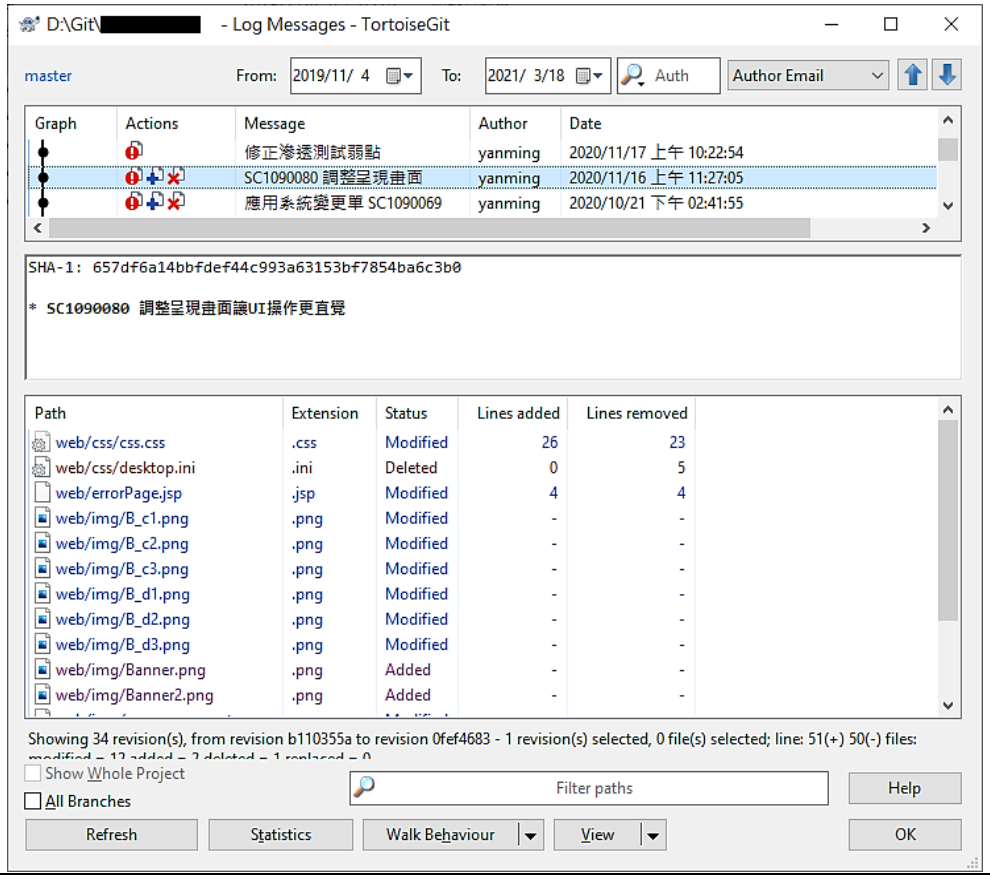
控制措施	資通系統不使用預設密碼
	 資料來源：本計畫整理 圖75 Apache Tomcat 7 預設帳號密碼設定檔範例
驗證實務	▪ 資通系統資料庫與資通系統伺服器等軟體元件如使用預設密碼，則未符合此控制措施。 ▪ 驗證人員宜訪談相關權責人員(如系統管理者與資料庫管理者等)，以了解資通系統所使用之相關軟體。 ▪ 驗證人員宜發展測試案例，如利用軟體元件官方說明手冊或搜尋引擎等方式取得預設密碼後，嘗試進行帳號登入，系統應拒絕登入。
佐證資料	▪ 機關訂定之系統發展維護辦法 ▪ 資通系統測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-4 獲得程序)

資料來源：本計畫整理

2.5.5.3 於系統發展生命週期之維運階段，應執行版本控制與變更管理

本文件之智慧財產權屬數位發展部資通安全署擁有。

表61 系統發展生命週期部署與維運階段控制措施 3

控制措施	於系統發展生命週期之維運階段，應執行版本控制與變更管理
適用等級	中、高
內容說明	▪嚴謹之版本控制與變更管理可強化系統安全性與可用性。在維運階段可能因需求變更、系統除錯、功能精進等原因而需要變更系統組態，而版本控制在記錄系統組態在某段時間內之變更行為，使得使用者在需要時可取回特定版本，變更管理應予安全管制，須避免被惡意植入不當軟體、後門及電腦病毒等危害系統安全之元件。 ▪實務上可建立程式館或使用版本控制軟體工具，以方便追蹤歷次之變更版本。免費版本控制工具如 CVS、Git 及 Subversion 等，這些工具可將每次版本所有簽入檔案狀態儲存下來，並描述該版本之變更用途，如修正錯誤或新增功能等，這些描述可協助系統管理者理解各版本狀態差異，並在將來可視需求還原至先前特定版本。免費版本控制工具 Git 操作畫面範例詳見圖 76。 

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	於系統發展生命週期之維運階段，應執行版本控制與變更管理
	資料來源：本計畫整理 圖76 Git 操作畫面範例 ▪系統管理者進行系統變更作業，應符合機關規範，完成申請與審核程序後始可進行，如填寫資通系統變更作業申請單。執行變更作業前，宜先執行系統備份作業並訂定復原計畫，以保留原有系統作為異常時之衡量基準或復原準備。系統變更完成後，應更新相關系統操作文件及紀錄。 ▪機關應以積極管理為原則，避免完全由委外廠商負責。若系統元件變更作業係委由廠商執行，應經過申請審核相關程序，並在機關人員監督下完成變更。
驗證實務	▪如機關未執行版本控制與變更管理，則未符合此控制措施。 ▪驗證人員宜檢視機關訂定之資通系統相關規範，或訪談相關權責人員(如系統管理者等)，以了解資通系統如何進行版本控制與變更管理。 ▪驗證人員宜抽查版本控制與變更管理作業相關紀錄，如抽查資通系統近期之需求變更申請紀錄，應追蹤其對應之程式版本，以驗證是否符合機關規定。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統變更作業申請紀錄 ▪資通系統版本變更紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-10 開發人員組態管理)

資料來源：本計畫整理

2.5.6 系統發展生命週期委外階段

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.5.6.1 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

表62 系統發展生命週期委外階段控制措施

控制措施	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
適用等級	普、中、高
內容說明	▪應依據適用之法規命令與行政規則(含規範與指引等文件)及機關任務/營運需求，在資通系統、系統元件或資通系統服務合約納入安全相關要求，如可能包含安全功能要求、保護與安全相關文件要求、安全檢測活動要求及驗收標準等。 ▪資通系統委外安全需求可參考技服中心「資通系統委外開發 RFP 資安需求範本(V3.0)」[6]，內容範例詳見圖 77。 **3. 需求說明** **3.1 整體需求說明** 詳細條列系統之各項功能要求及系統作業流程，並詳細說明之。 3.1.1 功能需求 3.1.2 系統作業流程說明 **3.2 資安需求** 委託機關應依據「資通安全責任等級分級辦法」之附表十「資通系統防護基準」，選取適用項目，包含 41 項技術面、13 項管理面之需求項目(詳附件 1)，以及 22 項資通系統防護基準之控制措施(詳附件 2、3)。 資料來源：本計畫整理 圖77 資通系統委外開發 RFP 資安需求範本
驗證實務	▪如委外開發之資通系統未將安全需求納入委外契約，則未符合此控制措施。 ▪驗證人員宜檢視委外契約，確認其中是否納入系統安全需求，應包含機密性、完整性及可用性等構面。
佐證資料	資通系統委外契約

本文件之智慧財產權屬數位發展部資通安全署擁有。

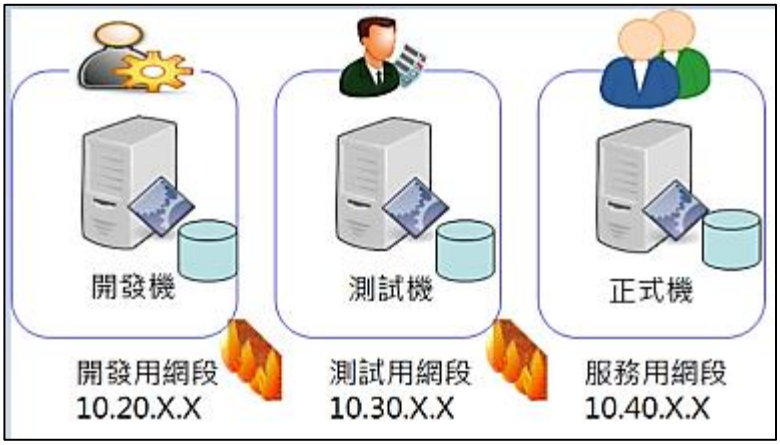
控制措施	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約
參考文獻	▪ 安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-4 獲得程序)

資料來源：本計畫整理

2.5.7 獲得程序

2.5.7.1 開發、測試及正式作業環境應為區隔

表63 獲得程序控制措施

控制措施	開發、測試及正式作業環境應為區隔
適用等級	中、高
內容說明	▪ 應運用獨立之測試環境對資通系統變更進行分析，獨立之測試環境是指實體或邏輯上區隔、運作環境不同之環境，足以確保在測試環境中活動不會衝擊在正式作業環境中活動，正式作業環境中資訊不會無意中傳送給測試環境。應確保區隔環境時所需安全強度，如隔離相互間網路存取等，以網段區隔不同作業環境示意圖詳見圖 78。  資料來源：本計畫整理 圖78 作業環境區隔示意圖

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	開發、測試及正式作業環境應為區隔
	▪開發環境、測試環境及正式作業環境區隔成不同之設備及網段，限制所能存取之應用程式及資料庫，以保護正式作業環境系統及資料。實務上開發人員常以本機電腦為開發環境，並連結使用本機端之資料庫進行應用程式開發。開發完畢再將應用程式部署至測試主機，並連結至測試用資料庫，供測試人員進行測試使用。俟測試完畢，再將應用程式部署至正式環境，並連結至正式資料庫提供上線服務。
驗證實務	▪如未對正式作業環境進行存取保護，導致部署於正式環境資通系統與其內資料可能會受到開發環境與測試環境汙染，或是發生未經授權存取行為，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員(如系統管理者與網路管理者等)，以了解資通系統開發、測試及作業環境之規劃。 ▪驗證人員宜檢視資通系統開發、測試及正式作業環境，包含其連結之資料庫，開發與測試環境之區隔方式，以不危害正式環境運作及資料內容為原則，同時須保護正式資料之機密性、完整性及可用性。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統部署之防火牆規則
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 8-組態管理 Configuration Management (控制措施編號 CM-2 基準組態) ▪安全控制措施參考指引(修訂)(V2.0)_附件 8-組態管理 Configuration Management (控制措施編號 CM-4 安全衝擊分析)

資料來源：本計畫整理

2.5.8 系統文件

2.5.8.1 應儲存與管理系統發展生命週期之相關文件

本文件之智慧財產權屬數位發展部資通安全署擁有。

表64 系統文件控制措施

<table>
<tr><th>控制措施</th><th>應儲存與管理系統發展生命週期之相關文件</th></tr>
<tr><td>適用等級</td><td>普、中、高</td></tr>
<tr><td>內容說明</td><td>系統發展生命週期之相關文件應以書面或電子化形式保存，並被納入管理程序。系統相關文件儲存與管理範例，詳見圖 79。
<table>
<tr><th>文件/紀錄名稱</th><th>編號</th><th>保存年限</th></tr>
<tr><td>軟體發展計畫</td><td>依建構項目規範編碼</td><td>結案後 2 年</td></tr>
<tr><td>軟體需求規格書</td><td>依建構項目規範編碼</td><td>結案後 2 年</td></tr>
<tr><td>系統規格書</td><td>依建構項目規範編碼</td><td>結案後 2 年</td></tr>
<tr><td>軟體測試計畫</td><td>依建構項目規範編碼</td><td>結案後 2 年</td></tr>
<tr><td>維護手冊</td><td>依建構項目規範編碼</td><td>結案後 2 年</td></tr>
<tr><td>軟體使用手冊</td><td>依建構項目規範編碼</td><td>結案後 2 年</td></tr>
<tr><td>系統文件審查表</td><td>NCCST_FT_040</td><td>結案後 2 年</td></tr>
<tr><td>系統原始碼</td><td>依建構項目規範編碼</td><td>結案後 2 年</td></tr>
<tr><td>測試問題紀錄表</td><td>NCCST_FT_041
合併於軟體測試報告</td><td>結案後 2 年</td></tr>
<tr><td>軟體測試報告</td><td>依建構項目規範編碼</td><td>結案後 2 年</td></tr>
<tr><td>驗收紀錄表</td><td>NCCST_FT_042</td><td>結案後 2 年</td></tr>
</table>
資料來源：本計畫整理

圖79 系統相關文件儲存與管理範例</td></tr>
<tr><td>驗證實務</td><td>▪ 如未儲存與管理系統發展生命週期之相關文件，則未符合此控制措施。
▪ 驗證人員宜檢視儲存之系統發展生命週期之相關文件，須符合機關資安政策與變更管理程序。</td></tr>
<tr><td>佐證資料</td><td>▪ 機關訂定之文件管理規範
▪ 資通系統相關文件</td></tr>
<tr><td>參考文獻</td><td>▪ 安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-5 資訊系統文件)
▪ 安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-10 開發人員</td></tr>
</table>

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應儲存與管理系統發展生命週期之相關文件
	組態管理)

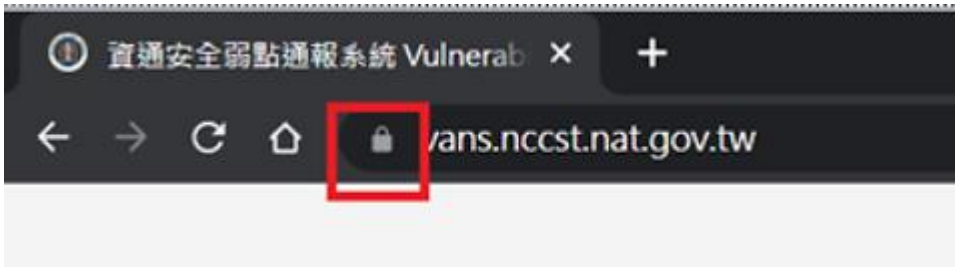
資料來源：本計畫整理

2.6 系統與通訊保護

2.6.1 傳輸之機密性與完整性

2.6.1.1 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

表65 傳輸之機密性與完整性控制措施 1

控制措施	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
適用等級	高
內容說明	資通系統可實作加密機制，如 HTTPS、SSH、SFTP 及 VPN 等加密傳輸協定，或透過應用程式等適當方式，先行將資訊加密後再傳輸，以保護資料機密性與完整性。當站台啟用 HTTPS，於瀏覽器網址列上會出現安全鎖頭圖示，範例詳見圖 80。  資料來源：本計畫整理 圖80 站台啟用 HTTPS
驗證實務	▪如資通系統未採用傳輸加密機制，亦無其他替代之實體保護措

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	施，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員(如系統管理者與網路管理者等)，以了解資通系統所使用之加密機制。 ▪驗證人員宜發展測試案例以驗證系統確實使用加密傳輸協定，如檢視資通系統是否允許使用未加密之傳輸協定進行頁面存取及資料傳輸，如仍允許全部或部分非公開頁面使用 HTTP 存取，或允許使用未加密之 Telnet 與 FTP 等，必要時可使用 Wireshark 等網路封包分析工具，驗證是否使用加密協定。 ▪驗證人員宜確認是否使用其他足以保護資料傳輸過程機密性與完整性之實體保護方案，如專屬線路或透過應用程式加密等。
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統加密連線之測試報告
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 19-系統與通訊保護 System and Communications Protection (控制措施編號 SC-8 傳輸機密性和完整性)

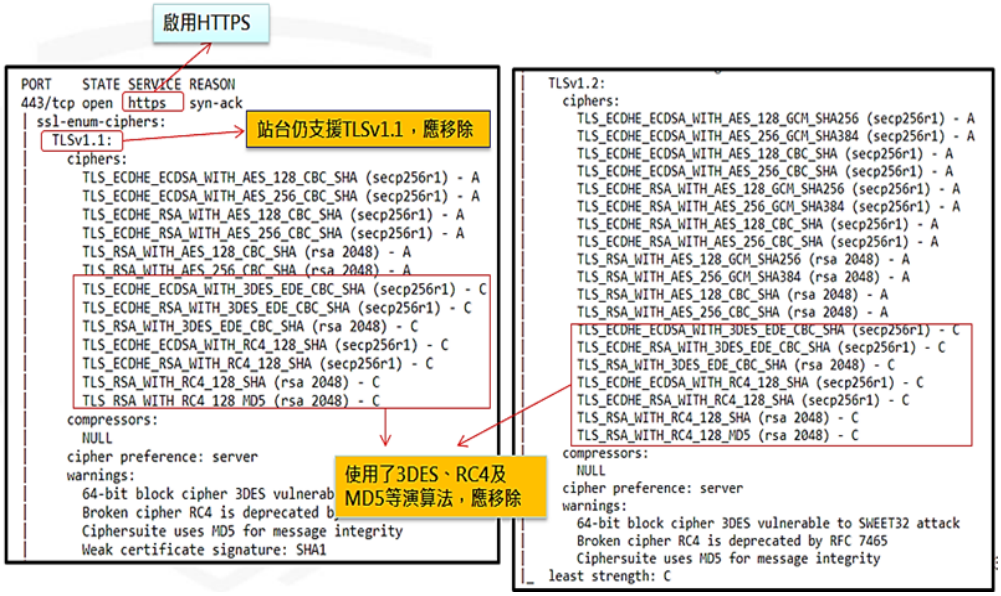
資料來源：本計畫整理

2.6.1.2 使用公開、國際機構驗證且未遭破解之演算法

表66 傳輸之機密性與完整性控制措施 2

控制措施	使用公開、國際機構驗證且未遭破解之演算法
適用等級	高
內容說明	SSL V3 及 TLS1.0 皆已被視為安全性不足，若無相容性問題，建議停用。110 年 3 月，RFC 8996 標準[10]正式棄用 TLS1.0 及 TLS 1.1。對 IE、Edge、Chrome、Safari 及 Firefox 而言，目前皆建議網站採用 TLS 1.2，而網頁連線也以 TLS 1.2 為主。另外，加密協定所使用之演算法(Ciphers)亦有安全考量，如 RC2、RC4、DES 及 3DES 等加密演算法已遭破解，建議可改用 AES 與 RSA 等尚

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用公開、國際機構驗證且未遭破解之演算法
	未遭破解之加密演算法。
驗證實務	▪如資通系統啟用 SSL V3、TLS1.0 及 TLS1.1 等通訊協定，或所使用演算法包含 RC2、RC4、DES、3DES、MD5 及 SHA 等安全性不足之加密或雜湊演算法，則未符合此控制措施。 ▪驗證人員宜驗證資通系統所允許通訊協與所使用加密演算法，檢測方式如使用 nmap 檢測工具，使用 Windows 命令提示字元之檢測指令如下： namp --script ssl-enum-ciphers -p 443 網站位址 執行結果範例詳見圖 81，範例中顯示站台仍使用不安全之 TLS1.1 傳輸協定，並且使用 3DES、RC4、SHA 以及 MD5 等演算法，應從站台設定移除。  資料來源：本計畫整理 圖81 Nmap 檢測 ciphers
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統加密連線之測試報告，如 Nmap 檢測結果
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 19-系統與通訊保護 System and Communications Protection (控制措施編號 SC-12 密鑰

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用公開、國際機構驗證且未遭破解之演算法
	建立和管理) ▪ OWASP Web Security Testing Guide[9] ▪ RFC8996[10]

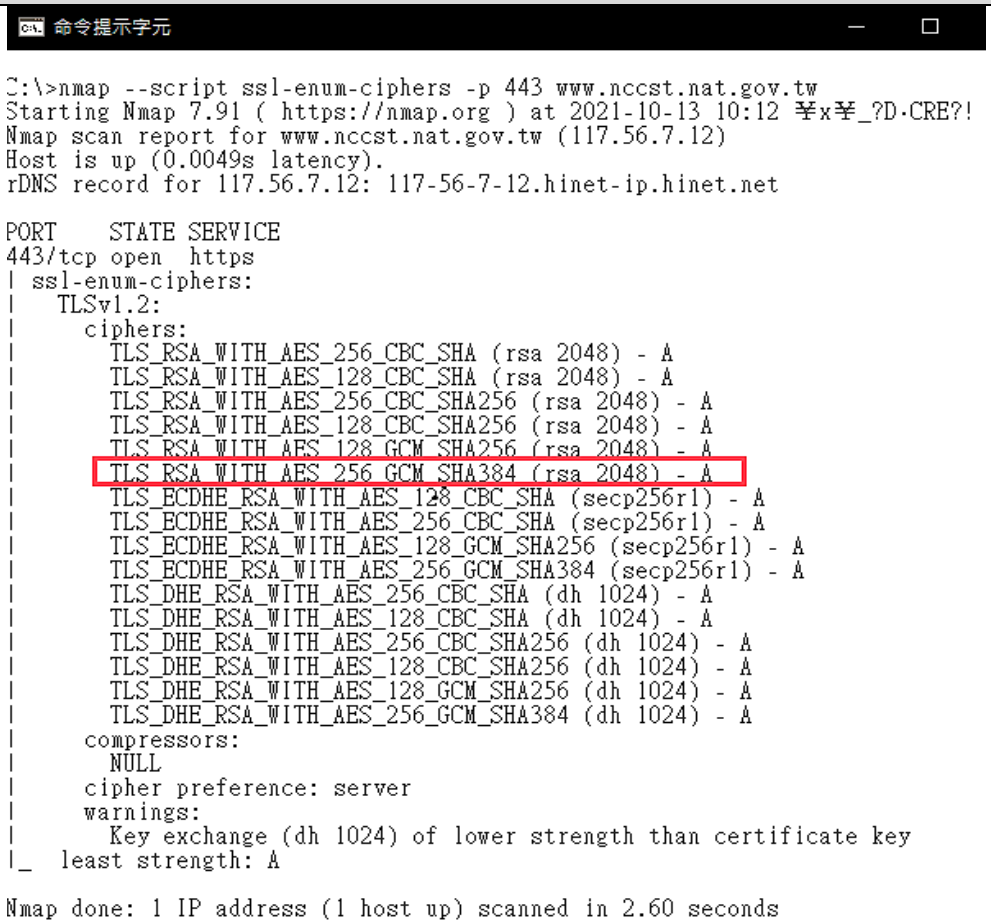
資料來源：本計畫整理

2.6.1.3 支援演算法最大長度金鑰

表67 傳輸之機密性與完整性控制措施 3

控制措施	支援演算法最大長度金鑰
適用等級	高
內容說明	伺服器進行加密傳輸(如 HTTPS 等)時，可能因作業系統與資通系統伺服器元件版本等技術限制，僅能使用特定之加密演算法及金鑰長度範圍，此時宜設定資通系統可支援較長之金鑰長度，以降低金鑰被破解風險。
驗證實務	▪ 驗證人員宜發展測試案例，驗證資通系統所允許之加密演算法，並檢視其金鑰長度。如資通系統未設定使用在技術許可範圍內之最大長度金鑰，原則上未符合此控制措施。 ▪ 檢測方式如使用 nmap 檢測工具，檢測指令範例如下： namp --script ssl-enum-ciphers -p 443 網站位址 執行結果範例詳見圖 82。從範例中 Ciphers 列表中顯示，以 TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)為例，其 AES 演算法使用之金鑰長度可達 256 位元，SHA 演算法金鑰長度可達 384 位元，而 RSA 演算法使用之金鑰長度可達 2048 位元，資通系統使用之加密演算法可參考此金鑰長度設定值。

本文件之智慧財產權屬數位發展部資通安全署擁有。

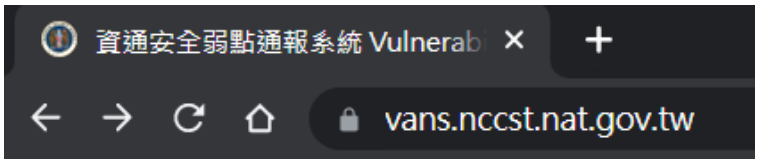
控制措施	支援演算法最大長度金鑰
	 資料來源：本計畫整理 圖82 Nmap 檢測 ciphers 長度
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統加密連線之測試報告，如 Nmap 檢測結果
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 19-系統與通訊保護 System and Communications Protection (控制措施編號 SC-12 密鑰建立和管理) ▪OWASP Web Security Testing Guide[9]

資料來源：本計畫整理

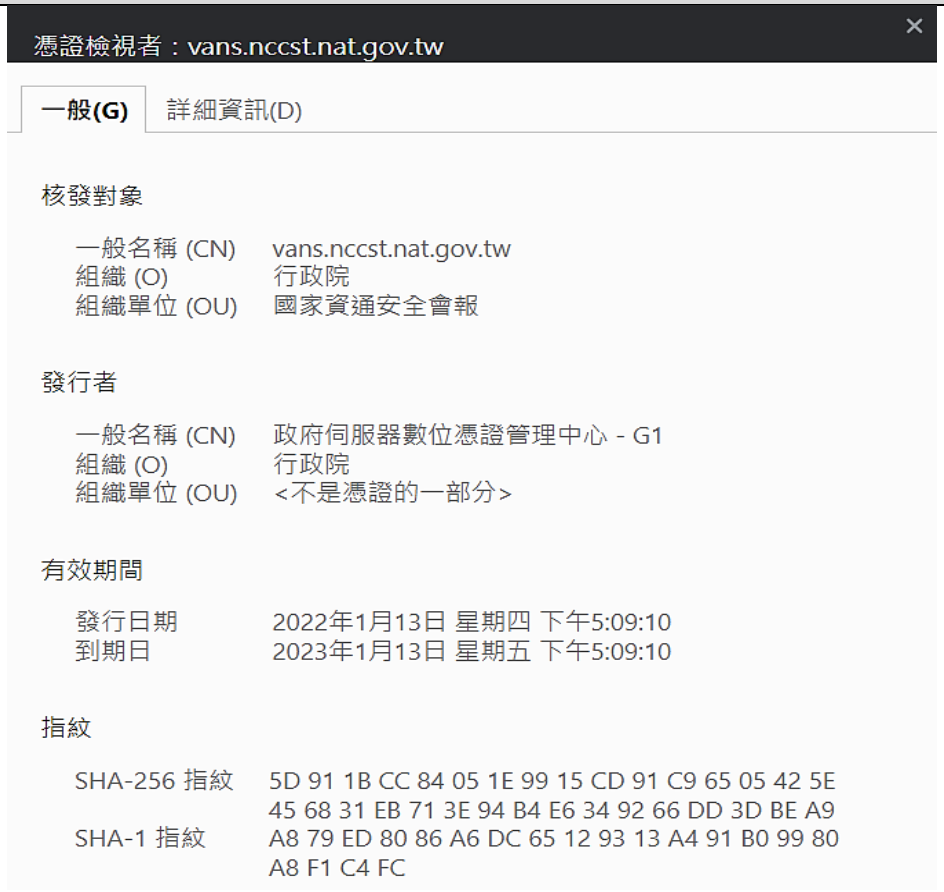
本文件之智慧財產權屬數位發展部資通安全署擁有。

2.6.1.4 加密金鑰或憑證應定期更換

表68 傳輸之機密性與完整性控制措施 4

控制措施	加密金鑰或憑證應定期更換
適用等級	高
內容說明	為避免 TLS 憑證被人惡意破解偽造，資通系統應設定憑證使用效期並定期更換。開對外服務站台應使用公正第三方所簽發之 SSL 憑證，以政府伺服器數位憑證管理中心(GTLSCA)為例，109 年 9 月 1 日起所簽發之 TLS 憑證已調整為 1 年效期。機關內部使用之站台若使用自行簽發之 TLS 憑證，亦須避免使用萬年憑證，應評估資安風險及使用需求後，設定合理使用效期。
驗證實務	▪ 資通系統若使用已過期之 SSL 憑證，則未符合此控制措施。 ▪ 驗證人員宜訪談系統管理者並檢視 SSL 憑證日期資訊，資通系統應設定合理之憑證效期，不得使用已過期之憑證。檢視站台 SSL 憑證之步驟範例，詳見圖 83 至圖 85。  資料來源：本計畫整理 圖83 檢視 SSL 憑證步驟 1  資料來源：本計畫整理 圖84 檢視 SSL 憑證步驟 2

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	加密金鑰或憑證應定期更換
	 資料來源：本計畫整理 圖85 檢視 SSL 憑證步驟 3
佐證資料	▪ 機關訂定之系統發展維護辦法 ▪ 機關訂定之金鑰管理規範 ▪ 資通系統憑證資訊
參考文獻	▪ 安全控制措施參考指引(修訂)(V2.0)_附件 19-系統與通訊保護 System and Communications Protection (控制措施編號 SC-12 密鑰建立和管理) ▪ 安全控制措施參考指引(修訂)(V2.0)_附件 8-組態管理 Configuration Management (控制措施編號 CM-3 組態變更控制)

資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.6.1.5 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

表69 傳輸之機密性與完整性控制措施 5

控制措施	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
適用等級	高
內容說明	▪伺服器端之金鑰一旦外洩，則加密機制視同無效，嚴重危害系統之機密性，故應訂定相關作業標準或管理規範，以妥善保護金鑰。應依據金鑰產生、分配、儲存、存取及銷毀之要求，實作應有之安全控制措施，確保金鑰機密性、完整性及可用性。 ▪資通系統使用政府核發之憑證時，建議可依照 GCP 政府憑證入口網(https://gcp.nat.gov.tw)提供之「公鑰憑證安全性檢查表」，驗證各項目之檢查機制，以確保身分認證或數位簽章之安全性，使用範例詳見圖 86。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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

應用系統使用公鑰憑證處理之安全檢查表

國家發展委員會 109 年 9 月

說明：為確保各機關(構)開發之應用系統使用政府核發之憑證進行身分認證或數位簽章之安全性，爰訂定下列安全檢查項目，請各機關(構)於驗收時，應確實檢查符合性。

項次	安全檢查項目	檢查結果
1	系統應由安全管道取得 Root CA 的自簽憑證(Self-Signed Certificate)，並妥善安全保存於系統中	☐ 通過 ☐ 不通過
2	系統應設定所信賴的憑證保證等級，並檢查憑證之憑證政策(Certificate Policies)欄位所記載的 Policy OID 是否符合憑證保證等級的要求，對於不符保證等級之憑證應拒絕存取(例如正式上線系統應對測試等級的憑證加以拒絕)	☐ 通過 ☐ 不通過
3	系統應檢查 CA 本身憑證確為 Root CA 所簽發的憑證 (至少需檢查憑證的 Issuer Name (DN)是否與 Root CA 自簽憑證的 Subject Name(DN)相符，並以 Root CA 自簽憑證所記載的 Public Key 檢驗 CA 本身憑證的簽章)	☐ 通過 ☐ 不通過

資料來源：本計畫整理

圖86 公鑰憑證安全性檢查表範例

驗證實務	▪如未訂定伺服器端之金鑰保管管理規範或未實施應有之安全防護措施，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員及檢視機關作業規定等方式，驗證機關已訂定伺服器端金鑰管理規範並落實執行，針對金鑰保護之

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
	安全防護措施應包含機密性、完整性及可用性之保護，如防止伺服器金鑰被未經授權之存取、置換或毀損。
佐證資料	▪機關訂定之系統發展維護辦法 ▪機關訂定之金鑰管理規範
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 19-系統與通訊保護 System and Communications Protection (控制措施編號 SC-12 密鑰建立和管理)

資料來源：本計畫整理

2.6.2 資料儲存之安全

2.6.2.1 資通系統重要組態設定檔案及其他具保護需求之機密資訊應加密或以其他適當方式儲存

表70 資料儲存之安全控制措施

控制措施	資通系統重要組態設定檔案及其他具保護需求之機密資訊應加密或以其他適當方式儲存
適用等級	高
內容說明	▪機關應評估資通系統所需保護之機密資訊，如存放個人資料之資料庫表格或欄位等。 ▪資通系統常利用組態設定檔案存放一些於運作過程中會使用參數，好處為可避免將參數值寫死於應用程式內而造成後續維護變更困難。惟部分參數可能包含機密資訊，如資料庫連線位址資訊與帳號密碼等，這些資訊若以明文形式留存於組態設定檔案內可能提高資料外洩的風險，故應加密或以其他適當方式保護。 ▪實務上依照開發框架及軟體元件不同特性，可能支援對整個組態設定檔案加密機制，或是針對其中特定參數進行加密保護，如僅加密資料庫連線字串等。以.NET 資通系統為例，組態檔是標準 XML 格式檔案，其資料庫連線字串會寫於 web.config 組態檔案

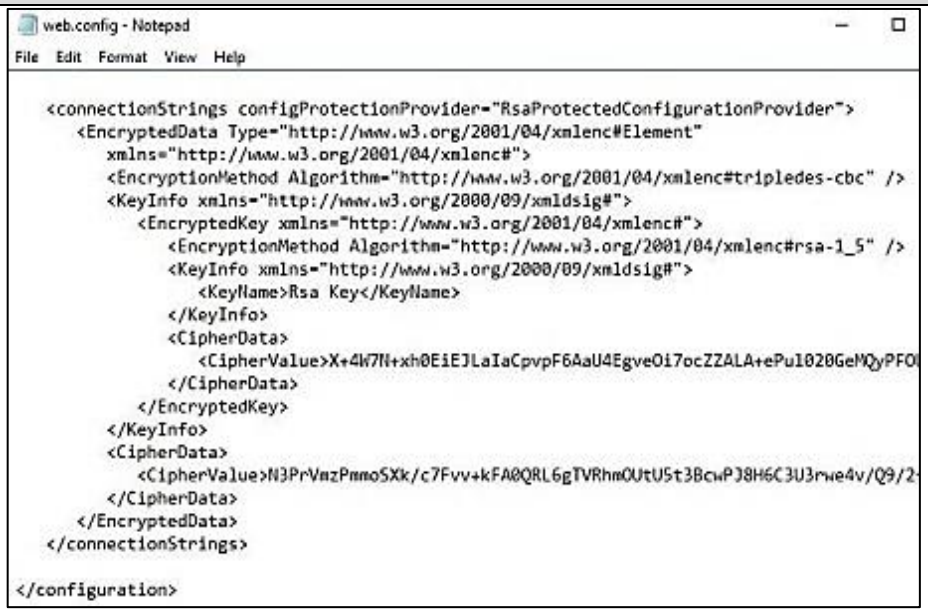
本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統重要組態設定檔案及其他具保護需求之機密資訊應加密或以其他適當方式儲存
	內，並透過<connectionStrings>元素進行設定，範例詳見圖 87。 資料來源：本計畫整理 圖87 connectionStrings 使用範例 ▪.NET 提供使用者利用.NET IIS 註冊工具，加密或解密組態設定檔案內機密資訊。系統運作過程中，則會自動解密 web.config 內元素。加密方式如透過命令提示字元，執行指令 aspnet_regiis.exe -pef appSettings <專案目錄>，範例詳見圖 88。 資料來源：本計畫整理 圖88 aspnet_regiis 使用範例 ▪connectionStrings 經過加密處理後，web.config 會呈現非明文形式結果，範例詳見圖 89。

```
<connectionStrings>
  <add
    name="NorthwindConnectionString"
    connectionString="Data Source=serverName;Initial
    Catalog=Northwind;Persist Security Info=True;User
    ID=userName;Password=password"
    providerName="System.Data.SqlClient"
  />
</connectionStrings>
```

```
C:\Windows\Microsoft.NET\Framework\v4.0.30319>aspnet_regiis.exe -pef appSettings
Microsoft (R) ASP.NET RegIIS version 4.0.30319.0
Administration utility to install and uninstall ASP.NET on the local machine.
Copyright (C) Microsoft Corporation.  All rights reserved.
Encrypting configuration section...
Succeeded!
```

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統重要組態設定檔案及其他具保護需求之機密資訊應加密或以其他適當方式儲存
	 資料來源：本計畫整理 圖89 connectionStrings 加密結果範例
驗證實務	▪ 如資通系統重要組態設定檔案及其他具保護需求之機密資訊應加密或以其他適當方式儲存(如實體隔離、專用電腦作業環境及資料加密等)，則未符合此控制措施。原則上，資通系統至少應加密保護資料庫連線位址資訊與連線帳號密碼等機密資訊，針對儲存機密資訊(如個人資料等)之資料庫表格或欄位亦應實作適當保護機制。 ▪ 驗證人員宜訪談相關權責人員(如系統管理者等)，以了解系統組態設定檔儲存方式，如檢視系統組態設定檔，不得以明文呈現資料庫連線資訊及帳號密碼等機密資訊，須使用適當加密方式(如檔案加密、連線字串等重要組態欄位加密等)確保機密性。 ▪ 驗證人員宜訪談相關權責人員(如資料庫管理者等)，以了解系統資料庫所採用之資料保護技術，如加密資料庫表格或特定欄位等。 ▪ 若組態設定值僅透過簡單編碼(如 Base64 編碼等)，因無法有效保護機密性，原則上未符合此控制措施。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	資通系統重要組態設定檔案及其他具保護需求之機密資訊應加密或以其他適當方式儲存
佐證資料	▪機關訂定之系統發展維護辦法 ▪資通系統組態設定檔
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 19-系統與通訊保護 System and Communication Protection (控制措施編號 SC-28 靜置資訊之保護) ▪保護連線資訊。https://docs.microsoft.com/

資料來源：本計畫整理

2.7 系統與資訊完整性

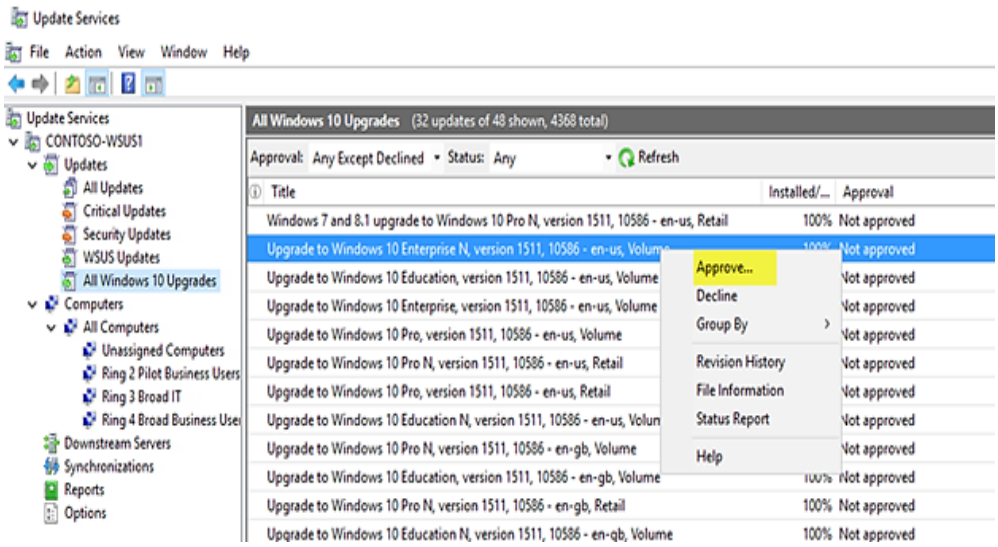
2.7.1 漏洞修復

2.7.1.1 系統之漏洞修復應測試有效性及潛在影響，並定期更新

表71 漏洞修復控制措施 1

控制措施	系統之漏洞修復應測試有效性及潛在影響，並定期更新
適用等級	普、中、高
內容說明	▪應定期進行軟體元件漏洞修復與更新，包含作業系統、資通系統伺服器、開發框架，以及第三方函式庫等軟體元件。例如，以微軟 WSUS[14]管理派送安裝 Windows 作業系統更新，範例詳見圖 90。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	系統之漏洞修復應測試有效性及潛在影響，並定期更新
	 資料來源：[14]WSUS 圖90 WSUS 操作畫面 ▪ 系統管理者應確認作業系統等相關修正或更新程式對資通系統之影響，建立技術脆弱性資訊取得管道，評估可能帶來風險，以免貿然在正式環境套用修補程式或更新元件版本，可能因相容性問題而造成對系統服務運作產生預期外影響。例如，先於測試環境套用更新程式，確認不會對系統服務造成危害後，始於正式環境進行更新。惟當發生重大安全弱點，為爭取修補時效可能無法執行全面性測試，建議仍應測試主要功能流程未受影響後，再進行修補更新。
驗證實務	▪ 如未定期更新修復資通系統漏洞，未建立適當測試流程，則未符合此控制措施。 ▪ 驗證人員宜確認資通系統元件更新機制，如接收廠商釋出之最新修正與安全性改良，或依機關規定時程檢查元件版本更新。 ▪ 驗證人員宜訪談相關權責人員、檢視機關作業規定及檢閱系統變更紀錄與弱點修補報告等方式，驗證機關已具備適當之系統漏洞修復機制。
佐證資料	▪ 機關訂定之系統發展維護辦法

本文件之智慧財產權屬數位發展部資通安全署擁有。

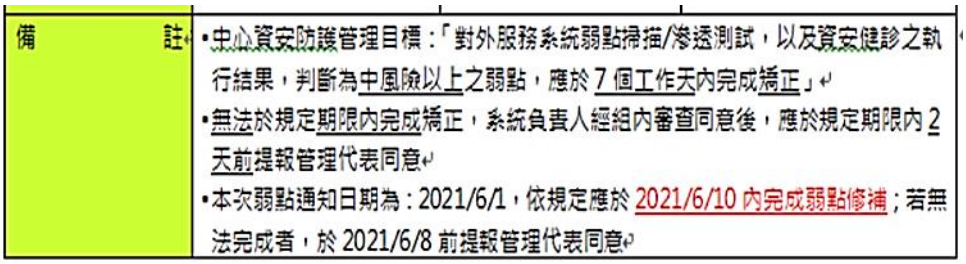
控制措施	系統之漏洞修復應測試有效性及潛在影響，並定期更新
	▪弱點掃描、滲透測試及源碼掃描等安全檢測報告與修補紀錄
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-2 漏洞修復) ▪安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-11 開發人員安全測試及評估)

資料來源：本計畫整理

2.7.1.2 定期確認資通系統相關漏洞修復之狀態

表72 漏洞修復控制措施 2

控制措施	定期確認資通系統相關漏洞修復之狀態
適用等級	中、高
內容說明	宜注意相安全漏洞訊息(如透過 CVE 相關訊息網站、廠商安全通告等)，若發現採用之軟體或元件具有安全漏洞，或是由弱點掃描等安全性檢測所檢出之系統漏洞，皆應設法修復並定期追蹤修復進度，並配合定期之安全性檢測確認複測。定期確認資通系統相關漏洞修復之狀態範例詳見圖 91。
驗證實務	▪如未定期確認已知資通系統漏洞修復進度，如雖執行弱點掃描卻未落實修補作業，則未符合此控制措施。



資料來源：本計畫整理

圖91 定期確認資通系統相關漏洞修復之狀態

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	定期確認資通系統相關漏洞修復之狀態
	▪驗證人員宜訪談相關權責人員、檢視機關作業規定及檢閱系統變更紀錄與弱點修補報告等方式，驗證是否已定期追蹤漏洞修復狀態。
佐證資料	▪機關訂定之系統發展維護辦法 ▪弱點掃描、滲透測試及源碼掃描等安全檢測報告 ▪弱點修補紀錄
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-2 漏洞修復) ▪安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-11 開發人員安全測試及評估)

資料來源：本計畫整理

2.7.2 資通系統監控

2.7.2.1 發現資通系統有被入侵跡象時，應通報機關特定人員

表73 資通系統監控控制措施 1

控制措施	發現資通系統有被入侵跡象時，應通報機關特定人員
適用等級	普、中、高
內容說明	應建立資通安全通報機制(如正式之通報程序及資安事件通報聯絡人等)，當發現資通系統遭不當存取、竄改、毀損等疑似入侵攻擊跡象時，可透過當面告知、電話、簡訊、電子郵件訊息等適當聯絡方式，通知相關人員進行適當處理，人員通知表列包含網路管理者、系統管理者、系統擁有者或各級資安人員等。監控通報作業規範範例詳見圖 92。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	發現資通系統有被入侵跡象時，應通報機關特定人員
	6.2 系統監看異常通報 由戰情室監控人員透過資安事件管理平台監控本中心資安設備事件日誌，包含網域主機、防火牆、入侵偵測系統及防毒系統等，若系統有異常事件發生，則依矯正及預防措施程序通報處理。 資料來源：本計畫整理 圖92 系統監控通報作業範例
驗證實務	▪如未建立可靠之系統入侵通報流程，則未符合此控制措施。 ▪驗證人員宜檢視機關作業規定或訪談相關權責人員，以了解是否建立通報應變機制。 ▪驗證人員宜確認通報管道之順暢，驗證相關人員聯絡資訊之正確性，以確保系統入侵警示可有效傳達給特定人員。
佐證資料	▪機關訂定之監控作業程序 ▪機關訂定之通報應變作業程序
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-4 資訊系統監視)

資料來源：本計畫整理

2.7.2.2 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

表74 資通系統監控控制措施 2

控制措施	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
適用等級	中、高

本文件之智慧財產權屬數位發展部資通安全署擁有。

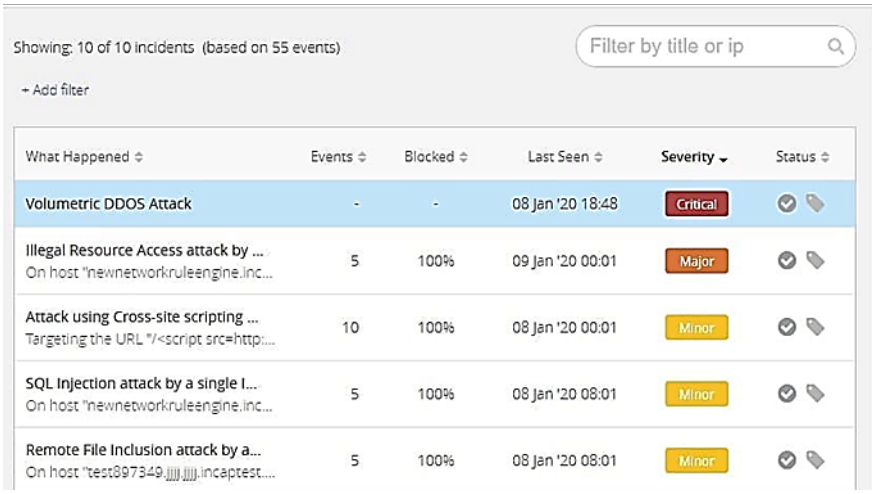
控制措施	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用
內容說明	資通系統之監控能力可透過各種工具與技術達成(如 WAF、IPS、IDS、惡意程式防護工具，日誌監控及網路監控軟體等)。系統連線監控工具使用範例詳見圖 93。  資料來源：本計畫整理 圖93 系統連線監控工具儀表板
驗證實務	▪如未建立資通系統監控機制，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員及檢視機關作業規定等方式，驗證已監控資通系統之連線行為，確認已具備必要偵測能力，可發現潛在惡意攻擊及未授權使用行為。
佐證資料	機關訂定之監控作業程序
參考文獻	▪安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-4 資訊系統監視)

資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

2.7.2.3 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

表75 資通系統監控控制措施 3

控制措施	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
適用等級	高
內容說明	應採用自動化工具，以支援近乎即時之事件分析。自動化工具包含基於主機、基於網路、基於傳輸，或基於儲存之事件監控工具或安全事件/資訊管理(SIEM)技術，提供即時分析警示或透過機關資通系統產生通知，如部署 IPS、IDS、WAF 及 UTM 防火牆等具備自動化監控能力之網路安全防護產品。以 WAF 偵測並分析資安事件範例詳見圖 94。  資料來源：本計畫整理 圖94 WAF 偵測並分析資安事件
驗證實務	▪如資通系統未採用自動化工具監控進出之通信流量，或無法進行異常事件分析，則未符合此控制措施。 ▪驗證人員宜訪談相關權責人員及檢視機關作業規定等方式，驗證機關已採用自動化工具監控進出之通信流量，並提供必要資訊供資安人員檢視與分析。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	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
佐證資料	▪機關訂定之監控作業程序 ▪資安事件分析紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-4 資訊系統監視)

資料來源：本計畫整理

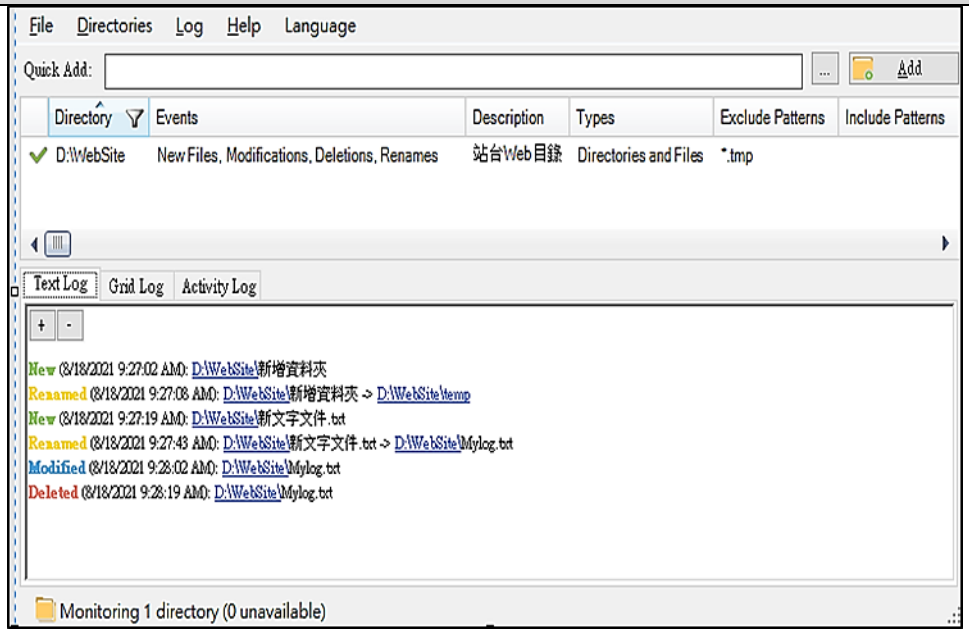
2.7.3 軟體及資訊完整性

2.7.3.1 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊

表76 軟體及資訊完整性控制措施 1

控制措施	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊
適用等級	中、高
內容說明	▪資通系統軟體及資訊，包含應用程式、網站重要目錄與組態設定檔等，皆是惡意攻擊者最喜愛目標，如植入惡意檔案或竄改網頁內容等手法，破壞資通系統完整性。應使用適當技術與工具，檢查重要軟體及資訊內容是否被惡意竄改。 ▪完整性檢查技術如使用密碼雜湊函數、同位元檢查及循環冗餘檢查等。亦可評估採用目錄檔案監控工具，可自動偵測應用程式與網站目錄或檔案之異動事件，當發現檔案異動時會留下相關日誌紀錄並提出示警。目錄檔案監控工具操作畫面範例詳見圖 95。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊
	 資料來源：本計畫整理 圖95 目錄檔案監控工具操作畫面範例
驗證實務	▪ 如未使用完整性驗證技術或工具，無法驗證資通系統軟體及資訊是否被惡意竄改，則未符合此控制措施。 ▪ 驗證人員宜檢視機關訂定之系統發展管理辦法，並訪談相關權責人員(如系統管理者與資安人員等)，以了解是否建立完整性檢查機制。機關可能透過即時偵測、定期進行雜湊值比對等方式，驗證內容是否遭到未授權之變更。
佐證資料	機關所使用之完整性驗證工具，如檔案雜湊值等
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-7 軟體、韌體及資訊之完整性)

資料來源：本計畫整理

2.7.3.2 使用者輸入資料合法性檢查應置放於資通系統伺服器端

本文件之智慧財產權屬數位發展部資通安全署擁有。

表77 軟體及資訊完整性控制措施 2

控制措施	使用者輸入資料合法性檢查應置放於資通系統伺服器端
適用等級	中、高

內容說明	▪ 資通系統應檢查使用者輸入之有效語法與語義(如字元集、長度、數值範圍及可接受值等)，驗證輸入匹配指定之定義格式及內容。若資通系統接受惡意攻擊者提供之輸入而構成不正確編碼之結構化訊息，則該攻擊者可能插入惡意命令或特殊字元，導致資料被解釋為控制資訊或中繼資料。因此，模組或元件接收受污染輸出將會執行錯誤操作，或無法正確地解釋資料。傳遞到解譯器前預審輸入資料，可防止內容無意地被解釋為命令。
	▪ 輸入驗證(Input Validation)有助於強化輸入資料之正確性與合法性(Valid)，並可抵禦 XSS 與各種注入式攻擊，建議實作方式如建立資訊輸入白名單等，指定已知可信賴來源資訊輸入與可接受格式，或是以黑名單過濾惡意資料。輸入驗證若僅於使用者端實作，容易被惡意攻擊者利用竄改 Cookie 或網路封包內容等手法繞過檢查機制，故應實作於伺服器端以確保輸入驗證機制之有效性。以.NET 資通系統為例，可透過啟用 ValidateRequest 設定，讓.NET 檢查所有網頁請求，由於檢查機制是實作於伺服器端，因此無法輕易繞過，當使用者端輸入與提交惡意字元(如「<」或「>」)時，ValidateRequest 會檢查並發出警示。另一個使用範例為利用正規表示法檢查輸入資料字元，範例詳見圖 96。範例中表示檢查所輸入欄位包含英文大小寫等字元最多達 40 個字元。
	`<%@ language="C#" %>`
	`<form id="form1" >`
	`<asp:TextBox ID="txtName" />`
	`<asp:Button ID="btnSubmit" Text="Submit" />`
	`<asp:RegularExpressionValidator ID="regexpName"`
	`ErrorMessage="This expression does not validate."`
	`ControlToValidate="txtName"`
	`ValidationExpression="^[a-zA-Z'.\s]{1,40}$" />`
	`</form>`
	資料來源：本計畫整理
	圖96 .NET 檢查資料合法性範例

驗證實務	▪ 如資通系統未於資通系統伺服器端實作使用者輸入資料合法性檢查，則未符合此控制措施。

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	使用者輸入資料合法性檢查應置放於資通系統伺服器端
	▪驗證人員宜訪談相關權責人員或透過檢視系統功能規格書，以了解資通系統如何實作輸入資料合法性檢查。從弱點掃描或滲透測試報告中亦可能觀察到輸入資料檢查機制缺失，如 Injection 與 XSS 等弱點成因通常與缺乏有效之輸入驗證有關。 ▪驗證人員可評估發展測試案例，以驗證檢查機制有效性，不可因使用者端檢查機制(如 JavaScript 檢查等)被停用，而被惡意攻擊者利用建置 OWASP Zed Attack Proxy (ZAP)或 Burp Suite 等代理伺服器(Proxy)輕易繞過檢查機制，或造成系統解析錯誤、損毀及產生資安弱點(如 Injection 與 XSS 等)。
佐證資料	▪系統功能規格書 ▪資通系統輸入合法性檢查之測試紀錄
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-10 資訊輸入的驗證)

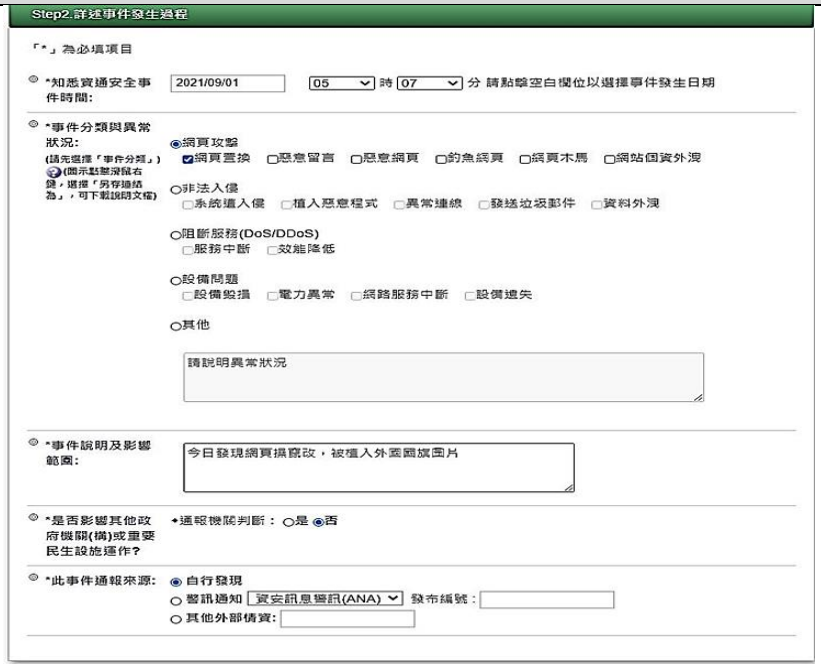
資料來源：本計畫整理

2.7.3.3 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

表78 軟體及資訊完整性控制措施 3

控制措施	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
適用等級	中、高
內容說明	當發現資通系統完整性遭受破壞，如當發現資料庫或檔案被不當竄改、網站頁面被惡意置換、被植入惡意指令碼或元件等資安事件時，應依照我國資安法規及機關資安政策規範採取適當行動，如進行事件通報、緊急應變與災後復原等相關安全保護措施。例如，當機關業務承辦人員發現系統被植入惡意內容，破壞系統完整性，依規定進行資安通報，國家資通安全通報應變網站操作範例詳見圖 97。

本文件之智慧財產權屬數位發展部資通安全署擁有。

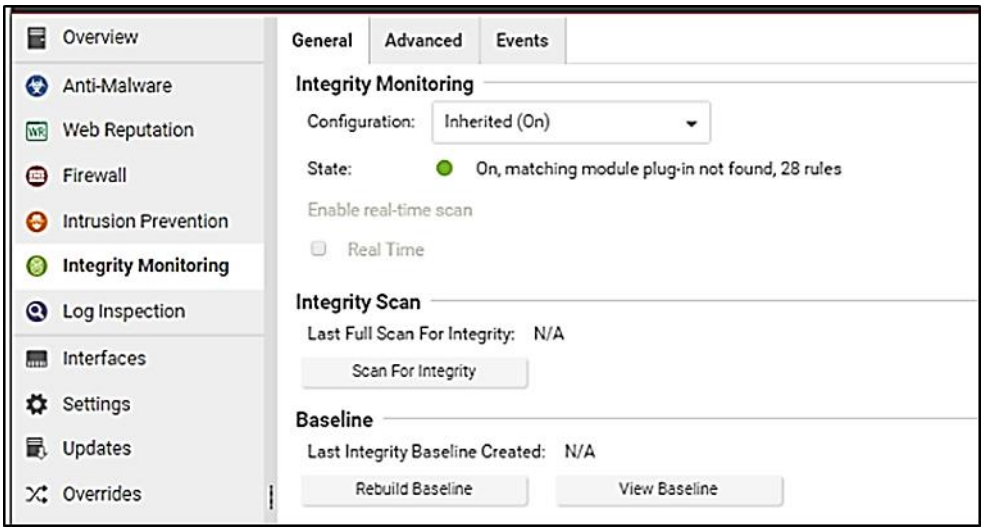
控制措施	發現違反完整性時，資通系統應實施機關指定之安全保護措施
	 資料來源：本計畫整理 圖97 進行資安通報範例
驗證實務	如資通系統完整性被破壞，卻未實施相關必要處理，則未符合此控制措施。驗證人員宜檢視機關資安政策與規範或訪談相關權責人員等方式，了解在發現資通系統完整性遭受破壞時之處置動作。
佐證資料	▪機關訂定之系統發展維護辦法 ▪機關訂定之通報應變作業程序 ▪機關訂定之監控作業程序
參考文獻	安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-7 軟體、韌體及資訊之完整性)

資料來源：本計畫整理

2.7.3.4 應定期執行軟體與資訊完整性檢查

本文件之智慧財產權屬數位發展部資通安全署擁有。

表79 軟體及資訊完整性控制措施 4

控制措施	應定期執行軟體與資訊完整性檢查
適用等級	高
內容說明	定期驗證軟體與資訊之完整性，以發現未經授權竄改行為，如透過即時偵測、進行雜湊值比對等方式，定期驗證內容是否遭到未授權之變更。實務上常先建立基準線(Baseline)，意即將軟體與資訊初始狀態記錄下來，作為後續在進行完整性驗證檢查時比對依據。目前市面上存在多款完整性監視與驗證軟體，除可即時偵測檔案目錄異動行為，亦支援完整性掃描動作，比對檔案現況與基準線之落差，完整性掃描操作範例詳見圖 98。  資料來源：本計畫整理 圖98 目錄檔案監控工具操作畫面範例
驗證實務	▪ 如未定期執行軟體與資訊完整性檢查，則未符合此控制措施。 ▪ 驗證人員宜檢視機關資安政策與規範或訪談相關權責人員，以了解執行軟體與資訊完整性檢查之方式與週期，並檢視完整性檢查執行紀錄與成果，確認檢查機制之有效性。
佐證資料	▪ 機關訂定之系統發展維護辦法 ▪ 完整性檢查執行紀錄

本文件之智慧財產權屬數位發展部資通安全署擁有。

控制措施	應定期執行軟體與資訊完整性檢查
參考文獻	▪ 安全控制措施參考指引(修訂)(V2.0)_附件 20-系統與資訊完整性 System and Information Integrity (控制措施編號 SI-7 軟體、韌體及資訊之完整性) ▪ 安全控制措施參考指引(修訂)(V2.0)_附件 18-系統與服務獲得 System and Services Acquisition (控制措施編號 SA-10 開發人員組態管理)

資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

3. 結論

依分級辦法第十一條規定，各機關自行或委外開發之資通系統，應依附表十所定資通系統防護基準執行控制措施。本文件旨在協助政府機關確認資通系統防護措施是否符合資通系統防護基準之規定，惟不同資通系統因架構設計、技術及使用需求等差異，難以完全適用所有資通系統類型，宜以整體資安風險為考量，評估所施行安全控制措施之有效性與適切性。附件為資通系統防護基準檢核表提供機關參考使用，其中除提供檢核表，亦設計 3 個資通系統自評範例，可參考其中內容自行發展符合機關需求之檢核表，提供系統承辦人員檢查系統防護現況，各範例系統說明詳見表 80。

表80 附件系統範例說明

系統名稱	系統等級	填答問項	系統說明
範例系統 1	普	35 項	自行開發之公開網站，服務對象為一般民眾，無提供會員註冊登入功能，僅作網頁資料呈現。系統管理者仍需以帳號密碼登入系統後臺進行維護管理作業。未啟用 HTTPS 加密保護，亦未設定客製化錯誤頁面。
範例系統 2	中	58 項	委外開發之內部使用資通系統，服務對象為機關內部同仁，需通過 AD 認證。
範例系統 3	高	78 項	自行開發之對外服務資通系統，需使用自然人憑證登入，雖全站台啟用 HTTPS，惟仍使用安全強度不足之 TLS1.1 傳輸協定。

資料來源：本計畫整理

本文件之智慧財產權屬數位發展部資通安全署擁有。

4. 參考文獻

[1]資通安全責任等級分級辦法

[2]安全控制措施參考指引(修訂)(V4.0)。https://www.nccst.nat.gov.tw/

[3]使用雜湊程式碼確定資料完整性。微軟。https://docs.microsoft.com/

[4]電腦機房異地備援機制參考指引(V1.0)。https://www.nccst.nat.gov.tw/

[5]Wireshark, www.wireshark.org

[6]資通系統委外開發RFP資安需求範本(V3.0)。https://www.nccst.nat.gov.tw/

[7]Capturing Security Requirements through Misuse Cases, Sindre and Opdahl

[8]Threat Modeling, www.microsoft.com

[9]OWASP Web Security Testing Guide, https://owasp.org/

[10]RFC8996, https://datatracker.ietf.org/doc/html/rfc8996

[11]OWASP 源碼檢測工具列表。
https://owasp.org/www-community/Source_Code_Analysis_Tools

[12]滲透測試服務 RFP 範本(V5.0)。https://www.nccst.nat.gov.tw/

[13]Nmap, https://nmap.org/

[14]WSUS, https://docs.microsoft.com

本文件之智慧財產權屬數位發展部資通安全署擁有。

5. 附件

附件 1 資通系統防護基準檢核表

本文件之智慧財產權屬數位發展部資通安全署擁有。