BCCS 漢昕科技

資安整備專家

高雄市政府教育局資訊安全管理系統維運及驗證輔導服務案資通系統防護基準及委外監督教育訓練

陳俊茂

漢昕科技股份有限公司

2026/5/5

大綱

- 資通安全責任等級分級辦法簡介
- 資通系統盤點與安全等級評估
- 資通系統防護基準驗證實務
- 委外監督管理

BCCS 漢昕科技

資安整備專家

資通安全責任等級分級辦法簡介

資通安全管理法與子法

- 資通安全管理法
  - 資通安全管理法施行細則
  - 資通安全責任等級分級辦法
    - 附表九　資通系統防護需求分級原則
    - 附表十　資通系統防護基準
  - 資通安全情資分享辦法
  - 資通安全事件通報及應變辦法
  - 特定非公務機關資通安全維護計畫實施情形稽核辦法
  - 公務機關所屬人員資通安全事項懲戒辦法

最新修正：115年1月7日

資通安全責任等級分級辦法

- 資通安全責任等級
  - 公務機關及特定非公務機關
  - A、B、C、D、E

公務機關

- 中央與地方機關（構）
- 公法人

特定非公務機關

- 關鍵基礎設施提供者（如台電）
- 公營事業（如台電）
- 政府捐助之財團法人（如工研院）

附表	內容
附表一~附表八	詳列A級~E級公務及特定非公務機關之應辦事項
附表九	• 各機關自行或委外開發之資通系統應完成資通系統分級 • 普、中、高
附表十	資通系統防護基準-依系統分級實作安全控制措施

資通安全責任等級分級辦法

用詞說明

名詞	說明	出處
資通系統	指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統	資通安全管理法第一章總則第3條
核心資通系統	• 支持核心業務持續運作必要之系統 • 依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者	資通安全管理法施行細則第7條
自行或委外開發之資通系統	各機關自行或委外開發資通系統應依附表九所定資通系統防護需求分級原則完成資系統分級，並依附表十所定資通系統防護基準執行控制措施	資通安全責任等級分級辦法第11條

應辦事項要求

資通安全責任等級	機關屬性	辦理內容
A	• 公務機關 • 特定非公務機關	• 針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。 • 應於初次受核定或等級變更後之一年內完成；資通系統新增、系統分級變更或其適用防護基準有異動情形時，亦同。
B	• 公務機關 • 特定非公務機關	
C	• 公務機關 • 特定非公務機關	• 針對自行或委外開發之資通系統，依附表九完成資通系統分級。其後應每年至少檢視一次資通系統分級妥適性。 • 應於初次受核定或等級變更後之一年內依附表九完成分級，並於二年內完成附表十控制措施；資通系統新增、系統分級變更或其適用防護基準有異動情形時，亦同。
D	各機關	無相關要求
E		

附表九 資通系統防護需求分級原則

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

資通系統之防護基準等級，以任一構面之防護需求等級之最高者定之

風險評估構面

- 機密性(Confidentiality)
  - 造成未經授權之資訊揭露
  - 如資料庫資料被竊取、網站不當洩漏民眾個資等
- 完整性(Integrity)
  - 造成資訊錯誤或遭竄改等情事
  - 如網站首頁被惡意置換、系統遭植入惡意檔案等
- 可用性(Availability)
  - 造成對資訊、資通系統之存取或使用之中斷
  - 如阻斷式服務攻擊(DoS)、軟硬體毀損等
- 法律遵循性(Compliance)
  - 未確實遵循資通系統設置或運作涉及之資通安全相關法令
  - 如未實作資通系統防護基準控制措施等

附表十 資通系統防護基準

存取控制	事件日誌與可歸責性	營運持續計畫	識別與鑑別
• 帳號管理 • 最小權限 • 遠端存取	• 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	• 資料備份 • 系統備援	• 使用者之識別與鑑別 • 身分驗證管理 • 鑑別資訊保護

系統與服務獲得	系統與通訊保護	系統與資訊完整性
• 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	• 傳輸之機密性與完整性 • 資料儲存之安全	• 漏洞修復 • 資通系統監控 • 軟體及資訊完整性

系統防護需求等級

高	• 78→80項防護需求
中	• 58→61項防護需求
普	• 35→44項防護需求

附表十 資通系統防護基準範例

附表十 資通系統防護基準

系統防護需求分級 / 控制措施		高	中	普
構面	控制措施			
存取控制	帳號管理	一、應依機關規定之情況及條件，使用資通系統。 二、監控資通系統帳號，如發現帳號違常使用時，回報管理者。 三、等級「中」之所有控制措施。	一、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。 二、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。 三、等級「普」之所有控制措施。	一、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。 二、已逾期之臨時或緊急帳號應刪除或禁用。 三、資通系統閒置帳號應禁用。 四、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。
	最小權限	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。		
		一、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		

小分類

大分類

向下相容

BCCS 漢昕科技

資安整備專家

資通系統盤點與安全等級評估

資通系統分級

- 依據「資通安全責任等級分級辦法」附表九資通系統防護需求分級原則，辦理資通系統分級。

資通系統

- 資通系統
  - 自行開發
  - 委外開發
  - 可以設定與管控權限
- 例如
  - 系統、網站（頁）、平台、資料庫、AD、電子郵件系統（〇）
  - Windows作業系統、防毒軟體、個人電腦軟體、印表機軟體（X）

資通系統安全等級評估表

「高雄市教育局〇〇系統」資通系統安全等級評估表				
機密等級：□公開使用 ■內部使用 □限制使用 □高度限制使用				
文件編號：				版次1.2
紀錄編號：				填表日期：115年 月 日
功能說明：				
業務屬性：□行政類 ■業務類				
影響構面				資通系統安全等級
1.機密性	2.完整性	3.可用性	4.法律遵循性	

資通系統安全等級評估表

步驟1：設定影響構面等級			
影響構面		安全等級	原因說明
1.機密性	初估		新建置系統首次評估，既有系統填寫上次評估內容
	異動		系統變更以致影響資安風險或防護需求時，請填寫此項
2.完整性	初估		
	異動		
3.可用性	初估		
	異動		
4.法律遵循性	初估		
	異動		

原因說明及安全等級請參考資通安全責任等級分級辦法附表九 資通安全防護需求分級原則

資通系統防護需求分級原則

1.機密性

普	中	高
（等級1） 對1種類人造成1種影響	（等級2） 對2種類人造成2種影響	（等級3） 對3種類人造成3種影響
系統中保有[何種資料]，如未經授權的資訊揭露，或資料外洩，可能對[本單位、學校、使用者、老師、學生]的[業務運作、資產或名譽]等方面造成輕微的影響，或不影響	系統中保有[何種資料]，如未經授權的資訊揭露，或資料外洩，可能對[本單位、學校、使用者、老師、學生]的[業務運作、資產或名譽]等方面造成嚴重的影響	系統中保有[何種資料]，如未經授權的資訊揭露，或資料外洩，可能對[本單位、學校、使用者、老師、學生]的[業務運作、資產或名譽]等方面造成災難性的影響

資通系統防護需求分級原則

- 1.機密性(舉例)

系統保有何種資料，若外洩造成的誰的何種權益受損，如名譽或財產

系統中保有學生與老師的資料，包含姓名、電話、住址，但有經過去識別化，如未經授權的資訊揭露，或資料外洩，可能對老師與學生的名譽方面造成輕微的影響，或不影響；但對本單位或學校的名譽可能產生輕微的影響

資通系統防護需求分級原則

2.完整性

普	中	高
（等級1） 對1種類人造成1種影響	（等級2） 對2種類人造成2種影響	（等級3） 對3種類人造成3種影響
系統中保有**[何種資料]**，未經授權的資料若遭竄改，造成系統資料錯誤，可能對**[本單位、學校、使用者老師、學生]**的**[業務運作、資產或名譽]**等方面造成輕微的影響，或不影響	系統中保有**[何種資料]**，未經授權的資料若遭竄改，造成系統資料錯誤可能對**[本單位、學校、使用者、老師、學生]**的**[業務運作、資產或名譽]**等方面造成嚴重的影響	系統中保有**[何種資料]**，未經授權的資料若遭竄改造成系統資料錯誤，可能對**[本單位、學校、使用者、老師、學生]**的**[業務運作、資產或名譽]**等方面造成災難性的影響

資通系統防護需求分級原則

- 2.完整性(舉例)

系統資料遭到竄改，造成何種影響，如業務中斷

系統中保有學生與老師的資料，包含姓名、電話、住址，未經授權的資料若遭竄改，造成系統資料錯誤，可能對本單位的業務產生部分影響，需要手動更正，連到造成其他系統資料帶入錯誤，影響嚴重。

資通系統防護需求分級原則

3.可用性

普	中	高
（等級1）	（等級2）	（等級3）
系統中保有**[何種資料]**，如有資訊、資訊系統之存取或使用上的中斷，可能對**[本單位、學校、使用者、老師、學生]**的**[業務運作、資產或名譽]**等方面造成輕微的影響，或不影響	系統中保有**[何種資料]**，如有資訊、資訊系統之存取或使用上的中斷，可能對**[本單位、學校、使用者、老師、學生]**的**[業務運作、資產或名譽]**等方面造成嚴重的影響	系統中保有**[何種資料]**，如有資訊、資訊系統之存取或使用上的中斷，可能對**[本單位、學校、使用者、老師、學生]**的**[業務運作、資產或名譽]**等方面造成災難性的影響

資通系統防護需求分級原則

- 3.可用性(舉例)

系統發生中斷將會造成何種影響或結果

系統中保有學生與老師的資料，包含姓名、電話、住址，如有資訊、資訊系統之存取或使用上的中斷，可能對本單位以及使用者的業務運作明顯產生影響，屬於嚴重影響

資通系統防護需求分級原則

4.法律遵循性

普 （等級1）	中 （等級2）	高 （等級3）
其他資通系統設置或運作於法令有相關規範之情形。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。

資通系統防護需求分級原則

- 4.法律遵循性(舉例)

系統設置依照何種法規設置，如未依照法規設置將會造成什麼結果

本系統之設置或運作如未依照資通安全責任等級分級辦法之資通系統防護基準規定辦理，將可能使得ＯＯ系統發生未經授權存取

普：導致系統發生資安事件。

中：影響組織內外人員執行業務之公正性及正當性，並使相關人員受行政罰、懲戒或懲處。

資通系統安全等級評估表

步驟2：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	行政類：一般行政業務相關系統，如人事差勤 業務類：本單位專屬業務相關系統，如學籍系統	
	異動		

步驟3：業務衝擊分析

項目			時間(小時)	原因說明
目標回復時間： 系統恢復正常作業的目標時間	RTO	初估		
		異動		
目標回復時點： 能容忍的最大資料遺失時間長度	RPO	初估		
		異動		
最大可容忍中斷時間： 業務能停擺的極限時間	MTPD	初估		
		異動		

業務衝擊分析

- MTPD 是「最大可容忍中斷時間」，指業務能停擺的極限時間。
- RTO 為「復原時間目標」，指系統恢復正常作業的時間。
- RPO 為「資料復原點目標」，指能容忍的最高資料遺失量。
- 三者原則為：RTO < MTPD，且 RPO 決定備份頻率。

BCCS 漢昕科技

資安整備專家

資通系統防護基準驗證實務

構面1 存取控制

帳號管理

- 建立帳號管理機制
- 臨時與緊急帳號管理
- 閒置帳號管理
- 帳號定期審查
- 系統操作限制
- 帳號自動登出
- 系統使用規定
- 系統帳號監控

最小權限

- 最小權限原則

遠端存取

- 遠端存取授權
- 權限檢查實作
- 連線監控
- 連線加密
- 來源管制

帳號管理－建立帳號管理機制

- 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（普中高）
  - 系統帳號如應用程式、作業系統及資料庫等帳號，不可由系統管理者任意調整異動，應符合「KH-EB-B-008存取控制管理程序書」，並經權責人員簽核後始可進行作業。
    - ➢ 如填寫紙本申請單流程（如：系統帳號／權限異動申請等），或利用系統線上申請審核流程來完成。
  - 整備重點：宜完善帳號管理機制

帳號管理—臨時與緊急帳號管理

- 已逾時之臨時或緊急帳號應刪除或禁用（普中高）
  - 臨時或緊急帳號可能為暫時性業務需求而開立，惟若已無繼續使用需求則應停止使用，以減少帳戶盜用風險
  - 機關可能定期以人工帳號清查，設計系統自動刪除／禁用逾期帳號
  - 整備重點：
    - ➢確認臨時或緊急帳號之定義與管理作為

帳號管理－閒置帳號管理

- 資通系統閒置帳號應禁用(普中高)
  - 閒置帳號係指久未登入的帳號
  - 常見原因如未移除已調、離（退）職人員之帳號權限等
  - 實務上可針對不同之資通系統與帳號類型定義不同期限
  - 整備重點：
    - ➢確認閒置權限之定義（如30天未登入等）
    - ➢確認管理作為（如定其人工帳號清查、或利用系統排程自動禁用等）

帳號管理—帳號定期審核

- 定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除（普中高）
  - 定期人工審核帳號異動紀錄，包含應用程式、作業系統及資料庫等系統相關元件之使用者帳號，以發現未經授權的帳號變更行為
  - 整備重點：完備稽核證據，如帳號審查紀錄等

	A	B
1		範例系統-AP帳號權限審查紀錄
2	系統名稱：	範例系統
3	OS管理員：	王小明
4	AP管理員：	張三
5	DB管理員：	李四
6	審查區間：	2021/1/1~2021/4/30
7	AP帳號管理員簽章：	
8	AP帳號管理員組長簽章：	
9		

帳號管理－系統操作限制

- 機關應定各系統之閒置時間或可使用期限與資通系統之情況及條件（中高）
  - 資通系統應考量系統使用需求及資安風險，訂定相關使用條件：操作閒置期限、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，例如：
    - 閒置時間設定：系統操作閒置期限15分鐘
    - 適用對象及網段：內部系統僅內部使用者利用AD帳號登入，並限制帳號來源IP位址： 10.0.2.1~ 10.0.2.250。
    - 存取權限：資通系統後臺僅限管理者帳號以本機(127.0.0.1)存取管理頁面
  - 整備重點：宜確認所定義之系統使用條件與限制

帳號管理—帳號自動登出

- 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（中高）
  - 系統應設定自動將閒置使用者登出之功能
    - ➢以ASP.NET站台為例
      - ◆組態設定值預設閒置期限為20分鐘
      - ◆也可透過程式碼設定
  - 或依資通系統使用需求訂定帳號使用時間限制
    - ➢如限制僅允許上班時間登入，或每次登入的操作時間上限等
  - 整備重點：宜確認系統已實作自動登出功能
    - ➢如檢視組態檔設定值或程式碼等
    - ➢發展測試案例實地測試

帳號管理－系統使用規定

- **應依機關規定之情況及條件，使用資通系統（高）**
  - 整備重點：確認沒有任何帳號違規使用之行為
  - 舉例：規範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
    - ➢測試遠端連線至資通系統後臺，是否有禁止存取

帳號管理－系統帳號監控

- 監控資通系統帳號，如發現帳號違常使用時回報管理者（高）
  - 帳號違常使用泛指有違日常行為模式之行為，例如：
    - 在異常時間登入資通系統
    - 未依其業務需求大量存取敏感性資料
    - 帳戶破解、越權存取等惡意行為
  - 監控資通系統帳號，如利用WAF等資安防護設備、SOC監控服務，或實作系統異常處理機制等
  - 當發現如帳號破解、越權存取等違規使用行為，向管理者告警通知， 如顯示警示畫面、寄送信件或簡訊等
  - 整備重點：確認已具備帳號監控與異常回報機制

最小權限－最小權限原則

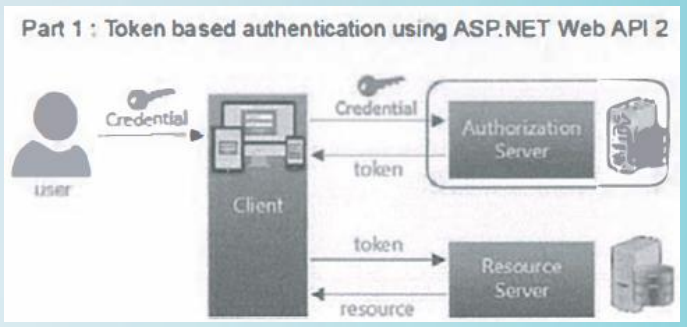
- **採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取（普中高）**
  - 授權決策採用最小權限原則，確保使用者或程序運行的權限等級不高於完成業務功能之所需
  - 實務上常區別特權帳號、內部使用者、非內部使用者等，限制存取授權範圍內之系統資源（如資料庫、檔案、功能頁面等）
  - 可透過定期帳號權限清查，審核帳號使用者與其權限是否滿足其業務所需之最小權限
  - 整備重點：宜檢視（包含但不限於）
    - ➢特權帳號之發放
    - ➢使用者或程序運行之存取權限
    - ➢資通系統任何與使用權限相關設定

遠端存取－遠端存取授權

- **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（普中高）**
  - 遠端存取是使用者（或程序）透過外部網路通訊存取資通系統的行為
    - ➢如透過Internet連線至機關對外服務站台，或以VPN連線至系統管理後臺等
  - 應通過權限檢查後始能存取系統資源，例如：
    - ➢站台除公開頁面外，使用者需完成登入並取得授權後才能操作系統
  - 建立使用限制、組態需求、連線需求以進行連線過程的安全控管，將這些資訊文件化則有助於使用者遵循以及提供稽核證據
  - 整備重點：宜檢視資通系統授權機制之有效性

遠端存取－權限檢查實作

- 使用者之權限檢查作業應於伺服器端完成（普中高）
  - 於伺服器端授權舉例：
    - ➢採用認證伺服器驗證使用者權限



  - 權限檢查常見缺陷為
    - ➢僅依賴使用者端的驗證程式（如JavaScript、Mobile APP等）或是瀏覽器Cookie設定值（如role="admin"等），容易被惡意竄改驗證資訊而繞過檢查機制或進行提權攻擊
    - ➢未檢查使用者權限，僅依賴隱藏頁面入口區分存取權限，容易被猜測或惡意破解功能路徑
  - 整備重點：宜檢視系統授權實作方式或發展測試案例

遠端存取－連線監控

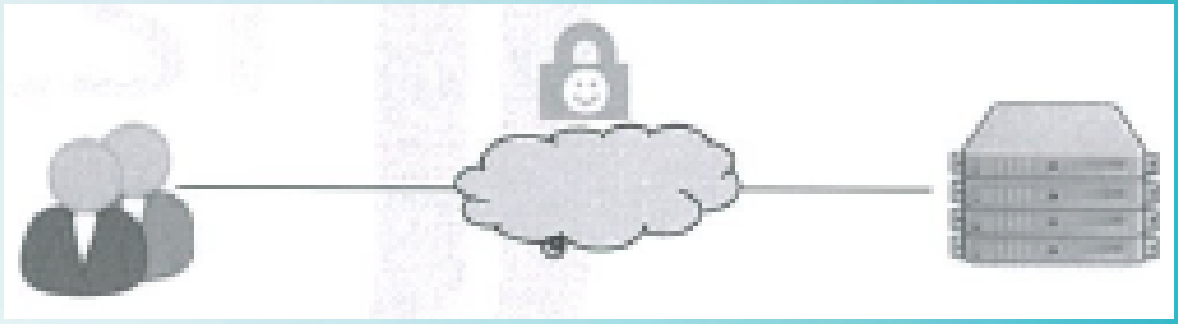
- 應監控遠端存取機關內部網段或資通系統後臺之連線（普中高）
  - 以VPN等技術遠端存取機關內部網段或資通系統後臺皆屬於高風險連線行為，故應進行監控以及時發現異常連線或惡意攻擊
  - 如部署網路安全設備（如WAF及IPS/IDS等）或使用SOC監控服務等
  - 整備重點：確認資通系統後臺監控機制，被納入監控範圍

遠端存取－加密機制

- 應採用加密機制（普中高）
  - 遠端存取資通系統時，應以加密機制保護機敏資料傳輸時之機密性。
  - 常見作法如採用HTTPS加密傳輸等，並選擇高強度之協定版本及演算法。
  - 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
  - 整備重點：檢視機關訂定之資通系統相關規範及系統設定，以確認資通系統所使用之遠端存取連線加密機制。

遠端存取－來源管制

- **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（普中高）**
  - 為避免全面性開放存取，系統可限制遠端存取來源以降低攻擊風險，如以白名單限定來源端位址或網段等
  - 例如，駐外單位欲存取內部系統，僅開放特定之來源IP存取
  - 整備重點：
    檢視相關存取控制設定，如系統組態設定檔案或防火牆規則等
    測試案例可模擬未符合規範之連線行為，如使用任意或未經許可之來源IP存取系統，系統應拒絕存取



構面2:事件日誌與可歸責性

記錄事件

- 日誌留存
- 事件記錄
- 管理者行為記錄
- 日誌審查

日誌紀錄內容

- 內容與格式

日置儲存容量

- 容量配置

日誌處理失效之回應

- 回應行動
- 即時通報

時戳及校時

- 時戳
- 校時

日誌資料之保護

- 存取控制
- 完整性
- 備份

記錄事件－日誌留存

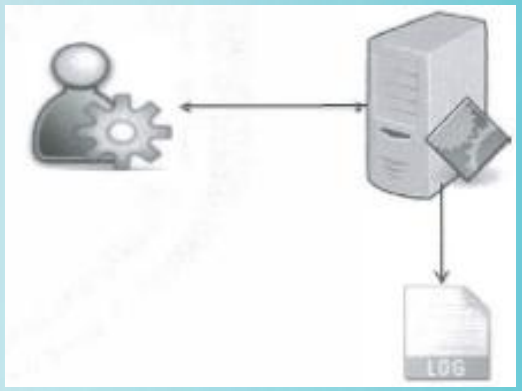
- **訂定日誌之記錄時間週期及留存政策，並保留日誌至少6個月（普中高）**
  - 應留存資通系統日誌(Logs)，如作業系統日誌(OS event log)、網站日誌(Web log)、應用程式日誌(AP log)及登入日誌(logon log)等，以符合程式除錯、行為歸責、稽核取證及法律規範等用途。
  - 日誌至少保留6個月
  - 整備重點：
    - ➢完備資通系統日誌，如作業系統日誌(OS event log)、網站日誌(Web log)、應用程式日誌(AP log)及登入日誌(logon log)等
    - ➢確認可檢視6個月內之日誌

記錄事件－事件記錄

- **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（普中高）**
  - 資通系統應具備Log機制，如針對身分驗證失敗、存取資源失敗、重要行為或資料異動、功能錯誤及管理者行為等
  - 但仍應避免留存冗雜訊息造成系統效能下降或儲存空間浪費
  - 整備重點：
    - ➢確認資通系統已啟用日誌記錄功能，可有效產出日誌
    - ➢確認日誌內容，包含重要之資通系統事件
    - ➢或發展測試案例，如模擬觸發特定事件之行為，如帳戶登入失敗，檢視對應日誌

記錄事件－管理者行為記錄

- 應記錄資通系統管理者帳號所執行之各項功能（普中高）
  - 資通系統應記錄管理者行為，有助於追查資安事件或發現濫權行為
  - 整備重點：
    - ➢確認管理者執行的重大功能相關日誌內容
      - ◆包含但不限於：帳號異動、系統功能設定變更、敏感性資料存取等
    - ➢或發展測試案例，如以管理者權限新增一筆帳號，檢視是否產生對應之日誌



記錄事件－日誌審查

- 應定期審查機關所保留資通系統產生之日誌（中高）
  - 機關應定期（如每季）審查日誌，檢視日誌內容以掌握是否在期間內曾發生重要的資安事件，如異常的存取行為、重大的系統錯誤等， 並將報告發現之問題提交予指定之人員處理
  - 可以人工定期檢視或透過日誌分析管理工具輔助
  - 整備重點：檢視定期審查日誌之相關紀錄

日誌紀錄內容－內容與格式(1/2)

- **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（普中高）**
  - 日誌內容為確保資安事件已充分描述，宜加入「人事時地物」等資訊
  - 為強化日誌可讀性，同一套日誌記錄系統（例如應用程式）應使用單一日誌機制（不應同時混用2種Logger)，產出Log格式應具一致性
    - ➢如Java應用程式不應同時使用log4J 與Java util logger等
  - 日誌內容應依法律、政策或業務等需求，納入任何必要資訊，如憑證資訊、日誌層級、系統介接資訊等
  - 整備重點：確認日誌內容與格式，並確認系統所使用的Logger

日誌紀錄與內容－內容與格式(2/2)

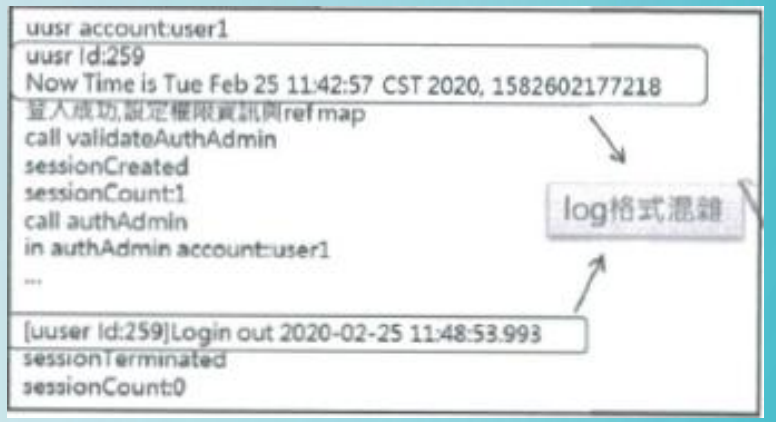
範例1：log留存於資料庫

內容格式受限

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	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

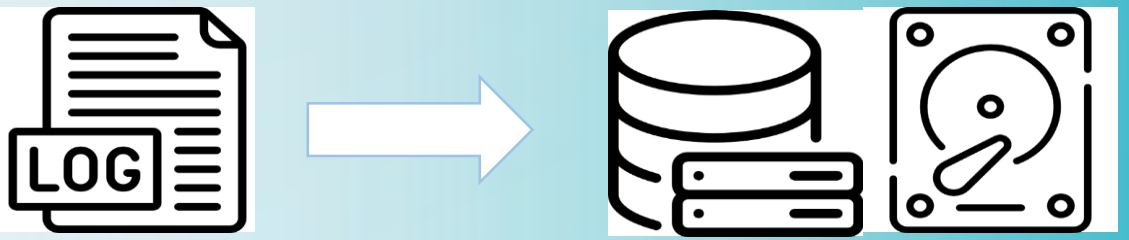
範例2：留存於檔案



五、應建置留存個人資料使用稽核軌跡（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

日誌儲存容量－容量配置

- 依據日誌儲存需求，配置所需之儲存容量（普中高）
  - 機關應計算及評估日誌之儲存空間使用量及成長速度，配置足夠硬碟或資料庫空間，減少因容量不足所造成的潛在損失或降低日誌記錄能力之發生率，舉例：
    - ➢日誌留存於檔案，存放於硬碟，儲存可用容量為60GB ，評估符合保存6個月之要求
    - ➢日誌留存於資料庫，定期備份至磁帶，並設定資料庫空間使用率警示，避免儲存容量不足情況發生
  - 整備重點：檢視日誌容量管理



日誌處理失效之回應－回應行動

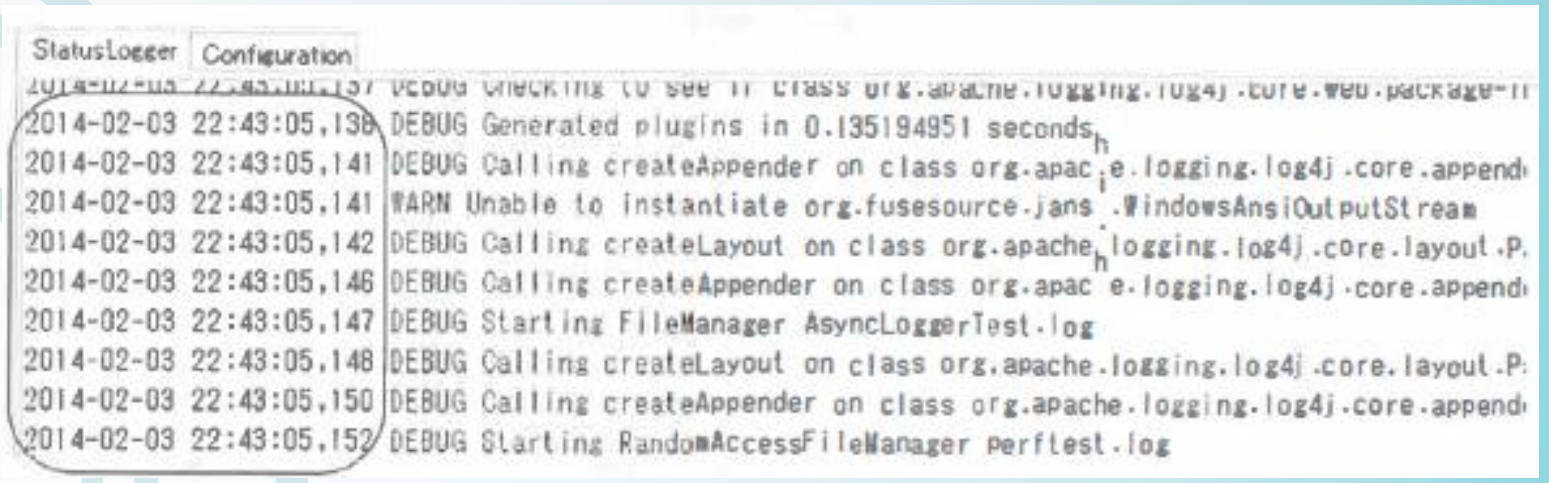
- 資通系統於日誌處理失效時，應採取適當之行動（普中高）
  - 失效原因，例如硬碟空間不足、資料庫連線中斷、系統功能異常等造成無法正常產生或留存日誌
  - 為避免危害系統可用性應評估相應之處理措施，例如（但不限於）：
    - ➢於系統畫面顯示警示訊息
    - ➢覆寫最舊的日誌（惟仍須確保符合日誌保留6個月以上之規定）
    - ➢以信件、簡訊或其他方式警示機關特定的人員或角色
  - 整備重點：考量日誌處理失效狀況及相應作為

日誌處理失效之回應－即時通報

- **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（高）**
  - 機關應定義需要即時通報之特定日誌處理失效事件、即時通報時效、特定通知對象及通知方式
  - 實作方式如當日誌伺服器因無法連線而無法寫入Log時，資通系統自動寄發通知信件或簡訊給系統管理者等
  - 整備重點：
    - ➢確認需要即時通報之日誌處理失效事件
    - ➢確認警告方式及對象

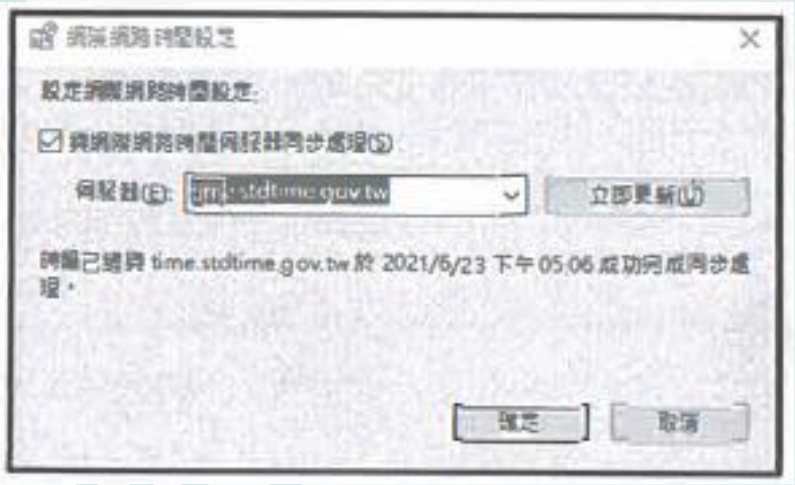
時戳及校時－時戳

- 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)（普中高）
  - LOG時戳格式應轉換成UTC或GMT格式，以利進行LOG分析，如設定台灣時區為UTC+8或GMT+8
  - 整備重點：確認時戳產生方式以及時間正確性



時戳及校時－校時

- 系統內部時鐘應定期與基準時間源進行同步（普中高）
  - 資通系統應定期完成時間同步作業，確保LOG內使用精確時間，有助於建立資安事件時間軸，加速資安事件追蹤作業
  - 整備重點：確認校時伺服器設定值之有效性

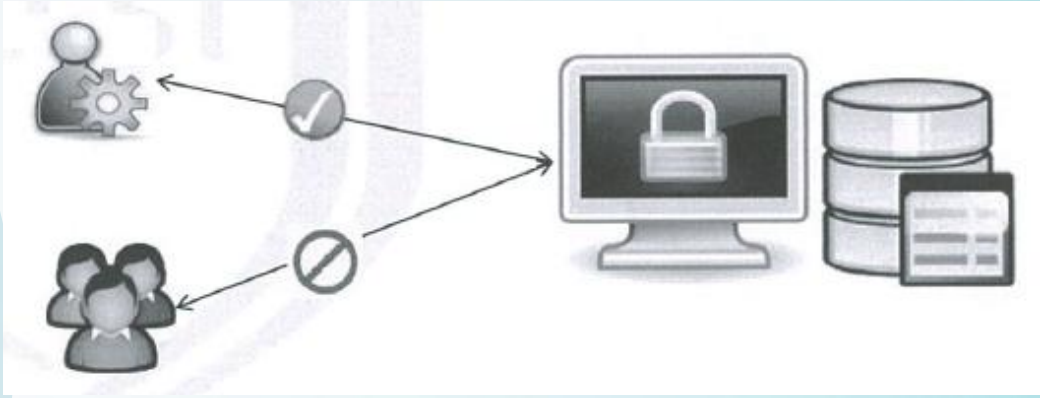


同步成功

任務上可能因防火牆阻擋或是錯誤的伺服器位址而同步失敗

日誌資訊之保護－存取控制

- 對日誌之存取管理， 僅限於有權限之使用者（普中高）
  - 系統日誌不可直接呈現於公開網頁供任意使用者檢視
  - 僅限已授權之權責人員（如系統或資料庫管理者等）存取日誌（如日誌檔案、資料庫或日誌伺服器等）
    - ➢日誌備份亦須納入存取控制保護
  - 整備重點：確認日誌授權存取對象



日誌資訊之保護－完整性

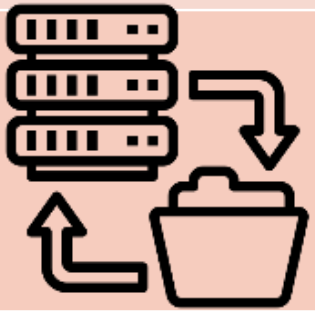
- 應運用雜湊或其他適當方式之完整性確保機制（中高）
  - 任何可有效防止或驗證日誌內容被竄改的機制，包含但不限於：
    - ➢將一筆日誌寫入資料庫時一併留存Log雜湊值
    - ➢留存日誌檔案雜湊值
    - ➢加密日誌
    - ➢使用目錄即時監控工具
    - ➢使用日誌分析管理工具之保護技術

- 整備重點：檢視機關實作日誌完整性，確保機制之有效性

日誌資訊之保護－備份

- 定期備份日誌至原系統外之其他實體系統（高）
  - 應定期執行日誌備份，並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或NAS等，或是利用磁碟與磁帶等儲存媒體存放備份資料
  - 整備重點：檢視機關日誌備份規範與執行情形

構面3：營運持續計畫



系統備份

- 復原點目標
- 系統源碼與資料備份
- 測試備份媒體
- 還原測試
- 異地備份

系統備援

- 復原時間目標
- 備援設備

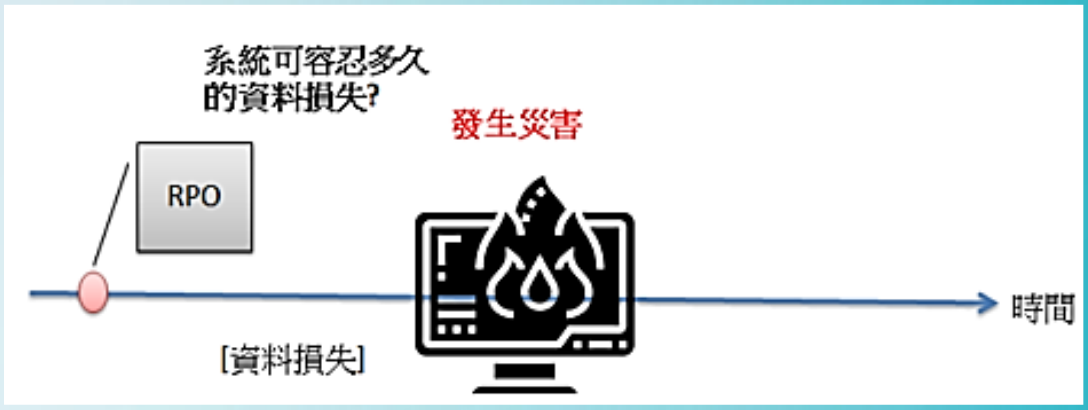
應辦事項要求

- （管理面）營運持續運作演練

資通安全責任等級	機關屬性	辦理內容
A	• 公務機關 • 特定非公務機關	全部核心資通系統每年辦理一次
B	• 公務機關 • 特定非公務機關	全部核心資通系統每二年辦理一次
C		
D	各機關	無需求
E		

系統備份－復原點目標(RPO)

- 訂定系統可容忍資料損失之時間要求（普中高）
  - 訂定復原點目標(Recovery Point Objective, RPO)
    - ➢當發生資料損失時，可使用最接近的備份資料進行復原
    - ➢資料備份頻率應滿足系統可容忍資料損失時間之要求
    - ➢例如若RPO訂定為1小時，則至少每小時備份資料一次
  - 整備重點：檢視機關RPO定義與執行情形



資料備份－資料備份

- 執行資料備份（普中高）
  - 機關應備份系統重要資料（如系統業務資料、組態設定等），不宜全數交由廠商管理保存，避免委外廠商倒閉或更換後無法維護系統之情形
    - ➢備份作業時機如廠商交付、內容變更時，或定期備份
  - 實務上如建置建構管理區集中存放，或使用版本控制系統（如Git、SVN等）或利用虛擬主機備份資料庫等備份方式
  - 整備重點：檢視資料備份規範與執行情形

建構管理區

資料備份－測試備份媒體

- 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（中高）
  - 備份媒體亦可能毀損，故應定期測試備份資料有效性
  - 整備重點：檢視備份媒體測試結果，測試週期應符合機關規定，測試內容需包含查檢備份資料的正確可用，如進行備份回復測試等

資料備份－還原測試

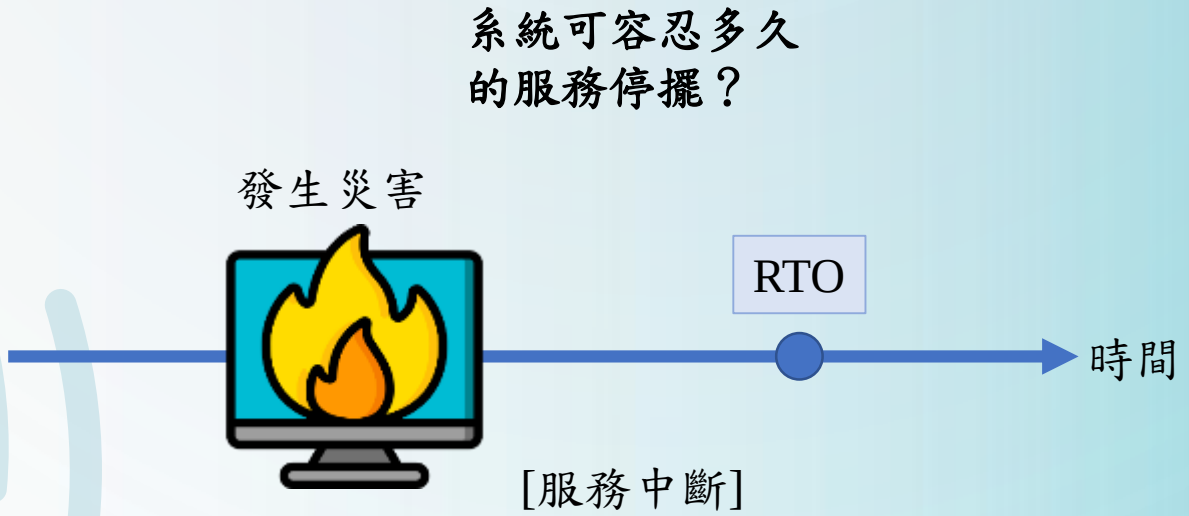
- 應將備份還原，作為營運持續計畫測試之一部分（高）
  - 營運持續計畫(BCP)應定期演練，在災害復原過程中應使用備份資料驗證備份機制可用性及完整性
  - 整備重點：檢視BCP執行紀錄

資料備份－異地備份

- 應建立資料異地備份機制（高）
  - 使用適當的實體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
  - 如使用DVD光碟儲存系統軟體備份，並置於防火櫃中妥善保管等
  - 整備重點：檢視機關備份規範與執行情形

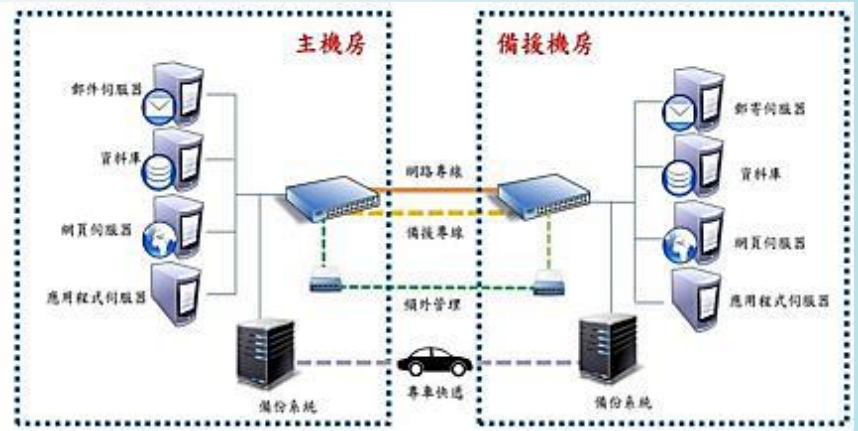
系統備援－復原時間目標(RTO)

- 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（中高）
  - 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)
  - 整備重點：檢視機關RTO定義與執行情形



系統備援－備援設備

- **應定期測試原服務中斷時，於可容忍時間內，由備援設備或其他地方式取代並提供服務（中高）**
  - 機關應規劃適當的備援機制以避免單點失效，當災害發生時應於所訂定之容忍時間內讓服務回復正常運作
  - 亦可能採用其他可確保服務運作之方案，如雲端環境、虛擬化還原技術等
  - 整備重點：檢視機關備援實作方式並評估是否可符合RTO要求



系統備援－備援啟動演練

- **應將備援啟動作為營運持續計畫測試之一部分（高）**
  - 機關應將備援啟動納入**營運持續計畫演練範圍**。
  - 營運持續計畫(BCP)應定期演練，在復原過程中應使用備援系統驗證備援機制可用性及完整性
  - 整備重點：檢視BCP執行紀錄

構面4:識別與鑑別

使用者之識別與鑑別

- 身分驗證
- 多重認證技術

身分驗證管理

- 變更預設密碼
- 禁止明文傳輸
- 帳戶鎖定
- 密碼複雜度與效期
- 密碼歷程
- 非內部使用者身分驗證管理
- 防自動化程式
- 密碼重設

鑑別資訊回饋

- 遮蔽密碼
- 密碼儲存安全

什麼是識別與鑑別？

識別
(Identification)

區別使用者是誰
如帳號

鑑別
(Authentication)

確認使用者是其宣稱主體
如密碼

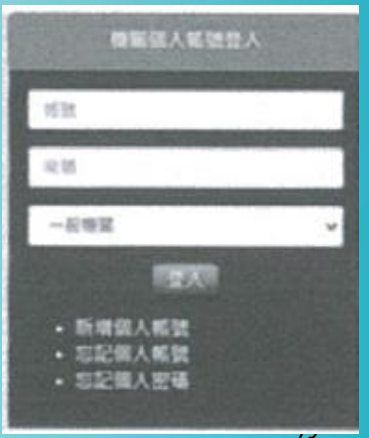
使用者之識別與鑑別－身分驗證

- 資通系統應具備唯一識別及鑑別使用者之功能，禁止使用共用帳號（普中高）
  - 實作身分驗證機制，如帳號、密碼
  - 避免共用帳號，如替使用者建立個人帳號（含系統管理者與一般使用者），以區分安全責任並強化可歸責性
  - 整備重點：
    - ➢確認資通系統已具備身分驗證機制
    - ➢盤點違規共用帳號使用行為

若共用帳號

出事找誰負責？

以個人帳號登入

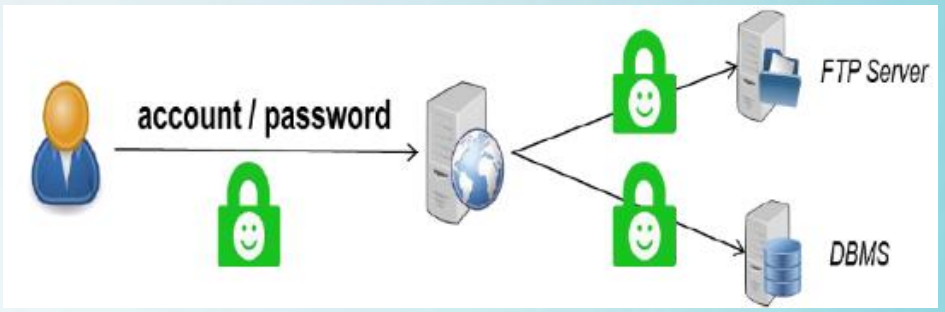


身分驗證管理－變更預設密碼

- 使用預設密碼登入系統時，應於登入後要求立即變更（普中高）
  - 若使用預設密碼（如由系統產生或人工配發），首次登入系統時應要求使用者變更
  - 預設密碼變更宜具備強制性，避免要求流於形式
  - 整備重點：
    - ➢確認資通系統是否使用預設密碼
    - ➢測試以預設密碼登入後，是否出現變更提示

身分驗證管理－禁止明文傳輸

- 身分驗證相關資訊不以明文傳輸（普中高）
  - 身分驗證相關資訊，如密碼，傳輸時應加密或編碼保護
  - 如建立已加密之安全通道（如HTTPS、SSH等），或是以應用程式加密或編碼等方式保護
  - 整備重點：
    - ➢抽查是否使用HTTP、Telnet、FTP等未加密協定傳輸帳密
    - ➢發展測試案例，如以網路封包分析軟體（如Wireshark等）攔截並檢視網路封包內容是否存在明文密碼



身分驗證管理—帳戶鎖定

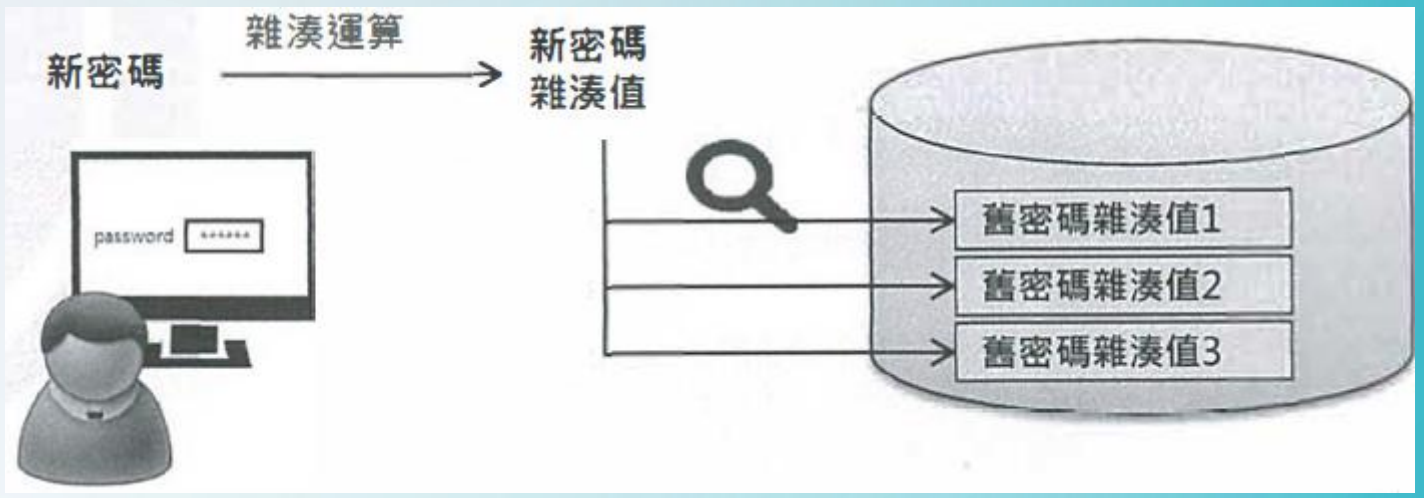
- 具備帳戶鎖定機制，帳號登入進行身分驗證失敗達5次後，至少15分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制（普中高）
  - 實作帳戶鎖定以避免密碼破解攻擊
  - 機關得視系統使用需求，自建之失敗驗證機制，如訂定不同之鎖定觸發條件與閉鎖期，或是其他身分驗證強化機制
  - 整備重點：確認資通系統帳號鎖定機制
    - ➢測試鎖定機制觸發條件以及鎖定期是否仍能登入

身分驗證管理－密碼複雜度與效期

- **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（普中高）**
  - 機關可自行定義密碼複雜度、最短與最長效期規定
    - 以Windows GCB為例，最短效期建議值1天，最長90天
  - 密碼複雜度可降低密碼破解風險
  - 最長效期目的在防止使用萬年密碼
  - 最短效期目的在防止使用者頻繁變更密碼以規避密碼歷程限制
  - 整備重點：
    - 確認資通系統以實作最低密碼複雜度、最短及最長效期
    - 如檢視組態設定或發展測試案例等

身分驗證管理－密碼歷程

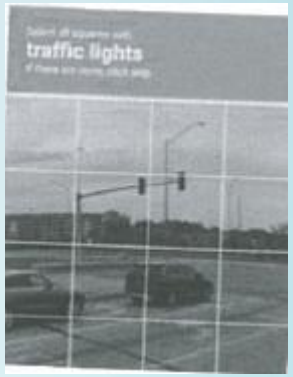
- 密碼變更時，至少不可以與前3次使用過之密碼相同（普中高）
  - 系統應記錄密碼歷程（非密碼明文形式）至少3代
  - 整備重點：發展測試案例，如連續變更密碼3次，檢視新設定密碼能否設為與先前3次重複



身分驗證管理－防範自動化程式

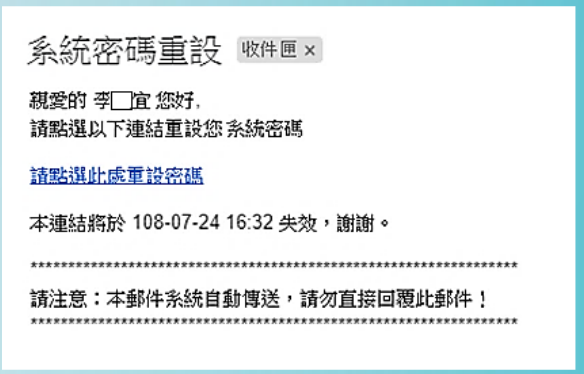
- 身分驗證機制應防範自動化程式之登入或密碼更換嘗試（中高）
  - 避免密碼破解，如實作Captcha或密碼鎖定機制
  - 整備重點：
    - ➢確認資通系統防護實作方式
    - ➢發展測試案例驗證防護機制有效性，如輸入正確、錯誤或是空白的驗證碼時 ，能否通過驗證

Captcha



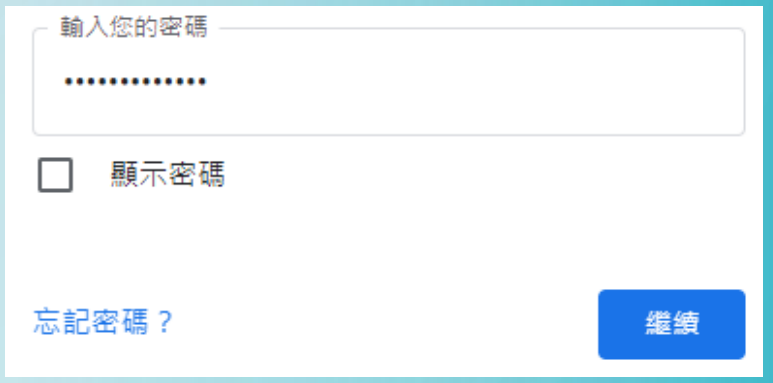
身分驗證管理－密碼重設

- 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（中高）
  - 符記(Token)，例如簡訊驗證碼或Email連結等
    - ➢一次性：不得重複使用同一個Token
    - ➢時效性：限制有效期限，如效期60分鐘
  - 整備重點：
    - ➢確認資通系統是否允許使用者自行重設密碼
    - ➢可發展測試案例，如確認是否成功發送符記，並測試當使用錯誤、空白、過期或重複使用的符記時是否仍能通過驗證



鑑別資訊回饋－遮蔽密碼

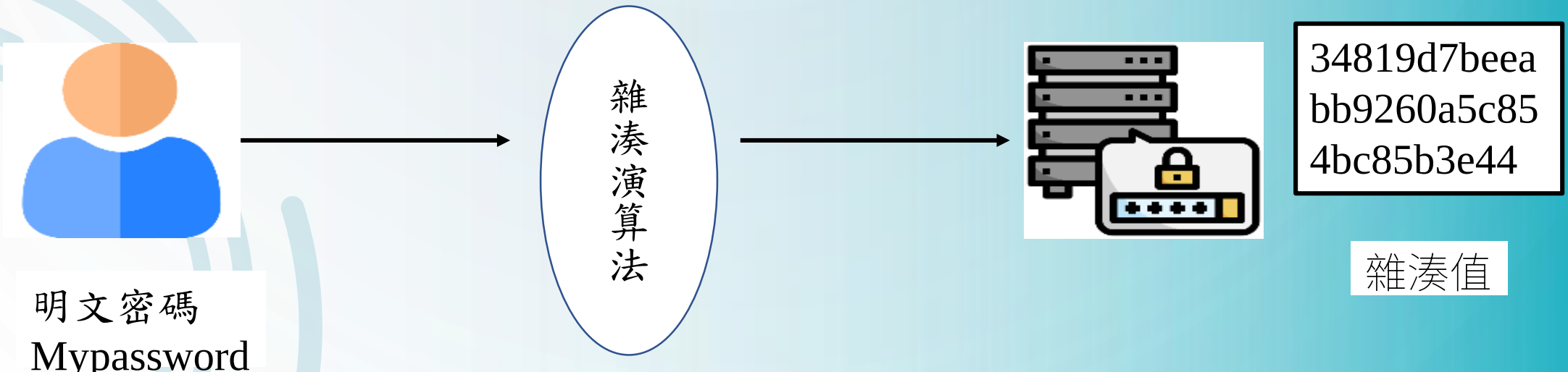
- 資通系統應遮蔽鑑別過程中之資訊（普中高）
- 資通系統應避免在使用者輸入密碼時被人從旁窺視
- 密碼輸入欄位不可顯示明文，實務上常以*顯示
- 不可使用HTTP GET傳遞帳號密碼等參數
- 整備重點：檢視密碼輸入欄位與網址列



https://example.com/login.phph?username=Tom&password=iLoveU

加密模組鑑別－密碼儲存安全

- 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（中高）
  - 雜湊具備單向特性，無法從雜湊值計算回推原始訊息（單向）
  - 不可儲存密碼明文字串，以避免惡意管理員或駭客入侵盜取密碼
  - 整備重點：檢視資料庫中密碼欄位資訊



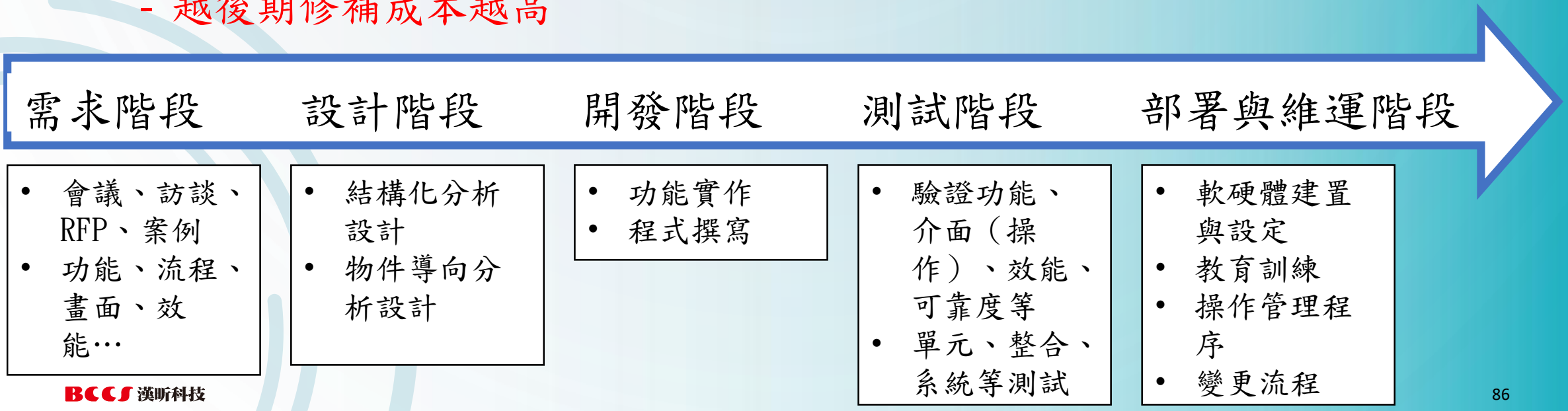
構面5：系統與服務獲得

系統發展生命週期

需求階段	設計階段	開發階段	測試階段	部署與維運階段	委外階段	獲得程序	系統文件
•確認安全需求	•威脅識別與風險評估 •安全需求修正	•安全需求實作 •避免常見漏洞 •隱藏詳細錯誤訊息 •源碼掃描 •嚴重錯誤通知機制	•弱點掃描 •滲透測試	•系統更新與修補 •禁用預設密碼 •版本控制與變更管理	•委外安全需求	•作業環境區隔	•文件儲存管理

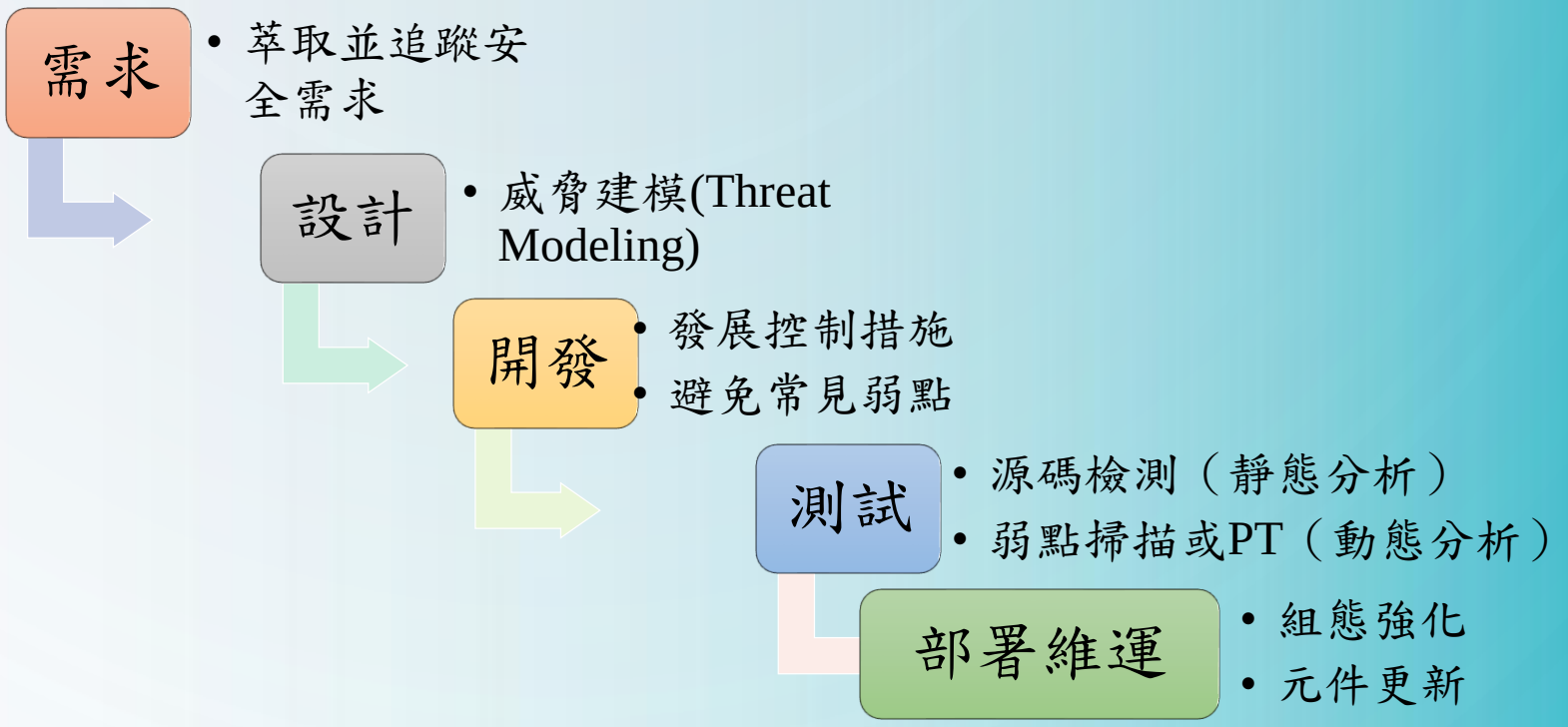
典型系統發展生命週期(SDLC)

- 強調功能面完善，以及專案如期完成
- 資安問題仰賴資安設備或安全檢測等方式
  - 被動反應
  - 集中後期
  - 越後期修補成本越高



安全系統發展生命週期(SSDLC)

- Secure System Development Life Cycle (SSDLC)
  - 強調在從專案開始的各階段及早加入安全思維，以打造具備安全體質的資通系統

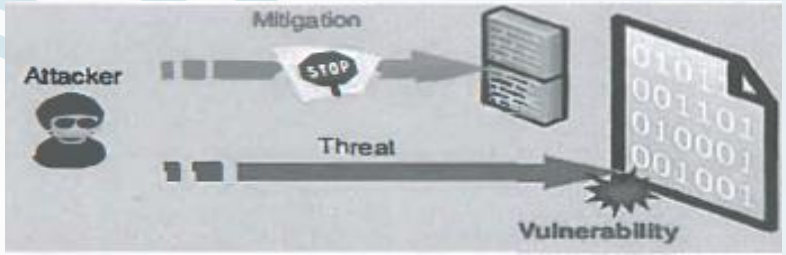


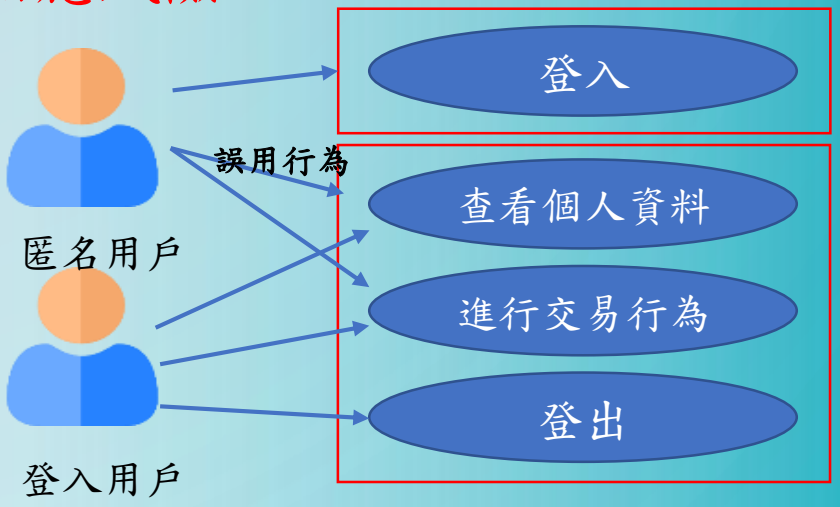
需求階段—確認安全需求

- **針對系統安全需求（含機密性、可用性、完整性）進行確認（普中高）**
- 機關確認安全需求方式，如自行發展設計系統安全需求檢核表進行需求確認，或參考國家資通安全研究院「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」等
- 整備重點：檢視機關訂定及確認安全需求機制

設計階段－威脅識別與風險評估

- 根據系統功能與需求，識別可能影響系統之威脅，進行風險分析及評估（中高）
- 如使用誤用模型分析或威脅建模(Threat Modeling)等足以有效識別資安威脅之方式，並進一步分析各種威脅之風險
- 整備重點：檢視機關識別系統威脅方式並評估相應風險





風險＝（可重製性＋可利用性＋可發現性）X（可能傷害＋影響人數）

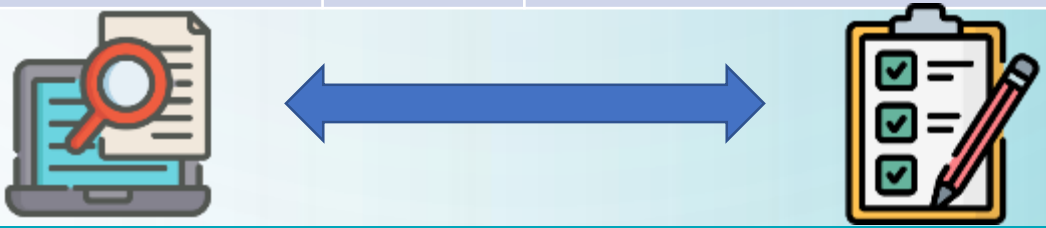
威脅發生的可能性

威脅發生的危害

設計階段－安全需求修正

- 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（中高）
  - 針對新發現之威脅或風險分析結果調修安全需求
  - 整備重點：檢視機關修正安全需求機制

威脅項目	風險值	控制措施
未對來源進行驗證	30	採用帳號密碼登入認證限制來源IP
未對資料進行加密保護	24	進行SSL/TLS加密
拒絕存取	18	使用分散式系統架構
未對資料進行完整性驗證	16	進行資料訊息摘要
使用過高系統權限	15	改採一般使用者權限執行



開發階段－安全需求實作

- 應針對安全需求實作必要控制措施（普中高）
  - 資通系統應訂定安全需求項目，包含機密性、完整性及可用性等相關要求，並應確實實作
  - 整備重點：確認系統安全等級需求實作
    - ➢至少應符合資通系統防護基準安全控制措施

專案名稱		網頁部落格		專案經理	○○○		專案期限	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	測是案件編號	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 Aauthorization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Validation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

開發階段－避免常見漏洞

- 應注意避免軟體常見漏洞及實作必要控制措施（普中高）
  - 應避免OWASP Top 10 及 CWE Top 25等常見漏洞
  - 整備重點：檢視機關相關管理規範及安全強化作為
    - ➢包含（但不限於）導入SSDLC安全開發流程，強化教育訓練與撰寫安全程式碼、執行源碼審查與安全性檢測等

- OWASP Top 10:2025

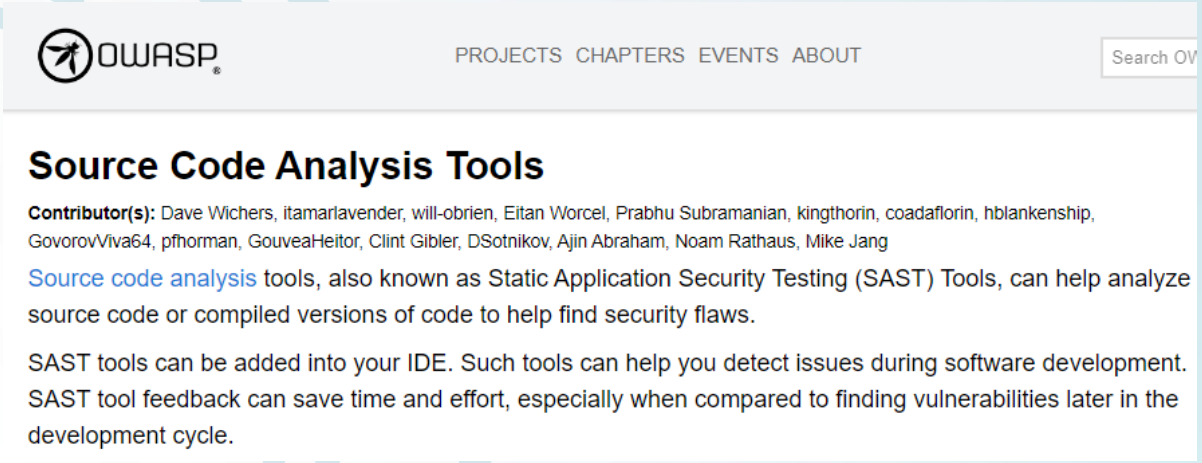
項次	中文	英文
A01:2025	權限控制失效	Broken Access Control
A02:2025	安全設定缺陷	Security Misconfiguration
A03:2025	供應鏈失效	Software Supply Chain Failures
A04:2025	加密失效	Cryptographic Failures
A05:2026	注入式攻擊	Injection
A06:2025	不安全設計	Insecure Design
A07:2025	身分驗證失效	Authentication Failures
A08:2025	軟體與資料完整性失效	Software or Data Integrity Failures
A09:2025	資安紀錄及監控失效	Security Logging and Alerting Failures
A10:2025	特殊狀況處理不當	Mishandling of Exceptional Conditions

開發階段－處理錯誤訊息

- 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（普中高）
  - 系統宜客製化錯誤頁面，隱藏錯誤程式碼位置及內容等機敏訊息
  - 帳號登入失敗時，不宜指出明確原因（如帳號不存在、密碼錯誤）
  - 整備重點：評估發展測試案例
    - ➢如存取不存在之網頁或輸入錯誤資料等：觀察所產出錯誤訊息

實作階段－源碼掃描

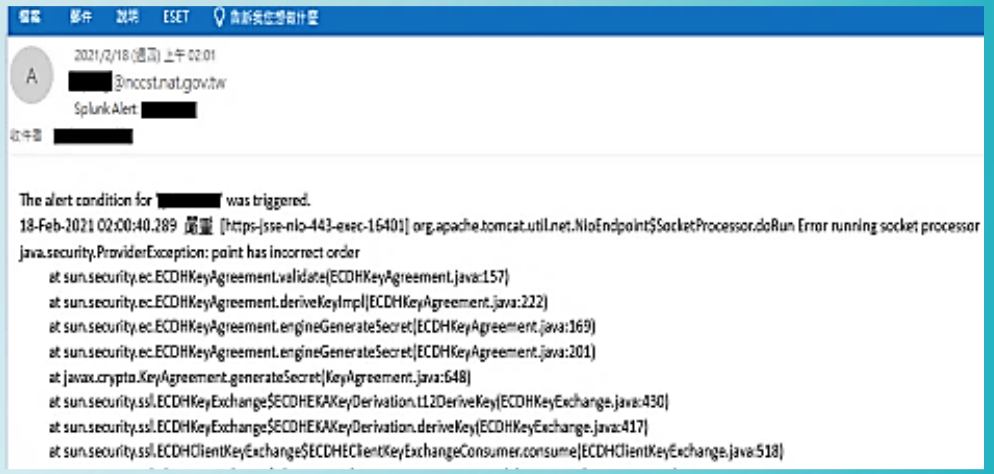
- 執行「源碼掃描」安全檢測（高）
- 執行源碼掃描以檢測源碼中的安全弱點
- 整備重點：檢視執行紀錄，確認檢測工具之適切性，持續管制追蹤弱點修補狀態
- 掃描工具如參考OWASP與NIST等列表



實作階段－嚴重錯誤通知機制

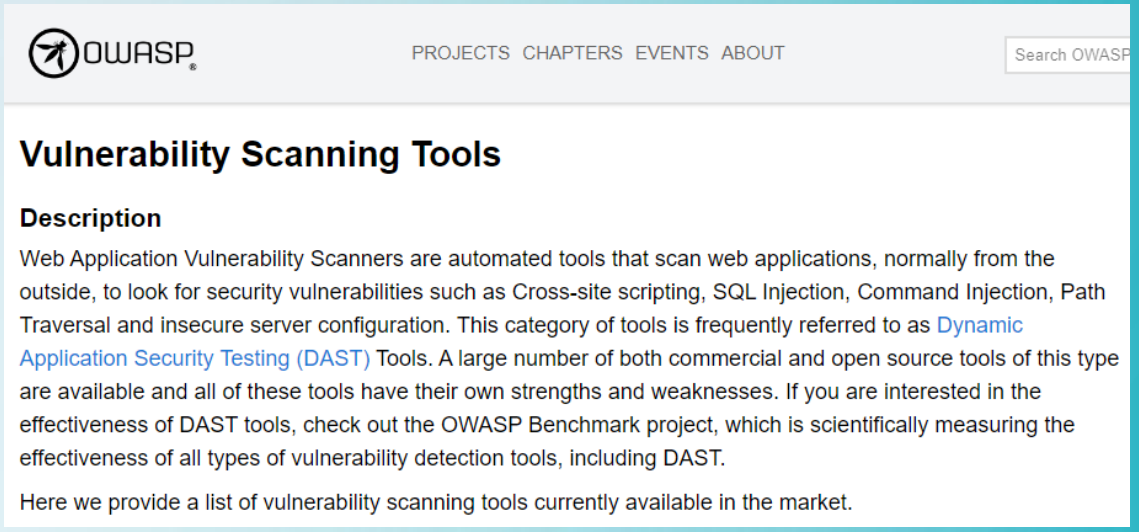
- 系統應具備發生嚴重錯誤時之通知機制（高）
  - 嚴重錯誤，如系統效能大幅度下降、服務停擺或駭客入侵破壞系統完整性等，嚴重影響業務正常運作
  - 系統應具備可靠且有效之系統錯誤通知機制，避免無人發覺與處理
  - 如實作系統例外處理(try-catch)功能，在發生嚴重錯誤時，自動以信件、簡訊或其他方式通知系統管理與承辦人員，利用SOC服務監控系統，提出即時異常警示
  - 整備重點：檢視系統錯誤通知機制

◦嚴重錯誤通知信件



測試階段－弱點掃描

- 執行「弱點掃描」安全檢測（普中高）
  - 使用自動化工具對目標進行掃描
    - ➢連接埠掃描、作業系統識別、版本掃描、弱點掃描等
  - 整備重點：檢視執行紀錄，確認檢測工具之適切性，持續掌握並追蹤弱點修補狀態
    - ➢OWASP整理之弱掃工具列表



應辦事項要求

資通安全責任等級	機關屬性	辦理內容
A	• 公務機關 • 特定非公務機關	全部核心資通系統每年辦理二次
B	• 公務機關 • 特定非公務機關	全部核心資通系統每年辦理一次
C	• 公務機關 • 特定非公務機關	全部核心資通系統每二年辦理一次
D	各機關	無需求
E	各機關	無需求

核心資通系統：

- 支持核心業務持續運作必要之系統，
- 或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則之規定，判定其防護需求等級為高者

測試階段－滲透測試

- 執行「滲透測試」安全檢測（高）
- 一般由資安專家手動進行，效果取決於人員經驗與技術
- 整備重點：檢視執行紀錄，並持續掌握追蹤弱點修補狀態

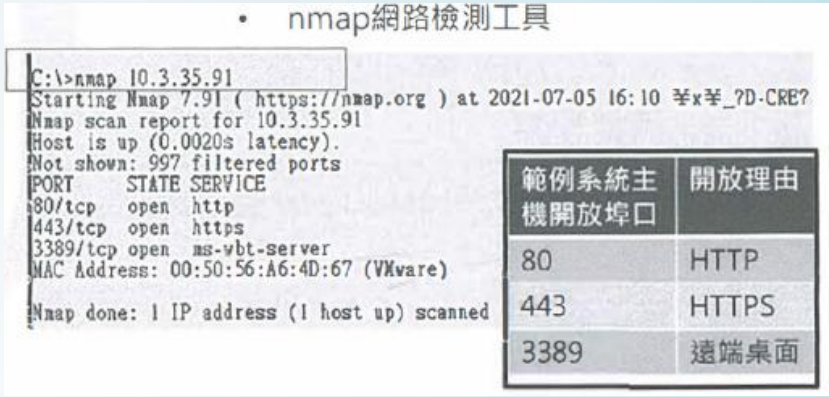
需求訪談	資訊蒐集	弱點掃描	弱點利用	報告撰寫
- 討論並確認測試範圍 - 確定執行日期及時間 - 確認執行方式 - 制定相關規則 - 定期進行溝通 - 撰寫執行計畫書	- 搜尋引擎 - 公開網站 - DNS查詢 - Whois查詢	- 連接埠掃描 - 作業系統鑑別 - 版本掃描 - 弱點掃描	- 證明威脅 - 取得權限 - 排除誤判	- 簡介 - 執行過程 - 執行結果 - 結論

部署與維運階段－系統更新與修補

- 於部署環境中應針對相關資通安全威脅，進行更新與修補（普中高）
  - 系統弱點修補及元件
    - ➢如作業系統安全性更新、JAVA、第三方函式庫等更新等

部署與維運階段－系統更新與修補

- 識別並關閉不必要服務及埠口（普中高）
  - 系統服務與埠口(Port)
    - ➢原則關閉，有需要才開放。可以正面表列需要開啟該服務及埠口之理由
    - ➢如利用Nmap等工具進行服務埠掃描（Port Scan）



部署與維運階段－禁用預設密碼

- 資通系統不使用預設密碼（普中高）
  - 相關軟體，如套裝軟體、資料庫、Web伺服器等，應避免使用預設密碼，建議於系統正式上線前停用或完成密碼變更
  - 部分舊版本元件仍內建預設密碼，存在被失誤啟用的風險
    - ➢例如：舊版Apache Tomcat 7內建預設帳號密碼
  - 整備重點：確認資通系統各軟體元件未啟用預設密碼

```
<tomcat-users>
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary.
-->
<!--
  NOTE:  The sample user and role entries below are wrapped in a comment
  and thus are ignored when reading this file. Do not forget to remove
  <!.. ..> that surrounds them.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="tomcat" roles="tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
-->
</tomcat-users>
```

部署與維運階段－系統源碼備份

- 執行系統源碼備份（普中高）
  - 機關應備份系統源碼（含原始程式碼、目的程式等）不宜全數交由廠商管理保存，避免委外廠商倒閉或更換後無法維護系統之情形
    - ➢備份作業時機如廠商交付、內容變更時，或定期備份
  - 實務上如建置建構管理區集中存放，或使用版本控制系統（如Git、SVN等）或利用虛擬主機備份等備份方式
  - 整備重點：檢視機關源碼備份規範與執行情形　建構管理區

部署與維運階段－版本控制與變更管理

- 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（中高）
  - 版本控制目的在需要時可取回特定版本，機關進行系統變更應訂定並遵循相關相關管理辦法或程序
    - ➢如導入版本控制軟體，並填寫相關流程申請審核表單
  - 變更管理之重點包含：
    - ➢系統開發與變更程序
    - ➢程式碼版本控制與追蹤
    - ➢變更上線前必要的安全活動
    - ➢回復程序
  - 整備重點：檢視版控與變更管理之有效性

委外階段－委外安全需求

- 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（普中高）
  - 將系統安全需求明確納入委外契約，並據以驗收
  - 如建議參考國家資通安全研究院「資通系統委外開發RFP資安需求範本(V3.0)」
  - 整備重點：檢視委外契約，須納入安全需求

獲得程序－第三方元件管理

- 識別資通系統使用之第三方軟體、服務、函式庫或其他元件（普中高）
  - 組織應列出系統中所有的組成成分，包含開源套件 (Open Source) 與第三方服務 (包含系統使用的 API 服務、雲端基礎設施)，識別這些第三方元件是否存在已知漏洞 (CVE)、是否已停止維護 (EOL)、或其授權合約是否包含資安合資條款。
  - 宜檢視
  - ➢組織是否有維護軟體清冊、SBOM 文件、系統架構圖中標註的第三方組件？
  - ➢確認開發規範文件、第三方函式庫核准記錄、靜態/動態程式碼掃描報告是否有審核流程？
  - ➢弱點掃描流程紀錄、針對供應商資安公告的追蹤紀錄，是否能快速比對現有系統是否有受影響？
  - 整備重點：檢視第三方元件清單是否建立並定期更新

獲得程序—作業環境區隔

- 開發、測試及正式作業環境應為區隔（中高）
  - 開發環境、測試環境與正式作業環境應透過網段或設備區隔等各種適當方式，實作應用程式與資料庫等存取控制，保護正式作業環境系統及資料
  - 整備重點：檢視環境區隔作法之有效性

系統文件－文件儲存與管理

- 應儲存與管理系統發展生命週期之相關文件（普中高）
  - 系統發展生命週期之相關文件應以書面或電子化形式進行文件保存，並被納入管理程序，例如：
    - 系統需求書
    - 系統規格書
    - 系統發展計畫
    - 系統測試報告
    - 系統驗收紀錄
    - 系統變更紀錄
    - 其他

文件/紀錄名稱	編號	保存年限
軟體發展計畫	依建構項目規範編碼	結案後2年
軟體需求規格書	依建構項目規範編碼	結案後2年
系統規格書	依建構項目規範編碼	結案後2年
軟體測試計畫	依建構項目規範編碼	結案後2年
維護手冊	依建構項目規範編碼	結案後2年
軟體使用手冊	依建構項目規範編碼	結案後2年
系統文件審查表	NCCST_FT_040	結案後2年
系統原始碼	依建構項目規範編碼	結案後2年
測試問題紀錄表	NCCST_FT_041 合併於軟體測試報告	結案後2年
軟體測試報告	依建構項目規範編碼	結案後2年
驗收紀錄表	NCCST_FT_042	結案後2年

  - 整備重點：檢視機關管理規範及執行結果

構面6:系統與通訊保護

傳輸之機密性與完整性

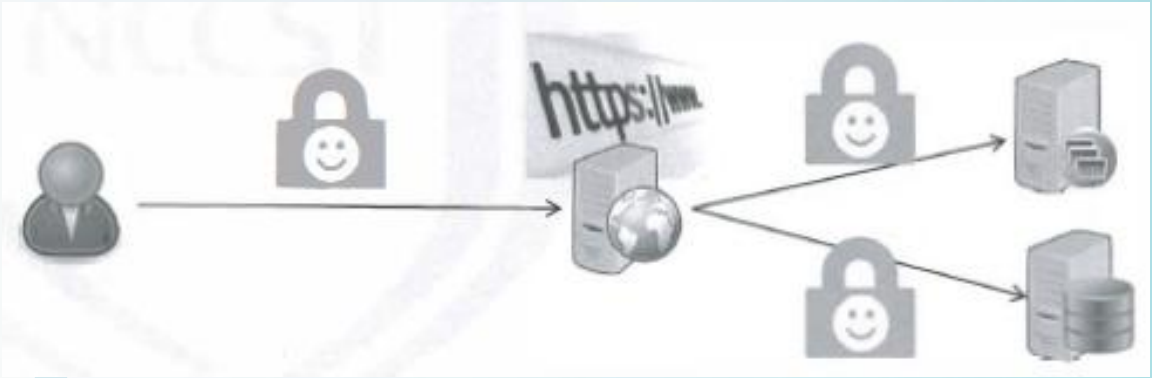
- 傳輸加密
- 演算法
- 金鑰長度
- 金鑰憑證更換
- 金鑰保管

資料儲存之安全

- 組態保護

傳輸之機密性與完整性－傳輸加密

- **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（高）**
- 資通系統應實作傳輸加密機制，如HTTPS、SSH、SFTP及VPN等加密傳輸協定，或其他足以確保資料機密性與完整性之安全控制措施
- 整備重點：確認資通系統任何傳輸方式已具備安全性保護



傳輸之機密性與完整性－演算法

- 使用公開、國際機構驗證且未遭破解之演算法（高）
  - 勿自行創建加密演算法
  - 停用已遭破解的演算法，如RC2、RC4、DES、3DES及MDS等
    - ➢可改用AES、RSA等較安全的演算法
    - ➢不安全的Cipher如TLS_RSA_WITH_RC4_128_MD5等
  - 停用不安全的網路傳輸協定，如SSLv3、TLS1.0及TLS1.1
    - ➢應採用TLSl.2以上
  - 整備重點：檢視資通系統使用之HTTPS傳輸協定與Ciphers


Google 發現 SSL 3.0 漏洞，小心「貴賓犬」攻擊!

文/ 陳曉莉 | 2014-10-15 發表

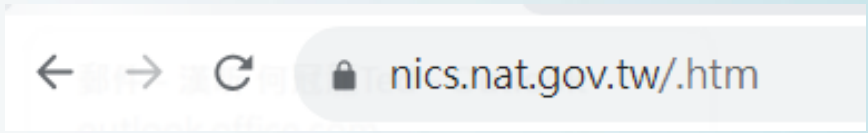
讚 0 分享


Google釋出Chrome 84，修補38個安全漏洞，正式移除對TLS 1.0/1.1的支援

當用戶造訪依舊採用TLS 1.0/1.1網站，Chrome 84就會出現插入式的全頁面警告

傳輸之機密性與完整性－金鑰憑證更換

- 加密金鑰或憑證應定期更換（高）
  - 避免使用萬年憑證而增加被破解的風險，已過期憑證應盡速更換
  - 對外服務站台應使用合法憑證中心（如政府憑證管理中心GCA等）核發之伺服器憑證
  - 內部站台若使用自簽憑證，亦應注意使用年限
  - 宜確認資通系統使用有效之Https憑證



傳輸之機密性與完整性－金鑰保管

- 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（高）
  - 機關應依據金鑰產生、分配、儲存、存取和銷毀之要求，建立和管理系統所使用密碼系統之密鑰
  - 強化存取控制，加密金鑰與加密資料應分開存放，以確保金鑰的機密性、完整性與可用性
  - 整備重點：檢視機關訂定之金鑰保管規範及執行結果

資料儲存之安全－組態保護

- 資通系統重要組態設定檔案及其他具保護需求之資訊加密或以其他適當方式儲存（高）
  - 如含有資料庫連線資訊及帳密之設定檔或連線字串等
  - 整備重點：檢視系統組態設定檔案，不可包含明文之機敏連線資訊

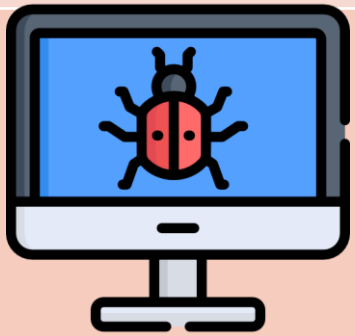
Web.config

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
 <connectionStrings>
  <add name= "Demo" connectionString="Data Source=資料庫ip;Initial
Catalog=SecurityDB;User ID=帳號;Password=密碼;Application Name=testAP;"
providerName="System.Data.SqlClient"/>
 </connectionStrings>
<startup><supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.6"/></startup>
</configuration>
```

```
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!
```

使用aspnet_regiis
加密連線字串

構面7:系統與資訊完整性



漏洞修復

- 修復漏洞及定期更新
- 確認漏洞修復狀態

資通系統監控

- 監控通報
- 監控資通系統連線
- 採用自動化監控工具
- 使用完整性驗證工具
- 於伺服器端檢查輸入
- 應變措施
- 定期檢查完整性

漏洞修復－修復漏洞及定期更新

- 系統之漏洞修復應測試有效性及潛在影響，並定期更新（普中高）
  - 與安全相關之軟體更新，包含修補程式(Patch)、服務包(Service Pack)及熱修復(Hotfix)等，系統元件之安全弱點亦可能藉由更新函式庫或程式版本等方式進行修補
  - 應定期進行軟體更新，完成更新可行性評估並通過測試後，始於正式環境進行更新
  - 整備重點：檢視更新及修補作法

漏洞修復－確認漏洞修復狀態

- 定期確認資通系統相關漏洞修復之狀態（中高）
  - 機關宜注意相關之安全漏洞訊息（如透過CVE相關訊息網站、廠商安全通告等）
  - 由弱點掃描及滲透測試等安全檢測活動所檢出之系統漏洞應設法修復並定期追蹤修復進度，或是配合定期之安全檢測作業確認複測
  - 整備重點：檢視機關弱點修補追蹤管理機制

資通系統監控－監控通報

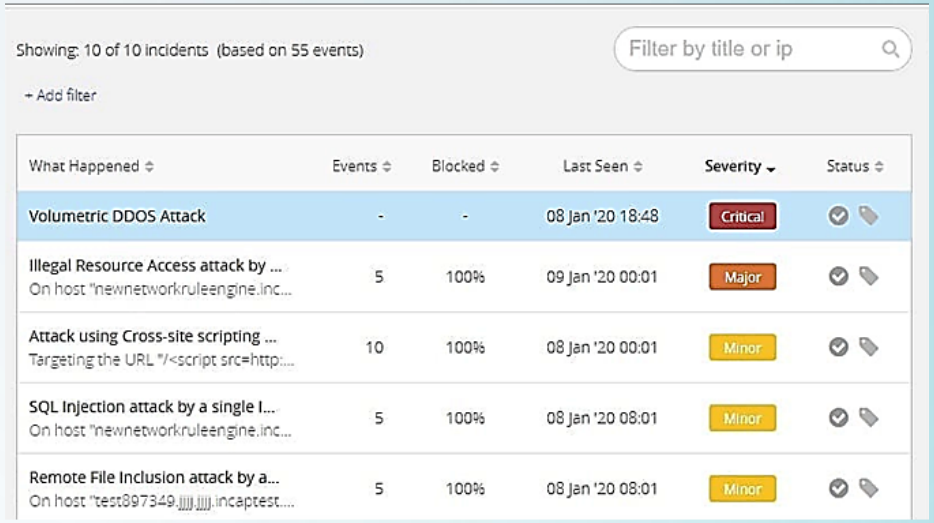
- 發現資通系統有被入侵跡象時，應通報機關特定人員（普中高）
  - 如告知系統管理人員或系統承辦人員等，並配合機關通報時效，告知機關資安通報窗口以進行內部或外部通報
  - 整備重點：
    - ➢檢視資通系統採用之監控機制
    - ➢確認通報方式及對象

資通系統監控－監控資通系統連線

- 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（中高）
  - 應具備監控資通系統之能力，如指派專業人員或使用監控設備， 用以偵測資通系統連線行為
  - 整備重點：檢視資通系統採用之監控機制

資通系統監控－採用自動化監控工具

- 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（高）
- 如部署 IPS、IDS 、 WAF、UTM防火牆等具備自動化監控能力之網路安全防護產品以監控資通系統網路行為
- 整備重點：檢視資通系統採用之監控機制



軟體及資訊完整性－於伺服器端檢查輸入

- 使用者輸入資料合法性檢查應置放於應用系統伺服器端（中高）
  - 輸入檢查(Input Validation)應實作於伺服器端，不可依賴客戶端檢查（如Java Script等），以避免被惡意繞過
  - 如利用正規表示式(Regular Expression)方式實作輸入字串過濾等

```
<%@ 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>
```

  - 整備重點：檢視資通系統輸入檢查機制

軟體及資訊完整性－使用完整性驗證工具

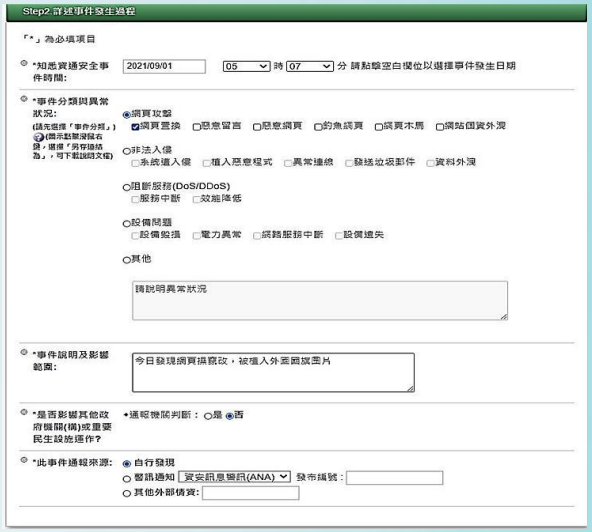
- 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊（中高）
  - 機關需可察覺特定軟體及資訊已被惡意竄改
  - 常見資安威脅，例如站台首頁被置換、網頁掛馬等
  - 完整性驗證工具，例如：
    - ➢雜湊
    - ➢數位簽章
    - ➢目錄監控軟體
    - ➢其他
  - 整備重點：
    - ➢確認已使用完整性驗證工具／技術
    - ➢評估完整性驗證之有效性

舉例：目錄監控軟體

軟體及資訊完整性－應變措施

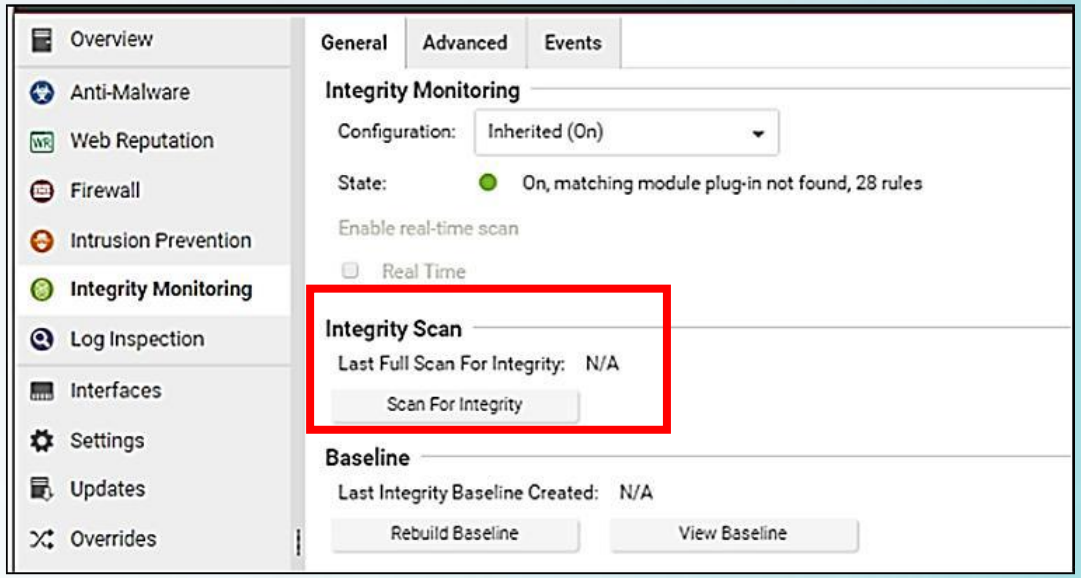
- 發現違反完整性時，資通系統應實施機關指定之安全保護措施（中高）
  - 在發現資通系統完整性遭到破壞時（如資料庫或檔案被不當竄改，站台被植入惡意指令碼或元件等），應採取適當之行動，如通知系統管理者進行緊急應變處置，並依規定之通報流程進行資安事件通報作業
  - 整備重點：檢視應變措施是否已符合資安法與機關相關管理規範

國家資通安全通報應變網站操作範例



軟體及資訊完整性－定期檢查完整性

- 應定期執行軟體與資訊完整性檢查（高）
  - 定期進行完整性檢查，以發現潛藏之資安事件
  - 實作方式如先記錄初始狀態（建立baseline)，利用排程定期檢查內容是否已經過變動等
  - 整備重點：檢視定期檢查相關執行紀錄



114年資通系統防護基準改善建議

一、系統資料填報完整性

1.建立年度填報檢核作業，由各系統管理人於每年初自行檢視並更新資料。

2.規範「系統環境資訊調查表」之必填欄位，未填寫者應退回補正。

二、防護基準與安全等級評估一致性

1.各單位應重新檢視防護基準與安全等級評估內容是否一致。

2.對「不適用」項目，須提供明確原因及業務合理性說明。

114年資通系統防護基準改善建議

三、帳號與身分驗證管理

1.建議所有系統採用密碼複雜度政策（最少八碼、含英數混合），並設置登入失敗鎖定機制。

2.系統須提供登入畫面截圖、操作記錄或驗證程式碼作為佐證。

四、日誌管理與備援機制

1.有系統均應明訂日誌保存期限（至少一年）及異常回報流程。

2.建立自動化日誌備份與稽核通知機制。

3.定期（每半年）進行備援演練與回復測試，保留測試報告作為佐證。

114年資通系統防護基準改善建議

五、委外維運與文件管理

1.建立委外系統清冊，列明廠商資訊、合約期程及稽核責任。

2.對外包廠商定期進行稽核或文件查驗，確保維護過程符合安全標準。

3.於合約中明訂「資安配合條款」，包括資料保密、弱點修補、稽核配合等要求。

六、佐證資料與文件一致性

1.各系統須保存稽核截圖、操作說明及日誌輸出結果。

2.稽核文件應由主管覆核後再行提交，以確保資料一致性與正確性

BCCS 漢昕科技

資安整備專家

委外監督管理

依據

- 資通安全管理法
- 個人資料保護法
- 教育部民國110年06月18日臺教資(四)字第1100068264B號令頒「教育部委外辦理或補助建置維運伺服主機及應用系統網站資通安全及個人資料保護管理要點」

資訊委外類別與形態-4類22種型態

系統發展類 (3種)	維運管理類 (10種)	顧問訓練類 (6種)	雲端服務類 (3種)
• 系統開發 • 系統維護 • 系統整合	• 設備操作、硬體維護、機房設施管理、備份與備援服務、網路與資安服務 • 網路管理、資料處理、資料登錄、整體委外、人力支援	• 顧問輔導 • 稽核審查 • 系統稽核 • 軟體驗證 • 教育訓練 • 整體規劃	• 軟體即服務(SaaS) • 平台即服務(PaaS) • 基礎設施即服務(IaaS)

資訊委外合約訂定考量因素

培訓和知識轉移

- 要求委外廠商提供相關的培訓計劃，以確保內部團隊具備適應委外管理的技能和知識。
- 確保知識轉移的有效進行，以便日後能夠自行管理和維護系統。

合規性和法律要求

- 確保委外廠商遵守所有相關的法律、法規和合規性要求，特別是涉及敏感資訊和個資的保護。
- 合約應包含相應的條款，以確保合規性和風險管理。
- 可參考工程會網站中政府採購-招標相關文件最新版本

服務變更和終止

- 明確規定服務變更和終止的程序和條件，包括通知期限、資料移交、合約終止後的責任等。
- 有助於確保順利轉換或終止委外合作關係。

資訊委外合約訂定考量因素(續)

知識產權和機密性

- 訂定條款及簽保密切結書，來保護大學的知識產權和機密性，確保委外廠商不會未經授權地使用或洩漏機構的機密資訊。

糾紛解決機制

- 確定適當的糾紛解決機制，例如談判、仲裁或訴訟程序。這有助於處理合約爭議，以確保雙方的權益得到保護。

審查人員資格考量因素

評估委外廠商的組織結構

- 了解委外廠商的組織結構，包括其組織規模、專業團隊成員的分布和層次。
- 確定供應商是否具備足夠的資源和能力來支持大學的需求。

檢視專業背景和經驗

- 審查委外廠商的專業背景和經驗，特別是與大學合作相關的領域。
- 檢視委外廠商的歷史紀錄、過去的專案案例和客戶評價等，以評估其專業水平和能力。

技能和培訓要求

- 明確定義所需的技能和培訓要求，並確保供應商的人員具備相應的專業知識和技能。
- 要求供應商提供相關的學歷、專業認證、培訓計劃和證書等方式來驗證。

審查人員的資格和證書

- 要求供應商提供其人員的資格和證書，例如資訊安全專業人員的CISSP證書、專案管理人員的PMP證書等。
- 這些證書可以證明人員具備相應的專業知識和技能。

建議書徵求文件（RFP)制定

明定委外廠商之責任與義務，針對資安管理部分，訂定相關規範要求，或要求廠商之服務建議書中提出相對應做法。

- 明定委外廠商之責任與義務
- 確認專案目標
- 界定專案範圍
- 掌握業務與資通系統現況(及風險評估歷史)
- 蒐集現行資訊軟硬體作業環境
- 擬訂需求內容(含資安功能需求)
- 制定服務水準指標(SLA)
- 規範交付項目與內容(含安全證明文件)
- 訂定專案管理需求(與階段性檢核)
- 訂定評選標準與方式
- 參考機關契約條文、資訊服務採購相關手冊與指引

建議書徵求文件（RFP）制定

- 建議額外增加的關鍵項目：
  - 訂定資安稽核權行使
  - 訂定資料退場與銷毀機制
  - 明定違約罰則與損害賠償

服務水準協議（SLA）

系統可用率

- 訂定系統可用率指標，以確保系統維持一定服務水準。

安全性

- 藉由系統安全、通信安全、人員管制及作業管制等方式，達成安全性目標。
- 確保資通系統，包含軟體、硬體、防火牆、資料庫及電信通訊等之機密性與可用性。

稽核作業

- 透過持續不斷改善管理各項相關作業，來提升績效並符合需求。
- 如發現不符合事項時，訂定矯正或預防措施完成時限，追蹤稽核作業服務水準。

審查人員資格考量因素(續)

安全背景檢查

- 對委外廠商的人員進行安全背景檢查。
- 更詳細的核對，例如：信用核對或犯罪紀錄檢核
- 確保其在資訊系統中敏感資訊的處理，並確保他們沒有過去的安全違規行為。

評估培訓和知識轉移計劃

- 確保委外廠商提供適當的培訓計劃，以確保他們的人員能夠適應大學的需求並有效地營運和管理系統。
- 評估培訓計劃的內容、執行方式和評估機制。

引用檢查和參考客戶

- 與供應商合作的參考客戶提供了有關供應商的寶貴意見和評價。
- 可以請求供應商提供參考客戶，或通過其他途徑聯繫與供應商合作過的機構，以了解他們的經驗和評價。

簡報完畢
Thank you for your

陳俊茂 Charles Chen
charles@bccs.com.tw