|  |
| --- |
| 南投縣政府**附表十、資通系統防護基準控制措施查檢表(高級適用)** |
| **單位(處/科)** |  | **管理人** |  | **填表日期** |  |
| **系統名稱** |  | **防護需求等級** | **□高** |
| **建置廠商****統一編號** |  | **維護廠商****統一編號** |  |
| **系統版本****類別** | **□共用1 □公版2□機關自用 □其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**註1：共用：2個以上機關共同使用之系統 (如戶政、地政、財政、人事差勤系統)。註2：公版：各機關依特定版本自行維運使用(如公務出國報告資訊網、電子公文系統)。 | **是否還有維護合約？****□無****□有，至\_\_\_\_\_\_\_\_為止** |
| **系統建置****方式** | **□自行委外 □租用服務 □購置套裝軟體****□自行開發 □主管/上級機關提供****□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

|  |
| --- |
| 1.**資通系統環境資訊** |
| **作****業****系****統** | □Windows，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □Mac OS，版本: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□Unix / Linux，版本: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □FreeBSD，版本: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□其他，名稱\_\_\_\_\_\_\_\_\_\_\_\_\_\_、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_註：請寫出「種類」和「版本號碼」，如**Windows**請寫 **2012 R2 Standard或Enterprise**、 **Linux**請寫**CentOS 6.8**、或其他，以利查出明確漏洞資訊。 |
| **程****式****語****言** | □C/C++，版本:\_\_\_\_\_\_\_\_\_\_ □C#，版本: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□Java，版本:\_\_\_\_\_\_\_\_\_\_ □JavaScript，版本:\_\_\_\_\_\_\_\_\_\_□Python，版本:\_\_\_\_\_\_\_\_\_\_ □PHP，版本:\_\_\_\_\_\_\_\_\_\_□Visual Basic .NET，版本: \_\_\_\_\_\_\_\_\_\_□其他，名稱\_\_\_\_\_\_\_\_\_\_\_\_\_\_、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_註：請填寫詳細版本，如**PHP**請寫**7.3.17**或其他，而非PHP 7。 |
| **Web****伺****服****器** | □無□有，放置地點：\_\_\_\_\_\_\_\_\_\_\_(如：機關機房、租用雲端機房、廠商代管等)□Apache HTTP Server、版本:\_\_\_\_\_\_\_\_\_\_ □Apache Tomcat Server，版本:\_\_\_\_\_\_\_\_\_\_□Microsoft IIS、版本：\_\_\_\_\_\_\_\_ □Nginx、版本:\_\_\_\_\_\_\_\_\_\_□其他，名稱\_\_\_\_\_\_\_\_\_、版本:\_\_\_\_\_\_\_\_\_ 、發行商\_\_\_\_\_\_\_\_\_註：請填寫詳細版本，如Tomcat請寫7.0.65或其他，而非Tomcat 7.0，**若使用陸資廠商發行的軟體請特別標註**。 |
| **資****料****庫** | □無□有，放置地點：\_\_\_\_\_\_\_\_\_\_\_ (如：機關機房、租用雲端機房、廠商代管等)□DB2、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_ □SQLite、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_□Oracle、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_ □MySQL、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_□PostgreSQL、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_ □Sybase、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_□Microsoft SQL Server、版本: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□其他，名稱\_\_\_\_\_\_\_\_\_、版本: \_\_\_\_\_\_\_\_\_ 、發行商\_\_\_\_\_\_\_\_\_註：請填寫詳細版本，如Oracle Database請寫12.1.0.1，而非僅寫12，**若使用陸資廠商發行的軟體請特別標註**。 |
| **網****站****框****架** | □無□有，□Struts、版本:\_\_\_\_\_\_\_\_\_\_\_ □Spring、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_ □Laravel、版本:\_\_\_\_\_\_\_\_\_\_ □Django、版本:\_\_\_\_\_\_\_\_\_\_\_\_ □Swing、版本:\_\_\_\_\_\_\_\_\_\_\_ □Angular、版本:\_\_\_\_\_\_\_\_\_\_\_\_\_□.Net Framework、版本: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□其他，名稱\_\_\_\_\_\_\_\_、版本:\_\_\_\_\_\_\_\_ 、發行商\_\_\_\_\_\_\_\_\_註：請填寫詳細版本，**若使用陸資廠商發行的框架請特別標註**。 |

| **軟****體****元****件****清****單****軟****體****元****件****清****單** | 元件名稱 | 版本 | 發行/維護團隊 | 是否有正式授權 |
| --- | --- | --- | --- | --- |
| 範例：log4j | 2.4 | Apache | Apache License 2.0 |
| 範例：Bootstrap | 5.1.0 | Bootstrap Core Team | The MIT License |
| 範例：jQuery | 3.6.0 | jQuery Team | The MIT License |
| 範例：Ckeditor | 5 | CKSource | GPLv3 |
| 範例：ClosedXML | 0.95.1 | 開源元件 | The MIT License |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 註：**範例請自行刪除**，表格不敷使用請自行增加或附件方式，版本請參考範例填寫詳細，**若使用陸資廠商提供的元件請特別標註**。 |
| **系****統****使****用****連****接****埠****清****單** | 範例：80/HTTP |  |  |  |  |
| 範例：443/HTTPS |  |  |  |  |
| 範例：22/SSH |  |  |  |  |
| 範例：3306/MySQL |  |  |  |  |
| 範例：3389/RDP |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 註：**範例請自行刪除**，表格不敷使用請自行增加或附件方式，**請詳細填寫包含Web伺服器、資通系統本身、資料庫等所需要使用到的連接埠及協定**。 |
| **帳****戶****管****理****系****統** | □系統自行管理 □Active Directory □LDAP Server □Single Sign-On□自然人憑證或其他卡式憑證 □生物辨識 □其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **是****否****提****供****API****介****接****服****務** | □是，並依照數位發展部之[共通性應用程式介面指引](https://file.data.gov.tw/content/about/%E5%85%B1%E9%80%9A%E6%80%A7%E6%87%89%E7%94%A8%E7%A8%8B%E5%BC%8F%E4%BB%8B%E9%9D%A2%E6%8C%87%E5%BC%95.pdf)辦理□否 |
| **是****否****含****有****機****敏****資****料** | ※技服中心管考系統填報項目，請自行評估是否填寫，如不填寫請略過□是，包含(可複選)：□一般個資(如：員工或民眾姓名、電話、電子郵件、身分證字號等)□特種個資(個資法第6條定義) □師生個資 □稅務資料 □心理輔導諮商資料□其他\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□否 |
| **是****否****與****民****生****權****益****有****關** | ※技服中心管考系統填報項目，請自行評估是否填寫，如不填寫請略過□是(如：租賃、稅務、教育、求職就業、社會福利、醫療、考試等)□否 |
| **是****否****備****妥****流****量****清****洗****機****制** | ※技服中心管考系統填報項目，請自行評估是否填寫(擇一)，如不填寫請刪除□是，自行建置流量清洗設備及機制□是，網站租用CDN服務，並具備流量清洗機制□是，已委託GSN、電信業者於需要時提供流量清洗服務□否，無任何清洗機制□否，非對外系統□由其他機關營運，本單位僅使用 |
| **是****否****備****妥****CDN****啟****用****作****業****程****序** | ※技服中心管考系統填報項目，請自行評估是否填寫(擇一)，如不填寫請刪除□是，已租用CDN服務並建立啟用作業程序或流程□否，尚無此作業程序□否，非對外系統□由其他機關營運，本單位僅使用 |
| **是****否****備****妥****靜****態****網****頁** | ※技服中心管考系統填報項目，請自行評估是否填寫(擇一)，如不填寫請刪除□是，且可以於10分鐘內切換至靜態網頁□是，但無法於10分鐘內切換至靜態網頁□否，無靜態網頁、但有備份/備援機制□否，無任何機制□否，非對外系統□由其他機關營運，本單位僅使用 |

| 資通系統防護基準控制措施**(填寫欄位若不敷使用請自由修改或以附件方式作業)** |
| --- |
| **高級**系統適用項目 |
| **類別** | **安全控制措施** | **機關檢視結果** |
| 存取控制(1~5) | 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。

(帳號管理)(管考系統驗證代碼:C0101) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，勾選下列已具備之程序：□帳號申請□帳號建立□帳號修改□帳號啟用□帳號停用□帳號刪除不具備之程序改善規劃：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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。(遠端存取)

(管考系統驗證代碼:C0103) | □**符合**，已建立遠端存取申請流程及表單□ 其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 使用者之權限檢查作業應於伺服器端完成。(遠端存取)

(管考系統驗證代碼:C0103) | □**符合**，權限檢查作業已於伺服器端完成□ 其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應監控遠端存取機關內部網段或資通系統後臺之連線。(遠端存取)

(管考系統驗證代碼:C0103) | □**符合**，已利用資安設備或服務對內部使用者(含外點單位、維護廠商)允許自遠端來源存取內部網段或資通系統後臺**(含AP前後台、DB、OS)**之行為進行監控並留下記錄，監控方法為**(擇一即可，可複選)**：□ 防火牆□ WAF(應用程式防火牆)□ IPS/IDS(入侵預防/偵測系統)□ SoC監控服務□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應採用加密機制。(遠端存取)

(管考系統驗證代碼:C0103) | □**符合**，請選擇實作措施**(請視情況單選或複選)**：□已申購政府或受信任的第三方SSL憑證並套用於資通系統□Windows環境啟用「需要安全的RPC通訊」組態設定□UNIX/Linux環境使用SSH加密連線方式□任何人遠端存取內部網段之服務採用VPN連線方式 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 事件日誌與可歸責性(6~13) | 1. 訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。(記錄事件)

(管考系統驗證代碼:C0201) | □**符合**，**日誌紀錄已有保存至少\_\_\_個月(含AP前後台、DB、OS)**□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(記錄事件)

(管考系統驗證代碼:C0201) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□已記錄帳號登出入事件，並定義\_\_\_\_\_\_\_\_\_\_為特定事件(如登入失敗、非辦公時間登入等，請依系統業務性質自行增加定義)□已記錄系統操作或錯誤事件，並定義\_\_\_\_\_\_\_\_\_\_為特定事件(如資料送出、輸入格式錯誤等，請依系統業務性質自行增加定義) □已記錄資料查詢或存取事件，並定義\_\_\_\_\_\_\_\_\_\_為特定事件(如資料搜尋、資料匯出等，請依系統業務性質自行增加定義)□其他已定義及記錄之特定事件：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應記錄資通系統管理者帳號所執行之各項功能。(記錄事件)

(管考系統驗證代碼:C0201) | □**符合**，已記錄資通系統管理者/特權帳號所執行之各項功能記錄**(含AP前後台、DB、OS)**□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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，採用單一的日誌機制，確保輸出格式的一致性，並應依資通安全政策及法規要求納入其他相關資訊。(日誌紀錄內容)

(管考系統驗證代碼:C0202) | □**符合**，已達成控制措施所述項目**且未混用NLog與Log4Net等Log工具** □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，請勾選已實作項目：□事件類型(登出/入、修改、刪除等)□發生時間□發生位置(IP/設備名稱)□使用者身分識別(帳號名稱、權限等)□採用單一日誌機制**且未混用NLog與Log4Net等Log工具**□已依評估及納入其他相關日誌資訊不具備之項目改善規劃：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 依據日誌儲存需求，配置所需之儲存容量。(日誌儲存容量)

(管考系統驗證代碼:C0203) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□儲存於本機/儲存設備/log伺服器(擇一)日誌檔案總保存容量 \_\_\_\_\_MB/GB/TB日誌檔案之儲存空間可用容量 \_\_\_\_ ％□儲存於系統資料庫日誌紀錄資料表容量 \_\_\_\_\_\_MB/GB/TB資料庫儲存空間可用容量 \_\_\_\_\_ ％□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 資通系統於日誌處理失效時，應採取適當之行動。(日誌處理失效之回應)

(管考系統驗證代碼:C0204) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□透過\_\_\_\_\_\_\_\_\_方式(如信件、簡訊)通知管理人員並停止產出日誌□透過\_\_\_\_\_\_\_\_\_方式(如信件、簡訊)通知管理人員並覆寫最舊的日誌檔案□透過\_\_\_\_\_\_\_\_\_方式(如信件、簡訊)通知管理人員並全系統關閉□透過\_\_\_\_\_\_\_\_\_方式(如信件、簡訊)通知管理人員並部分系統關閉或有限的功能降級運作□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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)。(時戳及校時)

(管考系統驗證代碼:C0205) | □**符合**，系統日誌時戳與**系統內部時鐘(可對應UTC或GMT)**一致□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 對日誌之存取管理，僅限於有權限之使用者。(日誌資訊之保護)

(管考系統驗證代碼:C0206) | □**符合**，資通系統日誌僅限以下人員調閱，**並存有授權紀錄文件** **(擇一即可，可複選)：** □系統管理者 □系統維護廠商 □管理權責單位主管授權之使用者 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 營運持續計畫(14、15) | 1. 訂定系統可容忍資料損失之時間要求。(系統備份)

(管考系統驗證代碼:C0301) | □**符合**，**資料備份週期**為：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 執行系統源碼與資料備份。(系統備份)

(管考系統驗證代碼:C0301) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，請勾選已實作項目：□系統源碼備份□資料備份不具備之項目改善規劃：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明(如合約允許廠商可不提供系統源碼)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 識別與鑑別(16~24) | 1. 資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。(內部使用者之識別與鑑別)

(管考系統驗證代碼:C0401) | □**符合**，系統僅提供單位內部使用，並已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 使用預設密碼登入系統時，應於登入後要求立即變更。(身分驗證管理)

(管考系統驗證代碼:C0402) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明(如未有預設密碼)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 身分驗證相關資訊不以明文傳輸。(身分驗證管理)

(管考系統驗證代碼:C0402) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□使用安全之傳輸協定，如:TLS1.2□使用適當之加密演算進行傳輸□使用適當之雜湊演算進行傳輸□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(身分驗證管理)

(管考系統驗證代碼:C0402) | □**符合**，請勾選實作方式(單選)：□如控制措施所述之方式□機關自建之失敗驗證機制，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(對非內部使用者，可以機關自行規範辦理。) (身分驗證管理)

(管考系統驗證代碼:C0402) | □**符合**，已實施所述控制措施**(下列項目請勾選及填寫)**強制最低密碼複雜度：□\_\_字元□英文大小寫□數字□符號強制密碼最短效期 \_\_\_\_\_ 天(效期期間內無法變更，建議不超過1天)強制密碼最長效期 \_\_\_\_\_ 天(效期過後必須變更，建議不超過6個月) □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，請勾選已實作項目： □啟用最低密碼複雜度 □啟用密碼最短效期 □啟用密碼最長效期不具備之項目改善規劃：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 密碼變更時，至少不可以與前3次使用過之密碼相同。(身分驗證管理)

(管考系統驗證代碼:C0402) | □**符合**，**機關內**已實施控制措施所述項目 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 上述兩點(20、21)所定措施，對非內部使用者，可依機關自行規範辦理。(身分驗證管理)

(管考系統驗證代碼:C0402) | □**符合，**請勾選實作方式**(單選)**：□本系統僅提供內部使用者存取□已針對外部使用者之密碼管理自行訂定規範□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 資通系統應遮蔽鑑別過程中之資訊。(鑑別資訊回饋)

(管考系統驗證代碼:C0403) | □**符合**，於輸入密碼時顯示\*號、˙號或空白等隱碼或遮蔽方式，**且不會將帳號密碼顯露於網址列**□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 資訊系統應識別及鑑別非機關使用者(或代表機關使用者行為的程序)。(非內部使用者之識別與鑑別)

(管考系統驗證代碼:C0404) | □**符合**，系統有提供對外服務(如外單位、民眾)，並已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 系統與服務獲得(25~33) | 1. 針對系統安全需求(含機密性、可用性、完整性)進行確認。(系統發展生命週期需求階段)

(管考系統驗證代碼:C0501) | □**符合**，請勾選實作方式**(擇一即可，可複選)**： □參考行政院技服中心參考指引－安全軟體發展流程指引實作控制措施進行確認 □參考行政院技服中心－資通系統委外開發RFP資安需求範本(V2.0)-附件1資通系統資安需求項目檢核表進行檢核 □利用資通安全責任等級辦法附表九－資通系統防護需求等級原則進行確認□以內部管理制度流程進行需求評估及確認 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應針對安全需求實作必要控制措施。(系統發展生命週期開發階段)

(管考系統驗證代碼:C0503) | □**符合**，請勾選實作方式**(擇一即可，可複選)**： □已參考行政院技服中心參考指引－安全軟體發展流程指引實作控制措施進行實作**及追蹤管理** □已依照資通安全責任等級辦法附表十－資通系統防護基準控制措施進行實作**及追蹤管理** □使用資通安全需求追蹤矩陣(SRTM)進行追蹤管理 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應注意避免軟體常見漏洞及實作必要控制措施。(系統發展生命週期開發階段)

(管考系統驗證代碼:C0503) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□已參考行政院技服中心參考指引－安全軟體發展流程指引實作控制措施進行實作□已透過資安工具或其他檢測方式及修補OWASP TOP10或CWE/SANS TOP 25 漏洞□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(系統發展生命週期開發階段)

(管考系統驗證代碼:C0503) | □**符合**，請勾選實作方式**(擇一即可，可複選)**： □已設定僅顯示簡短錯誤訊息及代碼 □已設定導向另行設計之錯誤畫面 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 執行「弱點掃描」安全檢測。(系統發展生命週期測試階段)

(管考系統驗證代碼:C0504) | □**符合**，已於系統測試階段進行弱點掃描、並將\_\_\_風險以上(含)之弱點進行修補□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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(系統發展生命週期部署與維運階段)

(管考系統驗證代碼:C0505) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，請勾選已實作項目： □作業系統、軟體元件皆已更新至最新版 □已關閉並管制無申請之服務及埠口不具備之項目改善規劃： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 資通系統不使用預設密碼。(系統發展生命週期部署與維運階段)

(管考系統驗證代碼:C0505) | □**符合**，資通系統未使用任何預設密碼□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明(如無預設密碼機制)： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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。(系統發展生命週期委外階段)

(管考系統驗證代碼:C0506) | □**符合**，已將控制措施所描述要求加入合約□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明(如未委外維護)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應儲存與管理系統發展生命週期之相關文件。(系統文件)

(管考系統驗證代碼:C0508) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 系統與資訊完整性(34、35) | 1. 系統之漏洞修復應測試有效性及潛在影響，並定期更新。(漏洞修復)

(管考系統驗證代碼:C0701) | □符合，已實施此控制措施，**範圍包含但不限於**作業系統、應用程式伺服器、開發框架及第三方元件**(擇一即可，可複選)**：□每\_\_\_\_天 **手動或透過自動方式(如WSUS)**進行更新，並**留有修補及相關測試記錄**□每\_\_\_\_天 配合**弱點掃描、滲透測試或源碼檢測結果將\_\_\_風險以上(含)**或修補建議進行修補更新作業，並**留有修補及相關測試記錄(對照第29項)**□每\_\_\_\_天 配合**政府機關資安弱點通報機制(VANS)**進行**檢視及修補**，並**留有修補及相關測試紀錄**□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，請勾選已實作項目：□已定期檢視系統漏洞並執行更新修補作業□已於測試環境/備機進行修補測試並留有**測試記錄**不具備之項目改善規劃： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 發現資通系統有被入侵跡象時，應通報機關特定人員。(資通系統監控)

(管考系統驗證代碼:C0702) | □**符合**，當發生資通系統入侵事件，依內部程序通報機關所指定之人員□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| **中、高級**以上系統適用項目**(填寫欄位若不敷使用請自由修改或以附件方式作業)** |
| --- |
| **類別** | **安全控制措施** | **機關檢視結果** |
| 存取控制(36~40) | 1. 已逾期之臨時或緊急帳號應刪除或禁用。(帳號管理)

(管考系統驗證代碼:C0101) | □**符合**，臨時帳號或緊急帳號之**使用效期**為 \_\_\_\_ 天**請勾選逾期之臨時或緊急帳號處置方法：**□每\_\_\_\_天**定期人工審查**已逾期之臨時或緊急帳號□每\_\_\_\_天**系統自動**刪除或禁用□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 資通系統閒置帳號應禁用。(帳號管理)

(管考系統驗證代碼:C0101) | □**符合**，帳號如超過 \_\_\_\_ 天 **未登入**，視為閒置帳號**請勾選逾期之閒置帳號處置方法：**□每\_\_\_\_天**定期人工審查**閒置帳號並禁用□每\_\_\_\_天**系統自動**禁用閒置帳號□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。(帳號管理)

(管考系統驗證代碼:C0101) | □**符合**，請勾選實作方式**(單選)**：□每\_\_\_\_天**人工進行**系統帳號清查作業**(對照第37、38項)**□每\_\_\_\_天**系統自動審核**系統帳號，並**具備通知機關授權人員結果**之機制□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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。(最小權限)

(管考系統驗證代碼:C0102) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(遠端存取)

(管考系統驗證代碼:C0103) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□已透過內部申請機制(例如：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進行限制)□利用資安設備或軟體進行遠端存取來源控制(如設定黑、白名單)□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 事件日誌與可歸責性(41~43) | 1. 應定期審查機關所保留資通系統產生之日誌。(記錄事件)

(管考系統驗證代碼:C0201) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□\_\_\_天 完成至少1次人工審查系統日誌並**留有審查記錄**□已建置日誌記錄管理系統，並\_\_\_天自動審查並產製報表後**由指定人員對報表進行審查及核章**□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 系統內部時鐘應定期與基準時間源進行同步。(時戳及校時)

(管考系統驗證代碼:C0205) | □**符合**，請勾選實作方式(單選)： □統一與**機關自建NTP Server**同步IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □統一使用**外部/上級機關提供之NTP Server**同步 IP：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應運用雜湊或其他適當方式之完整性確保機制。(日誌資訊之保護)

(管考系統驗證代碼:C0206) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□利用雜湊函數、同位元檢查或循環冗餘檢查等技術進行新舊值比對□利用壓縮加密並異地備份確保完整性□**以可合法使用或授權之目錄檔案監控工具偵測**日誌異動□將日誌以CD-ROM/DVD-ROM或其他具唯讀特性的儲存媒體進行保存□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 營運持續計畫(44~46) | 1. 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。(系統備份)

(管考系統驗證代碼:C0301) | □**符合**，請勾選實作方式**(擇一即可，可複選)**： □每\_\_\_\_天 **手動測試**系統及資料備份 □備份系統每\_\_\_\_天 **自動測試**並產報表 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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。(系統備援)

(管考系統驗證代碼:C0302) | □**符合**，系統最大可容忍中斷時間為\_\_\_\_小時□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(系統備援)

(管考系統驗證代碼:C0302) | □**符合**，已建置備援設備或其他備援機制、或適當方式(如人工作業)取代並提供服務□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 識別與鑑別(47~49) | 1. 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。(身分驗證管理)

(管考系統驗證代碼:C0402) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□登入頁面設置CAPTCHA驗證碼機制□監控異常登入行為並封鎖來源IP或將帳戶鎖定□使用雙因子驗證機制(信件驗證碼、APP或實體驗證器產生一次性密碼)□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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(Token)。(身分驗證管理)

(管考系統驗證代碼:C0402) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□寄發**EMAIL驗證連結**，時效\_\_\_\_\_(EX:5分)□寄發**簡訊驗證碼**，時效\_\_\_\_\_(EX:5分)□僅接受使用者本人臨櫃辦理重設作業□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□不適用，請說明(如使用AD服務)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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。(加密模組鑑別)

(管考系統驗證代碼:C0404) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□密碼經加密(如AES 256bit、RSA 2048bit)儲存□密碼經雜湊(如SHA-256、ECDSA)儲存□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 系統與服務獲得(50~53) | 1. 根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估。(系統發展生命週期設計階段)

(管考系統驗證代碼:C0502) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：**□使用機關內部風險評鑑程序進行分析**□使用誤用模型(Misuse case)進行風險分析□參考微軟提出之威脅建模(Threat Modeling)□以STRIDE方法進行威脅分析□以DREAD風險計算方法進行風險分析□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(系統發展生命週期設計階段)

(管考系統驗證代碼:C0502) | □**符合**，已於系統設計階段進行風險評鑑作業，並將須修正項目納入開發需求□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(系統發展生命週期部署與維運階段)

(管考系統驗證代碼:C0505) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□以內部管理制度之表單或其他紀錄方式進行版本控制與變更管理□以\_\_\_\_\_軟體(如：SVN、Git)進行版本控制與變更管理□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 開發、測試及正式作業環境應作區隔。(獲得程序)

(管考系統驗證代碼:C0507) | □**符合**，已將開發、測試及正式作業環境利用**實體設備**或**網段獨立**進行區隔□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 系統與資訊完整性(54~58) | 1. 定期確認資通系統相關漏洞修復之狀態。(漏洞修復)

(管考系統驗證代碼:C0701) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□每\_\_\_\_天 **人工確認**漏洞資訊並修補□已建置資通全弱點通報機制(VANS) □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。(資通系統監控)

(管考系統驗證代碼:C0702) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□使用IPS、WAF等資安設備進行監控□使用SoC服務 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 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。(軟體及資訊完整性)

(管考系統驗證代碼:C0703) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□使用**自行開發**之完整性驗證工具□**以可合法使用或授權之目錄檔案監控工具**進行偵測作業□使用雜湊函數、同位元檢查或循環冗餘檢查等技術□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。(軟體及資訊完整性)

(管考系統驗證代碼:C0703) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(軟體及資訊完整性)

(管考系統驗證代碼:C0703) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□通知管理者並暫時關閉系統□通知管理者並封鎖異常行為來源IP□通知管理者並實施內部訂定之保護措施□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| **高級**系統適用項目**(填寫欄位若不敷使用請自由修改或以附件方式作業)** |
| --- |
| **類別** | **安全控制措施** | **機關檢視結果** |
| 存取控制(59~62) | 1. 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。(帳號管理)

(管考系統驗證代碼:C0101) | □**符合**，已達成控制措施，填寫下列項目：□已定義系統閒置時間\_\_\_\_\_(EX:30分)□已定義系統可使用期限\_\_\_\_\_(EX:30分)□已定義系統之其他使用情況及條件，請勾選下列已定義項目，可複選：□帳號類型□功能限制□操作時段限制□來源位址□連線數量□存取資源□其他條件：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，請勾選及填寫已實作項目：□已定義系統閒置時間\_\_\_\_\_(EX:30分)□已定義系統可使用期限\_\_\_\_\_(EX:30分)□已定義系統之其他使用情況及條件，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。 不具備之項目改善規劃：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(帳號管理)

(管考系統驗證代碼:C0101) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□超過閒置時間之帳號，系統將自動登出□超過可使用期限之帳號，系統將自動登出 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應依機關規定之情況及條件，使用資通系統。(帳號管理)

(管考系統驗證代碼:C0101) | □**符合**，已依照控制措施58項次所定義之情況及條件使用資通系統 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 監控資通系統帳號，如發現帳號違常使用時回報管理者。(帳號管理)

(管考系統驗證代碼:C0101) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□已透過**資安設備(如WAF)**監控□已透過**資安服務(如SoC服務)**監控□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_監控發現異常時，請勾選向管理者回報方式**(擇一即可)**：□透過**人工回報**□於系統操作頁面顯示警告畫面□寄送警示信件或簡訊□其他回報方式：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 事件日誌與可歸責性(63~64) | 1. 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。(日誌處理失效之回應)

(管考系統驗證代碼:C0204) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，請勾選已實作項目：□已定義**需即時通報**之日誌處理失效事件，如：日誌紀錄儲存空間已滿載或無法連線造成日誌寫入失敗等□當發生時系統於\_\_\_\_小時內已Email等方式回報機關指定之管理人員不具備之項目改善規劃：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 定期備份日誌至原系統外之其他實體系統。(日誌資訊之保護)

(管考系統驗證代碼:C0206) | □**符合**，請勾選實作方式**(擇一即可，可複選)**： □每\_\_\_\_天 **手動備份**至原系統外之設備 □每\_\_\_\_天 **自動備份**至Log伺服器□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 營運持續計畫(65、66) | 1. 應將備份還原，作為營運持續計畫測試之一部分。(系統備份)

(管考系統驗證代碼:C0301) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(系統備份)

(管考系統驗證代碼:C0301) | □**符合**，已建立異地備份機制□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 識別與鑑別(67) | 1. 對資通系統之存取採取多重認證技術。(內部使用者之識別與鑑別)

(管考系統驗證代碼:C0401) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□使用自然人憑證或晶片卡□使用生物特徵，如指紋、臉部□使用雙因子驗證機制(信件驗證碼、APP或實體驗證器產生一次性密碼)□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 系統與服務獲得(68~70) | 1. 執行「源碼掃描」安全檢測。(系統發展生命週期開發階段)

(管考系統驗證代碼:C0503) | □**符合**，於開發階段執行系統源碼掃描並依結果修復漏洞□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 系統應具備發生嚴重錯誤時之通知機制。(系統發展生命週期開發階段)

(管考系統驗證代碼:C0503) | □**符合**，請勾選實作方式**(擇一即可，可複選)**： □使用自動化監控系統進行偵測並通知(如SoC服務) □已針對系統嚴重錯誤以Email通知 □已針對系統嚴重錯誤以電話語音或簡訊通知 □其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 執行「滲透測試」安全檢測。(系統發展生命週期測試階段)

(管考系統驗證代碼:C0504) | □**符合**，於測試階段執行滲透測試，並依結果修復漏洞□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 系統與通訊保護(71~76) | 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。(傳輸之機密性與完整性)

(管考系統驗證代碼:C0601) | □**符合**，請勾選實作方式**(擇一即可，可複選)**： □系統啟用HTTPS傳輸協定，且使用TLS1.2以上(含)版本安全協定□系統啟用HSTS(HTTP強制安全傳輸技術)確保所有傳輸過程強制使用HTTPS□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 使用公開、國際機構驗證且未遭破解的演算法。(傳輸之機密性與完整性)

(管考系統驗證代碼:C0601) | □**符合**，請勾選實作方式**(擇一即可，可複選)**： □使用AES 256bit、RSA 2048bit等加密演算□使用SHA-256、ECDSA等雜湊演算□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 支援演算法最大長度金鑰。(傳輸之機密性與完整性)

(管考系統驗證代碼:C0601) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 加密金鑰或憑證應定期更換。(傳輸之機密性與完整性)

(管考系統驗證代碼:C0601) | □**符合**，於加密金鑰或憑證過期前 \_\_\_\_ 天更換□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 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。(傳輸之機密性與完整性)

(管考系統驗證代碼:C0601) | □**符合**，已達成控制措施所述項目□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**部分符合**，請勾選已實作項目：□已訂定加密金鑰管理規範 □已實施應有之加密金鑰安全防護措施，如存放位置與存取權限、使用期限查檢等不具備之項目改善規劃：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明(如已過設計階段)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。備註：資通系統重要組態設定檔案，例如Web伺服器設定檔、資料庫設定檔等。(資料儲存之安全)

(管考系統驗證代碼:C0602) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□已將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□已將資通系統重要組態設定檔案及其他具保護需求之資訊以其他適當方式儲存**(勾選此項請於下方填寫儲存方式)**儲存方式：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 系統與資訊完整(77、78) | 1. 資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。(資通系統監控)

(管考系統驗證代碼:C0702) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□使用IPS、IDS、WAF、UTM或WAF等資安設備**自動即時監控並產製分析報告**□將資安設備之事件偵測日誌導向SoC服務進行監控並分析□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 1. 應定期執行軟體與資訊完整性檢查。(軟體及資訊完整性)

(管考系統驗證代碼:C0703) | □**符合**，請勾選實作方式**(擇一即可，可複選)**：□每\_\_\_\_天 使用**自行開發之完整性驗證工具**進行檢查□每\_\_\_\_天 **以可合法使用或授權之目錄檔案監控工具以可合法使用或授權之目錄檔案監控工具**自動執行檢查□其他措施：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不符合**，相關改善措施(方式/時間)：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□**不適用**，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 系統管理單位負責人員 | ： |  | 系統管理單位主管 | ： |  |