

國立故宮博物院 115 年度單位預算評估報告

國立故宮博物院(以下簡稱故宮)115 年度預算案歲入編列 6 億 6 萬 4 千元，較 114 年度預算數 6 億 752 萬 9 千元，減少 746 萬 5 千元(減幅 1.23%)；歲出編列 29 億 6,564 萬元，較 114 年度預算數(含追加預算，以下同)31 億 9,179 萬 7 千元，減少 2 億 2,615 萬 7 千元(減幅 7.09%)。謹就故宮 115 年度預算案評估如下：

四、近年故宮偶有資安事件，允宜檢討作業程序，確實依資訊安全管理規範執行各項資安管控措施，並定期稽核與監督，以維資訊安全

故宮 115 年度預算案「綜合規劃與推廣行銷」計畫編列 2 億 3,420 萬 9 千元、「文物安全、管理與修護」計畫編列 1 億 5,142 萬 1 千元。經查：

(一)115 年度預算案資安相關經費主要係辦理中央控制安全監控系統之資訊操作維護及資訊安全管理制度委外建置與驗證等

故宮 115 年度預算案於「綜合規劃與推廣行銷」及「文物安全、管理與修護」計畫項下編列資安相關經費計 1,121 萬 2 千元，主要編列內容如下：

1. ISMS 資訊安全管理制度委外建置與驗證 180 萬元。
2. 辦理南北院區資通安全威脅偵測管理(SOC)服務-高流量 160 萬元。
3. 辦理 VANS 系統、端點安全防護 EDR、SPAM SQR 垃圾郵件過濾、Virus SQR 電子郵件防毒、防毒暨端點安全防護、網路存取控制及 IP 位址管理等 150 萬元。
4. 辦理「打造 AI 智慧博物館共構數位涵容生態計畫」之 AI 智慧展示廳系統設備、客服系統、數位典藏系統與智慧化庫房系統開發等 135 萬元。

5. 辦理中央控制安全監控系統之資訊操作維護 463 萬元。
6. 文物典藏陳列空間建置 CCTV 雙迴路備援錄影儲存機制 33 萬 2 千元。

(二)近年故宮偶有未落實資通系統變更管理及作業環境控制措施等情事，允宜確實依資訊安全管理規範辦理

據審計部 112 年度中央政府總決算審核報告指出，故宮因應數位時代趨勢推動數位轉型，惟有未落實資通系統變更管理及作業環境控制措施等情事，包含：開發文物高階圖檔影像降階程式(以下簡稱影像降階程式)進行圖檔降階處理及開放於數位典藏系統供外界讀取，惟未依故宮資訊安全管理制度(Information Security Management System, ISMS)規範，落實辦理資通系統變更管理、區隔測試及正式作業環境等控制措施；持續進行網路資安架構調整，惟對下載交付使用之文物高階圖檔未實施保存與使用情形之追蹤查察，未於使用單位使用目的完成後要求刪除及銷毀，與故宮 ISMS 規範未合(詳表 1)。為降低機敏資料外洩與數位資產流失之風險，允宜落實資訊安全管理規範，嚴格控管存取權限、網路連通狀況並留存圖檔作業存取紀錄，並定期稽核與監督，以確保資訊安全。

表 1 近年故宮未落實資訊安全管理規範概況表

項目	內容摘要
1. 辦理文物數位化圖檔等資訊輸出入保存及加值運用，惟未依故宮 ISMS 規範，落實辦理資通系統變更管理、區隔測試及正式作業環境等控制措施	1. 故宮自 110 年開發影像降階程式，並置於內部伺服器使用，文物高階圖檔經降階處理後始開放於數位典藏系統供外界讀取，嗣因檔案降階作業之資料量過大處理費時，逕將影像降階程式移至對外服務伺服器，致遭人以自動化程式多次讀取局部高階圖像原始檔後，拼接成原圖販售，影響故宮智慧財產權利。 2. 又影像降階程式存取安全控制有以下情事： (1) 申請單位未填具資訊服務申請單經管理單位審核同意，即新增對外服務伺服器並將影像降階程式移至該伺服器。 (2) 故宮雖於文物高階圖檔外流事件發生後移除對外服務伺服器，並建置文物圖像上傳及調檔系統(以

項目	內容摘要
	下簡稱圖像上傳系統)採內部封閉式儲存設備及系統程式自動化處理作業，以阻絕文物高階圖檔外流風險，惟故宮於系統未上線前，即審核同意可自測試環境存取文物高階圖檔儲存區之權限，且有實際讀取紀錄。 (3)另故宮以圖像上傳系統屬內部網路使用且功能數量不多為由，未填具資訊服務申請單，於系統完成後即將測試環境轉換為正式環境之組態變更設定等。
2. 持續進行資訊網路資安架構調整，惟對下載交付使用之文物高階圖檔未實施保存與使用情形之追蹤查察，未於使用單位使用目的完成後要求刪除及銷毀	故宮文物高階圖檔外流事件發生後，雖已移除對外服務伺服器以阻絕文物高階圖檔外流風險，並強化存取權限控制及由專責管理人員依簽准之資訊服務申請單下載文物圖像數位原始檔案，交付申請單位，惟對下載後交付使用之文物圖像數位原始檔案，未實施保存及使用情形之追蹤查察，恐無法確保申請單位於授權使用目的之範圍內使用及未任意進行檔案複製或保留；亦未追蹤使用單位於使用目的完成後有無進行檔案刪除與銷毀。

資料來源：整理自 112 年度中央政府總決算審核報告。

綜上，近年故宮偶有未落實資通系統變更管理及作業環境控制措施等情事，允宜檢討作業程序，確實依資訊安全管理規範辦理，以改善並強化資通安全管理。