資訊處
Office of Information Technology

教育部所屬公務機關資安稽核分享

報告人：薛雅芳

110年9月8日

大綱

- 教育部資安稽核流程
- 機關自評
- 技術稽核
- 實地稽核
- 問題與討論

教育部資安稽核流程

- 實地稽核前1個月收到公文通知
- 機關自評→技術稽核→實地稽核
- 每季稽核結束後教育部函送資安稽核報告，受稽機關需於一個月內函報改善計畫，後續依教育部審查結果定期提報執行情形

教育部「資通安全實地稽核」待改善及建議事項之矯正預防措施				
項次	分類	項目	發生原因／因應作為辦理情形	時程規劃日期
-	(範例) 技術面	(供填寫格式參考，請自行刪除) 依資通安全責任等級分級辦法應辦事項規定，查機關WSUS更新派送主機未納入SOC監控，建議將重要基礎服務系統納入SOC監控範圍。	(供填寫格式參考，請自行刪除) 一、發生原因： 本機關SOC現行監控範圍因經費因素，未納入部分重要基礎服務系統（如WSUS更新派送主機）。 二、因應作為辦理情形： (一)已規劃於109年12月31日前進行本部WSUS更新派送主機之日誌收容，並由承商協助進行全天候資安事件即時監控及分析。 (二)定期檢視SOC監控範圍之合理性，視需要擴大監控範圍。	109年12月31日

機關自評

- 以電子郵件回報以下資料，準備時間2週
  - ✓資通安全實地稽核項目檢核表(適用公務機關)
  - ✓受稽機關現況調查表
  - ✓技術檢測基本資料調查表
  - ✓核心資通系統調查表
- 實地稽核2週前回報資安現況簡報(15分鐘)

機關自評階段作業-1

- 召開說明會
  - ✓說明技術檢測要求及評分標準
  - ✓調查技術檢測基本資料調查表
    - GCB例外管理清單：資安責任等級C級公務機關免辦
    - IoT設備清單
  - ✓調查使用者電腦清單
  - ✓調查資通安全通識課程受訓情形

機關自評階段作業-2

- 執行全機關資訊設備系統弱點掃描及網站弱點掃描
  - ✓不以資安設備及網路設備阻擋
  - ✓系統弱點掃描建議執行All port scan
  - ✓網站弱點掃描建議以核心資通系統及新建資通系統優先
  - ✓中風險以上漏洞都需修補
    - 防毒軟體使用之自簽憑證可免修補
- 其他建議
  - ✓核心資通系統執行內網滲透測試
  - ✓教育部稽核計畫建議執行資安健診

技術稽核作業說明-1

- 檢核項目範圍為全機關，挑選行政單位、教學單位(系所)及計畫單位各1個

項次	檢測項目	子項目	配分	資訊單位	行政單位	教學單位	計畫單位
				40%	20%	20%	20%
1-1	使用者電腦安全檢測	弱點掃描	10	20台	10台	10台	10台
1-2		安全防護	20	2台	1台	1台	1台
2	網路惡意活動檢測		5	單位網段	單位網段	單位網段	單位網段
3-1	核心資通系統安全檢測	滲透測試	20	1個			
3-2		防護基準	5				
4	網路架構檢測		15	網路架構	網路架構	網路架構	網路架構
5	目錄伺服器安全檢測		10	1台	1台	1台	1台
6	物聯網設備安全檢測		10	2台	1台	1台	1台
7	組態設定安全檢測		5	2台主機	1台電腦	1台電腦	1台電腦

技術檢核作業說明-2

- 稽核時程：2天
- 稽核團隊：教育體系資安檢核技術服務中心(陽明交通大學)檢核員6~8名及工作人員數名
- 準備事項：
  - ✓提供會議室、檢核場地及網路連線環境
  - ✓整體網路實體架構圖、網路邏輯架構圖、系統連線實體架構圖等網路架構圖
  - ✓使用者電腦清單
  - ✓協助於出口端收取內外流量6小時，包含路由器出入流量Mirror port設定並提供收取流量設備

技術檢核原則

- 所有技術檢核均要求未受資安設備(防火牆、WAF)或網路設備(IP管理、ACL)阻擋
  - ✓要求提供與檢測標的相同網段之IP
  - ✓本機防火牆為合理之防護方式

技術檢核-使用者電腦安全檢測-弱點掃描

- 進行全網段連接埠掃描（port scan），藉由掃描結果挑選可能存在風險之使用者電腦進行弱點掃描
- 執行方式：
  - ✓使用Nessus Pro
  - ✓到被挑選單位連接該網段執行port scan及弱點掃描
- 事前準備：
  - ✓執行全機關(或重點單位)網段弱點掃描並修補中風險以上漏洞
  - ✓個人電腦作業系統更新至Windows 10
  - ✓關閉微軟遠端桌面連線或設定本機防火牆

技術檢核-使用者電腦安全檢測-安全防護-1

- 依弱點掃描結果挑選高風險及不同作業系統版本之使用者電腦進行深度檢測，其檢測項目包含防毒軟體、安全性修補程式更新、應用程式更新及惡意程式檢測
- 執行方式：
  - ✓檢查個人電腦是否安裝防毒軟體
  - ✓檢查防毒軟體病毒碼、Windows Update、JAVA、Adobe Reader、Adobe Flash Player及Microsoft Office等微軟應用程式應用程式是否更新至官網最新版
  - ✓檢測個人電腦是否有惡意程式
  - ✓GCB規則導入情形

技術檢核-使用者電腦安全檢測-安全防護-2

- 事前準備：
  - ✓安裝防毒軟體，並將防毒軟體病毒碼、Windows Update、JAVA、Adobe Reader、Adobe Flash Player及Microsoft Office等微軟應用程式應用程式更新至最新版
  - ~~✓完成GCB規則導入設定~~
  - ✓注意久未開機的個人電腦，務必完成相關防護措施
- 其他建議：
  - ✓惡意程式檢測可透過資安健診服務執行
    - 或使用微軟惡意軟體移除工具(MSRT)及Sysinternals等免費工具執行

技術檢核-網路惡意活動檢測

- 依照行政院國家資通安全會報技術服務中心每週公布之惡意中繼站名單，針對機關使用者網段及核心系統管理員網段進行檢測
- 執行方式：
  - ✓收取出口端內外流量6小時進行分析
  - ✓於各單位網段檢測可否以ICMP協定連線惡意中繼站IP
  - ✓於各單位網段檢測可否以DNS解析惡意中繼站DN取得IP
- 事前準備：
  - ✓取得技術服務中心稽核當週最新名單

技術檢核-核心資通系統安全檢測-滲透測試-1

- 進行內網滲透測試，其檢測項目包含資通系統之權限存取、應用程式及系統弱點、系統通訊保護等，若資通系統使用單一簽入進行權限控管，則亦納入檢測範圍
- 執行方式：
  - ✓使用與核心資通系統同網段IP進行檢測，中間需無防護設備阻擋
  - ✓如資通系統需使用帳號密碼登入，需提供測試用帳號(前後台均需提供)
  - ✓檢測使用工具包含Nessus Pro、Acunetix、OpenVAS、ZAP、metasploit

技術檢核-核心資通系統安全檢測-滲透測試-2

- 事前準備：
  - ✓使用教育單位弱點檢測平台(EVS平台)進行弱點掃描
  - ✓檢測範圍不僅限於核心資通系統，其介接的單一登入系統、FTP Server等週邊系統設備均應納入檢測

- 其他建議
  - ✓委託廠商執行滲透測試時，建議採到場檢測模式

技術檢核-核心資通系統安全檢測-防護基準

- 依據系統等級(普中高)，針對核心資通系統之存取控制、識別與鑑別、系統與服務獲得、系統與資訊完整性及系統與通訊保護等控制措施進行檢測，並檢視源碼掃描、弱點掃描及滲透測試等檢測報告與修補紀錄，以及安全需求檢核結果
- 執行方式：
  - ✓針對核心資通系統調查表填報的資通系統防護基準實施情形抽查
- 事前準備：
  - ✓弱點掃描報告、滲透測試報告及修補紀錄

技術檢核-網路架構檢測-1

- 透過訪談與實際檢視方式驗證網路與系統之管理控制措施、網路與系統之安全控制措施、網路與系統架構之備援機制、防火牆規則及存取控制，並確認資通系統管理與防護情形
- 執行方式：
  - ✓網路架構訪談
  - ✓防火牆政策檢視
  - ✓稽核前全網段弱點掃描

技術檢核-網路架構檢測-2

- 事前準備：
  - ✓資通系統與設備應使用HTTPS連線，避免帳密明碼傳輸
  - ✓伺服器群主機執行弱點掃描並修補中風險以上漏洞，更新作業系統及使用新版套件
  - ✓重新檢視防火牆規則適切性，以最小開放為原則
    - 避免開放ANY to ANY服務
    - 伺服器群應限制SSH、RDP等遠端管理的來源IP
    - 正式環境與測試環境應依需求開放可連線來源
    - IoT設備存取控管，限制非必要開放的服務並僅限於校園內存取

技術檢核-目錄伺服器安全檢測

- 透過實際檢測方式，針對機關之網域主機進行防毒軟體、安全性修補程式更新及惡意程式檢測
- 執行方式：
  - ✓僅檢測Windows AD主機
- 事前準備：
  - ✓中正大學無AD主機，故本項未檢測

技術檢核-物聯網設備安全檢測-1

- 針對網路印表機、門禁系統、網路攝影機、無線網路基地台(AP)/無線路由器及環控系統等物聯網設備進行檢測，透過內部網路或臨機操作方式執行檢測作業，其檢測項目包含傳輸加密保護、身分鑑別與授權、用戶端與管理端網頁介面之安全性、軟體及韌體之安全性更新等
- 執行方式：
  - ✓使用Nessus弱點掃描
  - ✓臨機操作

技術檢核-物聯網設備安全檢測-2

- 事前準備：
  - ✓執行弱點掃描修補中風險以上漏洞
  - ✓韌體更新至最新版
  - ✓修改管理介面預設密碼
  - ✓限制可連線管理介面的來源IP
  - ✓建議關閉IPv6相關設定
  - ✓建議於防火牆限制非必要開放的服務並僅限於校園內存取

技術檢核-組態設定安全檢測

- 針對已公告之政府組態基準(GCB)項目，就網通設備、作業系統、瀏覽器及應用程式進行抽測
- 執行方式：
  - ✓依技術檢測基本資料調查表填寫導入項目抽測使用者電腦及網通設備
- 事前準備：
  - ✓填寫GCB例外管理清單
  - ✓確認終端設備已完成GCB相關設定

技術檢核-行政院110年資通安全稽核計畫增項

- 資料庫安全檢測
  - ✓透過訪談及實際檢視方式，抽測10項資料庫安全檢測項目，包含特權帳號管理、資料加密、備份保護、弱點管理、存取授權、稽核紀錄及委外管理等安全機制，確認資料庫安全管理與防護狀況

實地稽核作業說明-1

➢稽核範圍為全校

構面	稽核項目	配分
策略面	一、核心業務及其重要性	10
	二、資通安全政策及推動組織	10
	三、專責人力及經費配置	10
管理面	四、資訊及資通系統盤點及風險評估	10
	五、資通系統或服務委外辦理之管理措施	10
	六、資通安全維護計畫與實施情形之持續精進及績效管理機制	10
技術面	七、資通安全防護及控制措施	20
	八、資通系統發展及維護安全	10
	九、資通安全事件通報應變及情資評估因應	10

實地檢核作業說明-2

- 稽核時程：1天
- 稽核團隊：教育部長官領隊1名、教育機構資安驗證中心(中興大學)稽核員7名及工作人員數名
- 準備事項：
  - ✓提供會議室、檢核場地及網路連線環境
  - ✓啟始會議15分鐘資安現況簡報
  - ✓稽核相關佐證紀錄及文件(詳附件文件推薦準備列表)
    - 實際按稽核項目準備專卷
  - ✓建議資安長應出席啟始會議及結束會議
- 實地稽核報告於結束會議時當場確認

實地稽核重點

- 檢視是否完成資通安全管理法及相關規範要求事項
  - ✓是否訂定資通安全維護計畫及實施情形
  - ✓是否訂定資通安全事件通報及應變管理程序及實施情形
  - ✓資通安全責任等級分級辦法中各應辦事項實施情形
  - ✓資通系統分級及防護基準各控制措施辦理情形
    - 核心資通系統及新建資通系統為重點
  - ✓資通安全事件通報應變情形
    - 個資事件均屬3級資安事件
- 資安推動範圍是否擴及全校

實地稽核-策略面稽核重點

- 資通安全推動組織各單位參與情形
  - ✓建議資安推動組織擴大為全校各單位
- 管理審查會議參與人員是否涵蓋各單位；討論議案是否包含資通安全維護計畫所訂項目
- 資訊經費及資安經費編列比例
- 建立教育訓練管理機制，掌握各單位資通安全教育訓練實施情形
- 對全校教職員工（及各單位委外廠商及其人員）訂定切結保密協議並簽署

實地稽核-管理面稽核重點

- 資通系統及資訊資產盤點及風險評鑑方法論
  - ✓建議參考技術服務中心資通系統風險評鑑參考指引
- 依據「教育體系電子郵件服務與安全管理指引」，辦理公務業務或核心業務時，應使用學校配發之電子信箱收發公務所需資訊
- 電子郵件服務系統應辦理資通系統防護基準至少「中」以上之控制措施
- 資訊委外服務案廠商是否符合資通安全管理法施行細則第4條要求
  - ✓受託者應配置資通安全專業人員

實地稽核-技術面稽核重點

- 資安事件通報處理程序
- 各資通系統之防護基準控制措施實施情形
  - ✓遠端存取
  - ✓身分驗證管理
  - ✓漏洞修復-實地稽核前稽核員執行技術檢測
  - ✓系統與服務獲得(SSDLC)-針對新建資通系統之要求
- 政府組態基準設定(GCB)例外管理評估紀錄及檢討追蹤情形

實地稽核-行政院110年資通安全稽核計畫增項

- 管理面
  - ✓4.7 針對公務用之資通訊產品，包含軟體、硬體及服務等，是否已禁止使用大陸廠牌資通訊產品？
  - ✓4.8 是否列冊管理大陸廠牌資通訊產品，並明訂於 110 年底前完成汰換作業，且汰換前不得與公務環境介接？如有無法於期限內完成汰換或產品須與公務環境介接之情況，是否經行政院核定同意？
  - ✓5.16針對涉及資通訊軟體、硬體或服務相關之採購案，契約範圍內之委外廠商是否為大陸廠商或所涉及之人員是否有陸籍身分？是否允許委外廠商使用大陸廠牌之資通訊產品，包含軟體、硬體及服務等？

實地稽核-行政院110年資通安全稽核計畫增項

- 技術面
  - ✓7.5 機關參與本院資安會報對外資通系統實兵演練，是否就相關系統弱點訂定資安防護改善計畫，並落實執行？
  - ✓7.11是否完成資通安全弱點通報機制導入作業，並持續維運？

資訊處
Office of Information Technology

報告完畢、敬請指教