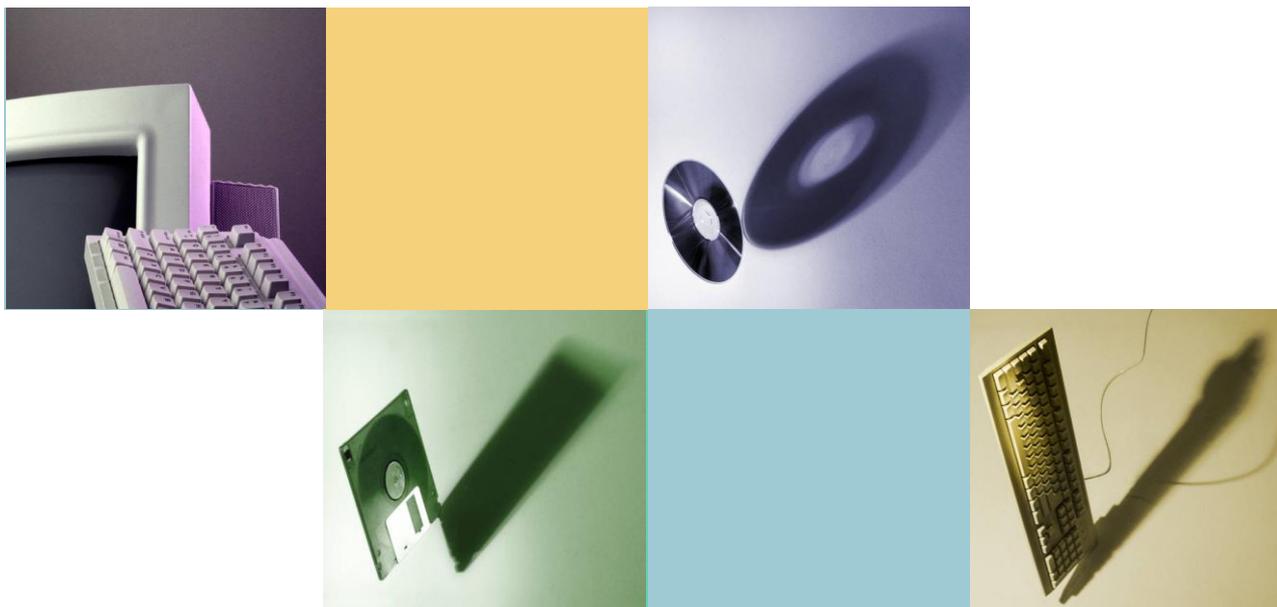


111年國立高中職學校資安實地稽核常見缺失



Thursday, Oct 27 2022

宜蘭大學 曾國旭

- C級學校無法避免的問題
 - 3.3 是否具備相關專業資安證照或認證？
 - 11.2 是否每兩年辦理一次資通安全健診？
 - 11.4 是否完成資通安全弱點通報機制導入作業？
- 上述項目為「資通安全責任等級分級辦法」附表五規定辦理事項，若無法降為D等級，就只能編經費完成(別忘了還有設置專職人員)



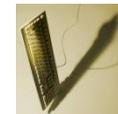
1. 資通安全政策之推動及目標訂定

- 1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？
 - 應加強監督資通安全目標推動情形之追蹤與改善，以落實資安推動事宜。(如何證明訂定之目標已達成→ISMS有效性量測表、管審會紀錄)
 - 「資通安全維護計畫」內容宜依學校現況進行調整。(如：核心系統最大可容忍中斷時間與資訊安全政策目標之關聯性、資安責任等級核定依據、執行資通安全健診)
 - 應定期審查「資通安全維護計畫」及「資通安全政策」(管審會紀錄，討論內容須遵循「資通安全維護計畫」中「三、資通安全維護計畫之持續精進及績效管理」所列之8項議題)



4. 資訊及資通系統之盤點及風險評估

- 4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？
 - 宜針對高風險資訊資產進行風險處理作業，並採取相對應之控制措施。
- 風險評鑑及管理必要步驟：
 - 資訊資產盤點(7大類)→資訊資產清單
 - 評估風險→威脅及弱點評估表
 - 訂定可接受風險值→會議紀錄(若沒有高風險資產，無須做風險處理)
 - 風險處理→風險評鑑彙整表(2份，含改善後再評鑑)、風險改善計畫表。
 - 產出「風險評鑑報告」(視程序書規定)



5. 資通安全管理措施之實施情況(1/5)

- 5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？
- 5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？
 - 應再評估設置機房CCTV錄影設備之必要性，以確保機房重要設備的保護。
 - 宜再評估CCTV錄影留存時間。(最好有6個月以上)
 - 宜再評估設置CCTV設置點，並避免放置易燃物。(機櫃後方有CCTV死角，機房內有紙箱)



5. 資通安全管理措施之實施情況(2/5)

- 5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？
 - 辦公場所應加強文件保存管制措施。(辦公場所文件保存狀況、個人電腦資源回收筒等)
- 5.19 是否定期執行各項系統漏洞修補程式？
 - 宜再加強個人電腦的資訊安全防護與控管。(螢幕保護設定、7-zip版本過舊、安裝WinRAR非授權軟體、密碼超過時間未變更等、Windows系統更新等)



5.資通安全管理措施之實施情況(3/5)

- 5.22 備份資料是否定期回復測試，以確保備份資料之有效性？
 - 宜定期進行資料備份回復測試與演練作業，以確保備份資料之可用性。(演練紀錄)
- 5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？
 - 傳送機敏性資料檔案應進行加密保護。(如：新生資料)



5. 資通安全管理措施之實施情況(4/5)

- 5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢?
 - 系統帳號應加強帳號管理並禁止共用帳號。
 - 機房重要設備與電腦系統應定期審查系統的特權帳號權限。(帳號清查範圍應包含所有主機、應用系統及網路設備→帳號清查紀錄表、帳號清查結果報告)
- 5.27 通行碼長度是否超過8個字元?
- 5.28 通行碼是否規定需有大小寫字母、數字及符號組成?
 - 通行碼宜依規定長度超過8個字元，並由大小寫字母、數字及符號組成。



5.資通安全管理措施之實施情況(5/5)

- 5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？
 - 機房區域網路宜與行政區域網路區隔。
 - 宜再審慎評估防火牆規則。(注意外對內全開之規則)
- 5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？
 - 對外網頁服務應採用https加密機制。
 - 應針對重要特定網路服務，作必要之控制措施。(限制防火牆管理者網路連線來源)



6.訂定資通安全事件通報及應變之程序及機制

- 6.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？
 - 「資通安全事件通報應變程序」的安全通報窗口資訊與實際作業相異。(通報窗口異動後應即時更新文件)
 - 應公告新版且正確的「資通安全事件通報應變程序」。
- 6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？
 - 應再加強發生資安事件等級判別之正確性，以適切地安控作為進行改善與預防。(事件等級應依「資通安全事件通報及應變辦法」第二條規定判別，只要涉及核心業務或核心資通系統，至少就是2級事件)



8. 資通安全維護計畫實施情形之精進改善機制

- 內部稽核計畫應於稽核前提出，並經主管同意後執行。內稽人員應受過訓練，並不得稽核本身經辦之業務
- 8.4 是否改正稽核之缺失？
 - 宜加強落實填寫「矯正與預防處理單」，並留存紀錄以進行後續追蹤改善作業。(內稽缺失)



9. 資通安全維護計畫及實施情形之績效管考機制

— 9.2 是否追蹤過去缺失之改善情形？

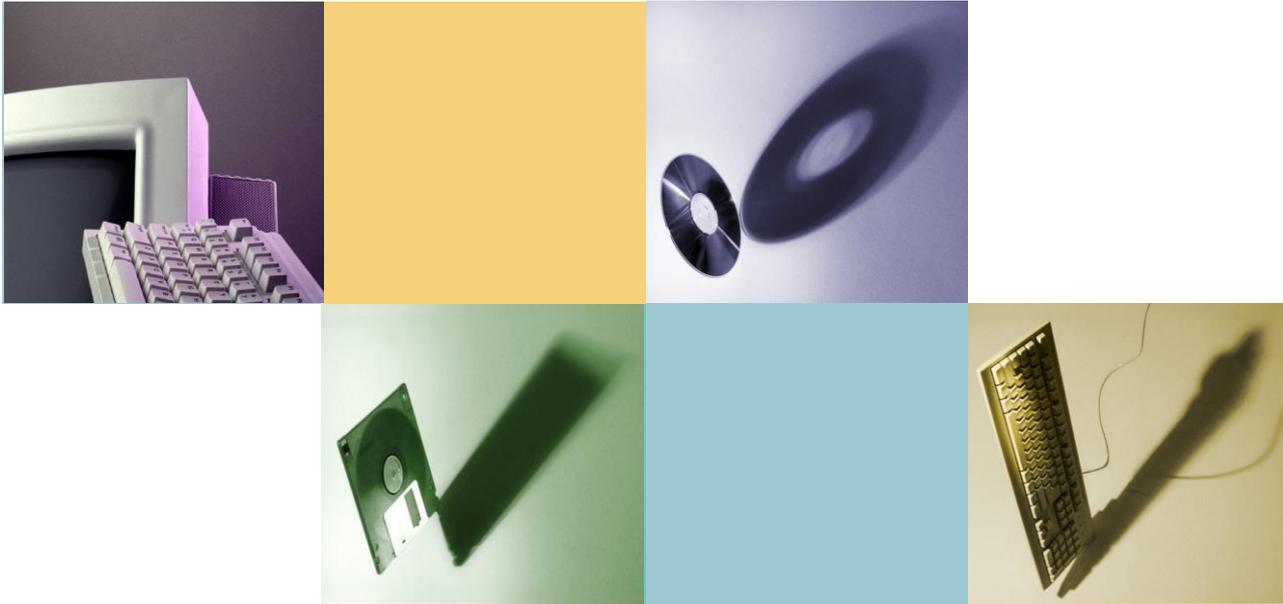
- 宜針對維護計畫不符合項目落實填寫「矯正與預防處理單」，並留存紀錄以進行後續追蹤改善作業。(線上填報及實地稽核缺失都要填)



10. 資通系統委外(含委辦)案之履約檢核及督導管理

- 10.1 資通系統委外(含委辦)是否簽訂協議書或契約？
- 10.2 是否落實檢核及履約督導管理？
- 10.3 委外(含委辦)相關人員是否簽訂保密合約書？
 - 資通系統委外契約應規範對廠商及系統的資安要求、資料返還與服務水準，並落實簽訂委外人員保密切結書。(可參考公共工程委員會合約範本)
 - 宜再審視資通系統最大可容忍中斷時間與委外契約書SLA間之關聯性。





THANKS !