111年實地稽核暨社群運作說明

國教署資安輔導團

國立華南高商　圖書館主任　劉耀明

現職及經歷：

1. 國立華南高級商業職業學校圖書館主任

2. 教育機構資安驗證中心(ISCB)稽核員(2013~)

3. 網路管理經驗25年(1997至今)

4. 行政院資安處資通安全專案稽核委員。

5. 教育部資通安全維護計畫與規範整合制度外部稽核人員

6. 國教署資安業務輔導團諮詢委員、實地稽核訪視委員、委外系統稽核委員。

專業證照：

1. ISO/IEC 27001:2013 Information Security Management System(ISMS) Lead Auditor (ISO/IEC 27001:2013資通安全管理制度(ISMS)主導稽核員)

2. BS10012:2017 / ISO 29100:2011 Personal Information Management System(PIMS) Lead Auditor (BS10012:2017 / ISO 29100:2011個人資訊管理系統(PIMS)主導稽核員)

3. ISO/IEC 27701:2019 Privacy Information Management System Lead Auditor (ISO/IEC 27701:2019隱私資訊管理系統主導稽核員)。

大綱

- 實地稽核說明
- 實地稽核查核項說明
- 社群運作

實地查核依據

- 資安法第十三條
  公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。

實地稽核說明

實地訪視對象

- 109年度31校訪視
- 110年度62校訪視
- 111年度79校訪視

實地稽核訪視內容及稽核小組

- 學校資通安全維護計畫管理
- 其他資通安全策略面、管理面、技術面等事項
- 實地稽核訪視小組由國教署遴聘教育機構ISCB稽核員、學校主管機關有關人員(政風室及祕書室)及承辦學校人員。

教育部國教署所轄公務機關111年度資通安全實地稽核查核表說明

1. 資通安全政策之推動及目標訂定

1.1 是否定義符合組織需要之資通安全政策及目標？

1.2 組織是否訂定資通安全政策及目標？

1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？

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？

1.5 是否隨時公告資通安全相關訊息？

2. 設置資通安全推動組織

2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？

2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？

2.3 是否訂定組織之資通安全責任分工？

3.配置適當之資通安全專業人員及適當之資源

3.1 是否訂定人員之安全評估措施？

3.2 是否符合組織之需求配置專業資安人力？

3.3 是否具備相關專業資安證照或認證？(本年度不列入實地稽核評分)。(C級單位必選項，D級可不適用)

3.4 是否配置適當之資源？

4. 資訊及資通系統之盤點及風險評估

4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？

4.2 各項資產是否有明確之管理者及使用者？

4.3 是否定有資訊、資通系統分級與處理之相關規範？

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？

風險評鑑(威脅弱點)參考準則

- 行政院資安會報技服中心
  資通系統風險評鑑參考指引(修訂)(V4.0)_附件4風險值工具與操作手冊附件一

威脅弱點評估表

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級（發生之可能性）低(1) 中(2) 高(3)	弱點等級（受到威脅利用之容易度）低(1) 中(2) 高(3)	風險值
LIB-CM-001	CM	防火牆	3	故障	系統失效	1	2	6
				網路攻擊	系統失效	1	3	9
LIB-CM-003	CM	內部閘道器	3	故障	系統失效	2	2	12
LIB-CM-004	CM	交換式集線器	3	故障	系統失效	2	2	12
LIB-CM-005	CM	網路環境	3	維護困難	線路完整性	1	2	6
				斷線	線路完整性	1	2	6
LIB-EV-001	EV	穩壓器	4	故障	已過年限	3	3	36
				突發性停電	無法供電	2	1	12
LIB-EV-002	EV	不斷電系統	4	故障	已過年限	3	3	36
LIB-EV-003	EV	機房	4	維護	位置	3	1	12
				人為破壞、入侵	位置	3	1	12
LIB-EV-004	EV	消房設施	4	消防設備期限	無法使用	1	2	8

風險評鑑彙整表

項次	資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值	風險再評估			
							威脅	弱點		資產價值	威脅等級	弱點等級	風險值
1	LIB-EV-001	EV	穩壓器	盛景電子	圖書館	4	故障	已過年限	36	4			
2	LIB-EV-002	EV	不斷電系統	NewSeed	圖書館	4	故障	已過年限	36	4			
3													
4													

風險改善計畫表

教育體系資通安全管理規範控制目標	現況說明	風險改善建議措施	教育體系資通安全管理規範條文	建議權責單位	預計改善時間與處理方式	與高風險資產之風險評估彙整表對照
A.11.2	使用年限即將到期	加強設備巡查，定期維護	設備	圖書館	110 年 1 月以不斷電系統支援穩壓器,不斷電系統定期檢測並更換電池	1,2

可接受風險值的決定

- 資訊資產之可接受風險值，需經資訊安全委員會開會決議，並記載於會議紀錄中。
- 資訊安全委員會每年召開會議檢討可接受風險值。可接受風險必須考量組織環境及作業之安全需求，並進行適當地調整。
- 資訊安全小組應針對高於可接受風險值項目，產出「風險評鑑彙整表」作為風險管理之依據。

5. 資通安全管理措施之實施情況

5.1 人員進入重要實體區域是否訂有安全控制措施？

5.2 重要實體區域的進出權利是否定期審查並更新？

5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？

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？

5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？

5. 資通安全管理措施之實施情況

5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？

5.7 重要資訊處理設施是否有特別保護機制？

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？

5.9 電源之供應及備援電源是否作安全上考量？

5.10 通訊線路及電纜線是否作安全保護措施？

5. 資通安全管理措施之實施情況

5.11 設備是否定期維護，以確保其可用性及完整性？

5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？

5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？

5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？

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？

5. 資通安全管理措施之實施情況

5.16 系統開發測試及正式作業是否區隔在不同之作業環境？

5.17 是否全面使用防毒軟體並即時更新病毒碼？

5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？

5.19 是否定期執行各項系統漏洞修補程式？

5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？

5. 資通安全管理措施之實施情況

5.21 重要的資料及軟體是否定期作備份處理？

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？

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？

5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？

5.25 是否訂定使用者存取權限註冊及註銷之作業程序？

5. 資通安全管理措施之實施情況

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？

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？

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？

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？

5. 資通安全管理措施之實施情況

5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？

5.32 重要系統是否使用憑證作為身份認證？

5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？

5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？

5.35 限制使用危害國家資通安全產品-大陸廠牌產品清冊列管

5.36 限制使用危害國家資通安全產品-汰換大陸廠牌產品(110/12/31前完成汰換，如無法如期汰換須於清冊述明理由。

321備份原則

- 至少備份三份
- 使用兩種不同形式
- 其中一份備份要存放異地
- 新議題：離線備份

系統修補

- XP、Windows 7 、Windows Server 2008等因微軟已不支援。
- Windows Update一定要進行更新。(不一定要最新，但要定時)
- 免費軟體注意更到最新版本及授權範圍，不用的軟體移除。
- 防毒軟體請利用學校的ApexOne(officescan)或微軟的Defender。

6. 訂定資通安全事件通報及應變之程序及機制

6.1 是否建立資通安全事件發生之通報應變程序？

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？

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？

資通安全通報應變

- 資安通報管理人員
- 臺灣學術網路各級學校資通安全通報應變作業程序

7. 定期辦理資通安全認知宣導及教育訓練

7.1 是否定期辦理資通安全認知宣導？

7.2 是否對同仁進行資安評量？

7.3 是否對同仁依層級定期舉辦資通安全教育訓練？

7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？

資通安全認知訓練時數

1. 全體同仁每人每年須接受3小時以上一般資通安全教育訓練。
2. 專職(責)人員以外之資訊人員每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
3. 專職(責)人員每年須接受12小時以上資通安全專業課程訓練或資通安全職能訓練。

8. 資通安全維護計畫實施情形之精進改善機制

8.1 是否設有稽核機制？

8.2 是否定有年度稽核計畫？

8.3 是否定期執行稽核？

8.4 是否改正稽核之缺失？

9. 資通安全維護計畫及實施情形之績效管考機制

9.1 是否訂定安全維護計畫持續改善機制？

9.2 是否追蹤過去缺失之改善情形？

9.3 是否定期召開持續改善之管理審查會議？

10. 資通系統委外(含委辦)案之履約檢核及督導管理(無則請填寫不適用)

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？

資安法施行細則第4條

各機關依本法第九條規定委外辦理資通系統之建置、維運或資通服務之提供（以下簡稱受託業務），選任及監督受託者時，應注意下列事項：

一、受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。

二、受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

三、受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

四、受託業務涉及國家機密者，執行受託業務之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境。

資安法施行細則第4條

五、受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

六、受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

七、委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行契約而持有之資料。

八、受託者應採取之其他資通安全相關維護措施。

九、委託機關應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

11. 其他應辦事項

11.1 是否每年檢視一次資通系統(自有及委外)分級妥適性？(普中高)

11.2 是否每兩年辦理一次資通安全健診？(弱掃)

11.3 是否完成資通安全防護(防毒軟體、網路防火牆、電子郵件過濾機制)？

11.4是否完成資通安全弱點通報機制導入作業(111年尚在導入階段，暫不列入評分，C級機關應於2年完成導入)

改善事項填寫

- 誰負責改善(人)
- 改善的方式(事)
- 改善的時間(時)
- 改善的區域(地)
- 改善的設備(物)

ISMS & 資通安全維護 施行應注意事項

- 說、寫、做一致
- 管理階層的支持
- 資通安全工作推動不是一個人的事
- 委外廠商的合約及管理
- 一般人員的教育訓練
- 融入變成日常的習慣

社群運作說明

社群運作目標

1. 地區輔導員主導，提升地區資安專責人員能力，
2. 整合地區資源，針對地區學校資安議題進行研究與探討，
3. 透過經驗分享與交流，達到專業互動成長之目的。

社群組成

社群成員以地區資通安全專責人員為主要組成，以地區分配為原則，並以該地區輔導員為地區社群會議召集人，輔導團遴聘一位專家學者擔任社群諮詢委員協助設群運作。

社群議題

學校網路安全、系統安全、應用程式安全、資安及個資管理、資料加密及身份認證授權、雲端安全及最新資安議題為主軸。

運作方式

運作方式可包含資安實務觀察與回饋、主題探討、主題經驗分享、專題講座、標竿楷 模學習、案例分析及專業領域研討等方式。

感謝聆聽

聯絡方式：05-2787140#139　E-mail：liu0604@mail.edu.tw