大專校院的資訊長
如何應對資安專章？

面對越來越嚴峻的網路安全威脅，大學需要積極提升資訊安全防禦能力。
申請資安專章計畫的補助，可強化並促進大學資安發展，
但也面臨需燒腦籌畫與落實執行的挑戰.....

徐國鈞
國立台北商業大學
資訊與網路中心主任
TOTORO.HSU@NTUB.EDU.TW

簡報大綱

1.資安強化專章價值

2.強化管理、降低負擔、走向永續

3.對提送計畫的建議與提醒

1.資安強化專章價值

資安強化專章價值 (1/2)

- 教育部為協助大學建立持續性與永續性的教研環境，不因資安事件受影響而中斷教學與研究，而規劃「資安強化專章」。
- 為讓學校高層重視並了解ISMS的建立不單僅由資訊中心負責，更仰賴各單位的參與。

資安強化專章價值 (2/2)

- 藉由專章，協助各校逐步：

1. 建立完善的ISMS制度，
2. 提升資安管理效能，
3. 降低資訊人員負擔，
4. 以達永續管理。

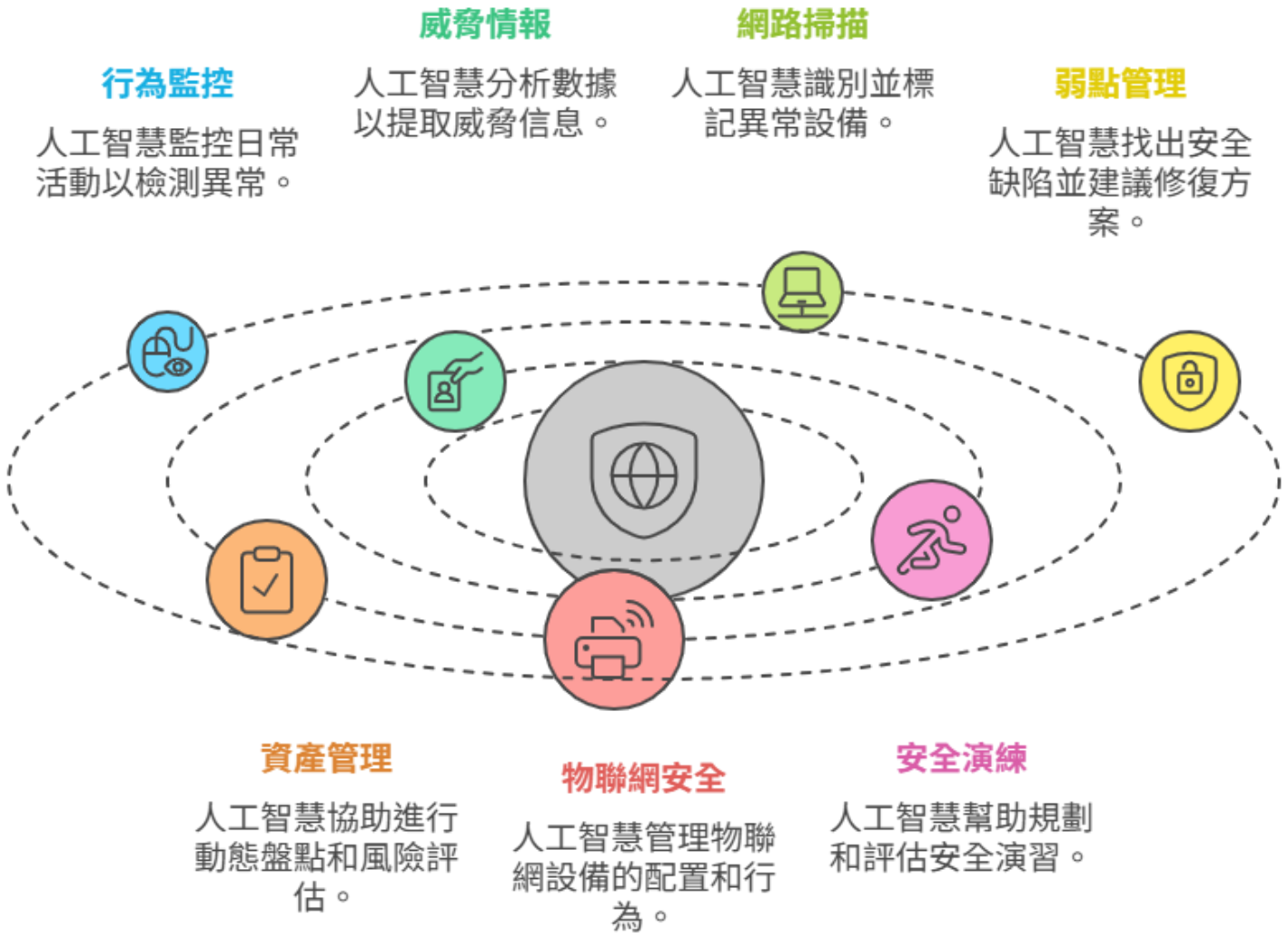
2.強化管理、降低負擔、走向永續

----資安管理自動化走向智能化藍圖

校園資安管理的痛點

- **任務越來越多**
  - 要管的設備越來越多
  - 要管的範圍越來越大
  - 要落實法遵應辦事項
  - 要導要驗ISMS
  - 要導(要驗)PIMS
  - 第一、二、三方的稽核、演練、攻防不斷
- **人不會多，甚至越來越少**
- **經費不會多，長期也是越來越少**
- **技術進步快**
- **工作壓力大**

應用AI在校園資安管理的藍圖



AI應用於資安定期性工作

威脅情報分析

分析全球威脅數據以更新和完善威脅模型。

日誌監控

檢測系統日誌中的異常行為以識別潛在風險。

漏洞管理

定期掃描系統中的漏洞並優先推薦修補。

資安意識訓練

分析員工行為以量身定制和提示安全訓練。

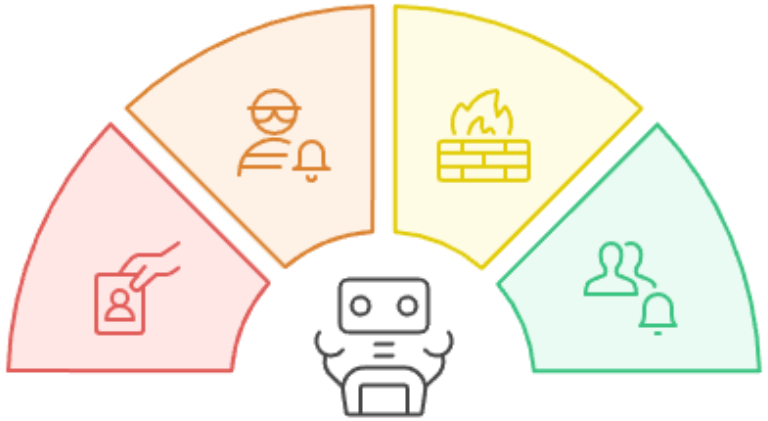
AI應用於資安事件性工作

數據洩露監控

AI 檢測潛在的數據洩露
並建議應對策略。

入侵檢測

AI 對可疑活動啟動防禦
並建議改進措施。



事件響應

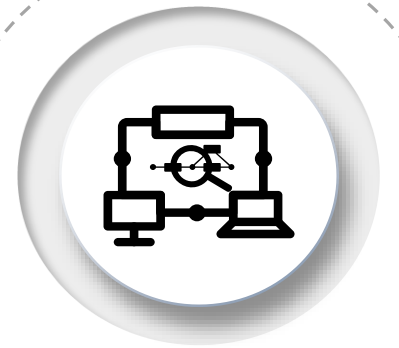
AI 在資安事件中分析威
脅並指導響應行動。

應急計畫測試

AI 模擬並優化應急計畫
以提高有效性。

AI應用於資安工作引導與催稽

AI應用校園網管的分析與處理

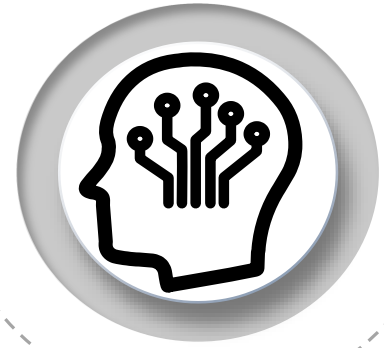


記錄分析

機器學習
建立營運基準線

發現網路異常態勢
與問題癥結點

狀態監控

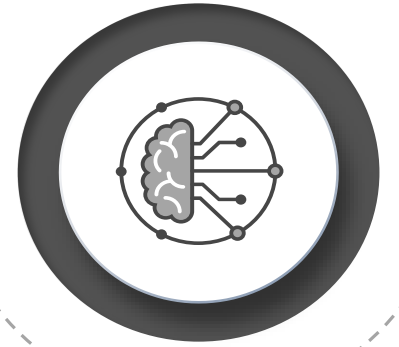


危機預警

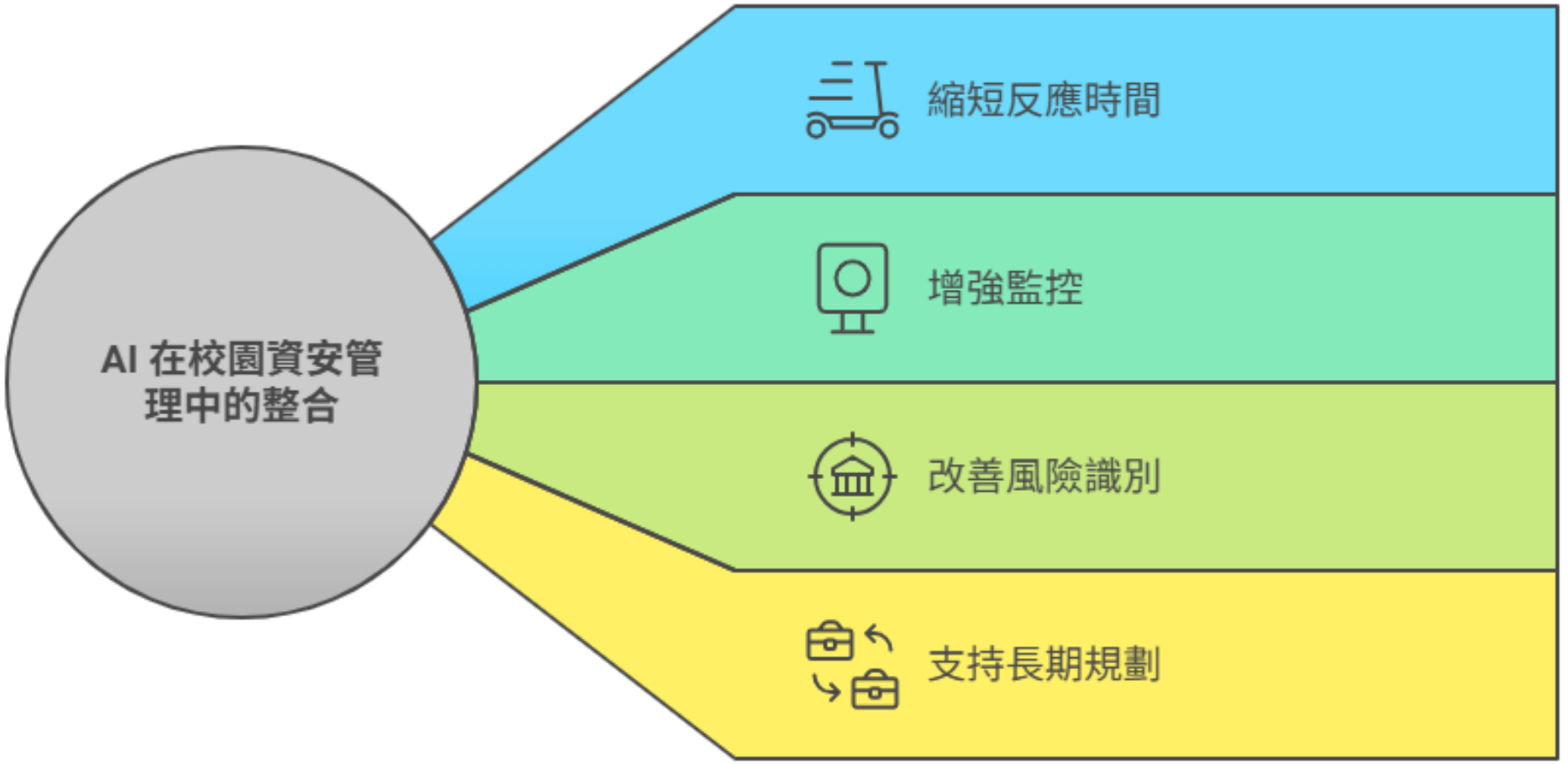
關聯性分析，識別問題確定根本原因 (RCA)

AI 提供專業建議
快速解決問題

提供對策



AI應用提升資安管理的效能



在校園資安領域的合作

- 校園資安領域各校沒有利益衝突
- 校園資安領域有各校目標相同
- 校際合作促進共同的利益
- 校際合作降低資源的重複配置
- 校際合作降低人員技術壓力

校園資安合作的方式

- 資安管理的雲端服務共用
- 技術交流與研討
  (持續循現有機制，如研討會、教育訓練、社群等)
- 技術人力服務的分享與互惠
- 資安相關工具的分享與互惠
- AI應用校園資安管理課題研究分工與共享

3. 對提送資安專章計畫的建議與提醒

提送時限與方式

1. 請於113年12月5日（星期四）下午5時前，將一階段成果報告暨第二階段計畫書(5頁為限，封面核章)及推動資訊安全強化預計投入之經費(附表1-1)，函報本部資訊及科技教育司（紙本或電子公文交換）；公文副本知會資安專章計畫辦公室（10025臺北市中正區濟南路一段321號（國立臺北商業大學資訊與網路中心）。
2. 如紙本函報 並於資安強化專章執行成果填報平臺表格6.1 上傳 計畫書掃描檔，可不繳交光碟。
3. 並於113年12月5日（星期四）下午5時前至資安強化專章執行成果填報平臺（https://sproutsec.moe.edu.tw/）填報附表1-2，紙本免附。

計畫書的架構

一、執行成效說明(112 至 113 年)

二、目前遭遇困難與建議解決方式

三、推動策略及預期效益(114 至 116 年)

（一） 基本資訊：

1. 學校單位數量(行政、教學與研究單位)：_____
2. 教師及職員數量：_____
3. 資通系統數量：_____
4. 委外系統數量：_____
5. 大陸廠牌資通訊產品數量：_____

（二） 學校推動資訊安全強化預計投入經費(附表 1-1)。

（三） 績效指標與執行說明(附表 1-2)。

在5頁計畫書的範圍

不包含在5頁中(為5頁計畫書的附件)

在資安專章執行成果填報平臺中填報

計畫書的架構 (補充說明)

一、執行成效說明(112 至 113 年)

二、目前遭遇困難與建議解決方式

三、推動策略及預期效益(114 至 116 年)

（一） 基本資訊：

1. 學校單位數量(行政、教學與研究單位)：_____
2. 教師及職員數量：_____
3. 資通系統數量：_____
4. 委外系統數量：_____
5. 大陸廠牌資通訊產品數量：_____

（二） 學校推動資訊安全強化預計投入經費(附表 1-1)。

（三） 績效指標與執行說明(附表 1-2)。

說明學校整體資安作為，
尚不用附佐證資料。

未來規劃，
原則上不用附佐證資料，
如已有相關草案可附。

計畫撰寫建議

- 各校可依四大面向(全校導入資訊安全管理系統、強化學校人員資通安全認知與訓練、確保資通系統管理量能、落實管理危害國家資通安全產品)撰寫計畫書。
- 可參照「資通安全責任等級分級辦法」應辦事項規劃資安作為，公立大專校院依核定的資安等級執行應辦事項，私立大專校院可依C級特定非公務機關應辦事項規劃。

附表1-1:學校推動資訊安全強化預計投入經費

資安專章計畫的經費要怎麼編列？

- 本期學校投入經費規劃之目地，為了解學校對資安投入的狀況，

  以「學校預計投入經費+前次資安專章補助經費」概估填報，不另列補助款及配合款項目。

附表1-1:學校推動資訊安全強化預計投入經費

資安專章計畫的經費要怎麼編列？

延續前期專章評核通過後，每年補助約70-130萬元。

70-80%	20-30%
經常門	資本門

依循高等教育深耕計畫經費使用原則

資安專章計畫經費運用方向

增加專兼任人員

增加資安人員，有助於提升校內資安管控。

人員培訓

提升校內人員資安意識與技能，降低安全風險。

軟硬體採購

更新安全軟硬體，提升防護能力。例如，防火牆、入侵偵測系統、防毒軟體。

安全檢測

定期進行安全檢測，發現潛在漏洞，進行修正。

附表1-2：績效指標與執行說明

- 本次計畫已依實地訪視訪談前兩年各校的達成情形，刪除大部分學校已完備之部分指標。另為使未來能深化資安措施，增修前次部分評核指標。

附表1-2：績效指標與執行說明

本次評核指標

1.全校導入資訊安全管理系統	2. 強化學校人員資通安全認知訓練	3. 確保資通系統管理量能	4. 落實管理危害國家資通安全產品
1.1 資通安全長之參與 1.2 資通安全推動組織 1.3 資通系統及資訊之盤點 1.4 資通安全風險管理 1.5 內部稽核 1.6 委外資安要求 1.7 業務持續運作演練 1.8 資訊安全管理系統(ISMS)適用範圍	2.1 提升教職員資安意識 2.2 提升系統開發及維護人員資安專業	3.1 資通系統集中化	4.1 禁止公務使用大陸廠牌資通訊產品 4.2 限制出租場域使用大陸廠牌資通訊產品

附表1-2 ◆全校導入資訊安全管理系統

推動策略	評核指標	補　充　說　明
資通安全長之配置	~~資安長配置~~	為使未來學校資安長深化掌握策略面的資安相關事務，建議應實質參與校內資安推動事務，並有資安長參與紀錄與說明。
	資安長參與支持之相關記錄	

附表1-2 ◆全校導入資訊安全管理系統

推動策略	評核指標	補　充　說　明
資通安全推動組織	~~成立資安推動組織~~	在資安相關的重大會議(如管審會等)中，單位主管親自出席會議，代理或請假比率不宜過高。
	由全校一級單位主管或副主管組成委員會並出席相關會議	
	落實管理審查(八大議題的納入)	實質審議，參考資通安全維護計畫範本所列 8 項議題均列入議程討論範圍。
	利害關係人關注與回應處置	在ISO 27001：2022本文4.2 瞭解關注方之需要及期望，新增(c)此等要求事項中之哪些要求事項，將透過資訊安全管理系統因應。 另在本文9.3管理審查，新增(c) 與資訊安全管理系統相關關注方之需要及期望的變更。

附表1-2 ◆全校導入資訊安全管理系統

推動策略	評核指標	補　充　說　明
資通系統及資訊之盤點	資訊資產清冊持續推動全校盤點、更新	1.績效指標%母數為盤點之全校所有單位(例如教學、行政、研究單位等)。 2.公立依照國立大專校院資通安全維護作業指引，每年應完成全校單位盤點；私立以完成全校單位盤點為原則。
	全校範圍系統持續完整盤點	
	全校範圍 IoT持續完整盤點及安全管控	

附表1-2 ◆全校導入資訊安全管理系統

推動策略	評核指標	補　充　說　明
資通安全風險評估	全校執行風險評估	建議應辦理全校性風險評估教育訓練，並將風險評估執行結果送至管審會報告。
	系統主機弱掃/網站弱掃、滲透測試、資安健診執行規劃	建議至少完成全部核心系統的弱掃、滲透、健診等。
	安全檢測結果修補管控制度及執行成效	建議至少完成全部核心系統高風險修補，中風險以下則依各校斟酌資安量能，逐年完成修補。

附表1-2 ◆全校導入資訊安全管理系統

推動策略	評核指標	補　充　說　明
內部稽核	持續推動並全校完成內部稽核作業	公務機關以每2年為週期完成全校所有單位的內部稽核；私立在本計畫建議比照C級特定非公務機關(在未來3年內，應至少完成全校所有單位的內部稽核1次)。

附表1-2 ◆全校導入資訊安全管理系統

推動策略	評核指標	補　充　說　明
委外稽核		深化委外資通安全，關注並強化下列三項指標。
委外資安強化	委外招標案納入資安規範	建議訂定合宜的選任及監督之要求與執行條文，應含括資通安全管理法施行細則第4條所列9大注意事項， 以及教育部資通安全實地稽核項目檢核表(五) 資通系統或服務委外辦理之管理措施之檢核項目。
	委外承辦人及廠商資安教育訓練	全校業務單位所屬人員從事資通系統自行或委外設置、開發、維運者(視為資訊人員)應皆須接受教育訓練。
	委外廠商作業及維護流程資安檢視	如何對委外廠商進行資安檢視，建議以「稽核或其他適當方式確認」受託業務之執行情形。

附表1-2◆全校導入資訊安全管理系統

推動策略	評核指標	補　充　說　明
業務持續運作演練	核心系統BCP(完備C.I.A.演練情境)	1.演練情境建議考量C.I.A.三構面之風險，並依資通安全責任等級，每兩年全部核心系統至少應演練1次。 2.須提供前兩年演練題目。
	重要資料異地備份及回復測試(至少全部核心系統及高級系統)	全部「核心」資通系統的備份規劃與執行(包含作業方式、週期、異地存放等)，若提供備份紀錄佐證宜將IP及較敏感資訊加以遮蔽，系統若採自動備份，仍宜將人工查核確認納入管理程序。
資訊安全管理系統(ISMS)適用範圍	資安目標及其達成之量測範圍達到全校	建議可從資安責任等級分級辦法機關應辦事項的策略面、管理面、技術面項目中，訂定全校性項目。

附表1-2 ◆強化學校人員資通安全認知與訓練

推動策略	評核指標	補　充　說　明
~~配置資通安全專職人員~~		依訪視成果多數學校已配置資安(專職/責)人員，也都積極考證照。
~~提升資工安全專職人員資安職能~~		
提升教職員資安意識	全校教職員 資安教育訓練達成比率	全校教職員每年參加資安教育訓練比率，母數應大於統計處公告之教職員數量。 建議規劃未達成者之資安強化相應措施。
	新進人員 資安政策認知訓練	說明對新進人員的資安訓練，若僅有網站公告方式進行宣導，宜評估宣導效果。
	社交工程演練被誘騙者 加強資安意識措施	對社交工程演練被誘騙者是否有後續處理或教育訓練。
	資安事件通報校內程序 宣導及演練	說明資安事件通報校內程序宣導方式，若僅有網站公告方式進行宣導，宜評估宣導效果。

附表1-2 ◆強化學校人員資通安全認知與訓練

推動策略	評核指標	補　充　說　明
提升系統開發人員資安專業	開發及維護系統符合資通系統防護基準執行控制措施	參考《資通安全責任等級分級辦法》附表十中，對於普、中、高資通系統防護要求。
	落實SSDLC文件	依照資通系統防護基準中規定，應落實安全系統發展生命周各階段相應資安控制措施。SSDLC應有各階段佐證文件，無論新舊系統皆須提供導入情形及達成情形。

附表1-2 ◆確保資通系統管理量能

推動策略	評核指標	補　充　說　明
資通系統集中化管理	重要資通設備設置地點(系統集中化執行率及配套措施)	全校系統向上集中的進度，以及所有配套管理程序，應具體規劃並落實。
	遠端維護採「原則禁止例外允許」方式	核心系統及向上集中系統環境應完全落實此原則，透過相關程序規範、防火牆申請核可、開通及關閉紀錄等進行管控，開放遠端存取原則以短天期為主。
	日誌內容、記錄時間週期及留存政策(核心系統優先落實但不限)	1.描述現行做法及未來規劃。 2.各機關於日常維運資通系統時，應訂定日誌之記錄時間週期及留存政策，並保留日誌至少6個月。

附表1-2 ◆落實管理危害國家資通安全產品

推動策略	評核指標	補　充　說　明
禁止公務使用大陸廠牌資通訊產	禁止採購作法及教育訓練宣導	建議私校比照C級特定非公務機關，訂定相關管理機制。
	既有列冊管理及管控措施、汰除	對於全校的大陸資通訊產品有具體的清查紀錄與清查方式。
限制出租場域使用大陸廠牌資通訊產品	出租場域禁用規定及教育訓練宣導	宜訂定場地委外契約或禁用規定，並對全校宣導或教育訓練。

附表1-2 ◆學校資安額外作為(加分項目)

推動策略	評核指標	補　充　說　明
創新或創意的規劃作為	自行新增	有別於規範的強化資安或管控之作為 (自籌項目或特殊資安規劃)。 *因平臺目前無填報者新增項目功能， 若有大於兩項的指標，請放入附件中說明。

附表1-2 ◆學校資安額外作為(加分項目)

資安額外作為建議：

- 「資通安全責任等級分級辦法」應辦事項，如：端點偵測及應變機制(EDR)導入、政府組態基準(GCB)導入、資通安全威脅偵測管理機制(SOC)建置、入侵偵測及防禦機制(IDS/IPS)建置、應用程式防火牆(WAF)建置、進階持續性威脅攻擊防禦措施(APT)建置、擴大弱點掃描/滲透測試實施範圍。
- 或「資通系統防護基準」做法，如：高級系統異地備份機制、中/高級系統備援機制、對外服務系統傳輸之機密性與完整性全面改善(啟用HTTPS、TLS等安全傳輸協定)。
- 或113年實地稽核新增查核項目，如：雲端服務應用資安防護、公務使用即時通訊軟體管控措施、配置其他資安專責人員。

報告完畢

徐國鈞
國立台北商業大學
資訊與網路中心主任
TOTORO.HSU@NTUB.EDU.TW