

出差報告

出差人員：蒲正寧

出差日期：民國 114 年 5 月 9 日（下午 3 小時）

上課地點：台灣大學進修推廣學院

課程名稱：資訊作業委外安全管理

課程內容：

本課程主要介紹資訊作業委外的資安管理，內容包含委外前之採購風險評估與管理方法，以及委外期間的資安監控措施。課程涵蓋國內相關法規要求，並說明在採購資訊產品或服務前應如何進行風險評估與風險管理。接著針對個資及資訊委外進一步探討如何選擇合適的廠商、進行供應商評鑑、簽訂保密協議與實施內部稽核。此外，課程亦分析委外作業各階段之監督重點，並提出常見缺失案例及防範要點，以確保整個委外作業符合資安要求。

課程重點與學習心得：

- 2024 年行政院國家資通安全情勢報告中指出的全球主要資安威脅分析，包含以下幾個面向：
 - 駭客利用 AI 技術發展出新型態的入侵與惡意詐騙手法。
 - 個人資料與憑證外洩，導致現有防護機制失效的情形增加。
 - 社交工程攻擊更為泛濫，APT 攻擊與勒索軟體的風險也顯著增加。
 - 資安(訊)供應商本身遭到攻擊，導致整個供應鏈安全受到威脅。
 - 資訊系統漏洞與弱點頻繁曝光並被惡意利用。
 - 雲端應用服務所面臨的安全威脅呈現多元化趨勢。

資安威脅的範圍與攻擊手法正快速擴展，組織需加強相關防禦措施，以因應日益複雜且多樣的網路攻擊形式。

- 公務機關、公立學校、公營事業等單位，除非業務必須且無替代方案，不得採購主管機關列為具資安風險的資通產品或服務。若涉及委外營運或場地使用，應事先納入契約或使用規定，並加強管理與宣導。如有採購需求，須經資安長及上級機關核准，報主管機關核定後，才能專案辦理。**此規範僅適用於公務機關、公立學校等公部門單位，私立學校及民間機構不在此限。**
- 資安人員若在最後階段才參與採購，容易因時程壓力忽略風險。應由各利害關係人組成團隊，共同評估資安風險，以降低後續問題。
- 採購資安風險管理應由跨部門團隊共同參與，包括請購單位採購人員、資

訊資安部門、技術部門、財務部門及法律部門。各部門分工合作，才能全面評估採購過程中的資安風險，降低潛在問題，確保整體採購安全與合規。

- 在採購過程中融入資安要求的良好做法，分為四大面向：
 1. **採購程序設計**：採購初期就應納入資安考量與預算規劃，確認產品或服務的影響範圍，進行系統整體規劃與資安防護等級評估。
 2. **採購合約規定**：要求供應商提供符合資安要求的證明，建立評估與問責機制，並訂定監督流程及明確資安責任條款。
 3. **風險管理**：實施供應商風險管理計畫（如市場調查）、供應鏈風險評估，並關注政府的禁用產品清單或指引。
 4. **教育訓練**：加強利害關係人的資安意識，教育採購與使用單位識別並處理資安風險，同時讓預算單位了解資安的重要性與潛在風險。

- 在撰寫 RFP（徵求建議書）時，應注意的資安相關重點，包括：
 1. 審查投標廠商及其專案人員的背景與資格。
 2. 說明專案組織架構及人力的資安需求。
 3. 評估廠商是否具備適任與資安管理的優勢。
 4. 明確列出採購產品或服務的資安要求。
 5. 規劃後續保固與維運服務內容。

在招標文件中把資安條件寫清楚，確保廠商具備安全能力並能提供長期支持。

- 在採購過程中要落實資安風險管理的好方法：應在採購條件中設定適當的資安標準和要求項目，並針對採購項目中的各個部分，考量適用的控制措施。接著，要透過驗證程序確認廠商是否真的達到標準，同時鼓勵供應商提出符合需求的解決方案。最後，採購過程中應導入敏捷式開發精神，與需求單位保持多方溝通，確保資安要求落實且彈性因應需求變動。

個資及資訊委外：

- 私立大學在將服務委外時，必須先確認是否涉及個人資料的處理。如果沒有涉及個資的收集、處理或利用，就不會被認定為個資的委外，自然也不適用《個資法》的相關規定。但一旦涉及個資，就要依法辦理。

- 私立大學屬於非公務機關，適用的個資法條文與公立學校不同，像是收集資料的依據、違法後的處理機制及行政處分都不一樣。雖然沒有國家賠償責任，但仍可能被主管機關開罰，因此仍需謹慎處理個資。

- 若學校將學生或教職員的個資交給外部廠商處理，一旦廠商發生資料外洩等事件，學校仍需負最終的法律責任。這代表在委外時不只要挑對廠商，更要確保廠商有能力保護資料，否則出事後責任仍由學校承擔。
- 根據個資法規定，對委外廠商的監督必須具體落實，並且要有書面紀錄。不管是集合、查核、報告或其他方式，都應保留證明，以便在發生爭議或主管機關稽查時證明學校有履行管理責任。
- 即使是小型私立大學，在與廠商簽約時也應把資安條件寫清楚，包括資料範圍、處理方式、委託目的、契約期間與終止後資料的處理方式，以及若廠商違約或資料外洩時的責任歸屬，才能有效保障學校自身權益。