資通安全導入實作分享

周冠吉

多元的資通安全管理制度

CNS 27000	資訊技術-安全技術-資訊安全管理系統-概觀與詞彙
CNS 27001	資訊技術-安全技術-資訊安全管理系統-要求事項
CNS 27002	資訊技術-安全技術-資訊安全控制措施之作業規範
CNS 27003	資訊技術-安全技術-資訊安全管理系統實作指引
CNS 27004	資訊技術-安全技術-資訊安全管理-量測
CNS 27010	資訊技術-安全技術-跨部門及跨組織通訊之資訊安全管理
CNS 27014	資訊技術-安全技術-資訊安全治理
CNS 27032	資訊技術-安全技術-網際安全指導綱要
CNS 15215	資訊技術-安全技術-資訊安全事故管理
CNS 15428	資訊技術-安全技術-存取控制之安全資訊物件
CNS 15482	公司治理之資訊技術
CNS 15653	資訊技術-安全技術-資訊與通信技術災害復原服務指引
CNS 14889	風險管理－詞彙
CNS 31000	風險管理－原則與指導綱要
CNS 31010	風險管理－風險評鑑技術
CNS 20000	資訊技術－服務管理－第1部：服務管理系統要求事項

多元的資通安全管理制度

- 資通安全管理法
- 資通安全事件通報及應變辦法
- 行政院及所屬各機關行動化服務發展作業原則
- 教育體系電子郵件服務與安全管理指引、
- 台灣學術網路(TANet)分散式阻斷服務(DDoS)通報應變作業指引
- 臺灣學術網路各級學校資通安全通報應變作業程序
- …

多元的資通安全管理制度

法律是道德的最低標準

法遵是資安作為的下限

超越單一的法遵，打造整合式資通安全管理制度

資通安全作業

- 9成是管理面的作業
- 1成是技術面的作業(遠端連線、安全通道、程式開發..等)
- 目前稽核方式：線上查檢、實地抽查

推動流程

- 前景分析
- 範圍與目標
- 政策制定
- 推動組織、人員配置
- 教育/認知訓練
- 文件規範/程序/辦法制定
- 驗證執行結果(KPI、BCP、內部稽核、管理審查會議)
- 最終精神-PDCA((Plan、Do、Check、Action)

資通安全活動的目的

- 近期資安事件問題逐年增加，連老師都是受害者
- 內部人員對資通安全的認知與處理態度消極
- 機關機敏資料量逐年增加、系統層漏洞逐增地被抽絲剝繭
- 政府機關的指示、要求與期望

前景分析

- 單位內部的要求、期望
- 第三方利害團體的要求、期望(教育部、縣市政府教育局、學生家長、委外廠商、訪客)

Q：思考一下，機關除上述的利害團體，其他還有哪些呢??

範圍與目標

- 範圍：全機關
- 對象：全校師生、同仁、服務廠商
- 目標制定(達成指標)
  - 定量化：能量化的目標=>要數據化、指標化
  - 定性化：不能量化的目標=>要標準化、細節化、具體化
- 目標(指標)檢測的頻率、達成率

Q：各舉例一下，量身訂定機關的定量化目標與定性化目標?

Q：各舉例一下，量身訂定機關的定量化目標與定性化目標?

- 定量化目標
  - 確保相關資訊安全措施或規範符合政策與現行法令之要求，每年至少進行一次查核
  - 每年至少進行一次業務持續計畫之測試及檢核
- 定性化目標
  - 確保資訊資產受適當之保護，防止未經授權或因作業疏忽對資產所造成之損害
  - 確保所有資訊安全事件或可疑之安全弱點，皆依適當通報程序反映，並予以適當調查及處理
  - 符合政府資訊安全相關政策、規定以及相關法令要求
  - 定期實施資訊安全教育

資通安全政策制定

- 機關資通安全最高指導原則
- 內容至少含括：
  - 目的、依據、範圍、達成目標、檢視更新頻率與方式、核准條件、公告與宣導作為

Q1：資通安全政策與資通安全維護計畫，是否需要個別獨立?
Q2：對第三方利害相關團體，如何進行公告與傳達?

成立推動的組織

- 目的：落實與督導機關執行資通安全維運的單位(成立000推動委員會)，並尋求機關主管的支持與資源支援
- (執行組、稽核組)、(策略規劃組、資安防護組、績效管理組)、(執行小組、緊急處理小組、稽核小組)、(政策推動組、風險管理組、稽核督導組、緊急處理組、教育訓練組)…等
- 資通安全長的指派
- 訂定推動組織和各組權責與職掌
- 人力配置
- 指派專職(責)人員

Q1：請檢視機關所制定的推動小組組織與資通安全維護計畫內的組織是否相同?權責是否一致?

Q2：指派委外廠商人員為專職人員，是否可以?

認知與教育訓練

- 認知訓練：目的、對象(全體人員)
- 教育訓練：目的、對象(至少包含資安人員)
- 執行頻率、執行方法(平台)
- 時數要求
- 效果驗證
- 人員保密要求：保密切結書

Q：資訊組長平常作業都很繁忙，無法抽空參加資安教育訓練，怎辦?

規範文件制定

- 資通安全要推動，就要制定符合法定法規要求與符合機關執行作業的規範，並落實執行。
- 將流程制度化：制定相關規範(程序、辦法、表單)
- 文件與紀錄管理程序、風險管理程序、管理階層審查程序、資安事件管理程序、業務持續運作管理程序、內部稽核及矯正管理程序、存取控制作業辦法、委外管理辦法、網路通訊管理作業辦法…等
- 規範應適切地進行保管，並供最新規範給必要相關人員查閱

Q：機關資通安全規範的機密等級都設定為公開資訊，是否恰當?

風險管理程序

- 目的：

  對機關內的資產進行風險評估，依評估結果對高風險資產進行適切性的管制與因應，以降低風險發生的機率與損害。

- 制定程序與準則
- 訂定風險值、可接受的風險值
- 風險處理、因應與追蹤
- 風險再評估
- 持續改善(PDCA)

實體環境管理-辦公室、機房

- 人員與設備進出管理
- 電源安全管理：UPS、穩壓器、防落雷裝置、電壓標示
- 環境安全管理：溫溼度管控、門禁管控、CCTV設置適切性
- 線路保護作為
- 資產移入(或移出)機關與報廢管理(與資產清冊、風險評估關聯)
- 待報廢設備的保護與管制

Q1：廠商進入機房，需要全程陪同嗎?

Q2：很多機關的主機機櫃與電腦教室共用空間，該如何降低安全疑慮?

通訊網路管理

- 邏輯網路架構圖
- 網段配置資料
- 遠端連線管控：申請、設定與監控(FW、VPN)
  - 來源IP、目的IP
  - 來源通訊埠(port)、資訊服務
  - 預設規則-全部阻擋
- 無線網路安全管理(校內師生同仁、廠商、訪客)、規範要求
- 緊急連絡清冊

Q：自我檢視防火牆的安全規則，有無發現不清楚的規則被設定?設定規則範圍的適切性(如：140.111.0.0/16全通、FTP服務全開通..等)?

資訊系統管理-電腦、伺服器

- 桌面淨空、螢幕保護設定
- 單一時間源校時(自動、手動)
- 作業系統更新(如：Windows update)
- 防毒軟體授權與病毒碼更新(授權-集中、單機；免費)
- 資料定期備份、資料備存於他單位(MOU協議)
- 容量管理
- 雲端安全評估
- 機敏資料保存、加密、傳輸
- 網頁服務安全傳輸協定(HTTPS)

資訊系統管理–電腦、伺服器(續)

- 密碼設定要求:長度、變更週期、複雜度、迭代數
- 帳號權限審查(如：OS、AP、DB)
- 遠端連線申請、核准、紀錄
- 程式開發管理、程式原始碼保存與版控、智慧財產權
- 原碼檢測、弱點掃瞄、滲透測試
- 系統與應用程式之錯誤訊息紀錄與分析

Q1：自我檢視防火牆，有無機關管理者的帳號?並且定期(半年)變更密碼?

Q2：自我檢視各系統中，是否仍有存在已合約終止的廠商帳號?

Q3：自我檢視各系統的連線紀錄，是否發現廠商帳號於非上班時段有連線登入的紀錄?

委外管理

- 委外廠商能力評估與篩選
- 委外合約與保密切結要求、機關資通安全政策的宣達
- 駐點人員安全作業準則、人員年度資安教育訓練與安全專業證照
- 委外資通設施的帳號申請與連線授權
- 定期交付紀錄資料、提出安全建議
- 機關得對服務廠商進行適切性的資通安全稽核(委託、查檢表)
- 合約終止之系統與資料的安全要求(帳號、權限與資料)

Q1：自我檢視機關有哪些委外廠商?

Q2：如何讓廠商了解機關的資通安全政策?有無保存廠商人員簽署的保密切結資料?

情資收集與資安事件通報

- 情資收集管道
- 資訊安全事件通報管理程序(1~4級資通安全事件)
- 公告與宣導
- 誰有告知義務：機關內所有人、服務廠商
- 通報平台、機關通報人(多位)
- 流程：

  發現->告知機關資通事件通報窗口->管理者確認通報資訊->通報機關資通安全長並到通報平台登錄->處理與因應資安事件->短期處置因應、長期預防作為->向機關資通安全長回報處理結果並至通報平台進行處理情形之記載->事件檢討(列入教育訓練或宣導事項)->持續追蹤。

Q1：發生資通安全事件，應多久進行通報平台的通報登錄?

Q2：請自我檢視通報平台的機關通報人帳號，是否皆為現任管理者帳號?

自我驗證執行結果

- KPI
- BCP
- 內部稽核
- 管理審查會議

驗證執行結果-KPI

- 目標達成情形、指標有效性量測
- 依資通安全政策所制定的目標，進行檢核以確認達成情形
- 內容至少含括：
  - 量測範圍
  - 目標項目
  - 量測指標
  - 量測依據
  - 量測頻率
  - 量測與分析人員
  - 實際量測資訊
  - 達成狀況(符合性確認)

Q1：自我檢視量測項目是否都依機關資通安全政策內的目標要求相符?

Q2：量測結果之達成率不佳，該怎辦?

驗證執行結果-KPI(續)

- 有效性量測表的範例表格

驗證執行結果-BCP

- 機關業務持續營運計畫，也就是資通安全演練作業。
- 目的：與萬安演習的概念一樣，為因應緊急狀態(情境)發生時的處理應變作為，以確保機關業務能持續推動，並適切地降低損害。
- 教育部每年度有推動的演練：社交工程演練、資安通報平台演練
- 事前擬定多項模擬情境=>紙本演練、實機演練(偕同廠商)
- 流程：

  演練計畫擬定、申請、審核->演練前置協調、支援請求與準備->依計畫執行演練作業->紀錄演練時間與內容->演練後之檢討與改進->留存演練腳本並持續更新

- 演練作業腳本的用處

Q：機關的資訊服務都已上雲端，請問我還需要做甚麼演練呢?

驗證執行結果-內部稽核

- 目的：自我檢視機關內資通安全執行狀況與落實情形
- 稽核方式：
  - 委託專業機構協助
  - 自訂稽核查檢表進行符合性檢視
- 稽核原則：
  - 慎選稽核日期與活動安排
  - 客觀性、獨立性、紀錄詳實
  - 自己業管不自稽

Q：機關人力有限，無法執行內部稽核作業，該怎辦?

驗證執行結果–管理審查會議

- 機關對校園資通安全推動的監管/協商/審核/督導的決策會議
- 參與者、列席者、外部專家學者
- 召開形式、頻率、紀錄
- 報告與討論議題：所有資通活動作業的報告綜合體，至少包括：
  - 資通安全政策更新
  - 第三方利害團體的要求與期望
  - 風險評鑑結果與高風險處置
  - 目標達成情形
  - 年度演練檢討與結果
  - 內部稽核結果與改善
  - 前次討論事項之追蹤
  - 矯正處理措施之改善與追蹤

Q：機關校長或資通安全長沒參加管理審查會議，但都會將會議記錄與結果，以公文形式給機關首長簽核，是否可行?

最終精神-持續矯正追蹤

- PDCA(Plan、Do、Check、Action)循環
- 如：
  - 對風險評估的高風險項目、弱點掃瞄/滲透測試/原碼檢測的高風險項目，進行改善並持續追蹤
  - 對第三方利害團體的要求與期望，進行持續性的追蹤與改善
  - 對稽核結果、資通相關會議之決議結果，進行改善、追蹤與落實
  - 對委外廠商之合約要求、安全要求，進行列管、督導與追蹤
  - 對異常網路連線、系統存取錯誤紀錄、故障設備，進行處理、追蹤、改善與預防

Q：若有需要大量資源才能完成矯正作為的項目，該怎辦?

謝謝聆聽

周冠吉

E-MAIL：EDITOR@MAIL.NTPU.EDU.TW