臺北市立大學

台北市立大學
112年資訊安全管理制度(ISMS)
擴大導入輔導

專案啟始會議

簡報人：曾立民 顧問師

中華民國 112年 7 月 28 日 SafeLink 博創資訊科技股份有限公司

簡報大綱

- 壹、專案目標與範圍
- 貳、本專案預期效益
- 參、專案工作規劃與執行
- 肆、專案組織與管理
- 伍、問題討論 (Q & A)

壹、專案目標與範圍

◆專案目標：

1. 符合「資通安全管理法」及其子法之要求。
2. 修訂現有資訊安全管理制度(ISMS)。
3. 強化及改善整體資訊安全管理之能力。
4. 提供資訊安全領域之諮詢顧問服務。

◆專案範圍：

本專案以貴校 ISMS 五年深耕計畫之 112 年度擴大導入單位:「教務處(註 冊組、課務組、招生組、分區教務組)、人事室」。

貳、本專案預期之效益

- **將資安及個資保護精神深植於組織文化中**
  - **以提昇服務品質、確保資訊安全與避免個資訴訟**
- 建立整合性之內稽、內控管理制度
- 建立**以利害關係人為導向**的內部控制制度以提昇服務品質與營運績效
- 提升組織整體資安防禦能力
- 落實風險控制、內部稽核與資訊安全防護等相關教育訓練
- 降低**外部攻擊**及**內部資訊(含個資)外洩**風險

參、專案工作規劃與執行

- 專案工作時程規劃(含甘特圖及規劃表)
- 精進ISMS及ISO27001驗證輔導流程
  - 明確的ISMS輔導流程與步驟
  - 依四個構面持續落實資訊安全管理制度
  - 依五個層面提升資通安全管理績效
  - 修訂客製化之ISMS管理文件
  - 監督核心資通系統委外辦理之管理措施
  - 提供資通安全管理法(含6子法)輔導服務
  - 提供核心資訊系統弱點掃描及滲透測試服務
- 辦理資通安全教育訓練(內訓共計12hr)

專案工作時程規劃甘特圖

- 「合約書」載明本專案時程(履約期限)為：
  - 112年8月12日至112年11月30日(決標日次日起至同年11月30日止)

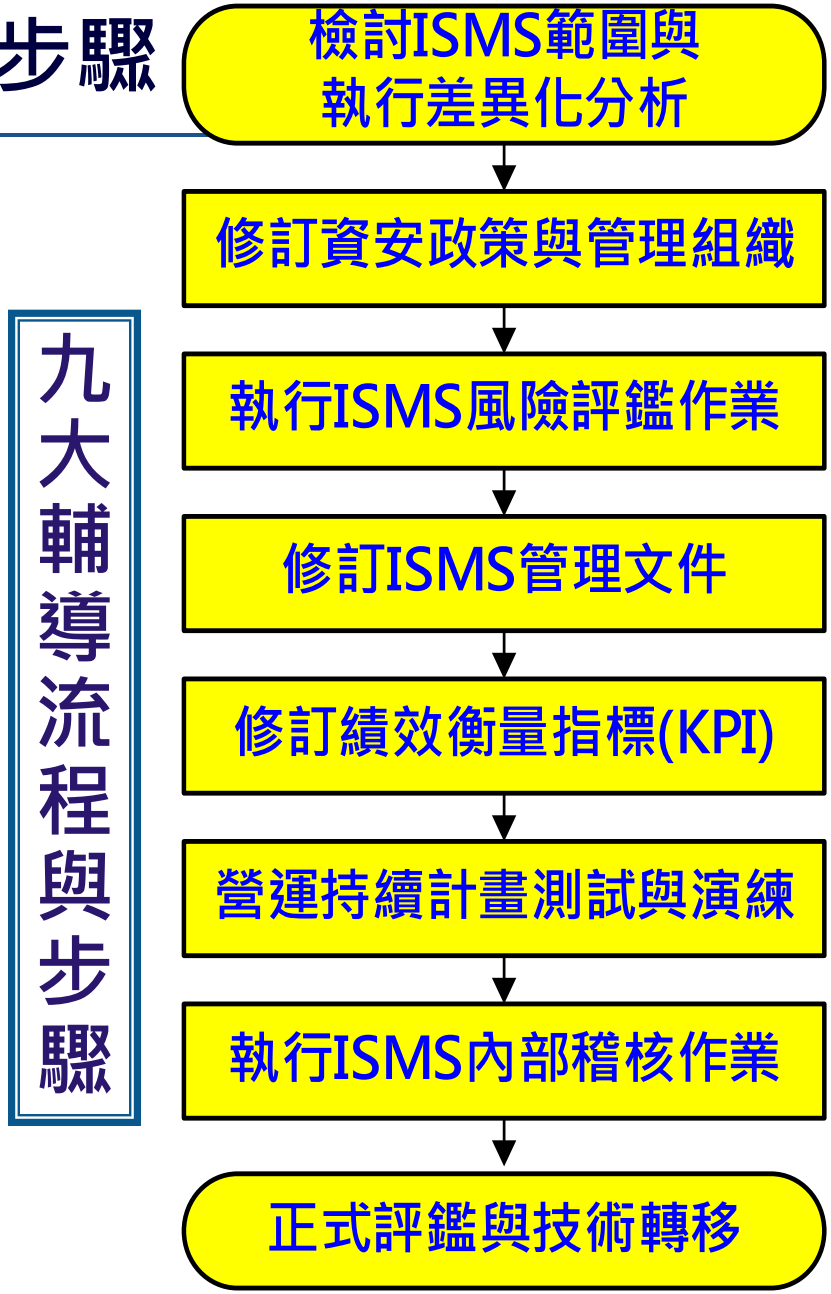
No.	工作名稱	開始	完成	2023年 08月 09月 10月 11月
1	輔導初期準備：現況需求分析與瞭解 簽署保密切結書(公司及個人)	2023/8/12	2023/8/31	
2	擬訂專案工作計畫書	2023/8/12	2023/8/31	
3	安裝資訊資產盤點及風險評鑑管理平台	2023/8/12	2023/8/31	
4	擬訂及辦理資訊安全教育訓練	2023/8/12	2023/10/31	
5	ISMS文件適用性之檢討與修訂作業	2023/9/1	2023/10/31	
6	執行資訊資產盤點及風險評鑑作業	2023/9/1	2023/10/31	
7	執行資通安全管理法輔導服務	2023/9/1	2023/11/30	
8	執行營運持續計畫測試及演練	2023/10/1	2023/10/31	
9	擬訂及執行ISMS內部稽核作業	2023/11/1	2023/11/15	
10	修正ISMS並實施改善措施	2023/11/16	2023/11/30	

專案應完成工作與交付項目

工作項目	應交付文件	契約規範交付日期	開始執行日期	預計交付日期
完成現況需求分析與瞭解	● 委外廠商及人員保密切結書 ● 專案工作計畫書	專案期間內	112/8/12	112/8/31
依據貴校資訊安全需求及各項變更事項，完成 ISMS 文件適用性之檢討與修正作業。	● 已修訂之資訊安全管理制度文件		112/9/1	112/10/31
依據貴校 ISMS 風險評鑑與管理方法及作業程序，完成 ISMS 相關資產之風險評鑑作業。	● 風險評鑑報告 ● 風險處理計畫(有不可接受風險須處理時)		112/9/1	
完成關鍵(核心)資訊系統之營運持續計畫(BCP)之演練	● 營運持續演練計畫 ● 營運持續計畫演練結果報告		112/10/1	
依據貴校內部稽核作業管理程序之規定，完成擬訂 ISMS 內部稽核計畫及執行內部稽核作業。	● 內部稽核計畫 ● 內部稽核結果報告		112/11/1	112/11/30
完成辦理資訊安全教育訓練	● 教育訓練計畫書 ● 教育訓練上課簽到表		112/8/12	

明確的ISMS輔導流程與步驟

- 輔導初期訪談診斷、檢討ISMS範圍與執行差異化分析作業
- 修訂資安政策&管理組織
- 執行ISMS風險評鑑作業
- 依資通安全法檢視及修訂ISMS管理文件
- 調整績效衡量指標(KPIs)
- 擬定營運持續計畫(BCP)與執行BCP之測試與演練
- 執行ISMS內部稽核作業
- 彙整工作與技術轉移

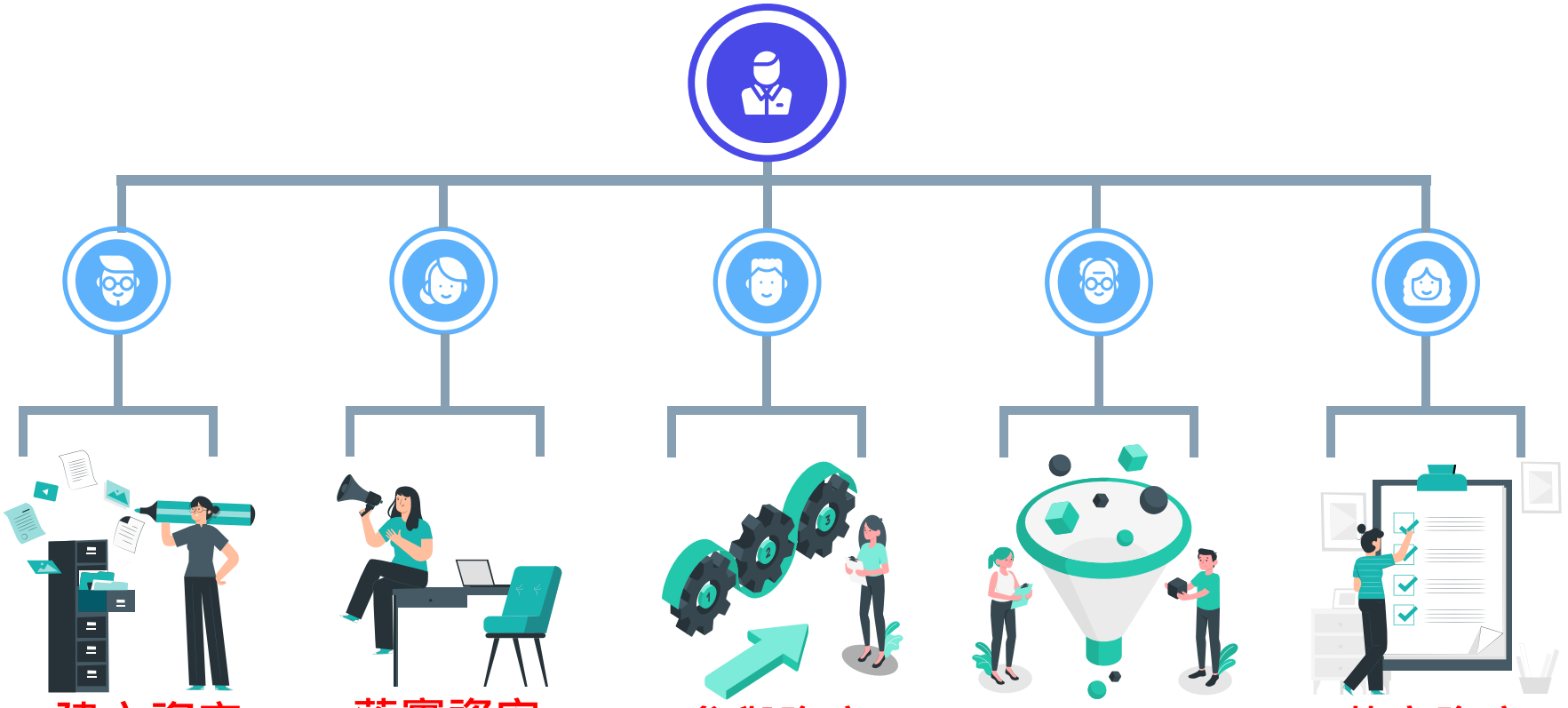


依四個構面持續落實資訊安全管理制度

策略面	管理面	技術面	防護基準
26/108	29/108	53/108	77
1.核心業務及其重要性 2.資通安全政策及推動組織 3.資安專責人力及經費配置	4.資訊及資通系統盤點及風險評估 5.資通系統或服務委外辦理之管理 6.資安維護計畫與實施情形	7.資通安全防護及控制措施 8.資通系統發展及維護安全 9.資通安全事件通報應變	存取控制、稽核可歸責性、營運持續計畫、識別鑑別、系統與服務獲得、通訊保護、系統與資訊完整性

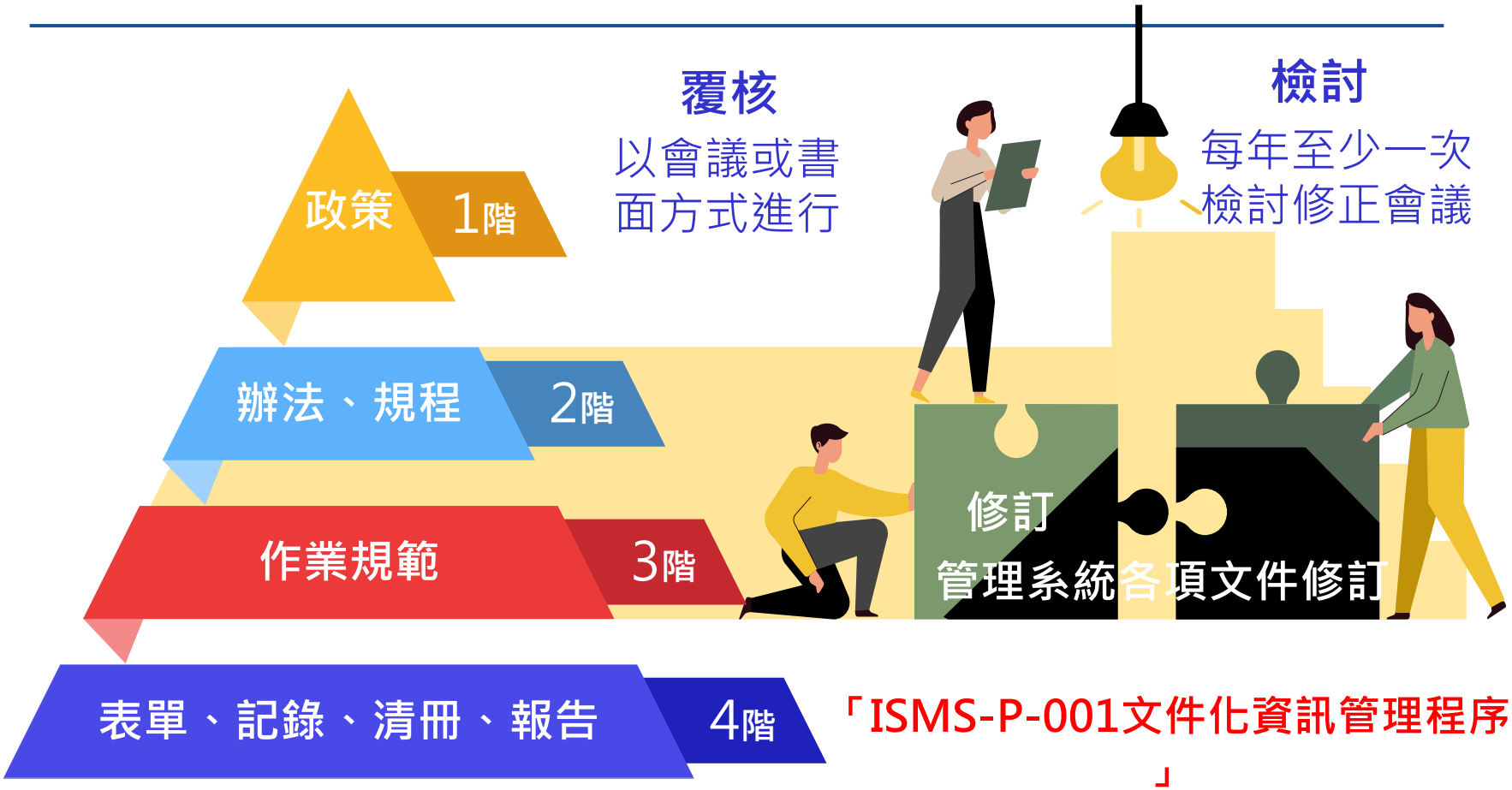
依據「資通安全實地稽核項目檢核表」與資安法「資通系統防護基準實施情形調查」確認貴局資安管理作為是否符檢核項目之法遵要求。

依五個層面提升資通安全管理績效



1.確認資安管理組織，負責推動、協調監督及審查資通安全管理事項
2.確認資安管理組織層級之適切性，且業務單位是否積極參與

修訂客製化之ISMS管理文件



「ISMS-P-001文件化資訊管理程序」

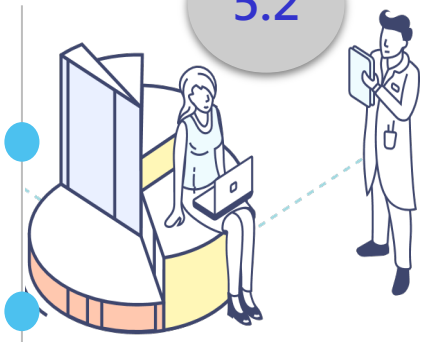
1.維運及審查及更新ISMS，確保制度符合最新法令法規
2.檢視ISMS運作紀錄之完整性及有效性，確保內控制度運作績效
3.針對重要業務訂定適當之變更管理程序，且落實管控資安風險。

監督核心資通系統委外辦理之管理措施

機關及委外廠商皆有PM

- 5.4 委外業務風險評估
- 5.6 RFP規範防護基準
- 5.5 分(轉)包資安措施
- 5.7 廠商資安管理評估
- 5.15 定期檢視人員媒體

5.2



廠商ISMS人員

5.3

- 5.11 資安責任保密規定
- 5.9 資安事件通報處理
- 5.12 定期或異常時稽核
- 5.13 廠商進出範圍限制
- 5.14 系統存取程序授權
- 5.8 系統安全檢測證明

5.1 委外安全管理程序 | 選商 | 監督 | 5.10 終止解除

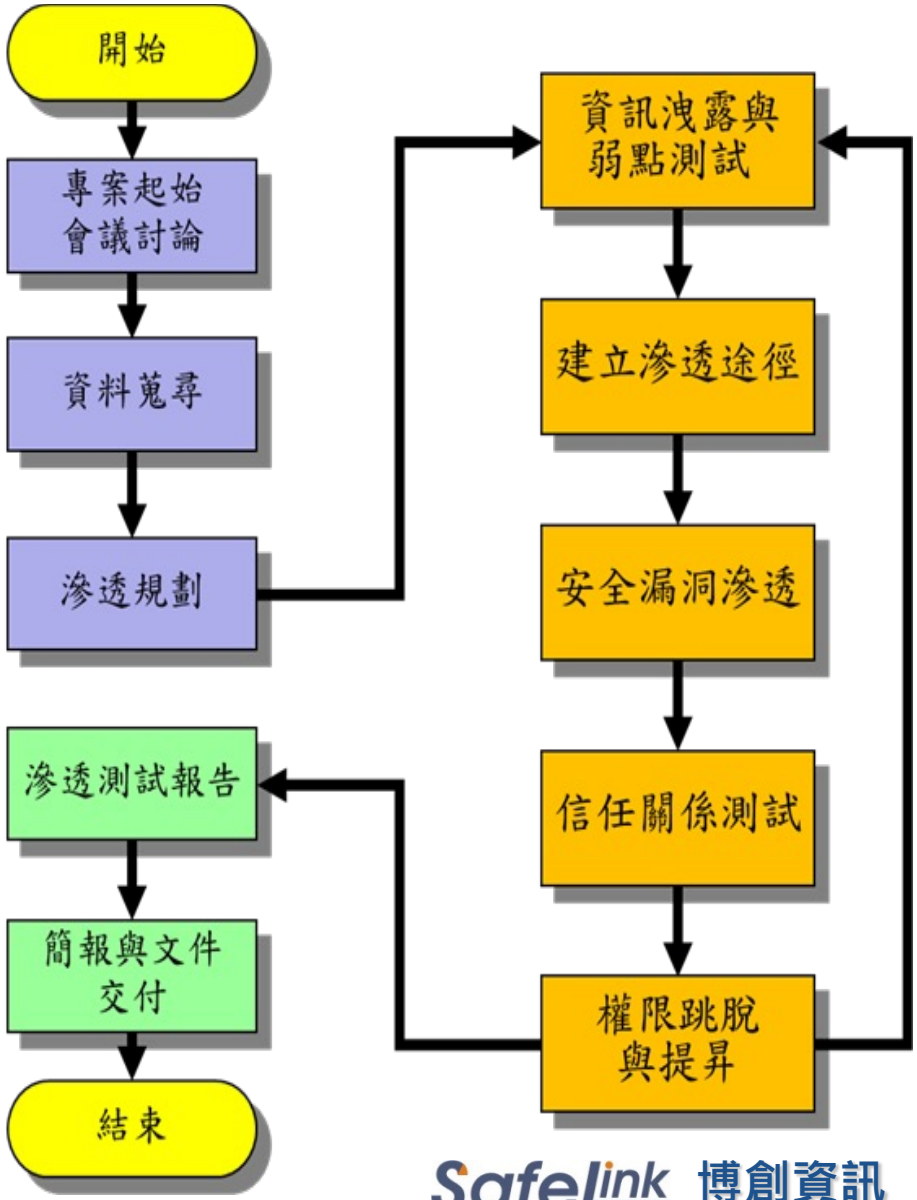
持續執行資訊作業委外安全管理程序(包含委外選商及監督相關規定)

提供資通安全管理法(含6子法)輔導服務

- 維護及修訂「**資通安全維護計畫**」
  - 每年定期依法令法規及上級機關之資通安全要求，修訂及維護「**資通安全維護計畫**」。
- 執行**資通系統分級及防護基準評估**作業
  - 依據資通系統安全等級評估結果，執行「**資通安全防護基準**」各項控制措施並追蹤改善
- 執行**資安法機關應辦事項查核**作業
  - 協助設計「**資安法C級機關應辦事項查核表**」並依據查檢項目逐項檢視「資訊安全管理制度」是否符合「資通安全管理法」之法遵要求。

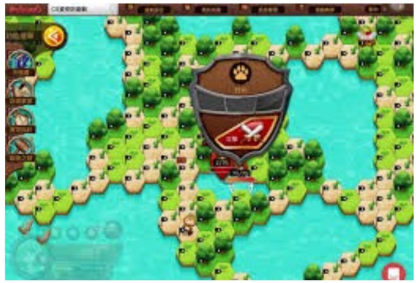
提供核心資訊系統弱點掃描及滲透測試服務

- 提供**核心資訊系統弱點掃描及滲透測試服務**(依據ISO27001標準: A.12.6.1 技術脆弱性的管理)
- 服務範圍
  - 選定貴局**核心資訊系統**進行弱點掃描及滲透測試服務
- 參考標準
  - OSSTMM
  - OWASP 等國際組織規範
- 服務效益
  - 稽核目前資安規劃之強度
  - 瞭解入侵者可能利用途徑
  - 稽核是否有資料外洩管道



資訊安全教育訓練課程規劃(內訓)

e等公務園學習平台



CS資安防衛戰

全民資安素養網

資安驗證中心課程

- 確認同仁了解資安責任**並善盡保密義務(已簽署保密協議)**
- 同仁瞭解**資安管理政策**&**個資保護管理政策**及應負之資安&個資責任
- **一般使用者**及**主管**每年接受3小時以上之資安通識教育訓練。

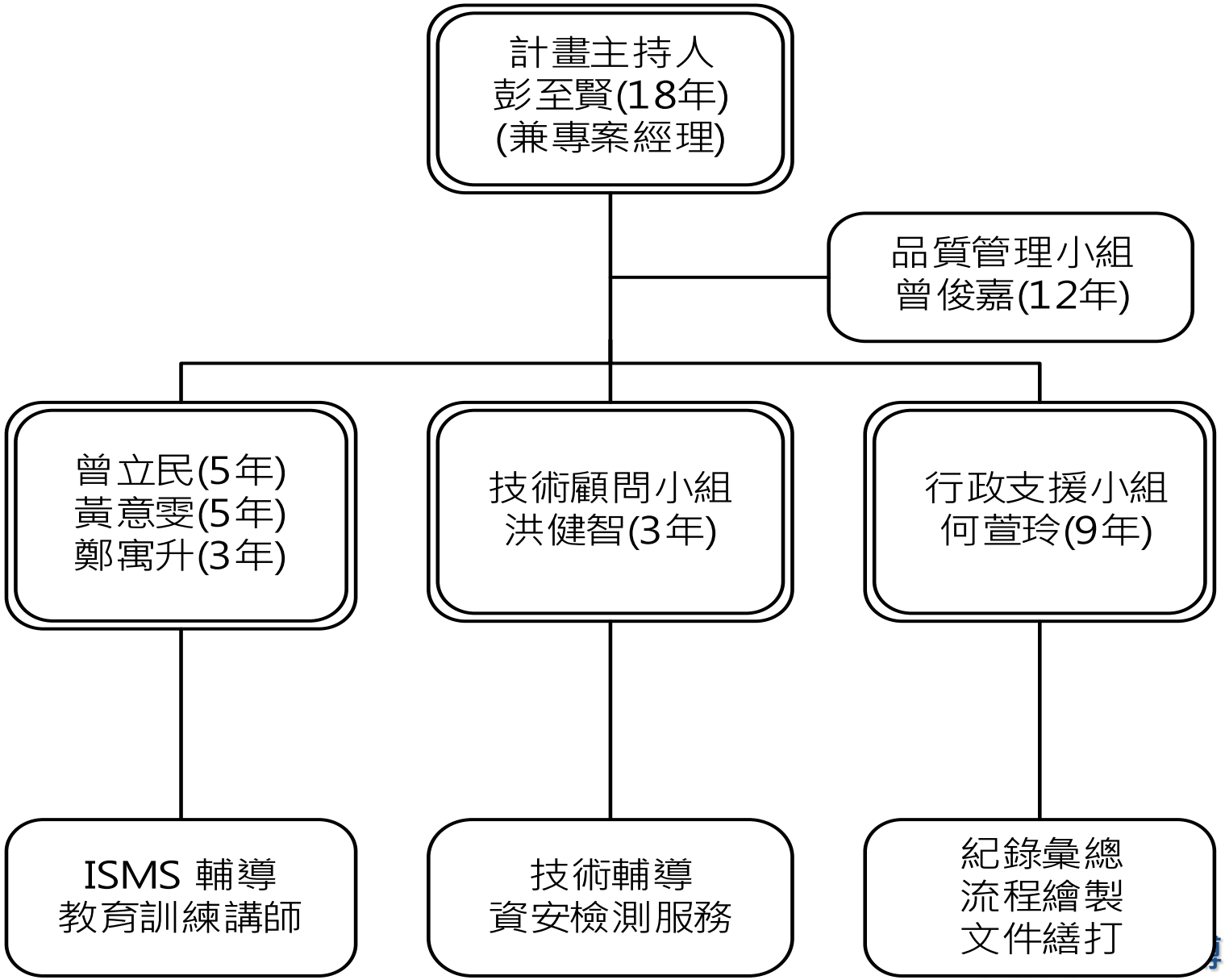
辦理資通安全教育訓練(內訓共計12hr)

課程名稱	課程大綱	上課時間	上課地點	參訓對象	授課講師	時數	梯次	時數小計
資訊資產管理概論與實務	一、概述 二、資產登錄 三、資訊安全措施規劃與執行 四、資訊資產之分類與管理 五、資訊安全措施-制度化 六、稽核與改進	預計10月	指定會議室	1.資安專責人員 2.上述資安代理人	曾立民	3	1	3
資通安全風險管理與評鑑實務介紹	一、資安風險介紹 二、資安風險評鑑 三、資安風險處理 四、資安風險評鑑實務介紹 五、結論	預計11月	指定會議室	1.資安專責人員 2.上述資安代理人	曾立民	3	1	3
ISMS基礎認知與內部稽核	一、ISMS標準簡介 二、控制項與應用 三、內部稽核簡介與應用	預11月	指定會議室	1.資安專責人員 2.上述資安代理人	曾立民	3	2	6
							總計：	12小時

肆、專業組織與管理

- 專案組織架構與分工
- 專案主要成員學經歷介紹
- 系統化專案管理方法

專案組織架構與分工


計畫主持人
彭至賢(18年)
(兼專案經理)
品質管理小組
曾俊嘉(12年)
曾立民(5年)
黃意雯(5年)
鄭寓升(3年)
技術顧問小組
洪健智(3年)
行政支援小組
何萱玲(9年)
ISMS 輔導
教育訓練講師
技術輔導
資安檢測服務
紀錄彙總
流程繪製
文件繕打

專案主要成員學經歷介紹

姓名	工作職掌	年資	學經歷、證照
彭至賢	計畫主持人 專案經理	18	**國立臺中科技大學-資訊工程系碩士** **資安與個資管理證照：** ISO27001 LA證照、ISO29100 LA證照、BS10012 LA證照、ISO 9001 LA證照、ISO27701LA證照、PMP/APMP國際專案管理師認證、微軟MCSE、IBM PSS及思科CCNA專業系統工程師認證、TPIPAS個人資料管理師證書、TPIPAS個人資料驗證師證書。 **相關經歷及專長：** ISO27001 / ISO9001 / ISO20000 / ISO22301 / ISO10015 / ISO27701驗證、資訊系統整合與管理、弱點掃描及滲透測試管理、TTQS人力資源規劃管理等。
曾俊嘉	品質管理小組 品質管理師	12	**逢甲大學-資訊工程學系 學士** **個資保護管理證照：** ISO27001 LA證照、ISO27701 LA證照、BS10012 LA證照、ISO29100 LA證照。 **相關經歷及專長：** ISO27001 / ISO27701 / BS10012 / ISO9001相關專案品質控管、人際關係管理、系統分析與程式撰寫、資訊系統平台規劃與建置。

專案主要成員學經歷介紹(續)

姓名	工作職掌	年資	學經歷、證照
曾立民	輔導顧問小組 輔導顧問師 教育訓練講師	5	國立高雄第一科技大學-金融學系 東海大學-資訊工程碩士（就讀中） 資安與管理證照： ISO27001 LA證照、ISO27701 LA證照、BS10012 LA證照、ISO29100 LA證照、內部控制與內部稽核訓練證明、資訊安全工程師(初級)證書。 相關經歷及專長： ISO27001(ISMS) / ISO27701 & BS10012(PIMS) 建置輔導及驗證、資通安全與個人資料保護管理。
鄭寓升	輔導顧問小組 輔導顧問師	4	國立臺北商業大學-商品創意經營系 資安與管理證照： ISO27001 LA證照、ISO27701 LA證照、BS10012 LA證照、ISO 29100 LA證照、ISO 27017 LA證照。 相關經歷及專長： ISO27001(ISMS) / ISO27701 & BS10012(PIMS) 建置輔導及驗證、資通安全與個人資料保護管理。

專案主要成員學經歷介紹(續)

姓名	工作職掌	年資	學經歷、證照
黃意雯	輔導顧問小組 輔導顧問師 教育訓練講師	3	文化大學-企業管理學士 資安與管理證照： ISO27001 LA證照、ISO27701 LA證照、BS10012 LA證照、ISO29100 LA證照。 相關經歷及專長： ISO27001(ISMS) / ISO27701 & BS10012(PIMS) 建置輔導及驗證、資通安全與個人資料保護管理。

專案主要成員學經歷介紹(續)

姓名	工作職掌	年資	學經歷、證照
洪健智	技術顧問小組 技術顧問師	3	**國立勤益科技大學-資訊工程系** **資安與管理證照：** 電腦軟體應用、硬體裝修、網頁開發設計、資訊系統整合與管理。 **相關經歷及專長：** 「個資盤點及風險評鑑管理工具」及「資訊資產盤點及風險評鑑管理工具」建置及維運。
何萱玲	專案秘書	9	**亞洲大學-保健營養生技學系** **管理與技術證照：** HACCP食品安全管制系統-基礎及進階證書、食品檢驗分析技術士丙級證照、食品技師證書。 **專案工作內容：** 處理本專案各項行政事宜（文件編製、紀錄彙總、相關流程繪製）。

系統化專案管理方法

- 定期及不定期召開
- 檢驗專案執行狀況
- 界定面臨重要問題

- 定期彙整工作進度
- 完成工作項目報告
- 進度與問題之檢討

- 電話或實地訪談調查
- 問題缺失追蹤與解決改善
- 落後原因及補救措施

- 輔導開發之ISMS管理文件是否符合需求
- 不符合事項追蹤與矯正

- 里程碑查核
- 指定監控項目審查
- 發現問題即時矯正

- 交付項目審查
- 前版審查缺失改善
- 審核驗收結果

- 內部每月審查
- 檢討專案狀況
- 預期目標達到

- 建立度量目標
- 資料蒐集與儲存
- 度量與分析結果

簡報完畢

敬請各位長官的
批評與指導

機敏個資不遮罩，
內神外鬼馬上到！