KPMG

TSP應如何打造安全的環境以創造金融生態圈

讓銀行放心與您界接

April, 2020

郭宇帆

KPMG 安侯企業管理股份有限公司
資訊科技諮詢服務 / 協理

seraphkuo@kpmg.com.tw

行業專長

- 金融業
- 高科技業
- 製造業
- 電子商務

相關國家之服務經驗

台灣　香港
美國　中國
新加坡

專業資格

- PMP國際專業管理師
- CHFI電腦駭客鑑識偵查員
- ISO 27001主導稽核員
- BS 10012主導稽核員
- ISO 22301 主導稽核員

專長領域

- 資訊安全管理系統導入
- 系統弱點評估及資訊系統強化
- 網路安全評估及滲透測試
- 機敏資料(營業秘密)安全保護
- 電子支付系統安控顧問諮詢
- 資安事件緊急應變能力調查
- 資訊風險管理策略及程序優化
- 金融風險顧問咨詢服務
- 海外外判法令遵循

專業經歷

- 安侯企業管理股份有限公司 Advisory 協理
- 勤業眾信聯合會計師事務所 ERS 經理
- 群環科技 加值服務事業群 資安產品經理
- 數聯資安 資安顧問/專案經理
- 鈺松國際 專案經理

講師經驗

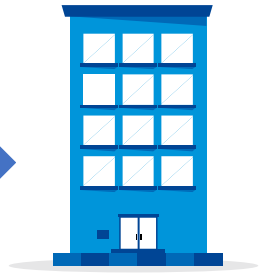
- 金融研訓院
- 大型半導體產業
- 投信投顧公會
- 電腦稽核協會
- TSIA IC設計委員會
- 資安人
- 新竹半導體協會
- 證基會
- 證券公會

於資訊安全與個人資料保護角度下，開放銀行面臨之衝擊

金融機構

高度監理

- 資訊安全控管程度高
  - ✓ 資通安全管理法
  - ✓ 金融機構內稽內控辦法
  - ✓ 各局發布之函文
  - ✓ 各金融機構公會頒佈之資訊安全自律規範
  - ✓ ISO27001
- 個人資料保護程度高
  - ✓ 個人資料保護法及其細則
  - ✓ 金融監督管理委員會指定非公務機關個人資料檔案安全維護計畫
  - ✓ BS10012



TSP業者

金融監督管理委員會

臺灣TSP業者應該建構資安與個資控管

第一階段

① 進行欄位格式檢查內容
② 採用TLS1.2(含)以上之通訊協定
③ 正面表列並限制僅接受所需之HTTP請求方法
④ 採取連線限制與逾時中斷等機制，以防範分散式阻斷攻擊
⑤ 使用HTTP強制安全傳輸協議(HSTS)

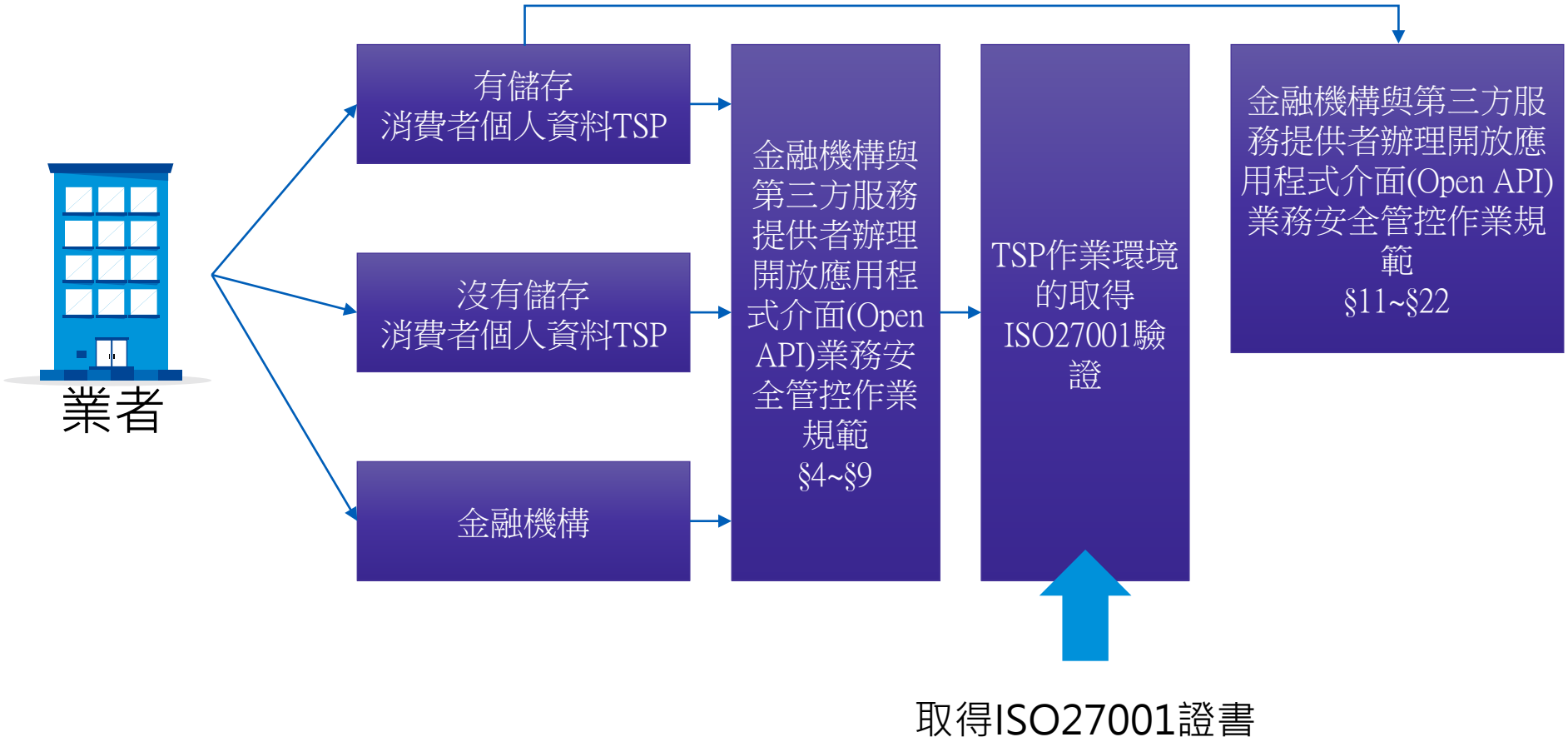
第二階段

金融機構與第三方服務提供者辦理開放應用程式介面(Open API)業務安全管控作業規範

① 消費者註冊時之身份確認安全設計、消費者資訊查詢之身份確認安全設計、網路型態與其安全設計、設計原則之共通要求與各類安全要求
② 資訊安全管理機制 ISO27001
③ 每年由公正第三方出具資訊系統及安全控管作業評估報告

參考資料: 財金資訊

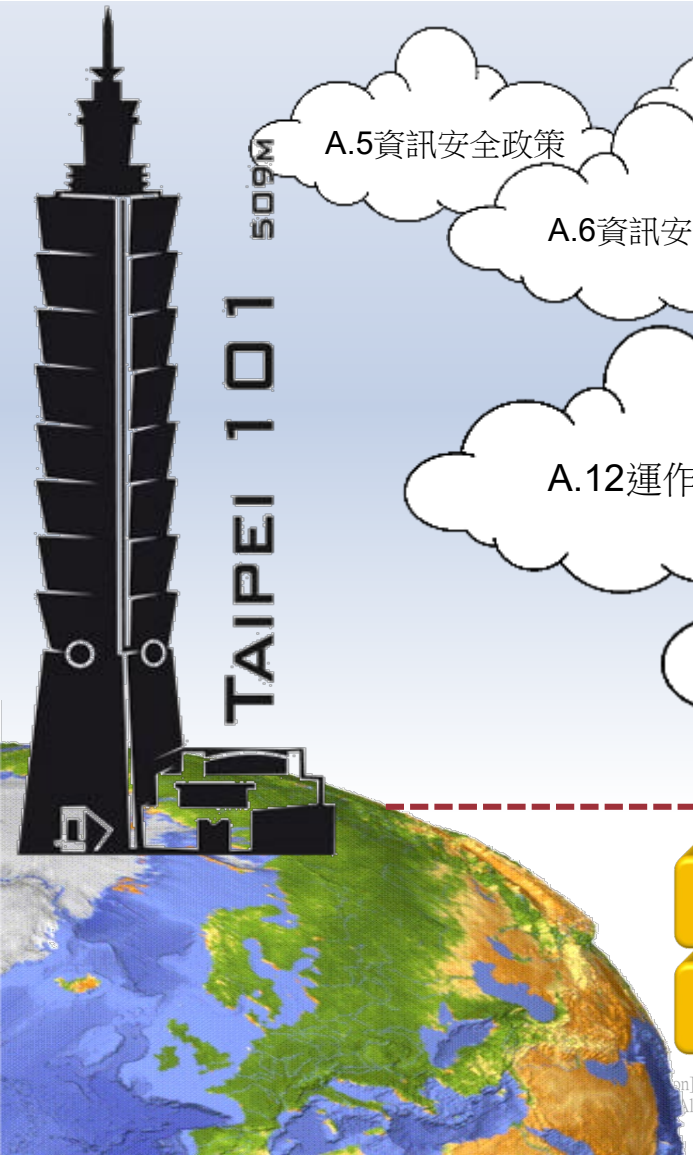
TSP業者需如何符合法規要求?



為你的TSP系統與資訊環境取得ISO27001為你晉升成為TSP業者首要任務

台灣的本土銀行幾乎皆取得ISO27001證書

ISO27001:2013所涵蓋之範圍



A.5資訊安全政策

A.8資產管理

A18遵循性

A.7人力資源安全

A.6資訊安全組織

A.14 系統獲取、開發及維護

A.16資訊安全事故管理

A.17營運持續管理的資訊安全層面

A.9存取控制

A.10密碼學

A.12運作安全

A.13通訊安全

A15供應者關係

A.11實體與環境安全

14大控制領域

風險評鑑

內部稽核

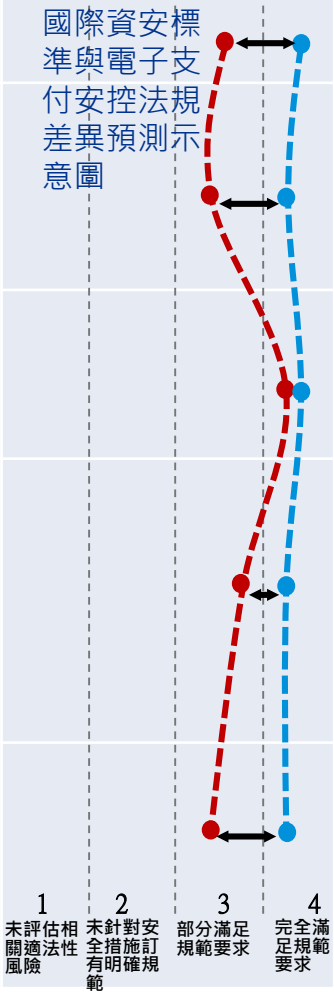
文件紀錄

管理審查

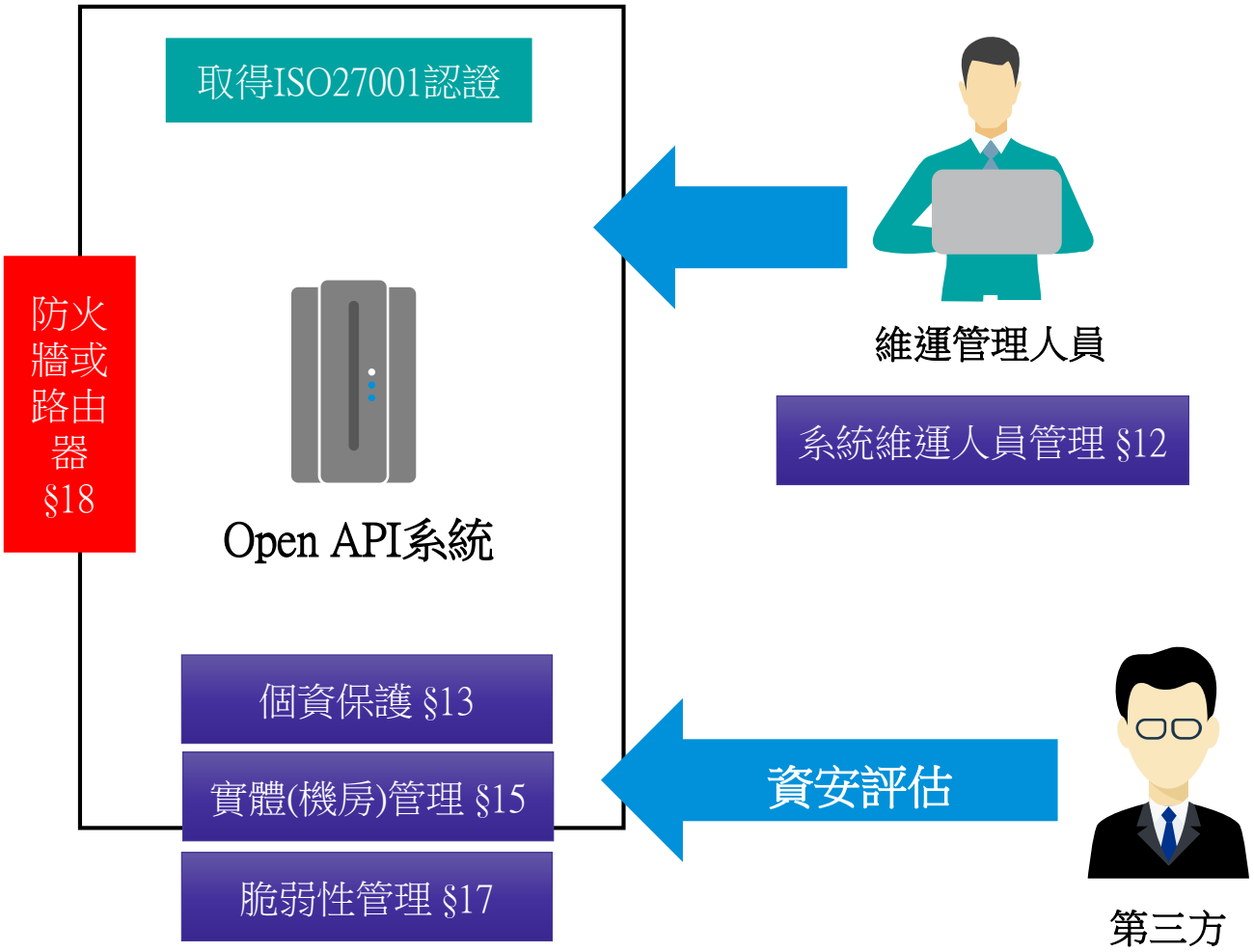
本文要求

安控基準VS ISO27001

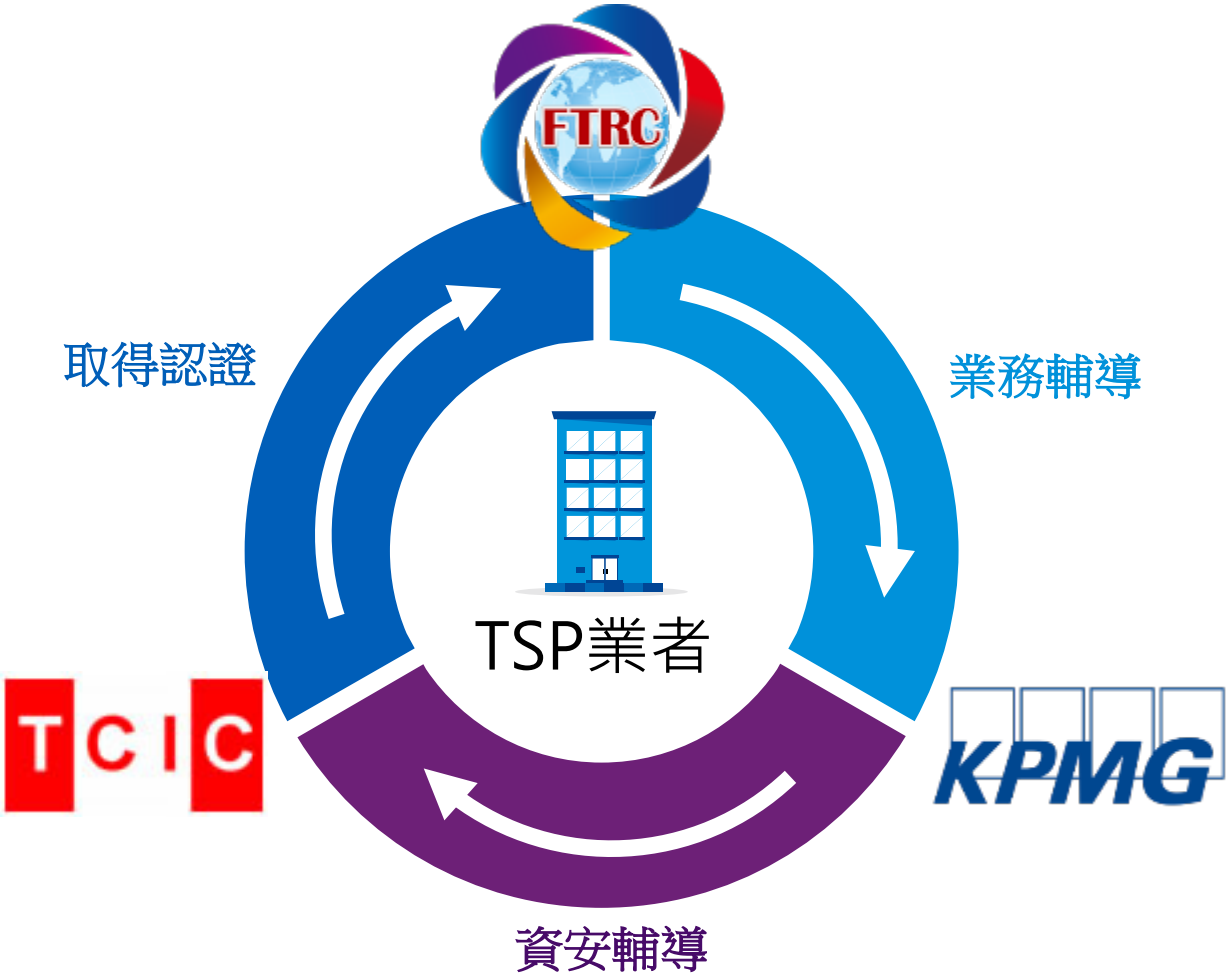
分類	安控基準	ISO 27001:2013	適法性成熟度評估範例
身分確認	第3條：註冊身分確認 第4條：登入身分確認	A.9 存取控制	國際資安標準與電子支付安控法規差異預測示意圖
交易安全	第6條：消費者資訊查詢安全規定 第7條：消費者資訊查詢交易安全設計說明 第8條：消費者資訊查詢之TSP平台設計原則 第9條：金融機構與TSP業者間設計共通要求 第10條：金融機構與TSP業者間設計安全要求	A.9 存取控制 A.10 密碼學 A.13 通訊安全 A.14 系統獲取、開發與維護	
營運控制	第11條：資安政策、內部組織與資產管理	A.5 資安政策 A.6 資安組織 A.7 人力資源安全 A.8 資產管理	
	第12條：系統維運人員管理 第13條：個資保護 第16條：營運管理 第20條：委外管理 第21條：資安事故管理 第22條：營運持續管理 第23條：法令遵循性	A.9 存取控制 A.18 遵循性 A.12 運作安全 A.15 供應者關係 A.16 資安事故管理 A.17 營運持續管理 A.18 遵循性	
技術控制	第14條：機敏資料隱私與金鑰管理 第15條：實體安全 第17條：脆弱性管理 第18條：網路管理 第19條：SDLC	A.10 密碼學 A.11 實體環境安全 A.12 運作安全 A.13 通訊安全 A.14系統獲取、開發與維護	



你需要跨出的第一步….



KPGM、政大與TCIC攜手合作，協助您取得ISO27001證書



KPMG協助您打造TSP系統的資訊安全環境

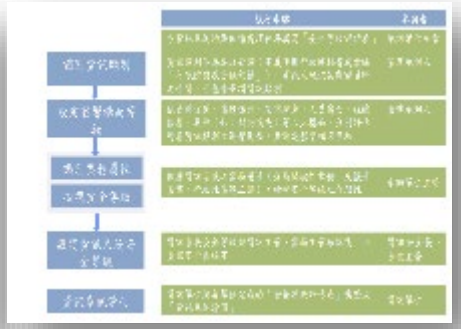
定義ISMS驗證範圍

以TPS系統做為驗證範圍，其相關之資訊作業皆在ISO27001導入之活動內

驗證範圍重要方法與步驟

完整評估資安目標、關注方期望、資源與現有或未來風險

依據系統重要性分類分級



依據貴公司組織架構，進行資安任務指派與分工

選定資安範圍與目標後，充分與組織成員進行溝通

ISMS導入規劃說明






第一檢查點 | 進行輔導訓練 | 資安制度建立 | 資安文件撰寫 | 第二檢查點 | 新技術與新科技 | 管理制度實施 | 第三檢查點 | 專家與單位人員意見 | 第四檢查點 | 第五檢查點

工作進度

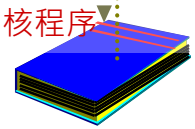
10% | 38% | 75% | 88% | 100%

工作步驟

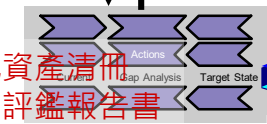
- 專案啟動
- 建立資訊安全政策及組織
- 資安風險評鑑作業準備
- 風險(含技術)評鑑作業
- 風險處理作業
- 資安管理架構制訂
- 資訊安全實施及操作
- 永續營運管理計畫
- 資安事件通報及回應機制
- 內部稽核及管理審查
- 進行驗證

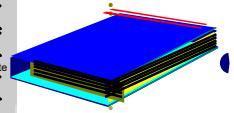
主要產出項目

- 資訊資產清冊
- 資訊安全政策文件
- 資訊安全管理組織文件
- 文件管理程序
- 內部稽核程序

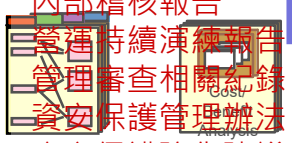


- 資訊資產清冊
- 風險評鑑報告書
- 風險評鑑工具
- 風險改善計畫





- 資訊安全四階文件



- 內部稽核報告
- 營運持續演練報告
- 管理審查相關紀錄
- 資安保護管理辦法
- 資安保護強化建議

稽核與審查

TCIC

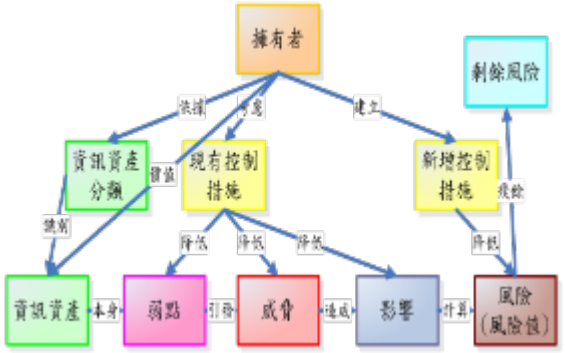
資訊安全管理制度之建立

建立資訊資產清冊

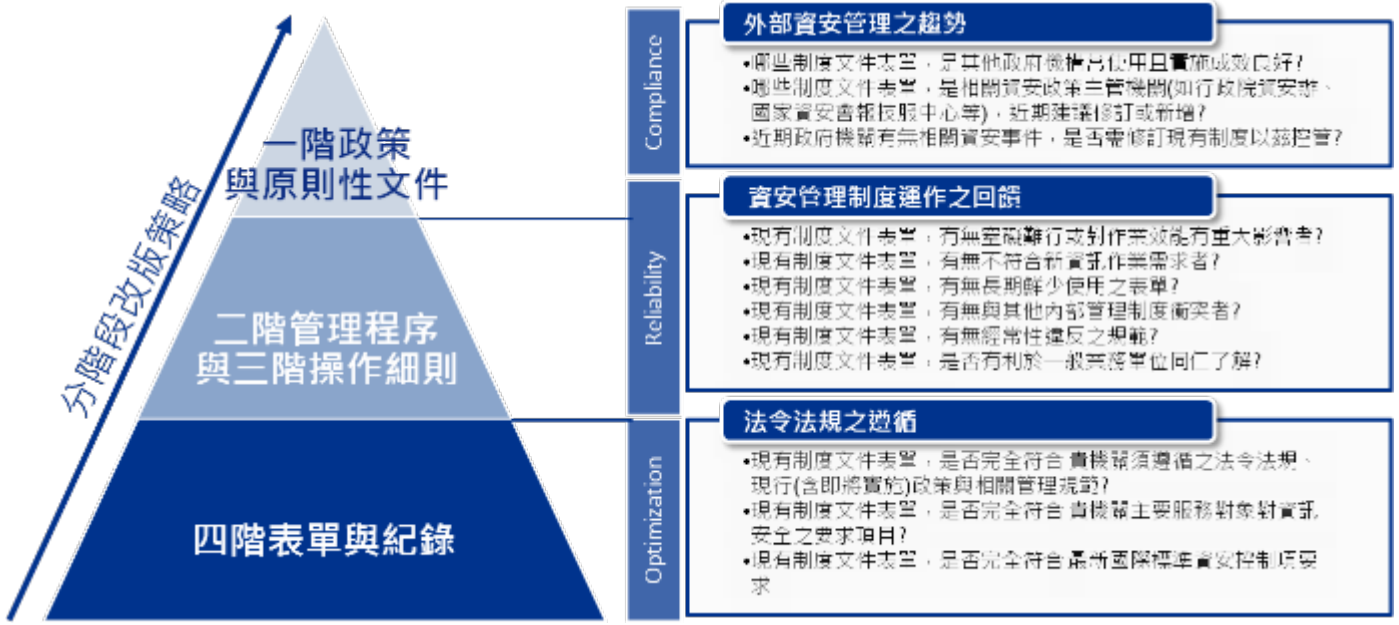
將資訊安全管理系統之資訊資產依據分類列示之清單，包含進行資訊資產分類與群組、評定資訊資產價值與識別資產管理者、擁有者與使用者

進行風險評鑑作業

找出資訊作業所面臨在機密性、完整性、可用性潛在之資訊安全風險，進而能加強各項管控措施以降低、轉移各項重大風險之影響



打造資訊安全管理制度文件



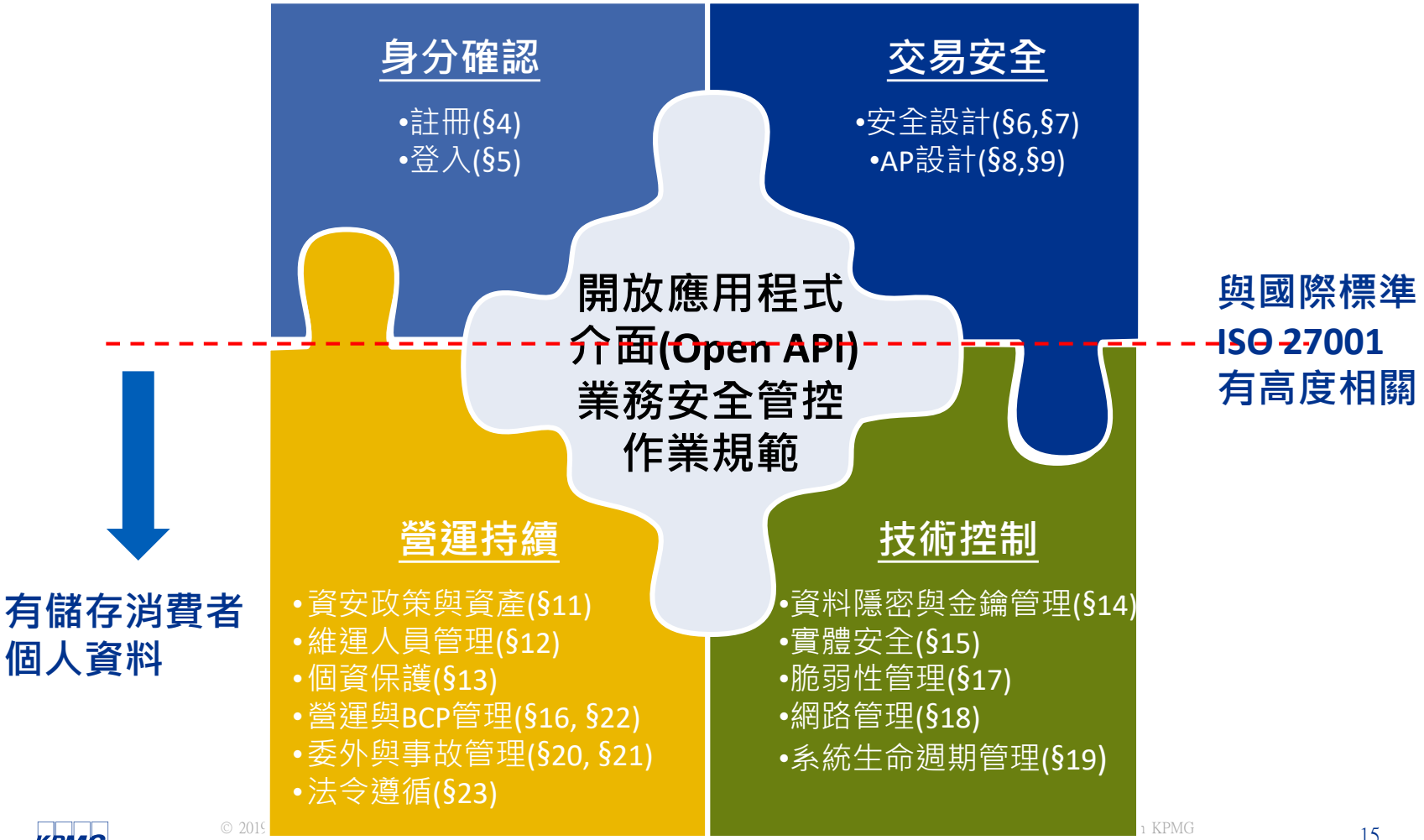
資安政策　存取控制管理　加解密機制管理

網路安全管理　專案管理　變更管理　系統獲取、開發及維護管理

人員安全管理規範　監視、量測與服務水準控制規範　文件管理規範

委外作業規範　矯正預防規範　事件通報與應變規範

於制度中需納入開放應用程式介面(Open API)業務安全管控作業規範



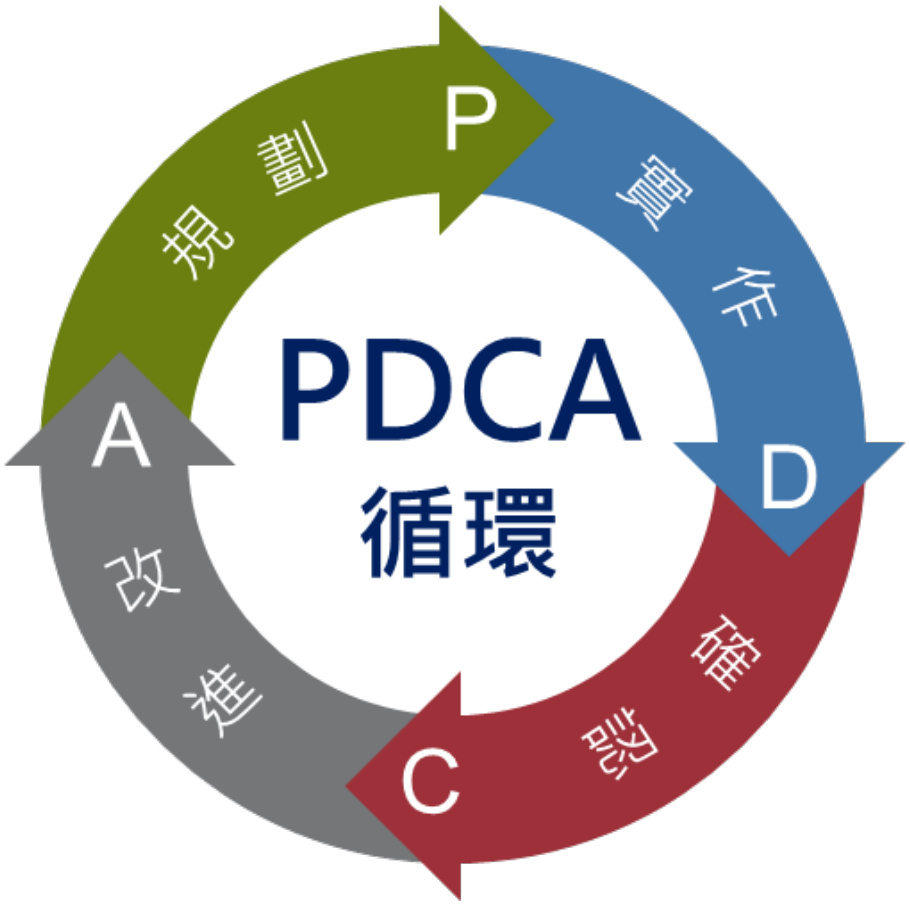
控管深度需符合法規要求

技術控制

§17 脆弱性管理

- 網頁程式異動偵測
- 惡意網站偵測
- 入侵防禦系統
- 防毒系統
- 上網管制
- 資安情資掌握
- 電子郵件社交工程演練(每年)
- 弱點掃描(每季)
- 原始碼檢視(每半年)
- 滲透測試(每年)

將ISO27001融入公司資訊運作



取得ISO27001是開始
而不是結束

ISO27001著重在落實
於日常維運中

謝謝聆聽
問題與討論

KPMG

Contact

郭宇帆 協理
+886 2 8101 6666 ext. 15754
seraphkuo@kpmg.com.tw

林軒宇 經理
+886 2 8101 6666 ext. 13915
tigerlin@kpmg.com.tw