資安推動重點工作

113年11月

報告大綱

資訊作業委外安全管理

1. 政府機關雲端服務應用資安
2. 113年資安服務共同供應契約
3. 限制使用危害國家資通安全產品
4. 委外管理之常見稽核發現

近期資安政策宣導

1. 112年度資安治理成熟度結果
2. 政府資安人員職能轉換訓練

資訊作業委外安全管理

1.政府機關雲端服務應用資安

政府機關雲端服務應用資安

◘ 機關使用雲端服務可參考國家資通安全研究院公布之【政府機關雲端服務應用資安參考指引】

種類	機關責任	雲端服務提供者責任
SaaS	• 確認遵循個人資料保護法、國家機密保護法 • 維護使用者帳號管理系統 • 管理使用者帳號與驗證	• 提供基礎設施支援(場所、電力、冷卻系統、電纜等) • 確保實體安全與可用性(伺服器、儲存裝置、網路頻寬等) • 負責應用服務與作業系統(OS)之更新與強化作業 • 資通安全機制之建立與維護(如防火牆、IDS/IPS、防入侵機制、防範惡意軟體之控制措施或封包過濾等) • 系統日誌留存與監控

（以SaaS為例）

參考指引下載： https://s.moda.gov.tw/qT8BKGCx5DoJ

使用者端安全性設定

例如，但不限於：

- 啟用雙重驗證機制
- 關閉信件自動預覽
- 封鎖外部圖檔
- 安全性設定檢查

雲端服務採購作業資安要求

- 為降低政府機關建置或使用雲端服務可能風險，辦理雲端服務採購作業建議參考行政院公共工程委員會113年5月17日公布之【資訊雲端服務採購契約範本】

限制資料存取、備份及備援所在地

機關雲端資料之存取、備份及備援之實體所在地不得位於大陸地區（含香港及澳門地區），且不得跨該等境內傳輸相關資料。

明定留存日誌(Log)6個月

☑應用程式日誌(AP log)　☑登入日誌(logon log)

☑網站日誌(web log)　☑作業系統日誌(OS event log)

雲端業者須符合ISO/CNS標準

☑CNS/ISO 27001
(資訊安全管理系統要求事項)

☑CNS/ISO 27018
(公用雲PII 處理者保護個人可識別資訊(PII)之作業規範)

機關得視情形勾選，並納入採購契約規範

契約範本下載：https://s.moda.gov.tw/K955kszbxp71

切　結　書（範例）

本廠商＿＿＿＿＿＿參與（招標機關）辦理（標的名稱）招標案，對於廠商之責任，包括刑事、民事與行政責任，已充分瞭解相關之法令規定，並願確實遵行，簽結承諾事項如下：

四、本公司及涉及本案之分包廠商，是否於中國大陸地區(含香港、澳門)設立相關團隊據點？如是，則該據點與本案履約間之關係為何？

☐否，本公司及涉及本案之分包廠商，皆未於中國大陸地區設立相關團隊據點。

☐是，該據點與本案履約間之關係，說明如下：

五、本公司針對本案所提供機關(共用)產品或服務之所屬一切資料存取、備份及備援之實體所在地是否有置於中國大陸地區(含香港、澳門)之情形？或跨該等境內傳輸相關資料？

☐否，本公司針對本案所提供機關(共用)產品或服務之所屬一切資料存取、儲存、備份及備援等作業，皆無置於中國大陸地區(含香港、澳門)之情形，且未經該等境內傳輸相關資料。

☐是，有置於中國大陸地區(含香港、澳門)或該等境內傳輸相關資料，說明如下：

投標廠商：　　（簽名蓋章）

「資料所在地及跨境傳輸切結書」可參考本署官網/相關作業指引

切結書範本下載：https://s.moda.gov.tw/MuZA8cRY1WhA

2. 113年資安服務共同供應契約

113年共同供應契約-新增紅隊演練服務

- 資通安全服務：新增第7組-「紅隊演練服務」

資安服務

原有服務

- 資安健診服務
- 資通安全威脅偵測管理服務
- 弱點掃描服務
- 滲透測試服務
- 社交工程演練服務
- 防火牆服務

新增

- 紅隊演練服務

於演練過程中，雙方視情況得異動演練目標，且經雙方同意後執行

紅隊演練服務預定於11月初上架共契，共7家廠商符合投標資格，可至「資訊服務採購網」查詢相關資訊

建議適用對象

- ✓ 已完善資安法遵事項，具一定規模資安防護能力
- ✓ 完成資訊資源向上集中之機關

服務目標

- ✓ 取得至少1個機關指定之控制權
- ✓ 取得至少1項機關指定之資訊類資訊資產

服務內容

1. 執行服務(演練)目標之演練工作
2. 完成交付文件
   (1)工作計畫書
   (2)初測及複測報告

資安服務廠商評鑑

- 為協助政府機關導入優質民間資安服務廠商，廠商評鑑結果將提供機關選擇委外廠商之參考

資安服務評鑑類別

1. SOC服務
2. 資安健診
3. 弱點掃描
4. 滲透測試
5. 社交工程演練

評鑑方式

機關評鑑 (30%)
由採購機關進行評鑑

委員評鑑 (70%)

本署前以10月9日資安法規字第1135000313號函請各採購機關協助填復「113年資安服務廠商評鑑表」，後續將納入機關評鑑分數

評鑑結果

【評鑑分數】

A級	90分(含)以上者
B級	80分(含)以上，且未滿90分者
C級	70分(含)以上，且未滿80分者
D級	60分(含)以上，且未滿70分者
E級	未滿60分者

參考連結：https://s.moda.gov.tw/vMbsqJuLoYts

3.限制使用危害國家資通安全產品

盤點陸牌設備方法

簡報內容現場展示

確認陸牌產品方式

簡報內容現場展示

4.委外管理之常見稽核發現

113年委外管理相關稽核發現

相關建議

廠商資安作為評估

檢視廠商資安作為 → 評估可能風險 → 規劃並執行控制措施 → 確認執行紀錄 → 保存文件以供未來查核

契約要求

參考工程會範本 → 施行細則第4條規定 → 擬定採購規範 → 招標文件自檢表 → 檢視招標文件

委外管理程序落實

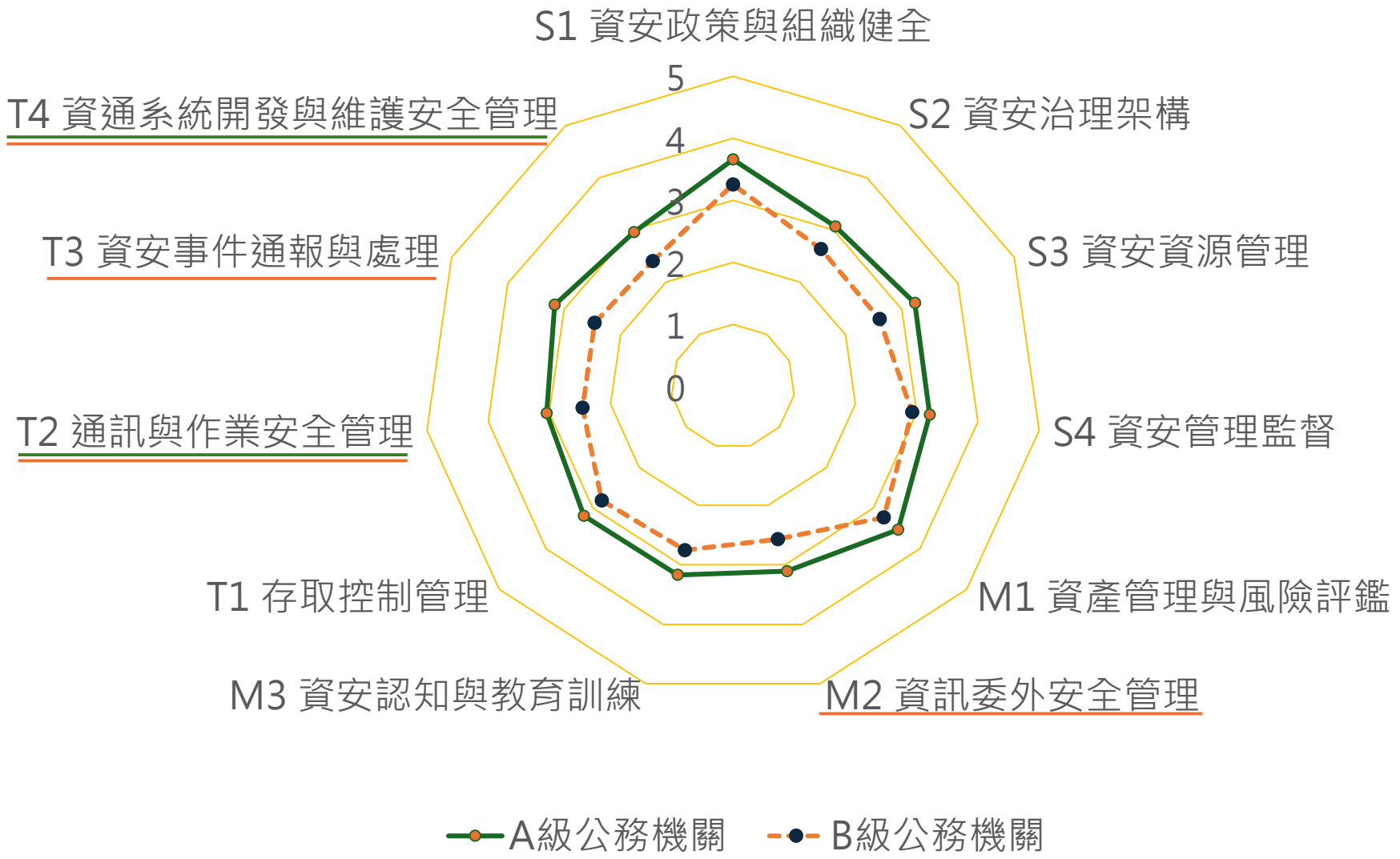
簽訂保密切結 → 人員、設備進出管制 → 遠端連線控管 → 委外廠商稽核 → 資料返還、銷毀

近期資安政策宣導

1. 112年度資安治理成熟度結果

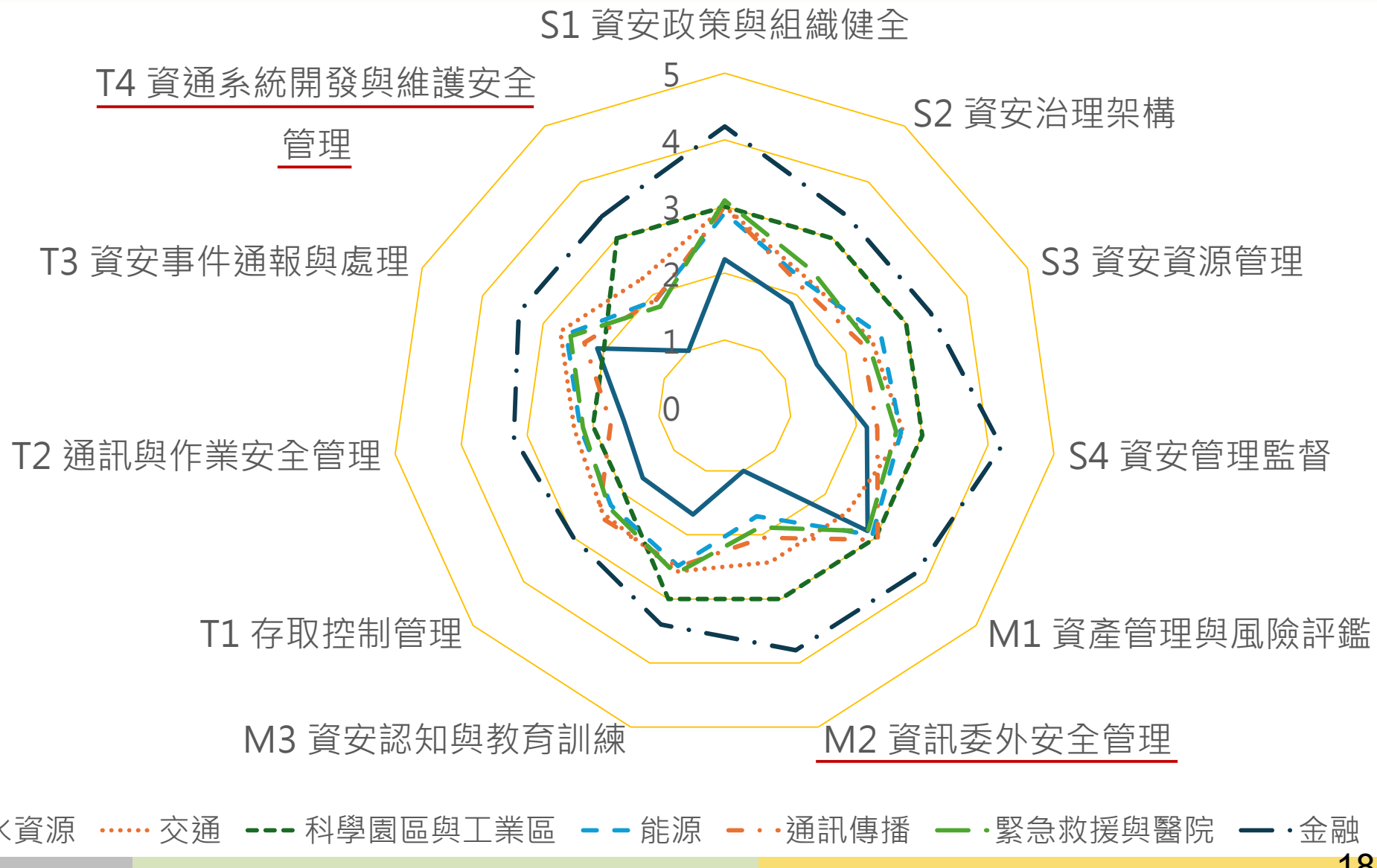
112年度公務機關IT資安治理成熟度評估結果

- A級機關在各資安構面表現均較B級機關佳
- **A級公務機關弱項為：**
  - ①T2.通訊作業管理面
  - ②T4.資通系統開發與維護安全管理
- **B級公務機關弱項為：**
  - ①M2.資訊委外安全管理
  - ②T2.T3.T4.技術面能力度相對較弱



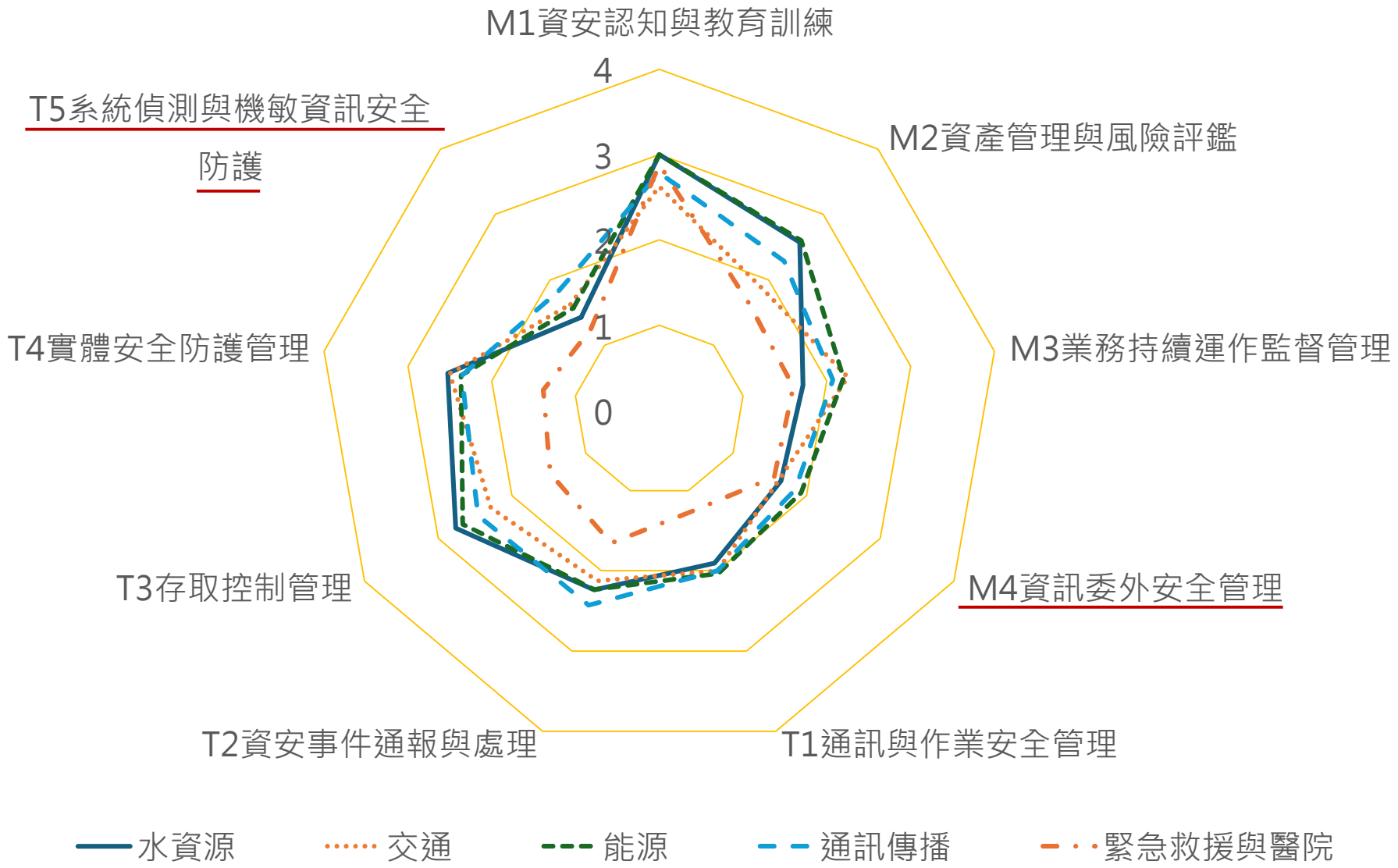
112年度CI提供者IT資安治理成熟度評估結果

- 金融、科技之關鍵基礎設施領域表現較佳，而水資源領域尚須努力
- 整體CI領域資安防護弱項：
  - **①M2.資訊安全委外管理**
  - **②T4.系統開發與維護管理**



112年度CI提供者OT資安治理成熟度評估結果

- 多數CI領域在**資安認知與教育訓練**能力度較佳。
- 各領域在OT工控領域構面差異明顯，**醫療領域面臨的困境較多**。
- 整體CI領域資安防護弱項：
  - **①T5.系統偵測與機敏資訊安全防護**
  - **②M4.資訊委外安全管理。**



2.政府資安人力職能轉換訓練

政府資安人力職能轉換訓練(1/2)

轉換訓練

- 修習**20學分或360小時**以上相關專業科目，取得**轉任資訊處理職系資格**
- **開課資訊**(包含開課學校及課程)本署將**發函相關機關**，並於本署**網站公告**
- 學員依需求參加**全修班**及**選修班**

課程內容

學校開設學分課程 18學分

【課程配當】
高考專業科目
(資訊處理4選2、資通安全3選2)
資訊相關課程
(5選2：程式設計、軟體工程、作業系統、系統分析與設計、人工智慧)

授課時數達18小時為1學分

資安職能 2學分
(資通安全概論 +1門專業選修)

= 符合轉任20學分(360小時)

- 由學校提交**開課計畫**，經**審查**通過後，列入本署**公告開課資訊**
- 現正於學校修習轉換訓練課程者，可通知該校洽本署提交開課計畫事宜

開課時間

費用核給

政府資安人力職能轉換訓練(2/2)

轉換訓練

課程內容

- 本專案113-114年學分班，**名額有限敬請把握，盡速完訓。**
- 學員須於**114年底前完訓**，始得核給自付費用
- 預11月上旬通知機關轉知擬參訓學員(由機關**薦派者優先保障**)

開課時間

- 利用**公餘時間**學習
- 預定113年**11月下旬**開課，訓期約6~8個月

費用核給

學員自付費用
給本專案同意之開課學校

完成規定課程
核給自付費用
80%

取得職能證書
核給自付費用
+15%

從事資安工作
核給自付費用
+5%

- 資安工作之職務內容為何？可參見本署官網FAQ3.2.
- 檢具**服務機關認可**從事資安工作資料，以核給費用