資通安全管理法

採購指引懶人包 A級

經濟部工業局廣告

指導單位｜行政院資通安全處
主辦單位｜經濟部工業局
受委託單位｜財團法人工業技術研究院
執行單位｜中華民國資訊軟體協會

前 言

民國 105 年國家安全會議與行政院共同召開「資安即國安策略會議」顯示政府全力支持發展國安及產業兼具的資安政策。為積極推動我國資通安全政策及加速建構環境以保障我國資安，總統府業於民國 107 年 6 月 6 日公告《資通安全管理法》，此法係屬我國重要法律興革，讓政府落實國家資安防護策略的同時，也為我國資安產業帶來嶄新的營運商機。

經濟部工業局為順應《資通安全管理法》下之資安趨勢，委託財團法人工業技術研究院與中華民國資訊軟體協會提供《資通安全管理法》採購指引懶人包，協助適用《資通安全管理法》機關如公務 / 非公務機關與關鍵資訊基礎設施業者等，掌握合規的產品或服務並提供建議資訊安全 / 產品服務商，讓資安服務 / 產品需求方獲取整合性資訊，透過建立資安產業交流及媒合平台，加速推動資安服務 / 產品領域產業商機媒合。

目 錄

出版機關｜ 經濟部工業局

編輯單位｜ 財團法人工業技術研究院 中華民國資訊軟體協會

機關電話｜ 0800-000-256

單位電話｜ 02-2737-7300 02-2553-3988

機關地址｜ 10651 臺北市大安區信義路三段 41-3 號

單位地址｜ 10651 臺北市大安區和平東路二段 106 號

10364 臺北市大同區承德路二段 239 號 6 樓

發刊日期｜ 110.12.01 / 110 版

歡迎線上下載【《資通安全管理法》採購指引懶人包】

網址：www.acw.org.tw/Match/Default.aspx?subID=38

網頁：跨域資安強化產業推動計畫 > 產業服務 > 資通安全法懶人包

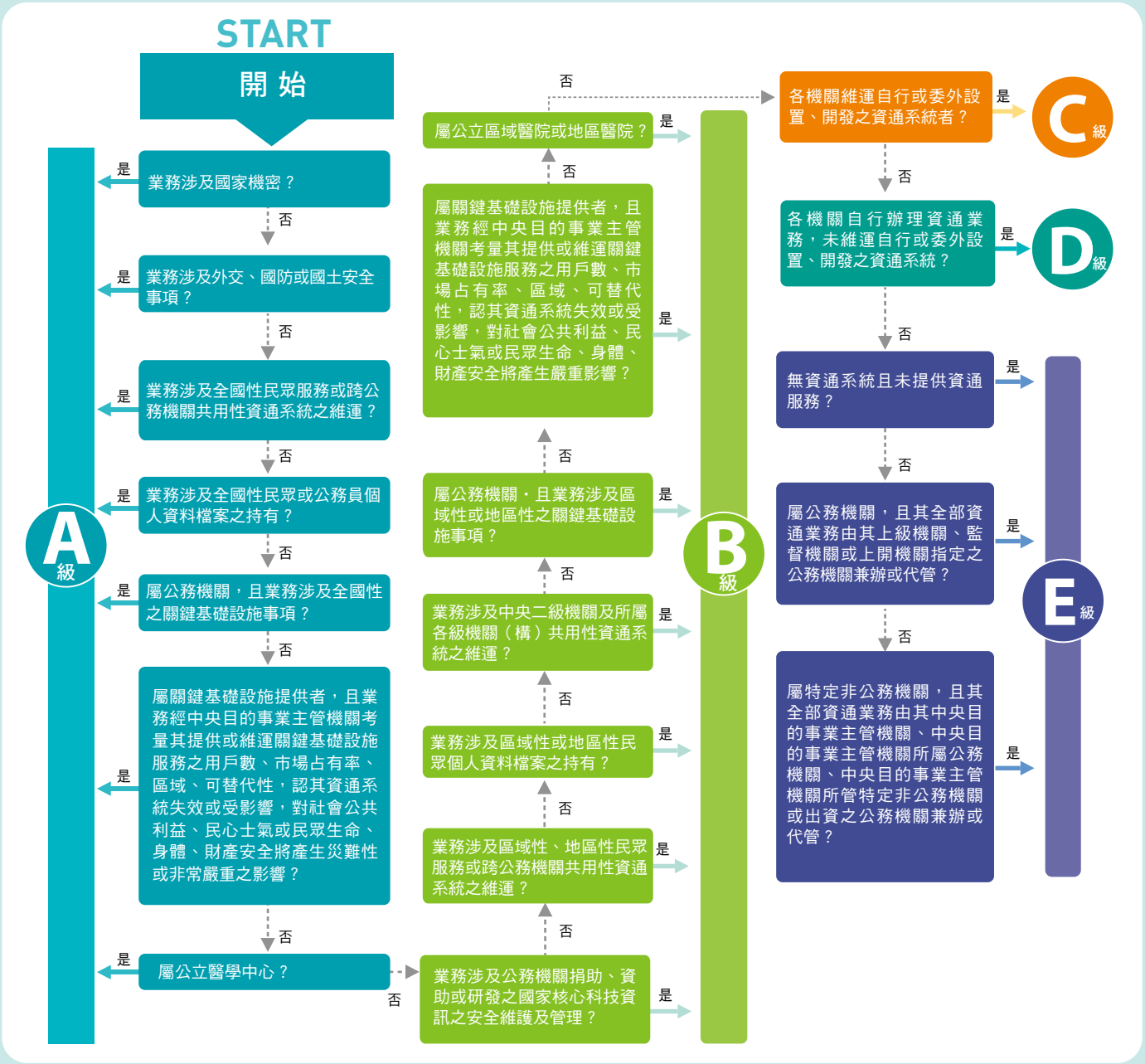
懶人包下載

第一章
《資通安全管理法》
懶人包

1《資通安全管理法》懶人包

1.1 導讀

Step 1 判定資通安全責任等級

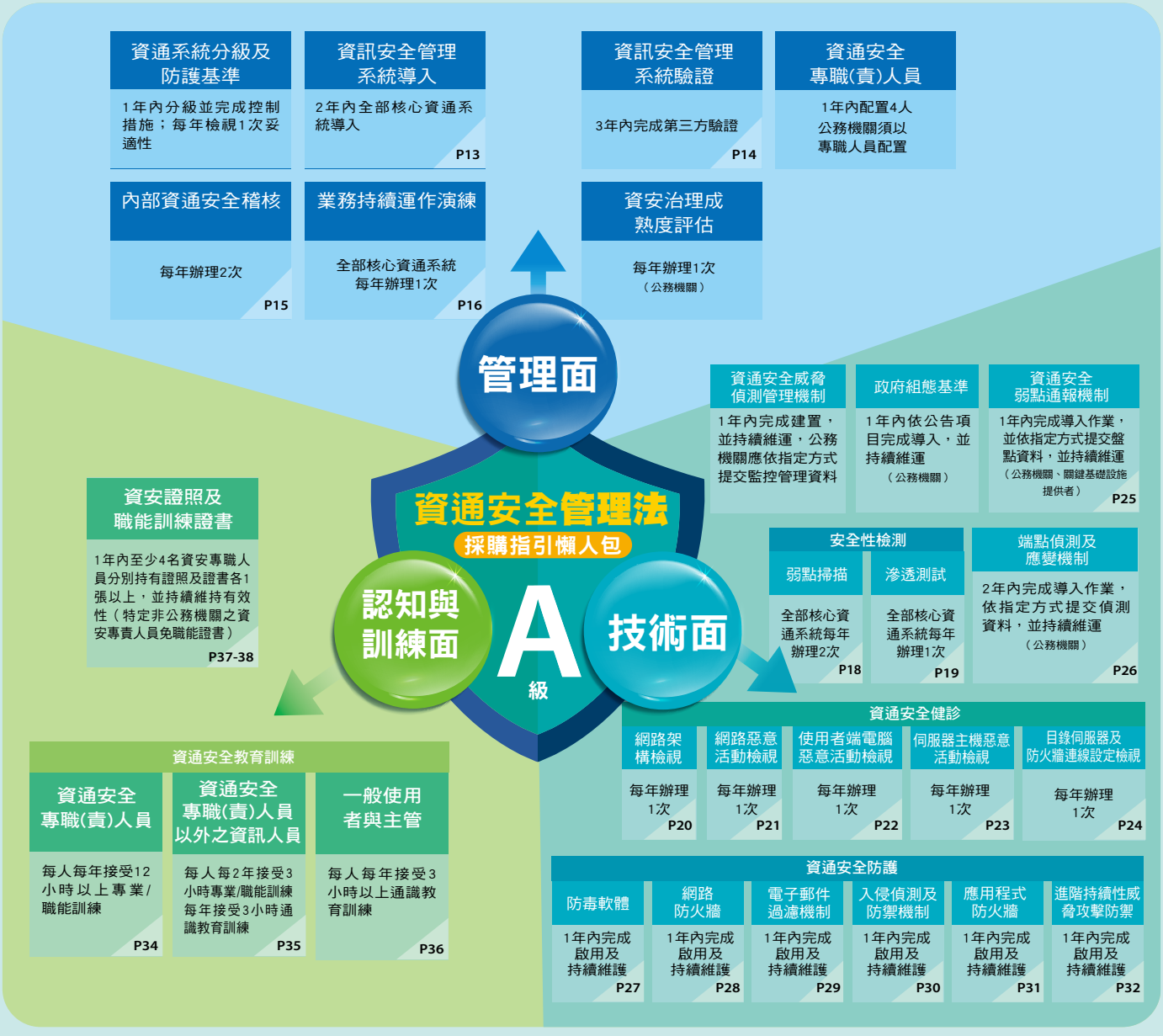


小提醒

- **資通安全責任等級判定以最高級為主：**各機關符合 2 個以上之資通安全責任等級者，以最高等級核列（資通安全責任等級分級辦法第 9 條）。
- **資通安全責任等級例外調整：**各機關得考量「業務中斷、業務資訊、功能失效、其他與資通系統相關事項」對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽影響程度，調整資通安全責任等級。（資通安全責任等級分級辦法第 10 條）。

Step 2 執行資通安全責任等級應辦事項

資通安全責任等級核定後應依期限完成應辦事項



小提醒

- **資通系統分級及防護基準：**請參閱《資通安全責任等級分級辦法》附表九完成資通系統分級且完成附表十控制措施。
- **資安治理成熟度評估：**請至行政院國家資通安全會報技術服務中心「資料索取 / 教材下載」(nicst.ey.gov.tw) 查閱推動說明且參閱「資安治理成熟度評審系統」(isg.nccst.nat.gov.tw)。
- **資通安全威脅偵測管理機制：**請至行政院國家資通安全會報技術服務中心之《政府領域聯防監控作業規範》(www.nccst.nat.gov.tw/GSOC) 查閱相關資訊。
- **政府組態基準：**請至行政院國家資通安全會報技術服務中心之「政府組態基準 (GCB)」(www.nccst.nat.gov.tw/GCB) 查閱規範資通訊終端設備之一致性安全設定相關資訊。

1.2《資通安全責任等級分級辦法》應辦事項綜整

依據《資通安全管理法》子法《資通安全責任等級分級辦法》制訂 A 級機關應辦事項如下：

制度面向	辦理項目	辦理項目細項	A 級機關
管理面	資通系統分級及防護基準		● 初次受核定或等級變更後之 1 年內，針對自行或委外開發之資通系統，依分級辦法附表九完成資通系統分級，並完成分級辦法附表十之控制措施； ● 其後應每年至少檢視 1 次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之 2 年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於 3 年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專職（責）人員		● 初次受核定或等級變更後之 1 年內配置 4 人。 ● 須以專職人員配置 (限公務機關適用)。
	內部資通安全稽核		每年辦理 2 次。
	業務持續運作演練		全部核心資通系統每年辦理 1 次。
	資安治理成熟度評估（公務機關適用）		每年辦理 1 次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理 2 次。
		滲透測試	全部核心資通系統每年辦理 1 次。
	資通安全健診	網路架構檢視	每年辦理 1 次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全威脅偵測管理機制		● 初次受核定或等級變更後之 1 年內，完成威脅偵測機制建置，並持續維運，公務機關依主管機關指定之方式提交監控管理資料。 ● 其監控範圍應包括本表所定「端點偵測及應變機制」(公務機關) 與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。
	政府組態基準 (公務機關適用)		● 初次受核定或等級變更後之 1 年內，依主管機關公告之項目，完成政府組態基準導入作業。 ● 持續維運。

制度面向	辦理項目	辦理項目細項	A 級機關
技術面	資通安全弱點通報機制 （公務機關、關鍵基礎設施提供者適用）		● 初次受核定或等級變更後之 1 年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 ● 本辦法中華民國 110 年 8 月 23 日修正施行前已受核定者，應於修正施行後 1 年內，完成資通安全弱點通報機制導入作業， 並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	端點偵測及應變機制 （公務機關適用）		● 初次受核定或等級變更後之 2 年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。 ● 本辦法中華民國 110 年 8 月 23 日修正施行前已受核定者，應於修正施行後 2 年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。
	資通安全防護	防毒軟體	初次受核定或等級變更後之 1 年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		電子郵件過濾機制	
		入侵偵測及防禦機制	
		應用程式防火牆	
		進階持續性威脅攻擊防禦	
認知與訓練面	資通安全教育訓練	資通安全專職（責）人員	每人每年至少接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練。
		資通安全專職（責）人員以外之資訊人員	● 每人每 2 年至少接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練。 ● 每年接受 3 小時以上之資通安全通識教育訓練。
		一般使用者與主管	每人每年接受 3 小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		● 初次受核定或等級變更後之 1 年內，至少 4 名資通安全專職人員， 分別各自持有證照及證書各 1 張以上，並持續維持證照及證書之有效性。（特定非公務機關免職能證書） ● 本辦法中華民國 110 年 8 月 23 日修正施行前已受核定者，應於修正施行後 1 年內符合規定。

小提醒

- **資通安全通識教育訓練：**泛指資通安全相關之通識性概念課程，或機關內部資通安全管理規定之宣導課程。
  公務人員學習紀錄登記時，請選課程代碼 522：資通安全（通識）。

1.3《資通安全管理法》採購指引各主題參考投標廠商或設備資格綜整

依據 A 級機關應辦事項，針對以下研析議題彙整參考投標廠商或設備資格，供各適用機關參閱。

小提醒

- **受託者安全管理：**《資通安全管理法施行細則》第 4 條第 1 項第 1 款規定，機關選任及監督受託者時，應注意受託者辦理受託業務之相關程序及環境，應具備完善之安全管理措施或通過第三方驗證。各機關應具備審查受託者能量並監督受託者資通安全維護情形。
- **採購原則：**資通安全產品有共同供應契約可供訂購者，應利用共同供應契約訂購原產地標示為臺灣之資通安全產品。

制度面向	辦理項目	辦理項目細項	參考投標廠商或設備資格
管理面	資訊安全管理系統導入		可參閱行政院國家資通安全會報技術服務中心「政府機關資訊安全管理系統 (ISMS) RFP」與以下參考投標廠商資格： ● 建議專案小組具備 ISO 27001 LA 或 CISSP (Certified Information Systems Security Professional) 相關資安專業證照。 ● 建議具有相當 ISO 27001 輔導導入顧問年資。
	資訊安全管理系統驗證		可參閱行政院國家資通安全會報技術服務中心「政府機關資訊安全管理系統 (ISMS) 第三方驗證 RFP」與以下參考投標廠商資格： ● 通過我國標準法主管機關委託驗證之機構（依據《資通安全責任等級分級辦法》要求）。 ● 針對核心資通系統實行第三方驗證稽核。
	內部資通安全稽核		● 建議專案小組具備 ISO 27001 LA 或稽核相關專業證照。 ● 建議具有相當 ISO 27001 資通安全稽核年資。
	業務持續運作演練		● 建議專案小組具備 ISO 27001 LA 或 ISO 22301 相關專業證照。 ● 建議具備 ISO 22301 標準顧問服務經歷。
技術面	安全性檢測	弱點掃描	可參閱行政院國家資通安全會報技術服務中心「弱點掃描服務 RFP」與以下參考投標廠商或設備資格： ● 建議執行 3 件以上之經驗。 ● 建議檢測項目需符合最新版 OWASP TOP 10 之項目。 ● 建議執行人員需接受過 CEH (Certified Ethical Hacker) 或其他類似相關課程訓練。 ● 掃描工具需取得授權使用的商用軟體。
		滲透測試	可參閱行政院國家資通安全會報技術服務中心「滲透測試服務 RFP」與以下參考投標廠商或設備資格： ● 建議執行 3 件以上之經驗。 ● 建議測試項目包含作業系統、網站管理、應用程式及密碼破解。 ● 建議執行人員需接受過 CEH 或其他類似相關課程訓練。 ● 掃描工具應取得合法授權。
	資通安全健診	網路架構檢視	可參閱行政院國家資通安全會報技術服務中心「資安健診服務 RFP」與以下參考投標廠商資格： ● 建議服務人員需接受過 CCNA(Cisco Certified Network Associate) 或其他類似網路管理相關課程訓練。

制度面向	辦理項目	辦理項目細項	參考投標廠商或設備資格
技術面	資通安全健診	網路惡意活動檢視	可參閱行政院國家資通安全會報技術服務中心「資安健診服務 RFP」與以下參考投標廠商資格： ● 封包監聽與分析：建議服務人員需接受過 NSPA (Network Security Packet Analysis) 或其他類似相關課程訓 。 ● 網路設備紀錄檔分析：建議服務人員需接受過 MCSE (Microsoft Certified Solutions Expert) 或其他類似相關課程訓練。
		使用者端電腦惡意活動檢視	可參閱行政院國家資通安全會報技術服務中心「資安健診服務 RFP」與以下參考投標廠商資格： ● 建議服務人員需接受過 CEH、CHFI (Computer Hacking Forensic Investigation) 或其他類似相關課程訓練。
		伺服器主機惡意活動檢視	可參閱行政院國家資通安全會報技術服務中心「資安健診服務 RFP」與以下參考投標廠商資格： ● 建議服務人員需接受過 CEH、CHFI 或其他類似相關課程訓練。
		目錄伺服器設定及防火牆連線設定檢視	可參閱行政院國家資通安全會報技術服務中心「資安健診服務 RFP」與以下參考投標廠商資格： ● 建議服務人員需接受過 CISSP、ISO/CNS 27001 LA 或其他類似相關課程訓練。
	資通安全弱點通報機制		可參閱行政院國家資通安全會報技術服務中心之政府機關資安弱點通報機制（VANS）專區及與技服中心介接測試之廠商名單。
	端點偵測及應變機制		1. 提供端點威脅即時檢測及監控、持續性威脅獵捕以發掘潛藏威脅並預先加以攔截。 2. 需定期提供分析報告。 3. 可列出可疑程式之威脅程度（以指數或等級表示）、判斷依據與其相關資訊（metadata）。 4. 協助單位進行資安事件調查及提供調查報告以符合資安法要求。 5. 依資安法主管機關公布之提交方式，匯出並提交偵測資料以符合資安法要求： (1) 提供資料對外轉拋、介接功能或 API 可供利用（如可由 SOC 透過聯防監控資料回傳管道回傳）。 (2) 可提供經分析後高風險樣本或事件相關資訊。
	資通安全防護	防毒軟體	● 建議使用資安測試機構 AV-Test 最近 1 年測試結果，防護分數（Protection Score）達 5.5 分以上之軟體。 ● 建議使用資安測試機構 AV-Comparatives 最近 1 年測試結果， Malware Protection Tests 取得 Advanced+（三星）等級之軟體。
		網路防火牆	● 建議產品已取得政府認可之檢測證書。 ● 建議需提供即時告警功能。 ● 建議具備 VPN 功能。 ● 建議可支援和建立多個規則和管理群組。
		電子郵件過濾機制	● 建議產品已取得政府認可之檢測證書。 ● 建議具備 SRL 發信來源信譽評等功能。 ● 建議具備內容過濾功能。

制度面向	辦理項目	辦理項目細項	參考投標廠商或設備資格
技術面	資通安全防護	入侵偵測及防禦機制	● 建議產品已取得政府認可之檢測證書。 ● 建議具備 DDoS 防護機制。 ● 建議具備程式控管能力。
		應用程式防火牆	● 建議產品已取得政府認可之檢測證書。 ● 建議針對最新版 OWASP 十大攻擊行為進行偵測與攔截。 ● 建議符合信用卡國際組織 PCI DSS 規範之要求。 ● 建議可防止或降低 DOS/DDOS 之攻擊。
		進階持續性威脅攻擊防禦	● 建議具備沙箱分析技術。 ● 建議特徵值比對功能。
認知與訓練面	資通安全教育訓練	資通安全專職（責）人員	● 資通安全專業課程訓練機構建議為： ◆主管機關認可之國內外發證機關（構）所核發之資通安全證照之國際組織或原廠授權教育訓練中心（依據資通安全管理法 FAQ）。 ◆國內外公私營訓練機構所以下列型態為限（依據資通安全管理法 FAQ）： ＊公私立大專校院。 ＊依法設立 2 年以上之職業訓練機構。 ＊依法設立 2 年以上之短期補習班。 ＊依法設立 2 年以上之學術研究機構或財團法人，其設立章程宗旨與才培訓相關且有辦理人才培訓業務。 ◆建議講師具備資安專業證照。 ◆建議講師擁有從事資安相關工作或資安授課經驗 2 年以上，具資安實務能力。 ● 資通安全通識課程訓練機構建議為： ◆登記有案之社、財團法人或公私立大專以上院校，或依公司法設立之公司。 ◆建議講師具備資安專業證照。 ◆建議講師擁有從事資安相關工作或資安授課經驗 2 年以上，具資安實務能力。
		資通安全專職（責）人員以外之資訊人員	
		一般使用者與主管	
	資通安全專業證照及職能訓練證書	資通安全專業證照	● 主管機關認可之國內外發證機關（構）所核發之資通安全證照（公告於行政院國家資通安全會報網站之資安管理法專區）並持續有效。 ● 如持有 Lead Auditor 相關證照，除證照有效外，每年度須提供至少 2 次實際參與證照內容有之稽核經驗佐證。 ● 建議訓練機構為國際組織或原廠授權教育訓練中心。 ● 建議講師具國際組織或原廠認證資格。
		資通安全職能評量證書	● 完成資通安全職能訓練機構（經行政院國家資通安全會報技術服務中心遴選公告）辦理之職能訓練，且通過職能評量，取得證書並持續有效。

小提醒

- 相關管理面、技術面及認知與訓練面之勞務採購，可參考行政院國家資通安全會報技術服務中心 (www.nccst.nat.gov.tw) 公告之資安服務 RFP(如：政府機關資安健診服務委外服務案 RFP 等) 辦理。
- 其他技術面之資通安全防護設備，可參考懶人包附錄廠商建議名單或推薦利用共同供應契約採購。

第二章
《資通安全管理法》
採購指引懶人包

SECURE

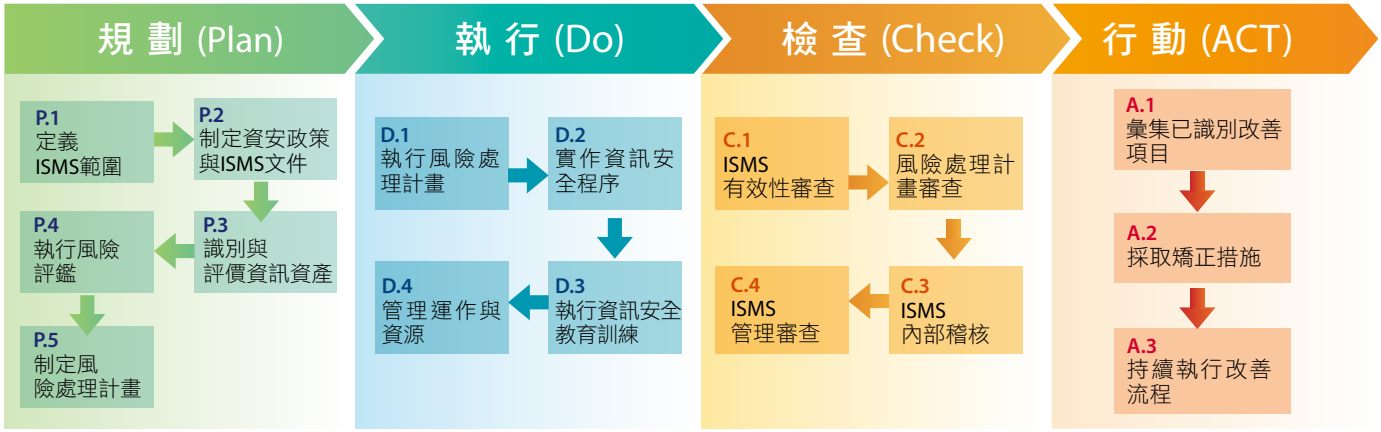
管理面

資通安全管理是全面性工作，主要目標在降低風險與提高管理效率，為確保《資通安全管理法》適用機關針對核心資通系統進行資安控管及維護，《資通安全管理法》子法特別針對管理面規定應辦理項目。針對《資通安全責任等級分級辦法》之管理面「資訊安全管理系統之導入與驗證」、「內部資通安全稽核」及「業務持續運作演練」議題進行資安控管實務研析，提出建立及執行管理面辦理項目應有之基本原則及建議性作法等，作為《資通安全管理法》各適用機關規劃及執行管理面之參考。

2.1 管理面

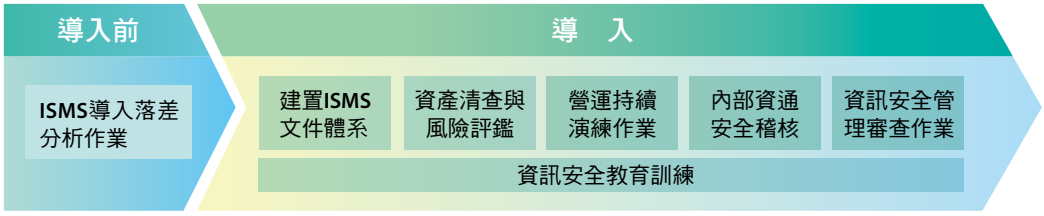
2.1.1 資訊安全管理系統導入

1. 資訊安全管理系統導入參考實作流程



2. 資訊安全管理系統導入參考採購需求項目

機關可尋求外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗可增加成功導入 ISMS 機率及有效控管組織中風險。採購人員在資訊安全管理系統導入建議書徵求文件 (RFP) 參考採購需求項目如下：



小提醒

- 可參閱行政院國家資通安全會報技術服務中心公告「政府機關資訊安全管理系統 (ISMS) RFP」。

3. 資訊安全管理系統導入參考廠商名單

資訊安全管理系統導入參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源	
	資安服務機構能量登錄	政府採購網決標
三甲科技股份有限公司	√	—
大同世界科技股份有限公司	√	—
中揚資訊有限公司	√	—
中華資安國際股份有限公司	√	√
中華電信股份有限公司	√	√
台灣應用軟件股份有限公司	√	√
台灣檢驗科技股份有限公司	—	√
安永企業管理諮詢服務股份有限公司	√	√
安侯企業管理股份有限公司	√	√
安華聯網科技股份有限公司	√	—
安碁資訊股份有限公司	√	√
自由系統股份有限公司	√	—
宏碁資訊服務股份有限公司	—	√
延宇資訊股份有限公司	—	√
昇達價值管理股份有限公司	—	√
阿逸多資訊有限公司	—	√
美思科法顧問股份有限公司	—	√
香港商英國標準協會太平洋有限公司台灣分公司	√	√
香港商漢德技術監督服務亞太有限公司—台灣分公司	√	—
荃豐科技有限公司	—	√
財團法人中華民國國家資訊基本建設產業發展協進會	—	√
偉立資訊有限公司	—	√
頂峰資訊有限公司	—	√
創逸科技服務有限公司	√	√
創穩資云股份有限公司	√	—

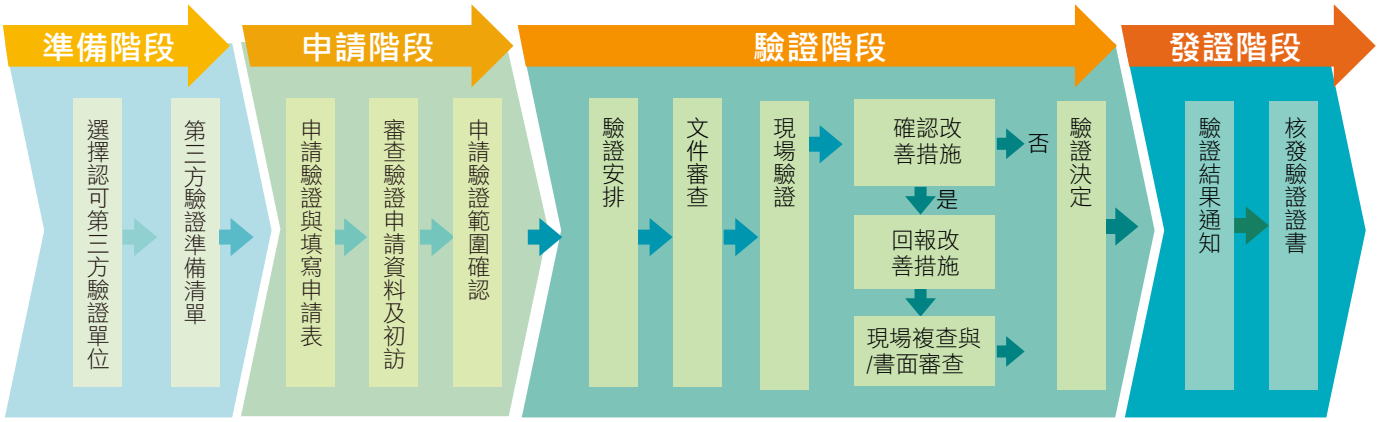
廠商名稱（以筆劃排序）	廠商具備資格來源	
	資安服務機構能量登錄	政府採購網決標
博創資訊科技股份有限公司	—	√
敦陽科技股份有限公司	—	√
智慧光資訊服務股份有限公司	—	√
登豐數位科技股份有限公司	—	√
策略數位服務有限公司	√	√
華電聯網股份有限公司	—	√
華緯資訊企業社	—	√
勤業眾信聯合會計師事務所	√	√
資拓宏宇國際股份有限公司	√	√
資誠聯合會計師事務所	√	√
漢昕科技股份有限公司	√	√
精誠科技整合股份有限公司	—	√
領導力企業管理顧問有限公司	√	—
德欣寰宇科技股份有限公司	√	√
德諾科技服務股份有限公司	√	√
數聯資安股份有限公司	√	—
璞方科技管理顧問股份有限公司	—	√
興創知能股份有限公司	—	√
諦錦有限公司	—	√
優士國際聯合顧問有限公司	—	√
環奧國際驗證有限公司	—	√
聯合報股份有限公司	—	√
聯準科技服務有限公司	√	√
賽博韓特科技有限公司	√	√
關貿網路股份有限公司	√	—

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄（www.acw.org.tw）為 108-110 年之合格廠商。政府採購網（web.pcc.gov.tw）決標紀錄，以 105-110 年 8 月資訊安全管理系統導入決標紀錄。

2.1.2 資訊安全管理系統第三方驗證

1. 資訊安全管理系統第三方驗證參考實作方式

ISMS 第三方驗證可分為 4 個階段，包含準備階段、申請階段、驗證階段與發證階段。並且在完成發證階段後會進行第三方驗證單位追蹤稽核 / 監督稽核，以及發證通過後 3 年屆滿則須進行重新驗證作業，以確保第三方驗證通過證書持續有效。



2. 資訊安全管理系統第三方驗證參考採購需求項目

應依期限完成資訊安全管理系統導入及公正第三方驗證並持續維持其驗證有效性。採購人員在資訊安全管理系統第三方驗證建議書徵求文件 (RFP) 參考採購需求項目如下：

小提醒

- 可參閱行政院國家資通安全會報技術服務中心公告「政府機關資訊安全管理系統 (ISMS) 第三方驗證 RFP」。

3. 資訊安全管理系統第三方驗證參考廠商名單

「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。《標準法》主管機關為經濟部，並且透過財團法人全國認證基金會 (TAF) 官網公告資訊彙整提供資訊安全管理系統第三方驗證參考廠商名單如下：

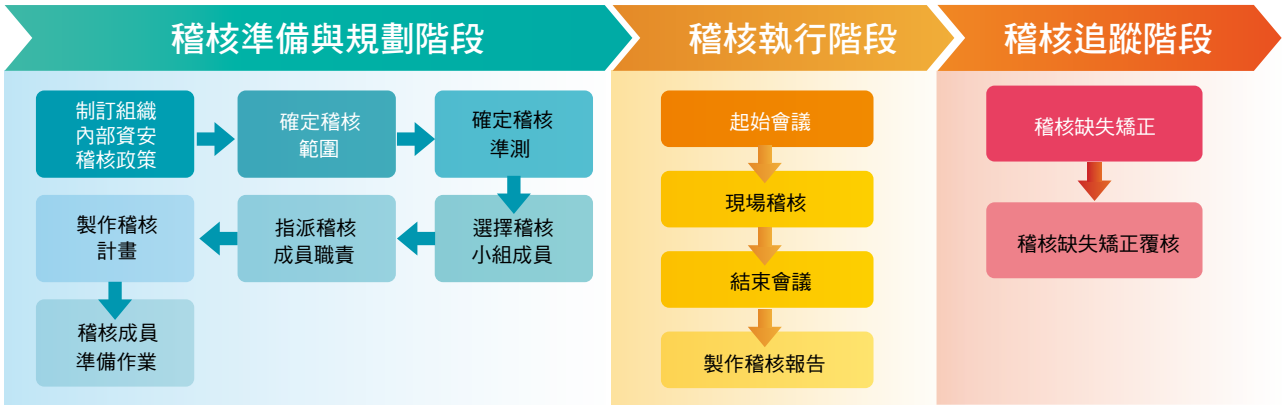
廠商名稱（以筆劃排序）	廠商具備資格來源	
	資安服務機構能量登錄	TAF 認可
台灣檢驗科技股份有限公司	–	√
香港商英國標準協會太平洋有限公司台灣分公司	√	√
艾法諾國際股份有限公司	–	√
環奧國際驗證有限公司	–	√
香港商漢德技術監督服務亞太有限公司台灣分公司	√	√

※ 備註：廠商具備資格來源自 TAF 官網（www.taftw.org.tw）「資訊安全管理系統」認可管理系統驗證機構名錄且查詢截止日為 110/9/30。資安服務機構能量登錄（www.acw.org.tw）為 110 年之合格廠商。

2.1.3 內部資通安全稽核

1. 內部資通安全稽核參考實作方式

各適用機關可參考下列內部資通安全稽核準備與規劃階段、稽核執行階段與稽核追蹤階段實施內部資通安全稽核各項細部執行工作項目。



2. 內部資通安全稽核參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，亦可透過外部專業資通安全顧問團隊豐富經驗學習內部稽核作業實施方式或相關知識作為後續內部人員自行維護基礎之奠定。採購人員在內部資通安全稽核建議書徵求文件 (RFP) 參考採購需求項目如下：

小提醒

- 資安法內稽應以機關內所有單位進行規劃，非僅針對資訊單位辦理。

服務項目	採購需求項目
內部資通安全稽核服務	1. 廠商應配合組織內部資通安全稽核時程提出「內部資通安全稽核計畫」。 2. 廠商應依據組織內部資通安全稽核程序指派符合資格稽核員並遵照「內部資通安全稽核計畫」對 ISMS 範圍依據稽核準則執行內部資通安全稽核作業。 3. 稽核作業完成後，廠商應於雙方約定期限內提交「內部資通安全稽核報告」。 4. 對於內部資通安全稽核作業之稽核結論及稽核發現協助研擬適切改善方案與改善復核。

3. 內部資通安全稽核參考廠商名單

內部資通安全稽核參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源	
	資安服務機構能量登錄	政府採購網決標
三甲科技股份有限公司	√	—
大同世界科技股份有限公司	√	—
中揚資訊有限公司	√	—
中華資安國際股份有限公司	√	√
中華電信股份有限公司	√	√
台灣應用軟件股份有限公司	√	√
台灣檢驗科技股份有限公司	—	√
安永企業管理諮詢服務股份有限公司	√	√
安侯企業管理股份有限公司	√	√
安華聯網科技股份有限公司	√	—
安碁資訊股份有限公司	√	√
自由系統股份有限公司	√	—
宏碁資訊服務股份有限公司	—	√
延宇資訊股份有限公司	—	√
昇達價值管理股份有限公司	—	√
阿逸多資訊有限公司	—	√
美思科法顧問股份有限公司	—	√
香港商英國標準協會太平洋有限公司台灣分公司	—	√
荃豐科技有限公司	—	√
財團法人中華民國國家資訊基本建設產業發展協進會	—	√
偉立資訊有限公司	—	√
頂峰資訊有限公司	—	√
創逸科技服務有限公司	√	√
創穩資云股份有限公司	√	—
博創資訊科技股份有限公司	—	√

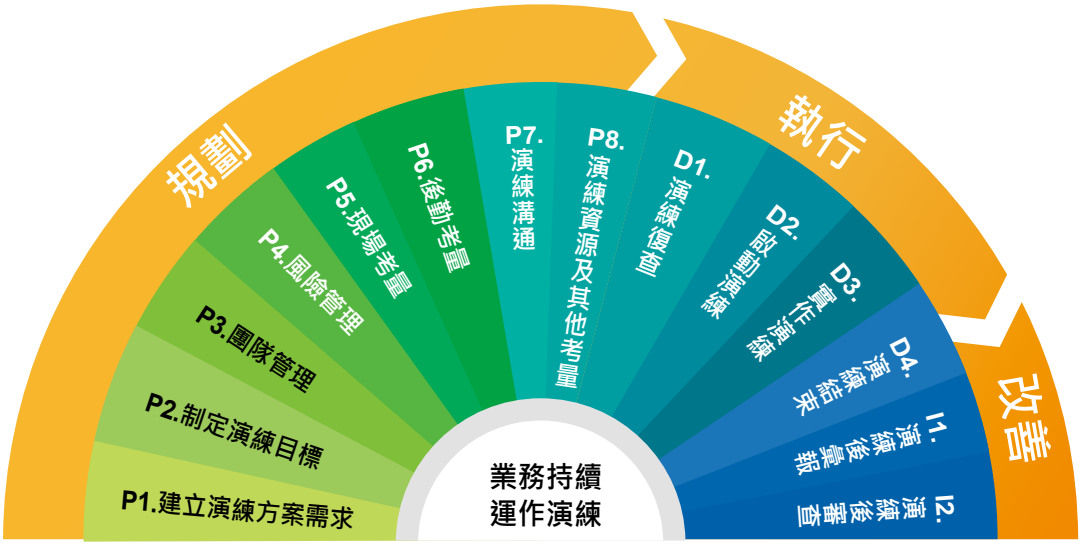
廠商名稱（以筆劃排序）	廠商具備資格來源	
	資安服務機構能量登錄	政府採購網決標
敦陽科技股份有限公司	—	√
智慧光資訊服務股份有限公司	—	√
登豐數位科技股份有限公司	—	√
策略數位服務有限公司	√	√
華電聯網股份有限公司	—	√
華緯資訊企業社（獨資）	—	√
勤業眾信聯合會計師事務所	√	√
資拓宏宇國際股份有限公司	√	√
資誠聯合會計師事務所	√	√
漢昕科技股份有限公司	√	√
精誠科技整合股份有限公司	—	√
領導力企業管理顧問有限公司	√	—
德欣寰宇科技股份有限公司	√	√
德諾科技服務股份有限公司	√	√
數聯資安股份有限公司	√	—
璞方科技管理顧問股份有限公司	—	√
興創知能股份有限公司	—	√
諦錦有限公司	—	√
優士國際聯合顧問有限公司	—	√
環奧國際驗證有限公司	—	√
聯合報股份有限公司	—	√
聯準科技服務有限公司	√	√
賽博韓特科技有限公司	√	√
關貿網路股份有限公司	√	—

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府採購網 (web.pcc.gov.tw) 決標紀錄以 105-110 年 8 月資訊安全管理系統導入決標紀錄。

2.1.4 業務持續運作演練

1. 業務持續運作演練參考實作方式

ISO 組織已於 2013 年公告 ISO 22398:2013《Societal security -- Guidelines for exercises》可提供不同規模或類型組織作為業務持續運作演練之參考，進而驗證營運持續計畫 (Business Continuity Planning，BCP)，以驗證策略的有效性。各適用機關實作業務持續運作演練可採用「規劃」、「執行」與「改善」等各階段執行各項細部工作項目。



2. 業務持續運作演練參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，可透過外部專業資通安全顧問團隊豐富經驗，學習業務持續運作演練實施方式或相關知識，奠定後續內部人員自行維護之基礎。採購人員在業務持續運作演練建議書徵求文件 (RFP) 參考採購需求項目如下：

服務項目	採購需求項目
業務持續運作演練服務	1. 廠商針對組織和資通系統辦理風險評鑑，依據風險評估結果更新營運持續計畫，並且提出適切營運持續演練計畫。 2. 廠商應配合到場進行業務持續運作演練，產出業務持續運作演練紀錄。 3. 依業務持續運作演練結果修正計畫。

3. 業務持續運作演練參考廠商名單

透過政府採購網與從「資訊安全管理系統導入參考廠商名單」中篩選官網公告資訊含有 ISO/IEC 22301 顧問導入服務，彙整提供業務持續運作演練參考廠商名單：

廠商名稱 （以筆劃排序）	廠商具備資格來源	
	政府採購網決標紀錄	官網
安侯企業管理股份有限公司	–	√
宏碁資訊服務股份有限公司	√	√
創逸科技服務有限公司	–	√
博創資訊科技股份有限公司	–	√
勤業眾信聯合會計師事務所	√	√
德欣寰宇科技股份有限公司	–	√
德諾科技服務股份有限公司	–	√
聯準科技服務有限公司	–	√
賽博韓特科技有限公司	–	√
數聯資安股份有限公司	√	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。政府採購網 (web.pcc.gov.tw) 決標紀錄以 102-110 年 8 月業務持續運作服務決標紀錄。

技術面

資通安全推動除了透過管理層面進行控管外，面對各項資訊安全風險亦可透過資通安全技術手法進行防禦，《資通安全管理法》各適用機關須掌握最新資通安全技術趨勢，才能在規劃與執行資通安全風險管理時，還能兼顧整體營運目標。針對《資通安全責任等級分級辦法》之技術面「資通安全防護」議題進行資通安全控管實務研析，提出建立及執行技術面辦理項目應有之基本原則及建議性作法等，作為《資通安全管理法》各適用機關規劃及執行技術面參考。

2.2 技術面

2.2.1 安全性檢測

2.2.1.1 弱點掃描

1. 弱點掃描參考實作方式

弱點掃描建議實作流程如下圖所示，包含執行網站弱點掃描、檢查伺服器、防火牆、入侵偵測系統等布建方式、檢查登入密碼的複雜度及 SSL 通訊界面：

2. 弱點掃描參考採購需求項目

機關可依預算額度洽詢外部專業資訊安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加網站安全弱點管理及有效控管組織風險，參考採購需求項目如下：

服務項目	採購需求項目
弱點掃描服務	1. 檢測項目須符合最新版 OWASP TOP 10 的項目。 2. 執行人員需接受過 CEH 或其他類似相關課程訓練。 3. 掃描工具需取得授權使用的商用軟體。 4. 進行網站掃描後，應提供弱點掃描結果及修補建議。 5. 完成網站的弱點修復或移除惡意程式後，應再次進行弱點複掃作業，確認網站已無相關弱點風險存在。

小提醒

- 可參閱政院國家資通安全會報技術服務中心公告「政府機關弱點掃描服務委外服務案 RFP」。

3. 弱點掃描參考廠商名單

弱點掃描參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
又碩電腦科技股份有限公司	√	—	—
三甲科技股份有限公司	√	—	√
大同世界科技股份有限公司	—	—	√
中芯數據股份有限公司	√	√	—
中華資安國際股份有限公司	√	√	√
中華龍網股份有限公司	√	—	√
互聯安睿資通股份有限公司	√	—	—
台灣恩益禧股份有限公司	√	—	—
白帽犀牛有限公司	√	—	—
光盾資訊科技有限公司	—	√	—
如梭世代有限公司	√	—	√
安侯企業管理股份有限公司	√	—	—
安華聯網科技股份有限公司	√	√	√
安碁資訊股份有限公司	√	√	√
安資捷股份有限公司	—	√	—
自由系統股份有限公司	√	—	—
宏碁資訊服務股份有限公司	√	—	—
協志聯合科技股份有限公司	√	—	—
承弘國際股份有限公司	√	—	√
昕恩科技有限公司	√	—	—
松之安資訊科技有限公司	—	—	√
果核數位股份有限公司	√	—	—
飛象資訊股份有限公司	√	—	√
凌群電腦股份有限公司	√	√	—
泰鋒電腦股份有限公司	√	—	—
神通資訊科技股份有限公司	√	—	—
動力安全資訊股份有限公司	√	—	—
統智科技股份有限公司	√	—	—
頂峰資訊有限公司	—	√	—

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
創逸科技服務有限公司	√	—	—
創穩資云股份有限公司	√	—	—
竣盟科技股份有限公司	√	—	—
策略數位服務有限公司	√	√	—
華電聯網股份有限公司	√	—	√
逸凡科技股份有限公司	√	—	—
鈊安資訊科技股份有限公司	√	—	—
雲勝雲端科技有限公司	√	—	—
勤業眾信聯合會計師事務所	√	—	—
新加坡商網達先進科技（台灣分公司）	√	—	—
詮睿科技股份有限公司	√	—	√
資拓宏宇國際股份有限公司	√	—	—
資通電腦股份有限公司	√	—	—
資誠聯合會計師事務所	√	—	—
漢昕科技股份有限公司	√	√	—
碩遠科技股份有限公司	√	—	—
精誠資訊股份有限公司	√	—	√
綠界科技股份有限公司	√	—	—
豪勉科技股份有限公司	√	—	—
德欣寰宇科技股份有限公司	√	√	—
叡揚資訊股份有限公司	√	—	—
盧氪賽忒股份有限公司	√	—	√
優易資訊股份有限公司	—	√	—
戴夫寇爾股份有限公司	√	—	—
賽博韓特科技有限公司	√	√	—
鎰威科技有限公司	√	—	—
關貿網路股份有限公司	√	√	√
關鍵智慧科技有限公司	—	√	—

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02。資安整合服務平台 (secpaas.org.tw) 廠商查詢截止日為 110/9/30。

2.2.1.2 滲透測試

1. 滲透測試參考實作方式

滲透測試建議實作流程如下所示：

2. 滲透測試參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加系統滲透管理及有效控管組織風險，參考採購需求項目如下：

服務項目	採購需求項目
滲透測試服務	1. 測試項目包含作業系統、網站管理、應用程式、資料庫及密碼破解。 2. 滲透測試工具使用人員須接受過 CEH、ECSA 或其他類似相關課程訓練。 3. 滲透測試服務人員須接受過 GPEN (GIAC Certified Penetration Testers)、GWAPT (GIAC Web Application Penetration Tester) 或其他類似相關課程訓練證明。 4. 進行滲透測試後，應提供滲透測試結果及修補建議。 5. 滲透發現之相關漏洞修補後，應進行複測以確認無相關弱點風險。

小提醒

- 可參閱行政院國家資通安全會報技術服務中心公告「政府機關滲透測試服務委外服務案 RFP」。

3. 滲透測試參考廠商名單

滲透測試參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
三甲科技股份有限公司	√	√	√
大同世界科技股份有限公司	√	—	—
工業技術研究院	—	—	√
中芯數據股份有限公司	√	√	—
中華資安國際股份有限公司	√	√	√
互聯安睿資通股份有限公司	√	—	√
白帽犀牛有限公司	√	—	—
光盾資訊科技有限公司	—	√	—
如梭世代有限公司	√	—	√
安侯企業管理股份有限公司	√	—	—
安華聯網科技股份有限公司	√	√	√
安碁資訊股份有限公司	√	√	—
承弘國際股份有限公司	√	—	√
昕恩科技有限公司	√	—	—
松之安資訊科技有限公司	—	—	√
果核數位股份有限公司	√	√	—
飛象資訊股份有限公司	—	—	√
凌群電腦股份有限公司	√	√	—
財團法人工業技術研究院	—	—	√
動力安全資訊股份有限公司	√	—	—
頂峰資訊有限公司	—	√	—
創逸科技服務有限公司	√	—	—

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
創穩資云股份有限公司	√	—	—
策略數位服務有限公司	√	—	—
華電聯網股份有限公司	√	—	√
雲勝雲端科技有限公司	√	—	—
勤業眾信聯合會計師事務所	√	—	—
新加坡商網達先進科技（台灣分公司）	√	—	—
詮睿科技股份有限公司	√	—	√
資通電腦股份有限公司	√	—	—
資誠聯合會計師事務所	√	—	—
漢昕科技股份有限公司	√	√	—
精誠資訊股份有限公司	√	—	√
綠界科技股份有限公司	√	—	—
德欣寰宇科技股份有限公司	√	√	—
數聯資安股份有限公司	√	√	√
盧氪賽忒股份有限公司	√	—	√
優易資訊股份有限公司	—	√	—
戴夫寇爾股份有限公司	√	—	√
聯準科技服務有限公司	√	—	—
賽博韓特科技有限公司	√	—	—
關貿網路股份有限公司	√	√	—
關鍵智慧科技有限公司	√	√	—

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02。資安整合服務平台 (secpaas.org.tw) 廠商查詢截止日為 110/9/30。

2.2.2 資通安全健診

2.2.2.1 網路架構檢視

1. 網路架構檢視參考實作方式

網路架構檢視建議實作流程如下圖所示，包含網路架構檢視前置作業、網路架構安全現況分析、至機關實地進行網路安全架構檢視、健診結果分析與說明，以及健診後，機關強化網路架構檢視安全管理系統等階段。

2. 網路架構檢視參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加網路管理及有效控管組織風險，採購人員在網路架構檢視建議書徵求文件 (RFP) 參考採購需求項目如下：

小提醒

- 可參閱行政院國家資通安全會報技術服務中心公告「政府機關資安健診服務委外服務案 RFP」。

3. 網路架構檢視參考廠商名單

網路架構檢視參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
三甲科技股份有限公司	√	√	√
大同世界科技股份有限公司	—	—	√
中芯數據股份有限公司	√	√	—
中華資安國際股份有限公司	√	√	√
中華龍網股份有限公司	√	—	√
台眾電腦股份有限公司	√	—	√
台灣恩益禧股份有限公司	√	—	—
永豐技服科技有限公司	√	—	—
光盾資訊科技有限公司	—	√	—
安侯企業管理股份有限公司	√	—	—
安華聯網科技股份有限公司	√	√	√
安碁資訊股份有限公司	√	√	√
協科資訊股份有限公司	√	—	—
果核數位股份有限公司	√	√	—
美思科法顧問股份有限公司	√	—	—
凌群電腦股份有限公司	—	√	√
動力安全資訊股份有限公司	√	—	√

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
頂峰資訊有限公司	—	√	—
創穩資云股份有限公司	√	√	—
策略數位服務有限公司	—	√	—
華苓科技股份有限公司	√	—	—
華電聯網股份有限公司	√	—	√
勤業眾信聯合會計師事務所	√	—	—
詮睿科技股份有限公司	—	—	√
誠雲科技股份有限公司	√	—	—
漢昕科技股份有限公司	√	√	—
精誠資訊股份有限公司	—	—	√
豪勉科技股份有限公司	√	—	—
領導力企業管理顧問有限公司	√	—	—
德欣寰宇科技股份有限公司	√	√	—
數聯資安股份有限公司	√	√	√
優易資訊股份有限公司	—	√	—
聯準科技服務有限公司	√	—	—
關貿網路股份有限公司	√	√	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02。資安整合服務平台 (secpaas.org.tw) 廠商查詢截止日為 110/9/30。

2.2.2.2 網路惡意活動檢視

1. 網路惡意活動檢視參考實作方式

網路惡意活動檢視建議實作流程如下圖所示，包含網路惡意活動檢視前置作業、網路安全現況分析、至機關實地進行網路惡意活動檢視、健診結果分析與說明，以及健診後，機關強化網路設備安全管理系統等階段。

2. 網路惡意活動檢視參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加網路管理及有效控管組織風險，採購人員在網路惡意活動檢視建議書徵求文件 (RFP) 參考採購需求項目如下：

小提醒

- 可參閱行政院國家資通安全會報技術服務中心公告「政府機關資安健診服務委外服務案 RFP」。

3. 網路惡意活動檢視參考廠商名單

網路架構檢視參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
三甲科技股份有限公司	√	√	√
大同世界科技股份有限公司	—	—	√
中芯數據股份有限公司	√	√	—
中華資安國際股份有限公司	√	√	√
中華龍網股份有限公司	√	—	√
台眾電腦股份有限公司	√	—	√
台灣恩益禧股份有限公司	√	—	—
永豐技服科技有限公司	√	—	—
光盾資訊科技有限公司	—	√	—
安侯企業管理股份有限公司	√	—	—
安華聯網科技股份有限公司	√	√	√
安碁資訊股份有限公司	√	√	√
協科資訊股份有限公司	√	—	—
果核數位股份有限公司	√	√	—
美思科法顧問股份有限公司	√	—	—
凌群電腦股份有限公司	—	√	√
動力安全資訊股份有限公司	√	—	√

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
頂峰資訊有限公司	—	√	—
創穩資云股份有限公司	√	√	—
策略數位服務有限公司	—	√	—
華苓科技股份有限公司	√	—	—
華電聯網股份有限公司	√	—	√
勤業眾信聯合會計師事務所	√	—	—
詮睿科技股份有限公司	—	—	√
誠雲科技股份有限公司	√	—	—
漢昕科技股份有限公司	√	√	—
精誠資訊股份有限公司	—	—	√
豪勉科技股份有限公司	√	—	—
領導力企業管理顧問有限公司	√	—	—
德欣寰宇科技股份有限公司	√	√	—
數聯資安股份有限公司	√	√	√
優易資訊股份有限公司	—	√	—
聯準科技服務有限公司	√	—	—
關貿網路股份有限公司	√	√	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02。資安整合服務平台 (secpaas.org.tw) 廠商查詢截止日為 110/9/30。

2.2.2.3 使用者端電腦惡意活動檢視

1. 使用者端電腦惡意活動檢視參考實作方式

使用者端電腦惡意活動檢視建議實作流程如下圖所示，包含使用者端電腦惡意活動檢視前置作業、安全現況分析、至機關實地進行使用者端電腦惡意活動檢視、健診結果分析與說明，以及健診後，機關強化使用者端電腦安全管理系統等階段。

2. 使用者端電腦惡意活動檢視參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加網路管理及有效控管組織風險，採購人員在使用者端電腦惡意活動檢視建議書徵求文件 (RFP) 參考採購需求項目如下：

小提醒

- 可參閱行政院國家資通安全會報技術服務中心公告「政府機關資安健診服務委外服務案 RFP」。

3. 使用者端電腦惡意活動檢視參考廠商名單

使用者端電腦惡意活動檢視參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
三甲科技股份有限公司	√	√	√
大同世界科技股份有限公司	—	—	√
中芯數據股份有限公司	√	√	—
中華資安國際股份有限公司	√	√	√
中華龍網股份有限公司	√	—	√
台眾電腦股份有限公司	√	—	√
台灣恩益禧股份有限公司	√	—	—
永豐技服科技有限公司	√	—	—
光盾資訊科技有限公司	—	√	—
安侯企業管理股份有限公司	√	—	—
安華聯網科技股份有限公司	√	√	√
安碁資訊股份有限公司	√	√	√
協科資訊股份有限公司	√	—	—
果核數位股份有限公司	√	√	—
美思科法顧問股份有限公司	√	—	—
凌群電腦股份有限公司	—	√	√
動力安全資訊股份有限公司	√	—	√

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
頂峰資訊有限公司	—	√	—
創穩資云股份有限公司	√	√	—
策略數位服務有限公司	—	√	—
華苓科技股份有限公司	√	—	—
華電聯網股份有限公司	√	—	√
勤業眾信聯合會計師事務所	√	—	—
詮睿科技股份有限公司	—	—	√
誠雲科技股份有限公司	√	—	—
漢昕科技股份有限公司	√	√	—
精誠資訊股份有限公司	—	—	√
豪勉科技股份有限公司	√	—	—
領導力企業管理顧問有限公司	√	—	—
德欣寰宇科技股份有限公司	√	√	—
數聯資安股份有限公司	√	√	√
優易資訊股份有限公司	—	√	—
聯準科技服務有限公司	√	—	—
關貿網路股份有限公司	√	√	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02。資安整合服務平台 (secpaas.org.tw) 廠商查詢截止日為 110/9/30。

2.2.2.4 伺服器主機惡意活動檢視

1. 伺服器主機惡意活動檢視參考實作方式

伺服器主機惡意活動檢視建議實作流程如下圖所示，包含伺服器主機惡意活動檢視前置作業、安全現況分析、至機關實地進行伺服器主機惡意活動檢視、健診結果分析與說明，以及健診後，機關強化伺服器主機安全管理系統等階段。

2. 伺服器主機惡意活動檢視參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加網路管理及有效控管組織風險，採購人員在伺服器主機惡意活動檢視建議書徵求文件 (RFP) 參考採購需求項目如下：

小提醒

- 可參閱行政院國家資通安全會報技術服務中心公告「政府機關資安健診服務委外服務案 RFP」。

3. 伺服器主機惡意活動檢視參考廠商名單

伺服器主機惡意活動檢視參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
三甲科技股份有限公司	√	√	√
大同世界科技股份有限公司	—	—	√
中芯數據股份有限公司	√	√	—
中華資安國際股份有限公司	√	√	√
中華龍網股份有限公司	√	—	√
台眾電腦股份有限公司	√	—	√
台灣恩益禧股份有限公司	√	—	—
永豐技服科技有限公司	√	—	—
光盾資訊科技有限公司	—	√	—
安侯企業管理股份有限公司	√	—	—
安華聯網科技股份有限公司	√	√	√
安碁資訊股份有限公司	√	√	√
協科資訊股份有限公司	√	—	—
果核數位股份有限公司	√	√	—
美思科法顧問股份有限公司	√	—	—
凌群電腦股份有限公司	—	√	√
動力安全資訊股份有限公司	√	—	√

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
頂峰資訊有限公司	—	√	—
創穩資云股份有限公司	√	√	—
策略數位服務有限公司	—	√	—
華苓科技股份有限公司	√	—	—
華電聯網股份有限公司	√	—	√
勤業眾信聯合會計師事務所	√	—	—
詮睿科技股份有限公司	—	—	√
誠雲科技股份有限公司	√	—	—
漢昕科技股份有限公司	√	√	—
精誠資訊股份有限公司	—	—	√
豪勉科技股份有限公司	√	—	—
領導力企業管理顧問有限公司	√	—	—
德欣寰宇科技股份有限公司	√	√	—
數聯資安股份有限公司	√	√	√
優易資訊股份有限公司	—	√	—
聯準科技服務有限公司	√	—	—
關貿網路股份有限公司	√	√	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02。資安整合服務平台 (secpaas.org.tw) 廠商查詢截止日為 110/9/30。

2.2.2.5 目錄伺服器設定及防火牆連線設定檢視

1. 目錄伺服器設定及防火牆連線設定檢視參考實作方式

目錄伺服器設定及防火牆連線設定檢視建議實作流程如下圖所示，包含前置作業、安全現況分析、至機關實地進行目錄伺服器設定及防火牆連線設定檢視、健診結果分析與說明，以及健診後，機關強化伺服器主機安全管理系統等階段。

2. 目錄伺服器設定及防火牆連線設定檢視參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加網路管理及有效控管組織風險，採購人員在目錄伺服器設定及防火牆連線設定檢視建議書徵求文件 (RFP) 參考採購需求項目如下：

小提醒

- 可參閱行政院國家資通安全會報技術服務中心公告「政府機關資安健診服務委外服務案 RFP」。

3. 目錄伺服器設定及防火牆連線設定檢視參考廠商名單

目錄伺服器設定及防火牆連線設定檢視參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
三甲科技股份有限公司	√	√	√
大同世界科技股份有限公司	—	—	√
中芯數據股份有限公司	√	√	—
中華資安國際股份有限公司	√	√	√
中華龍網股份有限公司	√	—	√
台眾電腦股份有限公司	√	—	√
台灣恩益禧股份有限公司	√	—	—
永豐技服科技有限公司	√	—	—
光盾資訊科技有限公司	—	√	—
安侯企業管理股份有限公司	√	—	—
安華聯網科技股份有限公司	√	√	√
安碁資訊股份有限公司	√	√	√
協科資訊股份有限公司	√	—	—
果核數位股份有限公司	√	√	—
美思科法顧問股份有限公司	√	—	—
凌群電腦股份有限公司	—	√	√
動力安全資訊股份有限公司	√	—	√

廠商名稱（以筆劃排序）	廠商具備資格來源		
	資安服務機構能量登錄	政府共同供應契約	資安整合服務平台廠商
頂峰資訊有限公司	—	√	—
創穩資云股份有限公司	√	√	—
策略數位服務有限公司	—	√	—
華苓科技股份有限公司	√	—	—
華電聯網股份有限公司	√	—	√
勤業眾信聯合會計師事務所	√	—	—
詮睿科技股份有限公司	—	—	√
誠雲科技股份有限公司	√	—	—
漢昕科技股份有限公司	√	√	—
精誠資訊股份有限公司	—	—	√
豪勉科技股份有限公司	√	—	—
領導力企業管理顧問有限公司	√	—	—
德欣寰宇科技股份有限公司	√	√	—
數聯資安股份有限公司	√	√	√
優易資訊股份有限公司	—	√	—
聯準科技服務有限公司	√	—	—
關貿網路股份有限公司	√	√	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02。資安整合服務平台 (secpaas.org.tw) 廠商查詢截止日為 110/9/30。

2.2.3 資通安全弱點通報機制

1. 資通安全弱點通報機制（VANS）導入參考實作方式

資通安全弱點通報機制係指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業；以下提供建議實作流程做為參考：

透過支援 VANS 之資產管理工具，彙整機關個人電腦及伺服器主機之資訊資產資料，將資產資料正規化為 CPE 格式，併同 Windows Update 資訊，上傳至資安法主管機關 VANS 系統，由 VANS 系統協助對彙總性資訊資產與國際弱點資料庫比對，回饋弱點比對結果予機關，機關再透由內部工具掌握相關弱點分布情形，據以執行資訊資產安全性更新作業。（有關 VANS 系統介接，請參考行政院國家資通安全會報技術服務中心之 VANS 專區 https://www.nccst.nat.gov.tw/VANS）。

2. 資通安全弱點通報機制（VANS）導入參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加弱點通報管理及有效控管組織風險，參考採購需求項目如下：

服務項目	採購需求項目
弱點通報機制	1. 軟體功能應具備可盤點與收集使用者電腦及伺服器主機上，已安裝之軟體資產與 Windows Update 資訊。 2. 上述軟體資產，至少包含 Windows 平台中之作業系統、應用程式、Java 函式庫等，軟體功能須可將軟體資產正規化為 CPE 格式，併同 Windows Update 資訊，產製符合 VANS 系統之上傳格式，讓機關可據以上傳至 VANS 系統。 3. 提供機關以 API 方式將 CPE 格式之軟體資產上傳至 VANS 系統，並可就 VANS 系統回饋之弱點資訊，找到機關內設備所在。

3. 資安弱點通報機制（VANS）導入參考廠商名單

資安弱點通報機制（VANS）導入參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源
	VANS 介接測試
ForeScout	√
中華數位科技股份有限公司	√
中華龍網股份有限公司	√
日月晶耀股份有限公司	√
旭辰資訊股份有限公司	√
捷睿智能股份有限公司	√
瑞思資訊股份有限公司	√
誠雲科技股份有限公司	√
達煬科技股份有限公司	√
睿明知通股份有限公司	√
精品科技股份有限公司	√
精誠資訊股份有限公司	√
優倍司股份有限公司	√
曜祥網技股份有限公司	√

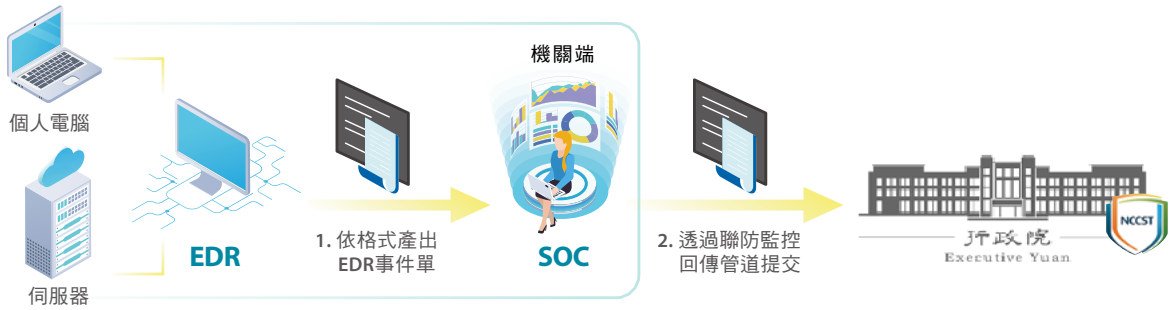
※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。VANS 介接測試係指經技服中心測試軟體資產上傳與 API 介接格式者（截至 110/10/05）

2.2.4 端點偵測及應變機制

1. 端點偵測及應變機制（EDR）導入參考實作方式

端點偵測及應變機制係指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業；以下提供建議實作流程做為參考：

布建於個人電腦及伺服器主機之 EDR 偵測到異常行為或惡意程式活動，並定期提供分析報告。資安法主管機關如公布指定提交偵測資料之方式（參考示意圖如下），EDR 須可配合產出相關資料格式並完成資料提交作業，以符資安法規定。



2. 端點偵測及應變機制（EDR）導入參考採購需求項目

機關可依預算額度洽詢外部專業資通安全服務資源，透過吸取資通安全專家知識及實務經驗，可增加端點偵測管理及有效控管組織風險，參考採購需求項目如下：

服務項目	採購需求項目
端點偵測及 應變機制服務	1. 提供端點威脅即時檢測及監控、持續性威脅獵捕以發掘潛藏威脅並預先加以攔截 2. 需定期提供分析報告 3. 可列出可疑程式之威脅程度（以指數或等級表示）、判斷依據與其相關資訊（metadata） 4. 協助單位進行資安事件調查及提供調查報告以符合資安法要求 5. 依資安法主管機關公布之提交方式，匯出並提交偵測資料以符合資安法要求 (1) 提供資料對外轉拋、介接功能或 API 可供利用（如可由 SOC 透過聯防監控資料回傳管道回傳） (2) 可提供經分析後高風險樣本或事件相關資訊

3. 端點偵測及應變機制（EDR）導入參考廠商名單

端點偵測及應變機制（EDR）導入參考廠商名單如下：

廠商名稱（以筆劃排序）	廠商具備資格來源
	政府共同供應契約
ACSI	√
Bitdefender	√
CheckPoint	√
COMODO	√
CounterTack	√
CrowdStrike	√
CyCarrier	√
Cylance	√
Fidelis-Cybersecurity	√
FireEye	√
Forcepoint	√
Fortinet	√
Kaspersky	√
LogRhythm	√
Malwarebytes	√
McAfee	√

廠商名稱（以筆劃排序）	廠商具備資格來源
	政府共同供應契約
Microsoft	√
PaloAltoNetworks	√
ReaQta	√
SentinelOne	√
Sophos	√
TeamT5	√
TREND	√
VMware	√
中芯數據股份有限公司	√
中華資安國際股份有限公司	√
中華數位科技股份有限公司	√
中華龍網股份有限公司	√
立寶科技股份有限公司	√
創泓科技股份有限公司	√
創穩資云股份有限公司	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。政府共同供應契約（web.pcc.gov.tw）包含標案案號 1090201 且契約終止日期為 110/04/07、標案案號 1090205 且契約終止日期為 110/10/02、標案案號 1100201 且契約終止日期為 111/04/19。行政院資通安全會報技術服務中心規劃邀集國內外 EDR 廠商討論配合意願（回傳格式、回傳方式），故現階段提供政府共同契約上之 EDR 產品廠商名單供參考。

2.2.5 資通安全防護

2.2.5.1 防毒軟體

1. 防毒軟體參考實作方式

根據組織安全政策，擬訂防毒策略，降低惡意攻擊的風險組織系統造成重大損害。

2. 防毒軟體參考採購需求項目

為了防止電腦病毒感染，在電腦上安裝防毒軟體是組織最基本的資安防線，提供即時病毒偵測，以及相關網頁安全性的掃描，避免電腦中毒而檔案損毀或隱私資料外流。採購人員在防毒軟體建議書徵求文件 (RFP) 參考採購需求項目如下：

產品名稱	採購需求項目
防毒軟體	1. 需求設備類型：工作站 / 伺服器 / 行動裝置 /SMTP/ 群組軟體防毒。 2. 可偵測病毒類型：病毒、蠕蟲、木馬程式、間諜程式、廣告軟體、Bot、零時差 (Zero-Day) 攻擊威脅、Rootkit 等惡意程式。 3. 病毒定義檔需要可以自動更新，並且部署到各設備中，以確保具有最新的定義檔，進行阻擋及防護作為。 4. 廠商所提供之防毒，需包含於 3 大防毒軟體評鑑機構 (AV-Comparatives, AV-TEST 與 Virus Bulletin) 所公布最新檢測排名。 5. 證明並強制執行組織 IT 政策與符合法規目標。

3. 防毒軟體參考廠商名單

防毒軟體參考廠商名單如下：

廠商名稱 （以筆劃排序）	資安服務機構能量登錄		政府共同供應契約合格廠商
	整合病毒與惡意程式防護檢測服務	防毒與惡意程式防護產品	防毒軟體產品
Sophos	—	—	√
三甲科技股份有限公司	√	—	—
中華資安國際股份有限公司	√	—	—
中華數位科技股份有限公司	√	—	—
台灣卡巴斯基實驗室	—	—	√
台灣恩益禧股份有限公司	√	—	—
台灣賽門鐵克股份有限公司	—	—	√
台灣邁克菲有限公司	—	—	√
安華聯網科技股份有限公司	√	—	—
安碁資訊股份有限公司	√	√	—
果核數位股份有限公司	√	—	—
眾至資訊股份有限公司	—	√	—
勤業眾信聯合會計師事務所	√	—	—
資通電腦股份有限公司	√	—	—
精誠資訊股份有限公司	√	—	—
網擎資訊軟體股份有限公司	√	√	—
豪勉科技股份有限公司	√	—	—
德欣寰宇科技股份有限公司	√	—	—
數聯資安股份有限公司	√	—	—
趨勢科技股份有限公司	—	√	√
關貿網路股份有限公司	√	—	—

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄（www.acw.org.tw）為 108-110 年之合格廠商。政府共同供應契約（web.pcc.gov.tw）標案案號 1090205 且契約終止日期為 110/10/02，標案案號 1100201 且契約終止日期為 111/04/19。

2.2.5.2 網路防火牆

1. 網路防火牆參考實作方式

根據組織安全政策，逐步擬訂網路防護策略，降低惡意攻擊的風險，避免組織系統造成重大損害。

2. 網路防火牆參考採購需求項目

經濟部工業局為推動資通安全產業發展，盤點資安業者技術能量，規劃建立資通安全服務機構能量分類與登錄機制，各機關可以依據資安防護需求進行採購，或從電子採購網資訊設備項下之電腦軟體下單，建構安全強固的產業環境。採購人員在網路防火牆採購時參考採購需求項目如下：

產品名稱	採購需求項目
網路防火牆	1. 防火牆的類型有網路層封包過濾、狀態偵測防火牆、代理伺服器防火牆、整合威脅管理 (UTM) 防火牆及新世代防火牆 (NGFW)，可視需求採購。 2. 防火牆規則可以依黑名單或白名單方式設定。 3. 防火牆具備使用及設定紀錄儲存，並支援遠端存放功能。 4. 須提供即時告警功能、具備 VPN 功能。 5. 可識別應用程式、防護加密流量，增加具備 API 介接功能尤佳，可使資安設備形成連合防護。

3. 網路防火牆參考廠商名單

網路防火牆參考廠商名單如下：

廠商名稱（以筆劃排序）	資安服務機構能量登錄	政府共同供應契約合格廠商
	防火牆產品	
Barracuda	—	√
Check Point	—	√
Cisco	—	√
COMODO	—	√
F5 Networks	—	√
Forcepoint	—	√
Fortinet	—	√
IMPERVA	—	√
Infoblox	—	√
Juniper	—	√
Radware	—	√
Sophos	—	√
WAF	—	√
WatchGuard	—	√
大同世界科技股份有限公司	√	—
中華資安國際股份有限公司	√	—

廠商名稱（以筆劃排序）	資安服務機構能量登錄	政府共同供應契約合格廠商
	防火牆產品	
中華電信股份有限公司臺灣北區電信分公司	—	√
四零四科技股份有限公司	√	—
兆勤科技股份有限公司	√	—
全球系統整合股份有限公司	√	—
安碁資訊股份有限公司	—	√
桓基科技股份有限公司	√	—
眾至資訊股份有限公司	√	—
勤紘科技股份有限公司	√	√
漢昕科技股份有限公司	—	√
豪勉科技股份有限公司	√	—
德欣寰宇科技股份有限公司	—	√
數聯資安股份有限公司	—	√
優易資訊股份有限公司	—	√
趨勢科技股份有限公司	√	—
關貿網路股份有限公司	√	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02，標案案號 1100201 且契約終止日期為 111/04/19。資安整合服務平台 (secpaas.org.tw) 廠商查詢截止日為 110/9/30。

2.2.5.3 電子郵件過濾機制

1. 電子郵件過濾機制參考實作方式

電子郵件安全依賴於良好規劃和管理原則，這些原則提供電子郵件系統和IT基礎架構安全性，透過適當規劃、系統管理和持續監控，得以維持有效安全性；藉由管理、維運和技術措施保護電子郵件系統，滿足其環境與資料的機密性、完整性和可用性需求，建議在安全實施和維護，應考量以下原則：

實施管理控制

安全的管理政策如組織的資訊安全策略和程序、風險評估及應變計劃。此外，組織應實施並提供安全意識和訓練，因許多攻擊部分或全部依賴於社交工程來操縱用戶。

以安全系統開發生命週期規劃系統

部署安全電子郵件系統的最關鍵方面是在安裝、配置和部署之前仔細規劃，應從系統開發生命週期的初始規劃階段考慮安性，在建置初期最大限度地提高安全性，可以有效地降低安全成本。

保護郵件伺服器應用程序

組織應安裝所需的最小郵件伺服器服務，並經由修補程序，配置或升級消除任何已知漏洞。保護郵件伺服器應用程序通常包括修補和升級郵件伺服器、配置郵件伺服器用戶身份驗證以及資源控制等。

保護郵件用戶端

為郵件用戶端提供適當等級的安全性需要仔細考慮以解決許多問題。包括安全地安裝、配置和使用郵件用戶端應用程序、啟用防毒、反垃圾郵件和反網路釣魚功能等。

確保傳輸安全

應加密用戶身份驗證，以保護訊息機密性和完整性的相關控制是部署安全的電子郵件解決方案，例如利用PKI技術對訊息進行加密和簽名。

保護作業環境

雖然郵件伺服器和郵件用戶端是電子郵件系統的兩個主要組件，但網路基礎結構對其安全作業至關重要，很多時候，網路基礎設施，包括防火牆、路由器、入侵檢測和防禦系統等元件，將在不受信任的網路和郵件伺服器之間提供第一道防禦。

2. 電子郵件過濾機制參考採購需求項目

電子郵件安全依賴於良好規劃和管理原則，這些原則提供電子郵件系統和IT基礎架構安全性，透過適當規劃、系統管理和持續監控，得以維持有效安全性；藉由管理、維運和技術措施保護電子郵件系統，滿足其環境與資料的機密性、完整性和可用性需求，建議在安全實施和維護，應考量以下原則：

產品名稱	採購需求項目
電子郵件過濾機制	1. 符合組織對於電子郵件安全的管理需求。 2. 提供過濾垃圾郵件、惡意威脅信件、進階威脅特定信件、病毒攻擊信件、社交工程信件等機制，杜絕外來不正當信件的入侵。 3. 具有郵件紀錄備份備援、附件管控、遠端調閱、密碼強度檢測、防偽偵測、進階防禦等功能。 4. 提供完善鑑別日誌以及自訂排程寄送鑑識報表。

3. 電子郵件過濾機制參考廠商名單

電子郵件過濾機制參考廠商名單如下：

廠商名稱（以筆劃排序）	資安服務機構能量登錄		政府共同供應契約合格廠商
	電子郵件安全管理與防護服務	電子郵件防護產品	
Barracuda	—	—	√
Bitdefender	—	—	√
COMODO	—	—	√
Forcepoint	—	—	√
NOPAM Themis	—	—	√
大同世界科技股份有限公司	√	—	—
大鈞科技股份有限公司	√	—	—
中華資安國際股份有限公司	√	—	—
中華數位科技股份有限公司	√	√	√
仁銓股份有限公司	√	—	—
立寶科技股份有限公司	√	—	—
兆勤科技股份有限公司	—	√	—
安碁資訊股份有限公司	√	—	—

廠商名稱（以筆劃排序）	資安服務機構能量登錄		政府共同供應契約合格廠商
	電子郵件安全管理與防護服務	電子郵件防護產品	
安資捷股份有限公司	√	—	—
思邦科技股份有限公司	√	—	—
凌群電腦股份有限公司	√	—	—
桓基科技股份有限公司	—	√	√
眾至資訊股份有限公司	√	√	—
創逸科技服務有限公司	√	—	—
漢昕科技股份有限公司	√	—	—
精誠資訊股份有限公司	√	√	—
網擎資訊軟體股份有限公司	√	√	—
德欣寰宇科技股份有限公司	√	—	—
數聯資安股份有限公司	√	√	—
趨勢科技股份有限公司	√	√	—
曜揚科技股份有限公司	√	—	—
鎧睿全球科技股份有限公司	√	√	—

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務 / 產品之能力。資安服務機構能量登錄（www.acw.org.tw）為 108-110 年之合格廠商。政府共同供應契約（web.pcc.gov.tw）標案案號 1100201 且契約終止日期為 111/04/19。

2.2.5.4 入侵偵測及防禦機制

1. 入侵偵測及防禦機制參考實作方式

入侵偵測及防禦系統的安全依賴於良好的規劃和管理原則，透過適當的執行、系統管理和持續監控，得以維持有效的安全性；藉由管理、維運和技術措施保護入侵偵測及防禦系統，建議在安全的實施和維護，應考量以下原則：

2. 入侵偵測及防禦機制參考採購需求項目

入侵偵測及防禦機制應依照組織內部網路的現狀進行規劃，達到所需的安全標準。採購人員在入侵偵測及防禦機制建議書徵求文件 (RFP) 參考採購需求項目如下：

產品名稱	採購需求項目
入侵偵測及防禦機制	1. 符合組織對於資訊蒐集、管理、偵測及預防等四個安全需求目標。 2. 可協助蒐集主機資訊及相關網路連接資訊、作業系統資訊、應用程式資訊及網路特性資訊等蒐集能力。對網路型 IDP 而言，條列網路層、傳輸層、應用層協定的分析，解釋分析執行的數量 (如特徵偵測、異常偵測及狀態偵測)。對主機型 IDP 而言，條列監視的特殊來源 (如日誌檔、系統檔、網路介面)，及解釋如何進行監測 (如改變的偵測、檔案存取要求的行為處理、TCP/IP 堆疊監測)。 3. 可識別事故 (Incident) 的型態，例如阻絕服務攻擊、後門程式 (Backdoor)、違反政策 (Policy Violation)、通訊埠掃描 (Port Scan)、惡意軟體 (Malware)(如蠕蟲、特洛伊木馬、惡意碼等) 及未經授權應用程式 / 協定，諸如 P2P 的使用。 4. 提供執行分析、確認告警正確性、事件及事件紀錄關連，包含郵戳 (Timestamp)、事件型態、事件來源與處理方式等機制及相符的 CVE 編號與影響程度等資訊，以修正政策設定如變更白名單 (Whitelist)、黑名單 (Blacklist)、定限 (Threshold) 等安全能力。

3. 入侵偵測及防禦機制參考廠商名單

入侵偵測及防禦機制參考廠商名單如下：

廠商名稱 (以筆劃排序)	資安服務機構能量登錄		政府共同供應契約合格廠商
	入侵偵測與防禦服務	入侵偵測與防禦產品	
三甲科技股份有限公司	—	√	—
大同世界科技股份有限公司	—	—	—
中孚科技股份有限公司	—	—	√
中華資安國際股份有限公司	—	√	√
四零四科技股份有限公司	—	√	—
安侯企業管理股份有限公司	√	—	—
安碁資訊股份有限公司	√	—	√
安資捷股份有限公司	√	—	—
均易科技股份有限公司	—	—	√
宏碁資訊服務股份有限公司	—	—	√
亞綸科技股份有限公司	—	—	√
佳儀國際有限公司	—	—	√
協科資訊股份有限公司	√	—	—
東宜資訊股份有限公司	—	—	√
東品資訊有限公司	—	—	√
飛泓科技股份有限公司	√	√	—
凌群電腦股份有限公司高雄分公司	—	—	√
殷諾科技股份有限公司	—	—	√

廠商名稱 (以筆劃排序)	資安服務機構能量登錄		政府共同供應契約合格廠商
	入侵偵測與防禦服務	入侵偵測與防禦產品	
泰鋒電腦股份有限公司	√	—	—
動力安全資訊股份有限公司	√	—	—
捷睿智能股份有限公司	—	√	—
眾至資訊股份有限公司	—	√	—
創穩資云股份有限公司	√	—	—
博威資訊有限公司	—	—	√
博鉅資訊股份有限公司	—	—	√
華苓科技股份有限公司	√	—	—
勤紘科技股份有限公司	—	—	—
勤業眾信聯合會計師事務所	√	√	—
新加坡商網達先進科技 (台灣分公司)	√	—	√
精誠資訊股份有限公司	—	—	√
豪勉科技股份有限公司	—	√	√
德欣寰宇科技股份有限公司	√	—	—
數聯資安股份有限公司	√	—	√
趨勢科技股份有限公司	—	√	—
鴻寬科技有限公司	√	—	—

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄（www.acw.org.tw）為 108-110 年之合格廠商。政府共同供應契約（web.pcc.gov.tw）標案案號 1090205 且契約終止日期為 110/10/02。政府採購網（web.pcc.gov.tw）決標紀錄，以 109-110 年 8 月入侵偵測採購決標紀錄。

2.2.5.5 應用程式防火牆

1. 應用程式防火牆參考實作方式

根據組織安全政策，擬訂網路安全策略，降低惡意攻擊的風險及避免組織系統造成重大損害。

2. 應用程式防火牆參考採購需求項目

經濟部工業局為推動資通安全產業發展，盤點資安業者技術能量，規劃建立資通安全服務機構能量分類與登錄機制，各機關可以依據資安防護需求進行採購，或從電子採購網資訊設備項下之電腦軟體下單，建構安全強固的產業環境。採購人員在網路防火牆採購時參考採購需求項目如下：

產品名稱	採購需求項目
應用程式防火牆	1. 可針對最新版 OWASP TOP 10 攻擊行為進行偵測與攔截。 2. 符合信用卡國際組織 PCI DSS 規範之要求。 3. 可防止或降低 DOS/DDOS 之攻擊。 4. 具備辨識敏感資料洩露功能，例如身份證字號、持卡人資料。

3. 應用程式防火牆參考廠商名單

應用程式防火牆參考廠商名單如下：

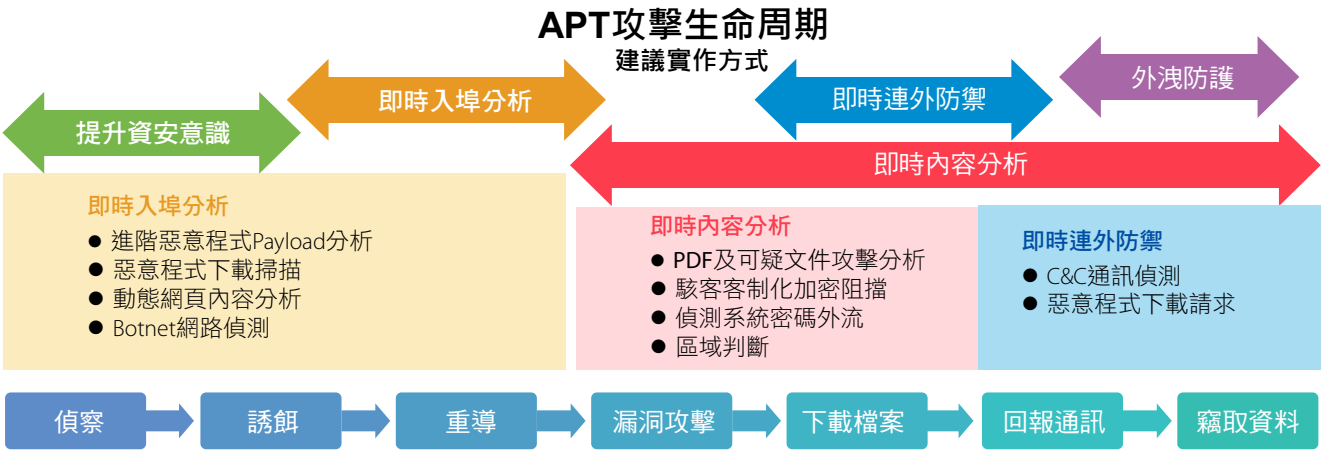
廠商名稱 （以筆劃排序）	資安服務機構能量登錄 應用程式防火牆產品	政府共同供應契約合格廠商
Barracuda Networks	—	√
IMPERVA	—	√
中芯數據股份有限公司	—	√
中華資安國際股份有限公司	√	—
中華電信股份有限公司臺灣北區電信分公司	—	√
安碁資訊股份有限公司	—	√
桓基科技股份有限公司	—	√
眾至資訊股份有限公司	√	—
華電聯網股份有限公司	—	√
勤紘科技股份有限公司	—	√
漢昕科技股份有限公司	—	√
豪勉科技股份有限公司	√	—
德欣寰宇科技股份有限公司	—	√
數聯資安股份有限公司	—	√
優易資訊股份有限公司	—	√
趨勢科技股份有限公司	√	—
關貿網路股份有限公司	—	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄 (www.acw.org.tw) 為 108-110 年合格廠商。政府共同供應契約 (web.pcc.gov.tw) 標案案號 1090205 且契約終止日期為 110/10/02、標案案號 1100201 且契約終止日期為 111/04/19。

2.2.5.6 進階持續性威脅攻擊防禦

1. 進階持續性威脅攻擊防禦措施參考實作方式

進階持續性威脅 (Advanced Persistent Threat，APT) 攻擊滲透的策略與手法，是精心策劃的鎖定目標攻擊，超越傳統特徵碼導向的安全機制，長期潛伏在組織的系統當中而不被發現，必須不斷提升自己的安全機制，應考量 APT 攻擊生命周期，才能偵測並防止這些新興攻擊和持續滲透：



2. 進階持續性威脅攻擊防禦措施參考採購需求項目

解決 APT 之防護方式，採購人員在建議書徵求文件 (RFP) 參考採購需求項目如下：

產品項目	採購需求項目
進階持續性威脅攻擊防護	1. 可結合與利用入侵防禦系統、次世代防火牆、安全電子郵件閘道、終端保全以及威脅偵測等工具，直接阻絕已知威脅與資訊行動的預防能力。 2. 具有惡意程式分析、內網滲透、隱匿行為、帳號入侵、資料外洩、檢查網路流量行為及使用者與內容等偵測能力。 3. 回應可能發生的事件，隔離使用者、裝置或內容，確保網路資源與組織資料安全的緩解能力。

3. 進階持續性威脅攻擊防禦措施參考廠商名單

進階持續性威脅攻擊防禦措施參考廠商名單如下：

廠商名稱（以筆劃排序）	資安服務機構能量登錄		政府共同供應契約合格廠商
	入侵偵測與防禦服務	入侵偵測與防禦產品	
Cellopoint	—	—	√
Check Point	—	—	√
Fidelis Cybersecurity	—	—	√
FireEye	—	—	√
Lastline	—	—	√
McAFee	—	—	√
Sophos	—	—	√
中華資安國際股份有限公司	√	—	√
中華數位科技股份有限公司	√	—	√
中華龍網股份有限公司	√	√	—
立寶科技股份有限公司	√	—	—
安侯企業管理股份有限公司	√	—	—
安華聯網科技股份有限公司	√	—	—
安碁資訊股份有限公司	√	—	—
安資捷股份有限公司	√	—	—
杜浦數位安全有限公司	—	√	—

廠商名稱（以筆劃排序）	資安服務機構能量登錄		政府共同供應契約合格廠商
	入侵偵測與防禦服務	入侵偵測與防禦產品	
協科資訊股份有限公司	√	—	—
果核數位股份有限公司	√	—	—
華電聯網股份有限公司	√	—	—
華碩雲端股份有限公司	√	—	—
勤業眾信聯合會計師事務所	√	—	—
奧義智慧科技股份有限公司	—	√	√
新加坡商網達先進科技（台灣分公司）	√	—	—
精誠軟體服務股份有限公司	—	—	√
網擎資訊軟體股份有限公司	√	—	—
豪勉科技股份有限公司	—	—	√
德欣寰宇科技股份有限公司	√	—	—
數聯資安股份有限公司	√	—	√
趨勢科技股份有限公司	—	—	√
鴻寬科技有限公司	√	—	—
鎧睿全球科技股份有限公司	—	√	—
關貿網路股份有限公司	√	—	√

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄（www.acw.org.tw）為 108-110 年之合格廠商。政府共同供應契約（web.pcc.gov.tw）標案案號 1090205 且契約終止日期為 110/10/02。

認知與訓練面

資通安全應當由基礎做起，《資通安全管理法》各適用機關中所有的人對於資通安全都有一定程度概念之後，《資通安全管理法》各適用機關控管的資通系統及各項防護自然可保持於一定安全等級之上。將針對《資通安全責任等級分級辦法》之認知與訓練面「資通安全教育訓練」議題進行實務研析，提出建立及執行認知與訓練面辦理項目應有之基本原則及建議性作法等，作為《資通安全管理法》各適用機關規劃及執行認知與訓練面之參考。

2.3 認知與訓練面

2.3.1 資通安全教育訓練

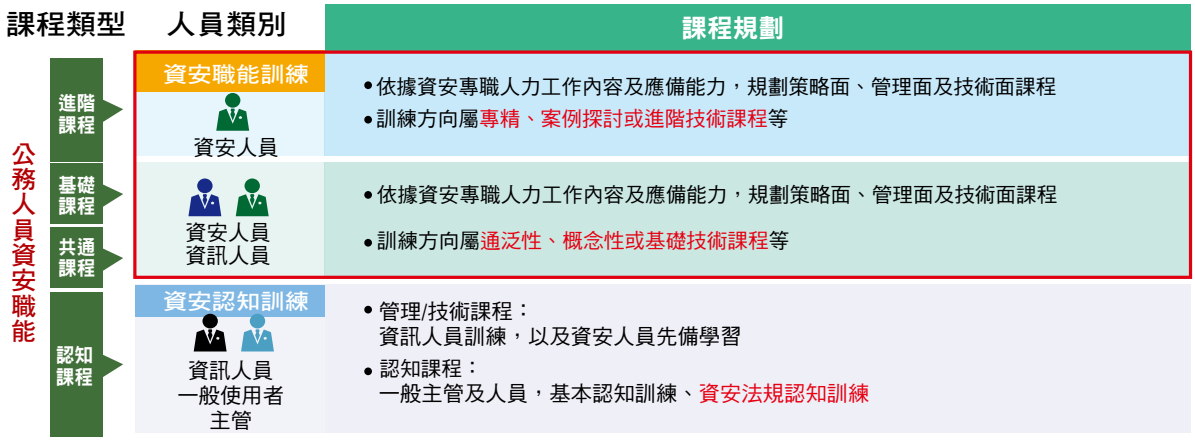
2.3.1.1 資通安全專職（責）人員

1. 資通安全專職（責）人員資通安全教育訓練參考實作方式

2. 資通安全專職（責）人員資通安全教育訓練參考採購需求項目

目前針對公務人員所擔任之職務與負責任務，規劃其執行業務時應具備之資通安全知識與技能，分策略面、管理面及技術面 3 個面向，建議依人員業務需求參與相關訓練，以增補對應之職能。

面 向	策略面應備能力	管理面應備能力	技術面應備能力
共通職能	具備資通安全基本認知及資通安全法規認知		
專業職能	●具資安策略規劃與推動能力 ●具資安管理業務審查能力 ●具資安資源協調規劃能力 ●具資安稽核與管理能力 ●具績效與成果監督能力	●具資安管理機制規劃與維運能力 ●具資安資源配置與管理能力 ●具資安風險與控制評估能力 ●具處理通報應變作業能力	●具網路管理能力 ●具事件處理能力 ●具資安檢測能力 ●具系統管理能力 ●具情資分析與分享能力



資料來源：行政院國家資通安全會報技術服務中心

3. 資通安全專職（責）人員資通安全教育訓練參考廠商名單

資通安全專職（責）人員資通安全教育訓練參考廠商名單如下：

資通安全職能訓練課程	
廠商名稱（以筆劃排序）	技術服務中心遴選通過
中國文化大學	√
中興大學	√
健行科技大學	√
崑山科技大學	√
逢甲大學	√
朝陽科技大學	√
臺北市職能發展學院	√
臺北醫學大學	√

符合資安法 FAQ3.15 資格		
實體課程優先	1. 參加技服中心舉辦之政府資通安全防護巡迴研討會，或所開設之資通安全策略、管理、技術相關課程	
	2. 參加資通安全專業證照清單上所列之訓練課程	
	3. 參加國內外之公私營訓練機構所開設或受委託辦理之資通安全策略、管理或技術訓練課程。前述第 3 種辦理之訓練機構以下列型態為限：	(1) 公私立大專校院
		(2) 依法設立 2 年以上之職業訓練機構
		(3) 依法設立 2 年以上之短期補習班
		(4) 依法設立 2 年以上之學術研究機構或財團法人，其設立章程宗旨與人才培訓相關，且有辦理人才培訓業務
線上課程每人每年認定上限為 6 小時	數位學習資源整合平臺「e 等公務園 + 學習平臺」	

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。技術服務中心（www.nccst.nat.gov.tw）為 109-110 年遴選通過資安職能訓練機構。依 FAQ3.15，資通安全專業課程訓練，係指可對應資安職能訓練發展藍圖中策略面、管理面、技術面之課程為原則（https://ctts.nccst.nat.gov.tw/about/Training）。符合資安法 FAQ3.15 資格，係指所辦理之資安專業訓練課程時數受資安法主管機關認可的機構資格。

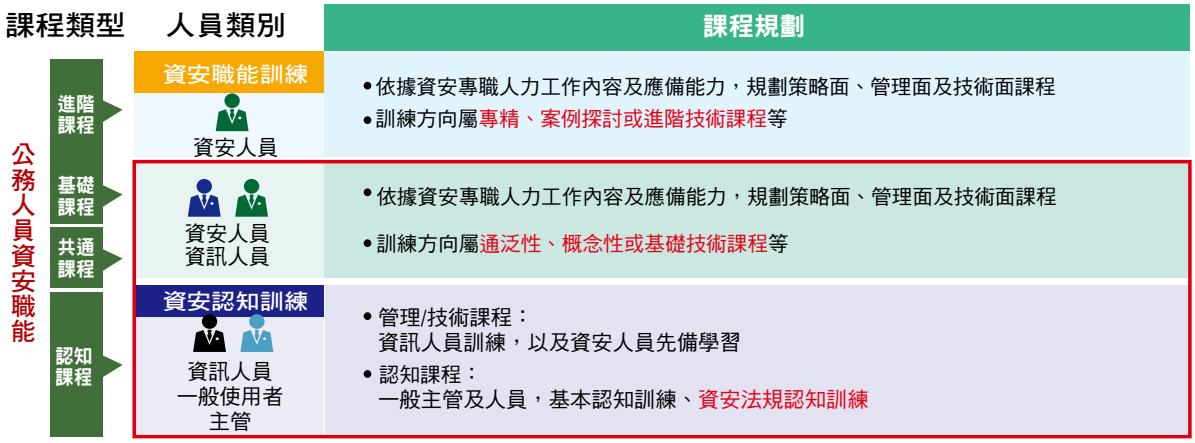
2.3.1.2 資通安全專職（責）人員以外之資訊人員

1. 資通安全專職（責）人員以外之資訊人員資通安全教育訓練參考實作方式

2. 資通安全專職（責）人員以外之資訊人員資通安全教育訓練參考採購需求項目

目前針對公務人員所擔任之職務與負責任務，規劃其執行業務時應具備之資通安全知識與技能，分策略面、管理面及技術面 3 個面向，建議依人員業務需求參與相關訓練，以增補對應之職能。

面 向	策略面應備能力	管理面應備能力	技術面應備能力
共通職能	具備資通安全基本認知及資通安全法規認知		
專業職能	●具資安策略規劃與推動能力 ●具資安管理業務審查能力 ●具資安資源協調規劃能力 ●具資安稽核與管理能力 ●具績效與成果監督能力	●具資安管理機制規劃與維運能力 ●具資安資源配置與管理能力 ●具資安風險與控制評估能力 ●具處理通報應變作業能力	●具網路管理能力 ●具事件處理能力 ●具資安檢測能力 ●具系統管理能力 ●具情資分析與分享能力



資料來源：行政院國家資通安全會報技術服務中心

3. 資通安全專職（責）人員以外之資訊人員資通安全教育訓練參考廠商名單

資通安全專職（責）人員以外之資訊人員資通安全教育訓練參考廠商名單如下：

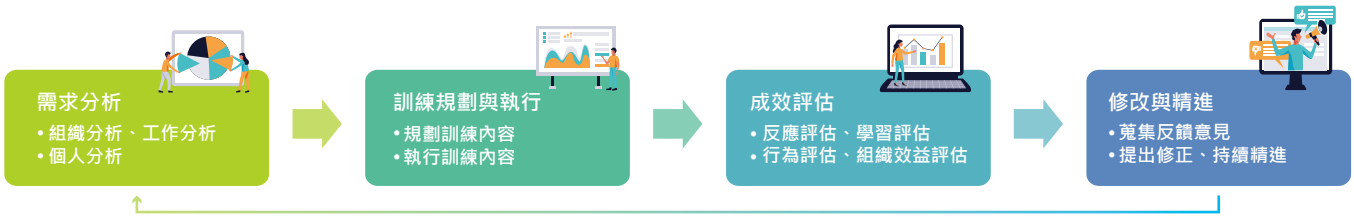
資通安全職能訓練課程	
廠商名稱（以筆劃排序）	技術服務中心遴選通過
中國文化大學	√
中興大學	√
健行科技大學	√
崑山科技大學	√
逢甲大學	√
朝陽科技大學	√
臺北市職能發展學院	√
臺北醫學大學	√

符合資安法 FAQ3.15 資格		
實體課程優先	1. 參加技服中心舉辦之政府資通安全防護巡迴研討會，或所開設之資通安全策略、管理、技術相關課程	
	2. 參加資通安全專業證照清單上所列之訓練課程	
	3. 參加國內外之公私營訓練機構所開設或受委託辦理之資通安全策略、管理或技術訓練課程。前述第 3 種辦理之訓練機構以下列型態為限：	(1) 公私立大專校院
		(2) 依法設立 2 年以上之職業訓練機構
		(3) 依法設立 2 年以上之短期補習班
		(4) 依法設立 2 年以上之學術研究機構或財團法人，其設立章程宗旨與人才培訓相關，且有辦理人才培訓業務
線上課程每人每年認定上限為 6 小時		數位學習資源整合平臺「e 等公務園 + 學習平臺」

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。技術服務中心（www.nccst.nat.gov.tw）為 109-110 年遴選通過資安職能訓練機構。依 FAQ3.15，資通安全專業課程訓練，係指可對應資安職能訓練發展藍圖中策略面、管理面、技術面之課程為原則（https://ctts.nccst.nat.gov.tw/about/Training）。符合資安法 FAQ3.15 資格，係指所辦理之資安專業訓練課程時數受資安法主管機關認可的機構資格。

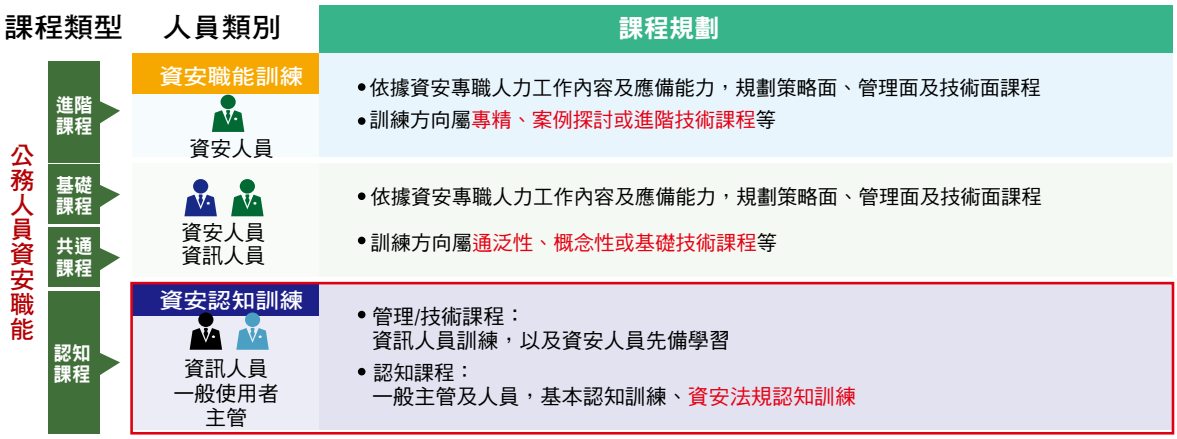
2.3.1.3 一般使用者與主管

1. 一般使用者與主管資通安全教育訓練參考實作方式



2. 一般使用者與主管資通安全教育訓練參考採購需求項目

公務人員資安職能規劃，係針對公務人員所擔任之職務與負責任務，規劃其執行業務時應具備之資通安全知識與技能。依據不同職務與任務，規劃資安實務訓練課程、發展教材並建立資安能力之評量制度。



資料來源：行政院國家資通安全會報技術服務中心

3. 一般使用者與主管資通安全教育訓練參考廠商名單

一般使用者與主管資通安全教育訓練參考廠商名單如下：

廠商名稱（以筆劃排序）	資安服務機構能量登錄	資安整合服務平台廠商	技術服務中心遴選通過	符合資安法FAQ3.15資格
三甲科技股份有限公司	√	√	–	–
中國文化大學推廣教育部	–	–	√	√
中華民國電腦技能基金會	–	–	–	√
中華民國電腦稽核協會	–	–	–	√
中華資安國際股份有限公司	√	√	–	–
中華電信股份有限公司	√	–	–	–
中華電信學院	–	√	–	√
中興大學創新產業暨國際學院	–	–	√	√
互聯安睿資通股份有限公司	√	√	–	–
可立可資安股份有限公司	√	–	–	–
台中市電腦商業同業公會	–	–	–	√
台灣資訊暨綠色產業發展協會	–	–	–	√
台灣數位安全聯盟	–	–	–	√
台灣檢驗科技股份有限公司	–	–	–	√
巨匠電腦股份有限公司	–	–	–	√
白帽犀牛有限公司	√	–	–	–
全智網科技股份有限公司	–	–	–	√
如梭世代有限公司	√	√	–	–
安永企業管理諮詢服務	√	–	–	–
安侯企業管理股份有限公司	√	–	–	–
安華聯網科技股份有限公司	√	√	–	–
安碁資訊股份有限公司	√	√	–	–
行政院國家資通安全會報技術服務中心	–	–	–	√
協志聯合科技股份有限公司	√	–	–	–
恆逸教育訓練中心	–	–	–	√
香港商英國標準協會太平洋有限公司	√	–	–	√
凌群電腦股份有限公司	–	√	–	–

廠商名稱（以筆劃排序）	資安服務機構能量登錄	資安整合服務平台廠商	技術服務中心遴選通過	符合資安法FAQ3.15資格
財團法人工業技術研究院	–	–	–	√
財團法人資訊工業策進會	–	–	–	√
健行科技大學推廣教育中心	–	–	√	√
崑山科技大學進修推廣處	–	–	√	√
逢甲大學	–	–	√	–
創穩資云股份有限公司	√	–	–	–
朝陽科技大學推廣教育處	–	–	√	√
勤業眾信聯合會計師事務所	√	–	–	–
新加坡商網達先進科技有限公司	√	–	–	–
經濟部	–	–	–	√
資拓宏宇國際股份有限公司	√	–	–	–
資通電腦股份有限公司	√	–	–	–
資誠聯合會計師事務所	√	–	–	–
漢昕科技股份有限公司	√	–	–	–
精誠軟體資訊有限公司	√	√	–	–
臺北市職能發展學院	–	–	√	√
臺北醫學大學	–	–	√	–
德欣寰宇科技股份有限公司	√	–	–	–
德諾科技服務有限公司	√	–	–	–
叡揚資訊股份有限公司	√	–	–	–
盧氪賽忒股份有限公司	√	√	–	–
靜宜大學推廣教育處	–	–	–	√
戴夫寇爾股份有限公司	√	√	–	–
聯準科技服務有限公司	√	–	–	–
鎧睿全球科技股份有限公司	–	√	–	–
關貿網路股份有限公司	√	–	–	–
關鍵智慧科技有限公司	√	–	–	–
鑒真數位有限公司	√	√	–	–

※ 備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。技術服務中心（www.nccst.nat.gov.tw）為 109-110 年遴選通過資安職能訓練機構。公務機關可至行政院人事行政總處公務人力發展學院（www.hrd.gov.tw）「e 等公務園＋學習平台」（elearn.hrd.gov.tw）修習資通安全相關課程以符合法遵要求。符合資安法FAQ3.15 資格，係指所辦理之資安專業訓練課程時數受資安法主管機關認可的機構資格。

2.3.2 專業證照及職能訓練證書

2.3.2.1 資通安全專業證照

1. 資通安全專業證照參考實作方式

市面上之資通安全專業證照琳瑯滿目，以下提供資通安全專業證照建議實作流程做為挑選證照之參考：

評估及分析

發證機構通常將資通安全專業證照會有級別上的差異。
申請者可視本身的工作需求、資格條件(經驗、技能)及未來目標來決定報考認證之主題與級別。

申請考照

申請者可與我國取得發證機構授權認證教育訓練及考試服務之訓練機構聯繫。

維持證照有效性

證照有效性之影響因素如下：
1.繳交年費
2.規定年限內至少要完成規定時數之專業教育時數
3.規定年限內至少要累積規定時數之專業執行經驗
4.符合發證機構之規範
5.規定年限內，指定之項目積分需達一定分數以上。

2. 資通安全專業證照參考採購需求項目

我國已有多家經原廠授權之資安專業證照教育訓練機構，組織可依需求透過前述機構協助人員取得資通安全專業證照。採購人員在資通安全專業證照建議書徵求文件 (RFP) 參考採購需求項目如下：

配合組織需求 提出訓練計畫書 → 依據訓練計畫書 實施訓練課程 → 協助取得 專業證照 → 協助維護專業 證照之有效性 → 提供成效 評估報告

3. 資通安全專業證照參考廠商名單

透過行政院國家資通安全會報公告資訊及相關官網資訊彙整資通安全專業證照發證機構名單如下：

發證機構（以筆劃排序）	行政院國家資通安全會報公告名單
經濟部	√
（ISC）[2]	√
Cisco	√
CompTIA	√
CREST	√
EC-Council	√
GIAC	√
ISACA	√
ISFCE	√
Offensive Security	√
ISA	√

廠商名稱（以筆劃排序）	原廠授權（認證教育訓練/考試服務）
中國文化大學推廣教育部	√
中華民國電腦技能基金會	√
中華民國電腦稽核協會	√
台灣檢驗科技股份有限公司	√
巨匠電腦股份有限公司	√
全智網科技股份有限公司	√
恆逸教育訓練中心	√
香港商英國標準協會太平洋有限公司	√
香港商漢德技術監督服務亞太有限公司	√
財團法人資訊工業策進會	√

※ 備註：廠商未列入廠商名單中，不表示其未具提供該項服務之能力。行政院國家資通安全會報（nicst.ey.gov.tw）與原廠授權查詢截止日為 110/9/30。資安法認可的資安專業證照，會定期公布在資安會報網站上，區分為管理面跟技術面；另也有「資通安全專業證照認可審查作業流程」，供機關申請異動安專業證照。
https://nicst.ey.gov.tw/Page/D94EC6EDE9B10E15/3386e586-1930-4f48-9b5e-1c9f256b7549

2.3.2.2 資通安全職能評量證書

1. 資通安全職能評量證書參考實作方式

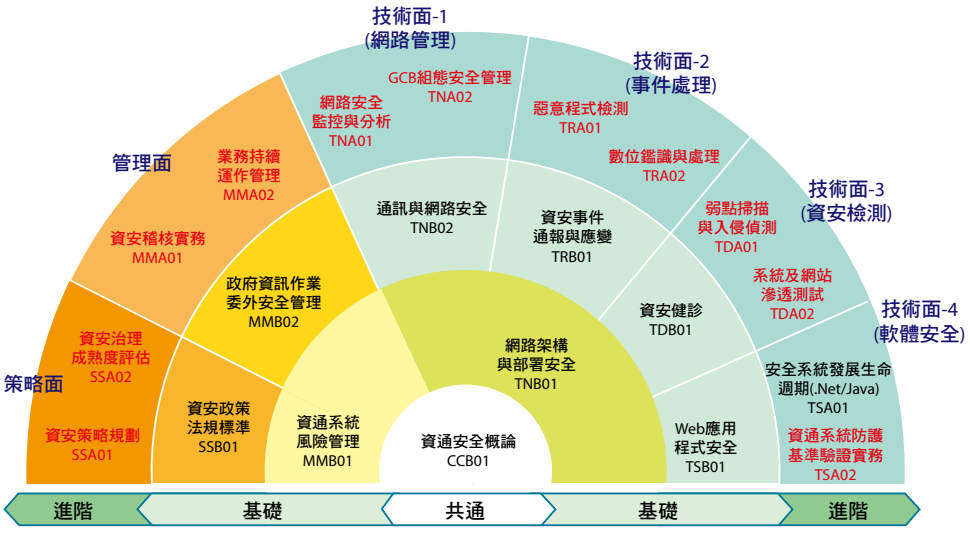
資通安全職能評量證書係指資安專職人員根據機關業務所需，參加資安職能訓練並通過評量取得證書，以下提供建議實作流程做為參考：

評估及分析	申請考照	維持證照有效性
資通安全職能課程類別依屬性分為策略面、管理面及技術面三面向應備能力，申請者可視本身的工作需求、資格條件(經驗、技能)及未來目標來選擇報名之課程。	申請者可由行政院國家資通安全會報技術服務中心遴選而出之資安職能訓練課程及評量服務機構聯繫。	證照維護方式如下：(二擇一) 一、重新參與訓練與評量 二、參與換證評量

2. 資通安全職能評量證書參考採購需求項目

公務人員資安職能規劃，建議針對其擔任之職務與負責任務，參考資安職能訓練發展藍圖，派員參與相關課程訓練，並可自行洽資通安全職能訓練機構開設專班供機關及所屬同仁集中受訓。

面 向	策略面應備能力	管理面應備能力	技術面應備能力
共通職能	具備資通安全基本認知及資通安全法規認知		
專業職能	●具資安策略規劃與推動能力 ●具資安管理業務審查能力 ●具資安資源協調規劃能力 ●具資安稽核與管理能力 ●具績效與成果監督能力	●具資安管理機制規劃與維運能力 ●具資安資源配置與管理能力 ●具資安風險與控制評估能力 ●具處理通報應變作業能力	●具網路管理能力 ●具事件處理能力 ●具資安檢測能力 ●具系統管理能力 ●具情資分析與分享能力



資料來源：行政院國家資通安全會報技術服務中心

3. 資通安全職能評量證書參考廠商名單

行政院國家資通安全會報技術服務中心遴選出資安職能訓練課程及評量服務機構名單彙整如下：

廠商名稱 （以筆劃排序）	技術服務中心遴選通過
中國文化大學	√
中興大學	√
台北市職能發展學院	√
健行科技大學	√
崑山科技大學	√
逢甲大學	√
朝陽大學	√
臺北醫學大學	√

※ 備註：技術服務中心（www.nccst.nat.gov.tw）109 -110 年遴選通過資安訓練機構。

第三章

《資通安全管理法》採購指引廠商名錄

3.《資通安全管理法》採購指引廠商名錄

依據《資通安全管理法》子法《資通安全責任等級分級辦法》制訂各等級應辦事項，針對以下研析議題彙整參考資通安全服務 / 產品廠商，以供適用等級機關予以參考。

★ 經濟部工業局技術服務機構服務能量登錄：通過經濟部工業局資訊安全技術服務機構服務能量登錄
▼ 資安檢測診斷服務團隊 / 資安整合服務平台廠商
＊ 政府採購網決標紀錄：刊登於政府電子採購網之決標公告
▲ 刊登於政府電子採購網之共同供應契約
◆ 經行政院國家資通安全會報公告之資通安全專業證照發證機構
■ 經國家資通安全技術服務中心遴選通過資通安全職能評量證書之資安訓練機構
◎ 經原廠授權教育訓練或考試服務之機構
※ TAF 官網公告「資訊安全管理系統」認可管理系統驗證機構
⊕ 官網：符合「資訊安全管理系統導入參考資訊安全服務廠商名單」且官網公告含有 ISO/IEC 22301 顧問導入服務
◇ 符合《資通安全管理法》FAQ3.15 資格
√ 經技服中心測試軟體資產上傳與 API 介接格式者

參考資訊安全服務 / 產品廠商（以筆劃及中文優先排序）	管理面				技術面															認知與訓練面				
					安全性檢測		資通安全健診					資通安全弱點通報機制	端點偵測及應變機制	資通安全防護						資通安全教育訓練			專業證照及職能訓練證書	
	資訊安全管理系統導入	資訊安全管理系統第三方驗證	內部資通安全稽核	業務持續運作演練	弱點掃描	滲透測試	網路架構檢視	網路惡意活動檢視	使用者端電腦惡意活動檢視	伺服器主機惡意活動檢視	目錄伺服器設定及防火牆連線設定檢視			防毒軟體	網路防火牆	電子郵件過濾機制	入侵偵測及防禦機制	應用程式防火牆	進階持續性威脅攻擊防禦	資通安全專職（責）人員	資通安全專職（責）人員以外之資訊人員	一般使用者與主管	資通安全專業證照	資通安全職能評量證書
又碩電腦科技股份有限公司					★																			
三甲科技股份有限公司	★		★		★▼	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼			★			★					★▼		
大同世界科技股份有限公司	★		★		▼	★	▼	▼	▼	▼	▼				★	★								
大鈞科技股份有限公司																★								
中孚科技股份有限公司																	▲							
中芯數據股份有限公司					★▲	★▲	★▲	★▲	★▲	★▲	★▲		▲					▲						
中國文化大學																				■◇	■◇	■◇	◎	■
中揚資訊有限公司	★		★																					
中華民國電腦技能基金會																				◇	◇	◇	◎	
中華民國電腦稽核協會																				◇	◇	◇	◎	
中華資安國際股份有限公司	★＊		★＊		★▲▼	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼		▲	★	★	★	★▲	★	★▲			★▼		
中華電信股份有限公司	★＊		★＊																			★		
中華電信股份有限公司臺灣北區電信分公司															▲			▲						
中華電信學院																					▼◇	▼◇		
中華數位科技股份有限公司												√	▲	★		★▲			★▲					
中華龍網股份有限公司					★▼		★▲	★▲	★▲	★▲	★▲	√	▲						★▼					
中興大學																				■◇	■◇	■◇		■
互聯安睿資通股份有限公司					★	★▼																★▼		
仁銓股份有限公司																★								
日月晶耀股份有限公司												√												
可立可資安股份有限公司																					★	★		
台中市電腦商業同業公會																				◇	◇	◇		
台北市職能發展學院																				■◇	■◇	■◇		■
台眾電腦股份有限公司							★▼	★▼	★▼	★▼	★▼													
台灣卡巴斯基實驗室														▲										
台灣恩益禧股份有限公司					★		★	★	★	★	★			★										
台灣資訊暨綠色產業發展協會																				◇	◇	◇		
台灣數位安全聯盟																				◇	◇	◇		

＊以上為參考名單，最新廠商名單請依各官網為準。

參考資訊安全服務／產品廠商（以筆劃及中文優先排序）	管理面				技術面															認知與訓練面				
					安全性檢測		資通安全健診					資通安全弱點通報機制	端點偵測及應變機制	資通安全防護						資通安全教育訓練			專業證照及職能訓練證書	
	資訊安全管理系統導入	資訊安全管理系統第三方驗證	內部資通安全稽核	業務持續運作演練	弱點掃描	滲透測試	網路架構檢視	網路惡意活動檢視	使用者端電腦惡意活動檢視	伺服器主機惡意活動檢視	目錄伺服器設定及防火牆連線設定檢視			防毒軟體	網路防火牆	電子郵件過濾機制	入侵偵測及防禦機制	應用程式防火牆	進階持續性威脅攻擊防禦	資通安全專職（責）人員	資通安全專職（責）人員以外之資訊人員	一般使用者與主管	資通安全專業證照	資通安全職能評量證書
台灣應用軟件股份有限公司	★*		★*																			◇		
台灣檢驗科技股份有限公司	*	※	*																	◇	◇	◇	◎	
台灣賽門鐵克股份有限公司														▲										
台灣邁克菲有限公司														▲										
四零四科技股份有限公司															★		★							
巨匠電腦股份有限公司																				◇	◇	◇	◎	
永豐技服科技有限公司							★	★	★	★	★													
白帽犀牛有限公司					★	★																★		
立寶科技股份有限公司													▲			★			★					
兆勤科技股份有限公司															★	★								
光盾資訊科技有限公司					▲	▲	▲	▲	▲	▲	▲													
全球系統整合股份有限公司															★									
全智網科技股份有限公司																				◇	◇	◇	◎	
如梭世代有限公司					★▼	★▼																★▼		
安永企業管理諮詢服務股份有限公司	★*		★*																			★		
安侯企業管理股份有限公司	★*		★*	*	★	★	★	★	★	★	★						★		★			★		
安華聯網科技股份有限公司	★		★		★▲▼	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼			★					★			★▼		
安源電腦股份有限公司																								
安碁資訊股份有限公司	★*		★*		★▲▼	★▲	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼			★	▲	★	★▲	▲	★			★▼		
安資捷股份有限公司					▲											★	★		★					
旭辰資訊股份有限公司																								
自由系統股份有限公司	★		★		★																			
艾法諾國際股份有限公司		※																						
行政院國家資通安全會報技術服務中心																				◇	◇	◇		
均易科技股份有限公司																	▲							
宏碁資訊服務股份有限公司	*		*	*⊕	★												▲							
杜浦數位安全有限公司																			▼					
亞綸科技股份有限公司																	▲							
佳儀國際有限公司																	▲							
協志聯合科技股份有限公司					★																	★		
協科資訊股份有限公司							★	★	★	★	★					★	★		★					
延宇資訊股份有限公司	*		*																					
承弘國際股份有限公司					★▼	★▼																		
昇達價值管理股份有限公司	*		*																					
昕恩科技有限公司					★	★																		
東宜資訊股份有限公司																	▲							
東品資訊有限公司																	▲							
東捷資訊服務股份有限公司																★								
松之安資訊科技有限公司					▼	▼																		
果核數位股份有限公司					★	★▲	★▲	★▲	★▲	★▲	★▲			★					★					
阿逸多資訊有限公司	*		*																					
思邦科技股份有限公司																★								
恆逸教育訓練中心																				◇	◇	◇	◎	
美思科法顧問股份有限公司	*		*				★	★	★	★	★													
飛泓科技股份有限公司																	★							
飛象資訊股份有限公司					★▼	▼																		

＊以上為參考名單，最新廠商名單請依各官網為準。

參考資訊安全服務／產品廠商（以筆劃及中文優先排序）	管理面				技術面															認知與訓練面				
					安全性檢測		資通安全健診					資通安全弱點通報機制	端點偵測及應變機制	資通安全防護						資通安全教育訓練			專業證照及職能訓練證書	
	資訊安全管理系統導入	資訊安全管理系統第三方驗證	內部資通安全稽核	業務持續運作演練	弱點掃描	滲透測試	網路架構檢視	網路惡意活動檢視	使用者端電腦惡意活動檢視	伺服器主機惡意活動檢視	目錄伺服器設定及防火牆連線設定檢視			防毒軟體	網路防火牆	電子郵件過濾機制	入侵偵測及防禦機制	應用程式防火牆	進階持續性威脅攻擊防禦	資通安全專職（責）人員	資通安全專職（責）人員以外之資訊人員	一般使用者與主管	資通安全專業證照	資通安全職能評量證書
香港商英國標準協會太平洋有限公司	★*	★※	*																	◇	◇	★◇	◎	
香港商漢德技術監督服務亞太有限公司台灣分公司	★	★※																					◎	
凌羣電腦股份有限公司					★▲	★▲	▲▼	▲▼	▲▼	▲▼	▲▼					★	▲					▼		
桓基科技股份有限公司															★	★▲		▲						
殷諾科技股份有限公司																	▲							
泰鋒電腦股份有限公司					★												★							
神通資訊科技股份有限公司					★																			
荃豐科技有限公司	*		*																					
財團法人工業技術研究院						▼														◇	◇	◇		
財團法人中華民國國家資訊基本建設產業發展協進會	*		*																					
財團法人資訊工業策進會																				◇	◇	◇	◎	
偉立資訊有限公司	*		*																					
健行科技大學																				■◇	■◇	■◇		■
動力安全資訊股份有限公司					★	★	★▼	★▼	★▼	★▼	★▼						★							
崑山科技大學																				■◇	■◇	■◇		■
捷睿智能股份有限公司																	★							
眾至資訊股份有限公司														★	★	★	★	★						
統智科技股份有限公司					★																			
逢甲大學																				■◇	■◇	■◇		■
頂峰資訊有限公司	*		*		▲	▲	▲	▲	▲	▲	▲													
創泓科技股份有限公司													▲											
創逸科技服務有限公司	★*		★*	*	★	★										★								
創穩資云股份有限公司	★		★		★	★	★▲	★▲	★▲	★▲	★▲		▲				★					★		
博威資訊有限公司																	▲							
博創資訊科技	*		*	*																				
博鉅資訊股份有限公司																	▲							
敦陽科技股份有限公司	*		*																					
智慧光資訊服務股份有限公司	*		*																					
朝陽科技大學																				■◇	■◇	■◇		■
登豐數位科技股份有限公司	*		*																					
竣盟科技股份有限公司					★																			
策略數位服務有限公司	★*		★*		★▲	★	▼	▼	▼	▼	▼													
華苓科技股份有限公司							★	★	★	★	★						★							
華電聯網股份有限公司	*		*		★▼	★▼	★▼	★▼	★▼	★▼	★▼							▲	★					
華碩雲端股份有限公司																			★					
華緯資訊企業社（獨資）	*		*																					
逸凡科技股份有限公司					★																			
鈊安資訊科技股份有限公司					★																			
雲勝雲端科技有限公司					★	★																		
勤紘科技股份有限公司															★▲			▲						
勤業眾信聯合會計師事務所	★*		★*	*⊕	★	★	★	★	★	★	★			★			★		★			★		
奧義智慧科技股份有限公司																			▲▼					
新加坡商網達先進科技（台灣分公司）					★	★											★▲		★			★		
瑞思資訊股份有限公司																								
經濟部																				◇	◇	◇	◆	

＊以上為參考名單，最新廠商名單請依各官網為準。

參考資訊安全服務／產品廠商（以筆劃及中文優先排序）	管理面				技術面															認知與訓練面				
					安全性檢測		資通安全健診					資通安全弱點通報機制	端點偵測及應變機制	資通安全防護						資通安全教育訓練			專業證照及職能訓練證書	
	資訊安全管理系統導入	資訊安全管理系統第三方驗證	內部資通安全稽核	業務持續運作演練	弱點掃描	滲透測試	網路架構檢視	網路惡意活動檢視	使用者端電腦惡意活動檢視	伺服器主機惡意活動檢視	目錄伺服器設定及防火牆連線設定檢視			防毒軟體	網路防火牆	電子郵件過濾機制	入侵偵測及防禦機制	應用程式防火牆	進階持續性威脅攻擊防禦	資通安全專職（責）人員	資通安全專職（責）人員以外之資訊人員	一般使用者與主管	資通安全專業證照	資通安全職能評量證書
補夢網數位科技有限公司																								
詮睿科技股份有限公司					★▼	★▼	▼	▼	▼	▼	▼													
誠雲科技股份有限公司							★	★	★	★	★													
資拓宏宇國際股份有限公司	★*		★*		★																	★		
資通電腦股份有限公司					★	★								★								★		
資誠聯合會計師事務所	★*		★*		★	★																★		
達煬科技股份有限公司																								
漢昕科技股份有限公司	★*		★*		★▲	★▲	★▲	★▲	★▲	★▲	★▲				▲	★		▲				★		
睿明知通股份有限公司																								
碩遠科技股份有限公司					★																			
精品科技股份有限公司																								
精誠科技整合股份有限公司	*		*		★▼	★▼																		
精誠軟體服務股份有限公司																			▲			★▼		
精誠資訊股份有限公司							▼	▼	▼	▼	▼			★		★	▲							
綠界科技股份有限公司					★	★																		
網擎資訊軟體股份有限公司														★		▲			▲					
臺北醫學大學																				■◇	■◇	■◇		■
豪勉科技股份有限公司					★		★	★	★	★	★			★	★		★▲	★	▲					
領導力企業管理顧問有限公司	★		★				★	★	★	★	★													
德欣寰宇科技股份有限公司	★*		★*	*	★▲	★▲	★▲	★▲	★▲	★▲	★▲			★	▲	★	★	▲	★			★		
德諾科技服務股份有限公司	★*		★*	*																		★		
數聯資安股份有限公司	★		★	*		★▲▼	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼			★	▲	★	★▲	▲	★▲					
緯育股份有限公司																								
叡揚資訊股份有限公司					★																	★		
璞方科技管理顧問股份有限公司	*		*																					
盧氪賽忒股份有限公司					★▼	★▼																★▼		
興創知能股份有限公司	*		*																					
諦錦有限公司	*		*																					
靜宜大學推廣教育處																				◇	◇	◇		
優士國際聯合顧問有限公司	*		*																					
優易資訊股份有限公司					▲	▲	▲	▲	▲	▲	▲				▲			▲						
優倍司股份有限公司																								
戴夫寇爾股份有限公司					★	★▼																★▼		
環奧國際驗證有限公司		※																						
環奧國際驗證有限公司	*		*																					
聯合報股份有限公司	*		*																					
聯成電腦有限公司																								
聯準科技服務有限公司	★*		★*	*		★	★	★	★	★	★											★		
賽博韓特科技有限公司	★*		★*	*	★▲	★																		
趨勢科技股份有限公司														★▲	★	★	★	★	▲					
鴻寬科技有限公司																	★		★					
曜祥網技股份有限公司																								
曜揚科股份有限公司																★								
鎧睿全球科技股份有限公司																★			▼			▼		
鎰威科技有限公司					★																			
關貿網路股份有限公司	★		★		★*▲	★▲	★▲▼	★▲▼	★▲▼	★▲▼	★▲▼			★	▲★			▲	★▲			★		
關鍵智慧科技有限公司					▲	★▲																★		

＊以上為參考名單，最新廠商名單請依各官網為準。

參考資訊安全服務 / 產品廠商 (以筆劃及中文優先排序)	管理面				技術面															認知與訓練面				
	資訊安全管理系統導入	資訊安全管理系統第三方驗證	內部資通安全稽核	業務持續運作演練	安全性檢測		資通安全健診					資通安全弱點通報機制	端點偵測及應變機制	資通安全防護						資通安全教育訓練			專業證照及職能訓練證書	
					弱點掃描	滲透測試	網路架構檢視	網路惡意活動檢視	使用者端電腦惡意活動檢視	伺服器主機惡意活動檢視	目錄伺服器設定及防火牆連線設定檢視			防毒軟體	網路防火牆	電子郵件過濾機制	入侵偵測及防禦機制	應用程式防火牆	進階持續性威脅攻擊防禦	資通安全專職(責)人員	資通安全專職(責)人員以外之資訊人員	一般使用者與主管	資通安全專業證照	資通安全職能評量證書
鑒真數位有限公司																						★▼		
(ISC)2																							◆	
ACSI													▲											
Barracuda															▲	▲		▲						
Bitdefender													▲			▲								
Cellopoint																			▲					
Check Point													▲		▲				▲					
Cisco															▲								◆	
COMODO													▲		▲	▲								
CompTIA																							◆	
CounterTack													▲											
CREST																							◆	
CrowdStrike													▲											
CyCarrier													▲											
Cylance													▲											
EC-Council																							◆	
F5 Networks															▲									
Fidelis Cybersecurity																			▲					
Fidelis Network																			▲					
Fidelis-Cybersecurity													▲											
FireEye													▲						▲					
Forcepoint													▲		▲	▲								
Fortinet													▲		▲									
GIAC																							◆	
IMPERVA															▲			▲						
Infoblox															▲									
ISA																							◆	
ISACA																							◆	
ISFCE																							◆	
Juniper															▲									
Kaspersky													▲											
Lastline																			▲					
LogRhythm													▲											
Malwarebytes													▲											
McAfee													▲						▲					
Microsoft													▲											
NOPAN Themis																▲								
Offensive Security																							◆	
PaloAltoNetworks													▲											
Radware															▲									
ReaQta													▲											
SentinelOne													▲											
Sophos													▲	▲	▲				▲					
TeamT5													▲											
TREND													▲											
VMware													▲											
WAF															▲									
WatchGuard															▲									

＊以上為參考名單，最新廠商名單請依各官網為準。

附　錄

附錄

附錄 1.《資通安全管理法》推動參考指引

為了達成安全可信賴的數位國家、健全臺灣資通安全產業創新生態系之願景，經濟部工業局設置「跨域資安強化產業推動計畫 ACW 平台」(www.acw.org.tw)，藉以打造指標資安測試場域，強化網通、物聯網等優勢產業資安能量、發展具備臺灣特色之資安產業核心能量，協助建構跨域資安示範解決方案、以及完備國內資安產業環境，培育專業人才、鏈結國際市場。

在 ACW 平台上備有標準驗證、實測場域、產業服務、新創與國際交流等項目可供瀏覽，適用機關更可透過「技術專欄」、「培訓資訊」、「通過驗證之產品資訊」、「能量登錄 / 自主產品」及「資安檢測診斷服務」等子項獲取《資通安全管理法》推動新知、查找通過驗證產品資訊等。

附錄 2.《資通安全管理法》採購指引懶人包諮詢窗口

若對於本份《資通安全管理法》採購指引懶人包有任何建議或問題需要諮詢，歡迎聯繫「跨域資安強化產業推動計畫」窗口：

窗口電話：02-25159665
電子郵件信箱：shuyutsai@itri.org.tw
服務時間：週一至週五上午 10:00 至下午 5:00

附錄 3.《資通安全管理法》採購指引懶人包相關連結網站

行政院資通安全處
www.ey.gov.tw

行政院國家資通安全會報
nicst.ey.gov.tw

行政院國家資通安全會報
技術服務中心
www.nccst.nat.gov.tw

e 等公務園+學習平臺
elearn.hrd.gov.tw

行政院人事行政總處公務人力
發展學院 www.hrd.gov.tw

經濟部工業局
www.moeaidb.gov.tw

跨域資安強化產業推動計畫
www.acw.org.tw

資安整合服務平台
secpaas.org.tw

資安治理成熟度評審系統
isg.nccst.nat.gov.tw

財團法人全國認證基金會
www.taftw.org.tw

政府採購網
web.pcc.gov.tw

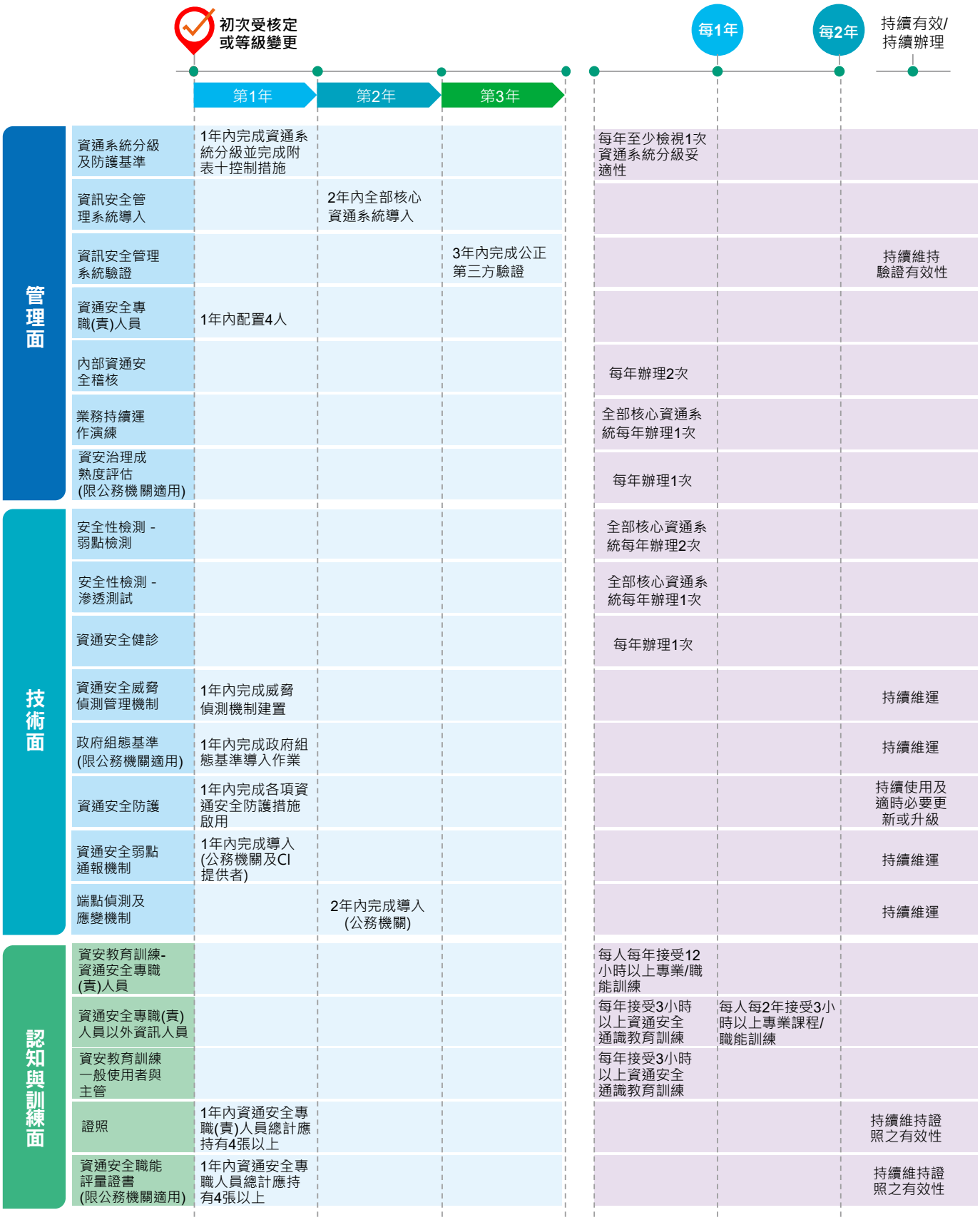
資安人才培訓服務網
ctts.nccst.nat.gov.tw

財團法人工業技術研究院
www.itri.org.tw

中華民國資訊軟體協會
www.cisanet.org.tw

附錄 4.《資通安全管理法》應辦事項實作時程參考

依據《資通安全管理法》子法《資通安全責任等級分級辦法》制定 A 級機關應辦事項，各項應辦事項實作時程彙整如下，供各適用機關參閱。



指導單位｜行政院資通安全處

主辦單位｜經濟部工業局

受委託單位｜財團法人工業技術研究院

執行單位｜中華民國資訊軟體協會