《資通安全管理法》採購指引懶人包

C 級

▶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
財團法人電信技術中心

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改革， 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財團法人電信技術中心提供《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

機關電話｜886-0800-000-256

機關地址｜10651 台北市大安區信義路三段 41-3 號

發刊日期｜108.08.07

編輯單位｜財團法人工業技術研究院
財團法人電信技術中心

單位電話｜886-2-2737-7300
886-2-8953-5600

單位地址｜10651 台北市大安區和平東路二段 106 號
22063 新北市板橋區遠東路 1 號 3 樓 B 室

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：新興資安產業生態系推動計畫網站>產業服務>資通安全法懶人包
- QRCode 下載：

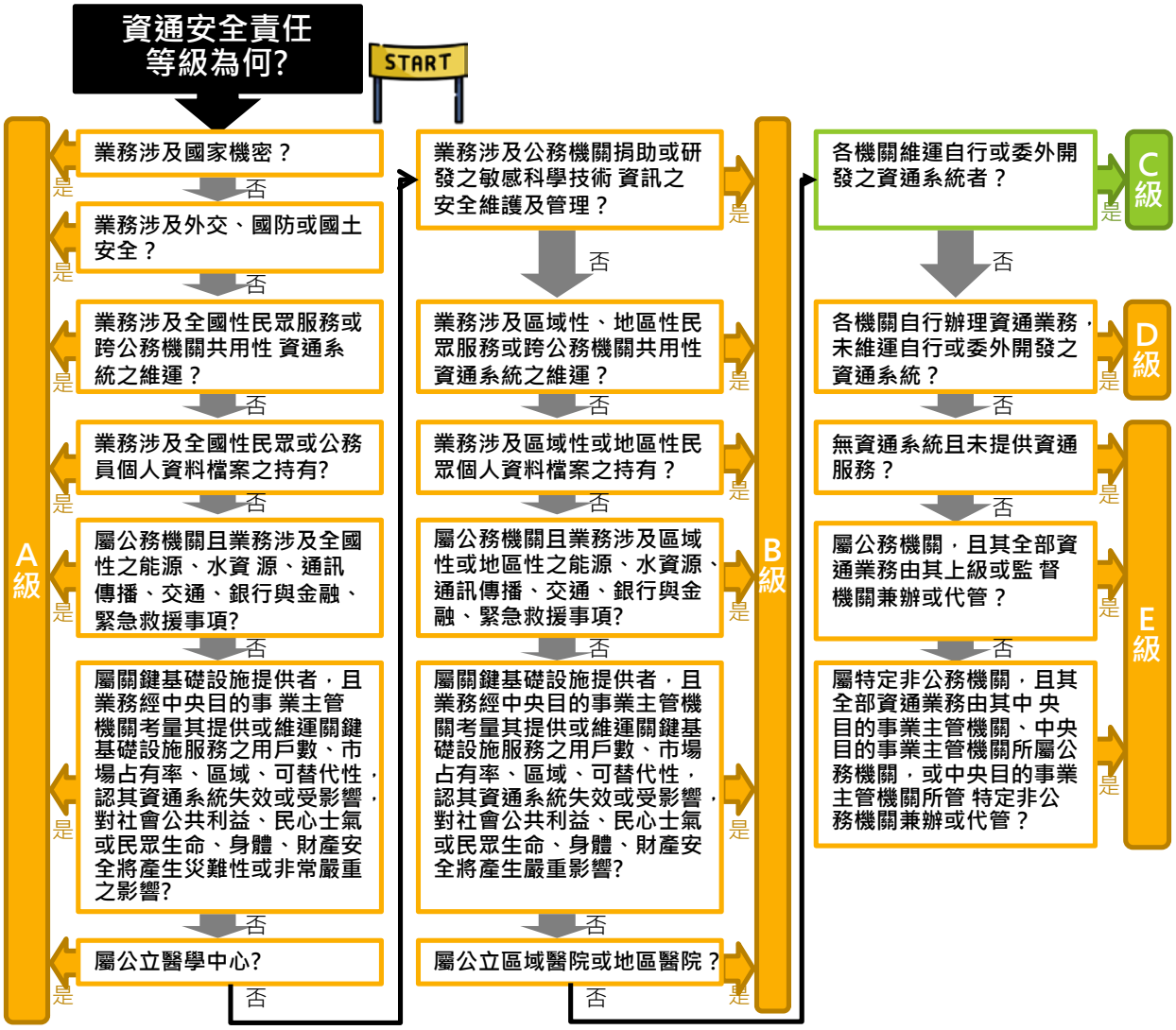
第 1 章

《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 資通安全責任等級：首先須要判定貴單位之資通安全責任等級。



資通安全責任等級範例：

等級	範例
A 級	公立醫學中心
B 級	區域醫院或地區醫院

小提醒

- 資通安全責任等級判定以最高級為主：各機關依「資通安全責任等級分級辦法」第 4 條至 8 條規定，符合二個以上之資通安全責任等級者，其資通安全責任等級列為其符合之最高等級。
- 資通安全責任等級例外調整：依「資通安全責任等級分級辦法」第 10 條規定，得考量{業務中斷、業務資訊、功能失效、其他與資通系統關聯}對國家、社會公共利益、人民生命、身體、財產安全或聲譽影響程度，調整各機關之資通安全責任等級。

Step 2 資通安全責任等級應辦事項：再依您的責任等級一步一步完成應辦事項，及查閱《資通安全管理法》採購指引細部資訊：

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。

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」制定 C 級機關應辦事項如下：

制度面向	辦理項目	辦理項目細項	C 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一 1 年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視 1 次資通系統分級妥適性。 ● 系統等級為「高」者，應於初次受核定或等級變更後之 2 年內完成附表十之控制措施。
	資訊安全管理系統導入		● 初次受核定或等級變更後 2 年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、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。 ● 並持續維持導入
	資通安全專責人員		● 初次受核定或等級變更後之 1 年內配置 1 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 2 年辦理 1 次。
	業務持續運作演練		全部核心資通系統每 2 年辦理 1 次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每 2 年辦理 1 次。
		系統滲透測試	全部核心資通系統每 2 年辦理 1 次。
	資通安全健診	網路架構檢視	每 2 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。 ● 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	
認知訓練面	資通安全教育訓練	資通安全及資訊人員	每年至少 1 名人員各接受 12 小時以上資通安全專業課程訓練或資通安全職能訓練。
		一般使用者與主管	每人每年接受 3 小時以上之一般資通安全教育訓練。
	資通安全專業證照及職能訓練證書	資通安全專業證照	● 初次受核定或等級變更後 1 年內資通安全專責人員總計應持有 1 張以上。 ● 持續維持證照之有效性。
		資通安全職能評量證書(限公務機關適用)	● 初次受核定或等級變更後 1 年內資通安全專職人員總計應持有 1 張以上。 ● 持續維持證書之有效性。

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《資通安全管理法》子法「資通安全責任等級分級辦法」制定 C 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 相關資安專業證照。 ● 建議具有相當 ISO 27001 輔導導入顧問年資。
	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 內部資通安全稽核年資。
	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	網站安全弱點檢測	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 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。
		系統滲透測試	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。 ● 掃描工具需取得授權使用的商用軟體。
	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。
		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 他類似相關課程訓練。 ● 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。

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
		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(Certified Ethical Hacker)、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(Certified Ethical Hacker)、CHFI (Computer Hacking Forensic Investigation)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(Certified Information Systems Security Professional)、ISO/CNS 27001 LA 或其他類似相關課程訓練。
	資通安全防護	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。
		防毒軟體	● 建議使用資安測試機構 AV-Test 最近一年測試結果，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 最近一年測試結果， Malware Protection Tests 取得 Advanced+（三星）等級之軟體。
		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。
認知訓練面	資通安全教育訓練	資通安全及資訊人員 一般使用者與主管	● 建議訓練機構為登記有案之社、財團法人；公私立大專以上院校；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（依據「資通安全責任等級分級辦法」要求）。 ● 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	通過行政院國家資通安全會報技術服務中心公告資安職能訓練機構遴選資格且通過認證所核發證書在效期內。

小提醒

- 相關管理面、技術面及認知訓練面之勞務採購，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 2 章

《資通安全管理法》採購指引懶人包

《資通安全管理法》採購指引懶人包

管理面

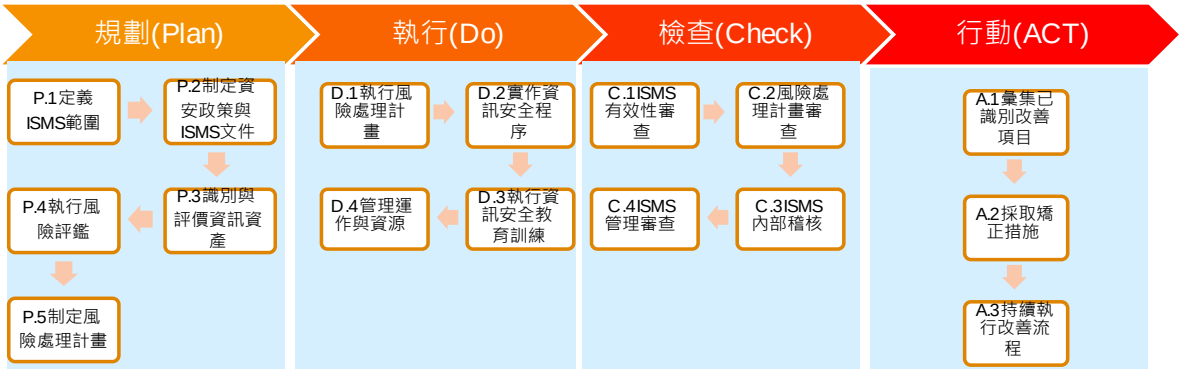
資訊安全管理是全面性工作，主要目標在降低風險與提高管理效率，為確保《資通安全管理法》適用機關針對核心系統進行資安控管及維護，《資通安全管理法》子法特別針對管理面規定應辦理項目。針對「資通安全責任等級分級辦法」之管理面「資訊安全管理系統之導入與驗證」、「內部資通安全稽核」及「業務持續運作演練」議題進行資安控管實務研析，提出建立及執行管理面辦理項目應有之基本原則及建議性作法等，作為《資通安全管理法》各適用機關規劃及執行管理面之參考。

2. 《資通安全管理法》採購指引懶人包

2.1 管理面

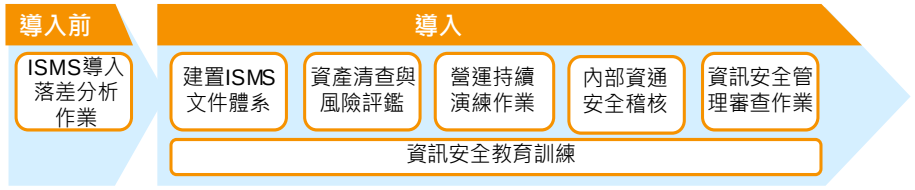
2.1.1 資訊安全管理系統導入

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

組織可尋求外部專業資訊安全服務資源，透過吸取資訊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 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」供參。

3. 資訊安全管理系統導入參考資訊安全服務廠商名單

資訊安全管理系統導入參考資訊安全顧問廠商名單如下：

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	✓	–
中華電信股份有限公司	–	✓
台灣應用軟件股份有限公司	–	✓
安侯企業管理股份有限公司	–	✓
安碁資訊股份有限公司	✓	✓
昇達價值管理股份有限公司	–	✓
美思科法顧問股份有限公司	–	✓
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	–	✓
創逸科技服務有限公司	✓	✓

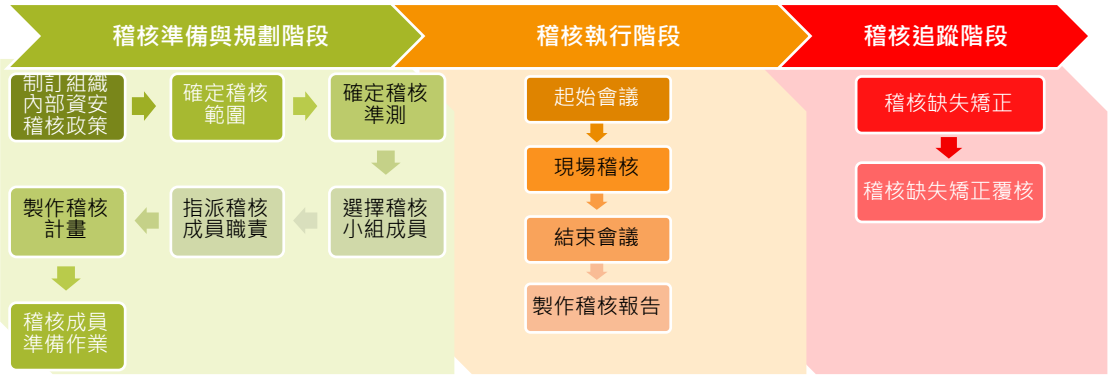
廠商名稱(以筆劃排序)	廠商具備資格來源	
	資安服務機構能量登錄	政府採購網決標
博創資訊科技股份有限公司	–	✓
勤業眾信聯合會計師事務所	✓	✓
資拓宏宇國際股份有限公司	–	✓
資誠聯合會計師事務所	–	✓
漢昕科技股份有限公司	–	✓
精誠科技整合股份有限公司	–	✓
德欣寰宇科技股份有限公司	–	✓
德諾科技服務股份有限公司	✓	✓
數聯資訊安全股份有限公司	✓	✓
璞方科技管理顧問股份有限公司	–	✓
聯準科技服務有限公司	–	✓

※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 107 與 108 年合格廠商。政府採購網(web.pcc.gov.tw)決標紀錄以 105 ~ 107 年資訊安全管理系統導入決標紀錄。

2.1.2 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

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，亦可透過外部專業資訊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：

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擬適切稽核發現改善建議方案與實作稽核發現改善覆核作業。

3. 內部資通安全稽核參考資訊安全服務廠商名單

內部資通安全稽核參考資訊安全服務廠商名單如下：

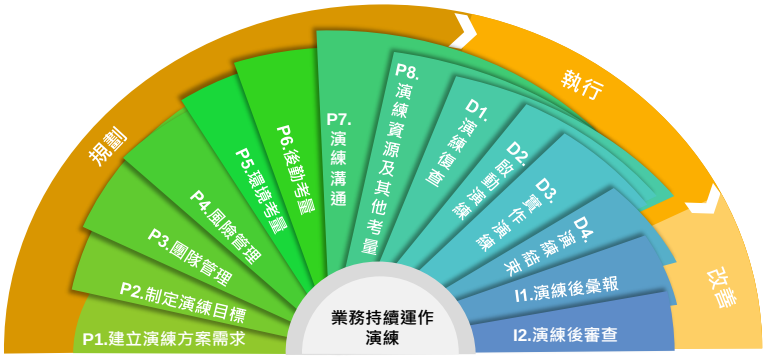
廠商名稱(以筆劃排序)	廠商具備資格來源	
	資安服務機構能量登錄	政府採購網決標
三甲科技股份有限公司	✓	–
中華電信股份有限公司	–	✓
台灣應用軟件股份有限公司	–	✓
安侯企業管理股份有限公司	–	✓
安碁資訊股份有限公司	✓	✓
昇達價值管理股份有限公司	–	✓
美思科法顧問股份有限公司	–	✓
財團法人中華民國國家資訊基本建設產業發展協進會	–	✓
偉立資訊有限公司	–	✓
創逸科技服務有限公司	✓	✓
博創資訊科技股份有限公司	–	✓
勤業眾信聯合會計師事務所	✓	✓
資拓宏宇國際股份有限公司	–	✓
資誠聯合會計師事務所	–	✓
漢昕科技股份有限公司	–	✓
精誠科技整合股份有限公司	–	✓
德欣寰宇科技股份有限公司	–	✓
德諾科技服務股份有限公司	✓	✓
數聯資訊安全股份有限公司	✓	✓
璞方科技管理顧問股份有限公司	–	✓
聯準科技服務有限公司	–	✓

※備註：廠商未列入廠商名單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 107 與 108 年合格廠商。政府採購網(web.pcc.gov.tw)決標紀錄以 105 ~ 107 年資訊安全管理系統導入決標紀錄。

2.1.3 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》規範作為不同規模或類型組織作為業務持續運作演練之良好實務手冊，並且執行和測試營運持續計畫(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」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

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，可透過外部專業資訊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作為後續內部人員自行維護基礎之奠定。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資訊安全服務廠商名單

透過政府採購網與從「資訊安全管理系統導入參考資訊安全服務廠商名單」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資訊安全服務廠商名單：

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	–	✓
安碁資訊股份有限公司	✓	✓
社團法人中華民國青年創業協會總會	✓	✓
財團法人安全衛生技術中心	✓	✓
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	✓	✓
精誠科技整合股份有限公司	–	✓
德欣寰宇科技股份有限公司	–	✓
德諾科技服務股份有限公司	–	✓

※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 ~ 107 年業務持續運作服務決標紀錄。

《資通安全管理法》採購指引懶人包

技術面

資訊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訊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訊安全技術趨勢，才能在規劃與執行資訊安全風險管理時，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「安全性檢測」、「資通安全健診」及「資通安全防護」議題進行資訊安全控管實務研析，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。

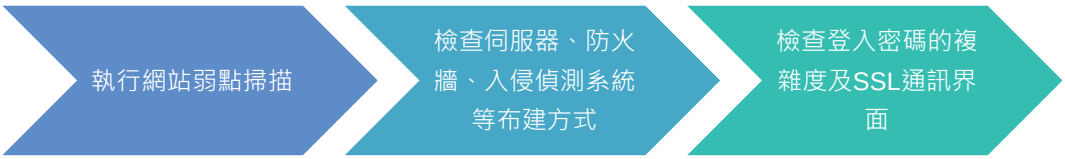
2.2 技術面

2.2.1 安全性檢測

2.2.1.1 網站安全弱點檢測

1. 網站安全弱點檢測參考實作方式

網站安全弱點檢測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. 網站安全弱點檢測參考採購需求項目

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，透過吸取資訊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中風險，參考採購需求項目如下：

服務項目	採購需求項目
網站安全弱點掃描服務	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. 進行網站掃瞄後，應提供弱點掃瞄結果及修補建議。 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 行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」供參。

3. 網站安全弱點檢測參考資訊安全廠商名單

網站安全弱點檢測參考資訊安全廠商名單如下：

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	✓	—	—
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數據通信分公司	—	✓	—
光盾資訊科技有限公司	—	✓	—
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	—	✓	—
飛象資訊股份有限公司	—	—	✓
凌群電腦股份有限公司	—	✓	—
創逸科技服務有限公司	✓	—	—
策略數位服務有限公司	—	✓	—
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	—	—	✓
漢昕科技股份有限公司	—	✓	—
精誠資訊股份有限公司	—	—	✓
數聯資安股份有限公司	—	✓	—
盧氪實忒股份有限公司	—	—	✓
優易資訊股份有限公司	—	✓	—

※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 107 與 108 年合格廠商。政府共同供應契約(web.pcc.gov.tw) 標案案號 1070205 且契約終止日期為 108/10/02。資安整合服務平台(secpaas.org.tw)廠商查詢截止日為 108/08/02。

2.2.1.2 系統滲透測試

1. 系統滲透測試參考實作方式

系統滲透測試建議實作流程如下所示：

2. 系統滲透測試參考採購需求項目

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，透過吸取資訊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中風險，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. 進行系統滲透測試後，應提供滲透測試結果及修補建議。 5. 被滲透之後相關漏洞修補的複測，以確認無相關弱點風險存在。

小提醒 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」供參。

3. 系統滲透測試參考資訊安全廠商名單

系統滲透測試參考資訊安全廠商名單如下：

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	✓	–	–
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數據通信分公司	–	✓	–
互聯安睿資通股份有限公司	–	–	✓
光盾資訊科技有限公司	–	✓	–
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	–	✓	–
凌群電腦股份有限公司	–	✓	–
策略數位服務有限公司	–	✓	–
華電聯網股份有限公司	✓	–	–
勤業眾信聯合會計師事務所	✓	–	–
詮睿科技股份有限公司	–	–	✓
漢昕科技股份有限公司	–	✓	–
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	–	–	✓
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 107 與 108 年合格廠商。政府共同供應契約(web.pcc.gov.tw) 標案案號 1070205 且契約終止日期為 108/10/02。資安整合服務平台(secpaas.org.tw)廠商查詢截止日為 108/08/02。

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

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，透過吸取資訊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中風險，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 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」供參。

3. 網路架構檢視參考資訊安全廠商名單

網路架構檢視參考資訊安全廠商名單如下：

廠商名稱(以筆劃排序)	廠商具備資格來源		
	ACW 資安檢測團隊	政府共同供應契約	資安整合服務平台廠商
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數據通信分公司	—	✓	—
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	—	✓	—
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	—	✓	—
策略數位服務有限公司	—	✓	—
華電聯網股份有限公司	✓	—	—
詮睿科技股份有限公司	—	—	✓
漢昕科技股份有限公司	✓	✓	—
精誠資訊股份有限公司	—	—	✓
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。ACW 資安檢測團隊(www.acw.org.tw)為 107 與 108 年資安檢測診斷服務團隊。政府共同供應契約(web.pcc.gov.tw) 標案案號 1070205 且契約終止日期為 108/10/02。資安整合服務平台(secpaas.org.tw)廠商查詢截止日為 108/08/02。

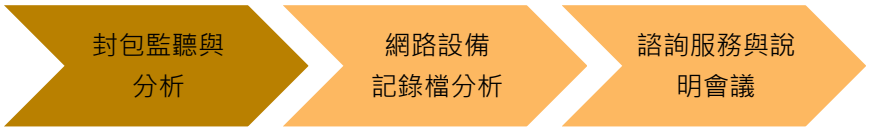
2.2.2.2 網路惡意活動檢視

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

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，透過吸取資訊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中風險，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 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」供參。

3. 網路惡意活動檢視參考資訊安全廠商名單

網路惡意活動檢視參考資訊安全廠商名單如下：

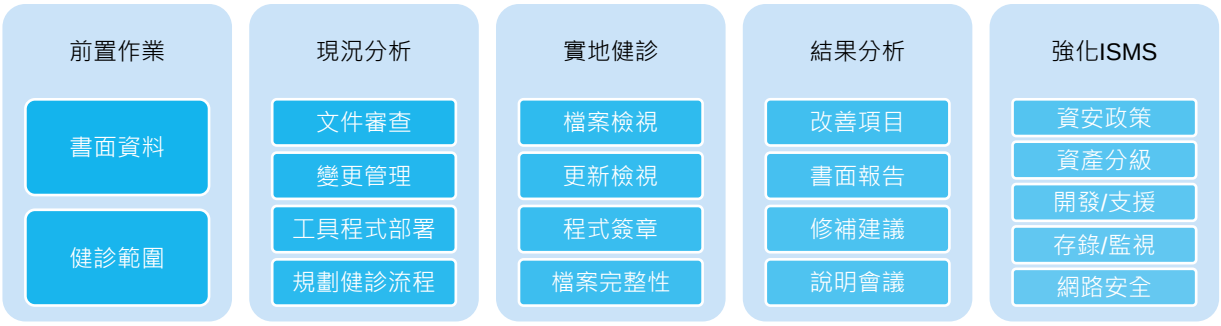
廠商名稱(以筆劃排序)	廠商具備資格來源		
	ACW 資安檢測團隊	政府共同供應契約	資安整合服務平台廠商
中芯數據股份有限公司	—	✓	—
中華資安國際股份有限公司	—	✓	—
中華電信股份有限公司數據通信分公司	—	✓	—
永豐技服科技有限公司	✓	—	—
光盾資訊科技有限公司	—	✓	—
安侯企業管理股份有限公司	✓	—	—
安華聯網科技股份有限公司	✓	—	—
安碁資訊股份有限公司	—	✓	—
果核數位股份有限公司	✓	✓	—
美思科法顧問股份有限公司	✓	—	—
凌群電腦股份有限公司	—	✓	—
策略數位服務有限公司	—	✓	—
華電聯網股份有限公司	✓	—	—
詮睿科技股份有限公司	—	—	✓
漢昕科技股份有限公司	✓	✓	—
精誠資訊股份有限公司	—	—	✓
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。ACW 資安檢測團隊(www.acw.org.tw)為 107 與 108 年資安檢測診斷服務團隊。政府共同供應契約(web.pcc.gov.tw) 標案案號 1070205 且契約終止日期為 108/10/02。資安整合服務平台(secpaas.org.tw)廠商查詢截止日為 108/08/02。

2.2.2.3 使用者端電腦惡意活動檢視

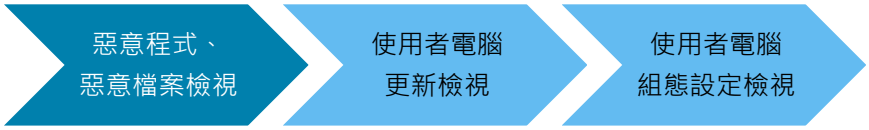
1. 使用者端電腦惡意活動檢視參考實作方式

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

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，透過吸取資訊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中風險，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 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」供參。

3. 使用者端電腦惡意活動檢視參考資訊安全廠商名單

使用者端電腦惡意活動檢視參考資訊安全廠商名單如下：

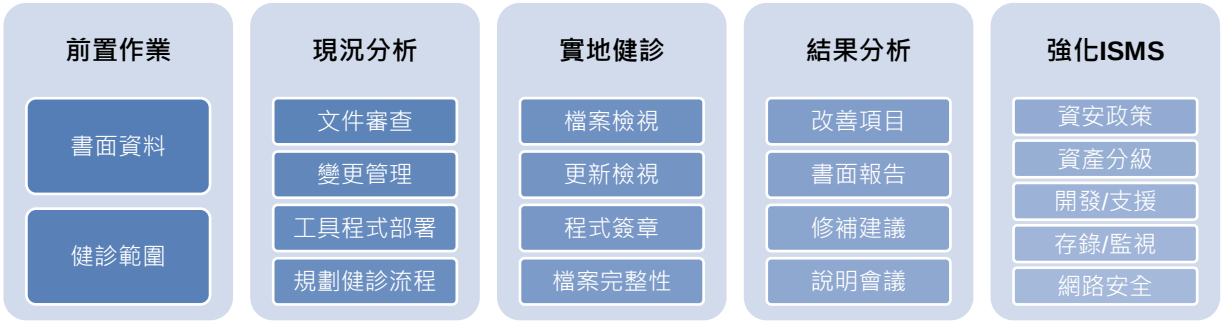
廠商名稱(以筆劃排序)	廠商具備資格來源		
	ACW 資安檢測團隊	政府共同供應契約	資安整合服務平台廠商
中芯數據股份有限公司	—	✓	—
中華資安國際股份有限公司	—	✓	—
中華電信股份有限公司數據通信分公司	—	✓	—
永豐技服科技有限公司	✓	—	—
光盾資訊科技有限公司	—	✓	—
安侯企業管理股份有限公司	✓	—	—
安華聯網科技股份有限公司	✓	—	—
安碁資訊股份有限公司	—	✓	—
果核數位股份有限公司	✓	✓	—
美思科法顧問股份有限公司	✓	—	—
凌群電腦股份有限公司	—	✓	—
策略數位服務有限公司	—	✓	—
華電聯網股份有限公司	✓	—	—
詮睿科技股份有限公司	—	—	✓
漢昕科技股份有限公司	✓	✓	—
精誠資訊股份有限公司	—	—	✓
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。ACW 資安檢測團隊(www.acw.org.tw)為 107 與 108 年資安檢測診斷服務團隊。政府共同供應契約(web.pcc.gov.tw) 標案案號 1070205 且契約終止日期為 108/10/02。資安整合服務平台(secpaas.org.tw)廠商查詢截止日為 108/08/02。

2.2.2.4 伺服器主機惡意活動檢視

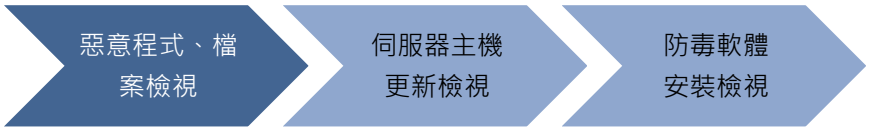
1. 伺服器主機惡意活動檢視參考實作方式

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

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，透過吸取資訊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中風險，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 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」供參。

3. 伺服器主機惡意活動檢視參考資訊安全廠商名單

伺服器主機惡意活動檢視參考資訊安全廠商名單如下：

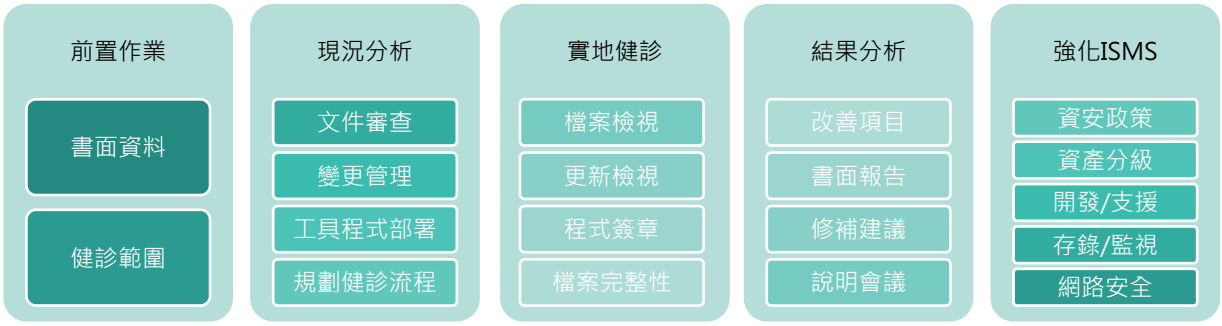
廠商名稱(以筆劃排序)	廠商具備資格來源		
	ACW 資安檢測團隊	政府共同供應契約	資安整合服務平台廠商
中芯數據股份有限公司	—	✓	—
中華資安國際股份有限公司	—	✓	—
中華電信股份有限公司數據通信分公司	—	✓	—
永豐技服科技有限公司	✓	—	—
光盾資訊科技有限公司	—	✓	—
安侯企業管理股份有限公司	✓	—	—
安華聯網科技股份有限公司	✓	—	—
安碁資訊股份有限公司	—	✓	—
果核數位股份有限公司	✓	✓	—
美思科法顧問股份有限公司	✓	—	—
凌群電腦股份有限公司	—	✓	—
策略數位服務有限公司	—	✓	—
華電聯網股份有限公司	✓	—	—
詮睿科技股份有限公司	—	—	✓
漢昕科技股份有限公司	✓	✓	—
精誠資訊股份有限公司	—	—	✓
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。ACW 資安檢測團隊(www.acw.org.tw)為 107 與 108 年資安檢測診斷服務團隊。政府共同供應契約(web.pcc.gov.tw) 標案案號 1070205 且契約終止日期為 108/10/02。資安整合服務平台(secpaas.org.tw)廠商查詢截止日為 108/08/02。

2.2.2.5 目錄伺服器設定及防火牆連線設定檢視

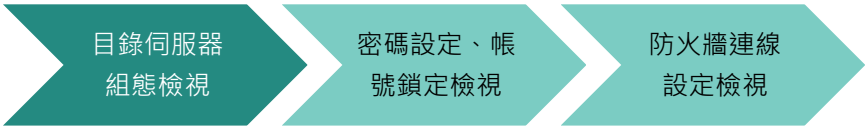
1. 目錄伺服器設定及防火牆連線設定檢視參考實作方式

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

組織本身規劃及足夠預算下可詢求外部專業資訊安全服務資源，透過吸取資訊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中風險，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 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」供參。

3. 目錄伺服器設定及防火牆連線設定檢視參考資訊安全廠商名單

目錄伺服器設定及防火牆連線設定檢視參考資訊安全廠商名單如下：

廠商名稱(以筆劃排序)	廠商具備資格來源		
	ACW 資安檢測團隊	政府共同供應契約	資安整合服務平台廠商
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數據通信分公司	—	✓	—
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	—	✓	—
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	—	✓	—
策略數位服務有限公司	—	✓	—
華電聯網股份有限公司	✓	—	—
詮睿科技股份有限公司	—	—	✓
漢昕科技股份有限公司	✓	✓	—
精誠資訊股份有限公司	—	—	✓
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。ACW 資安檢測團隊(www.acw.org.tw)為 107 與 108 年資安檢測診斷服務團隊。政府共同供應契約(web.pcc.gov.tw) 標案案號 1070205 且契約終止日期為 108/10/02。資安整合服務平台(secpaas.org.tw)廠商查詢截止日為 108/08/02。

2.2.3 資通安全防護

2.2.3.1 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訊安全產業發展，盤點資安業者技術能量，規劃建立資訊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. 網路防火牆參考資訊安全廠商名單

網路防火牆參考資訊安全廠商名單如下：

廠商名稱(以筆劃及中文優先排序)	資安服務機構能量登錄 防火牆產品	政府共同供應契約合格廠商
大同世界科技股份有限公司	✓	–
台灣思科系統股份有限公司	–	✓
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	✓	–
豪勉科技股份有限公司	✓	–
Barracuda	–	✓
Check Point	–	✓
Forcepoint	–	✓
Fortinet	–	✓
Juniper	–	✓
Sophso	–	✓
WatchGuard	–	✓

※備註：廠商未列入廠商名單中不表示其未具提供該項產品之能力。資安服務機構能量登錄(www.acw.org.tw)為 107 與 108 年合格廠商。政府共同供應契約(web.pcc.gov.tw)合格廠商查詢截止日為 108/05/31。

2.2.3.2 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：

產品項目	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. 防毒軟體參考資訊安全廠商名單

防毒軟體參考資訊安全廠商名單如下：

廠商名稱(以筆劃及中文優先排序)	資安服務機構能量登錄 整合病毒與惡意程式防護檢測服務	政府共同供應契約合格廠商 防毒軟體產品
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	–	✓
台灣賽門鐵克股份有限公司	–	✓
台灣邁克菲有限公司	–	✓
安碁資訊股份有限公司	✓	–
勤業眾信聯合會計師事務所	✓	–
資通電腦股份有限公司	✓	–
網擎資訊軟體股份有限公司	✓	–
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	✓	–
Sophos	–	✓

※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 107 與 108 年合格廠商。政府共同供應契約(web.pcc.gov.tw)合格廠商查詢截止日為 108/05/31。

2.2.3.3 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全性，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和訪問以及資源控制等。

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會話，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

電子郵件過濾機制，主要是為了防止機密資料外洩，以及完整保存往來的郵件。採購人員在電子郵件過濾機制建議書徵求文件(RFP)參考採購需求項目如下：

產品項目	採購需求項目
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. 具有郵件記錄備份備援、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資訊安全廠商名單

電子郵件過濾機制參考資訊安全廠商名單如下：

廠商名稱(以筆劃排序)	資安服務機構能量登錄名單		政府共同供應契約合格廠商
	電子郵件安全管理檢測與防護服務	電子郵件防護產品	
中華數位科技股份有限公司	✓	✓	–
安源電腦股份有公司	–	–	✓
安碁資訊股份有限公司	✓	–	–
安資捷股份有限公司	✓	–	–
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	✓	–	–
網擎資訊軟體股份有限公司	–	✓	–
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107 與 108 年合格廠商。政府共同供應契約(web.pcc.gov.tw)合格廠商查詢截止日為 108/05/31。

《資通安全管理法》採購指引懶人包

認知訓練面

資訊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訊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訊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」之認知訓練面「資通安全教育訓練」及「資通安全專業證照及職能訓練證書」議題進行實務研析，提出建立及執行認知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訓練面之參考。

2.3 認知訓練面

2.3.1 資通安全教育訓練

2.3.1.1 資通安全及資訊人員

1. 資通安全及資訊人員資通安全教育訓練參考實作方式

2. 資通安全及資訊人員資通安全教育訓練參考採購需求項目

依據資安作業內涵區分為資通安全人員及資訊人員，其職務能力需求及必選修領域課程建議如下，供採購人員列入建議書徵求文件(RFP)之參考。

人員類別	資通安全人員		資訊人員	
職務能力	基本資安認知	• 資安制度建置能力 • 資安稽核能力 • 資安事件應變處理能力	基本資安認知	• 資訊處理安全技能 • 系統安全防護能力
必修課程	• 電腦作業安全概念 • 資訊安全概論 • 機關資安管理規定 • 個人資料保護概論 • 資通安全相關法律	• 資安通識 • 資訊系統風險管理 • 資安事故處理 • 資通安全管理評鑑 • 個人資料保護管理 • 資安健診 • 業務持續管理	• 電腦作業安全概念 • 資訊安全概論 • 機關資安管理規定 • 個人資料保護概論 • 資通安全相關法律	• 資安通識 • WEB 應用程式安全 • 資訊系統風險管理 • 資通安全管理評鑑 • 雲端服務安全管理 • 資訊作業委外安全 • 網路架構部署安全 • 電子郵件安全 • 電子資料保護 • 資安事故處理 • 行動裝置安全 • 資安健診 • 無線網路安全 • 業務持續管理
選修課程	• 電子郵件安全 • WEB 應用程式安全 • 資訊作業委外安全	• 電子資料保護 • 行動裝置安全	• 業務持續運作管理 • 無線網路安全 • 新興科技資安議題 • 網路弱點評估實務 • 備援技術 • 通訊網路安全 • 入侵偵測與防護 • 防火牆理論與應用 • 作業系統安全管理 • 個人資料保護管理 • 新興科技資安議題	-

資料來源：行政院國家資通安全會報技術服務中心官網

3. 資通安全及資訊人員資通安全教育訓練參考資訊安全廠商名單

資通安全及資訊人員資通安全教育訓練參考資訊安全廠商名單如下：

廠商名稱(以筆劃排序)	資安整合服務平台			技術服務中心遴選通過
	資安服務機構能量登錄	合作研習機構	資安整合服務平台廠商	
二甲科技股份有限公司	✓	–	–	–
中國文化大學推廣教育部	–	–	–	✓
中華民國資訊軟體協會	–	✓	–	–
中華電信學院	–	✓	–	–
中興大學創新產業暨國際學院	–	–	–	✓
元智大學終身教育部	–	–	–	✓
台灣數位安全聯盟	–	✓	–	–
巨匠電腦股份有限公司	–	✓	–	–
安華聯網科技股份有限公司	✓	✓	–	–
協志聯合科技股份有限公司	✓	✓	–	–
社團法人中華民國南部科學園區產學協會	–	✓	–	–
健行科技大學推廣教育中心	–	–	–	✓
昆山科技大學進修推廣處	–	–	–	✓
逢甲大學推廣教育處	–	–	–	✓
朝陽科技大學推廣教育處	–	–	–	✓
勤業眾信聯合會計師事務所	–	✓	–	–
精誠資訊股份有限公司	–	–	✓	
臺灣資訊暨綠色產業發展協會	–	✓	–	–
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	–	✓	–	–
靜宜大學推廣教育處	–	–	–	✓
關貿網路股份有限公司	✓	–	–	–
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。資安服務機構能量登錄(www.acw.org.tw)為 107 與 108 年合格廠商。技術服務中心(www.nccst.nat.gov.tw) 為 107 與 108 年遴選通過資安訓練機構。

2.3.1.2 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

資通安全教育訓練建議實作流程包含四個步驟，依序為需求分析(P)、訓練規劃及執行(D)、成效評估(C)、修正及改善(A)。

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

依據資安作業內涵區亦分為一般使用者與主管，其職務能力需求及必選修領域課程建議如下，供採購人員列入建議書徵求文件(RFP)之參考。

人員類別	一般使用者	主管
職務能力	• 基本資安認知	• 基本資安認知 • 資安管理的決策能力
必修課程	• 電腦作業安全概念 • 資訊安全概論 • 機關資安管理規定 • 個人資料保護概論 • 資通安全相關法律 • 資通安全管理制度	• 電腦作業安全概念 • 資訊安全概論 • 機關資安管理規定 • 個人資料保護概論 • 資通安全相關法律 • 資通安全管理制度
選修課程	• 電子郵件社交工程防護 • 個人資料保護管理	• 政府資訊作業委外安全 • 資安事故處理 • 業務持續運作管理 • 個人資料保護管理 • 新興科技資安議題

資料來源：行政院國家資通安全會報技術服務中心官網

3. 一般使用者與主管資通安全教育訓練參考資訊安全廠商名單

一般使用者與主管資通安全教育訓練參考資訊安全廠商名單如下：

廠商名稱(以筆劃排序)	資安整合服務平台			技術服務中心遴選通過
	資安服務機構能量登錄	合作研習機構	資安整合服務平台廠商	
三甲科技股份有限公司	✓	–	–	–
中國文化大學推廣教育部	–	–	–	✓
中華民國資訊軟體協會	–	✓	–	–
中華電信學院	–	✓	–	–
中興大學創新產業暨國際學院	–	–	–	✓
元智大學終身教育部	–	–	–	✓
台灣數位安全聯盟	–	✓	–	–
巨匠電腦股份有限公司	–	✓	–	–
安華聯網科技股份有限公司	✓	✓	–	–
協志聯合科技股份有限公司	✓	✓	–	–
社團法人中華民國南部科學園區產學協會	–	✓	–	–
健行科技大學推廣教育中心	–	–	–	✓
崑山科技大學進修推廣處	–	–	–	✓
逢甲大學推廣教育處	–	–	–	✓
朝陽科技大學推廣教育處	–	–	–	✓
勤業眾信聯合會計師事務所	–	✓	–	–
精誠資訊股份有限公司	–	–	✓	
臺灣資訊暨綠色產業發展協會	–	✓	–	–
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	–	✓	–	–
靜宜大學推廣教育處	–	–	–	✓
關貿網路股份有限公司	✓	–	–	–
鑒真數位有限公司	✓	–	–	–

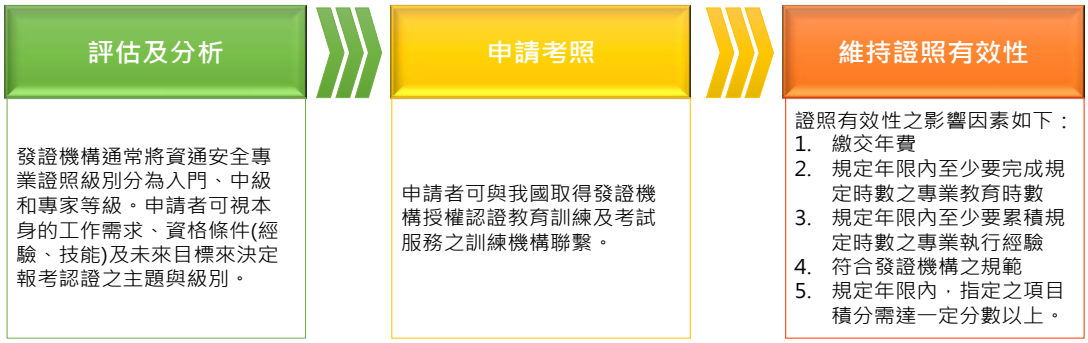
※備註：廠商未列入廠商名單中不表示其未具提供該項服務之能力。資安服務機構能量登錄(www.acw.org.tw)為 107 與 108 年合格廠商。技術服務中心(www.nccst.nat.gov.tw) 為 107 與 108 年遴選通過資安訓練機構。

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：



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：

3. 資通安全專業證照參考資訊安全廠商名單

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：

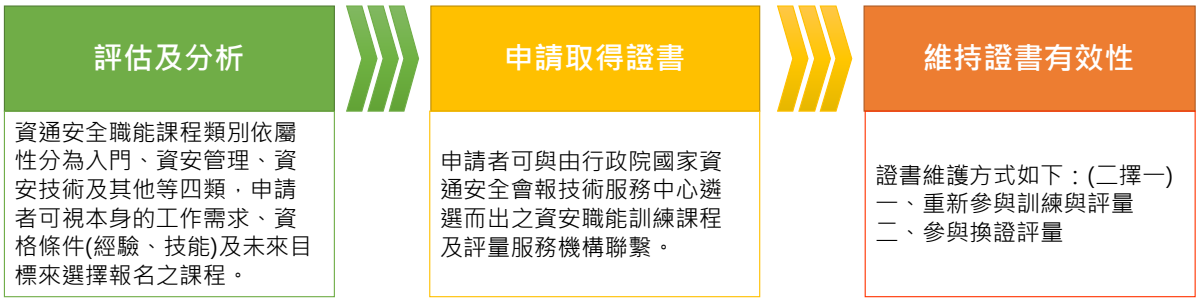
廠商名稱(以筆劃及中文優先排序)	廠商具備資格來源	
	行政院國家資通安全會報公告名單	原廠授權(認證教育訓練/ 考試服務)
中華民國電腦稽核協會	—	✓
中華民國電腦技能基金會	—	✓
巨匠電腦股份有限公司	—	✓
恆逸教育訓練中心	—	✓
財團法人資訊工業策進會	—	✓
(ISC)[2]	✓	—
BSI	—	✓
CompTIA	✓	—
CREST	✓	—
EC-Council	✓	—
Elearning Security	✓	—
GIAC	✓	—
ISACA	✓	—
ISFCE	✓	—
Offensive Security	✓	—
SGS	—	✓

※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(www.nicst.ey.gov.tw)與原廠授權查詢截止日為 108/05/31。

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訊人員、資安人員需根據機關業務所需，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：



2. 資通安全職能評量證書參考採購需求項目

依據行政院國家資通安全會報技術服務中心公告之資通安全職能課程資訊如下，供採購人員列入建議書徵求文件(RFP)之參考。

類別	公務人員資安/資訊人員 (實體課程)	所有公務人員 (數位課程：資安數位課程學習平台(elearn.hrd.gov.tw))		
課程	• 電子郵件安全 • Web 應用程式安全 • 資訊安全通識 • 資安事件處理 • 電子資料暨個資保護管理 • 資訊系統風險管理 • 政府資訊作業委外安全 • 資安健診 • 行動裝置安全 • 雲端服務安全管理	【基本認知類】 • 資訊安全概論 • 資安管理-個人篇 • 資安管理-主管篇 • 個人資料保護法介紹 • ISMS 制度標準介紹 • Windows 安全防護應用 • 涉外人員資安作業實務 • 電子郵件社交工程及防護	【資安管理類】 • 資安風險管理概觀 • 資安風險評鑑實務 • 個人資料保護管理篇 • 資訊安全管理系統政策制定與資訊安全組織建立 • 資訊資產管理 • 存取控制概觀 • 資訊安全稽核介紹與實務 • 個人資料保護_舉證責任與數位鑑識之觀點 • 行動設備安全 • 個人資訊管理系統國際標準介紹-以 BS10012 為例	【資安技術類】 • 網路安全概論 • 防火牆原理、架構及種類介紹 • 防火牆部署與管理 • 密碼學原理與技術 • 無線區域網路安全防護 • 營運持續管理(BCM)概觀 • 應用服務安全實作_Web 應用程式之威脅與防護 • 網路攻擊技術分析 • 弱點掃瞄技術 • 惡意軟體介紹與防治 • 電腦數位鑑識_基礎篇 • APT 目標攻擊因應之道

資料來源：行政院國家資通安全會報技術服務中心官網

3. 資通安全職能評量證書參考資訊安全廠商名單

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
中國文化大學推廣教育部	✓
中興大學創新產業暨國際學院	✓
元智大學終身教育部	✓
健行科技大學推廣教育中心	✓
崑山科技大學進修推廣處	✓
逢甲大學推廣教育處	✓
朝陽科技大學推廣教育處	✓
靜宜大學推廣教育處	✓

※備註：技術服務中心(www.nccst.nat.gov.tw)107~108 年遴選通過資安訓練機構。資安職能課程以天數(3 日或 2 日)及班別(自費班或補助班)做為收費標準，三天課程：自費班為$8,000 元，補助班為 2,000 元；兩天課程：自費班為$6,000 元，補助班為 1,500 元。職能證書有效期間為 3 年，自參與評量測驗當天起算。

第 3 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」制定各等級應辦事項，針對以下研析議題彙整參考資訊安全服務/產品廠商，以供適用等級機關構予以參閱。

★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

▼新興資安產業生態系推動計畫合作研習機構/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

▲政府共同供應契約：刊登於政府電子採購網之共同供應契約

◆行政院國家資通安全會報：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

■技術服務中心：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

◎原廠授權：經原廠授權教育訓練或考試服務之機構

※TAF 認可：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

參考資訊安全服務/產品廠商(以筆劃及中文優先排序)	C 級機關適用議題																參考議題			
	管理面			技術面										認知訓練面				管理面	技術面		
	資訊安全管理系統導入	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		資訊安全管理系統驗證	資通安全防護		
				網站安全弱點檢測	系統滲透測試	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	網路防火牆	防毒軟體	電子郵件過濾機制	資通安全及資訊人員	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		應用程式防火牆	入侵偵測及防禦機制	進階持續性威脅攻擊
三甲科技	★	★		★	★									★	★					★	
大同世界											★										
中芯數據				▲	▲	▲	▲	▲	▲	▲											
中國文化大學														■	■		■				
中華民國資訊軟體協會														▼	▼						
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				★▲	▲	▲	▲	▲	▲	▲		★								★▲	★▲
中華電信	＊	＊																			
中華電信數據通信分公司				▲	▲	▲	▲	▲	▲	▲											
中華電信學院														▼	▼						
中華數位科技												★	★								★▲
中華龍網																					▲
中興大學														■	■		■				
互聯安睿					▼																
元智大學														■	■		■				
台灣卡巴斯基實驗室												▲									

參考資訊安全服務/產品廠商(以筆劃及中文優先排序)	C 級機關適用議題																	參考議題			
	管理面			技術面										認知訓練面				管理面	技術面		
	資訊安全管理系統導入	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		資訊安全管理系統驗證	資通安全防護		
				網站安全弱點檢測	系統滲透測試	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	網路防火牆	防毒軟體	電子郵件過濾機制	資通安全及資訊人員	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		應用程式防火牆	入侵偵測及防禦機制	進階持續性威脅攻擊
台灣思科											▲										
台灣數位安全聯盟														▼	▼						
台灣應用軟件	＊	＊																			
台灣檢驗科技																◎		※			
台灣賽門鐵克												▲							▲		
台灣邁克菲												▲									
巨匠電腦														▼	▼	◎					
永豐技服						▼	▼	▼	▼	▼											
光盾資訊				▲	▲	▲	▲	▲	▲	▲											
安侯企業	＊	＊	⊕			▼	▼	▼	▼	▼											
安華聯網				★	★	▼	▼	▼	▼	▼				★▼	★▼				★		
安源電腦													▲								
安碁資訊	★	★	＊	★▲	★▲	▲	▲	▲	▲	▲		★	★						★▲	★	
安資捷													★						★	★	
艾法諾																		※			
杜浦數位																					▲
協志聯合														★▼	★▼						
昇達價值	＊	＊																			
果核數位				▲	▲	▼▲	▼▲	▼▲	▼▲	▼▲											
社團法人中華民國青年創業協會總會			＊																		
社團法人中華民國南部科學園區產學協會														▼	▼						
恆逸教育訓練中心																◎					
美思科法	＊	＊				▼	▼	▼	▼	▼											
飛象資訊			▼																		
香港商英國標準協會																◎		※			
香港商漢德																		※			
凌群電腦				▲	▲	▲	▲	▲	▲	▲											
桓基科技											★		★						▲		
財團法人中華民國國家資訊基本建設產業發展協進會	＊	＊																			

參考資訊安全服務/產品廠商(以筆劃及中文優先排序)	C 級機關適用議題																	參考議題			
	管理面			技術面										認知訓練面				管理面	技術面		
	資訊安全管理系統導入	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		資訊安全管理系統驗證	資通安全防護		
				網站安全弱點檢測	系統滲透測試	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	網路防火牆	防毒軟體	電子郵件過濾機制	資通安全及資訊人員	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		應用程式防火牆	入侵偵測及防禦機制	進階持續性威脅攻擊
財團法人安全衛生技術中心			✳																		
財團法人資訊工業策進會																◎					
偉立資訊	✳	✳																			
健行科技大學														■	■		■				
崑山科技大學														■	■		■				
眾至資訊											★		★						★		
逢甲大學														■	■		■				
創逸科技	★	★	⊕	★									★								
博創資訊科技	✳	✳	⊕																		
朝陽科技大學														■	■		■				
策略數位				▲	▲	▲	▲	▲	▲	▲											
華電聯網				★	★	▼	▼	▼	▼	▼											
勤紘科技											★									★	
勤業眾信	★	★	✳	★ ▲	★							★		▼	▼					★	★
奧義智慧科技																					▼ ▲
詮睿科技				▼	▼	▼	▼	▼	▼	▼											
資拓宏宇	✳	✳																			
資通電腦												★									
資誠聯合	✳	✳																			
漢昕科技	✳	✳		▲	▲	▼ ▲	▼ ▲	▼ ▲	▼ ▲	▼ ▲											
精誠科技	✳	✳	⊕																		
精誠軟體																					▲
精誠資訊				▼		▼	▼	▼	▼	▼											
網擎資訊												★	★								★
臺灣資訊暨綠色產業發展協會														▼	▼						
豪勉科技											★								★	★ ▲	▲
德欣寰宇	✳	✳	⊕			▼	▼	▼	▼	▼											
德諾科技	★	★	⊕											★	★						
數聯資安	★	★		▲	▲	▲	▲	▲	▲	▲		★	★	★	★				★	★ ▲	★ ▲
緯育股份公司														▼	▼						
璞方科技	✳	✳																			
盧氪賽忒				▼																	

參考資訊安全服務/產品廠商(以筆劃及中文優先排序)	C 級機關適用議題																	參考議題			
	管理面			技術面										認知訓練面				管理面	技術面		
	資訊安全管理系統導入	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		資訊安全管理系統驗證	資通安全防護		
				網站安全弱點檢測	系統滲透測試	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	網路防火牆	防毒軟體	電子郵件過濾機制	資通安全及資訊人員	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		應用程式防火牆	入侵偵測及防禦機制	進階持續性威脅攻擊
靜宜大學														■	■		■				
優易資訊				▲	▲	▲	▲	▲	▲	▲											
戴夫寇爾					▼																
環亞貝爾國際																		※			
環奧國際																		※			
聯準科技	＊	＊				▼	▼	▼	▼	▼											
趨勢科技												★▲	★						★▲	★	★▲
曜揚科技													▲								
鎧睿全球													★								
關貿網路					★▲	▼▲	▼▲	▼▲	▼▲	▼▲		★		★	★						★▲
鑒真數位														★	★						▼
(ISC)2																◆					
Barracuda											▲										
Bluepunkt																			▲		
Cellopoint																					
Check Point											▲										
CompTIA																◆					
CREST																◆					
EC-Council																◆					
Elearning Security																◆					
Forcepoint											▲										
Fortinet											▲										
GIAC																◆					
ISACA																◆					
ISFCE																◆					
Juniper											▲										
Lastline																					
Offensive Security																◆					
Sophos											▲	▲									
WatchGuard											▲										

* 以上為參考名單，最新廠商名單請依各官網為準，謝謝。

*「參考議題」不是 C 級機關適用議題，僅供參閱。

附錄

附錄

附錄 1.《資通安全管理法》推動參考資安專欄

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「新興資安產業生態系推動計畫 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」、「研習資訊」、「通過驗證的產品資訊」、「服務能量登錄機制」及「資安檢測診斷服務」等子項獲取資安管理法推動新知、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「新興資安產業生態系推動計畫」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

行政院國家資通安全會報	新興資安產業生態系推動計畫	資安整合服務平台
(nicst.ey.gov.tw)	(www.acw.org.tw)	(secpaas.org.tw)