經濟部工業局 111 年「跨域資安強化產業推動計畫」
資安檢測診斷服務申請須知

一、目的

經濟部工業局為促進產業資安防護能力提升，推動產業資安檢測診斷服務，透過「企業資安評級」、「主機系統弱點掃描」、「資訊設備組態檢測」、「網路封包側錄分析」、「惡意程式或檔案檢視」及「防火牆連線設定檢視」等檢測項目，協助受測企業掌握組織內部資安防護現況，並了解如何強化、改善缺失及進一步建立預防措施。

二、申請資格

申請受測企業須為依我國公司法設立，經主管機關核准登記之本國公司，且須為提供資訊服務業(註[1])營業項目者。

三、檢測項目

(一) 企業資安評級(含網路架構檢視)

(二) 主機系統弱點掃描

(三) 資訊設備組態檢測

(四) 網路封包側錄分析

(五) 惡意程式或檔案檢視

(六) 防火牆連線設定檢視

四、申請費用及繳費方式

資安檢測診斷服務由經濟部工業局部分補助，受測企業自行負擔金額如下：

[1] 依據經濟部商業司「公司行號及有限合夥營業項目代碼表」，商工登記公示資料查詢服務之所營事業資料，以代碼 I3 開頭之營業項目皆為資訊服務業。

(一) 第 1 類受測企業(檢測範圍 IP 數為 101~200)，總價新臺幣 19 萬元
(政府補助 14 萬元、受測企業自負 5 萬元)

(二) 第 2 類受測企業(檢測範圍 IP 數為 21~100)，總價新臺幣 13 萬 5 仟元
(政府補助 11 萬元、受測企業自負 2 萬 5 仟元)

受測企業選定類別後，請將自負款匯入以下帳戶，手續費或匯費由受測企業自行負擔；匯款後請將收據掃描 email 至 security@cisanet.org.tw。

匯款銀行：玉山銀行中山分行(銀行代號 808)

銀行帳號：0417-968-097989

匯款戶名：中華民國資訊軟體協會

受測企業應於申請通過後立即支付，未繳交費用者，計畫執行單位有權拒絕受理。

五、申請方式

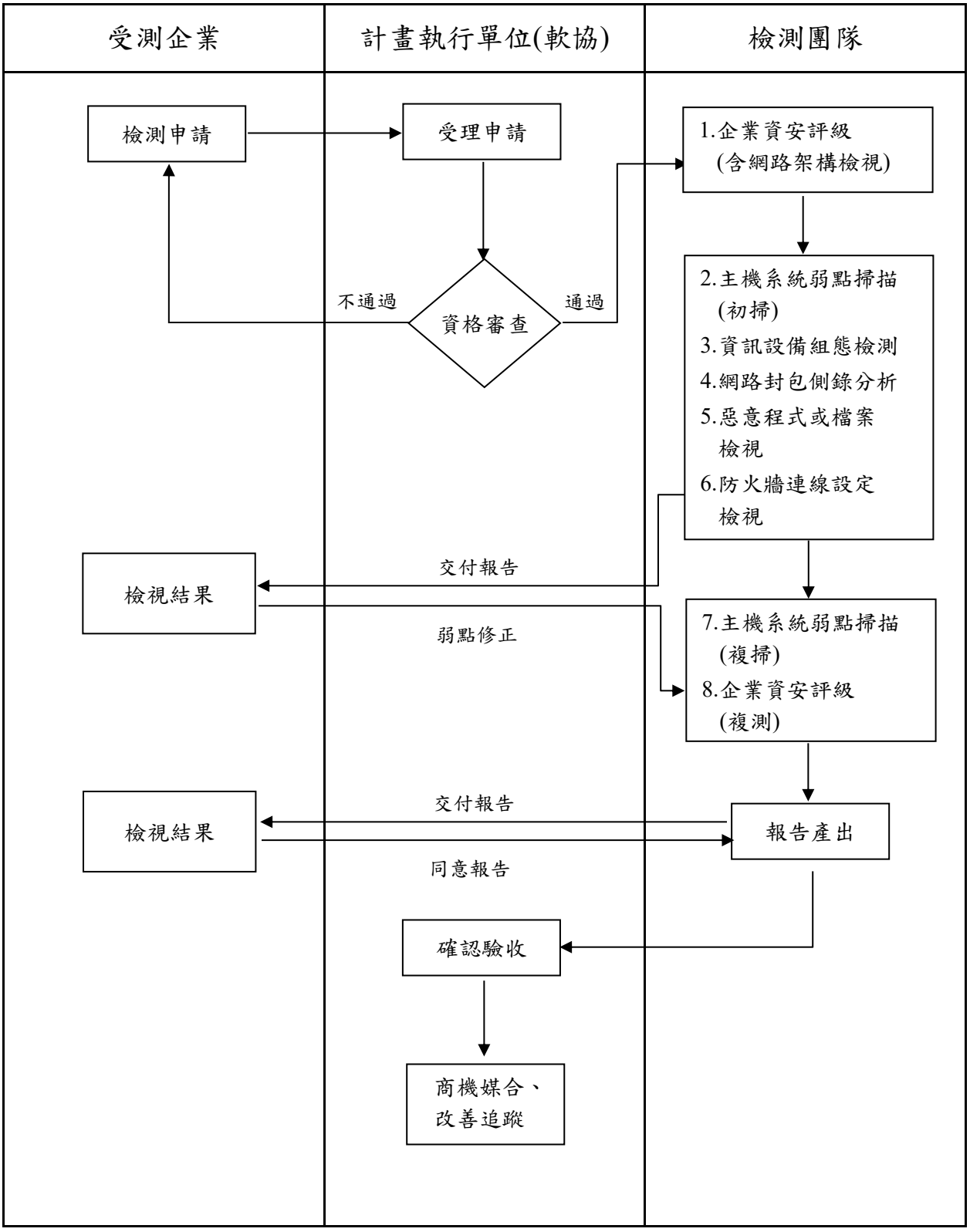
填寫「資安檢測診斷服務申請暨切結書」(請參見附件一)，並完成公司大小章用印後，將正本郵寄至 103 臺北市大同區承德路二段 239 號 6 樓 中華民國資訊軟體協會，註明「申請資安檢測診斷服務」。

六、檢測診斷服務團隊派案原則：

本服務將受理 30 家符合資格之企業申請，包含第 1 類 10 家、第 2 類 20 家，依申請先後順序額滿為止；受測企業可於本計畫遴選合格檢測團隊中，提出指定檢測團隊申請，未指定或團隊檢測數量已額滿，由計畫執行單位(軟協)依序派案。

檢測團隊將與受測企業簽訂保密切結書，以利本計畫執行。

七、資安檢測診斷服務申請及執行流程



八、企業資安評級評估作業

(一) 檢測團隊將訪談受測企業並協助填寫資安整合服務平台[2](SECPAAS)資安評級問卷，並提供改善建議及相關做法。

(二) 檢測團隊將分析資安評級初測及複測結果之差異，提供受測企業「企業資安評級評估報告」，報告內含「網路架構檢視」相關內容。

九、資訊安全技術檢測作業

(一) 主機系統弱點掃描：本項作業係使用合法授權之商用軟體，針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點掃描，至少包含以下掃描項目及其最新發布之 Common Vulnerabilities and Exposures (CVE)：

1. 作業系統未修正的弱點掃描
2. 常用應用程式弱點掃描
3. 網路服務程式掃描
4. 木馬、後門程式掃描
5. 帳號密碼破解測試
6. 系統之不安全與錯誤設定掃描
7. 網路通訊埠掃描

[2] 資安整合服務平台(SECPAAS) - https://secpaas.org.tw/

主機系統弱點掃描將進行初掃及複掃，執行方式如下：

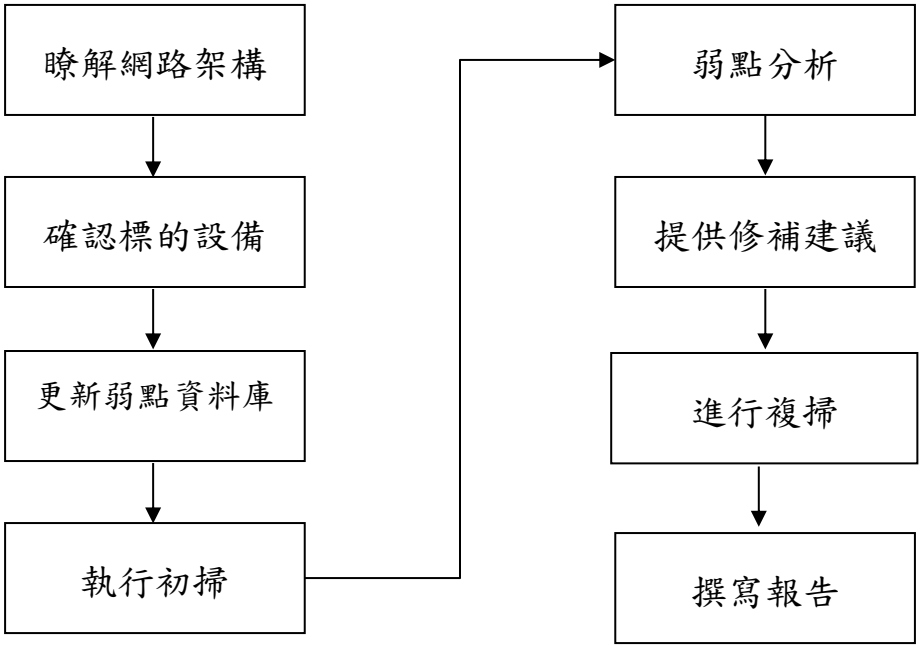


圖1：主機系統弱點掃描作業流程圖

(二) 資訊設備組態檢測：本項作業係使用合法授權之軟體，參考行政院國家資通安全會報技術服務中心官方網站「政府組態基準」專區所公布安全性檢視內容，確認受測企業指定之資訊設備組態安全設定，並至少完成表 1 之檢測項目。

表 1：安全性設定檢測項目表

項目	選項	說明	方式
安全性選項	1	帳戶：Administrator 帳戶狀態	停用
	2	帳戶：重新命名系統管理員帳戶	Renamed_Admin
	3	帳戶：Guest 帳戶狀態	停用
	4	帳戶：重新命名來賓帳戶名稱	Renamed_Guest
	5	網路存取：允許匿名 SID/名稱轉譯	停用

項目	選項	說明	方式
	6	網路存取：不允許 SAM 帳戶和共用的匿名列舉	啟用
	7	Microsoft 網路用戶端:傳送未加密的密碼到其他廠商的 SMB 伺服器	停用
	8	關閉自動播放	啟用 所有磁碟機
	9	AutoRun 的預設行為	啟用/不執行任何 Autorun 命令
帳戶原則	10	重設帳戶鎖定計數器的時間	15 分鐘
	11	帳戶鎖定期間	15 分鐘
	12	帳戶鎖定閥值	5 次不正確的登入嘗試
密碼原則	13	最小密碼長度	8 個字元以上
	14	密碼最長使用期限	90 天以下
	15	密碼最短使用期限	1 天
密碼原則	16	強制執行密碼歷程記錄	3 次以上
	17	使用可還原的加密來存放密碼	停用
	18	密碼必須符合複雜性需求	啟用
螢幕保護	19	啟用螢幕保護裝置	啟用
	20	螢幕保護裝置逾時	啟用，900 秒
	21	以密碼保護螢幕保護裝置	啟用
	22	記錄檔大小上限(KB)(安全性)	啟用，81920(KB)
	23	記錄檔大小上限(KB)(安裝程式)	啟用，32768(KB)
	24	記錄檔大小上限(KB)(系統)	啟用，32768(KB)
互動式登入	25	互動式登入：在密碼到期前提示使用者變更密碼	14 天
	26	互動式登入：不要求按 CTRL+ALT+DEL 鍵	停用

項目	選項	說明	方式
	27	互動式登入：不要顯示上次登入的使用者名稱	啟用
附件管理員	28	開啟附件時通知防毒程式	啟用
	29	隱藏移除區域資訊的機制	啟用
	30	不要保留檔案附件的區域資訊	停用

資料來源：行政院國家資通安全會報技術服務中心，「政府組態基準」專區，參考網址 https://www.nccst.nat.gov.tw/GCB

(三) 網路封包側錄分析作業：

1. 網路封包側錄分析：在受測企業有線網路(內網、外網、DMZ 區或 N 個網段)適當位置架設側錄設備，觀察內部電腦或設備是否有對外之異常連線或 DNS 查詢，並比對是否連線已知惡意 IP、中繼站(Command and Control，C&C)或有符合惡意網路行為的特徵。發現異常連線之電腦或設備需確認使用狀況與用途。
2. 網路設備記錄檔分析：檢視網路與資安設備(如防火牆、入侵偵測/防護系統等)紀錄檔，分析過濾內部電腦或設備是否有對外之異常連線紀錄，發現異常連線之電腦或設備需確認使用狀況與用途。

(四) 惡意程式或檔案檢視：

1. 使用者端電腦檢視：
   (1) 針對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。
   (2) 針對使用者電腦進行作業系統更新檢視；使用者電腦安裝之各項應用程式安全性更新，包含 Office 應用程式、Adobe Acrobat、及 Java 應用程式更新檢視；檢視使用者電腦是否使用已經停止支援之作業系統或軟體(如 Windows XP、Windows 7、Office 2003、Office 2007、Adobe Flash Player 等)；針對使用者電腦防毒軟體

安裝、更新及定期全系統掃描狀況進行檢視。

2. 伺服器主機檢視：

(1) 針對伺服器主機進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

(2) 針對伺服器主機進行作業系統更新檢視；檢視伺服器主機安裝之各項應用程式安全性更新，包含 Office 應用程式、Adobe Acrobat、及 Java 應用程式更新；檢視伺服器是否使用已經停止支援之作業系統或軟體(如 Windows XP、Windows 7、Windows Server 2008、Windows Server 2008 R2、Office 2003、Office 2007、Adobe Flash Player 等)；檢視伺服器是否使用不合宜之作業系統(如使用 Windows 10 等)；針對伺服器主機防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。

(五) 防火牆連線設定檢視：檢視由受測企業所提供 1 台防火牆的連線設定規則(如外網對內網、內網對外網、內網對內網)是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性(包含設置「Permit All/Any」與「Deny All/Any」等 2 項防火牆檢測規則確認)。

十、受測企業配合項目

(一) 受測企業申請檢測診斷服務時，請填寫「資安檢測診斷服務申請暨切結書」(請參見附件一)，以便檢測團隊了解受測環境，及早準備，並避免影響受測企業正常營運。

(二) 受測企業應提供聯絡專人，協助聯繫安排各項訪談、會議時間，及檢測作業時間、場地及設備。

(三) 受測企業應配合檢測團隊執行改善建議，並於主機系統弱點初掃發現企業網路潛在的安全威脅後，儘速進行弱點修補，以進行複掃。

十一、 受測項目總表說明

項次	檢測項目	說明
1	企業資安評級	本項作業係由檢測團隊訪談受測企業並協助填寫資安整合服務平台(SECPAAS)資安評級問卷，並分析資安評級初測及複測結果之差異，提供改善建議及相關做法。
2	主機系統弱點掃描	針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點掃描，找出受測企業網路潛在的安全威脅，並提供改善建議及複掃，以確認弱點是否排除，降低遭受入侵的風險。
3	資訊設備組態檢測	規範資通訊終端設備(如個人電腦)的一致性安全設定(如密碼長度、更新期限等)，以降低成為駭客入侵管道之風險。
4	網路封包側錄分析	觀察內部電腦或設備是否有對外之異常連線或 DNS 查詢，並比對是否連線已知惡意 IP、中繼站或有符合惡意網路行為的特徵，找出建立惡意連線的受駭主機，並提供強化改善建議。
5	惡意程式或檔案檢視	1. 針對個人電腦進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

項次	檢測項目	說明
		2. 針對伺服器主機進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。 3. 針對使用者電腦與伺服器主機進行作業系統更新檢視；使用者電腦安裝之各項應用程式安全性更新，包含 Office 應用程式、Adobe Acrobat、及 Java 應用程式更新檢視；針對使用者電腦防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。
6	防火牆連線設定檢視	檢視防火牆的連線設定規則(如外網對內網、內網對外網、內網對內網)是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性。

十二、 聯絡方式

計畫執行單位聯絡方式，電話：02-2553-3988 轉分機 371 或 375，

E-mail：security@cisanet.org.tw。