經濟部工業局 110 年「跨域資安強化產業推動計畫」
資訊安全檢測診斷服務團隊遴選須知

一、目的

資安事件層出不窮，產業鏈上下游的安全防護已成為國際重要議題，企業除了加強自身的資安防護能力，對於合作廠商及供應商的資安防護能力亦需加以重視，以確保商品生產或服務提供過程的各個環節都受到妥善的防護。為提升國內產業資安防護能力，經濟部工業局推動產業資訊安全檢測診斷服務，並透過供應鏈串聯產業上下游，鼓勵供應鏈或集團連鎖企業完善整體資安防護，進而促進供應鏈生態系統資安防護能力。資安檢測診斷服務包含「資訊安全風險現況評估」、「伺服主機弱點掃描檢測」、「資訊設備組態基準檢測」、「網路封包側錄分析」、「惡意程式檢視檢測」及「防火牆檢測」等健診項目，協助受測企業掌握自身資安管理與防護現況，並了解如何強化、改善缺失及進一步建立預防措施。

為遴選國內優秀資安業者協助提供資安檢測診斷服務，特訂定此遴選須知，邀請具備資格及服務能量之業者參加。

二、申請日期：依正式公告文件為準。

三、檢測期間：自受測企業申請通過並派案執行起，至 110 年 10 月 31 日前完成報告交付。

四、檢測服務團隊申請資格

(一)依我國公司法設立，中央主管機關經濟部核准登記之本國公司、或依法設立提供專業服務之合夥組織。請附團隊所有成員證明影本一份。

(二)檢測團隊之組成至少包含 1 家(含)以上公司，團隊成員應包含專案主持人、專案經理、資安風險現況評估人員及資安檢測診斷服務人員等，檢

測團隊及服務人員應具備下列資格條件，以確保服務水準，請填具附件一申請表並附證明文件一份。

1. 檢測團隊成員須提供近 3 年內執行本辦法所訂各項資安檢測診斷作業，每項檢測至少各 1 件，合計達 6 件(含)以上之實績。
2. 資訊安全風險現況評估人員，需具備 ISO/IEC 27001 Lead Auditor（主導稽核員）證照或課程完訓證明。
3. 資訊安全技術檢測作業人員，須具備以下資安相關證照或相關課程訓練證明至少 2 式，證照須於有效期間內，訓練證明須註明訓練期間：
   (1) 證照：CISSP (Certified Information Systems Security Professional)、CompTIA Security (CompTIA Security+)、SSCP (Systems Security Certified Practitioner)、CEH (Certified Ethical Hacking)、OSCP (Offensive Security Certified Professional)、ECSA (EC-Council Certified Security Analyst)、GIAC 技術類[1]等相關資安證照。
   (2) 課程訓練：接受過 CISSP (Certified Information Systems Security Professional)、CEH (Certified Ethical Hacker)、CompTIA Security (CompTIA Security+)、GIAC 技術類等相關資安課程訓練。

(三)團隊若為 2 家(含)以上業者組成，各成員需與主提案廠商簽署合作協議書一份。

(四)本年度資安檢測診斷服務以供應鏈為優先，檢測團隊需提出有意願受檢測之供應鏈或 3 家(含)以上受測企業名單。

五、檢測服務團隊遴選及派案原則

(一)本計畫預計遴選符合資格要求之團隊數隊，團隊成員需承諾於 110 年 10 月 31 日完成所有工作並正式結案，並於 110 年底前通過檢測項目之

[1] GIAC 技術類證照清單 - https://nicst.ey.gov.tw/Page/D94EC6EDE9B10E15/7ba35454-3644-4199-828d-cff2f2d077fc

資安服務機構能量登錄。

(二)本年度受測企業分類及經費如下：

類別	檢測範圍 IP 數	檢測診斷項目	經費(新台幣)
A	101~200	1.資訊安全風險現況評估 2.伺服器主機弱點掃描 3.網路封包側錄分析 4.GCB 組態檢測	每案 139,500 元 (政府補助 10 萬元、受測企業自負 39,500 元)
B	20~100		每案 89,500 元 (政府補助 8 萬元、受測企業自負 9,500 元)
C	101~200	1.資訊安全風險現況評估 2.伺服器主機弱點掃描 3.網路封包側錄分析 4.GCB 組態檢測 5.惡意活動程式/檔案檢視 6.防火牆檢視	每案 189,500 元 (政府補助 14 萬元、受測企業自負 49,500 元)
D	20~100		每案 119,500 元 (政府補助 10 萬元、受測企業自負 19,500 元)

(三)進階檢測服務，檢測團隊得依檢測服務能量，選填附件一申請表「進階檢測服務選項」欄位，檢測項目包含「產品及操作技術(OT)資安」、「網站弱點及個人資料掃描」、「社交工程」及「攻防演練」等；請團隊依自身檢測量能及意願填寫，填寫內容將一併提供受測企業參考，該欄位不影響本資安檢測診斷服務資格審核結果。因各領域產業特殊風險及 側重皆有不同，後續相關進階檢測服務需求，由檢測團隊與企業另行商議，不列入本資安檢測診斷服務範圍。

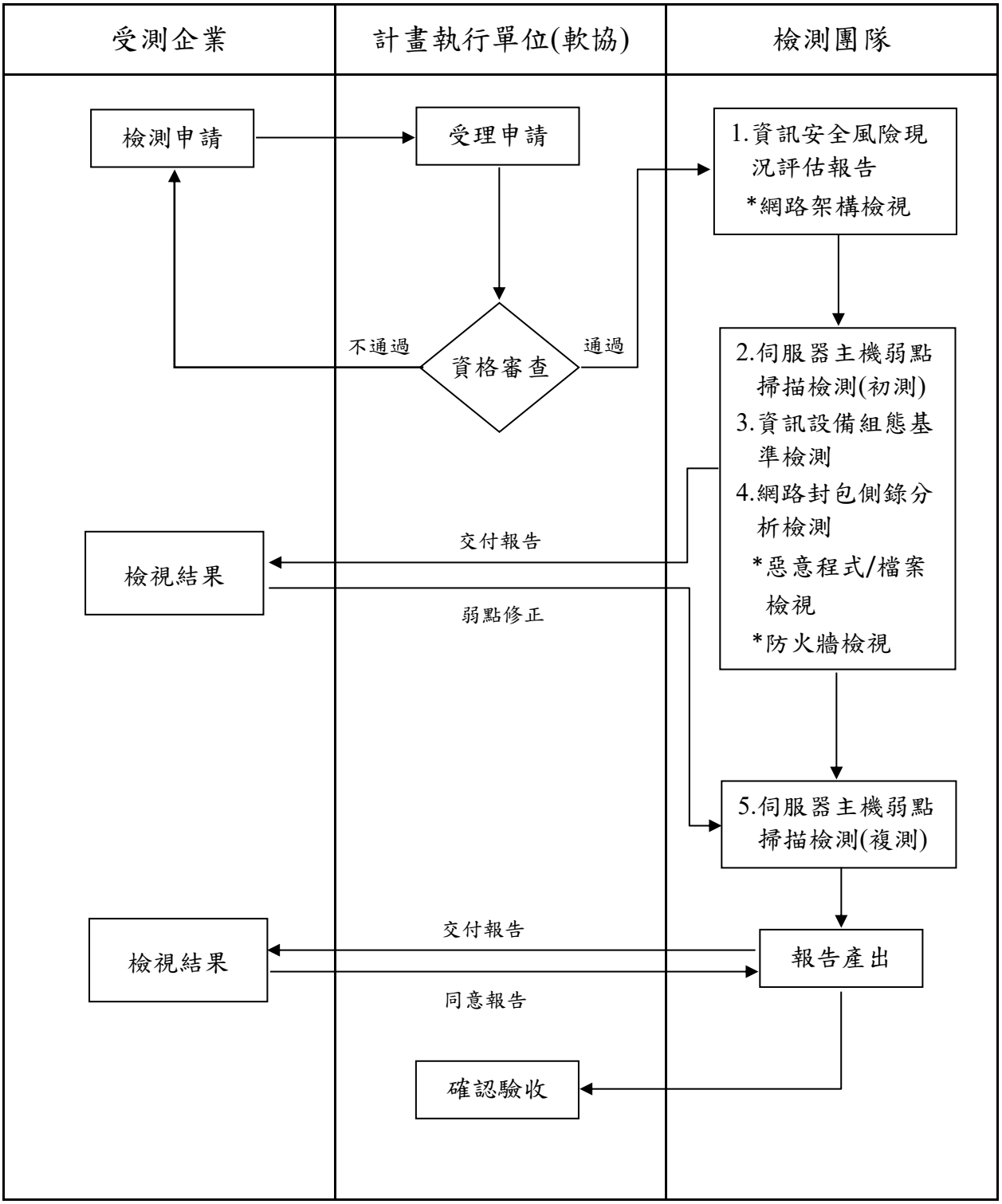
(四)110 年資安檢測服務將受理 40 家符合資格之企業申請，包含 A 類 5 家、B 類 13 家、C 類 10 家及 D 類 12 家，依申請先後順序額滿為止；將依遴選優先序位，並參考歷年參與本辦法實績為案件數量分配之依據。

(五)派案原則：

1. 檢測團隊推薦之受測企業，優先派案予該檢測團隊執行。
2. 受測企業可指定檢測團隊，未指定或團隊檢測數量已額滿，由計畫執

行單位依序派案，檢測團隊不得挑選或拒絕；若拒絕派案者，將視為違約並列入下年度提案評分參考。

六、資安檢測診斷服務申請及執行流程



*註：網路架構檢視、惡意程式/檔案檢視、防火牆檢視為C、D類受測企業檢測項目。

七、資安檢測執行規範

參與資安檢測診斷團隊必須簽訂專案合約及保密切結書，藉此保障雙方之權益，檢測團隊成員皆需遵循，內容如下：

(一)與計畫執行單位：檢測團隊主提案單位需與計畫執行單位簽訂合約及保密切結書。

(二)與受測企業：檢測團隊須向受測企業簽訂保密切結書。保證檢測過程中所取得之資料，絕不會以任何方式透露給任何第三方。

八、資訊安全風險現況評估作業

(一)參採資訊安全管理標準 ISO/IEC 27002 研擬「訪談分析紀錄表」，檢測團隊進行訪談後應產出「資訊安全風險現況評估報告」；C、D 類「資訊安全風險現況評估報告」須含「網路架構檢視報告」。

(二)「資訊安全風險現況評估報告」應整合伺服器主機弱點檢測、資訊設備組態基準檢測與網路封包側錄分析檢測結果，提供受測企業「總體資安風險評估報告」。

九、資訊安全技術檢測作業

(一)伺服器主機弱點掃描檢測作業：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設定、帳號密碼設定及管理方式等進行弱點檢測，系統弱點掃描的檢測項目須符合 Common Vulnerabilities and Exposures (CVE)發布的最新版本弱點內容，並參採 CVE 評分系統 CVSS (Common Vulnerability Scoring System)給予嚴重(Critical)、高(High)、中(Medium)、低(Low)及無(None)之弱點等級評分。檢測項目至少包含以下項目：

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檢測。

7. 網路通訊埠掃描。

伺服器主機弱點檢測作業需完成初、複測作業，其流程圖如下所示：

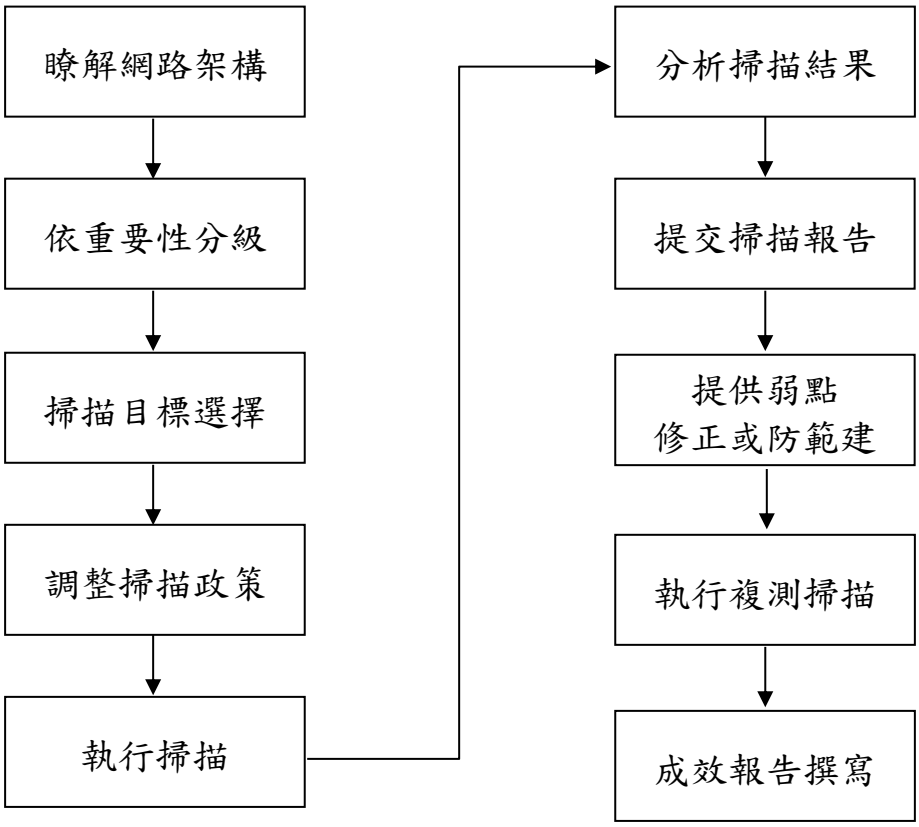


圖1：伺服器主機弱點掃描檢測作業流程圖

(二)資訊設備組態基準檢測作業：本項作業係透過合法授權之商用軟硬體，針對資通訊終端設備之資訊安全組態基準是否達到一致性安全設定狀態檢測。資訊設備組態基準設定值以政府組態基準(GCB)做為依據；組態基準檢測項目至少包含以下共通檢測項目，如下表列：

表 1：資訊設備組態基準共通檢測項目表

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
	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 分鍾
	11	帳戶鎖定期間	15 分鍾
	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
	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

項目	選項	說明	方式
	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
	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(GCB) Windows 設定對照表 V1.7(2020/7/20)，網址如下 https://www.nccst.nat.gov.tw/GCBDownloadDetail?lang=zh&seq=1078

(三)網路封包側錄分析作業：本項作業係透過網路封包監聽，了解組織網路是否有異常連線狀態。檢測作業分為「網路封包側錄分析」及「網路設備記錄檔分析」。

1. 網路封包側錄分析:以電腦設備至受測企業網路適當位置架設側錄點(如:側錄核心交換器流量封包),監聽軟體採用如:Tcpdump、Wireshark等工具，進行至少 7 天之網路封包監聽並分析，分析重點在於有無異常連線、是否連線已知惡意 IP，協助受測產業發現異常連線。
2. 網路設備記錄檔分析：將針對防火牆、入侵偵測防護系統等網路設備紀錄檔，分析過濾異常連線紀錄。網路設備紀錄檔分析以 1 個月內的紀錄為原則，依據分析與檢測結果進行彙整與研究，撰寫於報告書。

(四)惡意活動程式/檔案檢視：

1. 使用者端電腦檢視：使用者端電腦惡意程式或檔案檢視、安全性更新等。
2. 伺服器主機檢視：伺服器主機惡意程式或檔案檢視。
3. 安全設定檢視部分：網通設備組態設定檢視及設備記錄檔分析、應用程式伺服主機組態設定檢視、目錄伺服器(如 MS AD)組態設定檢視。

(五)防火牆檢視：檢視受測企業的防火牆連線設定規則，依據檢視結果分析企業網路之安全性弱點，確認來源/目的 IP 與通訊埠連通的適當性，防火牆開啟通訊埠檢視範圍需涵蓋 0~65535，並撰寫該服務對象「資訊安全技術檢測_防火牆規則檢視分項報告」。

十、檢測團隊應配合作業規定事項

(一)檢測團隊於需求訪談階段，需先就受測企業之網路架構及標的設備進行了解，如設備廠牌、系統版本等，以利後續進行弱點或漏洞分析及修補建議。

(二)檢測團隊應與受測企業協調取得適當時間進行檢測作業，並依排定之日期執行資安檢測。

(三)檢測期間若可能影響系統運作時，需提前通知本計畫執行單位及受測企業專案聯絡人，以因應緊急突發狀況。

(四)檢測期間若檢測團隊發現重大安全弱點或漏洞，應立即告知受測企業。

(五)執行資安檢測期間，檢測團隊若發現企業網路有駭客入侵行為或跡象時，應立即告知受測企業。

(六)專案合約終止時，檢測團隊應將有關資安檢測過程中處理之任何形式資訊，整理歸檔後交還受測企業，並留存交還紀錄以供備查。

(七)檢測工具應為取得合法授權之商用軟體，並應於每次檢測作業前，將工具之弱點資料庫更新至最新版本，並提供佐證資料，以確保本項服務之正確性。

(八)資安檢測作業執行前，須提出受測目標備份建議，避免發生非預期資料損毀或遺失等情形。作業執行期間，若需執行具侵入性質的檢測作業，需與受測企業進行確認，並於雙方議定之適當時間且具備應變措施與風險評估後，方能進行檢測作業。

(九)資安檢測作業執行期間，應避免執行具破壞系統可用性與完整性的檢測作業，如刪除、更改資料及更動原系統設定等行為。如為新增資料行為，該資料應明顯可識別為本次測試所產生，並通知受測系統相關人員。

(十)因執行資安檢測作業造成軟硬體設備服務中斷時，檢測團隊應立即停止測試工作，協助受測企業恢復正常運作，並調整測試之方法與策略，以確保系統無受影響，並經受測企業同意後繼續進行。

(十一)本計畫檢測團隊應接受執行單位實地稽核，確保檢測團隊於服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

(十二) 檢測團隊應協助受測企業解讀報告及建議後續處理方式。

十一、履約期間內檢測團隊應配合事項

(一)檢測團隊須於簽約當月起，每月 30 日（如遇假日則順延一個工作日）提出當月書面工作進度報告，以確保專案進行順利。

(二)檢測團隊須配合參加工作會議，提供專案進度報告。

(三)本須知服務內容涉及敏感資訊，檢測團隊不得轉包或分包予其他業者執行。

十二、驗收項目

每完成一案(受測企業)需交付以下報告：

(一) 與受測企業簽訂之保密切結書。

(二) 啟動會議現場照片二張、簡報及會議紀錄。

(三) 資訊安全風險現況評估報告(包含訪談分析紀錄表)。

(四) 資訊設備組態基準檢測報告。

(五) 弱點掃描檢測初、複測各一份報告。

(六) 網路封包側錄分析報告。

(七) 將所有檢測報告，彙整一份「總體資安風險評估」報告。

(八) 結案會議簡報及會議紀錄

(九) 受測企業意見調查表。

(十) 若進行 C、D 類檢測，需於訪談紀錄表中涵蓋網路架構檢視；另附惡意活動程式/檔案檢視、防火牆檢視報告各一份。

十三、申請時應檢附之文件

檢附「資訊安全檢測診斷服務團隊」申請書，請參見附件一。

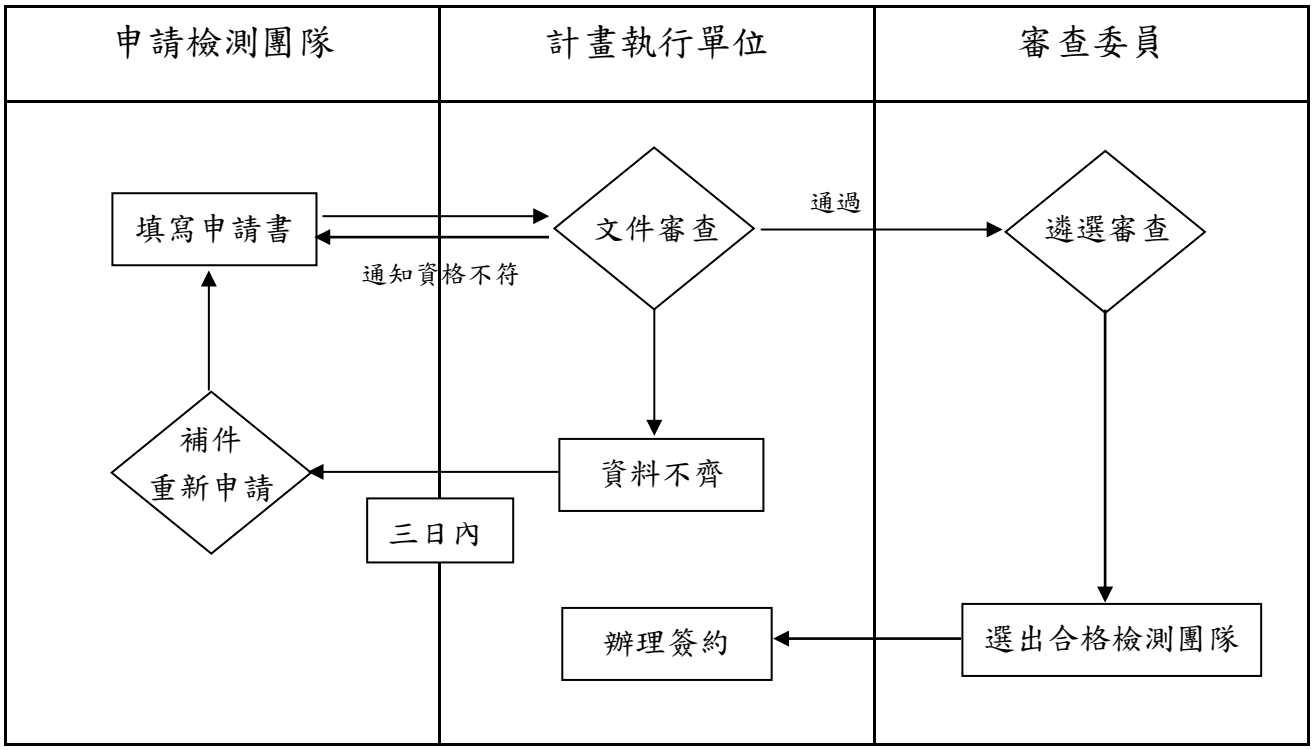
十四、申請方式

須完整填寫「資訊安全檢測診斷服務團隊申請書」及完成公司大小章用印後，將正本於期限內郵寄至 103445 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「資訊安全檢測診斷服務團隊申請書」，或先 Email 掃描電子檔，再後補文件正本。

聯絡人：甘世裕(Kevin)專員 kevin@cisanet.org.tw，電話 (02)2553-3988 分機 371。

十五、遴選審查流程及評分標準

本計畫成立遴選委員會,由審查委員依申請單位之書面資料及評分項目進行遴選，遴選審查流程如下圖所示，並說明如下：



(一) 第 1 階段：文件資格審查

本計畫執行單位依據本遴選須知進行資格及申請書文件資料正確性審核，經審核結果若有申請資格不符者，敘明原因後做退件處理；若僅為提供之書面資料未齊備時，限期於 3 個工作日內重新申請，逾時視同資格不符。

(二) 第 2 階段：召開遴選會議審查評選

針對符合遴選資格之企業，將召開遴選會議，並外聘具專業背景審查委員 3~5 名進行複審及評選。

(三) 評選標準(採序位法)

審查委員依下列各評選項目及配分，予以評選。

審查委員就個別團隊各評選項目及子項分別評分後予以加總，並依加總分數高低轉換為序位，分數最高者為序位 1，餘依分數排序，依序位合計較低者優先，選出符合資格之團隊。而出席委員評分平均低於 70 分者，為不合格團隊。

表 2：評選項目及配分表

項次	評選項目	評選內容	比例
1	團隊規模	檢測團隊規模與人力能量、 團隊實績與相關技術經驗	30%
2	執行方式與程序	資訊安全風險現況評估、伺服器主機弱點掃描方法、資訊設備組態基準檢測、網路封包側錄分析、惡意活動程式/檔案檢視、防火牆檢視（以上項目之需求確認、分析規劃、資訊蒐集、執行方式、工具等作業方法與程序）	40%
3	專案管理	進度時程控管、資料管制與品質保證、前年度之執行實績及完整性 （已提案過之團隊針對歷年進度做報告、未參與過之團隊，請提出每案預計完成期程及可執行案件數，及進度時程控管方式等）	20%
4	簡報答詢	廠商簡報與答詢內容是否清楚、完整	10%
合計			100%

十六、遴審查結果將以 Email 方式通知申請團隊聯絡人。

【附件一】

經濟部工業局 110 年「跨域資安強化產業推動計畫」

「資訊安全檢測診斷服務團隊」遴選申請書

一、團隊成員基本資料

1. 主提案並代表簽約廠商

<table>
<tr><th colspan="6">基 本 資 料</th></tr>
<tr><td>公司中文全名</td><td colspan="2"></td><td>負責人
姓名</td><td colspan="2"></td></tr>
<tr><td>核准設立日期</td><td colspan="2">民國　年　月　日</td><td>統一編號</td><td colspan="2"></td></tr>
<tr><td>公司資本額</td><td colspan="5"></td></tr>
<tr><td>公司聯絡地址</td><td colspan="5"></td></tr>
<tr><td>公司聯絡電話</td><td colspan="5">（　　）　　－</td></tr>
<tr><td rowspan="5">公司聯絡人</td><td>姓名</td><td colspan="2"></td><td>職稱</td><td colspan="2"></td></tr>
<tr><td>電話</td><td colspan="5">（　　）　　－
分機</td></tr>
<tr><td>傳真</td><td colspan="5">（　　）　　－</td></tr>
<tr><td>行動電話</td><td colspan="5"></td></tr>
<tr><td>E-mail</td><td colspan="5"></td></tr>
<tr><td rowspan="2">公司規模</td><td>總員工數</td><td colspan="2">□50人以下
□51-100人</td><td>□101-200人</td><td>□201人以上</td></tr>
<tr><td>資安部門人數</td><td colspan="2">□5人以下
□31-50人</td><td>□6-10人
□51-100人</td><td>□11-30人
□101人以上</td></tr>
<tr><td colspan="2">本團隊/公司執行本計畫最大服務能量</td><td colspan="4">□僅可執行A、B類案件數量_____案
□可執行A、B、C、D類檢測數量共_____案</td></tr>
<tr><td colspan="2">*本團隊/公司可提供的進階檢測服務選項</td><td colspan="4">□產品及操作技術(OT)資安　□社交工程
□網站弱點及個人資料掃描　□攻防演練</td></tr>
</table>

*註：因各領域產業特殊風險皆有不同，本選項僅用於提供受測企業參考，相關檢測服務需求，由檢測團隊與企業商議選購。

2.團隊成員一

<table>
<tr><th colspan="6">基 本 資 料</th></tr>
<tr><td>公司中文全名</td><td colspan="2"></td><td>負責人
姓名</td><td colspan="2"></td></tr>
<tr><td>核准設立日期</td><td colspan="2">民國　年　月　日</td><td>統一編號</td><td colspan="2"></td></tr>
<tr><td>公司資本額</td><td colspan="5"></td></tr>
<tr><td>公司聯絡地址</td><td colspan="5"></td></tr>
<tr><td>公司聯絡電話</td><td colspan="5">（　）　－</td></tr>
<tr><td rowspan="5">公司聯絡人</td><td>姓名</td><td colspan="2"></td><td>職稱</td><td colspan="2"></td></tr>
<tr><td>電話</td><td colspan="5">（　）　－
分機</td></tr>
<tr><td>傳真</td><td colspan="5">（　）　－</td></tr>
<tr><td>行動電話</td><td colspan="5"></td></tr>
<tr><td>E-mail</td><td colspan="5"></td></tr>
<tr><td rowspan="2">公司規模</td><td>總員工數</td><td colspan="2">□50人以下
□51-100人</td><td>□101-200人</td><td>□201人以上</td></tr>
<tr><td>資安部門人數</td><td colspan="2">□5人以下
□31-50人</td><td>□6-10人
□51-100人</td><td>□11-30人
□101人以上</td></tr>
</table>

3.團隊成員二

<table>
<tr><th colspan="6">基 本 資 料</th></tr>
<tr><td>公司中文全名</td><td colspan="2"></td><td>負責人
姓名</td><td colspan="2"></td></tr>
<tr><td>核准設立日期</td><td colspan="2">民國　年　月　日</td><td>統一編號</td><td colspan="2"></td></tr>
<tr><td>公司資本額</td><td colspan="5"></td></tr>
<tr><td>公司聯絡地址</td><td colspan="5"></td></tr>
<tr><td>公司聯絡電話</td><td colspan="5">（　）　－</td></tr>
<tr><td rowspan="5">公司聯絡人</td><td>姓名</td><td colspan="2"></td><td>職稱</td><td colspan="2"></td></tr>
<tr><td>電話</td><td colspan="5">（　）　－
分機</td></tr>
<tr><td>傳真</td><td colspan="5">（　）　－</td></tr>
<tr><td>行動電話</td><td colspan="5"></td></tr>
<tr><td>E-mail</td><td colspan="5"></td></tr>
<tr><td rowspan="2">公司規模</td><td>總員工數</td><td colspan="2">□50人以下
□51-100人</td><td>□101-200人</td><td>□201人以上</td></tr>
<tr><td>資安部門人數</td><td colspan="2">□5人以下
□31-50人</td><td>□6-10人
□51-100人</td><td>□11-30人
□101人以上</td></tr>
</table>

註：本表若不敷使用，請自行複製填寫。

二、檢測團隊執行經驗及專業證照

申請資格項目	佐證資料	提供資格文件之 團隊成員/人員姓名
1. 檢測團隊成員須提供近3年內執行本須知所訂各項資安檢測診斷作業，每項檢測至少各1件，合計達6件(含)以上之實績		
2. 資訊安全風險現況評估(至少具備1張)	□ISO/IEC 27001 Lead Auditor證照	
3. 資訊安全技術檢測作業(符合之有效證照或訓練課程完訓證明至少2式)	證照	
	□SSCP (Systems Security Certified Practitioner)	
	□CEH (Certified Ethical Hacker) (執行C、D類案件必備)	
	□OSCP (Offensive Security Certified Professional)	
	□ECSA (EC-Council Certified Security Analyst)	
	□CISSP (Certified Information Systems Security Professional)	
	□GIAC技術類證照	
	□CompTIA Security (CompTIA Security+)	
	□其他	
	課程訓練	
	□CISSP (Certified Information Systems Security Professional)	
	□CEH (Certified Ethical Hacker)	
	□GIAC技術類課程	
	□CompTIA Security (CompTIA Security+)	

申請資格項目	佐證資料	提供資格文件之團隊成員/人員姓名
	□NSPA(Network Security Packet Analysis)	
	□其他：	

申請資格項目	檢測方式說明	提供資格文件之團隊成員/人員姓名
4. 伺服主機弱點掃描檢測執行工具、版本及方式(執行工具需有嚴重、高、中、低等四個等級的弱點分類)	執行工具： 版本： 方式：	
5. 資訊設備組態基準檢測執行工具、版本及方式		
6. 網路封包側錄分析檢測執行工具、版本及方式		
7. 惡意活動檢視檢測方式		
8. 防火牆檢視檢測方式		

註：本表若不敷使用，請自行調整。

進階檢測服務項目	檢測方式說明(含計價方式)	提供資格文件之團隊成員/人員姓名
1. 產品及操作技術(OT)資安檢測方式		
2. 網站弱點及個人資料掃描檢測方式		

進階檢測服務項目	檢測方式說明(含計價方式)	提供資格文件之 團隊成員/人員姓名
3. 社交工程檢測方式		
4. 攻防演練檢測方式		

註：本表若不敷使用，請自行調整。

三、有意願受檢之供應鏈/企業名單

編號	企業名稱	產業別/主要營業項目	預計檢測類別 (如 A、B、C、D)
1			
2			
3			

註：本表若不敷使用，請自行調整。

四、檢測團隊分工及參與人員

專案人員	公司名稱	職稱	姓名
專案主持人			
專案經理			
資訊安全風險現況評估人員			
伺服主機弱點掃描檢測人員			
資訊設備組態基準檢測執行人員			
網路封包側錄分析檢測人員			
惡意活動/程式檢視			
防火牆檢視			

□**本團隊已詳細閱讀過申請書內容、遴選辦法及注意事項，並同意遵守。**

團隊代表公司蓋章

(公司大小章)

申請日期：民國 110 年　　月　　日