經濟部工業局 111 年「跨域資安強化產業推動計畫」
資安檢測診斷服務團隊遴選須知

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。

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 111 年 10 月 31 日前完成報告交付。

四、檢測服務團隊申請資格

(一)依我國公司法規定，經主管機關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。

(二)每一檢測團隊之組成至少包含 1 家公司；團隊若為 2 家(含)以上組成，其他成員需與主提案廠商簽署合作協議書。

(三)團隊人力至少應包含專案負責人/專案經理與資安檢測服務人員；檢測團隊及執行人員應具備下列資格條件，以確保服務水準。

1. 檢測團隊須通過檢測項目之資安服務機構能量登錄，並提供檢測團隊近 3 年內執行主機系統弱點掃描、資訊設備組態檢測、網路封包側錄分析、惡意程式/檔案檢視及防火牆連線設定檢視等檢測項目，每項

檢測至少各 1 件，合計至少達 5 件(含)之實績。

2. 檢測團隊須登錄資安整合服務平台[1](SECPAAS)，並完成「企業資安評級顧問」訓練課程；尚未取得者須承諾在執行檢測任務前登錄資安整合服務平台(SECPAAS)，並完成「企業資安評級顧問」訓練課程。
3. 團隊執行人員須具備 ISO/IEC 27001 主導稽核員證照或課程完訓證明至少 1 式。
4. 團隊執行人員須具備下列資安相關證照或課程完訓證明至少 2 式，並註明證照之有效期間或課程完訓證明之訓練期間：

（1）證照：

- CCNA (Cisco Certified Network Associate)
- CCNP Security (Cisco Certified Network Professional Security)
- CEH (Certified Ethical Hacker)
- CHFI (Computer Hacking Forensic Investigator)
- CND (EC-Council Certified Network Defender)
- CompTIA Network+
- CompTIA PenTest+
- CompTIA Security+
- CPENT (EC-Council Certified Penetration Tester)
- CPSA (The CREST Practitioner Security Analyst)
- Microsoft Certified: Azure Administrator Associate
- Microsoft Certified: Azure Security Engineer Associate
- OSCP (Offensive Security Certified Professional)
- SSCP (System Security Certified Practitioner)
- iPAS 資訊安全工程師中級能力鑑定
- 其他相關資安證照

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

（2）課程訓練：上述資安證照相關課程完訓證明。

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,檢測團隊需承諾於 111 年 10 月 31 日完成所有工作並正式結案。

(二)本年度受測企業分類及經費如下：

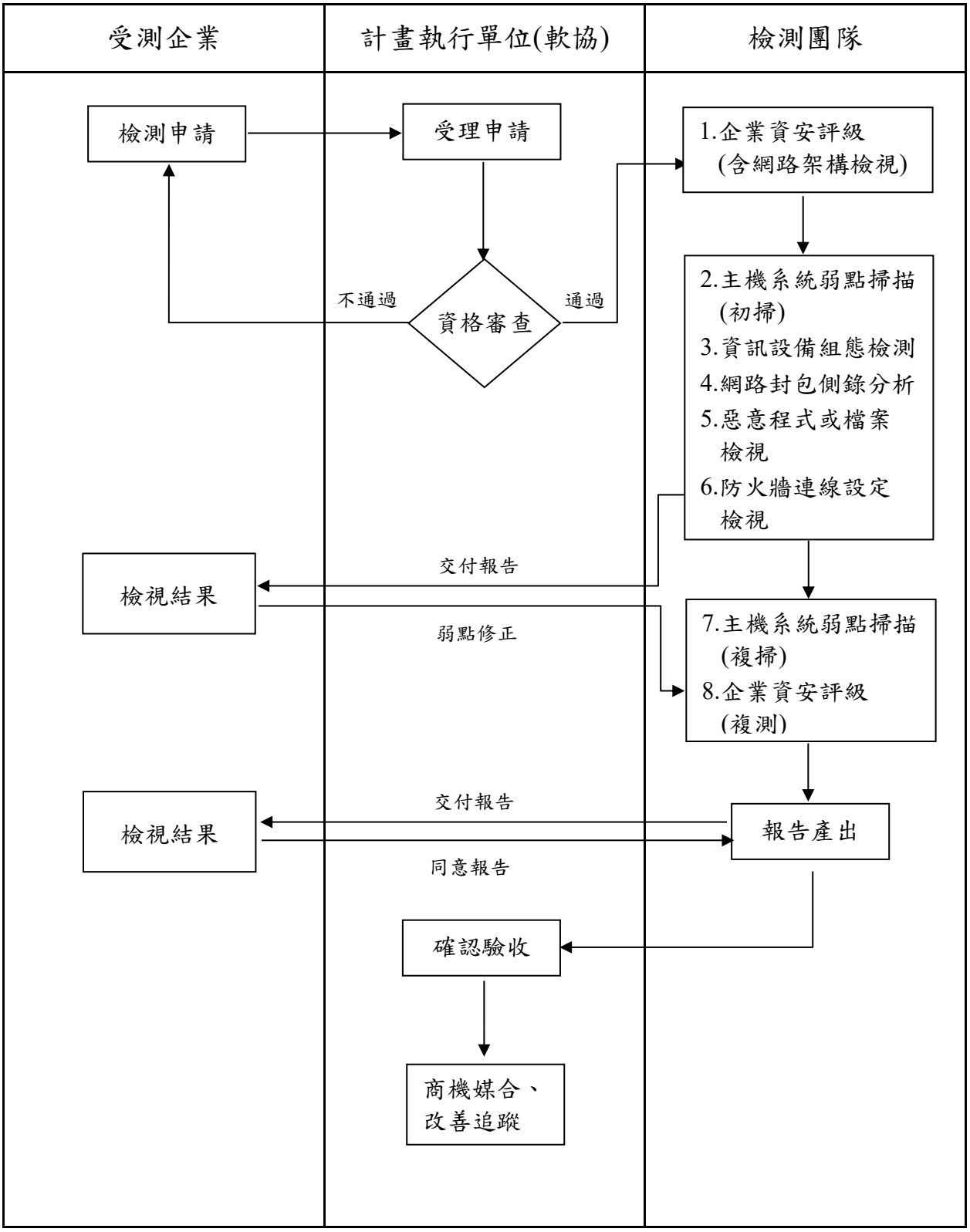
類別	檢測範圍 IP 數	檢測作業項目	經費 (新台幣)
第 1 類	101~200	1.企業資安評級 2.主機系統弱點掃描 3.資訊設備組態檢測 4.網路封包側錄分析 5.惡意程式或檔案檢視 6.防火牆連線設定檢視	每案總價 19 萬元 （政府補助 14 萬元、受測企業自負 5 萬元）
第 2 類	21~100		每案總價 13 萬 5 仟元 （政府補助 11 萬元、受測企業自負 2 萬 5 仟元）

(三)本年度資安檢測診斷服務將受理 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；將依遴選優先序位，並參考歷年參與本案實績為案件數量分配之依據。

(四)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，由計畫執行單位依需求派案，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



七、資安檢測執行規範

參與資安檢測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：檢測團隊須與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、企業資安評級評估作業

(一)檢測團隊應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，並提供改善建議及相關做法。

(二)檢測團隊應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」，報告須含「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

主機系統弱點掃描需進行初掃及複掃，執行方式如下：

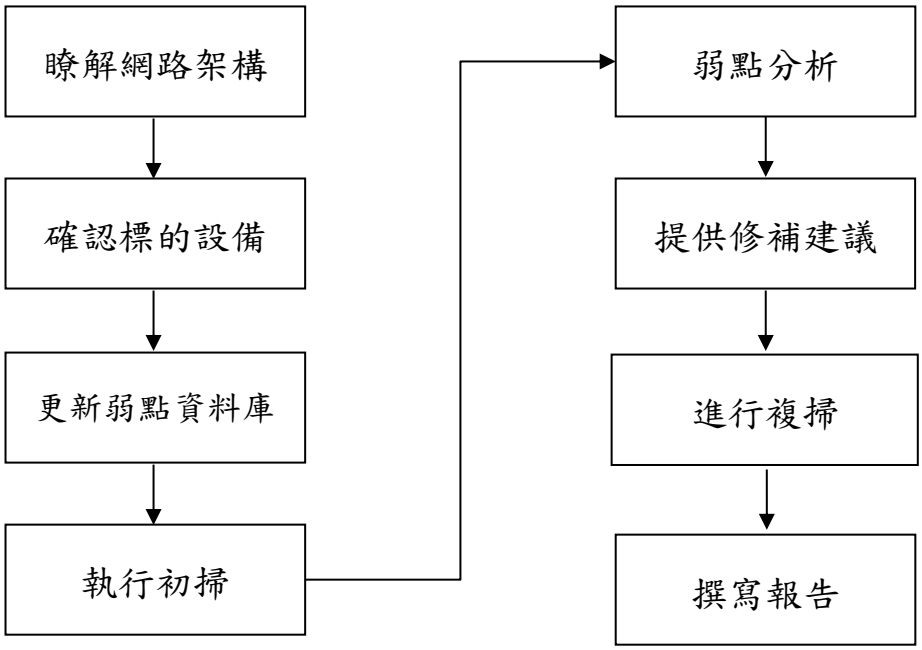


圖1 ：主機系統弱點掃描作業流程圖

(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
	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：

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. 網路設備紀錄檔分析：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：檢視受測企業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、檢測團隊應配合作業規定事項

(一)檢測團隊應於需求訪談階段先分就受測企業網路架構及受測設備進行了解，如設備廠牌、系統版本等，以利後續進行分析及改善建議。

(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。

(三)檢測期間若發現重大安全漏洞或惡意網路行為，應立即告知受測企業。

(四)專案終止時，檢測團隊應將有關檢測過程中處理之任何形式資訊，整理歸檔後退還受測企業或經受測企業同意後銷毀。。

(五)檢測工具須為取得授權使用的商用軟體，於每次使用前，將檢測工具之

資料庫更新至最新版本，以確保本項服務之完整正確。

（六）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。

（七）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。

（八）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。

（九）檢測團隊應接受計畫執行單位實地稽核，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。

十一、履約期間內檢測團隊應配合事項

（一）檢測團隊須於簽約次月起，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）本服務內容涉及敏感資訊，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 2 張、簡報及會議紀錄。

(三) 企業資安評級評估報告(包含網路架構檢視)。

(四) 主機系統弱點掃描報告(包含初掃及複掃)。

(五) 資安檢測服務報告(包含資訊設備組態檢測、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)。

(六) 專案執行紀錄檔(包含主機系統弱點掃描、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)。

(七) 結案會議簡報及會議紀錄。

十三、申請時應檢附之文件

檢附「資安檢測診斷服務團隊」遴選申請書，請參見附件一。

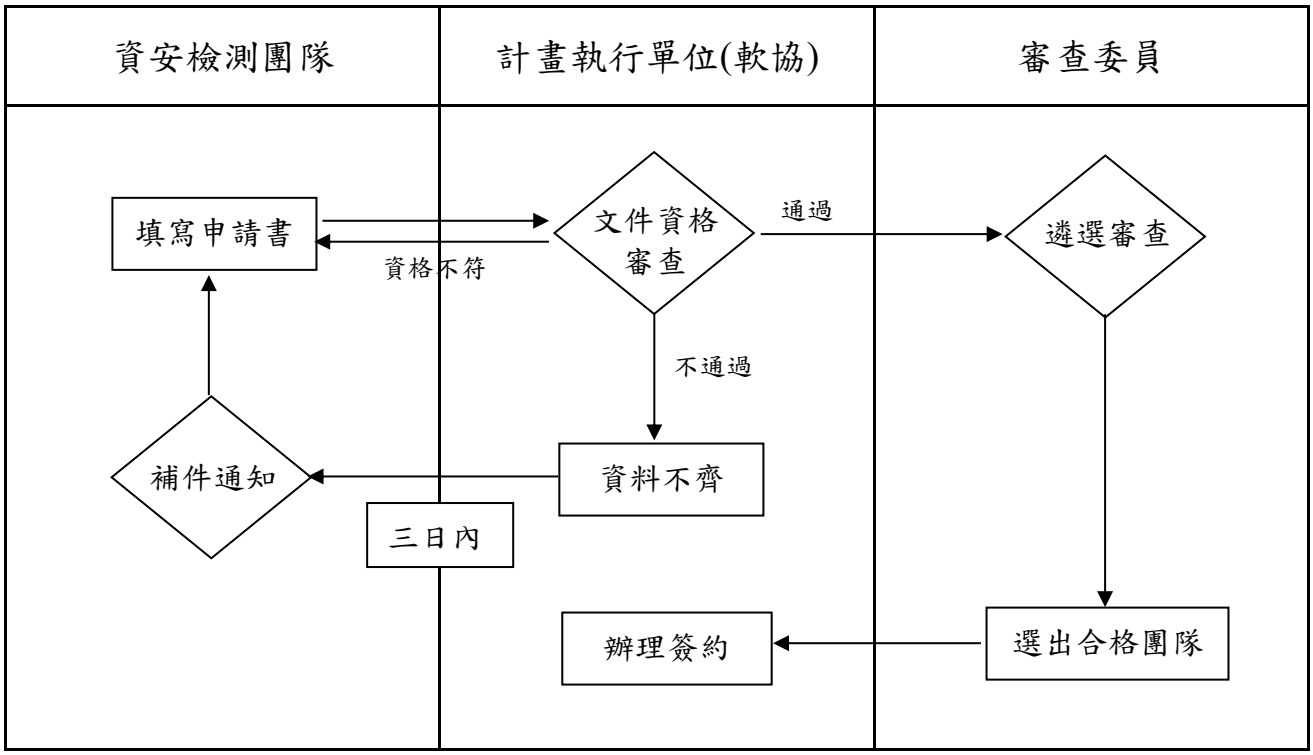
十四、申請方式

填寫「資安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「資安檢測診斷服務團隊申請書」。

計畫執行單位聯絡方式，電話：02-2553-3988 轉 371 或 375，E-mail：security@cisanet.org.tw。

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，將敘明原因並退件；若僅為提供之書面資料未齊備時，將通知申請單位並限期於 3 個工作日內補齊，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 名進行審查評選。

(三) 評選標準(採序位法)

審查委員依表 2 各評選項目及配分，就個別團隊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。而委員評分平均低於 70 分者，為不合格團隊。合格團隊之遴選優先序位，將做為案件分配之參

考依據。

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	• 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 • 防火牆連線設定檢視 本案檢測項目之需求確認、分析規劃、資訊蒐集、執行方式、檢測工具等	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、審查結果將以 Email 通知申請單位聯絡人。