【附件五】

資訊安全服務機構能量登錄服務項目之分項內容說明

(一)資訊安全服務項目

1.1 資訊安全或個人資料管理架構規劃與建置分項

1.1.1 資訊安全管理系統

釋義：資訊安全管理系統(Information Security Management System，ISMS)，是一套有系統管理資訊安全的方法，使用規劃(Plan)、執行(Do)、檢查(Check)、行動(Action)四個步驟循環進行。根據國際相關之標準，規定資訊安全管理系統必須包含資安管理系統之建立、實作、維護及持續改善，並包含資訊安全風險評鑑及處理之要求事項。
資安業者必須有能力協助組織建立資訊安全管理系統，並依循國際標準執行。

1.1.2 個人資訊管理系統

釋義：個人資訊管理系統(Personal Information Management System， PIMS)，是一套維護個人資料安全，保障個人隱私之系統，使用規劃(Plan)、執行(Do)、檢查(Check)、行動(Action)四個步驟循環進行，並遵循國際標準，符合個人資料保護法之規定。
資安業者必須有能力協助組織建立個人資訊管理系統，並依循國際標準，滿足個資法安全規範之要求。

1.1.3 制定風險管理與各項控管程序

釋義：資訊安全風險管理即是指對於資訊安全威脅所引發的可能性與後果進行識別、控制、降低或消除之運作過程。而風險管理控管程序即是指對於資訊安全威脅所引發的可能性與後果進行識別、控制、降低或消除之執行步驟。
資安業者必須有能力協助組織擬訂資訊安全風險管理之各項管理辦法與控管程序，並符合國際標準之要求。

1.1.4 資安監控中心

釋義：資安監控中心負責監看、偵測與防止企業資安事件的發生，並負責管理企業內的資安設備、網路設備、資料庫等可能引發資安疑慮的內容。
資訊業者必須能夠協助企業建立資安監控中心，進行資訊的安全管理、弱點管理、監看、事件處理與設備管理建置與執行等工作。

1.1.5 資安資訊分享與分析中心

釋義：資安資訊分享與分析中心能提供企業資安情資通報、整合與分享資訊功能，並進行資訊研判分析，提供企業資訊安全上情資整合與聯防之工作。

資安業者必須能夠協助企業建立資安資訊分享與分析中心，提供相關程序擬訂、技術建立及相關設備的佈建等,並協助整合國內外資源,建立資訊安全聯防體系。

1.1.6 資安緊急應變小組

釋義：資安緊急應變小組主要工作為及危機處理，危機處理則需要規畫危機處理程序、執行危機應變措施與通報，並進行事後分析及防範之工作。
資安業者必須能夠協助企業建立資安緊急應變小組，協助建立相關程序，提供緊急應變相關軟硬體設施，並能配合進行緊急應變處理等。

1.1.7 個資保護程序

釋義：規範個人資料之蒐集、處理及利用，個資法的核心是為了避免人格權受侵害，並促進個人資料合理利用。
資安業者必須能夠協助企業建立個資保護程序，並能有效進行個資保護的工作。

1.1.8 個資去識別化機制

釋義：去識別化是指資料能以代碼、匿名或隱藏的方式或其他方式，使得其他人無從識別為特定個人，去識別化之資料即非個資，能夠開放使用。
資安業者必須能夠協助企業建立去識別化標準程序，並能有效進行去識別化的工作。

1.2 資訊安全或個人資料管理系統驗證分項

1.2.1 資訊安全管理系統驗證

釋義：即是以驗證客戶的資訊安全管理系統為目的的驗證稽核。
資安業者必須為符合該標準組織所認可之合格驗證機構。

1.2.2 個人資料管理系統驗證

釋義：即是以驗證客戶的個人資料管理系統或隱私權標章為目的的驗證稽核。
資安業者必須為通過該個人資料管理系統或隱私權標章機構認可之合格驗證機構。

1.3 資訊安全防護能力分析與評估分項

1.3.1 執行弱點掃描分析作業

釋義：所謂弱點掃描分析是指使用自動化掃描工具對於網站或資訊系統之安全弱點或漏洞進行大規模的偵測活動，並能提供統計報表及適當修補建議。
資安業者必須有能力協助組織使用自動化掃描工具，對於組織網站或資訊系統進行大規模的偵測活動，尋找組織資訊安全弱點或漏洞，提供掃描結果統計報表與

明確說明，並能提出建議與改善作法。

1.3.2 評估資訊安全治理成熟度

釋義：所謂資訊安全治理是指能夠協助建立資訊安全治理架構，並能指導、監督與評估資訊安全治理架構之活動；評估資訊安全治理成熟度即是指評估資訊安全治理架構運作，確認達到成熟度的何種等級。資訊安全治理架構與成熟度等級須符合行政院資通安全會報之「政府機關資安治理成熟度評估機制規劃」之內容要求。
資安業者必須能夠協助組織建立資訊安全治理架構與成熟度評估機制，並協助組織進行成熟度評估作業，最後能夠提出改善計畫。

1.3.3 提供事件分析服務

釋義：當組織遭受重大資安事件時，能夠提供事件分析服務，找出事件發生根因，並提出改善計畫。
資安業者必須能夠協助組織在最快時間內，收集資訊並進行分析，找出事件根因並提出改善計畫。

1.3.4 提供資安事件因應及復原服務

釋義：當組織遭受重大資安事件時，能夠採取因應措施並快速回復正常運作。
資安業者必須能夠協助企業建立事件回應之標準作業程序與回應機制，並能依據標準作業程序與機制協助企業快速回復正常運作。

1.3.5 政府組態基準(GCB)檢測與評估服務

釋義：資安業者必須能夠協助企業或組織政府組態基準檢測、排除技術問題、並建立管理機制以維護組態維護與更新。

1.3.6 紅隊演練(Red Team Assessment)資安攻防模擬檢測服務

釋義：紅隊演練 (Red Team Assessment) 是在不影響組織正常營運的條件下，對組織的資訊設施進行模擬的入侵，在有限的時間內達成與組織約定的測試任務。
資安業者必須能夠協助組織進行全面的資安檢測，找出潛在的資安漏洞與立即性的風險，並協助提出改善計畫。

1.3.7 分散式阻斷服務攻擊(DDoS)攻擊演練服務

釋義：分散式阻斷服務(DDoS，Distributed Denial-of-Service)的攻擊會透過大量的服務請求來癱瘓組織的資訊網路系統，造成服務的中斷與損失，組織除了建置防禦機制之外，還可以透過 DDoS 攻擊演練服務來測試防禦機制是否有效。
資安業者必須能夠依據議定的攻擊方式，對接受服務的組織進行 DDoS 攻擊演練，並提供演練計畫書、演練結果報告文件。

1.3.8 特權帳號檢測服務

釋義：了解並分析特權帳號的使用行為，可以讓資安建立基本的防護，透過檢測評估特權帳號使用衍生的風險，促成組織落實特權帳號的盤點與管理。
資安業者透過工具與技術提供特權帳號檢測服務，讓組織了解其特權帳號的使用狀況以及潛在的威脅與風險。

1.4 資訊安全營運管理服務分項

1.4.1 資安監控中心(SOC)服務

釋義：資訊安全監控中心（Security Operation Center, SOC）也常稱為資安維運中心或資安營運中心，採取集中的方式監控組織資訊安全的狀況。透過整合與管理組織的資安訊息，對資安事件依照管控機制進行緊急的應變措施，並整合與分析資安事件。
資安業者應協助組織維運資訊安全監控中心，並依據組織設定的資安要求持續運作。

1.4.2 託管式資安管理與應變(MSS)服務

釋義：託管式資安管理與應變(MSS，Managed Security Service) 是為組織提供資安管理及應變的委外服務，由資安管理與應變廠商(MSSP)的專業人員規劃與協助 MSS 服務的客戶進行資安管理及應變。
資安業者應依據組織的資安提供資安管理及應變的委外服務， 並且達成議定合約的要求。

1.4.3 託管式偵測與應變(MDR)服務

釋義：託管式偵測及回應 (MDR，Managed Detection and Response) 是為組織提供資安威脅追蹤及應變的委外服務，由廠商的專業人員協助 MDR 服務的客戶監控網路、分析事件，並且處理各種資安狀況。
資安業者應依據組織的資安提供資安威脅追蹤及應變的委外服務， 並且達成議定合約的要求。

1.5 網路傳輸安全防護服務分項

1.5.1 入侵偵測與防禦服務

釋義：入侵偵測(IDS, Intrusion Detection System)與入侵防禦(IPS, Intrusion Prevention System)是指能夠偵測網路與網路上資料傳輸的行為，並對所獲得的資訊進行研判、比對，然後檢測出系統的異常行為或侵入的企圖，並能夠即時中斷、調整或隔離不正常或有傷害的網路資料傳輸行為。
資安業者必須能夠協助組織進行入侵偵測與防禦，並能夠即時中斷、調整或隔離不正常或有傷害的網路資料傳輸行為。

1.5.2 流量監控與防護服務

釋義：流量監控，協助組織掌握網路資料量傳輸的大小與效能，在安全防護上，能夠偵測出異常或超大量的流量，也內建於網路防火牆，透過服務鏈的方式，整合網路安全閘道，以確保組織上網的安全。
資安業者必須夠提供工具協助組織進行流量監控與防護，並能夠針對異常或超大量的流量進行改善之工作。

1.5.3 網路組態設定服務

釋義：組態設定在於規範組織網路終端設備一致性的安全設定，包括網路上的裝置、連結方式與配置等，降低網路被入侵或破壞的機會。
資安業者必須協助組織規劃網路各項組態設定，以利協助組織對於資訊安全之管控。

1.5.4 進階威脅保護服務

釋義：進階威脅是針對網路、端點或電子郵件進行的複雜攻擊。進階威脅防護則是結合多種類型的安全技術，能夠執行不同的角色，但仍能結合在一起完成防護的工作。
資安業者必須提供組織進階威脅保護檢測之服務，並快速排除攻擊行為。

1.5.5 弱點與漏洞管理服務

釋義：網路安全的弱點大致上分為「系統及程式本身的漏洞」及「管理疏失」，企業需要隨時進行檢測與修補之工作，以避免網路駭客與病毒的攻擊。
資安業者必須提供組織內部管理程序、軟硬體系統與應用程式與進行檢測，並針對網路安全弱點和漏洞進行分析，進而提供組織相關防護的解決方案。

1.6 資訊系統安全防護服務分項

1.6.1 整合病毒與惡意程式防護服務

釋義：電腦病毒或惡意程式，是一種在人為或非人為、在用戶不知情或未允許的情況下，能自我複製或運行的電腦程式；其目的為破壞電腦的正常運作，或是偷取用戶資料等。
資安業者必須針對病毒或惡意程式提供組織防護機制或整合方案，協助組織免除病毒及惡意程式之威脅。

1.6.2 滲透測試服務

釋義：滲透測試是由安全專家模擬駭客的攻擊行為，測試資訊系統的安全強度，讓組織提早發現潛在漏洞，並予以修復。
資安業者必須能夠進行各種模擬攻擊的滲透測試工作，協助組織找出資訊安全之

漏洞，並提交滲透測試報告。

1.6.3 程式源碼安全服務

釋義：源碼檢測或稱原始碼檢測 (Source Code Analysis) 是針對程式的原始程式碼，透過人工或是自動化檢測工具，尋找程式撰寫過程中潛在的漏洞，並提出修復方法。
資安業者必須能夠針對組織各類程式源碼進行安全性檢測，找出系統發展時所忽略之安全漏洞，提供組織據以修復之依據。

1.6.4 電腦稽核服務

釋義：稽核是指對於組織運作流程與資訊進行抽樣、勾稽、比對與分析。電腦數位稽核是指利用電腦輔助稽核技術與工具進行稽核工作的程序與方法，稽核範圍涵蓋資訊系統相關作業流程。
資安業者必須提供電腦數位稽核技術與工具，由第三方角度協助組織確認內部資訊作業是否依據既定程序執行，並提出電腦稽核發現事項。

1.6.5 進階威脅保護服務

釋義：進階威脅是針對網路、端點或電子郵件進行的複雜攻擊。進階威脅防護則是結合多種類型的安全技術，能夠執行不同的角色，但仍能結合在一起完成防護的工作。
資安業者必須提供組織進階威脅保護檢測之服務，並快速排除攻擊行為。

1.7 資料安全防護服務分項

1.7.1 資料庫安全管理與防護服務

釋義：資料庫為組織內結構化的資料，當資料在操作、傳輸與儲存過程中，可能面臨資料遺失與外洩之風險，因此對於資料操作過程中，必須使用資安技術與工具管控並保護組織的資料。
資安業者必須能夠針對組織資料庫進行管理、預防與偵測之工作，管理工作包括資料庫設定與組態管理、資料安全分類管理與定期安全掃描;預防工作包括加密、憑證與存取控管；偵測工作則包括活動監控、事件管理與資料外洩防護。

1.7.2 電子郵件安全管理與防護服務

釋義：電子郵件資安威脅包含釣魚詐騙、附件勒索軟體、偽網頁郵件、暴力攻擊與阻斷攻擊等。組織需要阻絕電子郵件資安威脅，進行安全管理，才能有效正常營運。
資安業者必須能夠協助組織建立電子郵件安全控管措施，並使用工具阻絕各種電子郵件攻擊方式，執行控管工作，並持續監督與維護。

1.7.3 網路內容安全管理與防護服務

釋義：網路內容安全管理包含用戶對於網頁內容的存取、員工上網管理與即時通訊軟體使用管理等，組織必須阻絕來自惡意程式、後門程式、垃圾郵件夾帶病毒、釣魚網站等攻擊。組織必須做好管控，隔絕資料外洩或遭到破壞的可能，因此需要持續進行網路上的內容管控。
資安業者必須提供組織針對網路內容安全的項目進行檢測與防護，確保組織網路內容之安全與正常運作。

1.7.4 電子資料安全管理與防護服務

釋義：電子資料包含組織資料庫、電子郵件、文書檔及相關的文字、影音檔等，電子資料安全管理在於阻絕不正常電子資料的存取、竄改與破壞。
資安業者必須能夠協助組織建立電子資料內容安全的存取控制，並經常進行檢測與防護，阻絕不正常的存取、竄改與破壞，確保組織電子資料之安全。

1.7.5 資料倉儲安全與防護服務

釋義：資料倉儲是將組織內異質性的資料加以儲存、合併與抽出使用，來輔助決策分析。資料倉儲安全檢測與防護是指對於資料倉儲之設備、內存資訊進行安全防護工作，包括針對資料倉儲進行安全監控、不當使用之偵測、限定資料倉儲之資料檔案的使用權、監測使用情況，進行去識別化工作，並即時資訊統計與回應之產品與服務。
資安業者必須針對資料倉儲的安全性，提供組織安全監控、偵測、使用管理與去識別化，即時資訊統計與回應之服務，確保倉儲中的資料不會被盜取及修改，進而影響組織運作。

1.8 數位鑑識採證與分析服務分項

1.8.1 電腦系統鑑識採證與分析服務

釋義：電腦系統鑑識，即是保存、識別、抽取、記載及解讀電腦系統上所遺留之資訊，包含各種檔案與資料庫之資訊，這些資訊稱為數位證據(Digital Evidence or Cyber Evidence)。並對這些數位證據進行分析其成因。
資安業者必須提供企業分析工具，進行保存、識別、抽取、記載及解讀電腦資訊，針對所面對的威脅，做進一步的鑑識與分析，以利協助組織解決資安的問題。

1.8.2 網路鑑識採證與分析服務

釋義：網路鑑識是監測、捕捉、紀錄與分析網路數據封包，比對系統日誌，進行流量分析，找出資安事件之成因。
資安業者必須提供企業分析工具，進行網路監測、捕捉、紀錄與分析網路數據封包，針對所面對的威脅，做進一步的鑑識與分析，以利協助組織解決資安的問題。

1.8.3 行動裝置鑑識採證與分析服務

釋義：行動裝置鑑識是指對於行動裝置上的資料進行保存、識別、抽取、記載及解讀，並對這些數位證據進行分析其成因。
資安業者必須提供企業軟體分析工具，能夠從行動裝置中取得資料，進行保存、識別、抽取、記載及解讀，針對所面對的威脅，做進一步的鑑識與分析，以利協助組織解決資安的問題。

1.9 行動與雲端安全防護服務分項

1.9.1 行動應用程式安全與防護服務

釋義：行動應用程式安全包括程式的發佈與更新、個人資料使用認證、連線管理、付費機制、程式碼安全及伺服器端的資訊安全等；組織必須確保使用者下載或是執行時相關傳輸與資訊的安全。
資安業者必須提供組織針對行動應用程式與伺服器端進行檢測及防護，確保組織對於所提供應用程式的交易資料、個人資料與伺服器端資料的安全。

1.9.2 雲端安全與防護服務

釋義：雲端安全包括針對雲端服務供應商及雲端使用者資訊安全的防護，雲端安全檢測與防護包括能夠對於資料外洩與遺失、帳號劫持、阻絕服務、服務濫用等威脅進行檢測與防護工作。
資安業者必須能夠提供雲端服務供應商及雲端使用者針對雲端應用程式、雲端平台與相關資料持續進行檢測與防護，確保雲端運算與重要雲端資料的安全性。

1.10 物聯網安全防護服務分項

1.10.1 物聯網產品安全與防護服務

釋義：物聯網產品指的是產品本身提供短距離或長距離的通訊功能，能夠透過網際網路進行產品操作與資料傳輸。物聯網產品安全檢測與防護是指對於物聯網產品使用過程中所產生的資料遺失、操作失當、控制權轉移、阻斷攻擊及勒索等威脅進行安全防護工作。
資安業者必須提供組織進行物聯網產品與物聯網產品使用過程所引發的安全性議題進行檢測與防護，確保物聯網產品使用的安全性。

1.10.2 智慧聯網安全與防護服務

釋義：智慧聯網是透過大量感知器進行資料收集與分析，或者透過機器彼此間的資料交換進行複雜的控制與自動化運作的智慧系統。智慧聯網安全檢測與防護是指必須持續監控與防護智慧聯網系統的運作，以免於遭遇侵入與進行不當行為的控制、攻擊與破壞。
資安業者必須提供組織智慧聯網系統端點的安全檢測、防範資料竄改與遺失、監

控與防護系統的正常運作，避免系統遭遇侵入與攻擊等。

1.11 電信通訊安全與防護服務分項

1.11.1 電信通訊設備與防護服務

釋義：是指對於通訊無線接取設備、控制器、路由器與交換器等設備進行安全功能檢測，並提供防護解決方案。
資安業者必須協助組織進行檢測，尋找通訊設備可能的安全漏洞，並提出防護解決方案。

1.11.2 通訊軟體安全與防護服務

釋義：是指對於手機之通訊軟體進行資通安全防護或檢測，以保護資料的使用、儲存及傳輸並阻絕核心底層的非法存取資訊。
資安業者必須提供組織檢測或防護工具，對於通訊軟體進行的安全檢測、監控或防護，避免資料被非法存取。

1.12 運轉控制系統安全與防護服務分項

1.12.1 運轉控制系統安全防護規劃服務

釋義：運轉控制系統安全防護規劃是指對於運轉控制系統制訂資訊安全政策與執行程序、建置安全的防護環境並定期執行入侵偵測、弱點掃描與稽核。
資安業者必須能夠協助組織制訂資訊安全政策、程序、建置安全的防護環境並定期執行安全程序與稽核。

1.12.2 運轉控制系統關鍵基礎設施檢測與防護服務

釋義：運轉控制系統關鍵基礎設施檢測與防護是指對於基礎架構進行定期檢測，評估可能存在的安全漏洞並發現可能的異常活動或判斷是否遭遇惡意入侵。
資安業者必須能夠協助組織進行相關的檢測與評估活動，並能提供相關的檢測與防護服務，例如資安健診、系統隔離性檢測、滲透測試與資安監控等服務。

1.12.3 運轉控制系統資安健診服務

釋義：針對運轉控制系統進行網路架構檢視、有線網路惡意活動檢測、使用者端電腦檢測、伺服器主機檢測及安全設定檢測等資安健診服務。
資安業者須能依議定之合約提供資安健診服務以及結果的分析報告。

1.12.4 運轉控制系統隔離性檢測服務

釋義：運轉控制系統可能會因為所採用的資訊系統而招致入侵，透過隔離性檢測可以發現這些可能存在的入侵弱點，進而排除達到隔離的效果。

資安業者須能執行運轉控制系統隔離性檢測，發現入侵的突破點，並提供解決的方法。

1.12.5 運轉控制系統滲透測試服務

釋義：模擬駭客的攻擊行為，測試運轉控制系統的安全強度，提早發現潛在漏洞，並予以修復。
資安業者須能進行各種模擬攻擊的滲透測試工作，找出運轉控制系統之資安漏洞，並提交滲透測試報告。

1.12.6 運轉控制系統資安監控服務

釋義：針對運轉控制系統進行監控環境部署、監控服務、資安事件處理及資安威脅預警等資安服務，網路與主機為資安監控服務的主要範圍。
資安業者須能依議定之合約提供運轉控制系統的資安監控服務。

1.13 提供資訊安全教育訓練分項

1.13.1 資訊安全意識教育訓練

釋義：即是針對組織資訊安全的需求，提升組織內部人員資訊安全意識的教育訓練。
資安業者必須有能力與師資，能夠針對資訊安全進行認知提升之相關訓練課程並提供師資進行教育訓練之工作。

1.13.2 資訊安全管理與法規教育訓練

釋義：即是針對組織資訊安全的需求，提供資訊安全管理架構以及相關法令法規的教育訓練。
資安業者必須有能力與師資，能夠針對組織需求發展資訊安全及相關法規之訓練課程，並提供師資進行教育訓練之工作。

1.13.3 資訊安全技術教育訓練

釋義：即是針對資訊安全防護，提供產品或技術教學之教育訓練。
資安業者必須有能力與師資，能夠資訊安全相關之產品或技術之訓練課程並提供師資進行教育訓練之工作。

(二)資訊安全產品服務項目

2.1 網路傳輸防護產品分項

2.1.1 防火牆產品

釋義：用以隔離公司內外部網路環境的軟體、硬體或軟硬體整合之產品，通常能協助封鎖企圖從網際網路存取網路內容的惡意使用者、病毒及蠕蟲；對於具有防禦入侵、網頁過濾、垃圾郵件過濾、網路負載與頻寬管制等功能的產品均屬於防火牆產品。

2.1.2 網頁應用程式防火牆產品

釋義：用以防禦針對網頁應用程式的攻擊活動，需設定安全規則，可以阻絕違反安全規則的封包，並分析應用層的網路流量及其內容，協助保護網頁應用程式之安全性，這類產品皆屬網頁應用程式防火牆產品。

2.1.3 虛擬私有網路防護產品

釋義：虛擬私有網路(Virtual Private Network, VPN)指的是在公共網際網路上使用加密通道建立一個私人且安全的網路。VPN 防護產品係指加密(Encryption)、認證(Authentication)、密鑰(Key)管理、數位憑證(Digital Certification)等加密的安全標準之相關產品。

2.1.4 無線網路安全產品

釋義：無線網路可透過開放的、無形的電波傳遞資料，因此可以輕易地被竊取，造成安全的威脅顧慮。無線網路安全產品泛指可以進行無線網路瀏覽器認證、IP 位址與 DNS 伺服器位址、無線網路識別碼(SSID)等機制的管控、流量監測與活動監督等之產品。

2.1.5 側錄偵測產品

釋義：側錄程式可記錄使用者在鍵盤上的動作內容，將資料傳送給惡意使用者，特別是在電腦上輸入個人身分認證或金融相關的認證資料。側錄偵測產品是指可以偵測被植入的側錄程式，或敦促使用者經常更換密碼、提醒儘速登出帳號，降低資料被不當攔截的機率之產品。

2.1.6 阻斷服務攻擊防禦產品

釋義：阻斷服務攻擊泛指利用殭屍網路或攻擊系統弱點、常伴隨著發送大量合法或偽造之請求，占用大量網路及設備資源，以達到癱瘓網路、延緩伺服器主機系統回應，造成組織商機流失之目的。能透過監測伺服器的資源及流量，主動且正確的判別是否為阻斷攻擊、即時回報伺服器回應與服務效率，進一步提供動態伺服器資源配置，優化網路品質的產品皆屬之。

2.1.7 入侵偵測與防禦產品

釋義：係指可即時監控、偵測與防禦攻擊事件的發生，並根據管理人員的設定，中止或阻絕入侵行為，涵蓋自動攔截棄置攻擊封包，留下攻擊活動之記錄、即時通知管理者等一系列應變措施之產品。

2.1.8 加密流量管理產品

釋義：透過加密的網路流量日漸增加，組織必須針對 SSL 網路流量進行解密、檢測與協調，並進行分析。SSL 加密流量管理產品必須能夠監看通訊閘道流量，並進行解密、分析，同時不影響網路運作效能。

2.1.9 網域名稱系統(DNS)通道資料外洩偵防系統

釋義：DNS 協定的弱點會造成隱藏通道的建構，進而使資料外洩，DNS 通道資料外洩偵防系統相關的產品可以偵查這一類的通道並進行阻絕，避免機敏資料外洩。

2.1.10 政府組態基準(GCB)檢測產品

釋義：能針對端點設備進行檢測，測試是否符合 GCB 組態設定值之產品皆屬之。

2.2 應用系統防護產品分項

2.2.1 防毒與惡意程式防護產品

釋義：電腦病毒或以破壞為目的的惡意程式，感染、寄生或附著於特定電腦程式或文件檔案中，干擾系統或網路正常之運作。防毒與惡意程式防護產品是指凡具備掃描、偵測、阻止電腦病毒或惡意程式進行攻擊或破壞之軟體均屬此類。

2.2.2 主機安全防護產品

釋義：凡是能夠針對主機進行有效檢查與過濾網路流量，防禦阻斷服務攻擊，設定威脅防護規則，以偵測與回應外部攻擊，均屬於主機安全防護產品。

2.2.3 弱點掃描與檢測產品

釋義：協助管理者分析與掌握其所管理的資訊軟硬體設備是否存在漏洞，進而修補漏洞、並將漏洞所造成的風險降到最低的方式。弱點掃描與檢測產品可持續且系統性的進行完整而徹底的健康檢查，以利於改善資安架構、加強防護水準、降低整體安全風險。

2.2.4 網頁內容存取控制產品

釋義：以針對資訊設備的不同使用者設定過濾器(filter)，防止電腦上的使用者存取網際網路上的不當內容(暴力、色情、機密等)。意即限定不同權限的使用者得以存取特定網頁內容，並且監控與管制其使用程度之相關產品皆屬之。

2.2.5 人員身分與存取控制產品

釋義：係指對於資訊軟硬體設備、軟體與系統使用範圍、帳號增減與異動、人員權限設定、身份界定、密碼管理等，與使用權、權限所有權相關的管理機制之產品。

2.2.6 憑證註冊管理系統產品

釋義：協助組織建立憑證管理系統、註冊管理系統、目錄伺服器對憑證作業流程執行嚴密的管理，提供憑證管理服務。凡是能夠提供申請者註冊、憑證的簽發、廢止、管理、產生稽核紀錄等管理機制與功能之產品皆屬之。

2.2.7 公開金鑰應用產品

釋義：電子憑證所需資訊身份控管、電子簽章、電子加密及資料保密簽章等類型之安全機制,均屬於公開金鑰應用領域。用以在網路上進行通訊雙方身分的確認，防止網路上偽冒、欺騙行為皆屬於公開金鑰應用產品。

2.2.8 郵件安全防護產品

釋義：以電子郵件為保護與偵測的對象，可攔截垃圾郵件、惡意程式與病毒、網路釣魚、對特定郵件內容或收發者可進一步加密與機密性保護、防止勒索軟體或進階持續性威脅攻擊、可發送郵件統計與異常通報之郵件安全管理機制之產品。

2.2.9 沙箱檢測產品

釋義：用以檢測出組織網路環境中，是否被不當的建置可執行惡意程式的作業環境，使得植入此程式的惡意使用者得以觀察該惡意程式所能造成的影響與干擾效果之相關產品。

2.2.10 白名單防禦技術

釋義：透過將合法之應用程式建置一列表，以正面表列方式限制系統僅能夠執行此列表所允許之相關服務，阻擋任何列表外之程式或軟體的執行，稱為白名單防禦技術。

2.3 資料安全防護產品分項

2.3.1 資料庫安全稽核產品

釋義：用以管制組織內員工以合法的身分、權限、透過正常管道，取得資料庫內容的途徑，檢核身份、帳號、權限，監測使用行為，並針對不當資料庫存取的行為，加以警告或阻擋相關的產品與服務。

2.3.2 電子郵件防護產品

釋義：指針對組織或個人，審查其郵件內容、追蹤郵件行為及動態改變，提供管理者有關即時的監控、完整的稽核紀錄，包含對往來郵件的紀錄、備份儲存，以及組織使用 email 資源，包括使用人數、傳送頻寬、流量高峰與低峰、主要傳送內容等服務之產品。

2.3.3 內容過濾產品

釋義:依照組織特定需求,禁止帶有色情或違反組織安全政策的資訊通過防火牆。

避免違法行為、提高保密效果、影響網路頻寬的產品皆屬之。

2.3.4 檔案硬碟加密產品

釋義：針對特定檔案或硬碟裝置，進行加密設定、為特定檔案使用人員進行權限管理的產品與服務。

2.3.5 數位版權管理產品

釋義：係指出版者用來管控容易在短時間內被大量複製、盜版、易於被傳播且需被保護對象的使用權、智慧財產權的數位化技術，以保護數位化內容(包含軟體、音樂、電影、硬體等)的使用權限，並限制不被允許之使用、檢視、拷貝、列印及修改的產品與服務。

2.3.6 資料備份與復原產品

釋義：泛指能達成資料的備份與損毀、遺失的復原，使數位化作業及相關資料得以確保的軟體、硬體之產品與服務。

2.3.7 資料加解密產品

釋義：針對需保密的資料進行資料轉換的加密、解密演算法、使用金鑰進行加密與解密的軟體產品。

2.3.8 資料倉儲資料防護產品

釋義：針對資料倉儲內所儲存的資料檔案進行監控與管制，包括資料存取的使用權、監測使用情況與即時資訊統計與回應，確保倉儲中的資料不會被盜取及修改之產品皆屬之。

2.3.9 資安事件分析產品

釋義：針對安全日誌或使用者行為，進行管理、收集及分析，進而即時分析使事件發生時提供自動化警示之產品皆屬之。

2.3.10 資安事件回應產品

釋義：針對緊急事件協助判斷發生情形與修正方式，提供事件回應團隊做出判斷之產品皆屬之。

2.4 資安管理產品分項

2.4.1 資安事件管理平台

釋義：支援資安事件管理(SIEM，Security Information Event Management)的平台，可收集監控環境中各項設備的事件資訊，並進行關聯分析。

2.4.2 資安威脅分析產品

釋義：能有效匯聚並整合多種來源的資安威脅情資，進行分析與研判的產品。

2.4.3 進階式攻擊防護引擎(APT engine)

釋義：進階持續性滲透攻擊(APT，Advanced Persistent Threat)以多元化的方式，對攻擊的標的進行進階且持續性的探索與攻擊，相關的進階式攻擊防護引擎(APT engine)可以透過各種技術阻斷進階式攻擊的流程，破壞攻擊方採用的規避或是入侵的技巧。

2.5 數位鑑識產品分項

2.5.1 數位鑑識資料備份產品

釋義：可以進行磁碟備份、檢驗與製作資料映像檔之工具產品。

2.5.2 數位鑑識資料收集產品

釋義：可以將磁碟中被刪除、毀損之資料進行檢視、檔案檢視、編輯、全文檢索資料搜尋或復原之工具產品。

2.5.3 密碼破解工具產品

釋義：可以破解作業系統與 BIOS 密碼、星號密碼、文件軟體密碼、壓縮檔密碼等之工具產品。

2.5.4 網路監控與追蹤工具產品

釋義：可以蒐集網路連線紀錄，尋找流量異常與行為異常之主機，紀錄發生之時間，並追蹤來源之工具產品。

2.5.5 數位鑑識產品

釋義：可以進行惡意程式分析、映像檔分析、記憶體分析、瀏覽日誌檔與相關紀錄、關鍵字搜尋與關聯分析等之工具產品。

2.5.6 行動裝置鑑識產品

釋義：能夠從行動裝置中取得資料，進行保存、識別、抽取、記載及解讀之工具產品。

2.6 行動與雲端防護產品分項

2.6.1 行動裝置端點防護產品

釋義：自攜設備(Bring Your Own Device，BYOD)已經是普遍的情況，組織除了需確保傳統的桌上型電腦和筆記型電腦之使用者端的設備安全，更需要管控智慧型

手機、平板電腦等裝置進入組織系統的機制。因此，針對作業系統與應用程式的弱點補強、修補程式的更新與安裝、網路存取控制機制及其限制，均屬於行動裝置端點防護產品的範疇。

2.6.2 行動裝置後門分析與防護產品

釋義：後門程式是利用植入遠端伺服器程式，再從用戶端連線登入進行攻擊的程式。凡是可以監控遠端連線方式登入，管理授權、集中控管使用者電腦環境，避免使用者不當使用、惡意攻擊、並能快速重置、備份、還原使用者端系統、限制使用外接存取設備等均屬於後門分析與防護產品範疇。

2.6.3 雲端防護產品

釋義：當企業在使用虛擬化、容器和雲端時，需保護其虛擬化資料中心、雲端部署以及混合環境。資安業者提供之雲端防護產品，可保護企業之雲端服務或作業流程，如:將防護融入開發營運流程當中、提供威脅防禦技巧以保護執行時期的實體、虛擬和雲端工作負載與容器、或提供部署前容器映像掃瞄皆屬之。

2.7 物聯網防護產品分項

2.7.1 智慧聯網防護產品

釋義：智慧聯網是透過大量感知器進行資料收集與分析，或者透過機器彼此間的資料交換進行複雜的控制與自動化運作的智慧系統。凡是能夠持續監控與防護智慧聯網系統的運作，以免於遭遇侵入與進行不當行為的控制、攻擊與破壞之系統產品皆屬之。

2.7.2 內嵌式系統防護產品

釋義：泛指能夠檢測內嵌式系統之安全性，避免軟體遭到竄改，並能持續監測與管制之產品與服務。

2.8 電信通訊安全防護產品分項

2.8.1 電信通訊安全防護軟硬體

釋義：可針對電信通訊的運作與營運提供安全防護的相關軟硬體。

2.9 運轉控制系統安全防護產品分項

2.9.1 運轉控制系統資安防護產品

釋義：能夠針對運轉控制系統之存取控制、網路監控、資料傳輸與資料備援進行

全面性管理與防護之產品。

2.9.2 運轉控制系統病毒與惡意程式防護產品

釋義：能夠針對運轉控制系統進行掃描、偵測、阻止電腦病毒或惡意程式進行攻擊或破壞之工具產品。

2.10 資安情資產品分項

2.10.1 資安情資分享與分析產品

釋義：協助組織分析資安情資通報、整合與分享資訊功能，自動化接收通報，並進行資訊研判分析之產品皆屬之。

2.11 區塊鏈安全產品分項

2.11.1 區塊鏈安全產品

釋義：區塊鏈係指藉由密碼學串接並保護內容的串連交易記錄。凡可對於區塊鏈之資訊安全進行防護之產品皆屬之。