<table>
<tr><th>項目</th><th>(七) 資通安全防護及控制措施</th></tr>
<tr><td>7.1</td><td>是否依法規定期辦理安全性檢測及資通安全健診?
1.全部核心資通系統辦理弱點掃描（A 級機關：每年 2 次；B 級機關：每年 1 次；C 級機關：每 2 年 1 次）
2.全部核心資通系統辦理滲透測試（A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次）
3.資通安全健診，包含網路架構檢視、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設定檢視等？(A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次)</td></tr>
<tr><td>7.2</td><td>是否針對安全性檢測及資通安全健診結果執行修補作業，且於修補完成後驗證是否完成改善？</td></tr>
<tr><td>7.3</td><td>【A、B 級機關適用】
是否完成政府組態基準導入作業？</td></tr>
<tr><td>7.4</td><td>【A、B 級公務機關應於 111 年 8 月 24 日前或核定後 1 年內完成；C 級公務機關應於 112 年 8 月 24 日前或核定後 2 年內完成】是否完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定方式提交資訊資產盤點資料？是否針對高風險弱點進行修補或執行其他控制措施?</td></tr>
<tr><td>7.5</td><td>【A、B 級公務機關應於 112 年 8 月 24 日前或核定後 2 年內完成】是否完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定方式提交偵測資料？是否偵測異常事件判定為資安事件後有回傳相關資料?</td></tr>
<tr><td>7.6</td><td>是否完成下列資通安全防護措施？
<table>
<tr><th>安全防護項目</th><th>A 級</th><th>B 級</th><th>C 級</th><th>D 級</th></tr>
<tr><td>防毒軟體</td><td>v</td><td>v</td><td>v</td><td>v</td></tr>
<tr><td>網路防火牆</td><td>v</td><td>v</td><td>v</td><td>v</td></tr>
<tr><td>電子郵件過濾機制</td><td>v</td><td>v</td><td>v</td><td></td></tr>
<tr><td>入侵偵測及防禦機制</td><td>v</td><td>v</td><td></td><td></td></tr>
<tr><td>應用程式防火牆
(具有對外服務之核心資通系統者)</td><td>v</td><td>v</td><td></td><td></td></tr>
<tr><td>進階持續性威脅攻擊防禦</td><td>v</td><td></td><td></td><td></td></tr>
</table></td></tr>
<tr><td>7.7</td><td>是否針對電子郵件進行過濾，且定期檢討及更新郵件過濾規則？是否針對電子郵件進行分析，主動發現異常行為且進行改善（如針對大量異常電子郵件來源</td></tr>
</table>

	之 IP 位址，於防火牆進行阻擋等）？是否有電子郵件之使用管控措施，且落實執行？是否依郵件內容之機密性、敏感性規範傳送限制？
7.8	是否建立電子資料安全管理機制，包含分級規則（如機密性、敏感性及一般性等）、存取權限、資料安全、人員管理及處理規範等，且落實執行？
7.9	是否建立網路服務安全控制措施，且定期檢討？是否定期檢測網路運作環境之安全漏洞？
7.10	是否已確實設定防火牆並定期檢視防火牆規則，DNS 查詢是否僅限於指定 DNS 伺服器？有效掌握與管理防火牆連線部署？
7.11	針對機關內部同仁及委外廠商進行遠端維護資通系統，是否採「原則禁止、例外允許」方式辦理，並有適當之防護措施？
7.12	網路架構設計是否符合業務需要及資安要求？是否依網路服務需要區隔獨立的邏輯網域（如 DMZ、內部或外部網路等），且建立適當之防護措施，以管制過濾網域間之資料存取？
7.13	是否針對機關內無線網路服務之存取及應用訂定安全管控程序，且落實執行？
7.14	資通系統重要組態設定檔案及其他具保護需求之資訊是否加密或其他適當方式儲存（如實體隔離、專用電腦作業環境、資料加密等）？是否針對資訊之交換，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性（如採行識別碼通行碼管制、電子資料加密或電子簽章認證等）？是否針對重要資料的交換過程，保存適當之監控紀錄？
7.15	是否建立帳號管理機制，並定期盤點?使用預設密碼登入資通系統時，是否於登入後要求立即變更密碼，並規定密碼強度、更換週期（限制使用弱密碼）？是否是最小權限？是否有使用角色型存取控制？有管理者權限之帳號是否有只用於管理活動？
7.16	是否針對電腦機房及重要區域之安全控制、人員進出管控、環境維護（如溫溼度控制）等項目建立適當之管理措施，且落實執行？
7.17	是否定期評估及檢查重要資通設備之設置地點可能之危害因素（如火、煙、水、震動、化學效應、電力供應、電磁輻射或人為入侵破壞等）？
7.18	是否針對電腦機房及重要區域之公用服務（如水、電、消防及通訊等）建立適當之備援方案？
7.19	是否訂定資訊處理設備作業程序、變更管理程序及管理責任（如相關儲存媒體、設備是否有安全處理程序及分級標示、報廢程序等），且落實執行？是否訂

	定資訊設備回收再使用及汰除之安全控制作業程序，以確保任何機密性或敏感性資料已確實刪除？
7.20	是否針對使用者電腦訂定軟體安裝管控規則？是否確認授權軟體及免費軟體之使用情形，且定期檢查？
7.21	是否針對個人行動裝置及可攜式媒體訂定管理程序，且落實執行，並定期審查、監控及稽核？
7.22	是否有網路即時通訊管理措施（如機密公務或因處理公務上而涉及之個人隱私資訊，不得使用即時通訊軟體處理及傳送等）？是否有即時通訊軟體安全需求及購置準則？
7.23	【適用行政院所屬公務機關，不論資安責任等級】機關所維運對外或為民服務網站，是否採取相關 DDoS 防護措施（例如靜態網頁切換、CDN、流量清洗或建置 DDoS 防護設備等），並確認其有效性?
7.24	機關是否對雲端服務應用進行相關資安防護管理?