資通安全實地稽核項目檢核表(適用特定非公務機關)

機關名稱：_____

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(一) 核心業務及其重要性							
1.1	是否界定機關之核心業務，完成資通系統之盤點及分級，且每年至少檢視 1 次分級之妥適性？						
1.2	是否將全部核心資通系統納入資訊安全管理系統(ISMS)適用範圍？ (A、B 級機關：全部核心資通系統 2 年內完成 ISMS 導入，3 年內通過公正第三方驗證，第三方核發之驗證證書應有 TAF 認證標誌；C 級機關：全部核心資通系統 2 年內完成 ISMS 導入)						
1.3	是否盤點核心資通系統，鑑別可能造成營運中斷事件之機率及衝擊影響，且進行營運衝擊分析(BIA)？是否明確訂定核心資通系統之系統復原時間目標(RTO)及資料復原時間點目標(RPO)？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
1.4	是否設置資通系統之備援設備，當系統服務中斷時，於可容忍時間內由備援設備取代提供服務？(資通系統等級中/高等級者適用)						
1.5	是否定期執行重要資料之備份作業，且備份資料異地存放？存放處所環境是否符合實體安全防護？						
1.6	是否訂定備份資料之復原程序，且定期執行回復測試，以確保備份資料之有效性？復原程序是否定期檢討及修正？						
1.7	是否針對核心資通系統制定業務持續運作計畫，並定期辦理全部核心資通系統之業務持續運作演練，包含人員職責應變、作業程序、資源調配及檢討改善等？(A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次)						
1.8	是否針對重要業務訂定適當之變更管理程序，且落實執行，並定期檢視、審查及更新程序(如業務調整後對外資訊更新等)？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(二) 資通安全政策及推動組織							
2.1	是否訂定資通安全政策及目標，由管理階層核定，並定期檢視且有效傳達其重要性？						
2.2	是否訂定資通安全之績效評估方式(如績效指標等)，且定期監控、量測、分析及檢視？						
2.3	是否有文件或紀錄佐證管理階層(如機關首長、資通安全長等)對於 ISMS 建立、實作、維持及持續改善之承諾及支持？						
2.4	是否成立資通安全推動組織，負責推動、協調監督及審查資通安全管理事項？推動組織層級之適切性，且業務單位是否積極參與？						
2.5	是否指派適當層級人員兼任資通安全管理代表，負責推動及督導機關內資通安全相關事務？						
2.6	是否建立機關內、外部利害關係人清單，並定期檢討其適宜性？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(三)、專責人力及經費配置							
3.1	資安經費占資訊經費比例？資訊經費占機關經費比例？資安經費編列是否符合業務需要？						
3.2	資通安全專責人員配置情形？是否有適切分工？ (A 級機關：4 人；B 級機關：2 人；C 級機關：1 人)						
3.3	是否指定專人或專責單位負責資訊服務請求/事件處理、維運及檢討，且有適切分工？						
3.4	是否訂定人員之資通安全作業程序及權責？是否明確告知保密事項，且簽署保密協議？						
3.5	人員是否瞭解機關之資通安全政策，以及應負之資安責任？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
3.6	資通安全專責人員是否每年接受 12 小時以上之資通安全專業課程訓練或資通安全職能訓練？(A、B、C 級機關適用)						
3.7	資通安全專責人員以外之資訊人員是否每 2 年接受 3 小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受 3 小時以上之資通安全通識教訓練？(A、B、C 級機關適用)						
3.8	一般使用者及主管是否每年接受 3 小時以上之資通安全通識教育訓練？						
3.9	資通安全專責人員是否各自持有資通安全專業證照 1 張以上，且維持證照之有效性？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(四) 資訊及資通系統盤點及風險評估							
4.1	是否確實盤點資產建立清冊(如識別擁有者及使用者等)，且鑑別其資產價值？						
4.2	是否訂定資產異動管理程序，定期更新資產清冊，且落實執行？						
4.3	是否建立風險準則且執行風險評估作業，並針對重要資訊資產鑑別其可能遭遇之風險，分析其喪失機密性、完整性及可用性之衝擊？						
4.4	是否訂定風險處理程序，選擇適合之資通安全控制措施，且相關控制措施經權責人員核可？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
4.5	是否訂定資通安全風險處理計畫，且妥善處理剩餘之資通安全風險？						
4.6	是否配合新增業務或組織調整時，適時檢視原風險評估作業，以確保相關控制措施之有效性？						
4.7	針對公務用之資通訊產品，包含軟體、硬體及服務等，是否已禁止使用大陸廠牌資通訊產品？						
4.8	是否列冊管理大陸廠牌資通訊產品，並已於 110 年底前將該產品自公務環境中移除？如該產品仍有與公務環境介接之情況，是否經行政院核定評估同意？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(五) 資通系統或服務委外辦理之管理措施							
5.1	是否訂定資訊作業委外安全管理程序，包含委外選商及監督相關規定，確保委外廠商執行委外作業時，具備完善之資通安全管理措施或通過第三方驗證？						
5.2	機關及委外廠商是否皆已指定專案管理人員，負責推動、協調及督導委外作業之資通安全管理事項？						
5.3	委外廠商是否配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員？						
5.4	是否針對委外業務項目進行風險評估，包含可能影響資產、流程、作業環境或特殊對機關之威脅等，以強化委外安全管理？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
5.5	是否依委外業務項目之性質允許委外廠商就委外業務項目分(轉)包？如允許分(轉)包，是否注意分(轉)包之範圍，以及分(轉)包之廠商是否具備資通安全維護措施？						
5.6	是否依資通系統分級，於徵求建議書文件(RFP)相關採購文件中明確規範防護基準需求？						
5.7	對於核心資通系統之委外廠商，是否針對其人員(如能力、背景等)及開發維運環境之資通安全管理進行評估？						
5.8	委外客製化資通系統開發者，是否要求委外廠商提供資通系統之安全性檢測證明，並針對非委外廠商自行開發之系統或資源，標示非自行開發之內容與其來源及提供授權證明？若該資通系統屬核心資通系統或委託金額達新臺幣一千萬元以上者，是否自行或另行委託第三方進行安全性檢測之複測？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
5.9	是否訂定委外廠商對於機關委外業務之資安事件通報及相關處理規範？委外廠商執行委外業務，違反資通安全相關法令或知悉資通安全事件時，是否立即通知機關並採行補救措施？						
5.10	委外關係終止或解除時，是否確認委外廠商返還、移交、刪除或銷毀履行契約而持有之資料？						
5.11	是否訂定委外廠商之資通安全責任及保密規定，且落實執行？						
5.12	是否定期或於知悉委外廠商發生可能影響委外作業之資通安全事件時，對委外廠商所提供之服務、報告及紀錄等進行管理及安全檢視(如廠商端實地稽核、要求廠商提供異常報告、要求廠商提供相關安全檢測紀錄等)，以利後續追蹤及管理？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
5.13	委外廠商專案成員進出機關範圍是否被限制？對於委外廠商駐點人員使用之資訊設備(如個人、筆記型、平板電腦、行動電話及智慧卡等)是否建立相關安全管控措施？						
5.14	是否訂定委外廠商系統存取程序及授權規定(如限制其可接觸之系統、檔案及資料範圍等)？委外廠商專案人員調整及異動，是否依系統存取授權規定，調整其權限？						
5.15	是否定期檢視並分析資訊作業委外之人員安全、媒體保護管控、使用者識別及鑑別、組態管控等相關紀錄？						
5.16	針對涉及資通訊軟體、硬體或服務相關之採購案，契約範圍內之委外廠商是否為大陸廠商或所涉及之人員是否有陸籍身分？是否允許委外廠商使用大陸廠牌之資通訊產品，包含軟體、硬體及服務等？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(六) 資通安全維護計畫與實施情形之持續精進及績效管理機制							
6.1	是否訂定、修正及實施機關資通安全維護計畫，且每年向上級或監督/主管機關提出資通安全維護計畫實施情形？						
6.2	是否落實管理階層(如機關首長、資通安全長等)定期(每年至少 1 次)審查 ISMS，以確保其運作之適切性及有效性？						
6.3	是否訂定內部資通安全稽核計畫，包含稽核目標、範圍、時間、程序、人員等，且落實執行？ (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)						
6.4	是否規劃及執行稽核發現事項改善措施，且定期追蹤改善情形？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
(七) 資通安全防護及控制措施							
7.1	是否針對全部核心資通系統定期辦理弱點掃描？(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)						
7.2	是否針對全部核心資通系統定期辦理滲透測試？(A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次)						
7.3	是否定期辦理資通安全健診，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)						
7.4	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？						

<table>
<tr><th>稽核項目</th><th>資通安全稽核檢核項目</th><th>符合</th><th>部分符合</th><th>不符合</th><th>不適用</th><th>簡述符合、部分符合、不符合或不適用之原因</th><th>紀錄文件</th></tr>
<tr><td>7.5</td><td>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？(A、B 級關鍵基礎設施提供者應於核定後 1 年內完成；C 級關鍵基礎設施提供者應於核定後 2 年內完成)</td><td></td><td></td><td></td><td></td><td></td><td></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><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.7	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之 IP 位址，於防火牆進行阻擋等)？						
7.8	是否建立電子資料(含防疫個資)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，有效掌握與管理防火牆連線部署？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
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)？是否針對系統與資料傳輸之機密性與完整性建立適當之防護措施？						
7.15	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，並限制使用弱密碼？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.16	是否訂定電子郵件之使用規則，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？						
7.17	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？						
7.18	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)？						
7.19	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？						
7.20	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.21	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，且落實執行？						
7.22	是否針對電子資料相關設備進行安全管理(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)？						
7.23	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？						
7.24	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？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
7.25	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？						
(八) 資通系統發展及維護安全							
8.1	針對自行或委外開發之資通系統是否依資通系統防護需求分級原則完成資通系統分級，且依資通系統防護基準執行控制措施？						
8.2	資通系統開發過程請是否依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求？						
8.3	資通系統開發前，是否設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等，且檢討執行情形？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
8.4	資通系統設計階段，是否依系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估？						
8.5	資通系統開發階段，是否避免常見漏洞(如 OWASP Top 10 等)？且針對防護需求等級高者，執行源碼掃描安全檢測？						
8.6	資通系統測試階段，是否執行弱點掃描安全檢測？且針對防護需求等級高者，執行滲透測試安全檢測？						
8.7	資通系統上線或更版前，是否執行安全性要求測試，包含邏輯及安全性驗測、機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試等，且檢討執行情形？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
8.8	資通系統開發如委外辦理，是否將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約？						
8.9	是否將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安保護措施？						
8.10	是否儲存及管理資通系統發展相關文件？儲存方式及管理方式為何？						
8.11	資通系統測試如使用正式作業環境之測試資料，是否針對測試資料建立保護措施，且留存相關作業紀錄？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
8.12	是否針對資通系統所使用之外部元件或軟體，注意其安全漏洞通告，且定期評估更新？						
(九) 資通安全事件通報應變及情資評估因應							
9.1	是否訂定資安事件通報作業規範，包含判定事件等級之流程及權責、事件影響及損害評估、內部通報流程、通知其他受影響機關之方式、通報窗口及聯繫方式等，並規範於知悉資通安全事件後 1 小時內進行通報，若事件等級變更時應續行通報？相關人員是否熟悉相關程序，且落實執行？						
9.2	是否訂定資安事件應變作業規範，包含應變小組組織、事前之演練作業、事中之損害控制機制、事後之復原、鑑識、調查及改善機制、相關紀錄保全等，且落實執行？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.3	是否建立資安事件相關證據資料保護措施，以作為問題分析及法律必要依據？						
9.4	近 3 年重大資安事件之通報時間、過程、因應處理及改善措施，是否依程序落實執行？						
9.5	是否訂定資安事件處理過程之內部及外部溝通程序？						
9.6	針對所有資安事件，是否保留完整紀錄，並與其他相關管理流程連結，且落實執行後續檢討及改善？						
9.7	是否建置資通安全威脅偵測管理(SOC)機制？監控範圍是否包括「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄？(A、B 級機關適用)						
9.8	是否訂定應記錄之特定資通系統事件(如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等)、日誌內容、記錄時間週期及留存政策，且保留日誌至少 6 個月？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.9	是否依日誌儲存需求，配置所需之儲存容量，並於日誌處理失效時採取適當行動及提出告警						
9.10	針對日誌之是否進行存取控管，並有適當之保護控制措施						
9.11	知悉資通安全事件後，是否於規定時間內完成損害控制或復原作業，並持續進行調查及處理,於 1 個月內送交調查、處理及改善報告，且落實執行？ (第一級或第二級事件：72 小時內完成損害控制或復原作業；第三級或第四級事件：36 小時內完成損害控制或復原作業)						
9.12	知悉第三級或第四級資通安全事件後，是否指派適當層級之人員召開會議研商相關事宜？						
9.13	是否建立資通安全情資之評估及因應機制，針對所接受之情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施？						

稽核項目	資通安全稽核檢核項目	符合	部分符合	不符合	不適用	簡述符合、部分符合、不符合或不適用之原因	紀錄文件
9.14	是否適時進行資通安全情資分享？分享哪些資訊？						