資通安全實地稽核項目檢核表(適用公務機關)

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，並依風險評鑑方法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)？						
1.3	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？						
1.4	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？						
1.5	核心資通系統是否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)？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？						
1.6	資通系統等級中/高等級者，是否設置備援機制，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？						
1.7	業務持續運作計畫是否已涵蓋全部核心資通系統，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	資安治理成熟度評估結果為何？是否進行因應？(A、B 級機關適用，以達到 3 級為目標)						
(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？如何確認人員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
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	是否指派副首長或適當人員兼任資通安全長，負責推動及督導機關內資通安全相關事務？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維護計畫及其他資安管理事項？推動組織層級之適切性，且業務單位是否積極參與？						
2.5	是否針對業務涉及資通安全事項之機關人員，進行相關之考核或獎懲？						
2.6	是否建立機關內、外部清單，並定期檢討其適宜性？						
(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？針對法遵要求作業、資安治理成熟度評估結果、稽核或事件缺失改善所需經費，是否合理配置？						
3.2	資安專職人員配置情形？是否配置其他資安專責人員？對應機關自身及對所屬資安作業推動，目前之資安人員配置是否進行合理性評估及因應？(A 級機關：4 位資安專職人員；B 級機關：2 位資安專職人員；C 級機關：1 位資安專職人員)						
3.3	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？						
3.4	各類人員是否依法規要求，接受資通安全教育訓練並完成最低時數？						
3.5	資通安全專職人員是否分別各自持有資通安全專業證照及職能訓練證書各 1 張以上，且維持其有效性？						
(四) 資訊及資通系統盤點及風險評估							
4.1	是否確實盤點資訊資產建立清冊(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？						

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
4.3	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？是否妥善處理剩餘之資通安全風險？						
4.5	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？其禁止且避免採購或使用之作法為何？						
4.6	機關如仍有大陸廠牌資通訊產品，是否經機關資安長同意及列冊管理?並於數位發展部資通安全署管考系統中提報?另相關控管措施為何?						
(五) 資通系統或服務委外辦理之管理措施							
5.1	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？						
5.2	委外辦理之資通系統或服務如涉及國家機密，是否記載於招標公告、招標文件及契約？並針對受託人員辦理適任性查核(辦理前是否有取得當事人書面同意，並依規定限制人員出境)？						
5.3	是否於採購前識別資通系統分級及是否為核心資通系統？並依資通系統分級，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？						
5.4	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？						
5.5	是否要求委外廠商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？其要求標準為？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？其負責督導的委外作業資通安全管理事項有哪些？						
5.6	委外業務如允許分包，對分包廠商之資通安全維護措施要求為？如何確認其落實辦理？						
5.7	對於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？						

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
5.8	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，並請其針對非自行開發之系統或資源，標示內容與其來源及提供授權證明？						
5.9	委外客製化資通系統開發者，若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？						
5.10	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？						
5.11	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？						
5.12	是否訂定委外廠商之資通安全責任及保密規定？						
5.13	是否對委外廠商執行受託業務之資安作為進行檢視？其時機及做法為何？針對查核發現，是否建立後續追蹤及管理機制？						
5.14	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？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？						
5.15	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？						
5.16	針對涉及資通訊軟體、硬體或服務相關之採購案、具委外營運公眾場域之委外案，契約範圍內是否使用大陸廠牌資通訊產品?就委外營運公眾場域之委外案是否於數位發展部資通安全署管考系統填報並經機關資安長確認?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？是否於契約內明訂禁止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？						
(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							

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
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？是否規劃及執行稽核發事項改善措施，且定期追蹤改善情形？						
6.3	【中央目的事業主管機關適用】 是否針對特定非公務機關之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告提出及其他應遵行事項，訂定相關辦法？						
6.4	是否針對所屬/監督之公務機關及所管之特定非公務機關稽核其資通安全維護計畫實施情形，包含訂定稽核計畫及提出稽核報告等？是否規劃及執行對所屬/監督機關稽核發現事項改善措施，且定期追蹤改善情形？						
6.5	是否針對所屬/監督之公務機關及所管之特定非公務機關通報之事件於規定時間內完成審核，且於 1 小時內依指定之方式向上通報？(第一級或第二級事件：8 小時內完成審核；第三級或第四級事件：2 小時內完成審核)						
6.6	【本項僅總統府與中央一級機關之直屬機關及直轄市、縣(市)政府適用】 是否對於其自身、所屬或監督之公務機關，每年辦理 1 次資安事件通報及應變演練?是否針對表現不佳者有強化作為？是否將新興資安議題、複合式攻擊或災害納入演練情境，以驗證各種資安事件之安全防護及應變程序？						
6.7	【本項僅總統府與中央一級機關之直屬機關及直轄市、縣(市)政府適用】 是否對於其自身、所屬或監督之公務機關，每半年辦理 1 次社交工程演練？是否針對開啟郵件、點閱郵件附件或連結之人員加強資安意識教育訓練？						
(七) 資通安全防護及控制措施							

<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>7.1</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><td></td><td></td><td></td><td></td><td></td><td></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><td></td><td></td><td></td><td></td><td></td><td></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><td></td><td></td><td></td><td></td><td></td><td></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？</td><td></td><td></td><td></td><td></td><td></td><td></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？</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>
<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之IP位址，於防火牆進行阻擋等)？</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
7.8	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	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？						
7.17	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)？						

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
7.19	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？						
7.21	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？						
7.22	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？						
7.23	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)？						
7.24	是否有即時通訊軟體管理措施、安全需求及購置準則？						
7.25	【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?						
7.26	機關是否對雲端服務應用進行相關資安防護管理?						
(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？						
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？						

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
8.5	資通系統開發階段，是否針對安全需求實作必要控制措施並避免常見漏洞(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？						
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)納入契約書？						
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？						
8.12	是否針對資通系統所使用之外部元件或軟體、韌體，注意其安全漏洞通告，且定期評估更新？系統之漏洞修復是否測試有效性及潛在影響?						
(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	【參與行政院資通安全會報資通系統實兵演練機關適用】 機關參與行政院資安會報對外資通系統實兵演練，是否就相關系統弱點訂定資安防護改善計畫，並落實執行？						
9.4	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？						
9.5	近1年所有資安事件及近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？						
9.6	是否訂定資安事件處理過程之內部及外部溝通程序？						
9.7	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，應依自身機關資通安全責任等級保存日誌，詳各機關資通安全事件通報及應變處理作業程序表二，且落實執行後續檢討及改善？						
9.8	【A、B級機關適用】 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「端點偵測及應變機制」與「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？SOC 是否有委外供應商？SOC 供應商是否依契約規範(包含SLA水準)確實履約？						
9.9	【A、B級機關適用】 是否依指定方式提交SOC監控管理資料？						
9.10	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？是否有啟用DNS相關紀錄日誌(有記錄到DNS行為的日誌)？是否有開啟監測內部網路連線至DMZ的日誌？日誌時戳是否對應世界協調時間(UTC)或格林威治標準時間(GMT)或相關校時主機?						
9.11	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？						
9.12	針對日誌之是否進行存取控管，並有適當之保護控制措施？						

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
9.13	是否監控資通系統以偵測攻擊與未授權之連線?是否辦理系統軟體及資訊完整性之控制措施?						
9.14	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)						
9.15	知悉第三級或第四級資通安全事件後，是否由資通安全長召開會議研商相關事宜，並得請相關機關提供協助？						
9.16	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？						
9.17	是否適時進行資通安全情資分享？分享哪些資訊？						