115年度數位發展部辦理政府機關受託者資通安全聯合稽核計畫

一、緣起：

隨著公務機關資通訊系統之數位化應用日益多元，各機關推動數位轉型，促進公私協力合作，建構共榮互信之委外服務模式尤顯重要，有助於提升行政效率與為民服務品質；惟各機關自行規劃並執行稽核作業，尚須投入相當人力與時間，造成行政負擔及成本增加；爰此，期藉由推動本計畫，減少各機關辦理委外廠商稽核所增加行政成本，同時解決資訊服務業者因面臨不同機關頻繁稽核，造成冗長作業時間與人力資源成本等衍生問題，進而提升政府機關委外品質與產業服務效能。

二、依據：

（一）資通安全管理法（以下簡稱資安法）第10條規定，各機關應選任適當之受託者，要求受託者建立有效之資通安全管理機制，並監督該機制之實施。

（二）各機關於資訊服務採購契約得訂定委由資安法主管機關籌組專案團隊辦理稽核作業。

三、執行單位：

由本部資通安全署（以下簡稱資安署）統籌規劃並據以執行稽核作業。

四、適用對象：

行政院所屬機關。

五、稽核作業時程規劃：

項次	期程	重點工作
一	籌備階段 (114年12月-115年1月)	研擬受託者聯合稽核計畫（草案）及本計畫重點檢視項目，並彙整各機關意見
二	前置作業（2月-3月）	(一)邀集候選受稽核廠商召開說明會議 (二)函頒計畫及公告候選受稽核廠商 (三)彙整各機關授權相關資料 (四)彙整各機關推薦之稽核委員名單
三	遴選稽核委員(4月)	(一)擇定受稽核廠商清單 (二)遴選各場次稽核領隊及稽核委員 (三)召開聯合稽核作業行前說明會
四	實施作業(5月-10月)	(一)完成各項稽核準備工作 (二)辦理受稽核廠商實地稽核 (三)完成稽核後一個月內提出稽核報告
五	檢討作業(11月-12月)	(一)研析受稽核廠商之共同發現事項 (二)追蹤及管考稽核結果之後續改善措施

六、遴選受稽核廠商：

（一）依據「數位發展部資通安全署資通安全作業管考系統」（網址：https://spm.nat.gov.tw/）盤點各機關系統清冊，115年度採試行作業方式，由資安署綜合評估「廠商維運機關核心資通系統數量」及「廠商服務機關數量」，遴選候選受稽核廠商並公告。

（二）上開公告候選受稽核廠商，資安署將依參與機關數量及稽核量能，擇定當年度受稽核廠商。

七、機關配合事項：

（一）參與條件：機關與廠商簽訂之契約條款中載明得委由資安法主管機關籌組專案團隊辦理稽核（詳行政院公共工程委員會「資訊服務採購契約範本」第十六條之第十七款）。

（二）基於符合前述參與條件，於資安署公告候選受稽核廠商後，由具意願參與機關向行政院直屬機關（如行政院所屬三、四級機關向行政院直屬機關）提出授權相關資料（附件1），提交由資安署彙辦。

（三）資安署彙整前揭參與機關授權後，由資安署發函通知受稽核廠商配合辦理相關稽核作業。

（四）各機關授權本計畫稽核團隊辦理稽核，機關視為同意稽核團隊審視契約專案內容，機關應通知廠商配合辦理。

（五）各機關授權本計畫之範圍，即視同符合資通安全管理法要求應定期確認受託業務之執行情形，倘若仍有未納入資安共通性查檢項目或特殊履約事項，得由各機關自行以其他適當方式辦理。

八、受稽核廠商配合事項：

（一）資安署於稽核前1個月通知受稽核廠商稽核日期，請受稽核廠商於資安署通知所定期限內交付相關資料，另於稽核日前2週通知廠商抽檢契約。

（二）廠商應交付資料包含：廠商資安推動情形說明簡報、資通安全聯合稽核重點檢視項目檢核表等。

九、稽核團隊組成：

（一）稽核領隊：資安署簡任人員擔任。

（二）稽核委員：由行政院直屬機關推薦參與機關之主管人員（具資通安全專業能力）至少2名，提交資安署遴選各場次稽核委員。每場次稽核團隊共計3至5名委員，其中得包含資安署指派主管人員擔任（附件2）。

（三）團隊成員對於所知悉或持有之相關機敏資訊或文件，應善盡保管及保密之責，並應簽署保密切結書。

十、稽核結果之管考作業：

資安署彙整受稽核廠商之稽核結果及改善精進措施，函送行政院直屬機關及其所屬參與機關。稽核結果共通性發現由資安署追蹤與管考；若涉及特定機關契約範圍，則由該機關自行辦理後續追蹤與管考。

十一、稽核重點：

本計畫以符合各機關履約範圍之共通性要求，並強化委外廠商資訊安全管理機制為目標，著重於技術構面訂定重點檢視項目（附件3）。

十二、稽核行政作業：

（一）資安署函請受稽核廠商配合稽核相關作業。

（二）資安署得視情形邀集當年度受稽核廠商召開說明會議或聯合稽核作業行前說明會。

（三）稽核相關行政工作由資安署統一辦理，負責實地稽核之各項準備工作，彙整機關提供之稽核發現事項，產出稽核報告等。

十三、稽核作業時間：4-5小時。

十四、稽核所需費用：

依據「中央政府各機關學校出席費及稿費支給要點」規定，各機關委員出席委辦計畫相關會議不得支給出席費，其交通費及住宿費等支出，由各機關依「國內出差旅費報支要點」規定，自行辦理報支核銷。

十五、附件：

附件1 授權同意調查表

附件2 稽核委員推薦名單

附件3 本計畫重點檢視項目

附件1

○○部（會）及其所屬機關參與115年度數位發展部辦理政府機關受託者資通安全聯合稽核計畫之授權同意調查表

一、機關承辦人聯絡資訊

機關	
單位	
姓名	
職稱	
公務電話	
公務信箱	

二、同意授權列表

編號	機關名稱	契約案名	履約範圍	系統名稱	廠商名稱 （限填報資安署公布之候選受稽核廠商）	廠商是否知悉稽核作業 （是/否）

備註：表格可以自行新增

附件2

○○部（會）及其所屬機關參與115年度數位發展部辦理政府機關受託者資通安全聯合稽核計畫之稽核委員推薦名單

一、機關承辦人聯絡資訊

機關	
單位	
姓名	
職稱	
公務電話	
公務信箱	

二、推薦委員清單

編號	機關	單位	姓名	職稱	公務電話	公務信箱	推薦理由

備註：表格可以自行新增

附件3
本計畫重點檢視項目

序號	構面	共通性檢核項目	稽核依據
1	電腦使用限制與設備認證管理	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？	資通安全管理法第10條第2項
2		是否訂定使用者電腦的軟體安裝管控規則，並定期檢查授權與免費軟體的使用情形？	
3	可攜式儲存媒體管控	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？	資通安全管理法第10條第2項
4	重要資訊組態與資料交換之安全管控	是否訂定設備日誌紀錄之留存政策，並保留至少6個月紀錄，且系統時間同步且準確？	資通安全管理法施行細則第7條第1項第7款
5	惡意程式防護	公司電腦及伺服器是否部署惡意程式防護方案並定期掃描，確保持續更新版本與病毒碼？	資通安全管理法施行細則第7條第1項第7款
6	對外網路防護	是否完成下列資通安全防護措施？ 防毒軟體、網路防火牆、電子郵件過濾機制、入侵偵測及防禦機制、應用程式防火牆（具有對外服務之核心資通系統者）、進階持續性威脅攻擊防禦	資通安全管理法施行細則第7條第1項第7款
7		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？	
8		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？	
9	遠端連線管理	是否避免允許遠端資料存取？若有遠端存取行為，是否具有相關保護措施？	資通安全管理法施行細則第7條第1項第7款
10	電子郵件防護	是否建立並落實電子郵件的過濾、分析與使用管控措施，定期更新過濾規則、偵測並處置異常行為，並依郵件機密性與敏感性規範傳送限制？	資通安全管理法施行細則第7條第1項第7款

序號	構面	特定契約檢核項目	稽核依據
1	配置適當之資通安全專業人員及適當之資源	是否已配置適當之資通安全專責人員？	資通安全管理法施行細則第7條第1項第1款
2	重要資訊組態與資料交換之安全管控	資通系統重要組態與敏感資訊是否採安全方式儲存？資料交換是否具備完整性、機密性之保護措施並留存監控紀錄？	資通安全管理法施行細則第7條第1項第7款
3	帳號密碼管理	是否建立並定期盤點帳號管理機制，要求預設密碼登入後立即更改且符合密碼複雜度規範（如包含禁用已知洩露密碼之機制），並優先導入多因子驗證（MFA），同時採行最小權限與角色型存取控制，並確保管理者帳號僅用於管理用	資通安全管理法施行細則第7條第1項第7款

		途？	
4	安全性更新與漏洞管理	是否針對安全性檢測結果執行修補作業，且於修補完成後驗證是否完成改善？	資通安全管理法施行細則第7條第1項第7款
5		受託業務包括客製化資通系統開發者，是否提供資通系統之安全性檢測證明，並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？	資通安全管理法施行細則第7條第1項第4款
6		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？	資通安全管理法施行細則第7條第1項第7款
7	系統安全開發	資通系統開發程序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？並是否有檢核機制?	資通安全管理法施行細則第7條第1項第7款
8		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？	
9		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？	
10		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？另是否執行安全性功能測試，且檢討執行情形？	

11		是否就其開發資通系統建立版本控管及變更管理機制，並留存相關紀錄？	
12		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？	
13		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？	
14	訂定受託者內部資通安全事件通報及應變之程序及機制	是否建立資通安全事件發生之通報應變程序？	資通安全管理法施行細則第7條第1項第5款
15		是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	
16	分包廠商資通安全維護措施	是否有委託其他分包廠商協助？與該分包廠商之委外契約中是否包含法律需求（如：個人資料保護法）、界定雙方有關人員權責、使用安全控管措施及作業程序、對分包廠商資安稽核權等條文？	資通安全管理法施行細則第7條第2款
17		如有分包廠商，是否已對分包廠商執行稽核並留下紀錄？	