全國農業金庫
114年度電腦系統資訊安全評估專案
規格及特別條款

全國農業金庫股份有限公司（以下稱本公司）採購「114年度電腦系統資訊安全評估專案」（以下稱本案）1批，其一般規定及特別條款如下：

甲、一般規定

壹、投標廠商應於投標時提供下列證明文件：

一、投標廠商在臺灣地區應設有「電腦系統資訊安全評估專案」之相關專責單位，並以書面述明部門名稱、地址、電話、人員配置等，於投標時提供相關證明文件。

二、投標廠商於投標截止日近三年內，應具備三家以上銀行業之電腦系統資訊安全評估專案服務經驗。

三、投標廠商須名列 SWIFT 組織之 CSP Certified Assessors Directory 內，並標示可對臺灣地區提供 SWIFT CSP 相關服務。

四、本案服務團隊應具備之資安證書及相關經驗：

服務團隊成員	資格
合規顧問	本案合規顧問至少 3 人，應具備下列 1 項以上之國際資安管理證照: 1. CISSP(Certified Information System Security Professional)證書。 2. CISM 國際資訊安全經理人(Certified Information Security Manager,CISM)證書。 3. CISA 國際電腦稽核師(Certified Information Systems Auditor,CISA)證書。 4. ISO 27001資訊安全管理系統主導稽核員考試合格證書。

技術顧問	本案技術顧問至少3人，應具備下列1項以上之資安國際證照: 1.EC-Council Certified Ethical Hacker (CEH)。 2.European Citizen Science Association (ECSA)。 3.Certified Incident Handler Course (ECIH)。 4.Computer Hacking Forensic Investigator (CHFI)。 5.Offensive Security Certified Professional (OSCP)。 6.Offensive Security Exploit Developer (OSED)。 7.Offensive Security Web Expert (OSWE)。

五、投標廠商應按投標金額 5%以現金、金融機構簽發之本票或支票、銀行保付支票、郵政匯票繳納押標金，未得標者無息退還，得標者得標後押標金轉為履約保證金，履約保證金經履約完成無待解決事項後轉為保固保證金，保證期滿且無待解決事項後無息發還保固保證金。

六、投標廠商如有政府採購法第 101 條所列之情事，經刊登於政府採購公報者，依同法第 103 條規定之期間內，不得參加投標或作為決標對象或分包廠商。

七、本規格稱 「以上」、「以下」、「以內」、「至少」、「高於」、「低於」 俱含本數。

貳、 本公司電腦系統分類及評估週期如下表，電腦系統依其重要性分為三類，本案辦理 114 年度資訊安全評估作業，合規檢視項目評估類別為第一、二類應用系統(約 32 套)。

電腦系統類別	定義	評估週期
第一類	直接對客戶自動化服務或對營運有重大影響之系統（如電子銀行、分行櫃檯、	每年至少辦理一次資訊安全評估作業。

	ATM自動化服務及SWIFT等系統）。	
第二類	經人工介入以直接或間接提供客戶服務之系統(如作業中心、客戶服務等系統)。	每三年至少辦理一次資訊安全評估作業。
第三類	未接觸客戶資訊或服務且對營運無影響之系統或設備（如人資、財會、總務等系統及物聯網設備）。	每五年至少辦理一次資訊安全評估作業。

參、114 年度電腦系統資訊安全評估專案項目：

評估項目		評估內容
一	資訊架構檢視	1. 檢視網路架構支配置、資訊設備安全管理規則之妥適性等，評估可能之風險，採取必要因應措施。 2. 檢視單點故障最大衝擊與風險承擔能力。 3. 檢視對於持續營運採取之相關措施之妥適性。
二	網路活動檢視	1. 檢視網路設備、伺服器及物聯網設備之存取紀錄及帳號權限，識別異常紀錄與確認警示機制。 2. 檢視資安設備之監控紀錄，識別異常紀錄與確認警示機制。 3. 檢視網路封包是否存在異常連線或異常網域名稱解析伺服器(Domain Name System Server,DNS Server)查詢，並比對是否為已知惡意網際網路協定(以下稱 IP)、中繼站或有符合網路惡意行為的特徵。
三	網路設備、伺服器、端末設備及物聯網等設備檢測	1. 辦理網路設備、伺服器、端末設備及物聯網等設備之系統弱點掃描與修補作業。 2. 網路設備（約 170 台）、個人電腦+端末機（約 600 台）、Server（約 250 台）、IOT 聯網設備（約 87 台）、ATM（5 台）。

		3. 系統弱點掃描需使用 Nessus 弱點掃描軟體。 4. 惡意程式檢測若需安裝 agent，需協助客戶進行佈署。 5. 檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新設定及更新狀態。 6. 檢測終端機及伺服器是否存在惡意程式，包括具惡意行為之可疑程式、有不明連線之可疑後門程式、植入一個或多個重要系統程式之可疑函式庫、非必要之不明系統服務、具隱匿性之不明程式及駭客工具等。 7. 檢測系統帳號登入密碼複雜度；檢視外部連接密碼，如檔案傳輸(File Transfer Protocol)以下稱 FTP 連線、資料庫連線等之儲存保護機制與存取控制。
四	網站安全檢測 (網路設備、伺服器及物聯網等設備且連線至 Internet 者)	1. 進行網站滲透測試，含登入電子銀行所採用之圖形或文字驗證碼。 2. 進行伺服器應用系統之程式原始碼掃描或黑箱測試。 3. 檢視伺服器目錄及網頁之存取權限。 4. 檢視伺服器是否有授權連線遭挾持、大量未驗證連線耗用資源、資料庫死結（deadlock）、CPU 異常耗用、不安全例外處理，及不安全資料庫查詢命令(包括無限制條件及無限制筆數)等情況。 5. 對外服務網站滲透測試，至少須包含如下，如有異動將依專案項目執行前實際盤點情形進行調整: (1) 農業金庫官網。 (2) 農漁會交流網。 (3) 代收業務整合平台。 (4) 專案農貸系統。 (5) 網路銀行（企業戶） (6) 網路銀行（個人戶）

		(7)教育訓練系統、 (8)SWIFT 正式及測試環境（採內部方式進行）。 (9)線上申貸系統。 (10) 董事及監察人會議資料專區。 (11) WEBATM。 (12) 友善個人網路銀行。 (13) 全國農業金庫顧客滿意度問卷調查表等網站。 6. 初測完成後須提供修補建議，於修補完成後需安排複測作業。
五	客戶端應用程式檢測	針對銀行交付給客戶之行動應用程式 APP，依據行動應用 APP 基本資安檢測基準，檢視本公司送檢測項目與作業程序是否符合規範辦理。 1、提供超文本傳輸協定 http、超文本傳輸安全協定 https、FTP 者應進行弱點掃描。 2、程式原始碼掃描或滲透測試。 3、敏感性資料保護檢測 如記憶體、儲存媒體 。 4、金鑰保護檢測。
六	安全設定檢視	1. 檢視伺服器（如網域服務 Active Directory、未加入 AD 網域主機、非 Windows 作業系統環境之主機)有關群組原則中之「密碼設定原則」與「帳號鎖定原則」設定。 2. 檢視之群組原則（GroupPolicy）中之「密碼設定原則」與「帳號鎖定原則」設定。 3. 檢視防火牆是否開啟具有安全性風險的通訊埠或非必要通訊埠，連線設定是否有安全性弱點。 4. 檢視系統存取限制（如存取控制清單 Access Control List）及特權帳號管理。 5. 檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新設定及更新狀態。

		6. 檢視金鑰之儲存保護機制與存取控制。
七	合規檢視	1. 114 年執行第一、二類應用系統檢視評估作業（約 32 套），實際數量將依執行前盤點情形進行調整。 2. 檢視電腦系統是否符合銀行公會制定之「金融機構資訊系統安全基準」之提升系統可靠性<技 1~技 25>及安全性侵害之對策<技 26~技 51>。 3. 檢視電子銀行相關系統是否符合「金融機構辦理電子銀行業務安全控管作業基準」之規範。 4. 檢視相關系統是否符合「金融機構提供行動裝置應用程式作業規範」之規範。 5. 檢視相關系統是否符合「金融機構提供自動櫃員機系統安全作業規範」之規範。 6. 檢視相關系統是否符合「金融機構運用新興科技作業規範」之規範。 7. 檢視相關系統是否符合「金融機構使用物聯網設備安全控管規範」之規範。 8. 檢視相關系統是否符合「金融機構提供QR Code掃描支付應用安全控管規範」之規範。 9. 檢視相關系統是否符合「金融機構辦理行動金融卡安全控管作業規範」之規範。 10. 檢視相關系統是否符合「電子支付機構資訊系統標準及安全控管作業基準」之規範。 11. 檢視相關系統是否符合「金融機構資通安全防護基準」之規範。 12. 檢視相關系統是否符合「主管機關及銀行公會相關函文」之要求。 13. 檢視SWIFT系統是否符合 SWIFT 公布之客戶安全計畫(Customer Security Programme)規範及銀行公會相關函文之要

		求，若與本辦法資訊安全評估作業衝突，依 SWIFT公布為主，並產出獨立SWIFT CSP合規檢視報告，報告內容須敘明CSCF（客戶安全控制框架）各控制項之評估結果。
八	社交工程演練	1. 針對本公司內部有電子郵件帳號之同仁。 2. 針對使用電腦系統人員，於安全監控範圍內，寄發演練郵件，統計社交工程郵件開啟率，並提供資通安全教育，以期提高同仁資安意識，防範惡意程式透過社交方式入侵。 3. 透過外部網路針對約 500 位人員進行 2 次社交工程演練，每次寄發 3-5 封不同類型信件。
九	DDos年度演練	1. 偵測頻寬消耗型與資源消耗型 DDoS 攻擊（包含：DNS Amplification、Application-level flood、SSDP Amplification、SYN flood、Ping of Death、ICMP flood、UDP flood）。 2. 檢視防禦有效性與應變機制。
十	資訊安全事件演練	1. SWIFT 攻擊與應變程序演練(腳本演練) 2. 個資外洩應變程序演練(腳本演練) 3. ATM 資安事件應變程序演練(腳本演練) 4. 資訊安全緊急應變演練(腳本演練)
十一	教育訓練	1. 檢視依據金融控股公司及銀行業內部控制及稽核制度實施辦法第 38-1 條，銀行業資訊安全專責單位人員，每年至少應接受十五小時以上資訊安全專業課程訓練或職能訓練。 2. 承 1，專案期間須提供 3 人次資通安全專業教育訓練之等值課程點數。

肆、 本案廠商應依「參、電腦系統資訊安全評估專案項目」之檢測結果產出各分項報告，另將整體評估結果彙整產出為「114 年度電腦系統資訊安全評估專案總結報告」，其內容應至少包含評估人員資格、評估範圍、評估作業項目與標的、評估記錄、評估時所發現之缺失項目與佐

證、缺失嚴重程度、缺失類別、風險說明、具體改善建議及社交演練結果。本案之檢測服務結果應確實列出本公司現階段資訊安全需改進之建議與解決方案。

乙、特別條款

壹、本案廠商同意履行以下情事：

一、本案廠商應提供第三方認證證明或公正第三方之驗證報告，如資訊安全管理國際標準要求或資訊安全管理系統國家標準（ISO/CNS 27001）有效證書；本案廠商若無法提供時，應配合本公司辦理資訊安全訪視作業。

二、本案廠商履行契約不得違反法令強制或禁止規定、公共秩序及善良風俗，對本公司經營、管理及客戶權益，不得有不利之影響，並應遵守農業金融法、銀行法、洗錢防制法、個人資料保護法、消費者保護法、中華民國銀行商業同業公會全國聯合會訂定之相關業務規章或自律公約及其他法令之規定。本案廠商應本於善良管理人之注意義務辦理本契約事宜,契約如有履行不能或履行困難之虞者,應即通知本公司。

三、本案廠商應建立標準作業程序，執行消費者權益保障、風險管理、內部控制及內部稽核制度，除應建立消費者爭端解決機制，包含解決時程、程序及補救措施外，另應提供聯絡窗口及電話詢答服務。

四、本案廠商同意金融監督管理委員會、中央銀行、中央存款保險公司、農業部農業金融署等機關或依農業金融法第七條規定之機關及本公司或委託獨立第三方單位進行辦理本契約相關事項之稽核。本案廠商應提供本契約之應辦事項相關資料或報告，配合金融檢查或稽核，並於期限內提供相關資料或報告。

五、本案廠商因履行契約應辦事項所應負之損害賠償責任，悉依民法及相關法令辦理。

六、本案廠商若有違反契約約定情事發生，除契約另有約定外，本公司得於通知本案廠商後終止或解除契約，本公司於主管機關命為終止或解除契約時亦同。

七、本案廠商履行契約應辦事項，對外不得以本公司名義為之，亦不得進行不實廣告，若違反致本公司受損，應負賠償責任。

八、本契約應辦事項若有重大異常、缺失或發現疑似資訊安全或個人資料外洩等異常事件或事故時，本案廠商應立即以口頭、電話等方式通知本公司，並配合本公司相關程序辦理異常排除及通報事宜，如必要應提供駐點服務。並於處理完成後，提供相關報告。

九、本案廠商因履行契約應辦事項所知悉一切有關本公司及本公司客戶等相關資料及內容，僅得揭露於本契約目的範圍內有接觸需要之本案廠商員工，本案廠商及其聘僱人員應保守秘密不得洩漏，並採取必要之安全措施，否則如致本公司遭受損害應由本案廠商負賠償責任；契約經終止、解除或期限屆滿後亦同。

十、本案廠商於契約履行期間應提供開發、維護(修)之服務人員名冊(含公司簽章）及經本案廠商員工簽署之「保密同意書」至本公司備查，且對其操守行為負責。

十一、本案廠商提供本公司使用之軟硬體應為合法，如有第三者主張本案廠商提供本公司使用之軟硬體有侵犯智慧財產權時，本公司同意儘速以書面通知本案廠商，本案廠商應負責為本公司提出抗辯或和解談判，所有經法院判決確定或成立和解應由本公司負擔之費用、損害賠償及本公司因此所支付之費用（含委聘律師酬金）、所受之損害等均由本案廠商負擔。

十二、本案廠商及分包商應擬定本契約項目之服務水準(SLA)：

1. 如無法訂定本契約項目之服務水準時，須擬定補償性控制措施。
2. 違反本公司資訊安全要求或因人員疏失等原因，導致發生資安事件或未達本公司資訊安全要求之服務水準時，應依契約所定罰則計付違約金予本公司，若因此造成本公司相關損害，本案廠商應與分包商依契約內容負連帶賠償責任。
3. 因本契約作業項目之性質、產品內容或服務，本案廠商無法提供服務水準或補償性控制措施時(如訂閱制服務、客制化套裝軟體、商業應用軟體、電腦週邊設備採購等），雙方之權利義務得依雙方協議內容另定之。

十三、本案廠商不得將本契約或基於本契約所生之權利義務，全部或一部分轉讓或複委託予其他第三人，但經本公司事先書面同意者不在此限。

十四、經本公司事先書面同意之複委託，其範圍及限制、條件均不得超出本契約；本案廠商應確認分包商具備資訊安全措施、遵循本公司資訊安全管理制度並簽署保密協議，如因分包商之不當行為致本公司發生損害時，本案廠商應與分包商負連帶損害賠償責任。

十五、本案廠商資訊安全責任。

1. 本案廠商須遵守本公司現有各項系統管理作業規定及安全管理規範。

2. 本案廠商於契約履行期間，如本案廠商人員異動時（完成階段性任務或離職等情形），本案廠商應會同委託單位將其借用之設備、軟體或其他物件返還予本公司，並移除相關作業權限。

3. 本案廠商不得任意複製或攜出本公司非對外公開之業務資料。本公司所提供之資訊資產及資料等，本案廠商均應於契約終止、解除或期限屆滿時返還予本公司，並刪除或銷毀因執行本契約而儲存持有之個人資料檔案，且不得以任何形式留存備份。本案廠商履行契約相關事務之資料處理流程及傳輸方式，應依本公司資料安全管控規定辦理。

4. 如需使用自攜資訊設備，應經本公司檢核同意後始得使用，且不得連接本公司內部網路。

十六、本案廠商禁止使用中國廠牌資通訊產品、軟體（如應用軟體、系統軟體、開發工具、客製化套裝軟體、APP 及電腦作業系統等）、硬體（包括具連網能力、資料處理或控制功能者皆屬廣義之資通訊設備）及資通訊服務。

十七、本案廠商所屬人員倘因參加本案系統建置、維護，致本公司蒙受損害，本案廠商應與其所屬人員負連帶賠償責任。

十八、本案廠商應遵循相關法令法規及其他適當資訊安全國際標準。

貳、 報價

本案以新臺幣為報價基礎，且分別依下表列出價格：

單位：元

項次	項目/內容	數量	單價	金額
1	114年度電腦系統資訊安全評估專案（內容為甲-參項目）	1批	000	000
合計				000

*以上報價應依規格內容報價(含稅)。

交貨、安裝及測試

一、 本案廠商須於簽約次日起5個月內完成全部事項，並交付「驗收應交付相關文件」(詳乙、參、二)，，如逾所訂期限，本案廠商須依照下列公式計付懲罰性違約金予本公司：

違約金 = 契約總價款 * 0.1% * 逾期日數

二、 如逾期超過前項約定期限1個月仍未完成交付時，除仍應依前述規定計付懲罰性違約金外，本公司得通知終止或解除契約之部分或全部，並沒入履約保證金，且不補償本案廠商所生之損失。

三、 上述各項懲罰性違約金之累計總額以契約總價款之20%為上限，本公司得自契約總價款或履約保證金中扣抵。

四、 配合各項檢測所需之檢測工具(包含硬體及軟體)，應由本案廠商提供並負責安裝與檢視，本公司不另行付費或提供相關設備。

參、 驗收與付款

一、 本案廠商依約交付相關文件後，經本公司簽認後，由本公司派員辦理驗收，驗收合格後，支付契約總價款。

二、 驗收應交付相關文件如下：

1. 專案管理暨工作計畫說明書（書面及電子檔各1份）。
2. 114 年度電腦系統資訊安全評估專案總結報告（書面及電子檔各1份）。
3. SWIFT CSP 合規檢視報告（書面及電子檔各1份）。

肆、 保固

本案廠商於本公司完成驗收之次日起，提供無償諮詢與建議1年。

伍、 本案廠商應依本公司電腦及資訊作業安全之相關規定建置安控作業環境及作業流程並提供相關文件。

陸、 本案廠商應對本案契約內容充分瞭解，並應依本公司之解釋切實執行辦理。

附件

資訊安全與服務水準協定(SLA)罰則

一、 資訊安全與服務水準規範

項目	項次	項目	規範標準
資訊安全	1	資訊安全管理	如有洩密、疏失、管理不善等情事，致本公司遭致損失。
	2	存取控制及保全	因故意或過失導致本公司資訊資產遭不當取得、刪除或變更等情事。
	3	事件通報	演練期間引起本公司發生資訊安全事件且未即通報造成損失。
服務水準	1	客服支援時段	技術支援服務時間規定為本公司營業日上午9時至下午5時，若因國定假日異動則以公告為準。
	2	問題回應時間	接獲本公司通知後（含電話、 簡訊、E-Mail、傳真、書面或其他通訊軟體等），須於通報後5日內回應，一般處理時間不應超過收件後隔日起算10天內，並透過電話服務協助系統問題之判斷、偵錯與故障排除，如有進一步到場鑑定維護之必要，須於3天內到場服務。

二、 相關說明：

（一）本案廠商違反資訊安全與服務水準規範，如須延長日期或非本案廠商之問題(不納入計罰)，須經本公司同意。

（二）本案廠商違反資訊安全與服務水準規範時，每違反 1 次，本公司得按契約總價之 0.1%計算懲罰性違約金。

（三）本案廠商指派之專案負責人及工作成員，未經本公司同意，不得更換，如有未經本公司同意自行更換時，每更換 1 次得依契約總價之 0.1%計算懲罰性違約金。

（四）本案廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本專案各項文件，包含版面及內容皆須嚴格要求一致性及正確性。交付之文件經本公司審閱，所發現錯漏處達 10 處以上，或業經本公司要求修訂仍未修訂者，本公司得按每字新臺幣 1,000 元計算懲罰性違約金。

（五）第(二)款至第(四)款之懲罰性違約金之累計總額以契約總價之 20%為上限。如懲罰性違約金總額達契約總價之 20%時，本公司得通知本案廠商終止契約或解除契約之部分或全部，且不補償本案廠商所生之損失。

(六) 本案廠商依各款應付之懲罰性違約金可自契約總價、履約保證金或保固保證金中扣抵。