全國農業金庫
入侵與攻擊模擬演練專案(BAS)
採購規格及特別條款

全國農業金庫股份有限公司（以下稱本公司）採購「入侵與攻擊模擬演練專案」(以下稱本案)1批，其規格及特別條款規定如下：

甲、規格

壹、一般規定

一、本案廠商應於投標時提供下列證明文件：

(一)提供原廠或代理商所開立之經銷授權證明文件。

(二)在臺灣地區設有「入侵與攻擊模擬演練專案(BAS)」部門，並述明部門名稱、地址、電話及人員配置等。

(三)近3年內需具有3家(含)以上金融機構(銀行業、證券業及壽險業)資安攻防演練經驗，如紅隊演練、滲透測試、攻防演練等資安服務經驗。

(四)本案服務團隊成員應具備之資安證書及相關經驗:

服務團隊成員		資格
專案經理	至少1人	一、曾擔任金融機構之相關資安攻防演練專案經理。 二、專案經理應具備下列資安管理國際證照至少 1 項: 1.PMP(Project Management Professional)證書。 2.CISSP(Certified Information System Security Professional)證書。 3.CISM國際資訊安全經理人(Certified Information Security Manager,CISM)證書。 4.CISA國際電腦稽核師(Certified Information Systems Auditor,CISA)證書。

專案顧問	至少2人	一、曾輔導金融機構之相關資安攻防演練實績。 二、專案顧問應具備下列資安國際證照至少1項: 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)上述服務團隊成員於本案廠商服務之勞健保證明或在職證明。

二、本案廠商應按投標金額5%之現金、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，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，保固期滿且無待解決事項後無息發還保固保證金，未得標者無息退還。

三、本案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，於同法第103條所定期間內，不得參加投標或作為決標對象或分包廠商。

四、本規格稱"以上"、"以下"、"以內"、"至少"、"高於"、"低於"俱含本數。

貳、專案需求

一、本案廠商需提供Breach and Attack Simulation(以下稱BAS)檢測應用技術，透過模擬駭客族群實際攻擊所運用之步驟與技術，針對本公司整體資訊安全防護進行有效性檢測，發掘潛在資安防護風險，並提供解決方案，以提升本公司整體資安防護能量。

二、BAS檢測應用技術，應以自動化、持續一致且風險可控的方式，對本公司進行資訊安全防護能量韌性測試，其模擬攻擊情境包括但不

限於外網滲透、釣魚郵件、資料外洩等。

三、本案廠商須提供至少 2 位具資安專業之人員成立本案顧問團隊，其資安專業應涵蓋滲透測試、紅隊演練、緊急應變與藍隊防護等專長。

四、本案廠商需另指派專案負責人(PM)，依據本案契約與工作計劃書管理本案之進行、管制與各項履約、驗收作業，如需變更專案負責人，需經本公司同意。

五、演練標的包含但不限於本條款所列系統，如網路防火牆、網頁應用防火牆、入侵偵測系統、進階持續性威脅防護系統、網頁安全閘道防護系統、電子郵件閘道防護系統、端點防護等。

六、本案廠商需依本公司資安架構進行評估，並提供演練計畫說明書。

七、本案廠商需依本公司需求派專案團隊到場進行正式演練，演練日期由雙方協調議定。

八、本案廠商需協助本案執行之環境部屬以及演練腳本設計事宜。

九、本案廠商應確保整體演練環境設定妥適性，不得對本公司造成危害，若演練期間發生異常或是疑似異常現象，本案廠商需能立即停止演練作業及各項執行工具，並協助恢復系統正常運作。

十、本案檢測所發現之相關防禦漏洞，需出具完整分析報告書，並安排至本公司進行簡報，針對相關弱點提出具體改善措施，以確認相關風險可被控管。

乙、特別條款

壹、本案廠商對於本案系統與文件同意履行以下事項：

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、本案廠商應遵守法令及本契約之規定，不得違反法令強制或禁止規定、公共秩序及善良風俗，並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，本案廠商應即通知本公司。

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應辦事項之稽核。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以直接實際損害為限。但有關人身傷害（包含死亡）、物之毀損、專利權及著作權之損害、本案廠商之故意或重大過失造成之損害賠償則不在此限。

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。

八、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）及經本案廠商人員簽署之「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必要費用、所受之損害等均由本案廠商負擔。

十二、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。

十三、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損害賠償責任。

十四、本案廠商及分包商應擬定本契約項目之服務水準：

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，本案廠商應依契約內容負賠償責任。

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有藉由參加本案系統建置、維護機會，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

本案廠商以新臺幣為報價基礎，且分別依下表列出價格：

單位：元

項次	品名	數量	單價	總金額
一	入侵與攻擊模擬演練專案(BAS)	乙式	000	000
			總金額:	000

*以上報價應依規格內容報價（含稅）。

參、交貨

一、本案廠商須於本公司簽約次日起2個月內依約交付相關文件，如逾此期限，本案廠商須依照下列公式計付違約金予本公司

違約金 = 契約總價款 * 0.1% * 逾期日數

二、如逾期超過2個月仍未完成文件交付，除仍應依前述規定計付違約金外，本公司得通知終止或解除契約。

三、本案逾期違約金之累計總額以契約總價款之20%為上限，並得自契約總價、履約保證金或保固保證金中扣抵。

肆、驗收與付款

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

二、應交付相關文件如下:

1.工作計劃書。

2.演練計畫說明書

3.演練服務報告書。

4.交貨簽認單。

伍、諮詢服務

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。

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 5（工作日）*8（小時）/周，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,每違反乙次,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，每更換乙次得依契約總價之 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)款之懲罰性違約金總額以契約總價之 20%為上限。如違約金逾契約總價之 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。