建 議 書 徵 求 文 件 **RFP Ver 8.0**

板信商業銀行

電腦系統資訊安全評估

專案建議書徵求文件

目　　錄

壹、 專案名稱

板信商業銀行 (以下簡稱本行) 電腦系統資訊安全評估專案 (以下簡稱本專案)。

貳、 專案說明

本行為因應中華民國銀行商業同業公會（以下簡稱「銀行公會」）實施之「金融機構辦理電腦系統資訊安全評估辦法」(以下簡稱「資訊安全評估辦法」)及本行訂定之「電腦系統資訊安全評估計畫」,透過獨立第三方執行資訊安全評估作業,檢視整體電腦系統(含自建與委外維運)既有控制措施之完整性與妥適性，發現潛在之資安威脅與弱點，藉以實施技術面與管理面相關控制措施，以改善並提升網路與資訊系統安全防護能力。

參、 專案目標

本專案期藉由獨立第三方執行資訊安全評估作業，檢視整體電腦系統(含自建與委外維運) 既有控制措施之完整性與妥適性，以達成下列專案目標：

一、 檢視既有控制措施，發現潛在之資安威脅與弱點。

二、 強化專案範圍內之資訊安全作業與資訊系統安全之防護能力。

三、 遵循金融主管機關之要求，提高同仁對於資訊安全之管理認知。

四、 結合國際資訊安全管理趨勢，強化新興科技資訊安全風險管控。

肆、 專案範圍

一、 本專案範圍為本行年度電腦系統資訊安全之檢測作業，系統明細詳如壹拾、現有環境架構。

二、 本專案的服務範圍包括資訊架構檢視、網路活動檢視、網路設備/伺服器/端末設備/物聯網等設備檢測、連線至 Internet 之網路設備/伺服器/物聯網等設備檢測、客戶端應用程式檢測、安全設定檢視、合規檢視和社交工程演練等資安專業服務。

三、 評估單位可就本行或本行之資安評估單位所提供之檢測工具、軟體或檢測報告，就其完整性、妥適性與合規性進行評估。

四、 於上述評估完畢後，評估單位需就評估過程之結果予以具體改善建議，並出具「電腦系統資訊安全評估報告」。

伍、 專案需求

本專案之規劃內容應包含但不限於下列工作項目，評估單位應具備完成各項服務所需之軟、硬體設備，專案執行期間需提供專案諮詢服務，並配合公司辦理說明會議。

一、 執行資訊安全評估作業

評估單位需就本專案範圍內之電腦系統執行資訊安全評估作業，詳細評估工作需求如下：

(一)資訊架構檢視

1. 檢視網路架構之配置、資訊設備安全管理規則之妥適性等，以評估可能之風險，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. 檢視對於持續營運所採取相關措施之妥適性。

(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(如：防火牆、入侵偵測或防禦、惡意軟體防護、資料外洩防護、垃圾郵件過濾、網路釣魚偵測、網頁防護等)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 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、端末設備及物聯網之弱點掃描與提供修補作業。
2. 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。
3. 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, FTP)連線、資料庫連線等)之儲存保護機制與存取控制。
4. 評估單位應於每季弱點掃描後進行報告說明，並協助本行進行弱點修補。

(四)網路設備、伺服器及物聯網等設備且連線至 Internet 者應辦理下列事項

1. 進行滲透測試，含登入個人網路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報告檢視或黑箱測試。
3. 檢視伺服器之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. 評估單位應彙整分析測試結果，提出測試報告，並視需求安排測試結果簡報。測試報告內容應包含：測試過程之紀錄及說明、測試結果及分析，以及具體可行之改善建議。並協助本行進行改善，並針對應修補之弱點進行追蹤管理和複測。

(五)客戶端應用程式檢測

針對銀行交付給客戶之應用程式(含 APP、安控元件)進行下列檢測：

1. 提供 http, https, FTP 者應進行弱點掃描。
2. 程式原始碼掃描報告檢視或滲透測試。
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。
5. 針對行動應用 APP 應依據經濟部工業局「行動應用 App 基本資安檢測基準」(最新版本)及 OWASP 公布之 Mobile APP Security Checklist L2 項目進行檢測(含初測及複測)，確認所有弱點皆完成修補並提供檢測報告及行動應用 App 基本資安檢測合格證明。

(六)安全設定檢視

1. 檢視伺服器(如網域服務 Active Directory)有關「密碼設定原則」與「帳號鎖定原則」設定。
2. 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。
3. 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。
4. 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。
5. 檢視金鑰之儲存保護機制與存取控制。
6. 評估單位依據檢視結果，於報告中提出詳細之檢視方法和相關發現事項，並提供改善建議或方案，協助本行執行改善。

(七)合規檢視

1. 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」有

關提升系統可靠性<技 1~技 25>及安全性侵害之對策<技 26~技 51>之規範。

2. 檢視電腦系統是否符合銀行公會制定之「金融機構辦理電子銀行業務安全控管作業基準」、「金融機構提供行動裝置應用程式作業規範」、「金融機構提供自動櫃員機系統安全作業規範」、「金融機構運用新興科技作業規範」、「金融機構使用物聯網設備安全控管規範」、「金融機構資通安全防護基準」、主管機關及銀行公會相關函文之要求。
3. 檢視電腦系統之 SWIFT 系統是否符合 SWIFT 公布之 Customer Security Programme 規範及銀行公會相關函文之要求，並獨立出具報告書，若與本辦法資訊安全評估作業衝突，依 SWIFT 公布為主。
4. 評估單位依據檢視結果，於報告中提出詳細之檢視方法和相關發現事項，並提供改善建議或方案，協助本行執行改善。

(八)社交工程演練

1. 針對使用電腦系統人員，於安全監控範圍內，寄發演練郵件，加強資通安全教育，以期防範惡意程式透過社交方式入侵。
2. 評估單位依據檢視結果，於報告中提出相關發現事項，並提供改善建議或方案，及協助本行執行改善。

陸、 專案時程

自簽約日起至 111 年 9 月 30 日前完成所有評估檢測項目，111 年 10 月初出具評估報告初稿，111 年 10 月 31 日前完成評估報告。

入圍或得標之供應商應於入圍或決標日起 1~2 週(日曆天)內交付工作計畫書予本行，交付項目必須包含但不限於以下項目：

1. 工作計畫書應以廠商投標時之「建議書」為基礎，並依採購評選意見修改

2. 內容除包括對本專案之執行敘述，含專案管理、組織、人力、分工、職掌、工作項目、執行程序(網路/個人電腦/伺服器)、時程說明(包括各項檢測之初、複測/起始會議/結束會議)、受測機關檢測範圍與影響、受檢測機關準備事項、工作進度稽核點及品質管理流程

3. 受檢測機關準備事項建議包括：受測個人電腦清單(IP、所安裝之作業系統與應用程式)、受測伺服器清單(IP、用途、所安裝之作業系統與應用程式、管理人員)、網路架構圖(標示部署設備位址)、網路設備紀錄檔、協同檢測人員名單

柒、 專案管理規劃

一、 專案組織與管理

評估單位**必須於建議書**中說明針對本專案執行之工作範圍、工作時程及運作管理方式。

(一)專案工作規劃

說明專案工作範圍、執行專案工作項目所需成立之專案組織、具體可行之專案執行策略與建議方案，以及專案進行過程中所建立之執行與管制紀錄。

(二)專案組織與人力

說明預計投入本專案之人數、組織架構、職責分工、人力配置與人員資歷(學經歷背景與技術專長)，專案人員應具備資訊安全相關資歷或具備資訊安全管理制度(如:ISO 27001)之實務輔導經驗。

(三)專案管制

專案進行期間，對於專案之進度與品質應建立監控方法，以期有效解決問題與

異常狀況，保護銀行機敏資料避免攜出外流，並明確說明雙方應配合與協調之事實。

二、 專案成員

本專案團隊人力至少應包含專案負責人/專案經理。服務人員應具備以下所列舉之技能，以確保服務水準和人員互相備援，並於建議書中檢附成員姓名、訓練證書或專業證照等影本以供審核。應具備必要資訊網路、系統技能說明如下:

(一) 具備資訊安全管理知識，如持有國際資訊安全經理人(Certified Information Security Manager, CISM) 證書或通過國際資安管理系統主導稽核員(Information Security Management System Lead Auditor, ISO 27001 LA)考試合格等，專案成員須合計至少3張證照。

(二) 具備資訊安全技術能力，如國際資訊安全系統專家(Certified Information Systems Security Professional, CISSP)證書等，專案成員須合計至少2張證照。

(三) 具備模擬駭客攻擊能力，如滲透專家(Certified Ethical Hacking,CEH)證書或事件處理專家(Certified Incident Handler,CIH)證書等，專案成員須合計至少3張證照。

(四) 熟悉金融領域載具應用、系統開發或稽核經驗。

(五) 參與本專案之成員需為評估單位之正式員工並具資安專業年資超過兩年以上無犯罪紀錄者，應檢附勞保投保證明。

三、 雙方配合事項說明

(一) 評估單位

評估單位應依據本專案需求規格書之要求，善盡誠實建議義務，不得作虛偽不實之敘述。對於因執行本專案所取得之本行相關檢視文件、檢測紀錄檔、組態參數、程式原始碼、側錄封包資料等與本案相關之全部資料，應負保密責任並提供適當保護措施，以防止資料外洩。

(二) 本行

對於執行本專案所需之相關文件與資訊，應詳實並依照時程提供。評估單位提供之建議書及電腦系統資訊安全評估報告不得任意複製與散播。

捌、 評估單位資格

為確保資訊安全及評估單位所提供的服務水準，評估單位應符合下列條件，並於服務建議書專章詳述：

一、 凡在政府機關登記合格，無不良紀錄之評估單位（檢附設立及登記證明、納稅證明及信用證明）且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。

二、 評估單位需熟悉金融領域載具應用、系統開發或稽核經驗。且擁有政府機構資安檢驗經驗或 5 家以上(含)金融機構資安相關建置、維護或顧問經驗。

三、 評估單位應具備獨立性，與提供、維護資安評估標的之機構無利害關係。

四、 評估單位成員需符合前揭專案成員資格之要求。

玖、 專案維護服務需求說明

一、資訊安全管理需求：

(一) 評估單位於執行本專案相關工作時，需確實遵守「資訊安全管理系統（ISMS）」之相關規定，且評估單位需以公司名義簽署「廠商保密切結書」，專案成員需以個人名義簽署「個人保密切結書」。

(二) 評估單位應配合本行要求，回答及解決本專案資訊安全技術相關問題。

(三) 傳輸報告及機敏資料時，需將檔案壓縮加密碼保護，並以電話告知密碼。

(四) 於專案服務期間如發現有風險時須提供立即風險控制相關建議方案。

二、品質需求

(一) 為確保專案如期如質完成，評估單位應針對本專案之需求，妥慎成立專案小組，執行本專案所需之各項作業，並指派專案經理負責督導工作項目。

(二) 評估單位應訂定品質管理流程，本行可據以進行稽核。

(三) 評估單位於專案期間應辦理啟始會議與結束會議，並視情況召開專案管理會議以掌控品質，會議討論內容與結果需作成紀錄與追蹤辦理，送本行備考。

三、專案管理需求

(一) 專案組織：至少包含行政管理與作業程序管理由不同人員負責，以確保專案進行之時程控管順遂。

(二) 執行任何會影響系統正常服務之檢測，必須於檢測10天(含)前提出申請，並經本行告知可執行時段，授權同意後始得進行。

(三) 本專案每年於三月至十月間進行電腦系統資訊安全評估作業，並於十月底前產出「電腦系統資訊安全評估報告」交付本行。

(四) 本專案所有內容及測試相關資訊不得揭露予任何第三人知悉，且應採取適當及必要之保護措施，以防止第三者不當或未經授權而取得或使用。

壹拾、 現有環境架構

■ **本年度檢測標的**

分類	網路設備數量	伺服器數量	終端數量	網站數量	提供Internet存取	資訊資產	備註	資安評估	
								滲透測試	網頁弱掃
1	0	5	0	4	V	第一類系統-01		V	V
1	0	8	0	1	V	第一類系統-02		V	V
1	0	8	0	1	V	第一類系統-03		V	V

1	0	0	0	1	V	第一類系統-04	依附於網路銀行	V	V
1	0	4	0	1	V	第一類系統-05		V	V
1	0	1	0	1	V	第一類系統-06		V	V
1	0	0	0	0	V	行動 APP-1(IOS、Android)	中台依附於網路銀行 工業局 L3 檢測(含 MAS 標章)、 CheckList L2	V	V
1	0	0	0	0	V	行動 APP-2(IOS、Android)	中台依附於新企業網路銀行 工業局 L3 檢測(含 MAS 標章)、 CheckList L2	V	V
1	0	4	0	0	V	第一類系統-07		V	V
1	0	5	0	0	V	第一類系統-08		V	V
1	0	2	0	0	X	第一類系統-09		-	-
1	0	3	0	0	X	第一類系統-10		-	-
1	0	2	0	0	X	第一類系統-11		-	-
1	0	1	0	0	X	第一類系統-12		-	-
1	0	1	0	0	X	第一類系統-13		-	-
1	0	2	0	0	X	第一類系統-14		-	-
1	0	12	0	0	X	第一類系統-15		-	-
1	0	2	0	1	X	第一類系統-16		-	-
1	0	4	0	1	X	第一類系統-17		-	-
1	0	2	0	1	X	第一類系統-18	須獨立產出 SWIFT CSP 檢核報告	V	-
1	0	2	0	0	X	第一類系統-19		-	-
1	0	4	0	0	X	第一類系統-20		-	-
1	0	1	0	0	X	第一類系統-21		-	-
2	0	5	0	1	X	第二類系統-01		-	-
2	0	1	0	1	X	第二類系統-02		-	-
2	0	1	0	1	X	第二類系統-03		-	-
2	0	13	0	1	X	第二類系統-04		-	-
2	0	1	0	1	X	第二類系統-05		-	-
2	0	1	0	0	X	第二類系統-06		-	-
2	0	1	0	1	X	第二類系統-07		-	-
2	0	1	0	1	X	第二類系統-08		-	-
2	0	2	0	1	X	第二類系統-09		-	-
2	0	2	0	1	X	第二類系統-10		-	-
2	0	3	0	1	X	第二類系統-11		-	-
2	0	1	0	0	X	第二類系統-12		-	-

2	0	2	0	0	X	第二類系統-13		-	-
2	0	2	0	1	X	第二類系統-14		-	-
2	0	1	0	0	X	第二類系統-15	僅與集保中心連線	-	-
2	0	1	0	0	X	第二類系統-16	僅與悠遊卡公司連線	-	-
2	0	2	0	0	X	第二類系統-17		-	-
2	0	1	0	0	X	第二類系統-18	僅供內部使用	-	-
2	0	1	0	0	X	第二類系統-19		-	-
2	0	1	0	0	X	第二類系統-20		-	-
2	0	1	0	1	X	第二類系統-21	僅供內部使用	-	-
2	0	1	0	1	X	第二類系統-22		-	-
2	0	1	0	0	X	第二類系統-23		-	-
2	0	2	0	0	X	第二類系統-24		-	-
2	0	1	0	0	V	第二類系統-25	僅供特定券商連線	-	-
2	0	1	0	0	X	第二類系統-26	專線連線	-	-
2	0	4	0	1	X	第二類系統-27		-	-
2	0	1	0	0	X	第二類系統-28	僅供特定總行部室連線	-	-
2	0	8	0	0	V	第二類系統-29		-	-
2	0	1	0	1	X	第二類系統-30	財務、風管	-	-
2	0	2	0	1	X	第二類系統-31		-	-
2	0	1	0	1	X	第二類系統-32	隆美案	-	-
2	0	4	0	1	X	第二類系統-33		-	-
2	0	0	0	1	X	第二類系統-34		V	V
2	0	-	0	1	V	第二類系統-35	開發中	V	V
3	0	1	0	0	X	第三類系統-01		-	-
3	0	1	0	0	X	第三類系統-02		-	-
3	0	1	0	1	X	第三類系統-03		-	-
3	0	1	0	0	X	第三類系統-04		-	-
3	0	2	0	1	X	第三類系統-05		-	-
3	0	1	0	0	X	第三類系統-06		-	-
3	0	2	0	0	X	第三類系統-07		-	-
3	0	4	0	1	X	第三類系統-08		-	-
3	0	1	0	0	X	第三類系統-09		-	-
3	0	2	0	1	X	第三類系統-10		-	-
3	0	1	0	1	X	第三類系統-11		-	-
3	0	1	0	1	X	第三類系統-12		-	-
3	0	1	0	1	X	第三類系統-13		-	-
3	0	1	0	1	X	第三類系統-14		-	-

3	0	2	0	0	X	第三類系統-15		-	-
3	0	1	0	0	X	第三類系統-16		-	-
3	0	1	0	1	X	第三類系統-17		-	-
3	0	2	0	1	X	第三類系統-18		-	-
3	0	1	0	1	X	第三類系統-19		-	-
3	0	8	0	2	X	第三類系統-20		-	-
3	0	2	0	1	V	第三類系統-21		V	V
3	0	1	0	0	X	第三類系統-22		-	-
3	0	1	0	1	X	第三類系統-23		-	-
3	0	7	0	1	X	第三類系統-24		-	-
3	0	1	0	1	X	第三類系統-25		-	-
3	0	1	0	0	X	第三類系統-26		-	-
3	0	1	0	1	V	第三類系統-27	僅保全公司可連入	-	-
3	0	1	0	2	V	第三類系統-28		V	V
3	0	1	0	0	X	第三類系統-29		-	-
3	-	-	76	-	X	第三類系統-30 (物聯網設備)	針對金融機構使用物聯網設備安全控管規範進行對應之檢測項目，並出具獨立報告，弱點掃描須含初複測	-	-
其他	0	0	500	0	X	櫃檯交易電腦（間接接觸客戶）	(抽樣 10%檢測)	-	-
其他	0	0	1000	0	X	一般 OA 電腦（無接觸客戶）	(抽樣 10%檢測)	-	-
其他	0	0	128	0	X	ATM 總數量	(抽樣 10%檢測)	-	-
其他	26	0	0	0	-	網路設備總數量 （Core switch 、 Router 等）		-	-
其他	21	0	0	0	-	資安設備總數量		-	-
其他	0	0	1200	0	-	郵件帳號數量 (社交工程演練)	電子郵件社交工程測試 含初、複掃、教育訓練、 課後測驗(兩次各一小時，以影片或實體授課方式進行)	-	-
其他	-	-	-	-	-	主機弱點掃描檢測作業	依據電子銀行安控規章 每季執行弱點掃描 (2022Q2~2023Q1) 端點數共計 562 台 含正式、測試伺服器 核心系統正式、測試伺服器 網路、資安設備、ATM	-	-

							櫃台工作站、OA 工作站 SWIFT 相關主機		
其他	0	0	0	0	-	DDoS 防護評估	中央存保資訊安全要求項目 1、需可提供至少 20M 攻擊頻寬及至少 20 個連線 IP 來源並配合本行之需求即時控制流量，確保線上系統不受影響。 2、攻擊方式提供快速及慢速攻擊(分別至少 2 種攻擊方式)，需擬定攻擊計劃並與本行協調後決定。 3、廠商執行測試服務須配合本行規劃之非營業時段進行(如晚上 10:00 至凌晨 00:00)進行。	-	-
其他	0	200	0	0	-	正式環境伺服器	執行伺服器安全設定檢視	-	-

壹拾壹、 交付項目

評估單位於專案期間應至少包含但不限於下列項目：

一、 工作計劃書：決標日起2週內交付。工作計畫書應以評估單位投標時之「建議書」為基礎，並依採購評選意見修改。內容除包括對本專案之執行敘述，含專案管理、組織、人力、分工、職掌、工作項目、執行程序(網路/個人電腦/伺服器)、時程說明(包括起始會議與結束會議)、預計檢測的範圍與影響、雙方準備事項、工作進度稽核點及品質管理流程。雙方準備事項建議包括：預計檢測之個人電腦清單(IP、所安裝之作業系統與應用程式)、預計檢測之伺服器清單(IP、用途、所安裝之作業系統與應用程式、管理人員)、網路架構圖(標示部署設備位址)、網路設備紀錄檔、協同檢測人員名單

二、 資訊安全評估服務報告：依工作計畫書載明之交付時程。文件內容至少包含評估人員資格、評估範圍、評估作業項目與標的、評估紀錄、評估時所發現之缺失項目、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。

三、 專案執行記錄檔：依工作計畫書載明之交付時程。文件內容應包括：各個人電腦的

資安檢測結果表、各伺服器主機的資安檢測結果表、網路側錄封包分析資料、發現惡意行為或惡意程式的過程紀錄(如果有發現)、外洩資料列表(如果有發現)、惡意程式(如果有發現)。

四、 其他專案文件

除上述專案文件外，評估單位應依各工作項目之性質與內容，詳述並交付相關文件或資料，如：評估發現、專案工作會議紀錄等。

壹拾貳、 驗收或付款事項與權責

一、 驗收事項

（一）依據雙方協議確定之工作說明書內容進行驗收。

（二）乙方應於完成工作說明書所載事項後以書面通知甲方進行驗收。

二、 驗收權責

(一) 評估單位應於簽約後依階段規劃完成必要之工作事項。

(二) 評估單位應依工作說明書規定時程，將各階段所列應交付項目交付本行簽收，如有違約事宜，本公司得以書面通知得標評估單位終止契約或解除契約之部分或全部，且不補償得標評估單位所生之損失。評估單位逾期三十日以上，本行得逕行解除合約。

(三) 若有不可抗力因素或係可歸責於本行之事由（例如：天災、未完成其他配合事項等）致評估單位無法如期完成上開工作者，不在此限。

三、 計價方式

各項費用均以新台幣(含稅)報價。

壹拾參、 智慧財產權

一、 本專案中如使用評估單位既有之文件，評估單位應授權本行為利用專案產品之目的，於該既有部分之著作權存續期間，且不違反文件之限制目的，有在任何地點使用之權利；評估單位不得終止此項授權，且本行不須額外支付任何費用。

二、 評估單位如有使用到開放源碼軟體時，需符合本行開放源碼相關規定且必須載明使用開放源碼之相關資訊。除負責所有授權許可證之問題外，並於合約中載明，若因使用開放源碼而造成本行及客戶損失時，評估單位須負責。

壹拾肆、 保密義務

評估單位特此聲明評估單位財務健全並具備能妥善處理受委託事項之專業技術與設施，

評估單位接受本行部分作業委外，處理受委託事項絕不影響本行健全經營、本行客戶權益及切實配合遵照 107 年 3 月 22 日行政院金融監督管理委員會金管銀(國)字第 10702710050 號函修正發布之「金融機構辦理電腦系統資訊安全評估辦法」與 95 年 09 月 18 日行政院金融監督管理委員會金管銀 (五) 字第 09500386200 號令修正發布之「金融機構作業委託他人處理內部作業制度及程序辦法」暨其嗣後更動之內容辦理。評估單位並保證如下：

一、評估單位保證本合約書所載之受委外項目，確為評估單位合法得辦理之營業項目，於契約有效存續期間內。評估單位須維持履行本契約書 所須取得及維持之一切核准、證照及許可；並遵照中華民國政府主管機關(包括但不限於行政院金融監督委會、經濟部商業司)之一切法令規定。

二、評估單位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、稽核作業及客戶權益，不得有不利之影響及配合確保遵循銀行法、洗錢防制法、電腦處理個人資料保護法、營業秘密法及其他法令之規定。

三、評估單位應訂立員工守則，並具備嚴謹之內部控制制度、經常性之查核及嚴密之稽核作業程序等，留存紀錄以供查核，契約內容如有履行不能、履行困難或履行困難之虞者，對本公司負有立即通知之義務。

四、評估單位同意配合金融監督管理委員會或金融監督管理委員會委託適當機構及本公司內、外稽核人員進行檢查或稽核及提供相關資料及報告，俾本公司足以確認行政院金融監督委會、中央銀行及中央存款保險股份有限公司等取得相關資料或報告及進行金融檢查，本公司於必要時（包括主管機關命其終止或解約）得於事前通知評估單位後終止契約。

五、評估單位就委外事項之範圍，同意主管機關得依銀行法第四十五條規定辦理。

六、評估單位對外不得以本公司名義辦理受委託處理事項。

七、評估單位不得為影響評選結果而利用管道藉與本公司人員或評選委員接觸之機會，採取如請託、關說或行賄等不當或不法行為，亦不得以支付佣金、比例金、仲介金、以謝金或其他利益及財物為條件，促成請購、採購及契約之簽訂，評估單位有上述情形之一者，本公司有權列為拒絕往來評估單位。

八、評估單位非經本公司書面同意，不得將作業複委託。

九、評估單位因本專案之執行，所知悉之一切與本公司業務直接、間接相關之資訊，以及其客戶之財產或帳戶資料，均應視為機密資料，不得以任何形式向第三人揭露。本保密條款於本專案終止或結束後仍繼續有效。

十、評估單位對其參與本專案之員工，應提供其名單予本公司，並對其操守及行為負責，且於簽約時應以公司及個人之名義分別簽訂「廠商保密切結書」及「個人保密切結書」。

壹拾伍、 資訊安全規範

一、乙方於本案作業期間，應遵守金融主管機關所頒訂之各項資訊安全規範及標準，並遵守甲方資訊安全管理及保密相關規定。

二、乙方所有參與本案人員均應據實簽署保密切結書，乙方並應對本案人員之保密義務負連帶保證責任，甲方並得對乙方實施之保密作業進行稽核。

三、乙方提供之設備（軟、硬體），應證明無內藏惡意程式（如病毒、蠕蟲、特洛伊木馬、間諜軟體等）及隱密通道（covert channel）或其他安全性問題。

四、倘因乙方提供之設備（軟、硬體）致甲方遭受損害，乙方應負賠償責任；如致他人權利受有損害時，乙方亦應負責。

壹拾陸、 其他規定

本建議書徵求文件所有條文敘述，概以本行之解釋為準，如有未盡事宜，應依相關法規或主管機關函釋辦理。