金融機構辦理電腦系統資訊安全評估辦法

本會 103 年 5 月 29 日第 11 屆第 2 次理事會議通過
103 年 7 月 10 日金管銀國字第 10300173840 號函洽悉
本會 105 年 10 月 14 日第 12 屆第 1 次理監事聯席會議通過
106 年 2 月 15 日金管銀國字第 10500259500 號函洽悉
本會 107 年 1 月 25 日第 12 屆第 14 次理監事聯席會議通過
107 年 3 月 22 日金管銀國字第 10702710050 號函洽悉

第一條　前言

為確保金融機構提供電腦系統具有一致性基本系統安全防護能力並遵循中華民國銀行商業同業公會全國聯合會制訂之「金融機構資訊系統安全基準」及「金融機構辦理電子銀行業務安全控管作業基準」，擬透過各項資訊安全評估作業，發現資安威脅與弱點，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，訂定本辦法。

第二條　用詞定義

一、SWIFT：係指環球銀行金融電信協會 (Society for Worldwide Interbank Financial Telecommunication)。

二、物聯網設備：係指具網路連線功能並連線於 Internet 或 Intranet 之嵌入式系統(具有小型作業系統)設備，包含自動化辦公設備(如數位錄影機、電話交換機、傳真機、錄音設備、影印機等)及不具備遠端操控介面功能之感測器。

第三條　評估範圍

一、 金融機構應就整體電腦系統(含自建與委外維運)依據本辦法建構一套評估計畫，基於持續營運及保障客戶權益，依資訊資產之重要性及影響程度進行分類，定期或分階段辦理資訊安全評估作業，並提交「電腦系統資訊安全評估報告」，辦理矯正預防措施，並定期追蹤檢討。

二、 評估計畫應提報董(理)事會或經其授權之經理部門核定，但外國銀行在臺分行，得由總行授權之人員為之。評估計畫至少每三年重新審視一次。

第四條　電腦系統分類及評估週期

一、 電腦系統依其重要性分為三類：

電腦系統類別	定義	評估週期
第一類	直接提供客戶自動化服務或對營運有重大影響之系統(如電子銀行、分行櫃台、ATM 自動化服務及 SWIFT 等系統)	每年至少辦理一次資訊安全評估作業
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

二、 單一系統且為數眾多之設備得以抽測方式辦理，抽測比例每次至少應占該系統全部設備之 10%或 100 台以上 (如 ATM、KIOSK 及分行櫃台端末設備等)；其中相同作業系統與安全更新之 ATM 及 ATM 之相關伺服器至少應抽測一台，相同 ATM 之相關伺服器應用系統版本至少應抽測一台。

三、 單一系統發生重大資訊安全事件，應於三個月內重新完成資訊安全評估作業。

第五條 資訊安全評估作業

一、 資訊安全評估作業項目：

(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、端末設備及物聯網等設備之弱點掃描與修補作業。

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。

(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。

(五) 客戶端應用程式檢測

針對銀行交付給客戶之應用程式進行下列檢測：

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)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。

(七) 合規檢視

１、檢視電腦系統是否符合本會制定之「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本會制定之「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」、主管機關及本會相關函文之要求。

３、檢視電腦系統之 SWIFT 系統是否符合 SWIFT 公布之 Customer Security Programme 規範及本會相關函文之要求，若與本辦法資訊安全評估作業衝突，依 SWIFT 公布為主。

二、　第一類電腦系統應依前款辦理資訊安全評估作業；第二類及第三類電腦系統於第一次辦理資訊安全評估作業時，得依系統特性選擇前款必要之評估作業項目，惟應於每次選擇項目辦理之翌次，依前款辦理完整評估，以瞭解銀行整體資訊系統風險；嗣後電腦系統依評估週期辦理時，亦同。

第六條　社交工程演練

每年應至少一次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。

第七條　評估單位資格與責任

一、 評估單位可委由外部專業機構或由金融機構內部單位進行。如為外部專業機構，應與提供、維護資安評估標的之機構無利害關係，若為金融機構內部單位，應獨立於電腦系統開發與維護等相關部門。

二、 辦理第一類電腦系統資訊安全評估作業之評估單位應具備下列各款資格條件；辦理第二類及第三類電腦系統資訊安全評估作業者，依評估作業項目需要，具備下列相關資格條件之一：

(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。

(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。

(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。

(四) 熟悉金融領域載具應用、系統開發或稽核經驗。

三、 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，評估單位應簽立保密切結書並提供適當保護措施，以防止資料外洩。

四、 評估單位及人員不得隱瞞缺失、不實陳述、洩露資料及不當利用等情事。

五、 本國銀行海外分支機構之資訊安全評估作業應依據當地國家或地區相關規定辦理，若當地無相關規定，仍應遵循本辦法規定。

第八條　評估報告

一、 「電腦系統資訊安全評估報告」(以下簡稱評估報告)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。

二、 應依據評估報告內容缺失程度區分風險等級，並擬定各風險對應之控管措施及處理時限，送稽核單位進行缺失改善事項之追蹤覆查。

三、 評估報告缺失覆查應提報董（理）事會或經其授權之經理部門，但外國銀行在臺分行，得由總行授權之人員為之，以落實由高階管理階層督導缺失改善。

四、 評估報告應併同缺失改善等相關文件至少保存五年。

第九條　公告實施

本辦法應經中華民國銀行商業同業公會全國聯合會理事會議核議通過，並報奉主管機關核備後公告實施，修正時亦同。