主題四

本國銀行近期資訊作業主要檢查缺失態樣及年度檢查重點說明

檢查局

107年2月5日

- 資訊作業檢查發現
- 107年度資安檢查重點

本國銀行資訊安全專案檢查

- ✓ **聚焦五大範疇之資訊作業專案**
  - 組織管理
  - 電子銀行安全控管
  - 個人資料安全維護
  - 災害應變
  - 委外作業管理
- ✓ **特定主題專案**
  - 電子商務資訊作業專案
  - 數位金融服務專案
  - SWIFT系統資安專案

本國銀行資訊作業專案檢查意見態樣

組織管理

- ✓ 未研訂資訊安全政策，或資訊安全政策內容或制定過程欠完善，或未落實執行。
- ✓ 作業規範之修訂與執行情形有欠確實。
- ✓ 職務分工有違牽制原則。
- ✓ 辦理自行查核業務有欠完善。

本國銀行資訊作業專案檢查意見態樣

電子銀行安全控管

- **網路安全控管及防範措施**
  - ✓網路架構設計不當及管控機制欠完備。
  - ✓網路防火牆規則設定不當或異動程序欠妥善。
  - ✓弱點掃描範圍或項目欠完整或未落實漏洞修補作業。
  - ✓網路監控作業欠妥適。

本國銀行資訊作業專案檢查意見態樣

電子銀行安全控管

- **系統維護與管理**
  - ✓未建置資訊資產管理機制，或作業管理欠落實。
  - ✓作業系統參數(如：密碼原則、稽核原則)設定管理或定期檢視作業欠妥。
  - ✓使用者帳號使用管理及權限設定欠妥適。
  - ✓對行員使用虛擬私有網路(VPN)，自行外登入銀行內部網路之控管措施欠妥適。
  - ✓對個人電腦網路位址、最高權限帳號、安裝之軟體及各類儲存裝置未建立控管機制或管理欠妥。

本國銀行資訊作業專案檢查意見態樣

電子銀行安全控管

- **電子銀行業務系統維護與管理**
  - ✓ 網路銀行交易安全設計，未符合安控作業基準。
  - ✓ 電子銀行系統所建立之預警監測條件設定欠完整
  - ✓ 對程式或資料變更管理有欠妥善。
  - ✓ 對電子郵件社交工程，未建置妥適安全控管機制
  - ✓ 對行動銀行等應用程式(APP)之設計及管理欠妥適。

本國銀行資訊作業專案檢查意見態樣

個人資料安全維護

✓個資清查未確實或範圍有欠完整。
✓正式與測試環境傳檔作業未建立妥適控管機制。
✓對個資之儲存(包括存放方式有無去識別化、加密情形)未建立妥適之控管機制。
✓涉及個資之報表或檔案等之存取控管有欠嚴謹。
✓對客戶個人資料檔案之刪除、保管及使用未建立相關控管機制。
✓涉及客戶個資檔案以明碼方式傳送，或將客戶個資檔案置於DMZ區，對外傳遞亦未建置完善之加密通訊保護機制。

本國銀行資訊作業專案檢查意見態樣

個人資料安全維護

- ✓未留存個資存取之完整稽核軌跡，或未建立覆核機制，或對稽核報表之覆核作業欠確實。
- ✓對隨身碟等可攜式儲存媒體未建立使用控管機制。
- ✓對網路芳鄰、電子郵件等具傳檔功能之應用程式使用控管欠妥。
- ✓對傳檔伺服器之使用者帳號密碼管理及存取權限設定欠妥適。
- ✓辦理個資外洩應變演練之模擬情境有欠完整或演練作業欠周延。

本國銀行資訊作業專案檢查意見態樣

災害應變

- ✓ 未辦理營運中斷衝擊分析及備援需求，或分析範圍未臻周全。
- ✓ 部分業務異地備援能力不足，或備援機制欠佳
- ✓ 辦理備援演練作業有欠確實或演練範圍不足，或演練結果未依規陳報及建立追蹤控管機制。

本國銀行資訊作業專案檢查意見態樣

委外作業管理

- ✓ 委外合約內容未符法令規定或所訂條款有欠妥善。
- ✓ 對廠商作業之監督管理欠當。
- ✓ 未妥善控管交易資料傳輸系統存取權限，致有非處理人員取得權限者；另未確實監控受託機構存取客戶資料情形，致有未經銀行許可即自行下載客戶交易資料。
- ✓ 對應用系統委外開發廠商之監督管理欠妥適。

電子商務資訊作業專案檢查意見態樣

電子支付及行動支付作業環境之安全管理

- ✓ 未妥適設定伺服器系統安全參數
- ✓ 弱點掃描及漏洞修補欠落實
- ✓ 管理規範未配合法規適時增(修)訂
- ✓ 特權帳號使用管理欠周延
- ✓ 異常交易篩選指標欠完整
- ✓ 辦理電腦系統資訊安全評估作業，對評估報告所列改善事項之後續追蹤管理欠確實。
- ✓ 對代收代付服務平台業者提供行動支付應用系統之資安及資料保護等未建立風險評估之管理機制

電子商務資訊作業專案檢查意見態樣

行動應用APP之安全管理

- ✓ 開發及上架作業程序及管理規範之訂定欠完整
- ✓ 對委外開發之APP未取得原始碼者未訂定因應措施
- ✓ 程式變更及原始碼檢測作業未臻周全等
- ✓ 對簽約合作之平台業者提供行動支付APP，均未建立事前驗證、測試及事後查核之機制

電子商務資訊作業專案檢查意見態樣

消費者保護

- ✓ 部分APP服務之使用者同意條款內容欠當
- ✓ 與異業合作推廣信用卡收單業務，合作對象涉及信用卡等機敏資料之蒐集、傳輸及處理，有逾越雙方所訂合約之交易模式，銀行未善盡監督管理之責

數位金融服務專案檢查意見態樣

數位金融服務系統運作管理

- ✓ 未落實執行所訂系統安全管理及使用者帳號存取權限等相關標準作業程序，如：主機(含資料庫)作業系統安全參數設定、使用者帳號授權、系統安全漏洞檢測及弱點修補作業、以及資訊安全事件之監控等。
- ✓ 對行動應用App之安全管理機制不足，如：未訂定App上架安控內部規範、未確實遵循銀行公會「金融機構提供行動裝置應用程式作業規範」，建立App所需權限之檢視機制及偽冒App偵測機制等。

數位金融服務專案檢查意見態樣

數位金融服務業務流程控管

✓對數位存款帳戶開戶審查作業欠完備，如：對於無關連客戶，卻使用同一IP申辦帳戶、或無關連客戶卻有留存相同手機號碼或電子郵件信箱等異常線上申辦情形，未建立系統檢核或人工審查機制，恐有被利用開立人頭帳戶之疑慮。

➢正確作法

依線上服務所涉非面對面交易之特性，建置異常開戶表徵，強化開戶審查措施。

數位金融服務專案檢查意見態樣

數位金融服務防制洗錢管作業

✓名單比對控管機制欠嚴謹或名單檢核流程欠妥適：如：名單資料庫之選用機制欠妥適、重要政治性職務之人(PEPS)建檔範圍欠完整、提供線上檢核流程之功能設計欠妥等。

✓對數位存款帳戶之高風險客戶持續審查作業欠妥善，如：未依規每年規劃辦理持續審查措施、或未完整記錄客戶審查結果、對不配合定期審查之帳戶尚無後續處理措施等。

✓對符合疑似不法或異常交易表徵之數位存款帳戶交易未依規進行查證作業，或未記錄查證情形並檢附查證資料等。

數位金融服務專案檢查意見態樣

數位金融服務業務流程控管

✓未落實內部控制三道防線運作機制，如：開辦電子銀行低風險交易業務前，未確實經法遵、稽核及資訊部門確認各項作業程序符合相關法規，多致數位存款帳戶開戶審查作業有多項未符合銀行公會作業範本之要求。

➢正確作法

應建立各部門間之洽會機制、留存驗證軌跡及各部門建議事項追蹤控管機制等

SWIFT系統資安專案檢查意見態樣

✓**SWIFT伺服器或工作站未實體隔離，且系統使用者帳號與授權管理欠當**

- 主機或工作站未建立專屬獨立網段或作其他適當區隔。
- 系統維護員持用最高權限帳號辦理日常維護作業；未完整納管作業系統高權限帳號且未覆核其作業稽核軌跡。
- 未妥適控管SWIFT應用系統高權限帳號(LSO、RSO及swpadmin)及定期檢視其他使用者帳號之授權狀況。
- 未落實檢核與設定系統安全參數。

SWIFT系統資安專案檢查意見態樣

✓網路安全防禦機制未臻落實

- **網路環境及SWIFT連線管理有欠嚴謹**，如：未妥適管控遠端連線SWIFT系統伺服器或工作站之功能；SWIFT系統伺服器啟用代理服務功能，可逕自連結網際網路；全行個人電腦或工作站均能以瀏覽器連結執行電文輸入作業，或專屬工作站可上網及收發電子郵件；未留存維護SWIFT伺服器稽核軌跡。
- **防火牆規則之維護管理欠妥**，如：防火牆規則檢視欠確實，未刪除無作業需求之連線，或防火牆規則過於寬鬆。
- **對海外分行未建立妥適網路通訊及資訊安全管理機制**，不利掌握及督導管理海外分行資安風險。
- **對網路資安事件未建立妥善之應變管理機制**，如：委外辦理網路安全監控作業，對廠商通報之網路資安事件，內部未建立相關通報處理程序。

SWIFT系統資安專案檢查意見態樣

✓SWIFT系統之資安控管欠周延

- **SWIFT電文系統架構之設計及存取權限控管欠妥**，如：收集電文資料儲存於SWIFT系統伺服器之磁碟目錄，且未管制存取權限。
- **未建立SWIFT應用系統程式變更管理程序**，如：未訂定標準程式更新程序，包括更新應用程式覆核機制；應用程式變更歷程未留存完整稽核軌跡；未定期檢視SWIFT系統及檔案之完整性。
- **系統日誌管理欠妥適，不利分析異常行為及預作警示**，如：未集中收錄重要及關鍵作業紀錄；系統稽核軌跡之監控指標欠完備；未建立系統日誌重要事項之檢視及對提示警告訊息後續處理等機制。
- 對SWIFT組織發布之連線安全事項或客戶資安計畫(CSP)，尚未完成差異化評估及規劃改善期程。

107年度資通安全管理檢查重點

- 資安專責單位與專責主管之設置及指派情形
- ATM及SWIFT等支付系統安全防護措施
- 數位金融業務應用系統安全控管機制：身分認證、交易安全設計、異常交易監控及預警等；APP開發及上架之管理機制。
- 網路安全措施：防火牆、入侵偵測防禦、弱點掃描及滲透測試等資安防禦措施；網路攻擊事件監控、通報及應變機制；模擬駭客攻擊情境演練作業。
- 數位證據之蒐集、保留程序與機制。

結　語

- 攻擊特徵
  - ✓利用長假前後發動攻擊
  - ✓入侵管道不明
  - ✓以合法掩護非法
- 金融機構弱點
  - ✓業務淩駕資安
  - ✓未落實內部控制措施

加強春節期間資安控管措施

持續注意強化資通安全防護機制，落實遵循相關資安自律規範。

感謝聆聽

敬請指教