缺失態樣

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。

缺失情節

- 對個資外洩應變演練之模擬情境，未依本會規定納入外部網路入侵、非法或異常使用行為所致之個資外洩事件等情境。
- 辦理個資演練僅為敘述性討論，未研擬具體演練案例；或未將個資外洩後如何防止損害擴大及通知客戶等重要作業程序納入演練，演練作業有欠確實、周延。

改善作法

- 對外部網路入侵及非法或異常使用行為等所致之個資外洩事件，應依規定納入演練情境辦理演練。
- 應訂定個資外洩事件通知當事人等應變演練處理程序，並確實辦理演練。

缺失態樣

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。

缺失情節

- 行員因業務需要，須由行外遠端連線至銀行內部處理事務，未申請虛擬私有網路帳號，以借用他人帳號作業，致有多人共用使用者帳號之情形。
- 對行員使用虛擬私有網路帳號登入銀行內部網路之行為，未留存使用稽核紀錄；或雖已留存使用稽核紀錄，惟未對該紀錄建立覆核機制。

改善作法

- 對行員使用虛擬私有網路帳號應訂定相關管理規範並建立控管機制。行員依規定提出申請，應依業務需要覈實審核，並嚴禁行員共用帳號，以明權責。
- 對使用虛擬私有網路帳號自遠端登入者，應留存使用之稽核紀錄，建立事後審核措施，並落實執行。

缺失態樣

未落實個人資料之使用及控管作業。

缺失情節

- 辦理資訊系統應用程式變更作業，有運用個人資料進行測試後，未予去識別化或刪除，逕留存於資訊部門檔案卷宗，不利個人資料保護作業。
- 申請將個人資料以電子檔案型式輸出利用，惟未建立個人資料運用後刪除之控管程序，不利於控管個人資料使用情形。

改善作法

應建立客戶資料產製運用及使用後刪除之控管機制。

缺失態樣

對於端點控制及敏感性個人資料遮罩之控管措施欠妥適；對外傳送電子郵件未建立有關個人資料之過濾機制。

缺失情節

- 對負責保單保全、收費及客戶服務話務人員有授予端點控管軟體解密權限，且其使用之個人電腦開放使用 USB，致有資料外流風險。
- 測試作業主機資料庫未對敏感性個人資料欄位予以遮罩；各作業部門對於作業過程中使用之個人資料仍置於本機電腦未予刪除，致他人登錄時仍可讀取之情形。
- 對於經由電子郵件系統對外傳送含有個資或機敏資料，未建立過濾機制及控管措施。

改善作法

- 涉及個資之存取，應嚴格控管該等資料之存取權限，依職務需要覈實授權，並應對資料之存取及傳遞建立申請、保管、使用及刪除等規範，並留存完整稽核軌跡、建立主管覆核及定期清查等管控機制。
- 應避免將客戶真實資料複製至測試環境作業，如確有須將未去識別化個資複製至測試環境之業務需求，應建立申請、刪除、留存完整稽核軌跡等管控程序。
- 應建置電子郵件內文過濾系統，並就對外傳送含有個資或機敏資料之電子郵件建立審核及追蹤控管機制。