專營電子支付機構檢查手冊(異動版)

一、業務管理(共 3 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.3.3.3	提供使用者辦理不特定金額代理收付實質交易之自動交易扣款時，是否確認特約機構之交易安全機制及交易爭議處理流程後始得辦理？	提供使用者辦理不特定金額代理收付實質交易之自動交易扣款時，是否依規定限制交易或用途？	1.電子支付機構管理條例第 18 條 2.電子支付機構業務管理規則第 7、10、11、17、18、21、24 條	因應「電子支付機構業務管理規則」第 11 條規定修正。
3.4.3	是否對現有外籍移工身分資料及居留證有效性進行持續審查？	是否於外籍移工註冊時及註冊後每月執行行蹤不明外籍移工之查核作業？	外籍移工國外小額匯兌業務管理辦法第 12~16 條	因應「外籍移工國外小額匯兌業務管理辦法」第 14 條規定修正。
3.6	是否於行動裝置應用程式揭示下列重要資訊	是否於外籍移工註冊及辦理匯兌交易時揭示下列重要資訊	外籍移工國外小額匯兌業務管理辦法第 12~16 條	因應「外籍移工國外小額匯兌業務管理辦法」第 16 條規定修正。

二、資訊作業(共 20 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.5	5.是否於每年四月底前由會計師檢視提出資訊系統及安全控管作業評估報告？	5.是否於每年四月底前由會計師檢視提出資訊系統及安全控管作業評估報告？	~~電子支付機構資訊系統標準及安全控管作業基準第 26 條~~ 電子支付機構資訊系統標	配合「電子支付機構資訊系統標準及安全控管作業基準」(下稱電支安控基準)修訂，修正所援

資料基準日：113 年 12 月 31 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
			準及安全控管作業基準第27條	引之條次。
2.4	4.是否每年檢視防火牆及具存取控制（Access control list，ACL）網路設備之設定？每年檢視防火牆是否開啟具安全性風險或非必要之通訊埠，連線設定是否有安全性弱點？	4.是否至少每年一次檢視防火牆及具存取控制（Access control list，ACL）網路設備之設定？	電子支付機構資訊系統標準及安全控管作業基準第21條	配合電支安控基準修訂，修正查核事項。
2.5 2.5.1 2.5.2	5.經由網際網路連接至內部網路進行遠距之系統管理工作，是否至少每年審查一次申請使用及授權之適當性？若涉及變更作業，是否採用照會或二項(含)以上安全設計並經主管授權？是否定義可連結之遠端設備並建立監控機制？ (1)如使用虛擬私有網路（VPN），是否訂定作業規範，建立日誌檢視、攻擊偵測、事件應變及事件復原機制，並採用高強度密碼或多因子進行身分驗證？ (2)如使用異地辦公之虛擬桌面	5.經由網際網路連接至內部網路進行遠距之系統管理工作，是否至少每年審查一次申請使用及授權之適當性？若涉及變更作業，是否採用照會或二項(含)以上安全設計並經主管授權？是否定義可連結之遠端設備並建立監控機制？	電子支付機構資訊系統標準及安全控管作業基準第21條	配合電支安控基準修訂，修訂網際網路連接至內部網路進行遠距之系統管理工作之查核事項。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	（VDI），是否訂定作業規範，避免連接本機印表機印出檔案、連接可卸除裝置存取檔案或透過剪貼簿於兩端剪貼資料，並採用高強度密碼或多因子進行身分驗證？			
2.10	10.是否每季進行資訊系統弱點掃描，並確認掃描工具為新版本？電子支付平臺是否每年執行滲透測試，並依風險等級進行處理及留存紀錄？	10.是否每季進行資訊系統弱點掃描？電子支付平臺是否每年執行滲透測試，並依風險等級進行處理及留存紀錄？	電子支付機構資訊系統標準及安全控管作業基準第20條	配合電支安控基準修訂，修正查核事項。
2.14	14.針對其他網路區域所連接具IP網路連線功能並實際連線於Internet或Intranet之辦公設備，是否建立管理清冊並定期更新，每年至少盤點一次並留存紀錄？是否具備安全性更新機制，或限制其網際網路連線能力、加強存取控制或進行網路連線行為監控？		電子支付機構資訊系統標準及安全控管作業基準第21條	配合電支安控基準修訂，新增物聯網設備之查核事項。
3.1.4.7	⑦應每年由合格實驗室依據行動應用資安聯盟「行動應用APP基本資安檢測基準」辦理並通過檢測；針對應用程式及其應用伺服	⑦應每年由合格實驗室辦理並通過檢測，且由資安專責主管確認完成改善。	電子支付機構資訊系統標準及安全控管作業基準第11條	配合電支安控基準修訂，修正查核事項。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	器之完整功能辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞；辦理國內外小額匯兌者，應依據 OWASP 公布之 Mobile ApplicationSecurity Checklist L2 項目辦理檢測；應建立檢測報告之檢視機制，並送資安專責主管監控及執行資訊安全管理作業。			
3.1.4.8	⑧應用程式及其應用伺服器新功能首次上線、系統架構異動或既有功能異動時，應針對新增或異動之程式辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞；辦理國內外小額匯兌者，應依據 OWASP 公布之 Mobile Top 10 項目辦理檢測，並修正中/高風險漏洞。	⑧應用程式及其應用伺服器於每年、新功能首次上限、系統架構異動或既有功能異動時，應針對新增或異動之程式辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞；辦理國內外小額匯兌者，應依據 OWASP 公布之 Mobile APP Security Checklist L2 或 Mobile Top 10 項目辦理並通過檢測，且由資安專責主管確認完成改善。	電子支付機構資訊系統標準及安全控管作業基準第 11 條	配合電支安控基準修訂，修正查核事項。
3.1.4.14	⑭行動應用程式有使用第三方函式庫或元件之需要時，應評估安全風險及妥善管控程序，並應留存評估記錄。		電子支付機構資訊系統標準及安全控管作業基準第 11 條	配合電支安控基準修訂，新增使用第三方函示庫或元件之查核事項。
3.1.6.6	⑥應設定安全性表頭（Security	⑥應設定安全性表頭（Security	電子支付機構資訊系統標	配合電支安控基準修

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	Headers），限定代理存取端僅針對指定之內容類型進行處理（X-Content-Type-Options：nosniff），並防止辦理身分確認之網頁為其他網站嵌入（X-Frame-Options：deny、sameorigin）。	Headers），限定代理存取端僅針對指定之內容類型進行處理（X-Content-Type-Options：nosniff），並防止辦理身分確認之網頁為其他網站嵌入（X-Frame-Options：deny）。	準及安全控管作業基準第11條	訂，修正查核事項。
3.1.8	(8)開放應用程式介面（Open API）：如有使用第三方開放應用程式介面之需要時，應進行安全風險評估及妥善管控程序，並應留存評估記錄。		電子支付機構資訊系統標準及安全控管作業基準第11條	配合電支安控基準修訂，新增使用開放應用程式介面之查核事項。
3.3.1	(1)是否建立人員之註冊、異動及撤銷註冊程序，並依最小權限（least privilege）及僅知原則（need-to-know）配置適當之權限？	(1)是否建立人員之註冊、異動及撤銷註冊程序？	電子支付機構資訊系統標準及安全控管作業基準第15條	配合電支安控基準修訂，修正查核事項。
3.3.2	(2)是否定期審查帳號與權限之合理性及異常存取紀錄？人員離職或調職時是否盡速移除權限？	(2)是否定期審查帳號與權限之合理性？人員離職或調職時是否盡速移除權限？	電子支付機構資訊系統標準及安全控管作業基準第15條	配合電支安控基準修訂，修正查核事項。
3.3.3	(3)最高權限帳號或具程式異動、參數變更權限之特權帳號是否符合下列要求：	(3)最高權限帳號或具程式異動、參數變更權限之特權帳號，是否依使用人員職務範圍等予以限	電子支付機構資訊系統標準及安全控管作業基準第15條	配合電支安控基準修訂，新增最高權限帳號或具程式異動、參數變

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.3.3.1 3.3.3.2 3.3.3.3 3.3.3.4	①應與日常維運帳號區隔，並列冊保管。 ②應使用特權帳號管理系統，採取適當之限制存取權限並評估設定之合理性，以降低帳號密碼洩露風險；無法由特權帳號管理系統納管之帳號，密碼應採兩人以上分持管理或其他管控措施，以符合作業牽制原則。 ③最高權限帳號使用時須先取得權責主管同意，並保留稽核軌跡，且定期覆核使用結果。 ④用於提供網際網路服務之伺服器及 AD（網域服務）主機者，應採雙因子認證。	制？相關使用是否經核准並留存稽核軌跡？		更權限帳號之查核事項。
3.8.3	(3)是否建置管控名單管理機制？對於線上即時交易是否即時驗證？非線上即時交易是否每日更新管控名單？使用於網際網路交易功能者，是否即時驗證？	(3)是否建置管控名單管理機制？對於線上即時交易是否即時驗證？非線上即時交易是否每日更新管控名單？	電子支付機構資訊系統標準及安全控管作業基準第12條	配合電支安控基準修訂，修正查核事項。
3.8.4	(4)儲值卡端末設備於非接觸式讀卡機交易時，若詢卡發現一張以上的卡片回應，是否主動拒絕交易，並顯示交易失敗？是否配合	(4)儲值卡端末設備設計是否為感應距離限縮 10 公分以下、交易過程是否有聲音、燈號或圖像等提示，以防止特約機構不當扣	電子支付機構資訊系統標準及安全控管作業基準第12條	配合電支安控基準修訂，修正查核事項。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	採用其他技術防護措施，如消費行為分析或讀卡機 SAM 卡 sign on 檢查（軟體式 SAM 讀卡機除外）？交易過程是否有聲音、燈號或圖像等提示，以防止特約機構不當扣款？	款？		
3.10 3.10.1 3.10.2	10.電子支付核心系統轉換或架構重大調整且逾內部規範之最大可容忍中斷時間者，是否符合下列要求： (1)系統異動前之準備工作：是否建立架構審查機制？是否建立上線及復原計畫，並建立多個檢核點及啟動復原之決策條件？是否進行上線變更審查及風險評估，辨識複雜度及影響範圍？是否召開上線協調會議？是否請資安人員參與異動前關鍵準備工作，如：架構審查、上線變更審查及風險評估、上線協調會議等事項？ (2)系統異動作業：是否執行系統及資料備份、驗證各項變更作		電子支付機構資訊系統標準及安全控管作業基準第 26 條	配合電支安控基準修訂，新增支付核心系統系統轉換或架構重大調整之查核事項。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.10.3	業及資料內容？ (3)系統異動後之事件管理：是否持續監控系統，確保資料正確、功能正常、系統穩定？是否成立應變小組，並落實事故應變？是否追蹤根因，提出短中長期改善方案並持續追蹤？			
5.2.1	(1)是否將各作業系統、網路設備及資安設備之日誌及稽核軌跡集中管理，進行異常紀錄分析，設定合適告警指標並定期檢討修訂？原始日誌及稽核軌跡是否至少保存二年？	(1)是否將各作業系統、網路設備及資安設備之日誌及稽核軌跡集中管理，進行異常紀錄分析，並設定合適告警指標並定期檢討修訂？	電子支付機構資訊系統標準及安全控管作業基準第24條	配合電支安控基準修訂，修正查核事項。
5.2.5	(5)是否建立資訊安全事故評估、通報、處理、應變及事後追蹤改善作業機制，並應留存相關作業紀錄？	(5)是否建立資訊安全事故通報、處理、應變及事後追蹤改善作業機制，並應留存相關作業紀錄？	電子支付機構資訊系統標準及安全控管作業基準第24條	配合電支安控基準修訂，修正查核事項。
6.4	4.支付核心系統之委外開發項目，專案成員是否有資安專責人員參與？是否妥善管理受託廠商之實體與邏輯存取權限；如涉個人資料交換，是否確認符合我國個人資料保護法相關規定？委外服務		電子支付機構資訊系統標準及安全控管作業基準第23條	配合電支安控基準修訂，新增支付核心系統委外開發之查核事項。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	變更前，是否執行資訊安全風險評估並擬訂風險處理措施？			
6.5 6.5.1 6.5.2 6.5.3 6.5.4	5.委託作業涉及使用雲端服務管理，包括： (1)是否訂定使用雲端服務之政策及原則，並採取適當風險管控措施？ (2)是否具專業技術及資源，監督雲端服務業者執行受託作業，或委託專業第三人輔助監督作業？ (3)對於自行委託，或與委託同一雲端服務業者之金融機構聯合委託獨立第三人查核雲端服務業者，是否確認其查核範圍涵蓋雲端服務業者受託處理作業相關之重要系統及控制環節？是否評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準？是否對所委託作業範圍進行查核並出具報告？ (4)傳輸及儲存客戶資料至雲端服務業者，是否採行客戶資料加密或代碼化等有效保護措施？是		電子支付機構業務管理規則第 45-1 條	1.配合「電子支付機構業務管理規則」修訂，新增之委外作業涉及使用雲端服務之查核事項。 2.配合電支安控基準修訂，新增雲端服務緊急應變計畫及終止委託移轉機制之查核事項。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	否訂定妥適之加密金鑰管理機制？			
6.5.5	(5)對委託雲端服務業者處理之資料，是否保有完整所有權？除執行受託作業外，是否確保雲端服務業者不得有存取客戶資料之權限，並不得為委託範圍以外之利用？			
6.5.6	(6)委託雲端服務業者處理之客戶資料及其儲存地如位於境外，是否保有指定資料處理及儲存地之權利？境外當地資料保護法規是否低於我國要求？除經主管機關核准者外，客戶重要資料是否在我國留存備份？			
6.5.7	(7)是否訂定雲端服務緊急應變計畫及終止委託之移轉機制？緊急應變計畫是否包含如何確保順利移轉至另一雲端服務業者或移回自行處理，並確保原受託雲端服務業者留存資料全數刪除或銷毀？		電子支付機構資訊系統標準及安全控管作業基準第23條	