玖、資訊作業之查核

業務別項目編號	查核事項	法令規章	評核項目編號
1	一、組織管理		28
1.1	(一)整體作業規劃、資安政策及規範之制定及執行		28
1.1.1	1.是否配合金融機構業務發展與營運目標之需要，建置跨部門之溝通平台共同研訂資訊作業短中長期計畫？董事會與高階管理階層對短中長期計畫是否參與？		28
1.1.2	2.資訊安全政策之訂定是否妥適，經董事會核准並定期檢討修訂？對於資訊安全政策是否確實有效遵循？		28
1.1.3	3.資訊作業相關之操作、管理、查核等各層面規定是否完整訂定，是否配合法令及業務現況適時檢討，並洽會有關單位(如資訊、稽核、企劃、會計、業務…等)共同參與增修？各項作業規範是否確實有效遵循？	「金融機構資訊系統安全基準」	28
1.1.4	4.首次辦理低風險交易之電子銀行業務，是否由資安、法遵及風控等單位建立各部門間之連繫機制、確認相關作業符合安控基準及相關定型化契約等相關法令規定，留存驗證軌跡及各部門建議事項追蹤控管機制？是否於開辦後六個月內重新檢視並作成報告?內部稽核單位是否依據交易量與金額等評估新種業務之風險，排定內部稽核計畫辦理查核，並對評估風險偏高者適時辦理專案查核，落實內部控制三道防線之運作？	「金融機構辦理電子銀行業務安全控管作業基準」	28
1.1.5	5.發展金融科技服務，董事會與高階管理階層是否有效評估金融科技經營與風險管理？是否同時評估金融服務使用雲端運算、大數據分析個資管理、行動應用App安全等資安風險？是否將相關資訊安全管理納入公司治理架構？		28
1.1.6	6.對海外分支機構資訊安全之督導管理： (1)總行管理單位是否督導海外分行訂定符合當地監管法令要求之資訊安全政策？ (2)是否建立符合國內外資安規定之安全管理制度？ (3)是否落實執行資訊安全控管措施？		28
1.2	(二)職能分工及自行查核情形		28

業務別項目編號	查核事項	法令規章	評核項目編號
1.2.1	1.各項工作是否依職責及牽制原則適當分工，並依業務需要配置適當人員及建立職務代理制度？		28
1.2.2	2.自行查核範圍是否完整？查核人員及查核頻率是否適當？執行情形是否確實？		28
1.2.2.1	(1)內部稽核作業規範是否包含資訊業務稽核規定？內容是否完備？		28
1.2.2.2	(2)辦理內部電腦稽核、自行查核，其稽核範圍是否完整？所訂查核項目是否完備？是否確實執行查核？		28
1.2.2.3	(3)稽核人員之指派是否妥適？是否符合分工牽制原則？		28
1.3	(三)人事管理與在職訓練		28
1.3.1	1.人事任免及適任性評估是否建立妥善管理制度，並落實執行？對資訊作業人員之進用，是否依規定填具保密切結書，並辦理人事查核，隨時督導考核？		28
1.3.2	2.是否建立資訊人員代理制度，並視實際需要建立輪調制度？		28
1.3.3	3.是否制定移交制度，對於調離職人員是否點收其保管之文物，取銷其使用者代號、密碼並收繳其通行證、卡及相關證件？		28
1.3.4	4.對預定解僱或已遞出辭呈之人員是否有控制其接近敏感之程式或檔案、並禁止在非正常上班時間使用電腦？		28
1.3.5	5.如有外雇人員，其管理是否有明確的規範，以確保重要資料無外洩之可能？		28
1.3.6	6.各級人員是否有充分的在職訓練及資安教育訓練？教育訓練計畫之擬定是否切合業務需要，年度教育訓練計畫執行情形是否落實？		28
2	二、網路及系統安全控管		28
2.1	(一)網路安全控管及防範措施		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.1.1	1.是否明訂網際網路作業相關管理辦法、作業規範及網路系統安全政策（如：防火牆原則、伺服器、網路資源存取控制、加密程序、使用者帳號維護、網路弱點掃描、漏洞修補、**電子郵件**及防毒軟體**之使用管理、網際網路存取之限制**）？俾作為網路維護作業之執行依據，並定期檢視修訂，以符合實際作業需求?		28
2.1.2	2.是否依據網路安全需求區分出獨立的網段(如Internet、DMZ、營運區、測試區、辦公區)？對聯外網站與內部網路或電腦系統間之路徑是否加以控管？		28
2.1.3	3.網路安全防禦系統(如防火牆、IDS、IPS、VPN、**電子郵件**閘道等)之設置情形？相關系統參數、規則設定維護**是否建立適當管制程序？**		28
2.1.3.1	(1)對未經防火牆之遠端存取是否予以過濾及管制？		28
2.1.3.2	(2)對網路各系統資源之存取權限是否依內部職務分工予以授權？**對敏感性資料檔案存取權限是否嚴加控管？**		28
2.1.3.3	(3)對網路系統使用者之建置管理是否嚴謹？對使用者帳號之密碼使用限制是否適當(如密碼有效期限、密碼長度、密碼輸入錯誤次數等)？		28
2.1.3.4	(4)對防火牆系統參數、規則設定是否建立適當程序以管制其設定值之異動？是否指定專人負責建置，並妥善保存設定相關文件及嚴格控管文件之使用？是否定期評估防火牆規則內容之妥適性並予適時調整？		28
2.1.3.5	(5)是否建立網路防禦措施有效性之評估機制及評估辦理滲透測試，並適時檢討改善以強化網路安全防禦機制？		28
2.1.3.5.1	A.使用整合多項功能模組之單一網路資安設備前，是否重新完整評估現有網路架構及資安防禦風險？		28
2.1.3.5.2	B.對嵌入式網路設備韌體所儲存之金鑰或憑證，是否建立相關運用管理機制(如：將更換金鑰訂為啟用網路設備之標準作業程序)？		28
2.1.3.6	(6)防火牆安全管理		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.1.3.6.1	A.對整體網路拓樸中，與外部連線之區域，以及內部的特定的安全區域，如：銀行核心業務，及網際網路等之網路連線是否架設防火牆予以區隔？		28
2.1.3.6.2	B.防火牆的實體存取是否置於機房以防止未經授權人員接近？防火牆管理系統之主控台是否使用鎖定保護程式？		28
2.1.3.6.3	C.防火牆之作業程序是否涵蓋防火牆之實體安全管理準則、防火牆過濾政策安全準則、防火牆設定之變更管理程序、工作站連線權限之申請與覆核程序、防火牆安控與稽核檢查程序等？		28
2.1.3.6.4	D.防火牆系統軟體是否定期配合版本更新進行新、舊版本差異及對現行作業影響等之評估分析，並辦理後續處理？		28
2.1.3.6.5	E.是否定期針對防火牆各項連線進行分析評估，包含異常的連線、遭拒絕之連線、潛在網路掃描活動的分析、連線來源位址？		28
2.1.3.6.6	F.防火牆政策所阻絕過濾之連線紀錄，是否已開啟稽核軌跡記錄之功能？		28
2.1.3.6.7	G.防火牆能否阻絕網路攻擊破壞，如：Node Spoofing、TCP SYN預測、Session Hijacking、Source Routing、DNS、ICMP等攻擊？		28
2.1.3.6.8	H.防火牆是否具備不同網路協定封包之過濾能力，以有效保護網路安全？		28
2.1.3.6.9	I.防火牆所設定封包過濾規則，如：來源位址/目的位址/協定別/服務埠/目標埠/封包長度/連線狀態等資訊是否妥當合適？		28
2.1.4	4.是否定期進行系統弱點及安全漏洞評估掃描作業？掃描範圍、項目及內容是否完整？頻率是否妥適？是否依風險等級進行評估影響性及採取適當修補措施並留存紀錄？		28
2.1.5	5.是否建立病毒偵測及預防程序，並定期辦理病毒碼更新？對重大電腦中毒事件是否確實釐清原因及研議防制對策？		28
2.1.6	6.網路活動日誌(Activity Logs)稽核軌跡(Audit Trail)及異常進出紀錄，是否完整留存，並建立警示機制與處理程序？是否建立機制定期檢討監控警示條件設定之妥適性？	「金融機構辦理電子銀行業務安全控管作業基準」	28

業務別項目編號	查核事項	法令規章	評核項目編號
2.1.6.1	(1)對於異常事件之監控及偵測條件是否明確定義，並定期檢討其妥適性？是否建立事件等級及通報處理程序，並據以辦理通報作業？		28
2.1.6.2	(2)對於網站資安事件之處理程序(包含事件發生後應採取之應變措施)是否妥適？		28
2.1.6.3	(3)對重要及關鍵作業或檔案之登入紀錄是否定期檢視，並就重要log進行備份？		28
2.1.7	7.是否訂定社交工程演練作業規範，明定辦理對象(含海外分行)、頻率、作業程序及教育訓練等項目，並定期(每年至少一次)辦理電子郵件社交工程演練？	**「金融機構辦理電腦系統資訊安全評估辦法」**	28
2.1.8	**8.對無線網路之使用，是否訂定相關管理措施，並對IEEE1394傳輸介面建立控管機制？**		28
2.1.9	9.對網路系統由IPV4轉換為IPV6，是否妥善規劃轉換程序及轉換期間各項風險因應措施？		28
2.1.10	**10.對全行員工(含海外分行)上網行為管理是否建立妥適之管控措施？**		28
2.1.11	11.是否依所訂評估計畫辦理電腦系統(含自建與委外維運)資訊安全評估作業(含海外分行)，並提交電腦系統資訊安全評估報告？缺失改善事項是否送稽核單位追蹤覆查？報告及相關文件是否至少保存5年？	「金融機構辦理電腦系統資訊安全評估辦法」	28
2.1.12	12.對交付給客戶之應用程式，有無辦理下列檢測： (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。	「金融機構辦理電腦系統資訊安全評估辦法」	28
2.1.13	13.對使用具網路連線功能之自動化辦公(OA) 設備(如：數位錄影機、電話交換機、錄音設備等)，是否建立安全性評估程序及安全控管機制？是否定期進行系統安全性更新或程式升級？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.1.14	14.對金融資安資訊分享與分析中心(F-ISAC)資安情資之接收與處理，是否建立妥善管理機制？		28
2.1.14.1	(1)是否依金融資安資訊分享與分析中心(F-ISAC)所訂「情資分享管理辦法」，建立資安情資內部作業處理流程與規範，並妥善處置所接收之資安情資？		28
2.1.14.2	(2)對所訂資安情資處理流程之相關控制措施，是否建立定期檢視機制，以確認其有效性？		28
2.1.14.3	(3)是否依內部控制三道防線機制，對資安警訊處理機制加強辦理自行查核及內部稽核？		28
2.2	(二)系統維護與管理		28
2.2.1	1.是否建立資訊資產管理系統，協助管理軟硬體設備之合法使用？是否限制個人電腦安裝VM系統？		28
2.2.2	2.是否建立作業系統安全參數檢核清單並定期檢視？安全參數設定(如使用者帳號之密碼有效期限、密碼長度、密碼輸入錯誤次數、啟動稽核事件紀錄等)是否符合資訊安全要求？		28
2.2.3	3.對各式主機系統之使用者帳號及其存取權限(含最高權限使用者帳號)之建置管理是否妥適？		28
2.2.4	4.是否對系統重要執行檔案，包含作業系統核心、應用程式執行檔、動態連結程式庫(DLL)、設定檔等進行例行性檢查，以確保未被竄改？		28
2.3	(三)應用系統開發維護管理		28
2.3.1	1.電子銀行業務系統維護與管理		28
2.3.1.1	(1)電子銀行應用系統架構是否妥適？交易安全設計(含客戶以網路方式開立數位存款帳戶)是否符合銀行公會訂定之「金融機構辦理電子銀行業務安全控管作業基準」？	「金融機構辦理電子銀行業務安全控管作業基準」	28
2.3.1.2	(2)辦理電子銀行系統應用程式及資料變更作業是否建立妥適之管制程序？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.1.2.1	A.是否訂有程式原始碼檢測作業程序，據以辦理檢測作業，並依檢測結果進行修補？		28
2.3.1.2.2	B.是否對應用程式建立嚴謹之版本控制程序，以有效管理應用程式變更作業？		28
2.3.1.3	(3)電子銀行交易資訊是否留存完整軌跡，電子銀行交易資訊是否備份至另一主機存放並建立每日檢視機制？		28
2.3.1.4	(4)對電子銀行系統異常事件是否訂有監測機制？		28
2.3.1.4.1	A.是否對觸發監測事件之基準或條件有明確合理之定義，並據以建立檢核及分析機制？		28
2.3.4.1.2	B.是否定期檢討監測機制之有效性？或依國內外案例適時修正監測條件，俾能及早警示特殊或異常事件？		28
2.3.1.4.3	C.對不同型態之電子銀行系統異常事件是否分別擬有因應對策及作業標準程序，並適時辦理演練？		28
2.3.1.5	(5)對自動櫃員機系統(含ATM之相關伺服器)安全維護作業，是否符合銀行公會訂定之「金融機構提供自動櫃員機系統安全作業規範」之要求？	「金融機構提供自動櫃員機系統安全作業規範」	28
2.3.2	2.系統開發管理	「金融機構資訊系統安全基準」	28
2.3.2.1	(1)有關系統之建置、變更、測試、轉換、上線等作業，是否有訂定規範或辦法？		28
2.3.2.2	(2)系統開發程序是否包括系統可行性研究、系統分析、設計、程式設計、測試、文件撰寫及系統評估等步驟，各階段工作所產生之文件是否均經主管審核控管以確保系統開發安全？		28
2.3.2.3	(3)系統開發階段是否訂有明確的作業進度計畫表，並妥善控制之？程式撰寫階段，是否將OWASP 等常見的網站應用程式弱點納入軟體開發安全參考，以避免產生類似弱點？	「金融機構資訊系統安全基準」	28
2.3.2.4	(4)系統開發、設計是否有由業務、稽核、會計、企劃等有關單位參與，以求操作、管理、查核各方面之考慮周全？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.2.5	(5)對於系統之可稽核性(auditability)，是否有徵求電腦稽核人員意見，並於開發過程中考量？		28
2.3.2.6	(6)系統實施前是否訂有測試計畫？所有程式、相關子系統及整體系統是否均經完全的測試？其測試結果是否均經系統分析師的覆核及有關主管核示？是否由使用單位作系統接受性測試?		28
2.3.2.7	(7)系統正式作業實施前，是否經業務、稽核、會計等單位參與驗收？對系統及說明文件、作業（操作）手冊、測試紀錄、轉換（實施）計畫之完整性以及是否符合原訂有關操作、管理、查核需求等，皆加以確實驗收？		28
2.3.2.8 2.3.2.8.1 2.3.2.8.2 2.3.2.8.3 2.3.2.8.4 2.3.2.8.5	(8)作業實施前是否訂有具體妥善轉換計畫？並經使用部門及有關主管核可後確實執行？轉換計畫是否視需要包含相關工作及其負責人與預定進度等？ a.有關新系統操作、資料管制、作業管制等之講習訓練？ b.軟、硬體設備之裝置，調整（如實務必要時）？ c.關聯作業之調整？ d.說明文件、紀錄文件之整理？ e.資料檔（轉換）程序及其核對與錯誤資料之更正、追蹤？		28
2.3.2.9	(9)實施系統轉換時，是否訂定妥適的雙軌作業期間及經確認新系統可靠後才正式啟用？		28
2.3.2.10 2.3.2.10.1 2.3.2.10.2 2.3.2.10.3 2.3.2.10.4 2.3.2.10.5	(10)已正式實施之作業，是否由有關單位人員對下列事項適時予以檢討、評估，以求改進，並作為今後開發其他電腦作業系統之參考？ a.業務電腦化後，操作、管理與查核上尚待加強、改進者？ b.系統內部控制功能之完整性？ c.程式、檔案設計修改頻率與主要修改原因之分析？ d.輸出資料、報表之實用性、完整性？ e.實際開發時間、人力、成本與原計畫之比較分析？		28
2.3.2.11	(11)委外開發之應用系統是否取得程式原始碼及程式修改授權或保固、維護期滿後一定期間之程式使用權？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.2.12	(12)系統或新功能首次上線前及至少每半年是否針對異動程式辦理程式碼掃描或黑箱測試作業，並針對掃描或測試結果執行風險評估及漏洞(或弱點)修補？	「金融機構辦理電子銀行業務安全控管作業基準」	28
2.3.3	3.系統維護管理		28
2.3.3.1	(1)對每一應用系統，是否均派專人負責維護的工作？系統運轉後，對於使用單位的滿意程度是否辦理調查分析，又對於運轉中常發生之操作員干預或程式設計師修改的現象是否定期檢討，以進行系統維護工作？是否確保關鍵性銀行業務資訊之隱密性？		28
2.3.3.2	(2)修改系統時，是否採取足夠的系統變更控制，以免其接觸未經許可修改的部份或正式作業系統？		28
2.3.3.3	(3)系統之重大變更是否比照開發新系統之程序，並由有關單位參與研討變更內容、範圍，並參與驗收？		28
2.3.3.4 2.3.3.4.1 2.3.3.4.2 2.3.3.4.3 2.3.3.4.4 2.3.3.4.5 2.3.3.4.6	(4)已正式實施之作業，其程式變更： a.是否均有提出書面申請，並經有關主管核准後方才修正? b.書面申請是否敘明變更內容及原因? c.修改後是否加以測試，主管審核其測試結果並確認該項變更不致影響或破壞系統原有的安全控制措施？ d.對修改前後程式是否利用公用程式作比對，並列印報表由主管審核? e.系統相關文件是否配合修正？ f.操作程序上如有變更是否通報有關單位？		28
2.3.4	4.文件資料管理		28
2.3.4.1	(1)各項文件資料是否依機密性分類？文件之存放取用是否有指定專人負責管理及妥善儲存保管？，對於文件資料之存取權利是否有適當之管制，其存取是否均留下紀錄？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.4.2 2.3.4.2.1 2.3.4.2.2 2.3.4.2.3 2.3.4.2.4 2.3.4.2.5 2.3.4.2.6 2.3.4.2.7	(2)已實施之系統是否有下列文件： a.系統說明書？ b.程式說明書？ c.操作說明書（含中心及端末）？ d.測試計畫書（含測試報告）？ e.系統轉換計畫書？ f.系統驗收紀錄？ g.與有關單位研討之會議紀錄？		28
2.3.4.3	(3)系統說明文件之撰寫及程式、檔案名稱之命名是否標準化？		28
2.3.4.4	(4)前述文件以電腦媒體形態保存時，對其建檔、變更、調閱，是否被授權人員始得為之，並留存紀錄？		28
2.3.4.5	(5)重要程式文件、清冊及防災應變故障復原計畫是否備份，異地保存？		28
2.3.5	5.程式、資料檔案管理		28
2.3.5.1	(1)系統程式及應用程式之登錄與維護是否由系統程式人員或指定專人負責？其登錄與維護是否均經申請、核可及覆核程序，並留存紀錄？		28
2.3.5.2	(2)正式作業程式館內程式之新增、刪除、修改，電腦系統是否留有紀錄，並定期列印查核？是否有防備未經授權者使用程式館措施？		28
2.3.5.3	(3)程式之登錄、變更過程中是否能控制同一程式在程式館內之原始碼(source code)及目的碼(object code)為同一版本？		28
2.3.5.4	(4)若於正常上班時間外緊急修改（增加）程式，是否訂有符合牽制原則之緊急進館程序？並是否有照規定程序執行？		28
2.3.5.5	(5)在特殊情況下，對正式作業檔案資料之更正是否要求以書面申請，並經核准？電腦是否留存完整之更正紀錄，如更正前、後比較表以憑查核所有更正皆經申請、核可程序？		28
2.3.5.6	(6)具有修改檔案資料或目的程式功能之公用程式(utility programs)是否嚴密管制其使用？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.5.7	(7)是否使用安全軟體(security software)對程式及資料檔案之存取加以控管？若有，評估其使用管理情形是否良好？		28
2.3.5.8	(8)對重要或機密性資料檔案是否採亂碼化措施加以保護，以防止不法之使用？其使用情形（含使用被拒絕）是否有紀錄，並憑以查核？		28
2.3.5.9	(9)正式作業與測試作業之程式、資料、工作控制指令等檔案是否分開存放？		28
2.3.5.10	(10)正式作業後所產生之主檔或其他重要資料檔案，是否作成備份檔，異地存放，以符安全？		28
2.3.5.11	(11)對資料庫存放於國外之金融機構(如:部分外商銀行)，是否訂有妥善管制措施，以確保資料之獨立性、完整性及穩定性，並能確保客戶權益？		28
2.3.6	6.行動支付業務系統維護與管理		28
2.3.6.1	(1)辦理行動信用卡業務，相關安全控管是否符合銀行公會訂定之「信用卡業務機構辦理行動信用卡業務安全控管作業基準」？	「信用卡業務機構辦理行動信用卡業務安全控管作業基準」	28
2.3.6.2	(2)行動支付應用APP之安全管理		28
2.3.6.2.1	A.辦理行動支付應用APP，相關安全控管是否符合銀行公會所訂之「金融機構提供行動裝置應用程式作業規範」之規定？	「金融機構提供行動裝置應用程式作業規範」	28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.6.2.1.1	a.是否每年辦理下列檢測：	「金融機構提供行動裝置應用程式作業規範」	28
2.3.6.2.1.1.1	(a)是否由合格實驗室依據經濟部工業局「行動應用APP基本資安檢測基準」辦理並通過檢測，且由資安專責單位確認完成改善?		
2.3.6.2.1.1.2	(b)是否針對應用程式及其應用伺服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?如因使用工具檢測可能導致之誤判或有解讀差異，經自行評估相關漏洞為可承擔之風險者，是否留存評估紀錄?		
2.3.6.2.1.1.3	(c)辦理資訊安全評估之評估單位是否針對應用程式及其應用伺服器依據「金融機構提供行動裝置應用程式作業規範」及OWASP公布之Mobile APP Security Checklist L2項目辦理並通過檢測，且由資安專責單位確認完成改善?		
2.3.6.2.1.1.4	(d)是否對合格實驗室及評估單位所提交之報告建立檢視機制，並送資訊安全專責單位監控及執行資訊安全管理作業?		
2.3.6.2.1.2	b.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是否辦理下列檢測：	「金融機構提供行動裝置應用程式作業規範」	28
2.3.6.2.1.2.1	(a)是否辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞?		
2.3.6.2.1.2.2	(b)如與資金轉移相關或對客戶權益有重大影響之各類電子轉帳及交易指示者，是否依據OWASP公布之Mobile Top 10項目辦理並通過檢測，且由資安專責單位確認完成改善?如因故需緊急上線者是否於1個月內完成?		
2.3.6.2.1.3	c.採用行動裝置應用程式作為交易再確認機制者，是否符合應用程式安全防護措施，包括：防入侵機制(如檢查App完整性、檢查函式庫完整性、防止螢幕遭覆蓋、防止逆向工程等)、執行期間保護機制(如防止打包或監聽、防止執行未授權程式碼、防止使用模擬器、防止在偵錯模式執行等)及機敏資料保護機制(如記憶體參數保護、儲存檔案保護、防止設備複製等)。	「金融機構提供行動裝置應用程式作業規範」	28
2.3.6.2.2	B.行動支付應用APP上架及變更之檢核程序		28
2.3.6.2.2.1	a.辦理行動支付應用APP開發及上架作業，是否建立相關控管程序？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.6.2.2.2	b.對行動支付應用App之存取權限，是否建立審核作業機制並留存書面紀綠及佐證資料？是否於上架前洽會相關部門，以評估其存取權限之適法性及安全性？		28
2.3.6.2.2.3	c.辦理行動支付應用APP程式變更作業，是否建立妥適之控管程序？(包含版本控管、原始碼檢測及引用第三方函式庫(API)等)		28
2.3.6.2.2.4	d.行動支付應用APP委外開發時，是否自廠商處取得程式原始碼？如未取得原始碼，是否評估可能面臨風險及未來對業務之影響，預先擬定因應措施？		28
2.3.6.2.3	C.信用卡收單機構簽訂「代收代付平台業者」為特約商店，由平台業者提供行動裝置應用程式（APP）供消費者信用卡交易下載使用，收單機構是否要求其APP須經由第三方機構參酌經濟部工業局「行動應用APP基本資安檢測規範」或國際組織支付應用軟體資料安全標準(PADSS)規範確認其安全防護？並提供證明文件供收單機構查驗？	信用卡收單機構簽訂「提供代收代付服務平台業者」為特約商店自律規範	28
2.3.6.3	(3)辦理行動金融卡業務，相關安全控管是否符合銀行公會訂定之「金融機構辦理行動金融卡安全控管作業規範」？	「金融機構辦理行動金融卡安全控管作業規範」	28
2.3.7	7.雲端服務、社群媒體或自攜裝置等新興科技之安全防護		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.7.1	(1)雲端服務安全控管	「金融機構運用新興科技作業規範」	28
2.3.7.1.1	A.是否制定雲端服務管理政策，並定期檢視？		
2.3.7.1.2	B.導入IaaS或PaaS雲端服務模式前，是否評估下列事項：		
2.3.7.1.2.1	a.雲端服務業者之合格條件、服務水準、復原時間、備援機制、供應鏈關係、權責歸屬及資訊安全防護等項目。		
2.3.7.1.2.2	b.雲端服務業者所提供之平台、協定、介面、檔案格式等，以確保互通性與可移植性。		
2.3.7.1.2.3	c.雲端服務業者所建置安全控管措施(如防火牆區隔)之妥適性，以確保其提供之資源與其他承租人所使用之資源各自獨立。		
2.3.7.1.3	C.是否建置妥適之資料存取管控機制(包含使用者帳號權限管理、身分驗證機制等)，以確保雲端服務業者未有存取客戶資料之權限，且不得為指定範圍以外之利用?		
2.3.7.1.4	D.對員工使用手機等行動裝置登入雲端運算服務系統存取客戶資料檔案，是否限制客戶資料被下載或儲存至行動裝置？		
2.3.7.1.5	E.銀行本身、主管機關及中央銀行，或其指定之人是否取得雲端服務業者執行作業之相關資訊及實地查核權力?經委託第三人之查核範圍是否涵蓋雲端服務業者處理作業相關之重要系統及控制環節?是否評估前述第三人之適格性及所出具查核報告之妥適性?		
2.3.7.1.6	F.若委託雲端服務業者處理之客戶資料及其儲存地位於境外，是否保有指定資料處理及儲存地之權利?除經主管機關核准外，客戶重要資料是否在我國留存備份?		
2.3.7.1.7	G.是否訂定妥適之緊急應變計畫?包括終止或結束作業委託時，能順利移轉至另一雲端服務業者或移回自行處理，及全數刪除或銷毀原雲端服務業者留存資料，且留存相關紀錄?		
2.3.7.2	(2)社群媒體控管程序：	「金融機構運用新興科技作業規範」	28
2.3.7.2.1	A.是否制定社群媒體管理政策，並定期檢視？		
2.3.7.2.2	B.有無制定社群媒體使用守則(包含可接受使用之社群媒體、功能等)？是否制定銀行發言規範，明定發言角色與權責？		
2.3.7.2.3	C.是否建立內容過濾與監視機制？		

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.7.3 2.3.7.3.1 2.3.7.3.2 2.3.7.3.3 2.3.7.3.4	(3)**自攜裝置安全控管：** A.是否制定自攜裝置管理政策，並定期檢視？ B.是否建置使用者身分與裝置識別之機制(如帳號密碼識別、裝置識別碼)？ C.**使用人員與裝置是否列冊管理，且至少每年審閱一次？**對自攜裝置採取之資安管控措施，是否包括制定自攜裝置連網環境標準?如未符合標準(如作業系統疑似遭破解或提權、未安裝病毒防護、重大漏洞未修復)，是否限制其連網功能? D.員工透過自攜裝置提供金融服務，對資料存取權限控管及資料保護措施(如資料加密或遮罩)是否妥適？	「金融機構運用新興科技作業規範」	28
2.3.8	8.辦理QR Code掃描支付業務，對QR Code掃描支付之交易安全，包含QR Code訊息傳輸安全需求及應用程式安全設計要求等，是否依銀行公會所訂「金融機構提供QR Code掃描支付應用安全控管規範」之規定辦理？	金融機構提供QR Code掃描支付應用安全控管規範	28
2.3.9	9.SWIFT系統資訊安全控管		28
2.3.9.1	(1)與SWIFT系統相關之網路安全防禦措施之建置是否妥適？(如：網路安全防禦系統之建置、防火牆安全管理、病毒偵測(含與資安公司之委外合約內容及執行情形)、網路異常進出紀錄等)		28
2.3.9.2	(2)本會銀行局105.9.5銀局(國)字第10500202300號函請各銀行對SWIFT系統加強管理之7項重點是否落實執行？(如：對SWIFT工作站或伺服器進行實體隔離、對SWIFT修補派送更新程式與作業進行控管等)	本會銀行局105.9.5銀局(國)字第10500202300號函	28
2.3.9.3	(3)SWIFT組織轉知SWIFT協會成員配合辦理之「客戶安全計畫」(CSP)強制控制措施及自我評估是否落實執行？(如：重要帳號使用雙因子認證密碼、確認SWIFT伺服器及工作站為獨立專用機器、定期檢視防火牆規則並監控異常事件及應變措施等)		28
2.3.9.4	(4)對SWIFT組織公告資安警訊及網路連線安全標準等事項，是否建立妥適之通報流程與因應處理機制?		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.3.9.5	(5)對主管機關或銀行公會公布SWIFT系統加強管理及資安管理措施等相關法令，是否建立外部法令有效傳達之管道，並落實發揮內部控制三道防線之功能?		28
2.3.10	是否建立物聯網設備管理清冊？物聯網設備相關安全控管是否符合銀行公會訂定之「金融機構使用物聯網設備安全控管規範」？辦理物聯網設備採購案，是否優先考量採購具有安全標章之物聯網設備，以降低相關作業風險？	1.「金融機構使用物聯網設備安全控管規範」 2.本會109.6.4金管銀國字第1090213176號函	28
2.3.11	與第三方服務提供者(TSP)透過開放應用程式介面(API)提供銀行非交易面之金融產品資訊，是否符合「中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範」？	「中華民國銀行公會會員銀行與第三方服務提供者合作之自律規範」	28
2.4	(四)主機操作管理	「金融機構資訊系統安全基準」	28
2.4.1	1.操作人員操作管理		28
2.4.1.1	(1)控制台及週邊設備（磁碟機、磁帶機、列表機等）是否僅限輪值操作員操作？		28
2.4.1.2	(2)是否備有作業手冊供操作員使用?操作員是否依作業說明（作業手冊、工作申請單）執行作業？		28
2.4.1.3	(3)是否有明訂操作人員可使用之指令清單？		28
2.4.1.4	(4)操作人員所輸入指令，是否都留下系統紀錄(Log)？並由其他人員負責核驗？		28
2.4.1.5	(5)對各項工作之執行情形，操作人員是否逐項確認簽註執行結果？並呈主管核閱？		28
2.4.1.6	(6)除例行作業外，假日及夜間等非營業時間使用正式電腦作業系統是否先經核准？		28
2.4.2	2.批次作業管理		28
2.4.2.1	(1)資訊中心是否訂定電腦批次作業程序規範臨時、緊急更改之准許及審核程序？		28
2.4.2.2	(2)例行性作業是否按預定的排程來處理，非例行性作業是否經申請核准？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.4.2.3	(3)批次作業若非自動排程是否有書面之排程表？工作執行之情形有否留存紀錄？對執行異常情形有否查核追蹤？		28
2.4.2.4	(4)對例行性作業發生異常狀況，有無訂定處理程序？並作紀錄？		28
2.4.2.5	(5)操作時發生異常狀況是否皆予記錄，並依操作手冊等文件之說明處理？發生嚴重問題時，是否依規定之報告程序，緊急通知主管等有關人員？		28
2.4.3	3.作業及系統日誌功能管理		28
2.4.3.1	(1)機房內是否設置工作日誌，記載電腦開關機紀錄、故障維護情形，及操作人員、時間等，並定期陳報？對異常情況有否查核追蹤？		28
2.4.3.2	(2)電腦系統運作紀錄或控制台操作紀錄是否逐日由系統管理人員查核？並保留適當之期間？對異常情形有否追蹤查核？		28
2.4.3.3	(3)電腦作業是否經常發生重覆處理(rerun)情形？其原因為何？有否採取適當措施以減少發生？		28
2.4.3.4	(4)對儲存體或記憶體之傾印(storage or memory dump)是否控管？對其作業情形是否確實記錄並註明作業之原因？		28
2.4.3.5	(5)上開日誌、紀錄及異常情形是否皆有呈閱主管？並依核示意見辦理或列入問題管理？		28
2.4.4	4.對於電腦軟硬體系統運作狀況及各項電腦資源之使用情形，是否定期予以統計分析與檢討改進？		28
2.4.5	5.中心端末機使用管理		28
2.4.5.1	(1)對經授權使用端末機人員之姓名、使用者代號或使用之作業卡卡號、起訖時間是否設簿登記，並經使用人簽章以明責任？登記簿是否與電腦使用人員資料檔內容相符？		28
2.4.5.2	(2)端末機使用人員資料之建檔、變更、註銷是否經申請、核准程序並留存紀錄？		28
2.4.5.3	(3)使用者密碼是否可由使用人視情況需要定期或不定期變更？		28
2.4.5.4	(4)端末機操作人員是否憑被授予之使用者代號或作業卡操作？有無共用同一使用者代號或作業卡之情形？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.4.5.5	(5)對於調離職人員，是否取消其使用者代號、密碼並收繳其作業卡？是否定期檢視系統上已建立之帳號，並移除無需使用或不屬於任何人員之帳號？		28
2.4.5.6	(6)由端末設備存取中心或端末設備系統之正式作業程式、檔案或工作執行指令，是否依使用人員職務工作範圍等予以限制？存取時是否先經核准或授權，並留存紀錄？對違規使用有否查核追究？		28
2.4.6	6.輸入、輸出資料管制		28
2.4.6.1	(1)由使用單位送交處理之輸入資料（原始憑證、媒體或透過網路傳送之資料）是否訂有檢核程序及控管措施？以確保輸入資料之正確性及合法性。		28
2.4.6.2	(2)經電腦檢核為異常或錯誤之輸入資料，是否由資料管制人員負責查明處理？		28
2.4.6.3	(3)報表或媒體等輸出資料送出前，對電腦處理情形是否正常，輸出資料內容是否完整、合理，有否經指定人員檢核後，始依限送出、或保存？留存之輸出資料是否妥為使用、保管或銷毀？重要資料分送程序是否妥善，俾期輸出資料適時送達使用單位？		28
2.4.6.4	(4)輸出報表之內容如以媒體保存時，有否訂定保存期限並妥善保存？		28
2.4.7	7.亂碼化作業安全管理		28
2.4.7.1	(1)為維護電腦作業亂碼系統正常運作，及確保亂碼化設備及作業之安全性，是否訂定跨行亂碼系統安全控管辦法？		28
2.4.7.2	(2)亂碼化作業安全控管人員，是否至少由二人以上人員擔任？且不得由亂碼化介面程式設計人員兼任？		28
2.4.7.3	(3)對於亂碼化介面程式之維護是否經由安全控管人員授權後，再進行修改程式？		28
2.4.7.4	(4)對於亂碼化設備系統之程式、資料執行備援及回復措施時，是否在兩位安全控管人員監督下進行？		28

業務別項目編號	查核事項	法令規章	評核項目編號
2.4.7.5	(5)有關亂碼化設備使用之備援磁帶、磁片等儲存媒體之保管是否隱密安全符合牽制原則（如由兩位安全控管人員會同封簽後密存）？取用是否經核可並留存紀錄？		28
2.4.7.6	(6)各種基碼之建立或變更是否經申請、核可，並留存紀錄？是否由兩位安全控管人員分別拆封，並在嚴密控管環境下分別輸入基碼資料？		28
2.4.7.7	(7)各種基碼建立或變更時是否由安全控管人員依一定程序核准後共同將其建立基碼之程式載入系統執行，執行後即將程式自系統中清除？		28
2.4.7.8	(8)為提昇安全層次，其亂碼化作業是否使用硬體執行？		28
2.4.8	8.是否建立關鍵業務主機作業系統版本提升更新及弱點修補機制(含未更新修補之風險評估)？對原廠已停止提供更新服務(EOS)者，是否評估對業務影響性及研擬妥適因應措施？		28
3	三、個人資料安全維護		22
3.1	(一)對涉及個資之應用系統功能、報表文件或電子檔之管理機制及資安教育宣導情形		22
3.1.1	1.對涉及個資之系統功能、報表、文件或電子檔，是否建立個資檔案清冊，並定期執行清查及留存相關作業紀錄？		22
3.1.2	2.是否定期對個資檔案安全防護，實施資料安全防護教育訓練及相關宣導措施？		22
3.2	(二)對個資之儲存、傳遞及使用之控管機制		22
3.2.1	1.存放於資料庫、檔案內之個資，是否建立妥適之去識別化或加密處理機制，相關存取是否建立控管機制，並留存完整稽核軌跡？(如:將正式營運資料複製到測試環境且未去識別化時，是否訂定控管機制？)		22
3.2.2	2.儲存客戶資料之重要資料庫主機是否置於內部網路，是否經由防火牆適當設定這些資料庫主機與對外主機之連線？		28
3.2.3	**3.對傳遞個資，是否建立妥適之加密及監控機制，並留存完整稽核軌跡？**		28

業務別項目編號	查核事項	法令規章	評核項目編號
3.2.4	4.對FTP、檔案分享(如網路芳鄰、SAMBA)、**檔案下載、電子郵件等傳檔功能之應用程式，是否訂定控管機制、留存完整稽核軌跡，並落實執行**？對不同網區間之**檔案傳輸系統，是否訂有管控機制，以避免不當夾帶或外洩個資檔。**		28
3.2.5	5.對行動碟、光碟、磁帶等**移動式儲存媒體及筆記型電腦、平板電腦等可攜式設備，是否建立使用管理機制、留存完整稽核軌跡**，並落實執行？		22
3.2.6	6.非公務機關提供電子商務服務系統，是否採取下列資訊安全措施？ (1)使用者身分確認及保護機制。 (2)個人資料顯示之隱碼機制。 (3)網際網路傳輸之安全加密機制。 (4)應用系統於開發、上線、維護等各階段軟體驗證與確認程序。 (5)個人資料檔案及資料庫之存取控制與保護監控措施。 (6)防止外部網路入侵對策。 (7)非法或異常使用行為之監控與因應機制。	「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第10條	28
3.2.7	7.執行個人資料保護機制、程序及措施，應記錄其個人資料使用、刪除、停止處理或利用等情況，留存軌跡資料或相關證據至少五年。	「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第14條	28

業務別項目編號	查核事項	法令規章	評核項目編號
3.2.8	8.將客戶生物特徵相關之辨識技術導入客戶服務，是否訂定相關管理措施？	「金融機構運用新興科技作業規範」、「金融機構辦理電子銀行業務安全控管作業基準」	22
3.2.8.1	(1)運用客戶生物識別資料(如聲紋、指紋等)，是否建立內部作業及資料保存之控管程序？		
3.2.8.2	(2)取得及利用客戶生物特徵資料前，是否先取得客戶同意並留存客戶同意之紀錄？		
3.2.8.3	(3)首次使用生物辨識技術、每年定期或技術有重大變更時，是否由資訊單位檢視該技術足以有效識別客戶身分？是否彙整相關資料交由資安、法遵及風控等單位進行確認，並留存驗證軌跡及各部門建議事項追蹤控管機制?		
3.2.8.4	(4)對生物特徵資料於傳輸過程中之相關控管措施，是否確認符合「金融機構辦理電子銀行業務安全控管作業基準」之規定？		
3.2.8.5	(5)採用間接驗證生物特徵技術者，是否善盡告知客戶使用上之風險，並提供間接驗證機制關閉管道？是否每年定期檢視並蒐集資安威脅情資，建立補償措施?		
3.2.8.6	(6)是否針對直接驗證生物特徵技術，建立其錯誤接受率及錯誤拒絕率之標準，並於上線前與每年定期檢視?若不符合銀行要求時，是否建立補償措施?		
3.2.8.7	(7)生物特徵資料儲存於銀行內部系統時，是否進行加密儲存、並分別儲存於不同之儲存媒體?加密金鑰是否儲存於符合FIPS 140-2 Level 3以上或其他相同安全強度認證之設備？		
3.2.9	9.保有個人資料之特定目的消失或期限屆滿者，是否依規定刪除、停止處理或利用?	「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第8條	22
3.2.10	10.設備或儲存媒體報廢或轉作他用時，是否採取防範資料洩漏之適當措施?	「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第9條	22
3.3	(三)對提供客戶資訊予委外機構、合作推廣、共同行銷或集團關係企業之管理機制		22

業務別項目編號	查核事項	法令規章	評核項目編號
3.3.1	1.將客戶資訊提供委外機構、合作推廣、共同行銷或集團關係企業，是否控管資料檔案傳遞過程之安全存取設定，且資料檔案經加密保護之隱密處理？		22
3.3.2	2.金融控股公司資訊中心中，各金融子公司對跨業之資料存取是否訂有規範，並符合相關法令規定（如個人資料保護法等），不得影響客戶權益？	「金融控股公司及其子公司自律規範」	22
3.3.3	3.金融控股公司因依法令規定彙整報送集團營運資料予主管機關及管理被投資事業之需要，要求子公司將其業務資料及客戶資料等提供金融控股公司建置資料庫時，是否與子公司簽訂保密協定？	「金融控股公司建置資料庫有關保密規範」	22
3.3.4	4.傳輸及儲存客戶資料至雲端業者，是否採行客戶資料加密或代碼化等有效保護措施?是否訂定妥適之加密金鑰管理機制?	「金融機構作業委託他人處理內部作業制度及程序辦法」第19-1條	22
4	四、災害應變		28
4.1	(一)營運中斷衝擊分析及備援措施		28
4.1.1	1.就各資訊系統中斷對銀行營運之衝擊是否辦理評估分析，並據以建構備援措施？	「金融機構資訊系統安全基準」	28
4.1.2	2.備援措施(含同地及異地備援)是否可於事故發生時支援重要業務？		28
4.1.2.1	(1)備援設備若非自行所有，是否有契約明定其支援方式，時間？是否能確保使用權利？		28
4.1.2.2	(2)重要程式或檔案之維護工作是否皆有備援人員？		28
4.1.2.3	(3)網路系統中各主要主機伺服器(包括防火牆主機)是否設有備援主機，以備主要作業主機無法正常運作時之用？		28
4.1.2.4	(4)網路系統中之防火牆與各主機是否定期做系統備份？包括完整系統備份，系統架構設定備份以及稽核資料備份?		28
4.1.3	3.機房及備援設備場所之安全管制措施是否適當(含網路伺服器、防火牆及其他連線設備硬體處所之安全管控情形)？		28
4.1.3.1	(1)環境安全防護-電腦設備及相關設施之安全防護是否完善？	「金融機構資訊系統安全基準」	28

業務別項目編號	查核事項	法令規章	評核項目編號
4.1.3.1.1	A.是否有完善的防火、防水、防震、防入侵、門禁（如機房自動門禁控制系統）及不斷電設備、穩壓、空調、停電照明設備等安全防護措施？相關機電、消防等設備之配置及管理是否妥適？		28
4.1.3.1.2	B.除不斷電設備外有無裝置自動發電機，以供長時間停電使用？		28
4.1.3.1.3	C.電腦設備是否使用獨立的電源系統？是否有專用之空調設備？		28
4.1.3.1.4	D.有無裝置火災自動警報系統？或自動滅火設備？		28
4.1.3.1.5	E.電腦及相關設備是否訂有維護契約，定期或不定期實施維護，並留存紀錄備查？		28
4.1.3.1.6	F.保險及維護契約涵蓋範圍是否完全？並在有效期間內？		28
4.1.3.1.7	G.對處理個人資料檔案之主機（含測試或發展用之主機）、週邊備及相關設施等電腦設備，有無設置特殊安全機制及對天然災害及其他意外災害之防護措施？		28
4.1.3.1.8	H.對於儲藏個人資料檔案之磁碟、磁帶等媒體，有無指定專人管理，並建立備援制度？		28
4.1.3.1.9	I.對重大資訊及網路硬體設備之擴充或更新作業，是否訂有嚴謹之作業程序並落實執行？		28
4.1.3.1.10	J.是否熟悉與財金公司間路由機制，並能妥善運用以降低營運中斷風險？		28
4.1.3.2	(2)人員進出管理 對進出資訊單位、辦公場所、機房、媒體室及文件保管室之人員與攜帶（搬運）之物品是否加以嚴格管制？		28
4.1.3.2.1	A.進出資訊單位建物、辦公場所、機房、媒體室及文件保管室之人員是否加以辨識並登記？		28
4.1.3.2.2	B.電腦機房、媒體室、文件保管室之門禁管制是否妥善？		28
4.1.3.2.2.1	a.電腦機房及媒體室（庫）及文件保管室（庫）有無指定專人負責管		28
4.1.3.2.2.2	b.機房進出人員除輪班操作員等機房工作人員外是否皆經核准及登記？媒體室（庫）進出人員除媒體管理員外是否皆經核准或授權，並保存進出紀錄？		28
4.1.3.2.2.3	c.機房及其他重要區域是否有門禁管制設備以控制人員進出？		28

業務別項目編號	查核事項	法令規章	評核項目編號
4.1.3.2.3	C.異地存放之備份程式及檔案，移送程序是否有控管？存放地點之安全措施是否嚴密？		28
4.2	(二)重要檔案回復能力		28
4.2.1	1.對重要或需要長期保留檔案(含應用、系統程式及資料檔等)是否有備援措施，其回復能力是否完整？	「金融機構資訊系統安全基準」	28
4.2.1.1	(1)系統程式，原始程式及目的程式是否抄錄備份，並異地存放安全場所？		28
4.2.2	2.對長期保留之重要檔案，是否明訂備份儲存媒體使用年限，並依規定期進行對錄測試或轉錄作業？		28
4.2.2.1	(1)媒體管理		28
4.2.2.1.1	A.媒體之採購、作廢是否經主管核准並留存申請單或紀錄簿備查？		28
4.2.2.1.2	B.對於儲存資料或程式之媒體是否闢成專室責成專人負責管理？		28
4.2.2.1.3	C.對於保管中、使用中之媒體是否皆予設簿登記控管，並定期派員盤點？因作業需要外借媒體，是否有經主管核准之申請單或紀錄單備查？		28
4.2.2.1.4	D.媒體新增、作廢是否經核准？媒體廢棄前或轉作他用時，是否先經銷磁或採取防範資料外洩之適當措施，以防儲存於媒體內之資料外		28
4.3	(三)緊急應變計畫及演練		28
4.3.1	1.是否訂有災害應變計畫以處理各種可能之意外（狀況），俾能在最短時間內，恢復電腦作業功能？應變計畫應是否包括電腦軟硬體系統故障時之復原程序、資料檔案遭毀損或入侵破壞之復原程序、使用備援系統之轉換程序或故障期間之權宜作業方式？		28
4.3.1.1	(1)是否訂定程式及檔案毀損時之重建程序？		28
4.3.1.2	(2)銀行及委外服務廠商是否訂定緊急應變及復原計畫，計畫內容之妥適性（考量面臨各類災難、重大疫情、人員罷工、資訊服務中斷等嚴重事故衝擊時，關鍵或高風險之組織、系統及營運流程等是否能持續運作），是否定期檢核緊急應變及復原計畫，以符合現行作業及經營策略，且於計畫中說明檢核的方法及頻率？		28

業務別項目編號	查核事項	法令規章	評核項目編號
4.3.1.3	(3)是否確保委外服務廠商得充分瞭解其應變計畫，在緊急狀況下是否有其他委外服務廠商可供替換？		28
4.3.1.4	(4)是否建立病毒及惡意程式等重大資安事件之復原因應對策並定期演練及檢討改善？		28
4.3.1.5	(5)是否訂定個人資料安全事故應變、通報及預防機制，定期辦理演練並留存紀錄？	「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」第6條	22
4.3.2	2.故障復原及災害應變計畫之演練週期、範圍及項目是否妥適？演練紀錄及檢討報告是否依分層負責呈報高階主管？		28
5	五、資訊作業委外管理		28
5.1	(一)委外作業風險評估、受託機構遴選作業及契約內容之管理		22
5.1.1	1.對主要核心業務是否於委外前辦理評估分析，並將法規遵循、營運風險、法律風險及維持業務營運不中斷的應變能力等項目納入評估？		22
5.1.2	2辦理受託機構遴選作業，是否建立妥適之遴選程序(包括設置評選小組、研訂評選標準、評選作業、議價程序及呈報遴選結果等)，並落實執行？		28
5.1.3	3法規規定之應記載事項是否均已納入合約載明？其他重要應注意事項，如委外服務品質保證、終止委託之通知時程及配合移轉程序等事項，是否明訂，相關條款是否妥適明確？	「金融機構作業委託他人處理內部作業制度及程序辦法」	22
5.2	(二)對受託機構之日常監督管理及查核機制		28
5.2.1	1.對受託機構是否建立妥適之監督管理程序：	「金融機構作業委託他人處理內部作業制度及程序辦法」	28
5.2.1.1	(1)委外作業如為受託機構人員到金融機構提供服務時，是否建立門禁、攜入設備、作業區網段區隔、系統及資料存取權限等安控措施？是否全程派員監督並留存紀錄？		28
5.2.1.2	(2)如為資訊系統委外維運者，對受託機構提交之報告或紀錄是否有專責單位檢視及處理，是否建立雙方定期溝通及品質控管之機制？		28

業務別項目編號	查核事項	法令規章	評核項目編號
5.2.2	2.當委外廠商或相關管理員工職務調動或離職時，網路系統相關的權限與設定是否刪除以避免未經授權之存取？		28
5.2.3	3.對異常狀況是否能即時掌握並確實追蹤控管後續處理情形，重大異常事項是否提報高階管理階層？	「金融機構作業委託他人處理內部作業制度及程序辦法」	22
5.2.4	4.對受託機構是否建立妥適之查核機制，包括訂定查核計畫、查核範圍(含人員職務分工、作業處理、媒體管理、資料檔案及程式變更、受託機構之自行查核情形、災變因應計畫演練等)、查核單位、抽樣標準，及查核結果之呈報與後續改善情形追蹤等，並落實執行？	「金融機構作業委託他人處理內部作業制度及程序辦法」	28