

六、內部管理

項目編號	查核事項	法令規章
1	(一)分層負責制度	
1.1	1. 總社部分	
1.1.1	(1)理(監)事會之成員、組織、職權暨其功能：	
1.1.1.1	①理(監)事任期均為三年，連選得連任，另章程內是否載明之理事人數最多不得超過 15 人，監事人數最多不得超過 5 人。	1. 信用合作社法第 16 條。 2. 信用合作社法施行細則第 4 條。
1.1.1.2	②理(監)事當選就任前，其個別認繳股金是否未少於就任前一年底信用合作社實收股金總額百分之十五除以確定當選理事、監事總人數之平均數額，任期內發生個別認繳股金少於平均數額者，理(監)事當然解任。	「信用合作社社員代表理事監事經理人應具備資格條件及選聘辦法」第 40 條及第 41 條。
1.1.1.3	③具有配偶、三親等以內之血親或一親等姻親關係	「信用合作社社員代表理事監事經理人應具備資格條件及選聘辦法」第 10 條。

六、內部管理

項目編號	查核事項	法令規章
1.1.1.4	者，是否未同時分任同一信用合作社之理事、監事或同任監事；同任理事者是否以二人為限。 ④信用合作社之理事、監事、經理人及職員是否未兼任其他金融機構任何職務。但因投資關係，並經中央主管機關核准者，得兼任被投資銀行之董事或監察人。	1. 信用合作社法第 17 條。 2. 本會 108.11.13 金管銀控字第 10802733981 號令。 3. 「銀行之董(理)事、監察人(監事)由其他金融事業負責人兼任」問答集。
1.1.1.5	⑤理(監)事會是否由不同背景之個人或法人組成，以避免理事會決議事項由個人或少數人控制支配。	
1.1.1.6	⑥信用合作社專業理事之資格及人數，是否符合「信用合作社社員代表理事監事經理人應具備	「信用合作社社員代表理事監事經理人應具備資格條件及選聘辦法」第 9 條。

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
1.1.1.7	資格條件及選聘辦法」第9條之相關規定？ ⑦辦理選任人員暨候選人（含社員代表、理事及監事）資格條件查詢方式是否符合規定？	本會 109.12.22 金管銀合字第 1090146101 號函。
1.1.2	(2)理事會之執行業務及對信用合作社業務經營之督導管理：	
1.1.2.1	①業務之執行，除本法或章程規定應由社員代表大會決議之事項外，是否均由理事會決議行之。	
1.1.2.2	②理事會之決議，除另有規定外，是否有過半數理事之出席，出席理事過半數之同意行之。	
1.1.2.3	③理事對於會議之事項，有自身利害關係致有害於	

六、內部管理

項目編號	查核事項	法令規章
1.1.2.4	信用合作社利益之虞時，是否未加入表決，且未代理他理事行使表決權。 ④信用合作社對其利害關係人授信達中央主管機關規定金額以上者，是否經三分之二以上理事之出席及出席理事四分之三以上之同意。	銀行法第 33 條。
1.1.2.5	⑤理事會是否負責核准並定期覆核整體經營策略與重大政策，理事會對於確保建立並維持適當有效之內部控制制度則負有最終之責任？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 6 條及第 7 條。
1.1.2.6	⑥信用合作社各部門業務及稽核處理辦法或細則，是否報經理事會核議通過後實施。	

六、內部管理

項目編號	查核事項	法令規章
1.1.2.7	⑦信用合作社是否設立隸屬理事會之內部稽核單位，以獨立超然之精神，執行稽核業務，並應至少每半年向理事會及監事（會）報告？ 內部稽核單位對金融檢查機關、會計師與內部稽核單位所提列檢查意見或查核缺失，及內部控制制度聲明書所列應加強辦理改善事項，是否持續追蹤覆查，並將其追蹤考核改善情形，以書面提報理事會及交付監事（會），並列為對管理單位及營業單位績效考核之重要項目？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 27 條及第 42 條。
1.1.3	(3)監事會之執行業務及對信用合作社業務經營之監督管理：	

六、內部管理

項目編號	查核事項	法令規章
1.1.3.1	①監事監查時，是否得請理事會提供各種簿冊，必要時，並可請理事或有關職員說明？	「合作社監事監查規則」第7條。
1.1.3.2	②年度結束，監事會是否提出書面報告，將監查結果報告社員代表大會？	
1.1.4	(4)組織系統及分層負責辦事執行情形：	
1.1.4.1	①各部室及分支機構家數。	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第12條。
1.1.4.2	②全社員工配置情形。	
1.1.4.3	③總社各層級之內部控制程序及職務分工。	
1.1.4.4	④各主要業務分層負責辦事細則，是否適度授權；且考量內部牽制功能，並定期檢討其執行情形。	

六、內部管理

項目編號	查核事項	法令規章
1.1.4.5	⑤是否根據各授權層級授信統計表加以分析，以瞭解實際之分層授權績效，並予以評估。	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第42條。
1.1.5	(5)總社對營業單位業務經營之督導管理：	
1.1.5.1	①業務處理章則之訂定是否完備，有關內規與通函，不得與主管機關頒佈之法令規章相悖，內容是否適時更新。	
1.1.5.2	②對營業單位之經營績效考核辦法，除就存款、放款等業務量及盈餘情形考量外，內部管理是否也列入考核？	
1.1.5.3	③總社對各營業單位經營績效是否按月列表比較，對盈餘較差或虧損之單位，是否督導該單位檢	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
1.1.6	討改進。	
1.1.6.1	(6)為因應管理及業務需要設置之跨單位功能性小組，應充分發揮其督導管理功能：	
1.1.6.2	①對全社營業單位辦理授信業務之貸款對象集中程度，是否作妥適的控管，俾降低授信風險。	
1.1.6.3	②對信用合作社各類部位風險、投資風險之管理，是否訂定妥適的部位限額、投資限額、停損點、交易員及經理之權限，俾降低可能之風險。	
	③建立資產負債到期日缺口分析表，以利流動性管理。為降低流動性風險，是否訂定妥適的流動性比率。	

六、內部管理

項目編號	查核事項	法令規章
1.1.6.4	④對營業單位吸收短期大額存款之依存度，應予以適當管理；大額存款之異動，是否適時通知資金調度部門，以利全社資金之控管與調度。	
1.1.6.5	⑤管理利率風險，是否訂定妥適的利率風險管理辦法，及利率敏感性資產對利率敏感性負債之比例、利率敏感性缺口對淨值或總資產之比例等可容許之範圍。	
1.1.6.6	⑥是否建立利率敏感性資產與負債之資料，並利用電腦模擬分析因利率變動對盈餘及自有資本之可能影響。	
2	(二)總社內部控制制度	1. 「金融控股公司及銀行業內部控制及稽核制
2.1	1. 對各項業務作業流程是否訂	

六、內部管理

項目編號	查核事項	法令規章
	定相關規範及處理手冊【如：出納、存款、授信、匯兌、投資準則、客戶資料保密、利害關係人交易規範、適用國際會計準則之管理、會計暨財務報表編製流程、總務、資訊、人事管理（含輪調及休假規定）、對外資訊揭露作業管理、委外作業管理、金融檢查報告之管理、金融消費者保護之管理、重大偶發事件之處理機制、防制洗錢及打擊資恐機制及相關法令之遵循管理（包括辨識、衡量、監控洗錢及資恐風險之管理機制）、永續資訊之管理、營運持續管理機制、信用合作社法第 15 條所定業務、其他業務之規範及作業程序】，有無配合法令規定與實際需要適時訂正？	度實施辦法」第 12 條。 2. 本會 106.9.7 金管檢制字第 10601503300 號函。
2.2	2. 是否建立自行查核制度；法令遵循制度、風險管理制度	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 9 條。

六、內部管理

項目編號	查核事項	法令規章
	及資訊安全制度；及內部稽核制度等內部控制三道模型？三道模型之架構是否使各單位瞭解其各自在機構整體風險及內部控制架構所擔任之職責與功能，並加強執行內部控制工作之單位與內部稽核單位之溝通協調，以維持有效適當之內部控制制度？	
2.3	3. 如有理事表示異議且有紀錄或書面聲明者，是否將異議意見連同經理事會通過之內部控制制度送各監事（會）？修正時，亦同？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第6條。
2.4	4. 內部控制制度訂定後，有無促使總分支單位切實執行？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第5條及第12條。
2.5	5. 信用合作社是否訂定經理事會通過之適當風險管理政策與程序，並應設置獨立之專責	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第20條及21條。

六、內部管理

項目編號	查核事項	法令規章
2.6	風險控管單位或指定一總社管理單位負責風險控管，並定期向理事會報告風險管理資訊？ 6. 有無設置災害緊急應變小組及通報人制度、制定「災害緊急應變對策」手冊、舉辦防災教育訓練與演習。	1. 「金融事業機構災害緊急應變對策手冊範本」。 2. 「金融機構應檢討災害緊急應變對策手冊強化災害預防相關措施」。
2.7	7. 金融機構辦理安全維護，是否訂定安全維護作業規範，報經理事會通過後實施，並報主管機關備查。	「金融機構安全維護管理辦法」第 3 條。
2.8	8. 金融機構是否設置安全維護督導小組，指定高階主管一人為召集人，督導辦理與檢測安全維護執行情形、教育訓練及定期操作演練。	「金融機構安全維護管理辦法」第 4 條。
2.9	9. 金融機構之安全設施(包括警報、報警系統、閉路電視錄影	1. 本會 95.6.13 金管銀(二)字第 09500234510 號令「金融機構之營業單位得免僱用駐衛警、

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
2.9.1	監視系統、金庫、運鈔車安全設備、營業櫃台及大出納區、防火設備、保全防盜系統及防衛器材)是否適當；錄影檔是否保存二個月(新開戶櫃檯、自動櫃員機及其週遭部分應至少保存六個月)，標示錄影日期，並妥適保管備查。 (1)監視錄影系統是否注意攝影角度、光源、影像清晰度、時間準點顯示，及設備之防潮、防塵、防熱？如有監視錄影系統影像不清晰或角度不清楚者，是否予以改善？	保全人員或其他警衛人員專責擔任警戒工作之規定」。 2. 本會 101.10.19 金管銀國字第 10120005240 號令修正「金融機構安全維護管理辦法」。 1. 金融機構安全維護管理辦法第 5 條第 6 款。 2. 本會銀行局 105.6.4 銀局(國)字第 10500130790 號函。
2.9.2	(2)對警察機關依規定調閱監視器影像，是否積極配合辦理，未有久未提供之情事？	1. 金融機構安全維護管理辦法第 5 條第 6 款。 2. 本會銀行局 105.6.4 銀局(國)字第 10500130790 號函。
2.10	10. 是否強化自動櫃員機之安全，防止遭受破壞，以維客戶之權益；對於報廢之自動	「金融機構自動櫃員機安全防護準則」。

六、內部管理

項目編號	查核事項	法令規章
2.10.1	提款機，應予嚴格控管或銷毀，杜絕被重新組裝之可能性。 (1)為使民眾提高警覺，是否主動於自動櫃員機上張貼公告或於操作過程加入警語，提醒民眾注意自動櫃員機並無提供身份證明之功能。	本會 95.12.20 金管銀（一）字第 09510005560 號函「為防範詐騙集團翻新手法誘騙民眾利用自動提款機匯出存款，請提醒民眾自動提款機並無提供身分證明之功能」。
2.10.2	(2)是否強化自動櫃員機之監控機制，例如：委外管理、汰換機制、硬體操作技術、程式名單之管理等，並加強對自動櫃員機功能異常警訊之應變處理能力，以強化防護功能，並提理事會報告？	本會 105.7.14 金管銀控字第 10560002380 號函。
2.11	11. 是否依洗錢與資恐風險及業務規模，建立洗錢防制內部控制與稽核制度？其內容是否包括洗錢防制法第 7 條第 1 項所列事項？	洗錢防制法第 7 條。

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
2.12	12. 金融機構共同營業時間是否為星期一至星期五上午九時至下午三時三十分。	本會 106.9.6 金管銀國字第 10620004072 號函。
2.12.1	(1)各金融機構如擬於非共同營業時間對外營業者，是否於本會銀行局網際網路申報系統登錄完成後，始得於所登錄之非共同營業時間對外營業，無須函報本會備查。惟對外營業前，請確定相關帳務處理準則、內部控制機制、資訊設備之設施及安全維護均已完備，並應於營業場所及網站揭露各營業單位對外營業時間、接受申辦之營業項目、交易日之確定及帳務處理等。	本會 106.9.6 金管銀國字第 10620004072 號函。
2.13	13. 對於新開戶者，是否訂有標準流程來確認客戶身分並瞭	1.「信用合作社防制洗錢及打擊資恐注意事項範本」。

六、內部管理

項目編號	查核事項	法令規章
2.14	解客戶；對於舊客戶，是否 明定相關措施，以持續注意 其交易行為是否與其身分、 收入或營業性質相一致。另 對疑似不法或顯屬異常交易 者是否依規採取處理措施？	2. 本會 103.8.20 金管銀法字第 10310004610 號 令修正「存款帳戶及其疑似不法或顯屬異常交 易管理辦法」。
2.14.1	14. 金融機構作業委託他人處理 內部作業制度及程序辦法： (1) 金融機構作業委託他人處 理時，是否有簽訂契約，並 依本辦法辦理。所稱委外內 部作業規範是否載明下列 事項：作業委外之政策及原 則、指定專責單位及相關單 位對委外事項控管之權責 分工、委外事項範圍及委外 程序、客戶權益保障之內部 作業及程序、風險管理原則 及作業程序、內部控制原則 及作業程序、其他委外作業 事項及程序。金融機構對於 作業委外負最終責任，應就	「金融機構作業委託他人處理內部作業制度及 程序辦法」。

六、內部管理

項目編號	查核事項	法令規章
2.14.2	委外事項之風險程度、重大性及對營運及客戶權益影響進行評估，依風險基礎方法採取適當之控管措施。 (2)專責單位是否有定期至財團法人金融聯合徵信中心所建置受委託機構暨員工登錄系統查詢相關資料，並留存查詢紀錄備查。	
2.14.3	(3)車輛貸款業務之行銷、消費性貸款行銷、房屋貸款行銷業務等有關貸款行銷作業委外，是否由金融機構自行辦理客戶及關係人之對保簽章作業。	
2.14.4	(4)金融機構申請應收債權催收作業之委外，是否向主管機關申請核准。	
2.14.5	(5)金融機構作業委外如涉及	

六、內部管理

項目編號	查核事項	法令規章
2.14.6	客戶資訊者，是否於契約簽訂時訂定告知客戶之條款；其未訂有告知條款者，金融機構應書面通知客戶委外事項，並明訂客戶於接獲金融機構通知未於一定合理期間以書面表示反對者，視為同意。 (6)金融機構是否定期及不定期對受委託辦理應收債權催收作業之機構進行查核及監督，確保無違反「金融機構作業委託他人處理內部作業制度及程序辦法」第十四條各款規定。	
2.14.7	(7)金融機構辦理應收債權催收作業之委外，是否將其受託委外機構基本資料公布於金融機構營業場所及網站，以利債務人核對催收機構之相關資料。	

六、內部管理

項目編號	查核事項	法令規章
2.14.8	(8)金融機構作業委外是否無違反法令強制或禁止規定、公共秩序及善良風俗，對經營、管理及客戶權益，不得有不利之影響，並確保遵循銀行法、洗錢防制法、個人資料保護法、消費者保護法及其他法令之規定。	
2.14.9	(9)委外作業如為受託機構人員到社提供服務時，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？	
2.14.10	(10)保全業者受託收送有價證券、支票、表單及現鈔，於客戶端收送時是否未代表銀行向客戶確認款項已	「金融機構作業委託他人處理內部作業制度及程序辦法」相關問題適用解說問答集第15則。

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
2.14.11	入帳等行為？ (11)金融機構將作業委託他人處理涉及使用雲端服務是否依相關規定辦理？如具重大性或依委外辦法第 18 條將作業委託至境外，是否向主管機關申請核准？	1. 「金融機構作業委託他人處理內部作業制度及程序辦法」第 18 條及 19 條。 2. 「金融機構作業委託他人處理內部作業制度及程序辦法」相關問題適用解說問答集—雲端委外。
2.15	15. 安全維護作業 金融機構對其營業處所、金庫、出租保管箱（室）、自動櫃員機及運鈔業務等執行安全維護措施，是否依下列規定辦理：	1. 「金融機構安全維護管理辦法」第 6 條。 2. 本會 95.6.13 金管銀（二）字第 09500234510 號令「金融機構之營業單位得免僱用駐衛警、保全人員或其他警衛人員專責擔任警戒工作之規定」。
2.15.1	(1)營業處所安全維護措施	
2.15.1.1	①營業處所設置之大額出納櫃檯，是否以堅固材質之柵欄或防彈玻璃加以區隔，並裝置適當安全設施。現金收付櫃檯高度是否適當，並設置自動鎖抽屜，經收現鈔	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
2.15.1.2	應隨手置入抽屜並上鎖或回送大出納處。 ②作業部門是否嚴格管制非工作人員進入，並於出入口裝置門禁管制設施。	
2.15.1.3	③各營業單位於營業時間是否僱用駐衛警、保全人員或其他警衛人員專責擔任警戒工作。但有正當理由，且營業單位已建置適當安全維護措施者，是否向主管機關申請免適用前揭規定。營業單位如其現金收付櫃檯已裝設密合式防護玻璃或其他安全隔離設施，於營業時間內，得免僱用駐衛警、保全人員或其他警衛人員專責擔任警戒工作。	

六、內部管理

項目編號	查核事項	法令規章
2.15.2	(2)金庫、出租保管箱(室) 安全維護措施：	
2.15.2.1	①金庫室、保管箱(室) 是否加強各項進出管制 設(措)施，不得呈常 開狀態。	
2.15.2.2	②金庫室鑰匙、密碼是否 指定二人以上分別控 管。金庫室門應裝置定 時鎖，管制開啟時間。	
2.15.2.3	③金庫室、保管箱(室) 如有淹水顧慮者，是否 裝置防、排水及其警報 系統設備。	
2.15.3	(3)自動櫃員機安全維護措 施：	
2.15.3.1	①自動櫃員機裝置時，是 否詳確評估其安全性， 慎選設置地點。對非設	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
	置於營業處所之行外自動櫃員機，須考量管轄單位是否方便監督管理，並優先選擇有保全設備或有警衛、值勤人員巡守之處所。	
2.15.3.2	②自動櫃員機是否裝置於明亮處所。	
2.15.3.3	③對設置之自動化服務設備，是否張貼進行交易應注意事項，設置防盜安全設備、防止他人窺視與使用者得察覺後方情況設施、照明及必要之防火逃生設備等。	
2.15.3.4	④金融機構是否督導營業單位，加強派員巡查行內外設置之自動櫃員機使用情形、門禁及相關防護設施。	

六、內部管理

項目編號	查核事項	法令規章
2.15.3.5	⑤建立自動櫃員機異常提領監控機制，是否指定專人負責。如查有異常情形，應儘速採取適當措施，妥善處理。不定時巡查自動櫃員機，防範歹徒破壞（假日及非營業時間尤為重要），並予以記錄。	本會 101.10.19 金管銀國字第 10120005240 號令修正「金融機構安全維護管理辦法」。
2.15.4	(4)運鈔業務安全維護措施：	
2.15.4.1	①辦理現金（含外幣）運送或對特定客戶提供收款服務時，除因特殊情況報經各單位總機構核准者外，是否均委由合格之專業運鈔保全業者辦理，並配合協助做好控管工作。如自行辦理現金運送應以專用運鈔車或普通車輛改裝之運	

六、內部管理

項目編號	查核事項	法令規章
2.15.4.2	鈔車為之，並注意運鈔作業安全維護。 ②普通車輛改裝之運鈔車是否裝置引擎電源阻斷開關及具有防搶、防盜功能之固定式密碼鎖鐵櫃或防盜運鈔箱(袋)，放置於車內隱密處，並配備必要之防禦警戒裝備、求援通訊設備及滅火器材。	
2.15.4.3	③運鈔路線及時間是否隱密及多變化，事先應做好狀況預判。	
2.15.4.4	④派員赴外收付款項，有無注意牽制及安全？是否未由保全業者自行辦理行外代收付？	1. 財政部 91.8.20 台財融(一)字第 0911000537 號令「金融機構派員辦理收付款項有關規定」 2. 「金融機構作業委託他人處理內部作業制度及程序辦法」相關問題適用解說問答集—現鈔運送作業範圍。
2.15.5	(5)簡易型自動提款機安全維	1. 金融機構安全維護管理辦法。

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
2.15.5.1	護措施： ①是否防護薄弱，未見加裝阻隔器材、柵欄或其他安全防護設備？	2. 本會105.2.3金管銀國字第10500027890號函暨內政部警政署 105.1.29 警署刑防字第1050050467號函。
2.15.5.2	②是否加裝警報感應系統，以於遭移動時能發生警示作用？	
2.15.5.3	③自動提款機區是否加裝隱藏式攝錄影機及收音等設備？	
2.15.5.4	④發生簡易型自動提款機竊盜未遂案件，是否即時通報警示其他單位防範？	
2.15.5.5	⑤是否落實金融機構安全維護管理辦法規定	

六、內部管理

項目編號	查核事項	法令規章
	(如:辦理員工自衛編組演練、安全檢測工作、與警察機關溝通聯繫管道等),加強簡易型自動提款機安全維護措施?	
2.16	16. 聘用顧問是否訂定內部遵循事項?遵循事項內容是否符合規定?	本會 106.11.22 金管銀合字第 10630002852 號函。
2.17	17. 總社管理單位是否就金檢缺失態樣,檢討相關內部控制制度,注意各項作業流程是否符合牽制原則,並確實督導營業單位落實執行各項作業規範?	本會 107.1.23 金管檢銀字第 1070604007 號函。
2.18	18. 與大陸地區法人、團體簽署合作協議,其簽署內容、合作範圍及實際從事業務往來,是否符合臺灣地區與大陸地區人民關係條例第 33-1 條第 1、2 項及其他相	本會 108.4.30 金管銀法字第 10801036730 號函。

六、內部管理

項目編號	查核事項	法令規章
2.19	關法令規定?簽署前是否提報理事會討論通過?	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 21 條。 本會 105.3.29 金管檢控字第 1050152063 號函。
3	19. 風險管理專責單位是否建立清楚適當之風險管理傳達、諮詢、協調與溝通機制，以利即時調整風險管理策略?	
3.1	(三)營業單位內部控制制度	
3.1.1	1. 一般事項 (1)各項業務作業流程(如：庫房管理、出納、存款、授信、外匯、匯款、票據託收、聯行往來、會計處理、電腦作業等)，是否符合有關法令規定暨總社之政策、內規與內控牽制原則? 總社是否定期檢討分社各項業務作業流程符合內控制度設計，並落實分社管理及監控機制?分社是否落實執行各項內部作業規範及自行查核工作?	

六、內部管理

項目編號	查核事項	法令規章
3.1.2	(2)對駐外單位之管理。	
3.1.3	(3)例外事項之管理，是否規定（如：存款戶未攜帶印鑑或存摺請求提款、放款文件單據未全請求撥款、營業時間外之收付款項等），以瞭解其牽制功能。	
3.1.4	(4)金融機構辦理保管有價證券業務，是否確實留下稽核軌跡，及加強內控防弊措施，使不致發生多開保管證明文書或衍生一票數賣之情形。	
3.1.5	(5)金融機構辦理客戶開戶錄攝之資料是否至少保存六個月？	1. 中華民國銀行公會國內金融機構受理存戶新開戶建立影像檔注意事項（本會 105.2.19 金管銀法字第 10500029440 號函備查）。 2. 「金融機構安全維護管理辦法」。
3.1.6	(6)是否依規強化金融消費者	1. 中央銀行外匯局 93.8.2 台央外柒字第

六、內部管理

項目編號	查核事項	法令規章
3.1.6.1	保護、防制偽鈔及洗錢防制，及強化辦理業務人員之偽鈔辨識能力並即時更新驗鈔機軟體或設備？ ①受理顧客兌換時，是否落實認識客戶程序(KYC)，確認客戶身分或基本資料？是否對現鈔來源加以瞭解？如疑似不法洗錢行為，是否依「洗錢防制法」等相關規定辦理？	0930039849 號函。 2. 本會 105.3.8 金管銀控字第 10560000600 號函。 3. 中央銀行外匯局 105.3.9 台央外柒字第 1050011586 號函。
3.1.6.2	②若發現偽造外國幣券，是否確實依「偽造變造外國幣券處理辦法」辦理？	
3.1.6.3	③發現可疑人物以偽鈔結售或匯款，是否即時通報並妥適保管可疑人物使用之偽鈔、物品與錄	

六、內部管理

項目編號	查核事項	法令規章
3.1.6.4	影畫面等資料？ ④分社外幣現鈔以託收方式送總社查驗，是否以會計科目列帳或設簿控管？	
3.1.6.5	⑤採購外幣驗鈔機是否簽訂維護合約(含軟體更新作業)？	
3.1.7	(7) 是否確實認識客戶，判斷客戶行為是否有異常特徵疑似人頭帳戶？對於瞭解客戶動機與目的及加強客戶身分確認等，是否依規辦理？對於冒用或偽變造身分證開戶者，是否立即通知警調機關處理及通報財團法人金融聯合徵信中心？	1. 中華民國銀行公會「防杜人頭帳戶範本」及「開戶作業檢核表範本」。 2. 「信用合作社防制洗錢及打擊資恐注意事項範本」。
3.2	2. 庫房管理	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.2.1	(1)庫房是否裝置保全防盜系統、自動報警、自動定時鎖等，安全措施是否嚴密妥善，庫房內是否裝置全天候錄影監視系統，進出金庫是否設簿登記？	「金融機構安全維護管理辦法」第6條。
3.2.2	(2)非營業時間金庫鑰匙、密碼是否輪流由二人以上共同保管，一人不得開啟，並嚴予保密。	
3.2.3	(3)庫房內外庫鎖匙及密碼，是否由主管人員(或其指定人員)及出納分別掌管會同啟閉，密碼是否隨掌管人員異動而更改。	
3.2.4	(4)庫房內有無未列帳之現金、票據、保管品及屬於私人之財物。	
3.2.5	(5)庫存現金是否一律存放庫	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.2.6	房內？庫存表是否存放庫房內？是否經會計簽章？ (6)管庫人員之交接及庫房之啟閉有無紀錄。	
3.2.7	(7)營業時間中，庫房內存放現金之錢櫃或現金庫房是否隨時上鎖，其鑰匙是否由大出納保管？	
3.2.8	(8)庫存現金(包括現金運送)有無投保？保險金額是否適當？庫存現金有無經常作不定期檢查並作成檢查紀錄。	
3.2.9	(9)櫃員箱內有無餘額表，該表是否經大出納或換人盤點後簽章？	
3.2.10	(10)有無加強員工自衛編組，實施防護區制，定期	

六、內部管理

項目編號	查核事項	法令規章
	演練，確立「安全維護人人有責」觀念？	
3.3	3. 出納制度	
3.3.1	(1)現金收付有無未憑收付款項傳票或憑單辦理。	
3.3.2	(2)收付傳票或憑單，內部各級人員應予簽章，除採櫃員制在授權額度內之收付另有規定外，收入部分是否在交易完成後，付出部分是否在付款前簽章齊全。	
3.3.3	(3)收付傳票或憑單，是否均加蓋收付訖戳記並加註日期。	
3.3.4	(4)現金收付傳票或憑單有否於辦理收付前後隨即編號並依序登入現金收付紀錄	

六、內部管理

項目編號	查核事項	法令規章
3.3.5	表。 (5)收付款項是否在規定營業時間內辦理；其於營業時間外收付款項，處理手續及內部牽制是否符合規定，並設簿登記備查。	「金融機構安全維護管理辦法」第6條。
3.3.6	(6)「運送中現金」之運出方法及安全措施是否妥善？是否投保運送險？收到行在報單未到達前有否先行列帳，核對報單與金額是否相符。	
3.3.7	(7)抽查櫃員應存備用現金與現金收付紀錄表結餘是否相符。	
3.3.8	(8)辦理分組出納（小出納制度）向出納部門經領備用款項，有否依規定手續辦理，營業時間結束後，有	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
	否歸併出納庫存。	
3.3.9	(9)採櫃員收付制度者，櫃員收付款項有無踰越授權額度？櫃員與出納間資金之收受有無紀錄？配置櫃員機使用者，每筆收付有無印錄於傳票上。	
3.3.10	(10)代收稅款公用事業費用等代理業務有無收款、掣發收據，結帳均由同一人辦理之情事；有無加強對櫃員收受現金之不定期查核。	
3.3.11	(11)駐外辦理收付人員向出納部門領支備用款，領用金額有否經主管人員核准，並填製傳票。	
3.3.12	(12)存款業務之付款、驗印與記帳工作，在一線制作	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.3.13	業，雖可由櫃員一人自行辦理，惟是否訂定適當的付款授權額度；在二線制作業，應分人辦理，以符合牽制。	「金融機構安全維護管理辦法」第6條。
3.3.14	(13)作業部門應嚴格管制非工作人員進入，並於出入口裝置門禁管制設施；大額出納櫃台，是否裝置適當安全設施；營業櫃台抽屜是否有裝設自動鎖，以確保鈔券安全。	
3.4	(14)有無檢討查核有關空白存單之管理、存單之開發、對帳暨受理存單為擔保之認證、設定等作業之內部控制事宜。	
3.4.1	4. 存款業務 (1)抽查傳票中已付訖之支票，取款條及存單等，是	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.4.2	否均經驗印後付款，其印鑑是否與客戶原留印鑑相符。	
3.4.3	(2)採用連線作業，每筆超過櫃員授權額度之收付，其認證印錄有無先經主管核章。	
3.4.4	(3)營業終了，科目日結單是否由非原經辦人員辦理。若由原經辦人員辦理，有無經會計人員加以覆核。	
	(4)金融機構派員赴客戶處收付存款是否於事前登記，事後由第3人確認，並定期寄送對帳單。金融機構派員赴證券商辦理代理收付款項業務及派員常駐辦理收付稅、費等各機關應繳庫之收入及公營事業或公用事業款，是否向本部	1. 本會 101.9.21 銀局(合)字第 10130002210 號函。 2. 財政部 91.8.20 台財融(一)字第 0911000537 號函「金融機構派員辦理收付款項有關規定」。 3. 信用合作社防範職員挪用客戶款項相關內控作業規範範本第 6 條。

六、內部管理

項目編號	查核事項	法令規章
3.4.5	提出申請？ (5)金融卡及密碼單之保管及使用是否符合牽制原則。	本會 106.6.27 金管檢銀字第 1060103830 號函。
3.4.6	(6)是否禁止辦理以「提現」為名，「轉帳」為實之交易，並列入內部稽核及自行查核重點。	
3.4.7	(7)對於未蓋收款訖章或轉帳章之收入傳票，有否嚴禁記帳員先行記帳。轉帳支出交易，櫃員應先核對印鑑相符，確認存款帳戶餘額足夠及蓋章後，再交由存款主管或會計核准及加蓋「轉帳支出」戳記於傳票上，再行辦理轉帳交易。	
3.4.8	(8)記帳機每日開機及清機工作是否留存紀錄；清機紀錄應送請主管或會計與科	

六、內部管理

項目編號	查核事項	法令規章
3.4.9	日日結單借貸總數相核對，如有不符，是否查明原因，並作「錯誤更正表」，經由主管核章。 (9)與軋帳有關之紀錄，如記帳機紙捲、清機紀錄、錯誤更正表、存款餘額表等，是否交由會計部門或指定專責人員，妥善保管。	
3.4.10	(10)研討「使用主管卡交易」事項內容務須具體可行，是否落實事前核准事後覆核之控管。	
3.4.11	(11)嚴禁行員一人辦理互為牽制之數項工作或代存戶保管存摺、印鑑、代辦存、取款項、代還放款等；主管人員對業務處理程序，是否善盡覆核責任；妥慎執管各項作業之	

六、內部管理

項目編號	查核事項	法令規章
	主管卡及戳記。	
3.4.12	(12)代理證券公司股款收付劃撥交割業務，是否未有以遲延借記轉帳支出傳票等方式，協助證券公司完成股款之結算交割。	本會 93.11.25 金管銀(三)字第 0938011934 號函「金融機構代理證券公司股款收付劃撥交割業務，不得以遲延借記轉帳支出傳票或延後記帳等方式處理」。
3.4.13	(13)金融機構在其營業廳內辦理代理收付證券商客戶之證券交易款項業務無須報經主管機關核准；出租營業廳部分空間或代銷代購非金融商品部分，是否檢具書面計畫報本會備查？	本會 106.7.11 金管銀合字第 10600085630 號函。
3.5	5. 授信業務	
3.5.1	(1)客戶繳還放款本金或利息是否未由授信人員兼辦收取。	
3.5.2	(2)重要債權憑證及單據（如	

六、內部管理

項目編號	查核事項	法令規章
3.5.3	借據還款本票客票、他項權利證書、設質之有價證券等）之保管是否安全，有無交由主管或出納部門收管。 (3)對金融機構辦理有價證券（如：股票、定存單、....）質借放款，應查核其種類、張數、金額、號碼是否與帳簿記載相符。	
3.6	6.匯款業務	
3.6.1	(1)匯出匯款之查核	
3.6.1.1	①連線作業：	
3.6.1.1.1	I 匯款連線作業是否指派匯款經辦人員、覆核人員及放行主管人員分別負責辦理，並與匯款連線作業之電腦系統所設定之有權使用人員相符。	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.6.1.1.2	II 匯款放行卡是否由放行主管妥善保管，並親自使用。	
3.6.1.1.3	III 匯款連線作業有關人員，其操作密碼是否定期更換，遇有人員異動，是否立即變更密碼。	
3.6.1.1.4	IV 匯款經辦人員辦理匯款，須離開端末機時，是否立即辦理簽退手續，以防止他人使用。	
3.6.1.1.5	V 各種匯出匯款是否先經收款程序後，再辦理匯款手續。	
3.6.1.1.6	VI 匯款連線作業之放行主管，是否對匯款經辦人員輸入匯款連線作業系統之匯款資	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.6.1.1.7	料，與客戶填寫的申請書內容、金額等核對相符後，親自使用匯款放行卡放行匯出，並於匯款申請書及電腦印錄之匯出匯款表核章。 VII 金融機構辦理匯款及無摺存款時，有關核對及確認客戶身分所需之範圍、程序及文件，是否依規定辦理？	1.「金融機構受理國內匯款及無摺存款確認客戶身分作業規範」。 2.「金融機構辦理國內匯款及無摺存款作業確認客戶身分原則」。
3.6.1.2	②人工作業：	
3.6.1.2.1	I 各種匯出匯款是否先經收款程序後，再辦理匯款手續。	
3.6.1.2.2	II 各種匯款之收款人員、押碼人員、匯出人員及記帳人員，是否由不同人員擔任，以符牽	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.6.1.2.3	制。 Ⅲ 電話匯款之發話人員或票匯、信匯之簽章人員與密碼編列人員，是否分由不同人員擔任，且應為總行核准之人員。	
3.6.2	(2)匯入匯款之查核	
3.6.2.1	①連線作業： 匯入匯款連線作業之入戶匯款自動入帳後，解付匯款單經由匯款主管核章後，交由匯款經辦人員結帳時，作為（借）聯行往來傳票附件。	
3.6.2.2	②人工作業：	
3.6.2.2.1	I 入戶電匯之接話人員與密碼核驗人員是否分由不同人員擔任，且應為總行核准之人員。	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.6.2.2.2	II 辦理匯款解付時，入戶電匯應核驗其押碼相符；票匯及信匯是否核對其印鑑相符後辦理。	
3.6.2.2.3	III 入戶電匯經核驗其押碼相符後，是否即入受款人存款帳戶或通知其具領。	
3.6.2.2.4	IV 當日接到匯款委託書後，是否即時登載應解匯款簿。	
3.6.3	(3) 匯款密碼及通匯印鑑卡之管理	
3.6.3.1	① 匯款密碼表，正本是否由經理妥善保管，副本是否由指定之襄理級以上人員妥慎保管及使用，其派任與授受應設簿登記控管。	

六、內部管理

項目編號	查核事項	法令規章
3.6.3.2	②匯款密碼表是否定期或不定期更換使用，掌管密碼編譯人員異動時，應立即更換密碼。	
3.6.3.3	③聯社及同業通匯印鑑卡是否整理完畢，並妥善保管使用。	
3.6.4	(4)匯款銷帳之管理	
3.6.4.1	①匯出匯款久未解訖部分，是否洽詢匯入行（付款行）查明原因。	
3.6.4.2	②匯出匯款之付款行寄來解款報單，是否核對付款行留存之印鑑，及時轉帳並於匯出匯款登記簿註明銷帳日期。	
3.6.4.3	③匯出匯款懸帳過久無法處理者，是否轉列「其他	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.6.4.4	應付款」科目。 ④匯入匯款已解付部分，是否於應解匯款簿註明解付日期。	
3.6.5	(5)其他 跨行通匯為金融業對客收費之服務項目，匯款申請書之回條不宜加註對客戶不公平待遇之文句。	中央銀行業務局 84.2.27(84)台央業字第 228 號函「為提升跨行通匯服務品質，央行邀集有關單位會商結論」。
3.7	7. 託收票據	
3.7.1	(1)櫃員收取客戶之託收票據，應按下列程序辦理：	
3.7.1.1	①櫃員受理託收票據時，是否審核票據要項齊全，背書連續，票據背面之託收人帳號與戶名填載齊全後，始可受理。	
3.7.1.2	②櫃員是否於託收票據正	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.7.1.3	面加蓋該社親收之特別橫線章。 ③櫃員收受客戶之託收票據，是否掣給客戶收據；對託收筆數較多之客戶，可以「託收票據存摺」發給客戶以替收據。	
3.7.1.4	④櫃員收受客戶之託收票據，是否登錄於「櫃員受理託收票據登記簿或明細表」後，送交託收票據經辦員簽章處理。	
3.7.2	(2)託收票據經辦員是否將當日受理之託收票據逐筆輸入電腦，並逐筆勾稽覆核其張數及金額，且應與電腦明細表及「託收票據日報表」相符。	
3.7.3	(3)託收票據經辦員是否依據	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
	輸入電腦，所列印「託收票據電腦明細表」的順序整理票據，及繕製以借「應收代收款」、貸「受託代收款」科目轉帳傳票，一併送交主管人員核章保管。	
3.7.4	(4)保管託收票據之主管人員是否核對託收票據號碼、金額、託收人所填寫之存款帳號，與電腦明細表之資料相符後入庫保管。	
3.7.5	(5)託收票據是否指定主管人員或非經辦人員，按本埠、外埠及到期日先後順序保管。	
3.7.6	(6)保管中之託收票據，若需抽換，是否請客戶填寫申請書、簽蓋原留印鑑，於驗印無誤經主管核准後辦	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.7.7	理。 (7)託收票據是否按期提示， 並如期全額存入委託人帳戶。 託收票據退票是否立即通知客戶領回。	
3.8	8. 會計處理	
3.8.1	(1)各項交易傳票是否經有關 人員簽章；主管核章時， 是否詳加核對傳票內容、 電腦列印之認證資料、應 記載事項，以免發生弊端。	
3.8.2	(2)各項交易傳票經主管核章 後是否交由會計部門整 理，並於營業終了據以編 製科目日結單（或指定非 原經辦人員編製科目日結 單）。	
3.8.3	(3)各級人員調閱傳票，是否 填具「傳票調閱單（簿）」	

六、內部管理

項目編號	查核事項	法令規章
	並經主管核准。	
3.8.4	(4)查核傳票整理情形：	
3.8.4.1	①有關人員之簽章是否齊全。	
3.8.4.2	②抽查傳票張數、金額與科目日結單或總傳票加以核對，是否相符。	
3.8.4.3	③傳票是否按時裝訂、編號、裝訂處有無經辦、會計及主管核章。	
3.8.4.4	④抽查科目日結單餘額是否與總分類帳餘額相符。	
3.8.5	(5)傳票未完備事項應設簿登記，並由會計部門隨時追蹤管理。	
3.8.6	(6)經會計轉帳的各類傳票，	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
	是否由會計詳加核對傳票內容、金額及應記載事項後，再行辦理。	
3.8.7	(7)會計業務主管不得兼辦出納或經理財務。	信用合作社會計作業規範範本第6章第6節。
3.8.8	(8)各種帳簿之啟用是否經各級人員簽章，帳簿記載應清晰，其錯誤之更正、過帳及空白作廢等手續，是否依照規定辦理。	商業會計處理準則第11及13條。
3.8.9	(9)日計表各科目餘額是否與各科目的總分類帳相符。	
3.8.10	(10)營業時間終了軋帳，各科目傳票張數、金額，是否與科目日結單、電腦連線作業之科目交易彙計查詢單，所列張數及金額相符。	

六、內部管理

項目編號	查核事項	法令規章
3.8.11	(11)填送主管機關各項定期性報表，是否確實填報正確。	銀行法第 45 條。
3.8.12	(12)傳票、帳簿、報表是否專設檔案室或庫房保管。其檔案室或庫房應配鎖，並注意安全及消防措施，以避免傳票等遭破壞、滅失。	
3.9	9. 金融機構國內分支機構之管理：	「金融機構國內分支機構管理辦法」。
3.9.1	(1)金融機構增設、遷移或裁撤分支機構，是否依主管機關規定填具申請書件申請。	
3.9.2	(2)金融機構經許可增設或遷移分支機構者，是否自核准之日起一年內，向主管機關申請核(換)發營業執照並開始營業。	

六、內部管理

項目編號	查核事項	法令規章
3.9.3	(3)金融機構開始或停止營業前，是否事先報主管機關備查。	金融機構國內分支機構管理辦法。
3.9.4	(4)金融機構欲成立簡易型分社，是否依「金融機構國內分支機構管理辦法」規定申請核准。其員工人數上限為八人，是否有符合安全維護及內部控制原則，辦理中小企業放款者，營業員工人數上限得提高為十人。	
3.10	10. 端末機作業管理	
3.10.1	(1)端末機使用管理	
3.10.1.1	①對經授權使用端末機人員之姓名、使用者代號或作業卡（控制卡、主管卡及櫃員卡）卡號、使用權限、起訖時間是否設簿登記，並經使用人簽章以明	

六、內部管理

項目編號	查核事項	法令規章
3.10.1.2	責任？登記簿是否與電腦使用人員資料檔內容相符？ ②若作業卡因毀損而需要更換時，是否依照申請手續重新申請？並將毀損之卡片繳回？	
3.10.1.3	③對授權由連線單位自行製作作業卡，其控管是否依規定程序辦理？	
3.10.1.4	④作業卡遺失時是否即時向主管人員報備，並註銷該作業卡號？	
3.10.1.5	⑤對備用作業卡之保管是否妥當？封存啟用時是否由會計人員會同辦理，並作成紀錄？	
3.10.1.6	⑥端末機使用人員資料（如	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.10.1.7	使用者代號、密碼、交易權限)之建檔、變更、註銷是否經申請、核准程序並留存紀錄？ ⑦ 端末機使用者代號之授予及各人之交易權限是否符合分工制衡原則？	
3.10.1.8	⑧ 使用者密碼(含主管密碼、端末機操作密碼、櫃員密碼等所謂「通行碼」)是否可由使用人視情況需要定期或不定期變更？	
3.10.1.9	⑨ 是否有適當之管制措施以防止櫃員於營業時間外使用端末機從事非法之交易？	
3.10.1.10	⑩ 處理或核可交易時是否均憑被授予之使用者代	

六、內部管理

項目編號	查核事項	法令規章
3.10.1.11	號或作業卡親自操作端末機？有無共用同一使用者代號或作業卡之情形？ ⑪操作人員暫時離機或他人需使用同一端末機時，是否由原操作人員簽退 (sign off, logon off)？	
3.10.1.12	⑫對於調離職人員是否取消其使用者代號並收繳其領用之作業卡？	
3.10.2	(2)交易處理控制	
3.10.2.1	①營業單位對於操作端末機、檢核輸出入資料、收付相關財務（如現金、票據）與日結處理等之分工與作業流程是否符合內部牽制原則？	

六、內部管理

項目編號	查核事項	法令規章
3.10.2.2	②對於各種傳票、登錄單、科目日結單等單據是否由有關人員覆核認證欄印錄之內容，並於認證欄核章？認證資料若印錄不清或重疊，而以人手補正時是否附電腦資料查詢單供主管查核簽章？	
3.10.2.3	③認證欄印錄內容，有無包含下列資料(交易代號、序號、櫃員代號、機號、主管代號、交易日期、時間、地點、金額)？機器印錄字體、深淺有無一致？	
3.10.2.4	④特殊交易之處理（如更正、沖銷、抵用）是否設簿登記，並由主管親自使用主管卡或密碼核准？或另有其他管制措施？	

六、內部管理

項目編號	查核事項	法令規章
3.10.2.5	⑤特殊交易登記簿是否切實與電腦輸出之特殊交易明細表核對，並經主管人員簽章確認？	
3.10.2.6	⑥一般性交易控管是否週延？對特殊交易是否可用一般性交易規避(如有摺交易可不經刷卡動作直接以鍵盤輸入帳號)？	
3.10.2.7	⑦下列各項交易是否均予列入特殊交易項下控管：	
3.10.2.7.1	I 各項更正(沖正)交易。	
3.10.2.7.2	II 變更利率交易。	
3.10.2.7.3	III 提前起息存款交易。	
3.10.2.7.4	IV 調整存款積數交易。	
3.10.2.7.5	V 磁條重建交易。	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.10.2.7.6	VI無摺提款(轉支)交易。	
3.10.2.7.7	VII變更透支契約到期日交易。	
3.10.2.7.8	VIII存單質權設定(登錄)解除。	
3.10.2.7.9	IX變更繳息檔交易。	
3.10.2.7.10	X建立金融卡透支額度交易、主管卡製作交易及變更帳卡磁條餘額交易等。	
3.10.2.7.11	X I 若未列入，有無其他內部牽制？	
3.10.2.8	⑧對於櫃員所作之交易（含端末機簽進、簽退）是否留下序時紀錄，以供查核？序時記錄資料異常情形(如結帳關機後重新	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.10.2.9	開機)有無查明？是否按日併同傳票裝訂或妥善保管？有無採用銷號單依序銷號以避免傳票遺漏或憑空輸入？若無，是否有其他控管方式？ ⑨電腦故障時若須採行離線或人工作業，是否依照規定程序辦理？	
3.10.2.10	⑩當電腦恢復連線作業時，是否備有適當的處理程序以防止交易的遺失或重覆輸入？	
3.10.2.11	⑪電腦故障期間之交易，於恢復連線作業時，事後補行輸入（原採人工作業），或補後送至中心主機（原採離線作業），對輸入資料之檢核是否確實妥慎？	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.10.3	(3)日結處理	
3.10.3.1	①營業單位日終結帳手續 是否有明文規定之程序？是否依櫃員日結、科目日結、營業單位日結逐項進行？如無則其結帳程序是否妥當？	
3.10.3.2	②機器印錄之科目日結單 是否由會計加以覆核？其借貸方筆數、金額是否與傳票加總核對？	
3.10.3.3	③結帳或關機後始發現有未輸入電腦或輸入錯誤之資料，是否有妥善處理程序？若當日無法補輸入或更正時，是否予以登記控管？	
3.11	11. 金融卡、密碼單及自動化服務機器管理	

六、內部管理

項目編號	查核事項	法令規章
3.11.1	(1)金融卡管理	
3.11.1.1	①金融卡之申請、保管、發交、遺失、作廢、銷戶等是否設簿登記控管？	
3.11.1.2	②金融卡及密碼單若由客戶至原申請單位領取，營業單位是否分開由兩位主管負責保管，並設簿登記？	
3.11.1.3	③金融卡領用收據及啟用登錄申請書印鑑是否與金融卡使用約定書原留印鑑相符？	
3.11.1.4	④金融卡啟用登錄申請書是否有啟用登錄認證並經主管核章？	
3.11.1.5	⑤客戶結清銷戶或因故終止使用，是否立即於金融卡磁條處打孔作廢，並辦	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.11.1.6	理金融卡註銷登錄交易？ ⑥ 客戶金融卡遺失或遭 CD/ATM 機器吸進時，是否依適當程序處理，以保障客戶權益？	
3.11.2	(2) 客戶密碼管理	
3.11.2.1	① 密碼單係由客戶到原申請單位領取，是否確定客戶親自前來領取時才發給密碼單？	
3.11.2.2	② 若密碼單係以郵寄方式寄給客戶，是否以掛號寄出？	
3.11.2.3	③ 客戶如果遺失密碼單或忘記密碼，是否有適當之控管程序予以處理？	
3.11.3	(3) 自動化服務機器使用管理	

六、內部管理

項目編號	查核事項	法令規章
3.11.3.1	①為提高自動化服務機器作業之品質及管理，是否訂有自動化服務機器業務處理要點或作業管理辦法？	
3.11.3.2	②自動化服務機器金庫門鑰匙、密碼、及鈔券匣鑰匙保管是否符合牽制原則？	
3.11.3.3	③使用自動化服務機器交易之最高金額及次數是否設有限制？	
3.11.3.4	④自動化服務機器現金之裝卸及清點是否由營業人員會同出納人員二人以上辦理？	
3.11.3.5	⑤維護自動化服務設備時（含程式換版、保養及故障維修），維護人員是否	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.11.3.6	執相關認可文件由專人在旁陪同，留存維護紀錄（含程式維護、設備故障維修情形及維護人員、時間），並定期陳報？對異常狀況有否追蹤查核？ ⑥如果連續輸入錯誤密碼超過限制次數，自動化服務機器是否能將卡片吸入？	
3.11.3.7	⑦自動化服務機器是否能將可疑或仿冒卡片吸入？	
3.11.3.8	⑧客戶每次使用自動化服務機器進行交易時，是否均印製交易明細表，載明交易日期、時間、種類、金額等資料供客戶參考？	

六、內部管理

項目編號	查核事項	法令規章
3.11.3.9	⑨對客戶存款如有不符之異常狀況是否建立通報機制及處置措施，並予以追查原因？	
3.11.3.10	⑩若因自動化服務機器故障或客戶操作不當而使卡片留在機器內時，是否有適當之處理程序？	
3.11.3.11	⑪自動化服務設備、發放客戶之使用手冊及金融卡上，是否標示或說明使用出現異常時應變處理方法（如即刻於他台機器上變更密碼或通知所屬金融機構及必要時掛失止付等）？	
3.11.3.12	⑫自動化服務機器之交易是否有收付明細及序時紙捲可供查核？此報表是否每日查核？	

六、內部管理

項目編號	查核事項	法令規章
3.11.3.13	⑬ 自動化服務機器旁是否裝置攝影機、錄影機或其他類似裝置？	中華民國銀行公會 92.9.19 全內安字第 2476 號函「訂定中華民國銀行公會會員安全維護執行規範」。
3.11.3.14	⑭ 對自動化服務機器之故障情形是否皆留下紀錄，並定期查核此報表？	
3.11.3.15	⑮ 金融機構設置自動化服務設備是否於每年十一月填具下年度設置之申請書，向主管機關提出申請，其經核定有業務區域者，限於該地區設置。 當年度擬置台數超過原申請台數時，金融機構得事先填具增加設置申請書，向主管機關提出申請。但一年以一次為限。	「金融機構營業場所外自動化服務設備管理辦法」第 3 條。
3.11.3.16	⑯ 金融機構遷移或裁撤營業場所外自動化服務設	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.11.3.17	備，是否於遷移或裁撤前 事先填具申請書向主管 機關申請。 ⑰金融機構是否於營業廳 外設置之自動化服務機 器上明顯標示金融機構 名稱、所屬營業單位、緊 急連絡電絡、服務項目及 服務時間，並應張貼或於 自動化服務設備螢幕顯 示進行交易應注意事 項。營業場所外設置自動 化服務設備之服務區，經 金融機構評估其業務需 要，並訂定內部管理規 範，報經理事會通過後， 得配置人員常駐在場，但 限於提供自動化服務設 備之管理及使用操作之 諮詢。前項服務區，如有 配置人員常駐，應以網際 網路申報系統向主管機	同上辦法第7條。

六、內部管理

項目編號	查核事項	法令規章
3.11.3.18	關申報。 ⑮在營業廳以外場所之自動化服務機器是否有適當之安全措施？	
3.11.3.19	⑯是否設置二十四小時客戶申訴服務專線，並揭示於自動化服務機器設置地點，受理客戶因使用自動化服務機器出現異常交易之申訴事件？	自動化服務機器（ATM）跨行金融交易糾紛處理要點。
3.11.3.20	⑰金融機構辦理電子銀行業務時，其交易面及安全面之安全需求及安全設計訂定之基本標準如下：	金融機構辦理電子銀行業務安全控管作業基準。
3.11.3.20.1	I 交易面之安全需求及安全設計是否符合：訊息隱密性、訊息完整性、訊息來源辨識性、訊息不可重覆性、無法	

六、內部管理

項目編號	查核事項	法令規章
3.11.3.20.2	否認傳送訊息及無法否認接受訊息。 II 管理面之安全須求及安全設計是否符合：建立安全防護策略、提高系統可靠性措施及制定作業管理規範。	
3.11.3.21	㉑ 金融機構自動化服務設備增加代售各種票證等功能免再逐案申請。	財政部 91.5.14 台財融(二)字第 0912000654 號函「金融機構自動化服務設備增加代售各種票證等功能免再逐案申請」。
3.11.3.22	㉒ 採購無障礙 ATM 時，是否以採購國際無障礙規格之 ATM 為原則及視障 ATM 是否增加操作畫面遮蔽功能。	銀行局 101 年 10 月 15 日銀局(國)字第 10100313940 號函發布起適用金融友善措施。
3.11.3.23	㉓ 新設及汰換無障礙 ATM 最高按鍵以 120 公分為上限及 ATM 機型符合輪椅使用需求若有墊高是	本會 101 年 6 月 7 日金管銀國字第 10120003370 號函發布起適用。

六、內部管理

項目編號	查核事項	法令規章
3.11.3.24	否列為優先改善標的。 24 採購無障礙 ATM 時，是否注意螢幕仰角及取鈔口位置深度，且裝置前是否從輪椅民眾需求角度思考適合設置地點。	本會 102 年 8 月 13 日金管銀國字第 10220003590 號函發布起適用。
3.11.3.25	25 增設及遷移分社時，是否於營業場所設置無障礙設施、設置無障礙服務櫃檯、服務鈴及引導專員且號碼機高度是否符合輪椅者需求。	1. 本會 102 年 6 月 28 日金管銀國字第 10220002840 號函發布起適用。 2. 本會 101 年 6 月 7 日金管銀國字第 10120003370 號函發布起適用。 3. 本會 101 年 6 月 18 日金管銀國字第 10200152790 號函發布起適用。
3.12	12. 辦理電子銀行業務	
3.12.1	(1)各項電子銀行業務（如電話銀行、行動銀行、網路銀行等）是否均依相關規定申請並經主管機關核准後始辦理？	
3.12.2	(2)是否建立良好的安全控管	金融機構辦理電子銀行業務安全控管作業基準。

六、內部管理

項目編號	查核事項	法令規章
3.12.3	作業基準？ (3)向主管機關申請核准經營「個人網路銀行業務服務」者，是否依中央主管機關訂定之「個人網路銀行業務服務定型化契約範本」之精神訂定契約，並於不違反相關法令規定及該範本精神下，得斟酌修改文字或增訂適當條款，並應配合辦理本範本之推廣及教育宣導工作。	「個人網路銀行業務服務定型化契約範本」。
3.12.4	(4)是否已依金融機構規模大小、性質、業務範圍對上述電子銀行業務訂定並執行安全政策（如：系統安全責任之劃分、網路及資料存取控制政策、防火牆政策、加密程序管理政策及控制、防毒軟體之使用政策）？前開安全政策是	金融機構辦理電子銀行業務安全控管作業基準。

六、內部管理

項目編號	查核事項	法令規章
3.12.5	否定期檢討、修訂，以符實際運作之需？ (5)有關電子銀行交易、付款服務及清算程序，與參加單位之間的協定是否註明未收取款項、清算、備份、或有事項、客戶服務及災害復原等事項之處理程序？	金融機構辦理電子銀行業務安全控管作業基準。
3.12.6	(6)與電子銀行有關之硬體、軟體及通訊設備（如：網路伺服器、防火牆....等）有無設置獨立空間，並建置適當之門禁管制？有否指定專責單位（人員）監管？	
3.12.7	(7)網路銀行網站是否已清楚列示各項資訊供消費者參考，以維護消費者之權益（如：投保存款保險及未列入承保範圍之金融產品、與	

六、內部管理

項目編號	查核事項	法令規章
3.12.8	網路銀行產品相關之真實性及隱密性之聲明、消費者最後一次退出網路銀行網站之時間...等?) (8)是否明訂與客戶、協力廠商或其他第三者(如:認證機構、結算機構、商家)等之權利義務關係契約?	
3.12.9	(9)電子銀行系統密碼管理程序是否適當?簽發密碼予客戶時相關控制及安全措施是否適當?	
3.12.10	(10)密碼設定之相關限制是否適當?如:	
3.12.10.1	①是否規定需設定為文數字之密碼?	
3.12.10.2	②是否規定密碼最少字數?	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
3.12.10.3	③是否設定密碼之有效期限？	金融機構辦理電子銀行業務安全控管作業基準。
3.12.10.4	④密碼是否以亂碼方式儲存？	
3.12.10.5	⑤是否設定密碼輸入錯誤失敗次數之控制？	
3.12.10.6	⑥是否強迫第一次登錄時須變更密碼？	
3.12.10.7	⑦須重新設定密碼時，其程序是否適當？	
3.12.11	(11)是否設定自動斷線（Time Out）機制，其作業程序是否妥適？	
3.12.12	(12)使用之加密技術是否符合「金融機構辦理電子銀行業務安全控管作業基準」？如：	

六、內部管理

項目編號	查核事項	法令規章
3.12.12.1	①加密技術使用之演算法的型態及演算法則是否符合規定？	
3.12.12.2	②是否使用特有或不知名之演算法？	
3.12.12.3	③加密鍵值之長度是否符合規定？	
3.12.12.4	④重要資料是否以加密方式儲存？	
3.12.13	(13)交易類別之安全設計是否符合規定？	金融機構辦理電子銀行業務安全控管作業基準。
3.12.14	(14)對電子憑證之申請、掛失及註銷是否訂定適當之作業程序及規範？	
3.12.15	(15)若自行管理數位簽章及認證，是否有足以供確認交易記錄和稽核功能管	金融機構辦理電子銀行業務安全控管作業基準。

六、內部管理

項目編號	查核事項	法令規章
3.12.16	理之記錄系統（即時間戳記-time stamping）？	
3.12.16.1	(16)認證（CA）機制是否適當管制，如：	
3.12.16.2	①對伺服器儲存之認證資訊及目錄是否適當保護？	
3.12.16.3	②當系統失靈或損壞時，緊急應變計畫是否足以因應？	
3.12.16.4	③是否宣告認證（CA）機制之適法性？	
3.12.16.5	④認證（CA）機制是否遵守相關標準（例如，NIST、IETF）？ 認證（CA）機制是否建立適當之稽核程序？	
3.12.16.5	⑤認證機制是否建立相關之限制？如：交易的數量、	

六、內部管理

項目編號	查核事項	法令規章
3.12.17	交易的型態、及有效日期等。 (17)若認證(CA)係委外辦理，是否已確認該認證機構之營運及作業控制機制均符合相關規範？	金融機構辦理電子銀行業務安全控管作業基準。
3.12.18	(18)電子(網路)銀行應用系統是否備有操作手冊(含內部人員及客戶端使用手冊)？是否隨時更新並供使用人員抽換？	
3.12.19	(19)電子(網路)銀行若係依賴網路服務廠商(ISP)建置其網路銀行業務，其對廠商之管理性監督是否包括下列項目：	
3.12.19.1	①網路服務廠商是否監控電子銀行線路？無法連線時是否通報銀行知悉？	

六、內部管理

項目編號	查核事項	法令規章
3.12.19.2	②網路服務廠商是否建立緊急應變計畫及災害復原程序？ 檢視網路服務廠商是否有足夠之支援人力？	
3.12.19.3	③受檢單位是否因受制於廠商支援能力而無法提供不同存取型態之服務？	
3.12.19.4	④是否由受檢單位自行定義或建立其防火牆參數？	
3.12.19.5	⑤網路服務廠商對銀行網際網路網址的變更有無適當之控管措施？	
3.12.19.6	⑥網路服務廠商之財務狀況是否健全？	
3.12.19.7	⑦網路服務廠商之安全管制情形是否適當？	

六、內部管理

項目編號	查核事項	法令規章
3.12.19.8	⑧當主要的網路服務廠商因網路失效或不適當之容量致無法處理時，有無替代方案？	
3.12.20	(20)辦理網路銀行業務，與存戶簽訂之契約是否符合維護消費者權益之規定。	「個人網路銀行業務服務定型化契約應記載事項」及「個人網路銀行業務服務定型化契約不得記載事項」。
4	(四)消費者保護教育及宣導	
4.1	1. 理事會與高階管理階層是否制定相關規範並定期監督	
4.1.1	(1)總社是否訂定消費者保護方針？	
4.1.2	(2)對新商品開發相關政策與作業規範有無妥適審核？審核要項中有無妥適納入消費者保護與法令遵循？	
4.1.3	(3)客戶紛爭之處理	「銀行業公司治理實務守則」。
4.1.3.1	①是否建立消費爭議處理制度（含處理流程	
		1. 金融消費者保護法第 13 條。 2. 104.5.25 金管法字第 1040054727 號函。 3. 本會 111.5.12 金管法字第 1110192104 號函修

六、內部管理

項目編號	查核事項	法令規章
4.1.3.2	SOP)，內容是否符合規定？ ②是否建置申訴專線及消費者服務專線？申訴部門與專線有無刊載於相關刊物及網站？	正「金融服務業公平待客原則」。 4. 信託業應負之義務及相關行為規範第 47 條。 5. 信用卡業務機構管理辦法第 52 條。 6. 「金融機構辦理現金卡業務應注意事項」第 15 條。
4.1.3.3	③處理客戶申訴是否妥當並符合內部規範？	
4.1.3.4	④是否按月統計客訴總件數、案件類別、處理績效，分析造成客訴之成因並謀求改善？	
4.2	2. 是否加強員工對消費者保護之知識及專業智能，以強化員工消費者保護觀念？(檢查時應適時對受檢單位加強宣導消費者保護業務之知識。)	
4.3	3. 查核對提供消費者相關產品之	1. 金融控股公司及銀行業內部控制及稽核制度

六、內部管理

項目編號	查核事項	法令規章
4.3.1	認識客戶（Know Your Customer, KYC）作業、風險告知及廣告揭露等是否訂定相關政策、規範及執行情形，落實客戶選擇作業？ (1)銷售商品是否善盡金融風險告知義務，確保消費者權益？	實施辦法第 12 條。 2. 金融消費者保護法第 8 條至第 10 條。
4.3.2	(2)以網際網路或電子資料交換方式使用信用卡消費或交易服務者，是否有簽訂約定，確實告知消費者利用網路消費之風險，並提醒消費者不可任意將信用卡相關資料登錄於網站或告知他人，及以正確網址進入交易網站，避免透過不明網路連結進入？	
4.3.3	(3)與消費者簽訂各項定型化契約時，是否預先約定限制或免除對消費者之責	1. 本會 100.1.13 金管銀合字第 09900422460 號函「為保護消費者權益，並兼顧市場公平競爭，有關金融服務費用之收取，應合理、公開、

六、內部管理

項目編號	查核事項	法令規章
	任?應記載及不得記載事項,是否符合規範?是否提供合理審閱期間?金融服務業對自然人或法人未符合金融消費者保護法第4條所定之條件,是否有協助其創造符合形式上之外觀條件者?	透明」。 2. 金融消費者保護法第6條至第7條。 3. 活期(儲蓄)存款契約附屬金融卡定型化契約應記載事項、不得記載事項與「活期(儲蓄)存款契約附屬金融卡定型化契約範本(信用合作社適用)。 4. 個人網路銀行業務服務定型化契約應記載事項、不得記載事項與「個人網路銀行業務服務定型化契約範本」。 5. 個人購屋貸款定型化契約應記載事項、不得記載事項與「個人購屋貸款定型化契約範本」。 6. 個人購車貸款定型化契約應記載事項、不得記載事項與「個人購車貸款定型化契約範本」。 7. 消費性無擔保貸款定型化契約應記載事項、不得記載事項與「消費性無擔保貸款定型化契約範本」。 8. 金融機構保管箱出租定型化契約應記載及不得記載事項與「金融機構保管箱出租定型化契約範本」。 9. 信用卡定型化契約應記載及不得記載事項與「信用卡定型化契約範本」。 10. 金融消費者保護法第6條及第7條。 11. 金融消費者保護法第4條。

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
4.3.4	(4)金融機構財務、業務資訊是否揭露？內容是否妥適？	「信用合作社年報應行記載事項準則」。
4.3.4.1	①信用合作社最近二年度財務報告曾出現稅後虧損者，應於年報揭露個別理事、監事及總經理之酬金。	「信用合作社年報應行記載事項準則」。
4.3.4.2	②考量信用合作社財務狀況，全體理事、監事領取酬金占稅後淨利超過百分之十五，且個別理事或監事領取酬金超過五百萬元者，應於年報揭露該個別理事或監事酬金。	「信用合作社年報應行記載事項準則」。
4.3.5	(5)手續費與其他費用收取之遵循法令規定與契約規範，是否均於契約中以明顯字體充分揭露，以利消費者瞭解？	1. 本會 104.8.4 金管檢地字第 1040156142 號函。 2. 銀行業暨保險業辦理消費者信用交易廣告應揭示總費用範圍及年百分率計算方式標準。 3. 本會 103.8.5 金管銀合字第 10330002771 號函。
4.3.6	(6)廣告內容有無虛偽、詐	金融消費者保護法第 8 條。

六、內部管理

項目編號	查核事項	法令規章
4.3.7	欺、隱匿或其他足致他人誤信之情事？是否確保其廣告內容之真實？對金融消費者所負擔之義務是否低於廣告之內容及進行業務招攬或營業促銷活動時對金融消費者所提示之資料或說明？ (7)金融機構應於平面及動態媒體廣告、開卡文件及申請書中加註民眾易懂之警語。	本會 96.5.22 金管銀（四）字第 09640002910 號函「金融機構辦理現金卡業務應注意事項」。
4.3.8	(8)各類廣告、金融商品標示與管理是否合理？其金融商品之文宣廣告是否有誇大不實情事？	1. 金融消費者保護法第 8 條。 2. 金融服務業從事廣告業務招攬及營業促銷活動辦法。
4.3.9 4.3.9.1	(9)金融商品之廣告文宣 ①是否訂定廣告、業務招攬及宣傳資料製作之管理規範，及散發公布之	1. 金融服務業從事廣告業務招攬及營業促銷活動辦法第 4、5 及 6 條。 2. 信託業營運範圍受益權轉讓限制風險揭露及行銷訂約管理辦法第 20 條及 21 條。

六、內部管理

項目編號	查核事項	法令規章
4.3.9.2	控管作業程序？廣告或宣傳資料是否均經部門主管、法務主管及法令遵循主管，確認內容無不當或不實陳述及違法情事？ ②非屬辦理信託或財富管理業務之櫃檯是否有置放相關商品說明書等資料？是否有主動對一般大眾就特定投資標的進行廣告、業務招攬及營業促銷活動？對已簽訂信託契約之客戶，得就特定投資標的以當面洽談、電話或電子郵件聯繫、寄發商品說明書之方式進行推介，惟是否不包含教育程度為國中畢業以下或有全民健康保險重大傷病證明之非專業投資人？	3. 信用卡業務機構管理辦法第 18 及 20 條。 4. 信託業從事廣告、業務招攬及營業促銷活動應遵循事項。

六、內部管理

項目編號	查核事項	法令規章
4.3.9.3	③從事廣告、業務招攬及營業促銷活動之內容或作法是否符合規定？	
4.3.10	(10)金融商品廣告文宣、約定書、申請書、公開說明書、商品說明書、風險預告書及客戶須知之揭示內容是否妥適，如：	1. 金融消費者保護法第 10 條。 2. 金融服務業提供金融商品或服務前說明契約重要內容及揭露風險辦法第 3 條及第 5~9 條。 3. 本會 100.12.12 金管法字第 10000707321 號令訂定「金融服務業從事廣告業務招攬及營業促銷活動辦法」第 3、4、5、6 條。
4.3.10.1	①廣告文宣資料之製作原則及揭露事項與內容是否符合規定？	4. 中華民國信託業商業同業公會 114.7.9 修正「中華民國信託業商業同業公會會員辦理信託業務之信託報酬及風險揭露應遵循事項」第 18 條。
4.3.10.2	②約定書、申請書、公開說明書、商品說明書、風險預告書及客戶須知之揭示內容及方式是否符合規定？	
4.3.10.3	③個別產品說明書或特定約定條款是否依規定充分揭露銀行收取之費用，或自交易對手取得之報酬？	

六、內部管理

項目編號	查核事項	法令規章
4.3.10.4	④向金融消費者說明重要內容及揭露風險時，是否留存相關資料？	金融機構作業委託他人處理內部作業制度及程序辦法。
4.4	4. 金融機構將作業委外辦理時，是否有落實告知消費者，並於網站上公告？	
4.5	5. 金融機構是否於其網站建立消費者服務區？是否加強消費者保護教育觀念及提供相關之訊息，並充實各項消費資(警)訊？	
4.6	6. 金融機構委外，是否就客戶權益保障訂定內部作業及程序，其內容包括：	
4.6.1	(1)作業委外如涉及客戶資訊，是否於契約簽訂時訂定告知客戶條款；其未訂有告知條款者，金融機構是否有書面通知委外事項，並應依個人資料保護法之規定辦	

六、內部管理

項目編號	查核事項	法令規章
4.6.2	理。 (2)是否包括客戶資訊提供之條件範圍及其移轉之程序方法。	金融機構作業委託他人處理內部作業制度及程序辦法。
4.6.3	(3)是否包括對受委託機構使用、處理、控管前款客戶資訊之監督方法。	
4.6.4	(4)是否有訂定客戶糾紛處理程序及時限，並設置協調處理單位，受理客戶之申訴。	
4.6.5	(5)受委託機構是否定期或隨時向金融機構回報債權催收處理、客戶申訴處理等情形；受委託機構及員工於內部管理或催收作業等有違反法規之情形時，是否將相關案情立即回報金融機構。	
4.7	7.不良債權催理作業是否符合相	

六、內部管理

項目編號	查核事項	法令規章
4.7.1	關法令規範？ (1)金融機構辦理應收債權催收作業之委外，是否注意受催收債務人或第三人申訴情形，並定期、適時向財團法人金融聯合徵信中心所建置受委託機構暨員工登錄系統查詢相關資料，如有達依委外契約規定受委託機構是否解聘不適任員工標準，及金融機構應終止與受委託機構契約之重大事由時，有否依本辦法及委外契約規定辦理。	金融機構作業委託他人處理內部作業制度及程序辦法。
4.7.2	(2)金融機構出售不良債權，除應依「金融機構出售不良債權應注意事項」辦理外，是否依本會 102.7.31 金管銀合字第 10230002420 號函規定辦理？	本會 102.7.31 金管銀合字第 10230002420 號函。
4.7.3	(3)對買入已出售債權機	

六、內部管理

項目編號	查核事項	法令規章
4.8	構，催理作業是否符合法令規定定期審視，以作為日後是否再度出售債權與此機構之依據？	
4.8.1	8. 查核金融機構對個人資料保護相關政策、作業規範及其執行情形是否妥適？ (1) 客戶個人資料保密相關政策與作業規範之制訂，實際作業是否有違反法令規定與內規之情形？	
4.8.1.1	① 查詢金融聯合徵信中心資料是否有依規徵取當事人同意書辦理？	「個人資料保護法」。
4.8.1.2	② 辦理作業委外處理時，是否有遵照「金融機構作業委託他人處理內部作業制度及程序辦法」暨相關法令規定，落實客戶資料保密管理？並督導委外作	「金融機構作業委託他人處理內部作業制度及程序辦法」。

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
4.8.1.3	業之受託機構，落實客戶資料保護情形？ ③對於授權銀行業者交叉使用個人資料部分，是否提供充分之選擇權供客戶勾選？	
4.8.1.4	④銀行履行個人資料保護法第 8 條之告知義務時：	本會 101.10.24 金管銀合字第 10130002690 號函。
4.8.1.4.1	I 其告知書內容是否過於概括。	
4.8.1.4.2	II 告知書與同意書是否未明顯區隔。	
4.8.1.4.3	III 於客戶不同意其蒐集個人資料，或因業務往來關係終止等因素要求刪除其個人資料時，是否建立內部標準作業流程，並於作業完成時，告知當事人。	

六、內部管理

項目編號	查核事項	法令規章
4.8.1.4.4	IV是否將個資法之執行事項，列入內部控制及稽核項目。	
4.8.2	(2)內部稽核是否將客戶資料保密作業列為查核重點及實際查核之情形？內部稽核報告內容有無揭露員工保密教育及客戶資料保密管理項目。	「金融控股公司及銀行業內部控制及稽核制度實施辦法」。 本會106.1.10金管銀外字第10650000070號函。 「金融機構作業委託他人處理內部作業制度及程序辦法」相關問題適用解說問答集—現鈔運送作業範圍。
4.8.3	(3)銀行業者在運用客戶生物識別資料時，內部作業及資料之保存是否有嚴謹之控管程序？取得及利用客戶生物特徵資料前，是否取得客戶同意並留存客戶同意之紀錄？	
4.8.4	(4)辦理「現金運送作業」委外之範圍是否符合規定？是否除一般運鈔作業外，並未包括委託保全業者自行辦理行外代收	

六、內部管理

項目編號	查核事項	法令規章
4.9	付，而未由金融機構從業人員辦理？ 9. 是否落實執行「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」之相關規定，如有尚未完成之應辦事項，是否儘速完成，並列為內部稽核追蹤事項？	1. 「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」。 2. 本會銀行局 103.6.26 銀局（合）字第 10300144610 號函。
4.9.1	(1) 是否依其業務規模及特性，衡酌經營資源之合理分配，配置管理之人員及相關資源，以規劃、訂定、修正與執行其個人資料檔案安全維護計畫、業務終止後個人資料處理方法、資安事故應變、通報及預防機制、員工教育訓練、設備安全及資安措施等內部規範。	
4.9.2	(2) 有無依個人資料保護相關法令，定期查核確認所保有之個人資料現況、評估可產生之風險、訂定適當	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
4.9.3	之管理機制及列入內部控制及稽核項目。 (3)是否設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員設定保密義務。	
4.10	10. 透過電話行銷金融商品是否進行電話全程(係指認定接聽電話之人即為其欲進行推廣商品或服務爭取交易機會之對象時，至結束所進行之通話)錄音並留存紀錄?是否未以積極欺瞞或消極隱匿交易資訊，爭取交易機會?	1. 本會 100.8.24 金管銀票字第 10000227711 號函。 2. 本會 105.9.21 金管銀法字第 1050054766 號書函。
4.11	11. 遞延(預付)型商品或服務無法提供如屬社會重大案件，受理申請停止繼續付款，是否免除由消費者個別提供存證信函?是否依商品或服務提供之比例計算消費者應支付不足之款項及應退還消費者溢繳之款	本會 106.5.19 金管銀合字第 10600009800 號函。

六、內部管理

項目編號	查核事項	法令規章
4.12	項？ 12. 金融機構將自聯徵中心所查得客戶之信用資料，是否未利用於「授信目的」範圍外之行銷運用？	本會111.3.16金管銀國字第11002733091號函。
5	(五)資訊作業制度	
5.1	1. 資訊安全政策、內部組織及資產管理	信用合作社資通安全防護基準第3條
5.1.1	(1) 資訊安全政策是否經理事會決議或經其授權之經理部門核定？	
5.1.2	(2) 資訊安全相關要求是否對所有員工及供應商公布或傳達？	
5.1.3	(3) 是否訂定資訊作業相關管理及操作規範，經理事會通過後實施，修正時亦同？	
5.1.4	(4) 是否每年檢討資訊安全政策及前款管理及操作規範，並於發生重大變更（如新頒布法令法規）時審查，以持續	

六、內部管理

項目編號	查核事項	法令規章
5.1.5	確保其合宜性、適切性及有效性？ (5)是否依據作業流程，識別人員、表單、設備、軟體、系統等資產，建立資產清冊、網路架構圖、組織架構圖及負責人，並定期清點以維持其正確性？	
5.1.6	(6)是否定義人員角色及責任並區隔相互衝突的角色？	
5.1.7	(7)是否依據作業風險及專業能力選擇適當人員擔任其角色並定期提供必要教育訓練？	
5.1.7.1	①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？	
5.1.7.2	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，是否有擔任同一項工作（如維護同一項系統）時間過長情形？	

六、內部管理

項目編號	查核事項	法令規章
5.1.7.3	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，取消其使用者代號、密碼並收繳其通行證、卡及相關證件？	
5.1.7.4	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？	
5.1.7.5	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？	
5.1.7.6	⑥是否訂有年度教育訓練計畫並編列預算？教育訓練計畫之擬定及實施是否切合需要？	
5.1.7.7	⑦各級人員是否有充分的在職訓練？是否訂有員工交叉訓練計畫，以期至少有兩人可執行相同的工作互為支援？	
5.1.7.8	⑧資訊安全之人力與訓練及管理作業是否依「金融控股公司及銀行業內部控制及稽核制	
		本會 111.7.26 金管銀合字第 11102102331 號令。

六、內部管理

項目編號	查核事項	法令規章
5.1.7.8.1	度實施辦法」第 24 條第 1 項但書所稱主管機關對信用合作社辦理資訊安全相關規定辦理，如： I 是否指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。但屬有限責任中華民國信用合作社聯合社南區聯合資訊中心之會員社，得指派經理以上或職責相當之人兼任？	
5.1.7.8.2	II 信用合作社是否依下列規定設置適當資訊安全人力資源：	
5.1.7.8.2.1	A. 上一會計年度決算後淨值達新臺幣 30 億元以上或放款總餘額達新臺幣 200 億元以上者，是否設置資訊安全主管及資訊安全人員？	
5.1.7.8.2.2	B. 未達上述規模者，是否設置至少 1 名資訊安全人	

六、內部管理

項目編號	查核事項	法令規章
5.1.7.8.3	員？ Ⅲ前點資訊安全主管及資訊安全人員除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。	
5.1.7.8.4	Ⅳ信用合作社資訊安全主管或資訊安全人員負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情形，依金融控股公司及銀行業內部控制及稽核制度實施辦法第8條第1項規定辦理內部控制制度聲明書之出具、揭露及公告申報，並由資訊安全長聯名出具。	
5.1.7.8.5	Ⅴ信用合作社資訊安全主管及資訊安全人員，每年應至少接受15小時以上資訊安全專業課程訓練或職能訓練。總社資訊單位、財務保管單位及其他管理單位之人員，每年至少須接受3小	

六、內部管理

項目編號	查核事項	法令規章
5.1.7.8.6	時以上資訊安全宣導課程。 VI第一點有關配置資訊安全 長之規定，信用合作社應於 本令生效日後九個月內調 整至符合規定。信用合作社 應於符合第二點適用條件 起六個月內調整。	
5.2	2.實體安全管理	
5.2.1	(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？	
5.2.1.1	①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？	
5.2.1.2	②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？	

六、內部管理

項目編號	查核事項	法令規章
5.2.1.3	③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？	
5.2.1.4	④有無裝置火災自動警報系統？或自動滅火設備？	
5.2.1.5	⑤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？	
5.2.1.6	⑥保險及維護契約涵蓋範圍是否完全？並在有效期間內？	
5.2.1.7	⑦對處理個人資料檔案之主機（含測試或發展用之主機）、週邊設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？	

六、內部管理

項目編號	查核事項	法令規章
5.2.1.8	⑧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？	
5.2.2	(2)是否建立機房門禁管制，並將營運設備集中於機房內，以確保僅允許經授權人員進出？非授權人員進出是否填寫進出登記，並由內部人員陪同及監督？進出登記紀錄是否定期審查，如有異常應適當處置？	
5.2.3	(3)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？	
5.2.4	(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	

六、內部管理

項目編號	查核事項	法令規章
	檢查，以確保未被竄改？	
5.2.5	(5)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？	
5.2.6	(6)自建與委外維運之電腦系統，是否依「信用合作社辦理電腦系統資訊安全評估辦法」之規定辦理評估作業？	本會107.8.3金管銀合字第10701121410號函備查之中華民國信用合作社聯合社所報「信用合作社辦理電腦系統資訊安全評估辦法」。
5.2.7	(7)對營運環境管理人員之要求，有無依下列事項辦理：	信用合作社資通安全防護基準第4條。
5.2.7.1	①建立人員之註冊、異動及撤銷註冊程序，用以配置適當之存取權限；人員離職時是否儘速移除權限。	
5.2.7.2	②列管硬體設備、應用軟體、系統軟體之最高權限帳號及具程式異動、參數變更權限之帳號。	

六、內部管理

項目編號	查核事項	法令規章
5.2.7.3	③確認人員之身分及存取權限，必要時得限定其使用之機器或網路位置(IP)。	
5.2.7.4	④人員超過 15 分鐘未操作個人電腦時，是否設定密碼啟動螢幕保護程式或登出系統？	
5.2.7.5	⑤採用固定密碼進行身分確認者是否符合下列要求：	
5.2.7.5.1	I. 訂定密碼檢核邏輯，確保密碼長度至少為 12 碼，並要求密碼複雜度。若無法達成，應執行風險評估，並採取適當的替代控制措施，以確保系統安全性。	
5.2.7.5.2	II. 提供給人員使用之帳號於使用後三個月內應變更密碼，如參考其他依據並進行相關風險評估，得考量於使用後六個月內變更密碼。	
5.2.7.5.3	III. 提供給系統使用之帳號	

六、內部管理

項目編號	查核事項	法令規章
5.2.7.6	應採取適當之管控措施（如限制人工登入、監控告警）。 ⑥加解密程式或具變更權限之公用程式（如資料庫工具程式），是否已列管並限制使用，防止未經授權存取並保留稽核軌跡。	信用合作社資通安全防護基準第 12 條。
5.2.8	(8)提供客戶使用之公用電腦，是否符合下列要求：	
5.2.8.1	①建立上網管制措施，限制連結非業務相關網站，以避免下載惡意程式。	
5.2.8.2	②建立病毒偵測機制並定期更新病毒碼或建立白名單管控機制，以避免安裝未授權程式。	
5.2.8.3	③限制可攜式儲存裝置介面存取(如 USB 埠)。	
5.2.8.4	④提醒避免瀏覽器留存客戶輸入資訊，並定期清理客戶留存資料(如帳號、cookie)。	

六、內部管理

項目編號	查核事項	法令規章
5.2.8.5	⑤如有設定重新安裝或系統還原時，應先安裝安全修補程式，並更新病毒碼或建立白名單管控機制後，再開放使用。	
5.3	3. 系統開發及維護管理	
5.3.1	(1) 系統開發管理	
5.3.1.1	①有關係統之建置、變更、測試、轉換、上線等作業，是否有訂定規範或辦法？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？	
5.3.1.2	②系統開發程序是否包括下列各步驟，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？	
5.3.1.2.1	I 系統可行性研究？	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.3.1.2.2	II 系統分析?	
5.3.1.2.3	III 系統設計?	
5.3.1.2.4	IV 程式設計?	
5.3.1.2.5	V 測試工作?	
5.3.1.2.6	VI 實施(轉換)事宜?	
5.3.1.2.7	VII 文件撰寫?	
5.3.1.2.8	VIII 系統評估?	
5.3.1.3	③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?	
5.3.1.4	④系統之開發、設計，對於個人資料之蒐集、處理及利	「個人資料保護法」第 5 條。

六、內部管理

項目編號	查核事項	法令規章
5.3.1.5	用，有無逾越金融機構特定目的之必要範圍或有無妨害當事人之權益？ ⑤若涉及個人資料檔案之應用，其程式之設計及管理有無妥善規劃，以防止資料遭不當使用？測試用之機敏資料，是否先進行資料遮蔽處理或管制保護？	
5.3.1.6	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？測試環境是否符合下列要求：	
5.3.1.6.1	I 是否評估並辦理：	
5.3.1.6.1.1	A. 應建立病毒偵測機制並定期更新病毒碼或建立白名單管控機制，以避免	

六、內部管理

項目編號	查核事項	法令規章
5.3.1.6.1.2	安裝未授權程式。 B. 應隨時掌握資安事件，針對高風險或重要項目立即進行清查及應變。	信用合作社資通安全防護基準第 11 條。
5.3.1.6.1.3	C. 應定期進行弱點掃描，並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，填寫評估結果及處理情形，採取適當措施並確保作業系統及軟體安裝經測試且無弱點顧慮之安全修補程式。	
5.3.1.6.1.4	D. 應避免採用已停止弱點修補或更新之系統軟體及應用軟體，如有必要應採用必要防護措施。	
5.3.1.6.2	II 是否避免同時共用不同環境(如營運環境、測試環境、辦公環境)之設備、憑證金鑰、資源存取帳密及使用 者 配 置 檔 (User Profiles)?	

六、內部管理

項目編號	查核事項	法令規章
5.3.1.6.3	Ⅲ 是否限制連接網際網路？ 如有需要是否遵循銀行公會所訂定之相關電子銀行相關自律規範辦理？	
5.3.1.7	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？	
5.3.1.8	⑧實施系統上線，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？	
5.3.1.9	⑨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？	

六、內部管理

項目編號	查核事項	法令規章
5.3.1.9.1	I 業務電腦化後，操作、管理與查核上尚待加強、改進者？	信用合作社資通安全防護基準第 15 條。
5.3.1.9.2	II 系統內部控制功能之完整性？	
5.3.1.9.3	III 程式、檔案設計修改頻率與主要修改原因之分析？	
5.3.1.9.4	IV 輸出資料、報表之實用性、完整性？	
5.3.1.10	⑩ 核心資通系統與第一類電腦系統中個人網路銀行、企業網路銀行、行動銀行、ATM 自動化服務及分行櫃台之系統轉換、架構重大調整或跨版本升級前，是否符合下列要求：	
5.3.1.10.1	I. 系統轉換前之準備工作：	
5.3.1.10.1.1	甲、轉換前關鍵準備工作，	

六、內部管理

項目編號	查核事項	法令規章
5.3.1.10.1.2	如：架構審查、上線變更審查及風險評估、上線協調會議等具資安控制性之事項，並有資安(主管)人員參與，以及由資安長發揮統籌資安政策推動與資源調度之工作。如係委外處理者，已要求受委託機構協同委託機構之資安長及資安(主管)人員共同參與。 乙、建立架構審查機制，從 AP、DB、資安、網路、平台、營運等面向進行評估，並評估一次過版或平行運轉可行性。	
5.3.1.10.1.3	丙、檢視相關設備容量，評估營運及業務需求所需備載容量(如跨行交易平台、企業應用系統整合 EAI、企業服務匯流排 ESB 等)。另是否已建置擬真測試環境，測試新系統或	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.3.1.10.1.4	功能相容於既有營運環境之架構、設備及參數。 丁、檢視各項測試個案，依據影響範圍進行功能測試(如單元、整合、迴歸等)及非功能測試(如壓力、相容等)，並進行整體性演練。	
5.3.1.10.1.5	戊、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。	
5.3.1.10.1.6	己、進行上線變更審查及風險評估，辨識複雜度及影響範圍，檢視測試個案及上線復原計畫之完整性。	
5.3.1.10.1.7	庚、要求廠商上線支援，並能緊急提供備品、更高容量設備、問題查找及修正人力。	
5.3.1.10.1.8	辛、預留復原作業及上線驗證時間。	
5.3.1.10.1.9	壬、召開上線協調會議，安排工作項目並確保各項	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.3.1.10.1.10	準備到位。 癸、提前公告，佈署足夠客 服資源並進行教育訓練 (含異常話術)。	
5.3.1.10.2	II. 系統轉換作業：	
5.3.1.10.2.1	甲、成立指揮中心，逐步執 行上線計畫，檢視每一個 檢核點，必要時召開復原 決策會議。	
5.3.1.10.2.2	乙、執行系統及資料備份， 以因應復原時所需。	
5.3.1.10.2.3	丙、驗證各項變更作業，確 保如預期結果。	
5.3.1.10.2.4	丁、驗證各項資料內容，確 保資料完整性。	
5.3.1.10.2.5	戊、逐步啟動各項作業並監 控網路及系統，確保提供 足夠資源。	
5.3.1.10.3	III. 系統轉換後之事件管 理：	
5.3.1.10.3.1	甲、持續系統監控，確保資 料正確、功能正常、系統 穩定。	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.3.1.10.3.2	乙、落實事故應變，以消費者權益及持續營運優先處理。	
5.3.1.10.3.3	丙、成立應變小組，集中管理問題並適時調配各單位資源。	
5.3.1.10.3.4	丁、追蹤問題根因，提出短中長期改善方案並持續追蹤。	
5.3.1.11	⑪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？	
5.3.1.12	⑫第一類電腦系統上線前及針對異動程式是否至少每半年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，依據不同風險訂定適當措施及完成時間，執行矯正、記	金融機構提供自動櫃員機系統安全作業規範。 信用合作社資通安全防護基準第 10 條

六、內部管理

項目編號	查核事項	法令規章
5.3.2	錄處理情形並追蹤改善？	
5.3.2.1	(2)系統維護管理 ①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？	
5.3.2.2	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？	
5.3.2.3	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？	
5.3.2.4	④已正式實施之作業，其程式變更：	
5.3.2.4.1	I 是否均有提出書面申請，並經有關主管核准後方才修正？	

六、內部管理

項目編號	查核事項	法令規章
5.3.2.4.2	II 書面申請是否敘明變更內容及原因？	
5.3.2.4.3	III 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？	
5.3.2.4.4	IV 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。	
5.3.2.4.5	V 系統相關文件是否配合修正？	
5.3.2.4.6	VI 操作程序上如有變更是否通報有關單位？	
5.3.3	(3) 供應鏈風險管理	
5.3.3.1	① 資通系統與服務委外前，是否分析及規劃下列供應鏈資訊安全事項：	信用合作社資通系統與服務供應鏈風險管理規範第 4 條。

六、內部管理

項目編號	查核事項	法令規章
5.3.3.1.1	I 是否分析委外項目之資訊安全風險(如：可能受影響之資訊資產、流程及作業環境)與委外可行性，並依據分析結果擬訂資訊安全要求？	信用合作社資通系統與服務供應鏈風險管理規範第5條。
5.3.3.1.2	II 屬核心資通系統與第一類電腦系統之委外開發項目，以及屬第二、三類電腦系統，且供應商於契約存續期間得存取信用合作社機敏資料之委外開發項目，其專案成員是否有資訊安全人員參與？	
5.3.3.2	②選擇供應商前，是否執行下列事項：	
5.3.3.2.1	I 是否依據委外項目之性質訂定供應商需求建議書？內容是否明列供應商需符合之專業資格、資訊安全要求，以及資訊安全要求之服務水準？	
5.3.3.2.2	II 選擇供應商過程，如涉及信用合作社資訊交換，是否於資訊交換前簽署保密協議書？	

六、內部管理

項目編號	查核事項	法令規章
5.3.3.2.3	Ⅲ 是否執行安全評估以選任合適之供應商：	信用合作社資通系統與服務供應鏈風險管理規範第 6 條。
5.3.3.2.3.1	A. 是否注意作業委託供應商對信用合作社服務集中度之適度分散？如存在集中度過高之疑慮，是否依評估結果擬訂對應之風險處理措施？	
5.3.3.2.3.2	B. 是否評估供應商對所委託項目之資訊安全管理機制？	
5.3.3.2.3.3	C. 是否評估供應商與其產品或服務提供地、實質受益人或控制權來源國是否符合國內相關規範要求？	
5.3.3.3	③ 供應商之委託契約或相關文件中，是否明確約定下列事項：	
5.3.3.3.1	I 是否要求供應商遵守相關法令法規及其他適當資訊安全國際標準要求，並訂定供應商未符合資訊安全要求或服務水準時之罰責標準？	
5.3.3.3.2	II 是否定義與供應商之資訊安全權責，規範供應商應實施之	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.3.3.3.3	資訊安全要求，包含人員管理、資訊存取與傳輸安全管控機制等？ III 非經書面同意，不得將作業複委託他人，是否定義委託業務得否複委託、得複委託之範圍與對象，及複委託受託者應具備之資訊安全措施？	
5.3.3.3.4	IV 是否與供應商約定資訊安全事件應變與通報程序、資訊安全事件損害賠償責任、系統或程式定期檢測與修復要求、保固服務、異常管理等服務要求？	
5.3.3.3.5	V 是否保留對供應商之稽核權？ 若供應商發生可能影響受託業務之資通安全事件時，是否確保其本身、金融監督管理委員會及中央銀行，或其指定之人能取得供應商辦理受託業務之相關資訊，包括資通安全控管機制及相關系統之查核報告，及實地查核權力？	

六、內部管理

項目編號	查核事項	法令規章
5.3.3.3.6	VI 是否明確約定供應商應確保交付之產品及其服務組件來源為合法取得或經合法授權使用，且產品或服務提供地、實質受益人或控制權來源國符合國內相關規範要求？	
5.3.3.3.7	VII 是否要求供應商確保交付之資通系統或程式，包含供應商提供之產品及其服務組件，無惡意程式及後門程式，並取得相關安全性測試結果或供應商安全性承諾？	
5.3.3.3.8	VIII 是否依據資料之機密等級、資料處理流程與傳輸方式，要求供應商實施資料安全管控？	
5.3.3.3.9	IX 是否訂定產品或服務之交付驗收程序和標準？	
5.3.3.3.10	X 對資通系統功能需求或資訊建置要求，是否包含資訊安全要求或控制措施？	
5.3.3.3.11	XI 是否已要求契約終止時，資訊資產與資料返還、移交、刪除或銷毀之要求？	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.3.3.4	④於供應商契約存續期間，是否注意下列原則：	信用合作社資通系統與服務供應鏈風險管理規範第7條。
5.3.3.4.1	I 信用合作社與供應商是否分別指定專人，負責督導及辦理各項資訊安全要求事項？	
5.3.3.4.2	II 與供應商間如涉個人資料交換，是否確認符合我國個人資料保護法相關規定，並確保僅授權者可存取資料及保留資料使用稽核軌跡？	
5.3.3.4.3	III 是否訂定供應商存取權限管理規範，妥善管理供應商之實體與邏輯存取權限？	
5.3.3.4.4	IV 是否定期對具邏輯存取權限之供應商辦理供應鏈資訊安全風險評估，並依據供應鏈資訊安全風險評估結果採取適當之資訊安全控管措施或提報適當主管層級核准可接受之風險等級？	
5.3.3.4.5	V 是否建立對核心資通系統與第一類電腦系統供應商資訊安全稽核之程序，包含稽核結	

六、內部管理

項目編號	查核事項	法令規章
5.3.3.4.6	果之改善追蹤機制？是否依據供應鏈資訊安全風險評估結果選擇合適之資訊安全稽核之方式與頻率，包含自行辦理或委託獨立第三方執行資訊安全訪視作業，或由供應商提供公正第三方之驗證報告？ VI 是否監督供應商針對其專案執行人員辦理資訊安全教育訓練？	
5.3.3.4.7	VII 是否依契約要求審查供應商所交付之系統或程式，包含供應商提供之產品及其服務組件之安全性測試結果或供應商安全性承諾？	
5.3.3.4.8	VIII 是否依據與供應商約定各項服務要求定期審查供應鏈服務之品質及相關規範合規情形？如有違反要求情節重大且不能限期改善者，是否執行供應商退場或替換機制？	
5.3.3.5	⑤ 供應商服務變更與契約終	信用合作社資通系統與服務供應鏈風險管理規

六、內部管理

項目編號	查核事項	法令規章
5.3.3.5.1	止時，是否符合下列事項： I 供應商提供之服務變更前（包含契約變更、供應商組織重大調整、業務重大異動或契約提前終止相關事宜），是否執行供應鏈資訊安全風險評估，並依評估結果擬訂對應之風險處理措施？	範第 8 條。
5.3.3.5.2	II 供應商契約終止時，是否於供應商依約完成產品或服務之移轉、交付驗收程序後，監督其完成資訊資產與資料返還、移交、刪除或銷毀，並移除供應商於服務期間所取得之實體與邏輯存取權限？	
5.3.3.6	⑥ 系統之開發或維護外包時，對軟體開發或維護規範之訂定，軟體設計或修改之督導、核定及驗收等是否比照自行開發設計準則及控管程序辦理？	

六、內部管理

項目編號	查核事項	法令規章
5.3.4	(4)系統生命週期管理	信用合作社資通安全防護基準第14條。
5.3.4.1	①是否訂定資訊系統開發設計規範並落實執行？	
5.3.4.2	②有無監督委外開發之應用軟體，並確保其有效遵循相關規定？	
5.3.4.3	③是否已確保系統軟體和應用軟體安裝最適安全修補程式？	
5.3.4.4	④針對系統架構重大變更或異動時，是否已訂定復原程序，並於上線前進行程序演練或實際演練？	
5.3.4.5	⑤是否已分別從技術、功能、情境等建立測試案例並進行端點對端點測試？	
5.3.4.6	⑥對於測試用之機敏資料，有無先進行資料遮蔽處理或管制保護？	
5.3.4.7	⑦於開發階段起至營運階段，是否已遵循變更控制程序處理並留存相關紀錄；營運環境變更(如執行、覆核)	

六、內部管理

項目編號	查核事項	法令規章
5.3.4.8	是否由二人以上進行，以相互牽制？ ⑧系統軟硬體變更是否已先進行技術審查並測試；套裝軟體不應自行異動，是否已先進行風險評估。程式不應由開發人員自行換版或產製比對報表，且是否已建立程式原始碼管理機制，以符合職務分工及牽制原則？	
5.4	4. 運作管理	
5.4.1	(1) 主機操作管理	
5.4.1.1	① 操作人員操作管理	
5.4.1.1.1	I 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？	
5.4.1.1.2	II 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？	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.1.1.3	III 是否有明訂操作人員可使用之指令清單？	
5.4.1.1.4	IV 操作人員所輸入指令，是否都留下系統記錄(Log)？並由其他人員負責核驗？	
5.4.1.1.5	V 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？	
5.4.1.1.6	VI 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？	
5.4.1.2	② 批次作業管理	
5.4.1.2.1	I 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？	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.1.2.2	II 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？	
5.4.1.2.3	III 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記錄？對執行異常情形有否查核追蹤？	
5.4.1.2.4	IV 對例行性作業發生異常狀況，有無訂定處理程序？並作記錄？	
5.4.1.2.5	V 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？	

六、內部管理

項目編號	查核事項	法令規章
5.4.1.3	③作業及系統日誌功能管理	
5.4.1.3.1	I 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？	
5.4.1.3.2	II 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？	
5.4.1.3.3	III 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？	
5.4.1.3.4	IV 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	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.1.3.5	明作業之原因？ V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？	
5.4.1.4	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（如主機及週邊設備、端末機等之使用狀況、每月交易情況、系統反應時間、及軟硬體故障情形），是否定期予以統計分析與檢討改進？	
5.4.1.5	⑤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，並遵循下列程序：	
5.4.1.5.1	I 除代登系統外於登入作業系統進行系統異動或資料	信用合作社資通安全防護基準第4條。

六、內部管理

項目編號	查核事項	法令規章
5.4.1.5.2	庫存取時，是否留存人為操作紀錄，並於使用後儘速變更密碼？因故無法變更密碼者，是否建立監控機制，避免未授權變更，並於使用後覆核其操作紀錄？ II 帳號是否採一人一號管理，避免多人共用同一個帳號為原則？如有共用需求，申請及使用是否有其他補強管控方式（如使用後更換密碼、代登入機制、密碼拆分保管等）？是否留存操作紀錄？是否能區分人員身分？	
5.4.1.5.3	III 最高權限帳號使用時是否先取得權責主管或授權人員同意並保留稽核軌跡？	
5.4.1.5.4	IV 具最高權限帳號、特殊功能（如程式或軟體異動、參數或組態變更權限等）權限帳號是否和日常維運用帳	

六、內部管理

項目編號	查核事項	法令規章
5.4.1.5.5	號區隔，並定期抽查使用結果，以防範未經授權使用？如為核心資通系統，是否於該等帳號被使用時，每日覆核使用結果？ V 提供網際網路服務之伺服器及 AD(網域服務)主機，對於最高權限帳號及特殊功能權限帳號，是否採雙因子認證？	信用合作社資通安全防護基準第 4 條。
5.4.1.5.6	VI 是否針對核心資通系統、第一類及第二類電腦系統依最小權限 (least privilege) 及僅知原則 (need-to-know) 配發權限予人員使用並定期審查帳號及權限之合理性，以符合職務分工及牽制原則？	
5.4.2	(2) 中心端末機使用管理	
5.4.2.1	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	

六、內部管理

項目編號	查核事項	法令規章
5.4.2.2	章以明責任？登記簿是否與電腦使用人員資料檔內容相符？ ② 端末機使用人員資料（如使用者代號、密碼、授權使用範圍等資料）之建檔、變更、註銷是否經申請、核准程序並留存紀錄？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？	
5.4.2.3	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？	
5.4.2.4	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	

六、內部管理

項目編號	查核事項	法令規章
5.4.2.5	形？ 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？	
5.4.2.6	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？	
5.4.3	(3)輸入、輸出資料管制	
5.4.3.1	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	

六、內部管理

項目編號	查核事項	法令規章
5.4.3.2	施？以確保輸入資料之正確性及合法性？ 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？	
5.4.3.3	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，俾期各種輸出資料適時送達使用單位？	
5.4.3.4	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？	
5.4.3.5	⑤個人資料檔案安全維護管	
	1.「金融監督管理委員會指定非公務機關個人資	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.3.5.1	理 I 為維護所保有個人資料之安全，是否已採取下列資料安全管理措施	料檔案安全維護辦法」。 2.信用合作社資通安全防護基準第5條。
5.4.3.5.1.1	A 訂定各類設備或儲存媒體之使用規範，及報廢或轉作他用時，採取防範資料洩漏之適當措施。	
5.4.3.5.1.2	B 針對所保有之個人資料內容，有加密之需要者，於蒐集、處理或利用時，採取適當之加密措施。	
5.4.3.5.1.3	C 作業過程有備份個人資料之需要時，對備份資料予以適當保護。	
5.4.3.5.2	II 保有個人資料存在於紙本、磁碟、磁帶、光碟片、微縮片、積體電路晶片、	信用合作社資通安全防護基準第5條。

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.3.5.2.1	電腦、自動化機器設備或其他媒介物者，是否採取下列設備安全管理措施：	
5.4.3.5.2.2	A. 實施適宜之存取管制。	
5.4.3.5.2.3	B. 訂定妥善保管媒介物之方式。	
	C. 依媒介物之特性及其環境，建置適當之保護設備或技術。	
5.4.3.5.3	Ⅲ對客戶應注意以確保其權益及維護其資訊安全、隱密性等有關事項；或為維護系統安全客戶應配合事項，是否以書面或其他適當方式表達，善盡告知之責任？	
5.4.3.5.4	Ⅳ有無定期或不定期對個人資料檔案實施資料安全防護教育訓練及其他必要措施？	

六、內部管理

項目編號	查核事項	法令規章
5.4.3.5.5	V 是否依執行業務之必要，設定相關人員接觸個人資料之權限及控管其接觸情形，並與所屬人員約定保密義務。	信用合作社資通安全防護基準第 5 條。
5.4.3.5.6	VI 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及控管機制，並定期進行清查及留存相關作業紀錄？並對核心資通系統及各類電腦系統確認所保有之個人資料進行風險評估及控管。	
5.4.3.5.7	VII 存放於測試主機資料庫內之個資是否建立妥適之去識別化或加密處理機制？存放於電腦（包括伺服器及個人電腦）內之個資是否建立妥適之管理機制？	
5.4.3.5.8	VIII 對傳遞個資是否建立妥適	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.3.5.9	之加密及管理機制(含洗錢防制大額通報作業流程控制設計及辦理情形)?	
5.4.3.5.10	IX 對行動碟、光碟、磁帶等移動式儲存媒體，及對FTP、網路芳鄰、電子郵件等傳檔功能之應用程式，是否建立使用管理機制？	
5.4.3.5.11	X 建立資料外洩防護機制，管制個人資料檔案透過輸出入裝置、通訊軟體、系統操作複製至網頁或網路檔案等方式傳輸，並留存相關紀錄、軌跡及證據。 XI 針對核心資通系統及各類電腦系統建置留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況。	信用合作社資通安全防護基準第5條。

六、內部管理

項目編號	查核事項	法令規章
5.4.3.5.12	XII 刪除、停止處理或利用所保有之個人資料後，是否留存下列紀錄：	
5.4.3.5.12.1	A. 刪除、停止處理或利用之方法、時間。	
5.4.3.5.12.2	B. 將刪除、停止處理或利用之個人資料移轉其他對象者，其移轉之原因、對象、方法、時間，及該對象蒐集、處理或利用之合法依據。	
5.4.3.6	⑥有機敏資料儲存於使用者端操作環境、機敏資料於網際網路上傳輸、使用者身分確認資料（如固定密碼、設備資訊、生物特徵）儲存於系統內等情形者，是否建立隱密性機制？	
5.4.4	(4)程式、資料檔案管理	
5.4.4.1	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	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.4.2	請、核可及覆核程序，並留存紀錄？ ②正式作業程式館內程式之新增、刪除、修改，電腦系統是否留有記錄，並定期列印查核？是否有防備未經授權者使用程式館措施（制度、系統控制）？	
5.4.4.3	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？	
5.4.4.4	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？	
5.4.4.5	⑤在特殊情況下，對正式作業	

六、內部管理

項目編號	查核事項	法令規章
5.4.4.6	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？ 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？	
5.4.4.7	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？	
5.4.4.8	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？	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.4.9	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？	
5.4.4.10	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？	
5.4.5	(5)媒體管理	
5.4.5.1	①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？	
5.4.5.2	②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？	
5.4.5.3	③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	

六、內部管理

項目編號	查核事項	法令規章
5.4.5.4	查？ ④媒體新增、作廢是否經核准？媒體廢棄前是否先經銷磁或其他處理，以防儲存於媒體內之資料外洩？	
5.4.6 5.4.6.1	(6)連線作業管理 ①對營業單位連線作業之操作、設備調撥及維護、故障排除及連線作業工作日誌之填報等事項是否有專責單位或人員負責，並予以記錄？	
5.4.6.2	②連線問題管理是否列入控管，並定期追蹤處理，呈閱主管，以免影響全行系統安全或客戶權益？	
5.4.7 5.4.7.1	(7)亂碼化作業安全管理 ①為維護電腦作業亂碼系統正常運作，及確保亂碼化設	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.7.2	備及作業之安全性，是否訂定跨行亂碼系統安全控管辦法？ 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？	
5.4.7.3	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？	
5.4.7.4	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？	
5.4.7.5	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	

六、內部管理

項目編號	查核事項	法令規章
5.4.7.6	用是否經核可並留存紀錄？ 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？	
5.4.7.7	⑦各種基碼於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(LOAD)系統中執行，執行後即將程式自系統中清除？	
5.4.7.8	⑧為提昇安全層次，其亂碼化作業是否使用硬體執行？	
5.4.8	(8)網路系統安全管理	
5.4.8.1	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	1. 金融機構辦理電子銀行業務安全控管作業基準。 2. 本會 111.5.20 金管銀合字第 1100207873 號函

六、內部管理

項目編號	查核事項	法令規章
5.4.8.2	牆原則、伺服器、網路資源存取控制、分散式阻斷服務防禦、加密程序、使用者帳號維護、電子郵件及防毒軟體之使用管理)？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？	洽悉中華民國信用合作社聯合社所報「信用合作社分散式阻斷服務防禦與應變作業程序範本」。
5.4.8.2.1	②有關網路管理是否建置一適當之網路系統的安全控管機制？ I 是否區分網際網路、非武裝區 (DMZ)、營運環境及其他 (如內部辦公區) 等區域，並使用防火牆進行彼此間之存取控管？機敏資料是否僅存放於安全的網路區域，未存放於網際網路及 DMZ 等區域？對外網際網路服務是否僅透過 DMZ 進行，再由 DMZ 連線至其他網	信用合作社資通安全防護基準第 13 條。

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.8.2.2	路區域？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？ II 對未經防火牆之遠端存取是否予以過濾及管制？	
5.4.8.2.3	III 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？	
5.4.8.2.4	IV 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)？	
5.4.8.2.5	V 對未經授權或違規之異常存取或進出網站情	

六、內部管理

項目編號	查核事項	法令規章
5.4.8.2.6	形，是否設計偵測、警示及追蹤之機制？ VI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？	
5.4.8.2.7	VII是否建立病毒偵測及預防程序，並定期辦理病毒碼更新或建立白名單管控機制？對重大電腦中毒事件是否確實釐清原因及研議防制對策？	
5.4.8.2.8	VIII是否定期評估網路安全控制系統並適時檢討並改進監控及偵測技術？	

六、內部管理

項目編號	查核事項	法令規章
5.4.8.2.9	IX 是否利用網路監控軟體並指定專人監看網路流量？並即時注意異常狀況？	信用合作社資通安全防護基準第 13 條。
5.4.8.2.10	X 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？	
5.4.8.2.11	XI 對於監視及偵測之異常事件是否明確定義須通報之事件？是否建置適當之通報機制，並依規定分別陳報單位主管或管理階層？	
5.4.8.2.12	XII 使用遠端連線進行系統管理作業時，是否使用加密通訊協定，且不得將密	

六、內部管理

項目編號	查核事項	法令規章
5.4.8.3	碼紀錄於工具軟體內。 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？	
5.4.8.4	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？	
5.4.8.5	⑤當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？	
5.4.8.6	⑥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	

六、內部管理

項目編號	查核事項	法令規章
5.4.8.7	連線？ ⑦是否定期進行弱點掃描？ 並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，填寫評估結果及處理情形，採取適當措施並確保作業系統及軟體安裝經測試且無弱點顧慮之安全修補程式？	
5.4.8.8	⑧是否避免採用已停止弱點修補或更新之系統軟體及應用軟體？如有必要是否採用必要防護措施？	
5.4.8.9	⑨防火牆安全檢查要點	
5.4.8.9.1	I. 針對整體網路拓樸中，與外部連線之區域，以及內部的特定的安全區域，如：信合社核心業務，及網際網路等之網路連線是否架設防火牆予以區隔？	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.8.9.2	II. 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？	
5.4.8.9.3	III. 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？	
5.4.8.9.4	IV 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？	
5.4.8.9.5	V. 是否定期針對防火牆各項連線進行分析評估，包	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.8.9.6	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？ VI. 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？	
5.4.8.9.7	VII. 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？	
5.4.8.9.8	VIII. 防火牆是否具備支援保護遠端撥接服務的能力及虛擬私有網路（VPN）之能力？	
5.4.8.9.9	IX. 防火牆是否具備不同網路協定封包之過濾能力，例如：FTP、HTTP、IPX、	

六、內部管理

項目編號	查核事項	法令規章
5.4.8.9.10	MIME、RPCs、SNMP、SMTP、TELNET、UDP 以有效保護網路安全？ X. 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？	信用合作社資通安全防护基準第 13 條。
5.4.8.9.11	XI 防火牆及具存取控制 (Access control list, ACL) 網路設備，是否遵循下列措施：	
5.4.8.9.11.1	A. 是否定期檢視防火牆及具存取控制 (ACL) 網路設備參數設定？	
5.4.8.9.11.2	B. 是否檢視所開啟的通訊埠與業務需求相符？	
5.4.8.9.11.3	C. 是否定期檢視高風險設定及六個月內無流量之防火牆規則評估其必要	

六、內部管理

項目編號	查核事項	法令規章
5.4.8.9.11.4	性及風險？ D. 是否針對已下線系統於半年內調整或停用防火牆規則？	
5.4.8.9.11.5	E. 是否每半年檢視 DMZ 之防火牆規則？	
5.4.8.10	⑩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？	
5.4.8.11	⑪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？	
5.4.8.12	⑫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？	

六、內部管理

項目編號	查核事項	法令規章
5.4.8.13	⑬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。
5.4.8.14	⑭對全社員工上網行為管理是否建立妥適之管控措施，限制連結非業務相關網站，以避免下載惡意程式？	
5.4.8.15	⑮經由網際網路連接至內部網路進行遠距之系統維護管理工作，是否遵循下列措施：	信用合作社資通安全防護基準第 13 條
5.4.8.15.1	I 是否建立授權機制，依據其申請項目提供必要授權？	
5.4.8.15.2	II 是否定義允許可連結之遠端設備，並確保已安裝必要資訊安全防護？	
5.4.8.15.3	III 是否加強變更作業之身分認證，於每次登入時得採	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.8.15.4	用照會或二項以上安全設計並取得主管授權，惟緊急故障排除仍須於事後向主管核備？	
5.4.8.16	IV 是否建立監控機制，留存操作紀錄，並由主管或獨立單位定期覆核？	
5.4.8.16.1	⑩提供員工經由外部網際網路連線使用之應用系統，是否遵循下列措施：	
5.4.8.16.1	I 是否定期執行弱點掃描、滲透測試及程式原始碼掃描並儘速完成弱點修補？	
5.4.8.16.2	II 是否建立網頁防竄改機制並將該等系統納入監控範圍？	
5.4.8.16.3	III 是否確保委外廠商交付之系統或程式無惡意程式及後門程式？	
5.4.8.17	⑪有機敏資料儲存於使用者端操作環境、機敏資料於網際網路上傳輸、使用者身分	

六、內部管理

項目編號	查核事項	法令規章
5.4.8.18	確認資料（如固定密碼、設備資訊、生物特徵）儲存於系統內等情形者，是否建立隱密性機制？ ⑱ 透過網際網路傳輸途徑辦理電子銀行之業務，其客戶身分確認資料如為固定密碼者，其固定密碼是否於儲存時應先進行不可逆運算（如雜湊演算法）？另為防止透過預先產製雜湊值推測密碼，是否進行加密保護或加入不可得知之資料運算？採用加密演算法者，其金鑰是否儲存於經第三方認證並符合 NIST FIPS 140-2 L3 之硬體安全模組內並限制明文匯出功能？	信用合作社資通安全防護基準第 6 條。
5.4.8.19	⑲ 營運環境採用硬體安全模組保護金鑰者，該金鑰是否由非該系統開發及維護單位之二個單位以上產製並分持管理其產製之基碼	信用合作社資通安全防護基準第 6 條。

六、內部管理

項目編號	查核事項	法令規章
5.4.8.20	單，另金鑰得以加密方式匯出至安全載具（如晶片卡）或備份至具存取權限控管之位置，供維護單位緊急使用。	信用合作社資通安全防護基準第8條、第9條。
5.4.8.21	⑳減少金鑰儲存之地點，並僅允許必要之管理人員存取金鑰，以利管理並降低金鑰外洩之可能性。	
5.4.8.22	㉑當金鑰使用期限將屆或有洩漏疑慮時，是否已進行金鑰替換。	
5.4.9	㉒機敏資料儲存於雲端服務業者，是否遵循中華民國銀行商業同業公會全國聯合會所訂定之雲端服務相關自律規範辦理。	
5.4.9.1	(9)營運管理 ①是否建立定期備份機制及備份清冊，備份媒體或檔案已妥善防護，確保資訊之可用性及防止未授權存取。	
5.4.9.2	②是否驗證備份資料之完整	

六、內部管理

項目編號	查核事項	法令規章
5.4.9.3	性、可用性及儲存環境的適當性。 ③是否建立適當保護機制及管理程序，並留存相關紀錄至少一年。	
5.4.9.4	④是否加強連續假期之資安防護並符合下列要求：	
5.4.9.4.1	I. 評估系統及電腦於連續假期開機必要性，如無必要，則須關閉連線服務或電源。	
5.4.9.4.2	II. 評估於連續假期結束後第一個營業日是否提前到班，以確保核心資通系統及第一類電腦系統正常運作。	
5.4.9.5	⑤核心資通系統、第一類電腦系統之營運環境容量管理是否符合下列要求：	
5.4.9.5.1	I. 依據資源使用狀況及容量需求，並考量軟體更新、生命週期、軟硬體運作相容性等因素，評估採	

六、內部管理

項目編號	查核事項	法令規章
5.4.9.5.2	用多重備援或冗餘配置 (Redundancies) 等方式，適時進行資源調整及擴充。 II. 定期評估核心資通系統是否有單點故障風險 (Single Point of Failure)，並導入高可用性或高可靠度的措施 (如 Active Active、Active Standby 或 Disaster Recovery)，避免因單點故障造成整體異常之情形。	
5.4.9.5.3	III. 依業務性質及設備功能等對核心資通系統訂定相關負載量要求，以強化系統穩定性，確保業務持續運作不中斷。	
5.4.9.5.4	IV. 針對核心資通系統特性、風險因素及所需效能，設定監控項目 (如效能，容量空間，負載量、	

六、內部管理

項目編號	查核事項	法令規章
5.4.9.5.5	頻寬等)、規則(如警示種類)、程序或規範。 V. 定期將監控結果適時通知相關權責單位,於完成相關處理及應變後,留存紀錄由權責單位核示。	信用合作社資通安全防護基準第 10 條。
5.4.10	(10)脆弱性管理:	
5.4.10.1	①是否建立上網管制措施,限制連結非業務相關網站,以避免下載惡意程式。	
5.4.10.2	②是否建立病毒偵測機制並定期更新病毒碼或建立白名單管控機制,以避免安裝未授權程式。	
5.4.10.3	③有無隨時掌握資安事件,針對高風險或重要項目立即進行清查及應變。	
5.4.10.4	④定期進行弱點掃描,並針對其掃描或測試結果進行風險評估,針對不同風險訂定適當措施及完成時間,填寫評估結果及處理情形,採取適當措施並確保作業系統	

六、內部管理

項目編號	查核事項	法令規章
5.4.10.5	及軟體安裝經測試且無弱點顧慮之安全修補程式。 ⑤避免採用已停止弱點修補或更新之系統軟體及應用軟體，如有必要，是否已採用必要防護措施。	
5.4.10.6	⑥有無偵測惡意網站連結並定期更新惡意網站清單。	
5.4.10.7	⑦是否建立入侵偵測或入侵防禦機制並定期更新惡意程式行為特徵。	
5.4.10.8	⑧定期執行電子郵件社交工程演練及教育訓練。	
5.4.10.9	⑨偵測釣魚網站，如有發現應採取必要措施。	
5.4.10.10	⑩是否建立 DDoS 攻擊監控及事故應變機制，並每年進行程序演練或實際演練。	
5.4.10.11	⑪是否評估建置網頁應用程式防火牆。	
5.4.10.12	⑫是否偵測提供網際網路服務之系統其網頁與程式異動，記錄並通知相關人員處	

六、內部管理

項目編號	查核事項	法令規章
5.4.11	理。 (11)開放網際網路連線使用之視訊會議使用管理，是否已依下列事項辦理：	信用合作社資通安全防護基準第 12 條。
5.4.11.1	①適時更換視訊會議代碼或密碼，避免重複使用。	
5.4.11.2	②機敏性會議採用高強度密碼或多因子進行身分驗證。	
5.4.11.3	③確認與會者身分後再進行會議，以確保會議內容不外流。	
5.4.11.4	④評估使用線上紀錄功能，避免會議內容外洩風險。	
5.4.11.5	⑤參加會議時已關閉非必要功能，並注意發送及分享資訊，避免機敏資料外洩。	
5.4.12	(12)異地辦公管理，是否符合下列要求：	
5.4.12.1	①VPN 使用管理	
5.4.12.1.1	I. 將 VPN、網路基礎架構設備之主機更新至最適版本，並使用安全設定。	
5.4.12.1.2	II. 提醒用於連入遠端作業	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.4.12.1.3	環境之主機，先安裝安全修補程式、更新病毒碼後再進行連線。	
5.4.12.1.4	III. 確認 IT 及資安人員已完成準備，包含日誌檢視、攻擊偵測、事件應變及事件復原機制。	
5.4.12.1.5	IV. 採用高強度密碼或多因子進行身分驗證。	
5.4.12.2	V. 確認 VPN 資源足以應付大量使用，若情況允許，可以透過設定流量管制，以讓有高流量需求的員工有充足的資源能夠使用。	
5.4.12.2.1	②虛擬桌面(VDI)使用管理 I. 針對伺服器及虛擬桌面軟體進行妥善設定，避免員工可以將虛擬桌面連接到本機印表機印出檔案內容，透過虛擬桌面存取本機主機檔案，連接可卸除裝置或透過剪貼簿於兩端剪貼資料。	

六、內部管理

項目編號	查核事項	法令規章
5.4.12.2.2	II. 適時進行軟體更新以修補最適漏洞，並向員工宣導不應安裝可疑程式避免中毒。	
5.4.12.2.3	III. 設定虛擬桌面在一段閒置時間後將螢幕鎖定或中斷連線，以免遭到被入侵之本機主機操控。	
5.4.12.2.4	IV. 禁止員工使用自動抓取關鍵字之鍵盤軟體，以免機敏資訊外洩。	
5.4.12.2.5	V. 採用高強度密碼或多因子進行身分驗證。	
5.4.12.2.6	VI. 使用全硬碟加密機制或限制下載，以防止虛擬桌面之檔案遭誤存於本機裝置中。	
5.4.13	(13)資訊安全事故管理是否符合下列要求：	
5.4.13.1	①將各作業系統、網路設備、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	信用合作社資通安全防護基準第 16 條。

六、內部管理

項目編號	查核事項	法令規章
5.4.13.2	定期檢討修訂。 ②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，並留存相關作業紀錄；另已定期辦理演練，以確保資安事故發生時相關通報、處理及應變作業之有效性。	
5.4.13.3	③如有資訊安全事故發生時，其系統交易紀錄、系統日誌、安全事件日誌妥善保管，並注意處理過程中軌跡紀錄及證據留存之有效性。	
5.5	5. 故障與災害應變管理	
5.5.1	(1)硬體設備備援管理	
5.5.1.1	①為提昇系統可靠性之措施，對下列各電腦設備及相關設施是否已有妥善之備援措施，可於事故發生時支援重要之業務？	
5.5.1.1.1	I 主機設備(包括電腦容量)。	

六、內部管理

項目編號	查核事項	法令規章
5.5.1.1.2	II 週邊設備。	
5.5.1.1.3	III 通訊設備。	
5.5.1.1.4	IV 電路(電力、不斷電設備)。	
5.5.1.1.5	V 端末控制設備及端末機。	
5.5.1.2	②備援設備若非自行所有，是否有契約明定其支援方式，時間及價格(如與廠商簽訂之備用契約或與同類機器使用者互締之支援契約)？	
5.5.2	(2)營運持續管理是否符合下列要求：	信用合作社資通安全防護基準第 17 條。
5.5.2.1	①是否已進行營運衝擊分析，定義最大可接受系統中斷時間，設定系統復原時間及資料復原時點，並考量下列因素，採取必要備援機	

六、內部管理

項目編號	查核事項	法令規章
5.5.2.1.1	制： I. 考量如有系統復原時間限制狀況下，必要時建立同地或異地備援機制(Disaster Recovery；DR)。	
5.5.2.1.2	II. 評估單點故障(Single Point of Failure)風險，必要時導入高可用性或高可靠度的措施(如 Active Active、Active Standby)，避免造成整體服務中斷之情形。	
5.5.2.1.3	III. 依業務性質及設備功能等對系統訂定相關負載量要求並進行妥適監控，以強化系統穩定性，確保業務持續運作不中斷。	
5.5.2.1.4	IV. 監控批次作業(如監控資源使用情況並應注意是否已執行完成所有作業程序，以避免影響正常交易)。	
5.5.2.2	②建立對於重大資訊系統事件或天然災害之應變程	

六、內部管理

項目編號	查核事項	法令規章
5.5.2.3	序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。	
5.5.2.4	③每年驗證及演練其營運持續性控制措施，以確保其有效性，並保留相關演練紀錄及召開檢討會議。	
5.6	④如遇尖峰作業、大量活動(如支付)或例行業務處理量較大(如撥薪)等時段，特別注意各類異常情形之監控並加強檢核系統資源，俾事先提出因應措施。	
5.6.1	6. 內部電腦稽核、自行查核及遵守法令制度之實施 (1)資訊業務是否明訂稽核(含稽核單位之電腦稽核及資訊單位自行查核)規範？稽核規範內容是否完備？	
5.6.2	(2)辦理內部電腦稽核、自行查	

六、內部管理

項目編號	查核事項	法令規章
5.6.3	核，其稽核範圍是否完整？ （如：使用者帳號管理、程式變更管理、資料變更管理、網路管理、委外作業管理、客戶保密作業…等項目之查核），是否確實執行查核？ (3)稽核人員之指派是否妥適？ 是否符合分工牽制原則？	信用合作社資通安全防護基準第 18 條
5.6.4	(4)法令遵循管理是否符合下列要求：	
5.6.4.1	①盤點與資訊安全相關法規規定，並將相關資訊安全要求與內部控制制度結合，定期進行法令遵循自評，以確保資訊安全之法令遵循性。	
5.6.4.2	②透過內部控制制度進行定期檢核，並於每年依據信用合作社聯合社所訂定之資訊安全評估相關自律規範，提出電腦系統資訊安全評估報告。	

六、內部管理

項目編號	查核事項	法令規章
5.7	7. 南資會員查核事項	
5.7.1	(1) 個資保護措施	
5.7.1.1	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及納管機制，並定期進行清查及留存相關作業紀錄？	
5.7.1.2	② 存放於電腦（包括伺服器及個人電腦）內之個資是否建立妥適之管理機制？（含南資中心檔案伺服器使用者權限之管理）	
5.7.1.3	③ 對傳遞個資是否建立妥適之加密及管理機制（含洗錢防制大額通報作業流程控制設計及辦理情形）？	
5.7.1.4	④ 對行動碟、光碟、磁帶等移動式儲存媒體，及對 FTP、檔案分享（如網路芳鄰、SAMBA）、檔案下載、電子	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
	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。	
5.7.2	(2)個人電腦管理	
5.7.2.1	①網路架設是否建立申請核准程序及管理機制？	
5.7.2.2	②是否研擬南資中心無法提供服務時之應變計畫並辦理演練？	
5.8	8.社群媒體控管程序	金融機構運用新興科技作業規範。
5.8.1	(1)是否制定社群媒體管理政策，並定期檢視？	
5.8.2	(2)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	

六、內部管理

項目編號	查核事項	法令規章
5.8.3	發言規範，明定發言角色與權責？ (3)是否建立內容過濾與監視機制？	
5.9	9. 自攜裝置安全控管	
5.9.1	(1)是否制定自攜裝置管理政策，並定期檢視？	
5.9.2	(2)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)？	
5.9.3	(3)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？	

六、內部管理

項目編號	查核事項	法令規章
5.9.4	(4)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。
5.10	10.雲端服務安全控管	
5.10.1	(1)是否制定雲端服務管理政策，並定期檢視？	
5.10.2	(2)導入 IaaS 或 PaaS 雲端服務模式前，是否評估下列事項：	
5.10.2.1	①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护等項目。	
5.10.2.2	②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。	
5.10.2.3	③雲端服務業者所建置安	

六、內部管理

項目編號	查核事項	法令規章
5.10.3	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。 (3)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？	
5.10.4	(4)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？	
5.10.5	(5)金融機構本身、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	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
5.10.6	作業之相關資訊及實地查核權力?經委託第三人查核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? (6)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?	
5.10.7	(7)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之資料，且留存相關紀錄?	

六、內部管理

項目編號	查核事項	法令規章
5.11	11. 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」。
5.12	12. 物聯網設備資安標準是否依「金融機構使用物聯網設備安全控管規範」之規定辦理？	「金融機構使用物聯網設備安全控管規範」。
6	(六)內部稽核制度及其他業務	
6.1	1. 總社部分	
6.1.1	(1) 該社有關內部稽核之重要政策、內規暨政府政策法令之配合情形、內部控制制度聲明書函報情形、稽核單位組織、職掌、人員及分工情形。	「金融控股公司及銀行業內部控制及稽核制度實施辦法」。
6.1.2	(2) 稽核人員之任職情形、操守、素養與訓練情形。	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 29 條、第 30 條、第 37 條、第 38 條。

六、內部管理

項目編號	查核事項	法令規章
6.1.3	(3)稽核作業計畫與實際執行情形。 內部稽核單位擬定年度稽核計畫是否將防制洗錢及打擊資恐法令遵循及計畫執行之標準作業程序，列入加強辦理查核事項，並就本會檢查所提列檢查意見，確實辦理追蹤改善？	1.「金融控股公司及銀行業內部控制及稽核制度實施辦法」第39條。 2.本局106.12.29檢局(證)字第1060159085號函。
6.1.4	(4)稽核手冊、稽核方式及工作底稿之評述，尤應對其作業有無流於形式詳予查核。	本會100.7.14金管檢地字第10001560874號函。
6.1.5	(5)於主管機關檢查結束或收到檢查報告後，內部稽核單位是否依重大性原則，即時通報理事及監察人(監事、監事會)，並提報最近一次理事會？報告內容是否包括檢查溝通會議內容、主要檢查缺失、遭金融主管機關調降評等、	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第42條及第43條。

六、內部管理

項目編號	查核事項	法令規章
	主管機關要求採行之重大缺失改善方案或可能採行之處分措施？對金融檢查機關、會計師與內部稽核單位所提列意見或查核缺失及內部控制制度聲明書所列是否加強辦理改善事項，有無切實追蹤管制，是否將其追蹤考核改善情形，以書面提報理事會及交付監事（會），並列為各單位績效考核之重要項目？	
6.1.6	(6)內部稽核報告處理	1.「金融控股公司及銀行業內部控制及稽核制度實施辦法」第36條、第39條、第40條。
6.1.6.1	①內部稽核報告內容揭露項目是否符合規定？	2.本會105.7.21金管檢制字第10501502582號函。
6.1.6.2	②內部稽核報告、工作底稿及相關資料之保存期限是否符合規定？	
6.1.6.3	③稽核報告是否交付監事	

六、內部管理

項目編號	查核事項	法令規章
6.1.6.4	查閱，並於規定期限內函送主管機關？函送之稽核報告是否與原報告內容相符？ ④對管理單位及營業單位所發生之重大缺失或弊端及對應負責之失職人員，是否於稽核報告揭露？	
6.1.6.5	⑤向本會申報內部稽核報告之標準、格式及相關事宜，是否符合規定？	
6.1.6.6	⑥是否於每會計年度終了後五個月內將上一年度內部稽核所見內部控制制度缺失及異常事項改善情形，陳報主管機關？	
6.1.7	(7)營業單位是否依規定辦理自行查核，函報有關單位	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第14條。

六、內部管理

項目編號	查核事項	法令規章
6.1.8	自行查核內容有無不實者，自行查核報告中是否有違反法令規章或情節嚴重者。 (8)業務單位（包括資訊、財務及資產保管單位）內部自行查核之方式、項目、次數及執行績效。	同上辦法第 14 條。
6.1.9	(9)信合社發生重大偶發事件是否立即依法令規定方式通知治安或其他有關機關採取緊急補救措施外，並應同時知會所屬直轄市或縣（市）政府之地方主管機關，通報範圍是否符合規定，且於通報重大偶發事件之次日起，於七個營業日內函報詳細資料（包括調查內容、處理方式及改善措施）或後續處理情形？	本會 115.2.6 金管銀合字第 11402741881 號令修正發布「金融機構通報重大偶發事件之範圍申報程序及其他應遵循事項」。

六、內部管理

項目編號	查核事項	法令規章
6.1.10	(10)稽核單位是否將業務單位對銀行法第三十二條、三十三條及三十三條之一之有關資料填報工作納入稽核範圍？	
6.1.11	(11)訂定各種作業及管理規則之訂定、修訂或廢止，必要時是否有法令遵循、風險管理、資訊安全等專責單位及內部稽核單位等相關單位之參與？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 12 條。 同上辦法第 41 條。
6.1.12	(12)具有業務或交易核准權限之各級主管及首次擔任營業單位之經理，是否於就任前符合規定之條件？ 首次擔任營業單位之經理，並應於半年內參與內部稽核單位之查核實習四	

六、內部管理

項目編號	查核事項	法令規章
	次以上，並撰寫心得報告呈總稽核核可後，由總稽核出具證明書併同留卷備查。	
6.1.13	(13)函報主管機關資料是否正確？	中央銀行業務局 89.1.10(八九)台央業字 0200044 號函「依建立支票存款戶基本資料檔處理要點填報支票存款戶資料」。
6.1.14	(14)應全面清查買入之有價證券，並檢討現行相關作業流程、空白單據之控管及有價證券之保管等內部控管事宜是否妥適，並加強金庫之管理，以防範可能發生之內部人員舞弊。	1.財政部 89.5.17 台財融字第 89732095 號函「金融機構應清查買入或保管有價證券，並檢討作業流程及內部控制」。 2.本會 99.12.13 金管檢地字第 0990156205 號函「為落實金融機構辦理現金盤點查庫作業及內部稽核執行情形」。 3.本會 99.9.23 金管檢地字第 0990156174 號函。 4.本會 98.12.23 檢局(銀)字第 0980154238 號函。 5.本會 98.1.14 金管檢地字第 09801581910 號函。
6.1.15	(15)金融業遭歹徒詐騙案件之原始通報單位、通報單	財團法人金融聯合徵信中心 87.11.2(87)金徵(業)字第 3213 號函。

六、內部管理

項目編號	查核事項	法令規章
6.1.16	位及通報內容是否嚴守秘密？ (16)金融機構同業往來應訂定對帳規範，內部稽核或自行查核是否辦理函證？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第16至19條。
6.1.17	(17)是否依規訂定「法令遵循主管制度」之相關事宜（含總機構負責單位、分支單位負責人職稱、遵循訓練計畫、自評事項及程序等）。	
6.1.17.1	①應設立一隸屬於總經理之法令遵循單位(該單位應辦理事項是否符合規定?)，負責法令遵循制度之規劃、管理及執行，並指派副總經理以上或職責相當之人擔任法令遵循長，綜理法令遵循事務，至少每半年向理事會及監事(會)報告。如發	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
6.1.17.2	現有重大違反法令或遭金融主管機關調降評等時，是否即時通報理事及監察人(監事、監事會)，並就法令遵循事項，提報理事會？ ②信用合作社法令遵循專責單位、營業單位、資訊單位、財務保管單位及其他管理單位是否指派人員擔任法令遵循主管，負責執行法令遵循事宜？	
6.1.17.3	③金融控股公司及銀行業是否以網際網路資訊系統向主管機關申報法令遵循長、法令遵循專責單位所屬人員之名單及受訓資料？	
6.1.17.4	④金融控股公司及銀行業法令遵循長、法令遵循	1.「金融控股公司及銀行業內部控制及稽核制度

六、內部管理

項目編號	查核事項	法令規章
6.1.17.5	專責單位主管及所屬人員、國內營業單位、資訊單位、財務保管單位及其他管理單位之法令遵循主管之資格條件是否符合相關規定？是否每年至少參加主管機關或其認定機構所舉辦或所屬金融控股公司(含子公司)或銀行業(含母公司)自行舉辦十五小時之在職教育訓練，訓練內容應至少包含新修正法令、新種業務或新種金融商品，前述在職訓練為自行舉辦之訓練方式應提報理事會通過，總機構需留存相關人員上課紀錄備查？ ⑤推出各項新商品、服務及向主管機關申請開辦新種業務前，是否由法令	實施辦法」第 16 條及第 19 條。 2. 本會 106.9.11 金管銀國字第 10600199650 號函。 1. 「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 17 條。 2. 本會銀行局 106.1.9 銀局(國)字第

六、內部管理

項目編號	查核事項	法令規章
6.1.18	遵循主管出具符合法令及內部規範之意見並簽署負責？ (18)是否訂定委外內部作業規範？是否管理督導受委託機構內部控制及內部稽核制度之建立及執行？	10500200470 號函。 「金融機構作業委託他人處理內部作業制度及程序辦法」。
6.1.19	(19)金融卡交易流程控管是否列為內部稽核重點項目，對跨行連線各項環節安全亦應加強查核？	
6.1.20	(20)網路銀行業務：	1. 「個人網路銀行業務服務定型化契約範本」。
6.1.20.1	①網路銀行業務是否明訂稽核規範？其規範內容是否完備？其業務開發設計階段，稽核單位是否參與？網路銀行實際查核範圍是否完整？是否確實查核？稽核人員之指派是否妥適？是否符	2. 金融機構辦理電子銀行業務安全控管作業基準。

六、內部管理

項目編號	查核事項	法令規章
6.1.20.2	合分工牽制原則？ ②網路銀行實際查核範圍是否完整？是否確實查核？稽核人員之指派是否妥適？是否符合分工牽制原則？	
6.1.21	(21)會計師查核 年度財務報表由會計師辦理查核簽證時，是否委託會計師辦理內部控制制度之專案審查，個人資料保護與防制洗錢及打擊資恐機制專案審查，另信用合作社是否於每年四月底前出具上一年度會計師確信報告，報直轄市政府或縣（市）政府並轉呈中央主管機關？	1.「金融控股公司及銀行業內部控制及稽核制度實施辦法」第44條、第47條。 2.本會106.3.22金管銀國字第10620000155號函。
6.1.22	(22)信用合作社總經理是否督導各單位審慎評估及檢討內部控制制度執行情形，由	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第8條。

六、內部管理

項目編號	查核事項	法令規章
6.1.23	理事主席、總經理及總稽核聯名出具內部控制制度聲明書（附表一），並提報理事會通過，於每會計年度終了後三個月內將內部控制制度聲明書內容於中央主管機關指定網站辦理公告申報？ 前項內部控制制度聲明書是否依規定刊登於年報？ 第一項規定對於經主管機關依法接管之信用合作社，不適用之。 (23)稽核單位應於稽核報告「各項業務作業控制與內部管理」項下，揭露對「存款帳戶及其疑似不法或顯屬異常交易管理辦法」第 19 條規定之辦理結果，其內容至少應包含下列事項：	本會 103.8.20 金管銀法字第 10310004610 號令修正「存款帳戶及其疑似不法或顯屬異常交易管理辦法」。
6.1.23.1	①有關「金融機構開戶作業審	

六、內部管理

項目編號	查核事項	法令規章
6.1.23.2	核程序暨異常帳戶風險控管之作業範本」遵循情形之查核結果。	
6.1.23.3	②有關「防杜人頭帳戶範本」遵循情形之查核結果。	
6.1.23.4	③有關「信用合作社防制洗錢及打擊資恐注意事項範本」遵循情形之查核結果。	
6.1.24	④對於營業單位自行查核之相關查核事項，是否落實執行之查核結果。	
6.1.25	(24)是否建立檢舉制度？是否於總機構指定具獨立行使職權之單位負責檢舉案件之受理及調查？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第13條。
6.1.25.1	(25)對本會檢查所提重大檢查意見提報董(理)事會之作業方式： ①每次函覆本會重大檢查意見之改善情形是否均提報董(理)事會，未以提報其他	

六、內部管理

項目編號	查核事項	法令規章
6.1.25.2	管理階層核准或常務董事會之方式替代？ ②是否以討論案方式提報董(理)事會，未以報告案或併入其他討論案提報？	
6.1.25.3	③是否於會議召集日前將議案通知各董(理)事，未以臨時提案方式提出？	
6.1.26	(26)稽核單位辦理本會檢查意見及面請改善事項之追蹤覆查作業，是否依據本會檢查所提相對應之處理意見及風險基礎原則確實辦理？	本會 114.5.14 金管檢控字第 1140602124 號函。
6.1.27	(27)總稽核兼任、異動及與理事間溝通情形之查核： ①總稽核是否未兼任與稽核工作有相互衝突或牽制之職務，包括該金融控股公司及銀行業內部應受內部稽核單位查核之單位主管及該金融控股公司及銀行業	1.「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 27 條 2.本會 111.3.15 金管檢制字第 11106000691 號令

六、內部管理

項目編號	查核事項	法令規章
6.1.28	之董事或監察人？ ②總稽核異動時，是否於事實發生日之即日起算五日內向主管機關函報其異動原因及異動內容，並副知異動之總稽核？ ③是否建立獨立理事、審計委員會或監察人（監事、監事會）與內部稽核單位間之溝通管道與機制，並由內部稽核單位將溝通情形每年向理事會報告？ (28)稽核人員（包括電腦稽核人員）是否依據投資規模、業務情況（分支機構之多寡及其業務量）、管理需要及其他相關法令規章之規定，配置適任及適當人數之專任稽核人員？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 29 條
6.1.29	(29)自行評估作業，是否每半年至少須辦理一次？辦理結果是否送法令遵循	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 17 條

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
6.1.30	專責單位備查？各單位辦理自行評估作業，是否由該單位主管指定專人辦理？自行評估工作底稿及資料是否至少保存五年？ (30)法令遵循專責單位是否依據業務分類或法令遵循重點設置適當數量之專業單位，以負責該項業務或法令相關之國內外營業單位監督、法令遵循執行及支援事項？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 18 條
6.2	2. 分社部分	
6.2.1	(1)總社有關自行查核之重要政策、內規。	
6.2.2	(2)自行查核作業計畫與實際執行情形。	
6.2.3	(3)自行查核方式及工作底稿之評述，尤應查核其作業有無流於形式。	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
6.2.4	(4)對金融檢查單位所提意見，內部稽核報告及自行查核報告所提應改善事項等，有無切實追蹤管制。	
6.2.5	(5)對電腦作業辦理自行查核情形。	
6.2.6	(6)分社是否依規定辦理自行查核，函報有關單位自行查核內容有無不實者，自行查核報告中是否有違反法令規章或情節嚴重者。	
6.2.7	(7)內部人員輪調制度及休假制度之執行情形。	
6.2.8	(8)是否依各單位之業務性質對於自行查核人員持續施以適當查核訓練？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第15條。

六、內部管理

項目編號	查核事項	法令規章
7	(七)風險管理機制:	
7.1	1. 是否訂定適當之風險管理政策與程序，建立獨立有效風險管理機制，以評估及監督其風險承擔能力、已承受風險現況、決定風險因應策略及風險管理程序遵循情形？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 20 至 23 條。
7.1.1	(1) 是否已訂定適當且經理事會核准通過之整體風險管理政策及重大風險相關之管理章則，且定期檢討修訂（至少 1 年 1 次）並提報理事會？	「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 20 條。
7.1.2	(2) 是否訂定妥適之偵測經營風險內部規範，經理事會通過並定期審視？是否依所訂偵測經營風險之內部規範，進行辨識、衡量、監視及控管經營風險？	1. 「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 20 至 23 條。 2. 本會 104.11.9 金管檢制字第 10401504971 號函。
7.1.3	(3) 是否建立妥適風險管理系統，以確實辨識、衡量、監視及控管經營風險？	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
7.2	2. 是否設置獨立之專責風險控管單位或指定一總社管理單位負責風險控管，並定期向理事會報告風險管理資訊，若發現重大暴險，危及財務或業務狀況或法令遵循者，是否立即採取適當措施並向理事會報告。	
7.3	3. 是否建立衡量及監控流動性部位之管理機制。	
7.4	4. 是否考量整體暴險、自有資本及負債特性進行各項資產配置，建立各項業務風險之管理。	
7.5	5. 是否建立資產品質及分類之評估方法，計算及控管大額暴險，並定期檢視，覈實提列備抵損失。	

六、內部管理

項 目 編 號	查 核 事 項	法 令 規 章
7.6	6. 是否對合作社業務或交易、資訊交互運用等建立資訊安全防护機制及緊急應變計畫。	
8	(八)防制洗錢及打擊資恐 本項查核項目請參考本局網站檢查業務項下「防制洗錢及打擊資恐專區」中之「信用合作社防制洗錢及打擊資恐檢查手冊」。 請至本局網站檢查業務項下「金融檢查手冊」之重要聲明第4點點選連結。	