

四、內部管理之查核

項 目 編 號	查 核 事 項	法 令 規 章
1	(一)分層負責制度之查核	
1.1	1.董事及董事會之職權與功能	
1.1.1	(1)董事之資格、人數及持股比率應符合票券商負責人及業務人員管理規則、公司法之規定。	1.票券商負責人及業務人員管理規則第 9 條 2.公司法第 192 條、第 197 條
1.1.2	(2)董事會與經理人應建立內部行為準則，包括訂定董事行為準則、員工行為準則等事項。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條
1.1.3	(3)董事會執行業務，應依照法令章程及股東會之決議。	公司法第 193 條第 1 項
1.1.4	(4)董事會開會時，董事應親自出席。董事出席委託其他董事代理出席董事會時，應於每	公司法第 205、206、207 條

項 目 編 號	查 核 事 項	法 令 規 章
1.1.5	<p>次出具委託書並列舉召集事由之授權範圍，且代理人以受理一人之委託為限。董事會之決議，應有過半數董事之出席，出席董事過半數之同意行之。董事會之議事，應作成議事錄，並完整記載董事出席狀況。</p> <p>(5)董事會所列議案如涉有董事本身利害關係致損及公司利益之虞時，應自行迴避，不得加入表決，亦不得代理其他董事行使其表決權。</p>	公開發行公司董事會議事辦法第 16 條第 1 項
1.1.6	<p>(6)常務董事會或董事長於董事會休會期間行使董事會職權，公司章程應明訂授權範圍，其授權內容或事項應具體明確，不得</p>	<p>1.公開發行公司董事會議事辦法第 8 條</p> <p>2.上市上櫃公司治理實務守則第 35</p>

項 目 編 號	查 核 事 項	法 令 規 章
1.1.7	<p>概括授權，且涉及公司重大利益事項，仍應經由董事會之決議。</p> <p>(7)公司召開董事會，除得視議案內容通知相關部門非擔任董事之經理人列席，並得邀請會計師、律師或其他專業人士列席會議外，是否有其他不應列席會議之人士參加，但討論及表決時應離席。</p>	<p>條第 3 項</p> <p>公開發行公司董事會議事辦法第 11 條</p>
1.1.8	<p>(8)董事會成員由內部經理人兼任情形，不宜因兼任情形比例過高，致董事會未能有效發揮其監督功能。</p>	<p>票券金融公司公司治理實務守則第 35 條第 2、3 項</p>
1.1.9	<p>(9)功能性委員會是否將所提議案交由董事會決議，以示對董事會負責（但審計委員會依證券交易法、公司法及其他法律規定行</p>	

項 目 編 號	查 核 事 項	法 令 規 章
1.1.10	<p>使監察人職權者，不在此限)。</p> <p>功能性委員會是否訂定行使職權規章，經由董事會通過。行使職權規章之內容至少包括委員會之權限及責任，行使職權過程（組織地位、委員之資格條件、行使職權流程等），及每年覆核與評估是否更新行使職權規章之政策。</p> <p>(10)公開發行票券公司獨立董事選舉，是否依公司法規定採候選人提名制度，並載明於章程，由股東就獨立董事候選人名單中選任之（金融控股公司持有發行全部股份之子公司，其獨立董事得由金融控股公司指派之）；董事會審議獨立董事候選人名</p>	<p>1.公開發行公司獨立董事設置及應遵循事項辦法第 5 條、第 7 條</p> <p>2.公司法第 204 條</p>

項 目 編 號	查 核 事 項	法 令 規 章
1.1.11	單，應於 7 日前通知董事，不宜以臨時動議提出。 (11)獨立董事與董事會如係由同一集團控制者，是否能獨立行使職權。	
1.1.12	(12)獨立董事有辭職者，應瞭解其辭職原因，並查核獨立董事辭職前後，董事會是否有通過重大影響公司權益之議案。	
1.1.13	(13)獨立董事於會議中表示意見，或表示反對意見，應列入紀錄並瞭解董事會採納情形。	1.票券金融公司公司治理實務守則 第 4 條第 2 項、第 34 條之 1、第 41 條 2.公開發行公司董事會議事辦法第 7 條第 2 項
1.1.14	(14)獨立董事兼任其他公開發行公司獨立董事	公開發行公司獨立董事設置及應遵

項 目 編 號	查 核 事 項	法 令 規 章
1.1.15	不得逾三家以上。 (15)票券金融公司董事會應認知營運所面臨之風險，監督其營運結果，並對於確保建立及維持適當有效之內部控制制度負有最終之責任。	循事項辦法第 4 條 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 條之 1
1.1.16	(16)董事會與經理人應建立內部行為準則，包括訂定董事行為準則、員工行為準則；董事行為準則至少應包括發現票券金融公司有受重大損害之虞時，應儘速妥適處理，立即通知審計委員會或審計委員會之獨立董事成員或監察人並提報董事會，且應督導所屬票券金融公司通報主管機關。	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
1.2	2.監察人之職權與功能	

項 目 編 號	查 核 事 項	法 令 規 章
1.2.1	(1)監察人資格、人數及持股比率應符合規定應符合票券商負責人及業務人員管理規則、公司法之規定。且不得兼任公司董事、經理人或其他職員。	1.票券商負責人及業務人員管理規則第 9 條 2.公司法第 222 條
1.2.2	(2)監察人各得單獨行使監察權，且得隨時調查公司業務及財務狀況，查核簿冊文件，並得請求董事會或經理人提出報告。	公司法第 221、218 條
1.2.3	(3)董事會或董事執行業務有違反法令、章程或股東會決議之行為者，監察人應即通知董事會或董事停止其行為。	公司法第 218 條之 2 第 2 項
1.2.4	(4)監察人對於董事會編造提出股東會之各種表冊，應予查核，並報告意見於股東會。	公司法第 219 條第 1 項
1.2.5	(5)依證券交易法規定發行股票之票券公司，是	107.12.19 金管證發字第 1070345233

項 目 編 號	查 核 事 項	法 令 規 章
1.3	否設計審計委員會替代監察人?(該公司如 為金控公司持有發行全部股份者，得擇一 設置審計委員會或監察人。)	1 號令
1.3.1	3.董事會議事運作： (1)董事會之召集，應於 3 日前通知各董事及監 察人。但章程有較高之規定者，從其規定。	公司法第 204 條
1.3.2	(2)重大議案是否以臨時董事會提出，議程檢附 之資料內容是否足以供董事充分瞭解。	公開發行公司董事會議事辦法第 3 條第 2 項
1.3.3	(3)會議紀錄應依規定詳實記載，開會過程應依 規定全程錄音或錄影存證並至少保存五 年。	公開發行公司董事會議事辦法第 18 條第 1 項
1.4	4.董事支領報酬情形：	
1.4.1	(1) 董事之報酬是否經章程訂明，或由股東會	1.公司法第 196 條

項 目 編 號	查 核 事 項	法 令 規 章
1.4.2	議定之？ (2)董事長不得有自行核定其本人報酬與酬勞 (如獎金)等不當情事。	2.票券金融公司年報應行記載事項 準則第 10 條第 2 款
1.4.3	(3)公司虧損，但董事報酬增加者，其報酬給 付是否合理。	3.公開發行票券金融公司財務報告 編製準則第 24 條
1.4.4	(4)董事酬勞占稅後純益之比例不得過高。酬 金政策、標準與經營績效應有關聯。	
1.4.5	(5)公司年報之公司治理報告，是否依規定揭 露最近年度給付董事、監察人、總經理、 副總經理及顧問酬金，及分派員工酬勞情 形。	
1.4.6	(6)全體董事、監察人領取財務報告內所有公 司之董事、監察人酬金占稅後淨利超過百	

項 目 編 號	查 核 事 項	法 令 規 章
1.4.7	<p>分之二，且個別董事或監察人領取酬金超過新臺幣一千五百萬元者，是否揭露該個別董事或監察人酬金。</p> <p>(7)是否於年度個體財務報告揭露監察人酬金資訊及公司薪資報酬政策。</p>	
1.4.8	<p>(8)上市上櫃票券金融公司最近一年度稅後淨利增加達百分之十以上，惟非擔任主管職務之全時員工年度薪資平均數卻未較前一年度增加者，是否揭露個別董事及監察人之酬金？</p>	票券金融公司年報應行記載事項準則第 10 條
1.4.9	<p>(9)上市上櫃票券金融公司最近一年度稅後損益衰退達百分之十且逾新臺幣五百萬元，及平均每位董事酬金（不含兼任員工</p>	票券金融公司年報應行記載事項準則第 10 條

項 目 編 號	查 核 事 項	法 令 規 章
1.5	<p>酬金)增加達百分之十且逾新臺幣十萬元者，是否揭露個別董事及監察人之酬金。</p> <p>5.分層負責辦理情形</p>	
1.5.1	(1)應訂定內部組織系統、單位職掌、業務範圍、授權及分層負責辦法。	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
1.5.2	(2)主要業務分層負責辦事，應符合內部控制原則，並定期檢討改善。	
1.5.3	(3)對部位風險、投資風險、利率風險、流動性風險及授信授權之管理，應定期持續覆核並評估其有效性。	
1.6	6.檢舉制度	金融控股公司及銀行業內部控制及稽核制度實施辦法第 34-2 條
1.6.1	(1)是否建立檢舉制度；是否於總機構指定具職權行使獨立性之單位負責檢舉案件之受理	

項 目 編 號	查 核 事 項	法 令 規 章
1.6.2	<p>及調查；是否提報董事會通過。</p> <p>(2) 檢舉案件之受理及調查過程，有利益衝突之人，是否予以迴避；被檢舉人為董事、監察人或職責相當於副總經理以上之管理階層者，調查報告是否陳報至監察人或審計委員會複審。</p>	
1.6.3	<p>(3) 檢舉制度是否包括下列事項：</p> <p>①檢舉人之身分資料保密、權利保障及保護措施。(包含不得因所檢舉案件而對檢舉人予以解僱、解任、降調、減薪、損害其依法令、契約或習慣上所應享有之權益，或其他不利處分)</p> <p>②任何人發現有犯罪、舞弊或違反法令之虞</p>	

項 目 編 號	查 核 事 項	法 令 規 章
1.6.4	<p>時，均得提出檢舉。</p> <p>③調查與配合調查之流程、迴避規定及後續處理機制之標準作業程序。</p> <p>④設置並公布檢舉管道。</p> <p>⑤受理之檢舉案件類型。</p> <p>⑥檢舉案件受理、調查過程、調查結果與相關文件製作之紀錄及保存。</p> <p>⑦檢舉案件之處理情形，應適度以書面或其他方式通知檢舉人。</p> <p>(4)調查後發現為重大偶發事件或違法案件，是否主動向相關機關通報或告發。是否定期對所屬人員，辦理檢舉制度之宣導及教育訓練。</p>	

項 目 編 號	查 核 事 項	法 令 規 章
1.7	7.公司治理	
1.7.1	<p>(1)公司治理相關事務，是否包括：</p> <p>①依法辦理董事會及股東會之會議相關事宜。</p> <p>②製作董事會及股東會議事錄。</p> <p>③協助董事、監察人就任及持續進修。</p> <p>④提供董事、監察人執行業務所需之資料。</p> <p>⑤協助董事、監察人遵循法令及其他依公司章程或契約所訂定之事項等。</p>	票券金融公司公司治理實務守則第44條之2
1.7.2	<p>(2)除法令另有規定者外，票券金融公司之公司治理主管得由公司其他職位人員兼任。公司 治理主管由公司其他職位人員兼任者， 是否確保其本職及兼任職務之有效執行，</p>	票券金融公司公司治理實務守則第44條之3

項 目 編 號	查 核 事 項	法 令 規 章
1.7.3	<p>且不得涉有利益衝突及違反內部控制制度情事。</p> <p>(3)公司治理主管是否取得律師、會計師執業資格或於證券、金融、期貨相關機構或公開發行公司從事法務、財務、股務或第四十四條之二所定公司治理相關事務單位之主管職務合計達三年以上。</p>	票券金融公司公司治理實務守則 44 條之 4
1.7.4	<p>(4)公司治理主管除初任者應自擔任此職務之日起一年內至少進修十八小時外，是否每年至少進修十二小時(其進修範圍、進修體系及其他進修事宜，參照上市上櫃公司董事、監察人進修推行要點規定辦理)。</p>	票券金融公司公司治理實務守則 44 條之 5
1.7.5	<p>(5)年報內容對公司治理報告是否可揭露董事</p>	「票券金融公司年報應行記載事項

項 目 編 號	查 核 事 項	法 令 規 章
1.7.6	<p>會、審計委員會運作情形或監察人參與董事會情形、董事會多元化政策、公司治理運作情形及與銀行業公司治理實務守則差異情形及原因、薪資報酬委員會或提名委員會組成及運作情形、推動永續發展執行情形、履行誠信經營情形等公司治理運作情形。</p> <p>(6)公司年報是否依「票券金融公司年報應行記載事項準則」第 11 條規定，記載股本來源、主要股東名單、股利政策及執行狀況，無償配股對公司營業績效及每股盈餘之影響，員工、董監酬勞之成數或範圍、酬勞金之估列基礎、以股票分派員工酬勞之股</p>	<p>準則」第 10 條第 3 款</p> <p>票券金融公司年報應行記載事項準則第 11 條</p>

項 目 編 號	查 核 事 項	法 令 規 章
1.7.7	<p>數計算基礎及估列數有差異之會計處理，董事會通過分配酬勞情形，前一年度員工、董監酬勞之實際分派情形，及票券金融公司買回該公司股份情形。</p> <p>(7) 公司年報是否依「票券金融公司年報應行記載事項準則」第 17 條規定，對營業概況記載經營之主要業務、本年度經營計畫、市場分析、金融商品研究與業務發展概況、長短期業務發展計畫，從業員工人數、平均服務年資及年齡、學歷分布比率，員工持有之專業證照及進修訓練情形，企業責任及道德行為，非主管職之全時員工最近 2 年人數、薪資平均數及中位數，資訊</p>	<p>本 會 111.2.21 金 管 銀 法 字 第 11102703781 號 令「票券金融公司年報應行記載事項準則」第 17 條</p>

項 目 編 號	查 核 事 項	法 令 規 章
1.7.8	設備，資通安全管理，勞資關係，重要契約等。 (8)票券金融公司是否揭露給付簽證會計師與其所屬事務所及關係企業之審計公費與非審計公費之金額及非審計公費服務內容。	本 會 111.2.21 金 管 銀 法 字 第 11102703781 號令「票券金融公司年報應行記載事項準則」第 10 條第 5 款
1.7.9	(9) 票券金融公司自一百十三年起應揭露氣候相關資訊，其中有關溫室氣體盤查及確信相關資訊依下列時程揭露於公司治理報告： ①實收資本額達新臺幣一百億元以上之票券金融公司之母公司個體，應自一百十三年起完成溫室氣體盤查及確信資訊揭露。	1. 本 會 113.2.22 金 管 銀 法 字 第 11302705091 號令 2. 票券金融公司年報應行記載事項準則第 10 條

項 目 編 號	查 核 事 項	法 令 規 章
	<p>②實收資本額達新臺幣一百億元以上之票券金融公司之合併財務報告子公司，及實收資本額達新臺幣五十億元以上且未達一百億元之票券金融公司之母公司個體，應自一百十四年起完成盤查資訊揭露，一百十六年起完成確信資訊揭露。</p> <p>③實收資本額達新臺幣五十億元以上且未達一百億元之票券金融公司之合併財務報告子公司，及實收資本額未達新臺幣五十億元之票券金融公司之母公司個體，應自一百十五年起完成盤查資訊揭露，一百十七年起完成確信資訊揭露。</p> <p>④實收資本額未達新臺幣五十億元之票券</p>	

項 目 編 號	查 核 事 項	法 令 規 章
1.7.10	<p>金融公司之合併財務報告子公司，應自一百十六年起完成盤查資訊揭露，一百十八年起完成確信資訊揭露。</p> <p>(10)票券金融公司應依下列時程揭露公司(含合併財務報告子公司)之減碳目標、策略及具體行動計畫：</p> <p>①實收資本額達新臺幣一百億元以上，應自一百十四年起完成揭露。</p> <p>②實收資本額達新臺幣五十億元以上且未達一百億元，應自一百十五年起完成揭露。</p> <p>③實收資本額未達新臺幣五十億元，應自一百十六年起完成揭露。</p>	本 會 113.2.22 金 管 銀 法 字 第 11302705091 號 令
1.8	8.審計委員會	

項 目 編 號	查 核 事 項	法 令 規 章
1.8.1	(1)設置審計委員會是否訂定審計委員會組織 規程；是否經董事會決議通過，修正時亦 同；審計委員會是否由全體獨立董事組 成，其人數是否少於三人，其中一人為召 集人，是否至少一人應具備會計或財務專 長。	公開發行公司審計委員會行使職權 辦法第 3 條、第 4 條
1.8.2	(2) 審計委員會是否至少每季召開一次，並於 審計委員會組織規程中明定之；召集時， 是否載明召集事由，並於七日前通知委員 會各獨立董事成員；審計委員會得決議請 公司相關部門經理人員、內部稽核人員、 會計師、法律顧問或其他人員列席會議及 提供相關必要之資訊，但討論及表決時是	公開發行公司審計委員會行使職權 辦法第 7 條、第 8 條

項 目 編 號	查 核 事 項	法 令 規 章
1.8.3	<p>否離席；召開時，公司是否設簽到簿；代理出席審計委員會時，是否每次出具委託書，並列舉召集事由之授權範圍，且以受一人之委託為限。</p> <p>(3)審計委員會之獨立董事成員對於會議事項，與其自身有利害關係者(配偶或二親等內血親)，是否說明其利害關係之重要內容，如有害於公司利益之虞時，不得加入討論及表決，且討論及表決時否應予以迴避，並不得代理其他獨立董事成員行使其表決權。因前項規定，致委員會無法決議者，是否向董事會報告，由董事會為決議。</p>	<p>公開發行公司審計委員會行使職權辦法第 9 條</p>
1.8.4	<p>(4) 審計委員會之議事，是否作成議事錄，詳</p>	<p>公開發行公司審計委員會行使職權</p>

項 目 編 號	查 核 事 項	法 令 規 章
1.9	實記載應記事項；議事錄是否由會議主席及記錄人員簽名或蓋章，於會後二十日內分送委員會各獨立董事成員，並應列入公司重要檔案，於公司存續期間妥善保存；是否將審計委員會之開會過程全程錄音或錄影存證，並至少保存五年。	辦法第 10 條、第 10-1 條
1.9.1	9.其他 (1)票券金融公司負責人及職員，除符合其他法令之兼任情形外，不得兼任他票券金融公司或金融機構任何職務。	票券金融管理法第 11 條第 3 項
1.9.2	(2)票券金融公司之董事、監察人、經理人及持有票券金融公司已發行有表決權股份總數超過百分之十者（包括其配偶、未成年子	票券金融管理法第 10 條第 1 項

項 目 編 號	查 核 事 項	法 令 規 章
1.9.3	<p>女及利用他人名義持有者在內)，應於每月五日以前，將其上月份持股之變動情形通知公司；公司應於每月十五日以前，彙總向主管機關或主管機關指定之機構申報。</p> <p>(3)前項之股票經設定質權者，出質人應即通知公</p>	票券金融管理法第 10 條第 3 項
1.9.4	<p>司；公司應於其質權設定後五日內，將其出質情形，向主管機關或主管機關指定之機構申報。</p> <p>(4)上市上櫃票券金融公司實收資本額達新台幣二十億元以上或外資及陸資持股比率達百分之三十以上者，應於股東會召開前 14 日內申報股東會年報。</p>	票券金融公司公司治理實務守則第 44 條之 1、44 條之 2、44 條之 3、44 條之 4、44 條之 5
2	(二)業務操作制度之查核	票券金融公司年報應行記載事項準則」第 23 條
2.1	1.查庫	

項 目 編 號	查 核 事 項	法 令 規 章
2.1.1	(1)盤點庫存有價證券，其種類、數量、金額是否與保管部門之保管有價證券明細表、交易部門之庫存有價證券明細表及會計部門之日計表帳列數是否相符？是否有保管已出售之票券情形？庫存票據有否以保管收據副本抵充者？	
2.1.2	(2)盤點授信質押擔保品有價證券，其種類、數量、金額是否與保證品明細表及存取備查登記簿相符？	
2.1.3	(3)盤點空白商業本票，其種類、數量是否與登記簿相符？	財 政 部 89.5.17 台 財 融 字 第 89732095 號函
2.1.4	(4)盤點空白銀行支、本票數量是否與明細表相符？	財 政 部 89.5.17 台 財 融 字 第 89732095 號函
2.1.5	(5)盤點總務零用金是否與會計帳列金額相符？	

項 目 編 號	查 核 事 項	法 令 規 章
2.2	2.庫房管理	
2.2.1	(1)庫房鑰匙及密碼是否由不同人員保管？是否會同開庫及關庫？營業時間進出庫房是否實施門禁管理？	1.金融機構安全維護管理辦法第6條第2款第2目 2.財政部 86.1.22 台財融字第86601348號令修正金融機構安全維護注意要點第1點第2項第4款
2.2.2	(2)庫房內外是否裝置自動錄影監視器？錄影帶內容是否清晰並保存一定期限？	1.財政部 86.1.22 台財融字第86601348號令修正金融機構安全維護注意要點第1點第1項第3款 2.金融機構安全維護管理辦法第5條第6、7款
2.2.3	(3)庫房鑰匙及密碼保管人員職務異動，是否將其列入移交？是否即時變更密碼？	票券金融公司安全維護執行規範第10條

項 目 編 號	查 核 事 項	法 令 規 章
2.2.4	(4)銀行保管箱之送存及提領程序控管是否妥當？	
2.3	3.印信章戳管理	
2.3.1	(1)業務部門及交易部門之印鑑(如保證章、簽證章、成交單及承諾書腰形章等)、有權簽章人員私章及重要公司印鑑保管使用是否符合牽制？是否於營業結束後送入金庫妥善保管？	
2.3.2	(2)各式印鑑是否製作列管清冊送交管理部門備查？印鑑保管人或其職務代理人異動時，是否即時更新印鑑列管清冊？	
2.4	4.員工職務、休假及輪調	
2.4.1	(1)每位工作人員有無書面之任務提示？是否經人事主管單位之核定或核備？其任務之分配是否與其組織規程規定一致？是否允	

項 目 編 號	查 核 事 項	法 令 規 章
2.4.2	許彈性之調派？ (2)是否訂定人員工作輪調及休假規範並確實執行？職務代理人之指派及工作內容是否符合牽制原則？	
2.4.3	(3)票券商業務人員應具備資格是否符合票券商負責人及業務人員管理規則之規定？於執行職務前，是否由所屬票券商向票券商公會辦理登記？是否有得撤銷登記之情事者？	票券商負責人及業務人員管理規則 第 13 條、第 14 條
2.4.4	(4)票券商業務人員是否參加票券商公會或其認可之機構或業務人員所屬票券商舉辦之金融相關業務專業職前訓練或在職訓練，並取得合格成績？其中初任及離職滿二年後再任之業務人員，是否於到職後半年內參加職前訓練？在職人員是否於任職期間	票券商負責人及業務人員管理規則 第 13-1 條

項 目 編 號	查 核 事 項	法 令 規 章
2.4.5	<p>參加在職訓練？訓練期間及時數是否符合主管機關規定？</p> <p>(5)公司副總經理、協理或與其職責相當者，是否具備下列資格之一：</p> <p>①票券金融公司或銀行工作經驗五年以上，並曾擔任票券金融公司或銀行總行副經理以上或同等職務，成績優良。</p> <p>②票券金融公司或銀行工作經驗三年以上，並曾擔任票券金融公司或銀行總行經理以上或同等職務，成績優良。</p> <p>③從事資訊、科技、法律、電子商務、數位經濟、財務會計、行銷或人力資源等專業領域之工作經驗十年以上，成績優良者。</p> <p>④有其他事實足資證明其具備票券業專業</p>	票券商負責人及業務人員管理規則第 6 條

項 目 編 號	查 核 事 項	法 令 規 章
2.4.6	知識或經營票券業之能力，可健全有效經營票券金融公司業務，並事先報請主管機關認可。 (5)徵、授信人員每年是否至少進修三小時永續金融相關訓練課程？	中華民國票券金融商業同業公會會員徵信準則第 7 條
2.5	5.空白商業本票	
2.5.1	(1)庫存空白商業本票異動時，是否列印空白商業本票異動表由經辦員核對及主管覆核簽章確認？每月是否定期辦理盤點？	財 政 部 89.5.17 台 財 融 字 第 89732095 號函
2.5.2	(2)營業單位經辦人員領取空白商業本票，是否憑經單位主管簽准之空白商業本票領取單領取？空白商業本票送交客戶，是否請其簽收？是否將簽收單存檔備查？領用單位與核發單位間是否相互勾稽？	財 政 部 89.5.17 台 財 融 字 第 89732095 號函
2.6	6.票、債券交易作業流程之控管	

項 目 編 號	查 核 事 項	法 令 規 章
2.6.1	(1)前、後檯作業是否嚴格劃分？交易員不得兼任交割、會計、資金、保管等工作。	財 政 部 89.5.17 台 財 融 字 第 89732095 號函
2.6.2	(2)買賣紀錄單（或作業單）及成交單是否詳實記錄交易之時間、種類、數量、金額、客戶名稱、承作利率、期間天期、交割方式等並經主管覆核？	1.票券金融管理法第 22 條 2.財政部 90.1.7 台財融（四）字第 0904000270 號令 3. 財政部 92.8.7 台財融（四）字第 0928011208 號令
2.6.3	(3)更改、刪除經系統確認序號之交易，是否由交易員填寫申請書並經交易主管核准辦理？成交單之補印，是否妥善控管？成交單之作廢及補印，日終是否列印電腦報表，供主管人員逐筆勾稽核對？空白成交單是否設簿登記控管？	
2.6.4	(4)首次往來、中途解約及大額交易等是否辦理交易確認？對其他一般交易是否辦理抽樣	

項 目 編 號	查 核 事 項	法 令 規 章
2.6.5	<p>性之交易確認？（如交易對象身分、交易條件、銀行帳號等內容）</p> <p>(5)承銷他保或免保商業本票及首次買入之銀行可轉讓定存單、銀行承兌匯票等，簽辦單是否經有權主管核准？取票、驗印及撥款是否嚴格控管？是否有作抽樣性之交叉確認？由非金融機構首次買入之銀行可轉讓定存單，是否徵提購買證明書？</p>	
2.6.6	<p>(6)承銷自保商業本票案件，額度動用請核書是否確實審核，並經有權主管核准？取票、驗印及撥款是否嚴格控管？</p>	
2.6.7	<p>(7)票券簽證承銷手續尚未完成，是否提前於次級市場賣出？取回簽證完成次營業日承銷之票券，日終是否交付保管人員簽收入庫保管？是否有客戶預蓋發行印鑑之空白商</p>	

項 目 編 號	查 核 事 項	法 令 規 章
2.7	業本票存庫情形？ 7.資金收付作業	
2.7.1	(1)資金人員執行交易資金收付，確認資金序號，新增或更改客戶銀行帳號是否有適當之控管？非交易資金收付是否亦有妥適之控管？	
2.7.2	(2)資金收付清單之作廢，日終是否列印報表供主管人員逐筆勾稽核對？	
2.8	8.支、本票簽發作業	
2.8.1	(1)支票簽發人員列印支、本票，抬頭人之更改是否有嚴格控管措施？支、本票之使用及作廢，日終是否列印使用記錄表，供主管人員逐筆勾稽核對？人工方式取消或更改抬頭及劃線是否嚴格限制？	
2.8.2	(2)庫存空白銀行支、本票是否定期盤點？由銀	財 政 部 89.5.17 台 財 融 字 第

項 目 編 號	查 核 事 項	法 令 規 章
2.9	行領用空白支、本票，是否有妥適之控管？	89732095 號函
2.9.1	9.交割作業 (1)派員交割是否留存交割紀錄並經主管覆核？交割人員是否兼任其他互相牽制之工作？非交割人員支援交割是否訂定辦法妥適管理？郵寄交割是否由交寄人簽收並留存大宗掛號清單備查？	
2.9.2	(2)承銷商業本票是否嚴格限制交易員擔任本身承作交易之交割取票工作？客戶郵寄或臨櫃交付商業本票是否有設簿登記控管？	
2.10	10.保管作業	
2.10.1	(1)是否依據賣出成交單取出票券，並核對保管收據正、副本、委託保管申請書及委託保管紀錄表是否相符？	
2.10.2	(2)執行整批列印暨簽署保管收據及債券存摺	

項 目 編 號	查 核 事 項	法 令 規 章
2.10.3	<p>及作廢、刪除、補印之作業程序是否有妥適之控管？</p> <p>(3)票券及實體債券送存之保管送存明細表是否由委託、受託雙方核對無誤後，簽章收存？受託保管銀行之銀行保管專用印鑑章是否正確？</p>	
2.10.4	<p>(4)未到期之保管收據副本是否妥善控管？空白保管收據是否按流水號碼順序設簿登記控管每日使用起訖及作廢號碼？經辦人及主管是否核對簽章？</p>	
2.10.5	<p>(5)提領保管到期之票、債券，是否核對票債券保管提取明細表與保管收據副本內容？領回交付保管人員入庫保管，是否有點收？</p>	
2.10.6	<p>(6)提領未到期之票、債券，是否有嚴格限制？客戶辦理中途解約，是否交付保管收據正</p>	

項 目 編 號	查 核 事 項	法 令 規 章
2.10.7	本或出具切結書辦理？ (7)委託銀行保管票、債券是否定期列印辦理對帳？是否由保管銀行有權人保管專用章簽章確認？	
2.10.8	(8)票券賣出或買進依成交單指定自行保管，是否核對票面金額、組合、發行日、到期日、每萬元單價與現券是否相符？交割人員取出交割是否簽名？	
2.10.9	(9)每日交易完成是否列印短期票券庫存明細表？是否核對庫存有價證券與明細表列出之面額、發票人、發票日、到期日、面額之組合無誤後，有權人簽章覆核無誤入庫保管？	
2.10.10	(10)票券商承銷及首次買入之債票形式短期票券，是否即時送存實券保管銀行（合作金	短期票券發行登錄集中保管帳簿劃撥作業辦法第 17 條

項 目 編 號	查 核 事 項	法 令 規 章
2.11	庫銀行)集中保管?是否經對方有權簽章人簽收確認?是否發送「送存訊息」至票券結算交割保管系統,與集保結算公司及實券保管銀行進行比對?	
2.11.1	11.會計作業 (1)會計帳日結後之交易操作是否嚴格限制? 分公司會計帳日結上傳總公司後,改帳操作是否妥適控管?	
2.11.2	(2)銀行存款帳戶是否每月定期辦理對帳?差異數是否編製銀行往來調節表?	
2.12	12.總、分公司間代辦往來事項 總、分公司間代辦往來,是否有妥適之控管措施?委託撥款予客戶,是否經雙方有權通話人確認相關資料後辦理?	
2.13	13.商業本票之兌償	

項 目 編 號	查 核 事 項	法 令 規 章
2.13.1	(1)自保商業本票到期兌償，除發票人信用不良外，是否嚴格限制以票易票？是否訂定以票易票管理辦法？以票易票未提示屆期之商業本票是否由業務部門點收及作廢？	
2.13.2	(2) 集中保管商業本票之兌償，是否將款項存（匯）入合作金庫銀行營業部之兌償專戶？若到期續發金額小於原到期金額，客戶是否將差額補足？	
2.14	14.授信押品管理	
2.14.1	(1)授信副擔保品託收客票之點收，是否與票據明細表核對並輸入電腦建檔？是否當日送存銀行備償專戶託收？是否定期補摺，並將已收妥入帳之客票辦理銷帳？客戶申請領回備償專戶存款，是否憑申請書辦理？	

項 目 編 號	查 核 事 項	法 令 規 章
2.14.2	<p>退票是否立即通知客戶補票或重行提式？</p> <p>撤票領回是否由客戶簽收？</p> <p>(2)客票異動時列印之客票副擔保餘額核對作業報表、託收票據到期未銷帳簡表及備償客票金額變動明細表是否確實核對並相互勾稽？</p>	
2.14.3	<p>(3)質押擔保品有價證券保管袋是否由保管人員與業務人員會封簽章入庫保管？保證品送存及提領作業是否有妥適之控管？押品收據是否設簿登記控管？客戶取回押品，押品收據是否取回註銷並加蓋「作廢」章？</p>	
2.15	<p>15.寄發對帳單</p> <p>是否每月定期核發寄送對帳單？是否留存郵寄清單紀錄備查？客戶回覆是否辦理追蹤？</p>	

項 目 編 號	查 核 事 項	法 令 規 章
2.16	16.客戶開戶暨基本資料建檔 客戶開戶及基本資料建檔作業是否有適當之控管措施？客戶銀行帳號、通訊地址、聯絡人等基本資料變更，是否辦理交叉確認？	
2.17	17. 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「票券金融公司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。	
2.18	18.認識客戶作業之查核	
2.18.1	(1)票券商以營業人身分辦理衍生性金融商品業務	
2.18.1.1	①票券商以營業人身分辦理衍生性金融商品交易，是否區分客戶為「專業客戶」及「一	

項 目 編 號	查 核 事 項	法 令 規 章
2.18.1.2	<p>般客戶」。</p> <p>②票券商對一般客戶提供衍生性金融商品交易服務，是否建立瞭解客戶程序及客戶屬性評估，以確實知悉客戶之投資經驗、財產狀況、交易目的及商品理解等特性；客戶投資屬性與其從事之衍生性金融商品交易是否適當。</p>	
2.18.1.3	<p>③票券商提供衍生性金融商品交易服務，是否向客戶揭露各項費用及其收取方式、交易架構及可能涉及之風險等相關資訊。</p>	
2.18.1.4	<p>④對一般客戶及屬自然人之專業客戶提供衍生性金融商品交易服務，是否提供風險預告書，其內容是否包括投資風險警語及商品風險說明。</p>	
2.18.1.5	<p>⑤產品說明書是否記載下列事項：</p>	

項 目 編 號	查 核 事 項	法 令 規 章
2.18.1.6	<p>I.重要事項摘要，包括商品中文名稱、以顯著字體標示商品風險，及客戶應詳閱產品說明書內容並注意商品之風險事項。</p> <p>II.商品或交易條件、最大可能損失及情境說明。</p> <p>III.各項費用及交易程序處理說明。</p> <p>⑥交易條件如有提前到期約定，是否載明提前到期之條件或說明票券金融公司得提前到期之權利、結算應付款數額之金額或計算方式。</p>	
2.18.1.7	<p>⑦以文字或情境分析解說最大可能獲利，及最大可能損失，是否加註情境分析結果不保證未來績效。</p>	
2.18.1.8	<p>⑧票券商提供衍生性金融商品服務是否說明</p>	

項 目 編 號	查 核 事 項	法 令 規 章
2.18.1.9	商品最低投資金額及投資金額給付方式； 是否說明客戶應負擔的各項費用與其收取方式。	本 會 107.10.15 金 管 銀 票 字 第
2.18.1.10	⑨客戶依契約規定得提前終止交易者，票券商是否說明終止交易時得領取金額之計算方式及給付方式；是否載明交易糾紛申訴管道。	
2.18.1.11	⑩風險預告書之投資風險警語，是否置於明顯易見之處，並以粗黑字體記載。	
2.18.1.12	⑪票券金融公司與一般客戶完成衍生性金融商品交易後，是否提供交易確認書（應包含交易確認書編號）及對帳單予客戶。	
2.18.1.13	⑫內部稽核單位是否將認識客戶作業納入年度稽核計畫並確實執行。	
	⑬以營業人身分經營外匯衍生性金融商品	

項 目 編 號	查 核 事 項	法 令 規 章
2.18.2	業務相關人員是否符合資格條件及在職訓練，是否依「銀行業辦理外匯業務管理辦法」第 14 條規定辦理。	10701139150 號
2.18.2.1	(2)防制人頭戶之查核作業 ①受理客戶交易時，是否於於首次交易日(含)前，徵提相關證明文件（個人戶應檢附身分證明文件親自辦理，法人戶則應檢附合法登記證明文件及負責人身分證明文件）；個人戶及法人戶負責人身分證明文件是否至內政部戶役政為民服務公用資料庫網站查核其國民身分證領補換資料；對查核及查詢結果是否予以影印留存。	票券金融公司防制人頭帳戶汜濫應注意事項範本
2.18.2.2	②客戶本人或其負責人因故無法親自辦理，	

項 目 編 號	查 核 事 項	法 令 規 章
2.18.2.3	而以書面委託第三人代辦時，對於委託書及委託事項是否為必要之查證；若查證有困難時是否予以婉拒。	
2.19	③對首次交易客戶所提供之往來銀行帳戶，是否即與銀行核對確認其帳號、戶名是否屬實。	
2.19.1	19.其他 (1)是否依據「票券金融管理法」第 25 條、「個人資料保護法」及「銀行法」第 48 條規定並參照其他相關規定（如金融機構資訊系統安全基準、金融業個人資料檔案安全維護計畫標準、金融機構辦理電子銀行業務安全控管作業基準等），訂定有關客戶交易資料安全及保密之規範？票券金融公司依「票券商提供客戶財務業務或交易有關資	1.票券金融管理法第 25 條 2.個人資料保護法 3.銀行法第 48 條 4.票券商提供顧客財務業務或交易有關資料規定第 3 點

項 目 編 號	查 核 事 項	法 令 規 章
2.19.2	料規定」提供客戶資料，是否以密件處理，並提示查詢機關應予保密？ (2)新進或在職人員教育訓練內容是否包括客戶交易資料安全及保密？	金融機構作業委託他人處理內部作業制度及程序辦法第4條
2.19.3	(3)有關金融聯合徵信中心信用資訊之查詢，是否有嚴格控管措施？是否定期列印查詢記錄留存，並與查詢申請書相互勾稽？	
2.19.4	(4) 是否訂定委外事項內部作業規範並經董事會核定？內容應包括：作業委外之政策及原則、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。是否訂定緊急應變計畫？票券金融公司是否確認對方能確保資料接觸者不外洩客戶資料，且不得為其他不當利用行為？是否就	

項 目 編 號	查 核 事 項	法 令 規 章
2.19.5	<p>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？董事會是否定期監督委外事項執行情形？是否有適當之盡職調查及定期審查程序？</p> <p>(5)個人資料檔案安全維護之查核 (註：應於 103.4.30 前調整作業程序，並於 103.4.30 前將執行情形送公會彙辦)</p>	102.11.8「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」
2.19.5.1	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。	
2.19.5.2	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	

項 目 編 號	查 核 事 項	法 令 規 章
2.19.5.3	風險、訂定適當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。	
2.20	20.金融消費者保護之查核	
2.20.1	(1)票券商與金融消費者訂立提供金融商品或服務之契約前，是否充分瞭解金融消費者之相關資料及依不同金融商品或服務之特性，建立差異化事前審查機制，以確保該商品或服務對金融消費者之適合度；是否向金融消費者充分說明該金融商品、服務及契約之重要內容，並充分揭露其風險。	1.金融服務業確保金融商品或服務適合金融消費者辦法 第 2 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 2 條及第 5 條
2.20.2	(2)票券商與金融消費者訂立契約時，是否有適當之單位及人員審核簽約程序及金融消費者所提供資訊之完整性後，始得辦理；另	1.金融服務業確保金融商品或服務適合金融消費者辦法 第 2 條 2.金融消費者保護法第 8 條第 3 項

項 目 編 號	查 核 事 項	法 令 規 章
2.20.3	<p>票券商是否不得藉金融教育宣導，引薦個別金融商品或服務。</p> <p>(3)票券商說明金融商品或服務契約之重要內容及揭露風險，是否遵守下列基本原則：</p> <p>①應本於誠實信用原則，並以金融消費者能充分瞭解之文字或其他方式為之。</p> <p>②任何說明或揭露之資訊或資料均須正確，所有陳述或圖表均應公平表達，並不得有虛偽不實、詐欺、隱匿、或足致他人誤信之情事，上述資訊或資料應註記日期。</p> <p>③銷售文件之用語應以中文表達，並力求淺顯易懂，必要時得附註原文。</p> <p>④所有銷售文件必須編印頁碼或適當方式，俾供金融消費者確認是否已接收完整訊息。</p>	<p>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</p>
2.20.4	<p>(4)票券商提供金融商品或服務，是否按金融商</p>	<p>金融服務業提供金融商品或服務前</p>

項 目 編 號	查 核 事 項	法 令 規 章
2.20.5	品或服務之性質於公開說明書、投資說明書、商品說明書、風險預告書、客戶須知、約定書、申請書或契約等說明文件，或經由雙方同意之網際網路或其他約定方式，說明及揭露重要內容 及可能涉及之風險資訊，並以顯著字體或方式表達；是否留存相關資料；依其他法令規定應錄音錄影者，是否依其規定辦理。	說明契約重要內容及揭露風險辦法第 7 條及第 9 條
	(5)金融服務業提供之金融商品屬複雜性高風險商品者，除以電子設備形式留存作業過程軌跡外，是否依金融消費者保護法第十條第四項規定錄音或錄影；錄音或錄影內容是否至少保存該商品存續期間加計三個月之期間；如未滿五年，是否至少保存五年以上但發生金融消費爭議時；是否保存至該爭議終結為止。	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 9 條
	(6)是否建立「消費爭議處理制度」，並納入下	本會銀行局 113.8.5 銀局（合）字第

項 目 編 號	查 核 事 項	法 令 規 章
2.21	<p>列事項：</p> <p>①對於消費爭議案件之處理，建立以風險為導向之升級陳報機制，並確認申訴態樣之根本原因，適時提出因應作為。</p> <p>②指定專責部門或人員處理消費爭議案件，並提升督導層級至副總經理。</p> <p>③明定受理爭議案件之回應方式，並提供金融消費者查詢爭議案件處理進度之管道。</p> <p>21.辦理不動產授信業務之查核，是否將下列事項納入內部控制制度及作業程序？</p> <p>(1)辦理授信限額控管，是否有歸類錯誤或實際應歸屬不動產業者未予歸入不動產業授信？</p> <p>是否依規定納入對非不動產業之保證，其資金使用係提供集團從事不動產業之關係企業使用者？</p>	<p>1130220584 號函</p> <p>本 會 110.12.17 金 管 銀 票 字 第 11002742782 號令</p>

項 目 編 號	查 核 事 項	法 令 規 章
	<p>(2)辦理不動產授信業務，是否確實評估土地開發興建計畫合理性及建案開發期程？</p> <p>(3)對授信戶所提供徵信資料，是否檢視其真實性及合理性？是否調查聯保人是否有其他財產？</p> <p>(4)辦理不動產擔保品之鑑估，是否參考鄰近地區其他類似案例最近成交價格？或對鑑估單價高於鄰近地區其他類似案例之成交價或實價登錄價格，是否分析差異原因並說明採較高鑑估價格之理由？或短期內對相似擔保品之鑑估單價差異大者，是否有合理說明？</p> <p>(5)辦理建商餘屋擔保授信，於授信額度屆期辦理續約時，對所徵擔保品均未售出，是否降低授信風險之機制(如提高利率或降低貸款成數等)？</p> <p>(6)對洽徵大量大樓地下室停車位為擔保品，是否分析擔保品所在區域對停車位之需求及</p>	

項 目 編 號	查 核 事 項	法 令 規 章
	評估停車位未搭配房屋單獨出售之難易程度？	
	(7)對以提供餘屋為擔保品申貸營運週轉金借款案件，授信戶近年無營業收入，且連年虧損，是否評估餘屋所在區域市場性及擔保品未來處分難易程度，並分析餘屋未來去化速度？	
3	(三)資訊作業之查核	
3.1	1.資訊單位查核	
3.1.1	(1)組織與管理	
3.1.1.1	①內部組織與職務分工	
3.1.1.1.1	I.資訊單位是否獨立於其他部門？	100.11.23 金 管 銀 國 字 第
3.1.1.1.2	II.是否有高階人員組成資訊作業推動小組負責審議、核准或督導、協調下列事項？	10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8
3.1.1.1.2.1	A.資訊作業重要規章。	月修訂「金融機構資訊系統安全基準」：營運基準(一)-3「為使資訊系統
3.1.1.1.2.2	B.資訊作業中、長期計畫。	順利運轉，應明確訂定劃分責任與權
3.1.1.1.2.3	C.資訊作業安全控管措施。	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.1.1.2.4	D.重要軟硬體系統購置、更新。	限之規章。」
3.1.1.1.2.5	E.資訊作業預算。	
3.1.1.1.2.6	F.資訊作業成本效益評估。	
3.1.1.1.2.7	G.重要專案之進度及目標達成情形。	
3.1.1.1.3	III.是否有明確資訊單位各科（組）職掌訂定？各科（組）權責是否有重疊情形？人員配置是否適當？	
3.1.1.1.4	IV.下列工作有無適當之職責分工？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(一)-2-運 9「為使資訊系統運轉順利，並防止非法事件發生，應有適當之職務分工，明確劃分業務範圍及責任、權限，以確定相互制衡體制。」
3.1.1.1.4.1	A.應用系統分析與設計。	
3.1.1.1.4.2	B.系統軟體建置與維護。	
3.1.1.1.4.3	C.電腦主機操作。	
3.1.1.1.4.4	D.連線管理(安全控管)。	
3.1.1.1.4.5	E.作業或資料管制。	
	若無，有無配合之控管措施？	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.1.1.5	V.對各項業務（工作）是否有人可代理？	本 會 111.5.16 金 管 銀 票 字 第 11101302162 號 令
3.1.1.1.6	VI.票券金融公司是否配置適當資訊安全人力資源及設備？ A. 票券金融公司上一會計年度決算後淨值達新台幣一百億元以上且資產總額達新台幣一千億元以上者，應指派副總經理以上或職責相當之人兼任資訊安全長，並配置資訊安全主管及資訊安全人員。 B. 未達規模者，應配置資訊安全主管及資訊安全人員。 C. 上述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。	
3.1.1.1.7	VII.票券金融公司資訊安全主管及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	

本會 111.5.16 金管銀票字第
11101302162 號令
「金融控股公司及銀行業內部控制

項 目 編 號	查 核 事 項	法 令 規 章
	<p>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 27 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(無資訊安全長者，由資訊安全主管)聯名出具。</p> <p>②管理辦法及作業規範之訂定</p> <p>I.為健全資訊作業制度，是否分別或綜合訂定下列有關規範？以作為資訊作業操作、管理、查核之依據：</p> <p>A.有關係統文件標準化之規範。</p> <p>B.有關係統開發、維護規範。</p> <p>C.有關電腦軟硬體系統及其附屬設施之管理規範。</p> <p>D.有關係統操作之一般規範。</p> <p>E.有關批次作業處理操作規範。</p> <p>F.有關程式及資料檔案管理及維護規範</p>	<p>及稽核制度實施辦法」第 38 條之 1 第 1 項但書所稱主管機關對票券金融公司辦理資訊安全之解釋令</p> <p>100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-1「為能正確安全運用資訊系統，日常各種作業處理程序等應標準化，並備妥完整之作業手冊。同時，對於系統故障或災害發生時，為使對系統之影響減至最小，並能在最短時間內復原系統，應明確訂定故障或災害發生時之系統操作程</p>
3.1.1.2		
3.1.1.2.1		
3.1.1.2.1.1		
3.1.1.2.1.2		
3.1.1.2.1.3		
3.1.1.2.1.4		
3.1.1.2.1.5		
3.1.1.2.1.6		

項 目 編 號	查 核 事 項	法 令 規 章
3.1.1.2.1.7	G.有關媒體管理規範。	序，整理完整之操作手冊。」
3.1.1.2.1.8	H.系統故障對策及災變因應措施。	
3.1.1.2.1.9	I.有關委外作業之管理規範。	
3.1.1.2.1.10	J.有關內部工作分配及其管理之規範。	
3.1.1.2.1.11	K.有關內部自行查核之規範。	
3.1.1.2.2	II.前述規範有關操作、管理、查核等各方面之規定是否完整？是否付諸實施，並適時檢討、修訂？	
3.1.1.2.3	III.工作計畫之訂定	
3.1.1.2.3.1	A.有無訂定電腦軟硬體、人力配置及資訊作業之短、中、長期計畫，並經該機構最高階主管核定？	
3.1.1.2.3.2	B.所訂計畫項目是否符合業務上之需求？	
3.1.2	(2)安全控制	
3.1.2.1	①環境安全防護	
3.1.2.1.1	I.電腦設備及相關設施之安全防護是否完	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.2.1.1.1	善？ A.是否有完善的防火、防水、防震、防犯（如機房自動門禁控制系統）及不斷電設備等安全防護措施？	
3.1.2.1.1.2	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？	
3.1.2.1.1.3	C.有無裝置火災自動警報系統及自動滅火設備？	
3.1.2.1.1.4	D.對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？	
3.1.2.1.1.5	E.保險及維護契約涵蓋範圍是否完全？並在有效期間內？	
3.1.2.1.2	II.機房是否放置非工作需要或危險物品？	
3.1.2.1.3	III.電腦媒體存放場所是否有防火、防水、防塵等安全防護措施？是否注意溫、濕度？	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.2.1.4	IV.系統說明文件存放場所是否有防火、防水等安全防護措施？	
3.1.2.2	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是否加以嚴格管制？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100年8月修訂「金融機構資訊系統安全基準」：營運基準(二)-1「為防止非法入侵、攜入危險物品、非法攜出物品等，對進出資訊中心或電腦機房等重要房間（館或室）之人、物，應加以管制。」
3.1.2.3	③備援措施	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100年8月修訂「金融機構資訊系統安全基準」：技術基準一-(一)-2 技 2「重要
3.1.2.3.1	I.電腦設備及相關設施是否有備援主機、週邊設備、網路傳輸設備、端末設備等及相關設施（如空調、電力、不斷電設備等）？或其他因應措施，如：與廠商簽訂備用契約或與	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.2.3.2	同類機器使用者互相締結支援契約？	之主機設備應設置備援設備」、技 3 「重要之周邊裝置應設置備援設備」、技 4「重要之通訊裝置應設置備援設備」、技 5「重要之通訊線路應設置備用線路」、技 6「端末系統裝置應設置備援設備」
3.1.2.3.2.1	II.程式及資料檔案 A.對重要或需要長期保留檔案（含應用、系統程式及資料檔等）是否有備份？備份媒體是否使用具有防火、防濕、防磁等之設備異地存放？安全措施是否嚴密？有無隨時更新？	
3.1.2.3.2.2	B.各種重要程式及資料檔案是否有損毀時之重建程序？	
3.1.2.3.3	III.人員 各項重要工作是否均有備援人員？	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.2.3.4	IV.系統說明文件 各項系統開發、設計或作業處理程序之說明文件，如以媒體型態儲存，是否備份異地妥為存放？	
3.1.2.4	④故障及災害因應對策	100.11.23 金 管 銀 國 字 第
3.1.2.4.1	I.是否分別或綜合訂定電腦軟硬體系統故障時之復原程序、使用備援系統之轉換程序或故障期間之權宜應變作業方式？	10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-24「為將資訊系統故障與災變對顧客、總行、營業單位之影響降至最低，同時儘早完成復原作業，應訂定故障災變之因應對策。」及營運基準(三)-25「於資訊系統發生故障或災害時，為使相關業務能在短時間內回復正常運作，應以假設事件為基礎，擬定災害備援作業計畫（緊急應變計畫）。」

項 目 編 號	查 核 事 項	法 令 規 章
3.1.2.4.2	II.前述故障復原程序，使用備援系統之轉換程序，或權宜應變之作業方式，是否定期或不定期辦理測試、演練？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-25-運 65 之 3-(7)「確立計畫之持續管理體制，實施定期之演練及訓練，須依演練之結果，檢討計畫內容，適時修正計畫內容，以符合實際需要。」
3.1.2.4.3	III.是否訂有災害應變計畫以處理各種可能之意外（狀況），俾能在最短時間內及最低成本下，恢復電腦作業功能？	
3.1.2.4.4	IV.應變計畫是否經最高主管批准？有無每年定期演練？有關人員是否確知在災害中應扮演之角色及責任？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8

項 目 編 號	查 核 事 項	法 令 規 章
3.1.3	(3)系統開發及維護控制	月修訂「金融機構資訊系統安全基準」營運基準(六)-1-運 84「為預防緊急狀況發生，應實施防災、防犯演練。」
3.1.3.1	①系統開發控制	1.100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國
3.1.3.1.1	I.若訂有系統開發、維護規範(standards)，是否包括下列項目，以作為系統開發、維護及文件製作之標準：	銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：技術基準(二)-1-技 9「為在設計階段提升軟體的可靠性，開發前提應明確化，同時考量具可靠性設計、採標準化之設計作業等，確保軟體的品質。」
3.1.3.1.1.1	A.系統開發／設計程序。	2.100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國
3.1.3.1.1.2	B.套裝軟體選擇基準。	銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安
3.1.3.1.1.3	C.程式設計標準。	
3.1.3.1.1.4	D.程式及系統測試方法及標準。	
3.1.3.1.1.5	E.實施（轉換）事宜。	
3.1.3.1.1.6	F.系統文件撰寫規格。	
3.1.3.1.1.7	G.系統/程式異動管理。	
3.1.3.1.1.8	H.系統評估。	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.3.1.2	II.系統開發是否依可行性研究、系統分析、系統設計、程式撰寫、系統測試及系統轉換之標準開發步驟進行？	全基準」：營運基準(四)-2「為確保系統開發及其內容變更之正確性，兼顧系統之安全性，應明確訂定系統開發、變更之作業程序、測試環境之建置等整合性之管理機制。」 3.100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」貳-(貳)-二-(四)運 70「為使開發及變更作業順利，應將在系統開發及變更各階段所使用之文件格式予以標準化。」 個人資料保護法第 5 條
3.1.3.1.3	III.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？	
3.1.3.1.4	IV.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？	
3.1.3.1.5	V.系統之開發、設計，對於個人資料之蒐集、處理及利用，有無逾越特定目的之範圍或妨害當事人之權益？是否與蒐集之	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.3.1.6	目的具有正當合理之關聯？ VI.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？	
3.1.3.1.7	VII.對於各項應用系統之控制設計，是否有徵求稽核人員意見，並於設計中考量？各項控制設計是否周延？	
3.1.3.1.8	VIII.各項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整之測試？其測試結果是否均經相關主管覆核？是否由使用單位作接受性測試？	
3.1.3.1.9	IX.作業實施前轉換計畫是否完妥並經確實執行？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(四)-2-運 69「確保正

項 目 編 號	查 核 事 項	法 令 規 章
3.1.3.1.10	X.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需求（功能）等，皆加以確實驗收？	式作業系統之安全，轉入正式作業時應明確規定其轉換程序。」
3.1.3.1.11	XI.系統實施時，是否訂定妥適的雙軌作業期間及經確認新系統之可靠性後才正式啟用？	
3.1.3.1.12	XII.已正式實施之系統，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，並作為開發其他新系統之參考？	
3.1.3.1.12.1	A.業務電腦化後，操作、管理與查核上尚待加強、改進者。	
3.1.3.1.12.2	B.系統控制功能設計之完整性。	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.3.1.12.3	C.程式及檔案資料修改頻率與原因之分析。	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100年8月修訂「金融機構資訊系統安全基準」：技術基準(二)-2-技15「在功能變更、新增作業時，為能確保程式的品質，應比照開發時提昇品質之對策。」
3.1.3.1.12.4	D.輸出報表之實用性、完整性。	
3.1.3.1.12.5	E.實際開發時間、人力、成本與原計畫之比較分析。	
3.1.3.2	②系統維護控制	
3.1.3.2.1	I.對每一應用系統，是否均派專人負責維護的工作？	
3.1.3.2.2	II.修改系統時，是否採取足夠的控制，以免修改人員接觸未經許可修改之部份？	
3.1.3.2.3	III.系統如需重大變更時，是否比照開發新系統之程序，由有關單位參與研討變更內容、範圍，並參與驗收？	
3.1.3.2.4	IV.已正式實施之作業，其程式變更：	
3.1.3.2.4.1	A.是否有書面申請，並經相關部門（使用單位、資訊單位）主管核准後方才修正？	
3.1.3.2.4.2	B.書面申請是否詳細敘明變更原因及內	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.3.2.4.3	容？ C.修改後是否加以測試（含第三者），並經主管審核其測試結果？對修改前後程式是否由換版人員利用公用程式作比對，並列印差異報表送主管審核？	
3.1.3.2.4.4	D.系統說明文件是否配合修正？	
3.1.3.2.4.5	E.操作程序上如有變更是否通報有關單位？	
3.1.3.3	③系統文件編製	1.100.11.23 金 管 銀 國 字 第
3.1.3.3.1	I.對已實施之系統是否有下列文件：	10000372210 號函核復，中華民國
3.1.3.3.1.1	A.系統需求分析報告。	銀行商業同業公會全國聯合會100
3.1.3.3.1.2	B.系統設計說明書。	年8月修訂「金融機構資訊系統安
3.1.3.3.1.3	C.程式設計說明書。	全基準」；營運基準(三)-9「為預防
3.1.3.3.1.4	D.操作說明（含批次作業及端末使用者操作說明）。	文件之不當使用或遺失等，應由專
3.1.3.3.1.5	E.測試計畫書（含測試報告及測試記錄）。	人按規定辦法管理之。」 2.100.11.23 金 管 銀 國 字 第

項 目 編 號	查 核 事 項	法 令 規 章
3.1.3.3.1.6	F.系統轉換計畫書。	10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100年8月修訂「金融機構資訊系統安全基準」；營運基準(四)-3-運71「為防止竄改及不當使用等，應訂定規格書等設計文件之保管方法。」
3.1.3.3.1.7	G.系統驗收紀錄。	
3.1.3.3.1.8	H.與有關單位研討之會議紀錄。	
3.1.3.3.2	II.各項系統說明文件或紀錄文件（如軟硬體系統變更申請單等）是否指定專人妥善整理與保管？調閱是否均經登記？	
3.1.3.3.3	III.前述文件如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，並留存紀錄備查？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100年8月修訂「金融機構資訊系統安全基準」營運基準(八)-1運87「系統開發、營運等委外處理，應事先明確訂定作
3.1.3.3.4	IV.系統說明文件之撰寫及程式、檔案名稱之命名是否標準化？	
3.1.3.4	④系統委外開發作業管理	
3.1.3.4.1	I.系統之開發或維護委外作業時，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？	
3.1.3.4.2	II.上述業務之委外作業，其開發、維護之預	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.3.4.3	定進度及作業安全、委託內容、機密維護、損害賠償等雙方權責之劃分，是否明訂於委外作業契約內？ III.委外作業業務是否有專人管理，並控制進度？	業目標及其範圍」、運87-1「以明確之程序選擇委外廠商」、運88「委託契約內容應包含安全政策等相關事項...應包含保密、安全與稽核條款」
3.1.3.4.4	IV.是否嚴禁委外作業廠商進入正式作業環境存取程式或資料？	100.11.23 金 管 銀 國 字 第
3.1.3.4.5	V.是否建立適當程序以檢核委外作業廠商修改程式內容係屬適當？並指定專人負責監控廠商維護活動？	10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100年8月修訂「金融機構資訊系統安全基準」：營運基準(三)-3「為防止電腦系統之非法使用，並求運轉順利，有關操作應實施申請、核可、執行、記錄、結果之確認等管理。」
3.1.3.4.6	VI.若廠商可透過電話線路撥接至受檢單位電腦診斷及維護系統，受檢單位是否建立適當程序以控制廠商存取範圍，並由電腦自動留存作業紀錄以供查核？	
3.1.4	(4)運作管理	
3.1.4.1	①主機操作管理	
3.1.4.1.1	I.控制台及週邊設備（磁碟機、磁帶機、列	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.1.2	表機等)是否僅限輪值操作員操作? 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?	100.11.23 金 管 銀 國 字 第 10000372210 號函核復,中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」營運基準(三)-3「為防止電腦系統之非法使用,並求運轉順利,有關操作應實施申請、核可、執行、記錄、結果之確認等管理。」、營運基準(三)-1-運 14「為正確且安全運轉資訊系統,應規定日常各種程序之作業手冊。」
3.1.4.1.3	III.每班作業是否至少有二名操作員輪值?對正常上班時間以外之留守人員是否注意牽制?	
3.1.4.1.4	IV.除例行作業外,假日及夜間使用正式電腦作業系統是否先經核准?	
3.1.4.1.5	V.例行性作業是否按預定的排程來處理?非例行作業是否均經申請核准?	
3.1.4.1.6	VI.作業排程是否妥當?若非自動排程是否有書面之排程表?對工作執行情形及結果有否留存紀錄?異常情形有否查核追蹤?	
3.1.4.1.7	VII.執行可直接變更目的程式及資料檔案等	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.1.8	之公用程式(utility programs)是否先經核准並留存紀錄？ VIII.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？	
3.1.4.1.9	IX.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？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(五)-3-運 79「為早期發現異常情況，應建立監控機制，訂定監控標的及監控方法等。」
3.1.4.1.10	X.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？	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.1.11	XI.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？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-19「為避免由於各種資源（構成電腦系統之硬體、系統軟體、應用軟體及各類檔案）之性能或容量極限所引起之事故或處理能力之下降，應實施各種資源之管理。」
3.1.4.2	②端末機使用管理	
3.1.4.2.1	I.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？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-2-運 16、運

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.2.2	II. 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?	17、運18「明確訂定各種資源、系統等之存取權限。」、「採取防止密碼外洩之措施。」、「明確訂定存取權限之授予及評估等作業程序。」
3.1.4.2.3	III. 使用者密碼是否可由使用者自行變更? 是否有限制最少字元(以超過 7 個字元為宜)? 是否有控制密碼有效期限及不得變更為前幾次使用過之密碼? 是否以亂碼儲存並控制不得以明碼輸出或顯示?	
3.1.4.2.4	IV. 系統最高權限使用者密碼，是否分人各持一半並密封妥善保管，如有拆封使用是否確實登記並隨即變更? 是否由系統自動留存作業紀錄俾供查核?	
3.1.4.2.5	V. 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?	

100.11.23 金 管 銀 國 字 第
10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.2.6	VI.由端末設備存取主機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？	<p>準」營運基準(三)-12-運 39「操作人員作業卡為操作端末設備時，確認其操作權限之方法，涵蓋鑰匙、通行碼、識別碼等。」</p> <p>100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-2「為防止資訊系統、檔案等各種資源遭非法使用或破壞，應依系統重要程度設定其存取使用權，並加以管理。」</p>
3.1.4.2.7	VII.對於調離職人員，是否立即取消其使用者代號、密碼並收繳其作業卡？	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.3	③輸入、輸出資料管制	
3.1.4.3.1	I.對業務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。	
3.1.4.3.2	II.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？	
3.1.4.3.3	III.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，始有限送出？	
3.1.4.4	④程式、資料檔案管理	100.11.23 金 管 銀 國 字 第
3.1.4.4.1	I.系統程式及應用程式之登錄與維護是否指定專人負責？其登錄與維護是否均經申請、核可及覆核程序，並留存紀錄？	10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100年8月修訂「金融機構資訊系統安全基
3.1.4.4.2	II.程式之登錄、變更程序是否能控制同一程式在程式館內之原始碼(source code)及目	準」：營運基準(三)-5-運25「為防止資料檔案之不當使用、篡改、毀損及

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.4.3	<p>的碼(object code)為同一版本？</p> <p>III.在特殊情況下，對正式作業檔案資料之更正是否以書面申請，並經核准？電腦是否留存完整之更正紀錄（內容），可憑以查核所有更正皆經申請、核可程序？</p>	<p>遺失等，其授受及保管，應由專人按規定辦理。」</p> <p>100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-5-運 26「為防止非法使用或篡改，凡資料檔案之修改，應先取得部門負責人之核准後按規定辦理，並驗證其辦理之結果。資料檔案修改紀錄，亦應依重要程度規定其保存期限。」</p>
3.1.4.4.4	IV.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	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.4.5	<p>使用？</p> <p>V.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，評估其存取權限控制是否嚴謹？</p>	<p>100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：技術基準二-(一)-2-技 31「檔案應設置存取控制（Access Control）的功能。」</p>
3.1.4.4.6	<p>VI.對重要或機密性之檔案是否採亂碼化措施加以保護，以防止不法之使用？</p>	<p>100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：技術基準二-(一)-1-技 28「為防止檔案遭複製或竊取等資料外洩，應對重要資料採用亂碼化處理。保存個</p>

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.4.7	VII.對重要檔案之使用（含使用被拒絕）是否有由電腦留存作業紀錄，以供查核？	資之載具或系統，應定期維護與更新。」
3.1.4.4.8	VIII.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？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(四)-2-運 68「為確保正式作業系統之安全性，應建立對正式作業系統不會造成影響之測試環境。尤其測試大型系統時，應制訂包括相關人員在內之測試度。
3.1.4.4.9	IX.是否禁止主機操作員存取正式作業程式、資料檔案及應用系統說明文件（操作手冊除外）？	
3.1.4.4.10	X.是否有資料庫管理員，負責資料庫使用上	

項 目 編 號	查 核 事 項	法 令 規 章
	<p>的協調和控制事宜？</p> <p>XI.資料庫管理員是否定期重新評估各作業的資料庫結構，並作成紀錄？</p> <p>XII.對資料庫管理人員及系統管理人員是否限制其存取及變更資料庫之資料？</p> <p>XIII.對於資料庫不成功的存取（如 security violation)是否有紀錄，並加以查核，以防止弊端？</p>	
3.1.4.5	⑤媒體管理	
3.1.4.5.1	I.對於儲存資料或程式之媒體是否責成專人負責管理？	
3.1.4.5.2	II.對於保管中或使用中之媒體是否皆予設簿登記控管，並定期派員盤點？	
3.1.4.5.3	III.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？	
3.1.4.5.4	IV.媒體廢棄前是否先經銷磁或其他處理，以防媒體資料外洩？	

項 目 編 號	查 核 事 項	法 令 規 章
3.1.4.5.5	V.正式作業所使用之媒體，是否貼有外標籤 （包含媒體編號、檔案名稱、建檔日期、 保存期限）？	
3.1.4.5.6	VI.因作業需要存取媒體是否有經主管核准 之申請單或紀錄單備查？	
3.2	2.網路系統安全查核	
3.2.1.	(1)管理辦法及作業規範	
3.2.1.1	①是否已明訂網際網路作業相關管理辦法及作 業規範？前開規範之訂定，稽核部門是否有 派員參與？	
3.2.1.2	②各項作業規範或管理辦法是否周延妥適、符 合內部控制原則？是否付諸實施，並適時檢 討、修訂俾切合實際？	
3.2.1.3	③是否已依機構規模大小、性質、業務範圍採 行能有效維持網路安全之政策（如：系統安 全責任之劃分、網路及資料存取控制政策、	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.2	防火牆政策、加密程序及控制、防毒軟體之使用政策)？前開安全政策是否定期檢討、修訂，以符實際運作之需？	
3.2.2.1	(2)主要資訊設備及安全措施 ①網路系統相關之硬體、軟體及通訊設備(如：網路伺服器、防火牆...等)有無適當之門禁管制措施？有否指定專責單位(人員)監管？	
3.2.2.2	②對電腦中心或其他存放文件之場所有無適當之安全管制措施？	
3.2.2.3	③對於各項軟、硬體設備是否有妥善之備援措施？	
3.2.3	(3)網路系統安全控管	
3.2.3.1	①是否建置一適當之網路系統安全管制措施，以控制網際網路與其內部網路或電腦系統間之活動(activity)？	
3.2.3.2	②有關網路系統安全管制是否指定專人負責管理，並明訂其職責？對系統使用者權限設定	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.3.3	<p>是否嚴謹？</p> <p>③有關網路系統對使用者之建置管理是否嚴謹？使用者密碼設定之相關限制是否適當？</p> <p>如：</p>	
3.2.3.3.1	I.是否規定需設定為文數字之密碼？	
3.2.3.3.2	II.是否規定密碼最少字數？	
3.2.3.3.3	III.是否設定密碼之有效期限？	
3.2.3.3.4	IV.密碼是否以亂碼方式儲存？	
3.2.3.3.5	V.是否設定密碼輸入錯誤失敗次數之控制？	
3.2.3.3.6	VI.是否強迫第一次登錄時須變更密碼？	
3.2.3.3.7	VII.系統是否控制不得使用前幾次用過的密碼？	
3.2.3.4	④是否限定使用者 login 系統失敗次數，以防止非授權人員無限制地嘗試密碼？	
3.2.3.5	⑤對系統資源（如：檔案資料）之使用權限設定是否嚴謹？	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.3.6	⑥安全管制類報表(如：系統管理者使用紀錄、非法存取使用紀錄....)是否周全？是否確實加以查核並依規定陳報或陳閱？	
3.2.3.7	⑦是否建立適當程序，以辨識任何未經過防火牆之遠端存取及如何監控、控制該項存取？	
3.2.3.8	⑧防火牆設定維護是否指定專人負責？其異動程序是否均經申請、核可及覆核程序，並留存紀錄？	
3.2.3.9	⑨變更防火牆設定是否經測試，並經主管審核其測試結果？防火牆設定文件是否配合修正？	
3.2.3.10	⑩對防火牆設定相關文件是否妥善保存，並嚴格控管文件之使用？	
3.2.3.11	⑪若防火牆係委外維護，受檢單位是否已明確定義其與廠商間之責任？	
3.2.3.12	⑫網路系統是否建置適當之病毒偵測及預防程序？	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.3.13	⑬各工作站是否建置防毒軟體，以偵測及預防病毒感染？	
3.2.3.14	⑭對重要資料之傳送是否加密，以確保網路傳輸資料之安全？	
3.2.4	(4)網路系統監控及偵測	
3.2.4.1	①是否定期評估網路安全控制系統，並適時檢討以改進監控及偵測技術？	
3.2.4.2	②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？	
3.2.4.3	③網路活動日誌（Activity logs）是否指定專人每日檢視並呈核主管？	
3.2.4.4	④對於監控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？	
3.2.4.5	⑤受檢單位若委外作業進行網際網路安全檢測（如入侵測試、病毒預防偵測等），是否注意下列事項：	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.4.5.1	I.是否由客觀第三者執行入侵測試？	
3.2.4.5.2	II.執行入侵測試之人員是否能提供適當地保證？	
3.2.4.5.3	III.如何決定測試頻率？係採一年至少執行一次入侵測試；或依管理者對風險分析及對風險之容忍度決定可接受之入侵測試頻率？	
3.2.4.5.4	IV.入侵測試結果是否經相關主管人員覆核？測試結果及相關文件是否嚴格管制調閱？	
3.2.5	(5)供應商管理。	
3.2.5.1	①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：	票券金融公司資通系統與服務供應鏈風險管理規範
3.2.5.1.1	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	票券金融公司資通系統與服務供應鏈風險管理規範第4條

項 目 編 號	查 核 事 項	法 令 規 章
3.2.5.1.2	要求? II.屬核心資通系統，或屬非核心資通系統， 且供應商於契約存續期間得存取公司機敏 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?	票券金融公司資通系統與服務供應 鏈風險管理規範第 5 條
3.2.5.2	②選擇供應商前，是否執行下列事項：	
3.2.5.2.1	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 業資格與資訊安全要求及服務水準？	
3.2.5.2.2	II.選擇供應商過程，如涉及公司資訊交換， 是否於資訊交換前簽署保密協議書？	
3.2.5.2.3	III.是否執行安全評估以選任合適之供應商， 包括是否評估供應商對公司服務集中度之 適度分散（如存在集中度過高之疑慮，應依 評估結果擬訂對應之風險處理措施）？是否 評估供應商對所委託項目之資訊安全管理 機制？是否評估供應商與其提供產品或服	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.5.3	<p>務位置？</p> <p>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：</p>	票券金融公司資通系統與服務供應鏈風險管理規範第6條
3.2.5.3.1	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？	
3.2.5.3.2	II.是否定義公司與供應商之資訊安全權責，規範供應商應實施之資訊安全要求，應包含人員管理、資訊存取與傳輸安全管控機制等，以落實資通系統供應鏈邊際防護？	
3.2.5.3.3	III.是否約定非經公司書面同意，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？	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.5.3.4	IV.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？	
3.2.5.3.5	V.是否與供應商約定服務品質、水準、效能、供應商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、異常管理等各項服務要求？	
3.2.5.3.6	VI.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、本會及中央銀行，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？	
3.2.5.3.7	VII.是否訂定資通系統功能需求或資訊建置要求，並包含資訊安全要求或控制措	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.5.3.8	施？是否訂定產品或服務之交付驗收程序和標準？ VIII.是否明確約定供應商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？	票券金融公司資通系統與服務供應鏈風險管理規範第 7 條
3.2.5.3.9	IX.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？	
3.2.5.3.10	X.是否訂定供應商契約終止時，資訊資產與資料返還、移交、刪除或銷毀之要求？	
3.2.5.4	④於供應商契約存續期間，是否注意以下原則：	
3.2.5.4.1	I.公司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？	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.5.4.2	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，以利追蹤資料使用狀況？	
3.2.5.4.3	III.是否識別供應商涉及之關鍵資訊資產，以加強風險管理？	
3.2.5.4.4	IV.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，以落實資通系統供應鏈邊際防護？	
3.2.5.4.5	V.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，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？	
	VI.是否建立對核心資通系統及於契約存續期間得存取公司機敏資料之非核心資	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.5.4.6	通系統供應商資訊安全稽核之程序（含稽核結果之改善追蹤機制）？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（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）？	
	VII.是否審查供應商針對其專案執行人員辦理資訊安全教育訓練之紀錄？	
3.2.5.4.7	VIII.是否依契約要求審查供應商所交付之系統或程式（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）？	
3.2.5.4.8	IX.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？	
3.2.5.4.9	⑤供應商服務變更與契約終止時，是否符合下列事項：	
		票券金融公司資通系統與服務供應鏈風險管理規範第 8 條

項 目 編 號	查 核 事 項	法 令 規 章
3.2.5.5	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),公司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?	
3.2.5.5.1	II. 供應商契約終止時,公司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?	
3.2.5.5.2	(6)緊急應變計畫及災害復原程序 ①是否適當評估網路系統無法運作時對該單位業務之影響?並已訂定緊急應變計畫及災害復原程序,其內容是否適當?	
3.2.6	②緊急應變程序能否有效掌控未經授權之侵入?該程序對遠端存取之控制是否符合安全	
3.2.6.1		

項 目 編 號	查 核 事 項	法 令 規 章
3.2.6.2	管制政策？是否嚴格監控其存取情形？對遠端存取是否留有稽核軌跡（audit log）？ ③對緊急應變計畫及災害復原程序是否加以演練並留存紀錄？ (7)內部稽核辦理情形	
3.2.6.3	內部稽核之範圍是否包括網路系統提供之各項業務、網路系統使用管理、委外作業管理、病毒偵測及預防、及檢核實際運作情形與所訂安	
3.2.7	控標準是否一致等？	
3.2.8	(8)雲端服務安全控管	票券金融公司辦理資訊安全防護自律規範
3.2.8.1	①是否制定雲端服務管理政策，並每年檢視一次？	票券金融公司辦理資訊安全防護自律規範第 5 條第 2 款
3.2.8.2	②導入 IaaS 或 PaaS 雲端服務模式前，是否評估下列事項：	票券金融公司辦理資訊安全防護自律規範第 5 條第 10 款
3.2.8.2.1	I. 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	

項 目 編 號	查 核 事 項	法 令 規 章
3.2.8.2.2	責歸屬及資訊安全防護等項目。 II. 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。	
3.2.8.2.3	III. 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。	
3.2.8.3	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？	票券金融公司辦理資訊安全防護自律規範第 5 條第 8 款
3.2.8.4	④票券金融公司本身、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	票券金融公司辦理資訊安全防護自律規範第 5 條第 5、6 款

項 目 編 號	查 核 事 項	法 令 規 章
3.2.8.5	述第三人之適格性及所出具查核報告之妥適性？ ⑤ 是否訂定妥適之緊急應變計畫？是否建立終止使用雲端服務之移轉策略及計畫，確保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？	票券金融公司辦理資訊安全防護自律規範第 5 條第 9 款
3.2.8.6	⑥ 是否確認雲端服務業者於設備更換及汰換設備內之資料經刪除或銷毀？是否定期確認雲端服務維持所需之服務水準，並定期檢視服務水準報告？	票券金融公司辦理資訊安全防護自律規範第 5 條第 10 款
3.2.8.7	⑦ 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？	票券金融公司辦理資訊安全防護自律規範第 5 條第 7 款
3.2.8.8	⑧ 是否留存人員對於雲端服務平台操作之稽核軌跡？是否避免雲端平台之稽核軌跡內容含有未加密之營運或客戶重要資料？	票券金融公司辦理資訊安全防護自律規範第 6 條

項 目 編 號	查 核 事 項	法 令 規 章
3.2.8.9	⑨將作業委託他人處理涉及使用雲端服務，是否依照「金融機構作業委託他人處理內部作業制度及程序辦法」及銀行公會「金融機構作業委外使用雲端服務自律規範」之規定辦理	票券金融公司辦理資訊安全防護自律規範第5條第12款
3.3	3.使用單位查核	
3.3.1	(1)端末電腦系統管理	
3.3.1.1	①設備安全防護	
3.3.1.1.1	I.業務單位如設有端末主機時，是否有設置獨立上鎖之房間，俾利進出管制？並由專人管理？	
3.3.1.1.2	II.端末主機房之各項安全防護措施是否適當？	
3.3.1.2	②程式、資料檔案管理	
3.3.1.2.1	I.系統維護人員在業務單位安裝或修改程式時，是否執相關認可文件並由業務單位負	

項 目 編 號	查 核 事 項	法 令 規 章
3.3.1.2.2	責人員陪同？ II.系統修改後是否經過詳細的測試驗收，並保留測試紀錄？程式變更有無留存換版紀錄？	
3.3.1.2.3	III.對於程式及資料檔案是否設定適當之存取限制？對重要檔案是否採取亂碼化措施加以保護，以防止不當之使用？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：技術基準二-(一)-1-技 28「為防止檔案遭複製或竊取等資料外洩，應對重要資料採用亂碼化處理。保存個資之載具或系統，應定期維護與更新。」
3.3.1.2.4	IV.對客戶個人資料、往來交易資料及其他相關資料是否訂定相關保密措施，以防外	

項 目 編 號	查 核 事 項	法 令 規 章
3.3.1.2.5	洩及非法使用？ V.對於程式及資料檔案毀損時是否訂有重建之程序？	
3.3.1.2.6	VI.對於重要之程式（含系統、應用程式）及資料檔案是否備分異地存放？	
3.3.1.3	③媒體管理	
3.3.1.3.1	I.對所使用之媒體（如磁片、磁帶）是否均有外標籤標明媒體編號、檔案名稱（內容）、建檔日期、保存期限？是否設簿登記控管？	
3.3.1.3.2	II.媒體存放場所是否有防水、防火、防犯等安全措施？是否保持適當之溫、濕度？	
3.3.1.4	④操作管理	100.11.23 金 管 銀 國 字 第
3.3.1.4.1	I.端末系統是否備有操作手冊供操作員參考使用？	10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100年8
3.3.1.4.2	II.端末系統在開關機時是否由專人依照所指定之程序執行？	月修訂「金融機構資訊系統安全基準」：營運基準(三)-1-運14「訂定日

項 目 編 號	查 核 事 項	法 令 規 章
3.3.1.4.3	III.是否備有工作日誌，記載電腦之開關機紀錄、故障維護情形及操作人員、時間等，並定期陳報？對異常狀況有否追蹤查核？	常作業手冊。」、運 15「訂定故障或災害發生時相關作業之操作手冊。」
3.3.1.4.4	IV.是否訂定中心主機或端末系統故障時之應變措施及復原程序？有無經過測試、演練並留存紀錄？	1.100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-24「為將資訊系統故障與災變對顧客、總行、營業單位之影響降至最低，同時儘早完成復原作業，應訂定故障災變之因應對策。」 2.100.11.23 金 管 銀 國 字 第

項 目 編 號	查 核 事 項	法 令 規 章
		10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-1-運 15「訂定故障或災害發生時相關作業之操作手冊。」
3.3.2	(2)端末機作業管理	3.100.11.23 金 管 銀 國 字 第10000372210 號函核復，中華民國銀行商業同業公會全國聯合會100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(六)-1-運 82、83、84「實施系統操作訓練。」、「實施事故應變操作訓練。」、「實施防災、防犯演練。」。
3.3.2.1	①端末機使用管理	
3.3.2.1.1	I.對經授權使用端末機人員之姓名、使用者	100.11.23 金 管 銀 國 字 第

項 目 編 號	查 核 事 項	法 令 規 章
3.3.2.1.2	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責任？登記簿是否與電腦使用人員資料檔內容相符？	10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-12「為預防端末機遭非法使用、啟動不當交易等，除應以操作人員識別卡管理外，同時應詳細記錄交易的操作內容，並加以檢核。」
3.3.2.1.3	II.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？	
3.3.2.1.4	III.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？	
3.3.2.1.5	IV.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？	
	V.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	

項 目 編 號	查 核 事 項	法 令 規 章
3.3.2.1.6	錄？ VI. 端末機使用人員資料（如使用者代號、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？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-12-運 38「為防止使用端末設備從事不正當交易，應依照交易內容，分別訂定端末設備操作者所能操作之權限範圍。」
3.3.2.1.7	VII. 端末機使用者代號之授予及其交易權限是否符合分工制衡原則？	
3.3.2.1.8	VIII. 使用者密碼(含主管密碼、端末機操作密碼、櫃員密碼)是否可由使用人視情況需要定期或不定期變更？	
3.3.2.1.9	IX. 是否有適當之管制措施以防止業務單位人員於營業時間外使用端末機從事非法	

項 目 編 號	查 核 事 項	法 令 規 章
3.3.2.1.10	<p>之交易？</p> <p>X.處理或核可交易時是否均憑被授予之使用者代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？</p>	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-12-運 39「為防止利用端末設備從事不正當交易，應指派專人負責管理操作人員作業卡，或使用者帳號。」
3.3.2.1.11	XI.對於調離職人員是否立即取消其使用者代號並收繳其領用之作業卡？	
3.3.3	(3)人員管理與訓練	100.11.23 金 管 銀 國 字 第
3.3.3.1	<p>①對每個人之職務是否有明確劃分及規定？有無依規定實施輪調及休假？</p>	10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(一)-2-運 9「為使資

項 目 編 號	查 核 事 項	法 令 規 章
3.3.3.2	②對每一作業是否至少有兩人以上可互為備援？	訊系統順利運轉，並防止非法事件發生，應有適當之職務分工，明確劃分業務範圍及責任、權限，以確定相互制衡體制。
3.3.3.3	③對各項業務是否均有詳細完整的操作說明並保持可用狀態？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8 月修訂「金融機構資訊系統安全基準」：營運基準(三)-1-運 14「為正確且安全運轉資訊系統，應規定日常各種程序之作業手冊。」
3.3.3.4	④端末主機或端末機操作員是否接受適當之訓練？	100.11.23 金 管 銀 國 字 第 10000372210 號函核復，中華民國銀行商業同業公會全國聯合會 100 年 8

項 目 編 號	查 核 事 項	法 令 規 章
3.3.3.5	⑤資訊安全主管及資訊安全人員，是否每年至少接受 15 小時以上資訊安全專業課程或職能訓練？其他人員，每年是否接受 3 小時以上資訊安全宣導課程？	月修訂「金融機構資訊系統安全基準」：營運基準(三)-1-運 14「訂定日常作業手冊。」、運 15「訂定故障或災害發生時相關作業之操作手冊。」 本 會 111.5.16 金 管 銀 票 字 第 11101302162 號令 「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 38 條之 1 第 1 項但書所稱主管機關對票券金融公司辦理資訊安全之解釋令
3.4	4.個人化資料自主運用平臺介接作業	
3.4.1	(1)向國發會申請介接本平臺為資料提供者或服務提供者，是否經過本會同意？	個人化資料自主運用平臺介接作業要點第 4 條
3.4.2	(2)是否產製當事人資料傳輸相關紀錄且保存至少二年？紀錄內容是否至少包含傳輸資料名稱、傳輸時間、傳輸對象、當事人身分、	個人化資料自主運用平臺介接作業要點第 7 條

項 目 編 號	查 核 事 項	法 令 規 章
3.4.3	資料傳輸成功與否等？ (3)就當事人資料之蒐集、處理及利用之流程，是否每年辦理內部查核工作，作成查核紀錄？且保存至少二年？並應配合國發會及本會之查核？	個人化資料自主運用平臺介接作業要點第 7 條
3.4.4	(4)涉及資訊安全維護及個人資料保護等有關事項，是否依資通安全管理法、個人資料保護法及相關法令規定辦理？	個人化資料自主運用平臺介接作業要點第 8 條
4	(四) 內部稽核制度之查核	
4.1	1.稽核單位之組織及編制	
4.1.1	(1)內部稽核單位應隸屬董事會，獨立執行稽核業務，應至少每半年向董事會及監察人(或審計委員會)提出報告。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 10 條第 1 項
4.1.2	(2)票券金融公司應置總稽核一人，綜理稽核業務；其職位應等同於副總經理，且不得兼任與稽核工作有相互衝突或牽制之職務。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 10 條第 2 項

項 目 編 號	查 核 事 項	法 令 規 章
4.1.3	(3)票券金融公司應依據投資規模、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 12 條
4.1.4	(4)稽核單位之人事任用、免職、升遷、獎懲、輪調及考核等，應由總稽核簽報董事長核定後辦理。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 10 條第 5 項
4.2	2.稽核人員之資格及訓練	
4.2.1	(1)總稽核之聘任、解聘或調職，應經審計委員會全體成員二分之一以上同意及提董（理）事會全體董（理）事三分之二以上之同意，並報請主管機關核准後為之。其他稽核人員應具備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 條第 2 項所訂之資格。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 10 條第 3 項及第 12 條第 2 項

項 目 編 號	查 核 事 項	法 令 規 章
4.2.2	(2)總稽核、稽核人員於充任前應參加主管機關認定機構所舉辦之稽核研習訓練，並取得結業證書；另每年參加主管機關認定機構或稽核人員所屬金融控股公司（含子公司）或銀行業（含母公司）自行舉辦之金融相關業務專業訓練，其最低訓練時數，正副主管及總稽核應達二十小時以上，其餘內部稽核人員應達三十小時以上，其中參加主管機關認定機構所舉辦之金融相關業務專業訓練不得低於應達訓練時數二分之一。	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 條第 1 項、第 2 項、第 3 項
4.2.3	(3)票券金融公司應將稽核人員之資歷及受訓資料，於每年一月底前依主管機關規定格式以網際網路資訊系統申報主管機關備查。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 21 條第 1 項

項 目 編 號	查 核 事 項	法 令 規 章
4.2.4	(4)內部稽核人員以超然獨立、客觀公正之立場，執行其職務，職務代理，應由內部稽核部門人員互為代理。	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
4.3	3.稽核單位之職掌	
4.3.1	(1)稽核單位應編製內部稽核工作手冊及底稿，內容至少應包括對內部控制制度各項規定與業務流程進行評估；稽核工作手冊（含電腦作業稽核規定）應配合業務，參照上年度增修之法令規章及內規修正。	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 條第 1 項第 1 款
4.3.2	(2)督導業務管理單位訂定自行查核內容與程序，及各單位自行查核之執行情形。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 14 條第 1 項第 2 款
4.3.3	(3)稽核單位應擬訂年度稽核計劃並切實執行。內部稽核報告應交付監察人（或審計	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 條第 1 項第

項 目 編 號	查 核 事 項	法 令 規 章
4.3.4	<p>委員會)查閱，除主管機關另有規定外，應於查核結束日起二個月內報主管機關，設有獨立董事者，應一併交付。內部稽核報告、工作底稿及相關資料應至少留存五年。</p> <p>(4)是否依公司業務特性訂定工作手冊、抽樣標準及缺失重要性分級機制，並定期檢討修訂並將主管機關要求列入內部稽核查核重點之事項列入查核項目且確實執行。</p>	<p>3款、17條第2項及第19條</p> <p>「票券金融公司稽核工作考核要點」附表、二、(一)、5</p>
4.3.5	<p>(5)一般查核之內部稽核報告內容至少應揭露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條第1項規定之事項及業務單位依票券金融管理法第49條準用銀行法第32條、第33條規定有關「授信明細表」及第33條之1「有利害關係者資料</p>	<p>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</p> <p>2.「票券金融公司稽核工作考核要點」附表、二、(一)、7</p>

項 目 編 號	查 核 事 項	法 令 規 章
4.3.6	表」之建檔情形。 (6)內部稽核所發現之缺失，皆應於稽核報告揭露。對重大缺失或弊端，內部稽核單位應有懲處建議權，並應於內部稽核報告中充分揭露對重大缺失應負責之失職人員。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 18 條第 2 項
4.3.7	(7)對委外事項執行情形應列入內部稽核之查核項目，並將查核結果於稽核報告中揭露。金融機構作業委外不得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，並應確保遵循銀行法、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。	金融機構作業委託他人處理內部作業制度及程序辦法第 9、19 條
4.3.8	(8)金融檢查機關報告各項評註所提缺失，稽核室應建檔追蹤督促改善。	

項 目 編 號	查 核 事 項	法 令 規 章
4.3.9	(9)稽核單位辦理內部稽核如有符合下列報送標準者，是否將該次查核情形依規定格式於查核結束日起二個月內向本會檢查局「單一申報窗口網站」之金融機構非財報類系統申報查核結果：①屬年度稽核計畫之查核且有制度面或有重大影響缺失及異常事項。②非屬年度稽核計畫之查核。	本會 105.7.21 金管檢制字第 10501502581 號函
4.4	4.自行查核	
4.4.1	(1)營業、財務、資產保管、資訊單位及國外營業單位應每半年至少辦理一次一般自行查核，每月至少辦理一次專案自行查核；自行查核報告應作成工作底稿，至少留存五年備查。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 25 條第 1 項、第 4 項
4.4.2	(2)自行查核應由單位主管指定非原經辦人員辦理並事先保密。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 25 條第 3 項

項 目 編 號	查 核 事 項	法 令 規 章
4.4.3	(3)內部稽核單位對金融檢查機關、會計師、內部稽核單位（含母公司內部稽核單位）與內部單位自行查核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，應持續追蹤覆查，並以書面提報董事會及交付監察人(或審計委員會)，並列為對各單位獎懲及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 26 條第 1 項
4.4.4	(4)內部稽核單位是否覈實督導各單位辦理自行查核並覆核其自行查核報告及持續對各單位自行查核人員施以適當稽核訓練。	「票券金融公司稽核工作考核要點」附表、二、(二)、9
4.5	5.遵守法令主管制度	
4.5.1	(1) 票券金融公司應設立一隸屬於總經理之法令遵循單位，負責遵守法令遵循主管制度	金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條第 1 項、

項 目 編 號	查 核 事 項	法 令 規 章
	<p>之規劃、管理及執行，並指派高階主管一人擔任遵守法令主管，綜理法令遵循事務，至少每半年向董事會及監察人或審計委員會報告，如發現有重大違反法令或遭金融主管機關調降評等時，應即時通報董事及監察人，並就法令遵循事項，提報董事會；總機構、國內外營業單位、資訊單位、財務保管單位及其他管理單位應指派人員擔任遵守法令主管，負責執行法令遵循事宜。國外營業單位法令遵循主管之設置應符合當地法令規定及當地主管機關之要求，除有下列情事者外，應為專任：(1)兼任防制洗錢及打擊資恐主管。(2)依當地法令明定得兼任無職務衝突之其他職務。(3)當地法令未明確規定，於與當地主管機關溝通並確認後，報經主管</p>	<p>第 4 項</p> <p>金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條第 2 項但書及本會 104.6.12 金管銀票字第 10440002790 號令</p>

項 目 編 號	查 核 事 項	法 令 規 章
4.5.1.1	機關備查者，得兼任無職務衝突之其他職務。 ①票券金融公司上一會計年度決算後淨值未達新臺幣一百億元或資產總額未達新臺幣一千億元規模者，其總機構法令遵循主管得兼任法務單位主管與防制洗錢及打擊資恐專責單位主管或非業務類之管理單位主管。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條第 5 項、第 6 項、第 7 項、第 8 項
4.5.1.2	②票券金融公司總機構法令遵循主管、法令遵循單位所屬人員、國內外營業單位、資訊單位、財務保管單位及其他管理單位之法令遵循主管應具備金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條第 5 項資格條件之一；且每年應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)或票券金融公司(含母公司)自行	

項 目 編 號	查 核 事 項	法 令 規 章
4.5.1.3	<p>舉辦十五小時之教育訓練，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。國外營業單位之法令遵循主管，每年應至少參加由當地主管機關或相關單位舉辦之法令遵循在職教育訓練課程十五小時，如當地主管機關或相關單位未舉辦法令遵循教育訓練課程，得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）或票券金融公司（含母公司）自行舉辦之教育訓練課程。【防制洗錢及打擊資恐專責單位設於法令遵循單位者，該專責單位人員充任前及每年應受之訓練，依防制洗錢及打擊資恐相關規定辦理，不受同條第5項及第6項規定限制。】</p> <p>③票券金融公司應以網際網路資訊系統向主</p>	金融控股公司及銀行業內部控制及

項 目 編 號	查 核 事 項	法 令 規 章
4.5.2	管機關申報總機構法令遵循主管、法令遵循單位所屬人員之名單及受訓資料。 (2)各單位法令遵循自行評估作業，應由單位主管指定專人辦理。自評頻率至少每半年一次。自行評估工作底稿應至少保存五年。	稽核制度實施辦法第 32 條第 9 項
4.5.2.1	①票券金融公司於推出各項新商品、服務及向主管機關申請開辦新種業務前，法令遵循主管應出具符合法令及內部規範之意見並簽署負責。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條第 1 項第 3 款
4.5.2.2	②訂定法令遵循之評估內容與程序，及督導各單位定期自行評估執行情形，並對各單位法令遵循自行評估作業成效加以考核，經簽報總經理後，作為單位考評之參考依據。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條第 1 項第 4 款
4.5.2.3	③內部稽核單位得自行訂定所屬單位法令遵循之評估內容與程序，及自行評估所屬單位	金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條第 2 項

項 目 編 號	查 核 事 項	法 令 規 章
	法令遵循執行情形，不適用「金融控股公司及銀行業內部控制及稽核制度實施辦法」第34條第1項第4款規定。	
4.6	6.內部控制制度執行情形聲明書	
4.6.1	(1)總經理應督導各單位檢討內部控制制度執行情形及評估營運健全性。	金融控股公司及銀行業內部控制及稽核制度實施辦法第34條第2項
4.6.2	(2)董事長、總經理、總稽核及總機構法令遵循主管聯名出具內部控制制度聲明書，並提報董事會通過，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揭露於公司網站，並於主管機關指定網站辦理公告申報。	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條第1項
4.6.3	(3)內部控制制度聲明書應依規定刊登於年報、股票公開發行說明書及公開說明書。	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條第2項

項 目 編 號	查 核 事 項	法 令 規 章
4.7	7.其他	
4.7.1	(1)票券金融公司具有業務或交易核准權限之各級主管，應於就任前具備金融控股公司及銀行業內部控制及稽核制度實施辦法第24條第1項規定之資格條件。	金融控股公司及銀行業內部控制及稽核制度實施辦法第24條第1項
4.7.2	(2)主管機關檢查報告所提列檢查意見，是否依指定期限函覆改善辦理情形，並持續追蹤覆查	「票券金融公司稽核工作考核要點」附表、三、(二)、11
4.7.3	(3)對於涉嫌舞弊案件或重大偶發事件應依法令規定之方式儘速向主管機關及中央銀行報告，並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；重大偶發事件之通報機制應納入金融機構內部控制及稽核制度。	「票券金融公司稽核工作考核要點」附表、三、(三)、13及「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」

項 目 編 號	查 核 事 項	法 令 規 章
4.7.4	(4)票券金融公司應於每會計年度終了前將次一年度稽核計畫及每會計年度終了後二個月內將上一年度之年度稽核計畫執行情形，依主管機關規定格式以網際網路資訊系統申報主管機關備查。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 22 條第 1 項
4.7.5	(5)票券金融公司應於每會計年度終了後五個月內將上一年度內部控制制度缺失與異常事項及其改善，依主管機關規定格式以網際網路資訊系統申報主管機關備查。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 23 條
4.7.6	(6)票券金融公司應訂定適當之風險管理政策與程序經董事會通過並適時檢討修訂。	金融控股公司及銀行業內部控制及稽核制度實施辦法第 35 條
4.7.7	(7)應設置獨立之專責風險控管單位，並定期向董事會提出風險控管報告。	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 1 項
4.7.8	(8)金融控股公司及銀行業內部控制及稽核制度實施辦法，增訂金融控股公司及銀行業	101.3.2 金管銀國字第 10120000510 號「金融控股公司及銀行業內部控制

項 目 編 號	查 核 事 項	法 令 規 章
4.7.9	<p>之業務規範及處理手冊中，應包括適用國際會計準則之管理及金融消費者保護之管理</p> <p>(9)票券金融公司應建立自行查核制度、法令遵循制度與風險管理機制及內部稽核制度等內部控制三道防線，以維持有效適當之內部控制制度運作。</p>	<p>及稽核制度實施辦法」：增訂金融控股公司及銀行業之業務規範及處理手冊中，應包括適用國際會計準則之管理及金融消費者保護之管理。</p> <p>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</p>
4.7.10	<p>(10)發生資通安全事件，且造成客戶權益受損或影響機構健全營運之重大偶發事件，是否於確認後三十分鐘內，先以電話向銀行局通報，再儘速續以網際網路申報系統辦理通報？</p>	<p>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第三點</p>
4.7.11	<p>(11)114 年起是否將永續資訊之管理納入內部控制制度，並將其列為年度稽核計畫之稽</p>	<p>公開發行公司建立內部控制制度處理準則第 8、13 條</p>

項 目 編 號	查 核 事 項	法 令 規 章
5	核項目 (五)公平待客原則	本會 111.5.12 金管法字第
5.1	1.是否建立公平待客原則之政策及策略，並提 報董事會通過；各項「公平待客原則」之 訂定及執行，是否納入內部控制及稽核制 度。	1110192104 號函「金融服務業公平 待客原則」第伍條
5.2	2.是否訂定具體執行各項「公平待客原則」策 略之內部遵循規章、行為守則及執行步驟？	
5.3	3. 是否指定副總經理以上主管及專責部門負 責規劃及推行，專責部門監督各部門「公 平待客原則」之執行，找出各部門可能違 反「公平待客原則」之環節，提出具體解 決方案，並於副總經理以上主管督導會議 提出檢討與因應，定期向董事會報告？是 否定期辦理教育訓練(每年至少 3 小時)？	

