

拾、資訊作業之查核

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|-----------------------|-----------------|
| 1 | 一、資訊單位查核 | 附註：1. 金控公司如有設置獨 |
| 1.1 | (一)組織與管理 | 立電腦中心則必須 |
| 1.1.1 | 1. 內部組織與職務分工 | 全部查核。 |
| 1.1.1.1 | (1)資訊單位是否獨立於其他部門？ | 2. 金控公司如未設置電 |
| 1.1.1.2 | (2)是否有高階人員組成資訊作業推動小組 | 腦中心，須查核第二 |
| | 負責審議、核准或督導、協調下列事項？ | 項管理資訊系統查 |
| 1.1.1.2.1 | ①資訊作業重要規章。 | 核、第四項使用單位 |
| 1.1.1.2.2 | ②資訊作業中、長期計畫。 | 查核；若內部有架設 |
| 1.1.1.2.3 | ③資訊作業安全控管措施。 | 網路者，須增加查核 |
| 1.1.1.2.4 | ④重要軟硬體系統購置、更新。 | 第三項網路系統安全 |
| 1.1.1.2.5 | ⑤資訊作業預算。 | 查核；若其資訊系統 |
| 1.1.1.2.6 | ⑥資訊作業成本效益評估。 | 係委外設計者，須增 |
| 1.1.1.2.7 | ⑦重要專案之進度及目標達成情形。 | 加查核一之(三)之 4 |
| 1.1.1.3 | (3)資訊單位各科(組)是否訂有明確職掌？ | 項系統外包管理。 |
| | | 金融機構資訊系統安全基準 |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|---|---|
| 1.1.1.4 | 各科(組)權責是否有重疊情形？人員配置是否適當？ (4)下列工作有無適當之職責分工？ | |
| 1.1.1.4.1 | ①應用系統分析與設計。 | |
| 1.1.1.4.2 | ②系統軟體建置與維護。 | |
| 1.1.1.4.3 | ③電腦主機操作。 | |
| 1.1.1.4.4 | ④連線管理(安全控管)。 | |
| 1.1.1.4.5 | ⑤作業或資料管制。 若無，有無配合之控管措施？ | |
| 1.1.1.5 | (5)對各項業務(工作)是否有人可代理？ | |
| 1.1.1.6 | (6)應配置資訊安全長及設置資訊安全專責單位與人員者，是否已依規定辦理？ | 1. 公開發行公司建立內部控制制度處理準則 2. 110.12.28 金管證審字第 11003656544 號「有關公開發行公司建立內部控制制度處理準則第九條之一規定之令」 |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|------------|--|---------|
| 1.1.2 | 2. 管理辦法及作業規範之訂定 | |
| 1.1.2.1 | (1)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： | |
| 1.1.2.1.1 | ①有關係統文件標準化之規範？ | |
| 1.1.2.1.2 | ②有關係統開發、維護規範？ | |
| 1.1.2.1.3 | ③有關電腦軟硬體系統及其附屬設施之管理規範？ | |
| 1.1.2.1.4 | ④有關係統操作之一般規範？ | |
| 1.1.2.1.5 | ⑤有關批次作業處理操作規範及有關程式及資料檔案管理及維護規範？ | |
| 1.1.2.1.6 | ⑥有關媒體管理規範？ | |
| 1.1.2.1.7 | ⑦系統故障對策及災變因應措施？ | |
| 1.1.2.1.8 | ⑧有關委外作業之管理規範？ | |
| 1.1.2.1.9 | ⑨有關內部工作分配及其管理之規範？ | |
| 1.1.2.1.10 | ⑩有關內部自行查核之規範？ | |
| | 上述規範之訂定，稽核部門是否有派員參 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|---|---------|
| 1.1.2.2 | 與？ (2)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？ | |
| 1.1.3 | 3. 工作計畫之訂定 | |
| 1.1.3.1 | (1)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？ | |
| 1.1.3.2 | (2)所訂計畫項目是否符合業務上之需求？ | |
| 1.2 | (二)資訊中心安全控制 | |
| 1.2.1 | 1. 環境安全防護 | |
| 1.2.1.1 | (1)電腦設備及相關設施之安全防護是否完善？ | |
| 1.2.1.1.1 | ①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？ | |
| 1.2.1.1.2 | ②除不斷電設備外有無裝置自動發電 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|---|--------------|
| 1.2.1.1.3 | 機，以供長時間停電使用？ ③有無裝置火災自動警報系統及自動滅火設備？ | |
| 1.2.1.1.4 | ④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？ | |
| 1.2.1.1.5 | ⑤保險及維護契約涵蓋範圍是否完全？並在有效期間內？ | |
| 1.2.1.2 | (2)機房是否放置非工作需要或危險物品？ | |
| 1.2.1.3 | (3)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？ | |
| 1.2.1.4 | (4)系統說明文件存放場所是否有防火、防水等安全防護措施？ | |
| 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？ | 金融機構資訊系統安全基準 |
| 1.2.3 | 3. 備援措施：電腦設備及相關設施是否有備援 | 金融機構資訊系統安全基準 |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|---|---------|
| 1.2.3.1 | 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同類機器使用者互相締結支援契約？ | |
| 1.2.3.1.1 | (1)程式及資料檔案 ①對重要或需要長期保留檔案（含應用、系統程式及資料檔等）是否有備份？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？ | |
| 1.2.3.1.2 | ②各種重要程式及資料檔案是否有損毀時之重建程序？ | |
| 1.2.3.2 | (2)人員：各項重要工作是否均有備援人員？ | |
| 1.2.3.3 | (3)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？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|--|--------------|
| 1.2.4 | 4. 故障及災害因應對策 | 金融機構資訊系統安全基準 |
| 1.2.4.1 | (1)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變作業方式？ | |
| 1.2.4.2 | (2)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？ | |
| 1.2.4.3 | (3)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？ | |
| 1.2.4.4 | (4)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？ | |
| 1.3 | (三)系統開發及維護控制 | |
| 1.3.1 | 1. 系統開發控制 | |
| 1.3.1.1 | (1)若訂有系統開發、維護規範（standards），是否包括下列項目，以作 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|--|---------|
| 1.3.1.1.1 | 為系統開發、維護及文件製作之標準： ①系統開發／設計程序 | |
| 1.3.1.1.2 | ②套裝軟體選擇基準 | |
| 1.3.1.1.3 | ③程式設計標準 | |
| 1.3.1.1.4 | ④程式及系統測試方法及標準 | |
| 1.3.1.1.5 | ⑤實施（轉換）事宜 | |
| 1.3.1.1.6 | ⑥系統文件撰寫規格 | |
| 1.3.1.1.7 | ⑦系統／程式異動管理 | |
| 1.3.1.1.8 | ⑧系統評估 | |
| 1.3.1.2 | (2)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？ | |
| 1.3.1.3 | (3)系統開發階段是否訂有明確的作業進度 計畫表，並妥善控制之？ | |
| 1.3.1.4 | (4)系統開發、設計是否有由業務、稽核、會 計、企劃等有關單位參與，以求操作、管 理、查核各方面之考慮周全？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|----------|--|--------------|
| 1.3.1.5 | (5)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？ | 個人資料保護法第 5 條 |
| 1.3.1.6 | (6)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？ | |
| 1.3.1.7 | (7)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？各項控制設計是否週延？ | |
| 1.3.1.8 | (8)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？ | |
| 1.3.1.9 | (9)作業實施前轉換計畫是否完妥並經確實執行？ | 金融機構資訊系統安全基準 |
| 1.3.1.10 | (10)系統正式作業實施前，是否經業務、稽 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|------------|--|---------|
| 1.3.1.11 | 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？ (11)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？ | |
| 1.3.1.12 | (12)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？ | |
| 1.3.1.12.1 | ①業務電腦化後，操作、管理與查核上尚待加強、改進者 | |
| 1.3.1.12.2 | ②系統控制功能設計之完整性 | |
| 1.3.1.12.3 | ③程式及檔案資料修改頻率與原因之分析 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|------------|---|--------------|
| 1.3.1.12.4 | ④輸出報表之實用性、完整性 | 金融機構資訊系統安全基準 |
| 1.3.1.12.5 | ⑤實際開發時間、人力、成本與原計畫之比較分析 | |
| 1.3.2 | 2. 系統維護控制 | |
| 1.3.2.1 | (1)對每一應用系統，是否均派專人負責維護的工作？ | |
| 1.3.2.2 | (2)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分？ | |
| 1.3.2.3 | (3)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？ | |
| 1.3.2.4 | (4)已正式實施之作業，其程式變更： | |
| 1.3.2.4.1 | ①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？ | |
| 1.3.2.4.2 | ②書面申請是否詳細敘明變更原因及內容？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|--|--------------|
| 1.3.2.4.3 | ③修改後是否加以測試（含第三者），並經主管審核其測試結果？ | 金融機構資訊系統安全基準 |
| 1.3.2.4.4 | ④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？ | |
| 1.3.2.4.5 | ⑤系統說明文件是否配合修正？ | |
| 1.3.2.4.6 | ⑥操作程序上如有變更是否通報有關單位？ | |
| 1.3.3 | 3. 系統文件編製 | |
| 1.3.3.1 | (1)對已實施之系統是否有下列文件？ | |
| 1.3.3.1.1 | ①系統需求分析報告 | |
| 1.3.3.1.2 | ②系統設計說明書 | |
| 1.3.3.1.3 | ③程式設計說明書 | |
| 1.3.3.1.4 | ④操作說明(含中心批次作業及端末使用者操作說明) | |
| 1.3.3.1.5 | ⑤測試計畫書(含測試報告及測試紀錄) | |
| 1.3.3.1.6 | ⑥系統轉換計畫書 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|--|--------------|
| 1.3.3.1.7 | ⑦系統驗收紀錄 | 金融機構資訊系統安全基準 |
| 1.3.1.1.8 | ⑧與有關單位研討之會議紀錄 | |
| 1.3.3.2 | (2)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? | |
| 1.3.3.3 | (3)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? | |
| 1.3.3.4 | (4)系統說明文件之撰寫及程式、檔案名稱之命名是否標準化? | |
| 1.3.4 | 4.系統外包管理 | |
| 1.3.4.1 | (1)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? | |
| 1.3.4.2 | (2)上述業務之外包,其開發、維護之預定進度及作業安全、委託內容、機密維護、損 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|--------------|
| | 害賠償等雙方權責之劃分，是否明訂於外包契約內？ | |
| 1.3.4.3 | (3)外包業務是否有專人管理，並控制進度？ | |
| 1.3.4.4 | (4)是否嚴禁外包廠商進入正式作業環境存取程式或資料？ | |
| 1.3.4.5 | (5)是否建立適當程序以檢核外包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？ | |
| 1.3.4.6 | (6)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？ | |
| 1.4 | (四)運作管理 | |
| 1.4.1 | 1. 主機操作管理 | 金融機構資訊系統安全基準 |
| 1.4.1.1 | (1)控制台及週邊設備（磁碟機、磁帶機、列表機等）是否僅限輪值操作員操作？ | |
| 1.4.1.2 | (2)是否備有作業手冊供操作員使用？操作員 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|--|---------|
| 1.4.1.3 | <p>是否依作業說明(作業手冊、工作申請單)執行作業？</p> <p>(3)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？</p> | |
| 1.4.1.4 | <p>(4)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？</p> | |
| 1.4.1.5 | <p>(5)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？</p> | |
| 1.4.1.6 | <p>(6)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？</p> | |
| 1.4.1.7 | <p>(7)執行可直接變更目的程式及資料檔案等之公用程式(utility programs)是否先經核准並留存紀錄？</p> | |
| 1.4.1.8 | <p>(8)機房內是否設置工作日誌，記載電腦開關</p> | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|----------|---|---------|
| 1.4.1.9 | 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？ (9)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？ | |
| 1.4.1.10 | (10)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？ | |
| 1.4.1.11 | (11)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？ | |
| 1.4.2 | 2. 中心端末機使用管理 | |
| 1.4.2.1 | (1)對經授權使用端末機人員之姓名、使用者 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|------------|--|---------|
| 1. 4. 2. 2 | 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？ | |
| 1. 4. 2. 3 | (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？ | |
| 1. 4. 2. 4 | (3) 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？ | |
| 1. 4. 2. 5 | (4) 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？ | |
| | (5) 端末機操作人員是否憑被授予之使用者 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| 1.4.2.6 | 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？ (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？ | |
| 1.4.2.7 | (7)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？ | |
| 1.4.3 | 3. 輸入、輸出資料管制 | |
| 1.4.3.1 | (1)對金控公司業務單位或子公司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。 | |
| 1.4.3.2 | (2)經電腦檢核為異常或錯誤之輸入資料，是否由資料管制人員負責查明處理？ | |
| 1.4.3.3 | (3)報表或媒體等輸出資料送出前，對電腦處 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|------------|--|---------|
| 1. 4. 4 | 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？ | |
| 1. 4. 4. 1 | 4. 程式、資料檔案管理 (1)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？ | |
| 1. 4. 4. 2 | (2)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)及目的碼(object code)為同一版本？ | |
| 1. 4. 4. 3 | (3)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？ | |
| 1. 4. 4. 4 | (4)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？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|----------|---|---------|
| 1.4.4.5 | (5)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？ | |
| 1.4.4.6 | (6)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？ | |
| 1.4.4.7 | (7)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？ | |
| 1.4.4.8 | (8)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？ | |
| 1.4.4.9 | (9)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）？ | |
| 1.4.4.10 | (10)是否有資料庫管理員，負責資料庫使用 上的協調和控制事宜？ | |
| 1.4.4.11 | (11)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？ | |
| 1.4.4.12 | (12)對資料庫管理人員及系統管理人員是否 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|----------|--|---------|
| 1.4.4.13 | 限制其存取及變更資料庫之資料？ (13)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？ | |
| 1.4.5 | 5. 媒體管理 | |
| 1.4.5.1 | (1)對於儲存資料或程式之媒體是否關成專室責成專人負責管理？ | |
| 1.4.5.2 | (2)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？ | |
| 1.4.5.3 | (3)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？ | |
| 1.4.5.4 | (4)媒體廢棄前是否先經銷磁或其他處理，以防媒體資料外洩？ | |
| 1.4.5.5 | (5)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）？ | |
| 1.4.5.6 | (6)因作業需要存取媒體是否有經主管核准 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| | 之申請單或紀錄單備查？ | |
| 2 | 二、管理資訊系統(MIS)查核 | |
| 2.1 | (一)是否開發管理資訊系統(MIS)，提供相關訊息供管理階層經營決策及風險控管之用？ 若有，系統開發設計是否包含下列項目： | |
| 2.1.1 | 1. 依金控公司之組織架構、業務性質及規模，明確定義營運活動、作業程序、內部控制點及經營風險，據以辦理系統規劃？ | |
| 2.1.2 | 2. 涵蓋金控公司整體之風險評估？ | |
| 2.1.3 | 3. 供各類管理及風險監控之資訊、表報？其內容是否完整且適時反應金控公司財務狀況、營運績效？ | |
| 2.2 | (二)金控公司對各單位以及與子公司間各電腦系統及資料庫之相容性是否經嚴謹評估後規劃妥適之整合策略，俾利金控公司經營階層透過通報系統即時取得正確之管理資訊。 | |
| 2.3 | (三)MIS 系統運作是否制定妥適且周延之管理 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| 2.4 | <p>規範？如：資訊傳輸安全機制、資料及程式異動控管程序、緊急備援措施等。</p> <p>(四)使用者是否清楚瞭解系統提供之各項功能、操作流程及通報程序？是否訂有相關規範及操作手冊，並適時依實際狀況辦理增(修)訂？</p> | |
| 2.5 | <p>(五)是否依金控公司經營規模、業務項目及經濟環境之變動，適時檢討、修訂系統功能？是否定期檢視系統管理表報內容之完整性、時效性及一致性，俾增進決策效率及發揮控管經營風險之效益？</p> | |
| 3 | 三、網路系統安全查核 | |
| 3.1 | (一)管理辦法及作業規範 | |
| 3.1.1 | 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？ | |
| 3.1.2 | 2. 各項作業規範或管理辦法是否周延妥適、符 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| 3.1.3 | 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. 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、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 | (二)主要資訊設備及安全措施 | |
| 3.2.1 | 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. 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？ | |
| 3.2.3 | 3. 對於各項軟、硬體設備是否有妥善之備援措施？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| 3.3 | (三)網路系統安全控管 | |
| 3.3.1 | 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）？ | |
| 3.3.2 | 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是否嚴謹？ | |
| 3.3.3 | 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？如： | |
| 3.3.3.1 | (1)是否規定需設定為文數字之密碼？ | |
| 3.3.3.2 | (2)是否規定密碼最少字數？ | |
| 3.3.3.3 | (3)是否設定密碼之有效期限？ | |
| 3.3.3.4 | (4)密碼是否以亂碼方式儲存？ | |
| 3.3.3.5 | (5)是否設定密碼輸入錯誤失敗次數之控制？ | |
| 3.3.3.6 | (6)是否強迫第一次登錄時須變更密碼？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|--|---------|
| 3.3.3.7 | (7)系統是否控制不得使用前幾次用過的密碼？ | |
| 3.3.4 | 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？ | |
| 3.3.5 | 5. 對系統資源（如：檔案資料）之使用權限設定是否嚴謹？ | |
| 3.3.6 | 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？ | |
| 3.3.7 | 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？ | |
| 3.3.8 | 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？ | |
| 3.3.9 | 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？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|--|---------|
| 3.3.10 | 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？ | |
| 3.3.11 | 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？ | |
| 3.3.12 | 12. 網路系統是否建置適當之病毒偵測及預防程序？ | |
| 3.3.13 | 13. 各工作站是否建置防毒軟體，以偵測及預防病毒感染？ | |
| 3.3.14 | 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？ | |
| 3.4 | (四)網路系統監控及偵測 | |
| 3.4.1 | 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？ | |
| 3.4.2 | 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？ | |
| 3.4.3 | 3. 網路活動日誌 (Activity logs) 是否指定專人每日檢視並呈核主管？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| 3.4.4 | 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？ | |
| 3.4.5 | 5. 受檢單位若自行導入或雇用外包廠商進行 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： | |
| 3.4.5.1 | (1) 是否由客觀第三者執行入侵測試？ | |
| 3.4.5.2 | (2) 執行入侵測試之人員是否能提供適當的 保證？ | |
| 3.4.5.3 | (3) 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？ | |
| 3.4.5.4 | (4) 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？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| 3.5 | (五)協力廠商管理 | |
| 3.5.1 | 1. 軟硬體買賣合約或外包維護合約內容是否包括作業安全、委託內容、機密維護、損害賠償等雙方權責之劃分？ | |
| 3.5.2 | 2. 是否建立適當控管程序以確保外包廠商維護程式係屬適當？並指定專人負責監控廠商維護活動及服務？ | |
| 3.5.3 | 3. 若廠商可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？ | |
| 3.6 | (六)緊急應變計畫及災害復原程序 | |
| 3.6.1 | 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？ | |
| 3.6.2 | 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管制政策？是否嚴格監控其存取情形？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|-----------|--|---------|
| 3.6.3 | 對遠端存取是否留有作業紀錄 (audit log) ? | |
| 3.7 | 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? | |
| 3.7.1 | (七)內部稽核辦理情形 | |
| 3.7.2 | 1. 是否明訂內部稽核(含自行查核)規範? 規範內容是否完備, 並確實據以辦理? | |
| 4 | 2. 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、外包業務管理、病毒偵測及預防、及檢核實際運作情形與所訂安控標準是否一致等? | |
| 4.1 | 四、使用單位查核 | |
| 4.1.1 | (一)端末電腦系統管理 | |
| 4.1.1.1 | 1. 設備安全防護 | |
| 4.1.1.1.1 | (1)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? | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------------|
| 4.1.1.2 | (2) 端末主機房之各項安全防護措施是否適當？ | 金融控股公司法第 42 條 |
| 4.1.2 | 2. 程式、資料檔案管理 | |
| 4.1.2.1 | (1) 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責人員陪同？ | |
| 4.1.2.2 | (2) 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？ | |
| 4.1.2.3 | (3) 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？ | |
| 4.1.2.4 | (4) 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，以防外洩及非法使用？ | |
| 4.1.2.5 | (5) 對於程式及資料檔案毀損時是否訂有重建之程序？ | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|--|---------|
| 4.1.2.6 | (6)對於重要之程式(含系統、應用程式)及資料檔案是否備份異地存放？ | |
| 4.1.3 | 3. 媒體管理 | |
| 4.1.3.1 | (1)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？ | |
| 4.1.3.2 | (2)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？ | |
| 4.1.4 | 4. 操作管理 | |
| 4.1.4.1 | (1)端末系統是否備有操作手冊供操作員參考使用？ | |
| 4.1.4.2 | (2)端末系統在開關機時是否由專人依照所指定之程序執行？ | |
| 4.1.4.3 | (3)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 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| 4.1.4.4 | 核？ (4)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？ | |
| 4.2 | (二)端末機作業管理 | |
| 4.2.1 | 1. 端末機使用管理 | |
| 4.2.1.1 | (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責任？登記簿是否與電腦使用人員資料檔內容相符？ | |
| 4.2.1.2 | (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？ | |
| 4.2.1.3 | (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？ | |
| 4.2.1.4 | (4)作業卡遺失時是否即時向主管人員報 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|----------|---|---------|
| 4.2.1.5 | 備，並註銷該作業卡號？ (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？ | |
| 4.2.1.6 | (6)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？ | |
| 4.2.1.7 | (7)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？ | |
| 4.2.1.8 | (8)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？ | |
| 4.2.1.9 | (9)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之交易？ | |
| 4.2.1.10 | (10)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 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|----------|---|--|
| 4.2.1.11 | 無共用同一使用者代號或作業卡之情形？ (11)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？ | |
| 4.3 | (三)人員管理與訓練 | |
| 4.3.1 | 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？ | |
| 4.3.2 | 2. 對每一作業是否至少有兩人以上可互為備援？ | |
| 4.3.3 | 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？ | |
| 4.3.4 | 4. 端末主機或端末機操作員是否接受適當之訓練？ | |
| 5 | 五、守法性 | |
| 5.1 | (一)金控公司是否已將「客戶資料保密措施」公告張貼於該公司之全球資訊網網站上，並連結於首頁明顯處？內容是否包含金控公司 | 1. 財政部 91.4.18 台財融(一)字第 0911000120 號令第 1 點 |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---|
| 5.2 | <p>及其子公司對於客戶個人資料、往來交易資料及其他相關資料訂定之書面保密措施等重要事項？</p> <p>(二)金控公司與子公司及各子公司間若涉及共用資訊系統設備時，是否就費用之分攤及法律責任之歸屬訂立契約，費用之分攤是否訂定公平合理之分攤原則？</p> | <p>2. 本會 112.1.9 金管銀法字第 11102253601 號令</p> <p>1. 金融控股公司及其子公司自律規範第 16 條「為確保屬於客戶資料之安全及避免因不當運用而損害客戶之權益，金融控股公司之子公司應建立客戶資料庫，妥善儲存、保管及管理客戶相關資料，並建立該客戶資料庫之安全措施，僅被授權員工始可使用客戶資料」</p> <p>2. 本會 93.9.13 金管銀（一）字第 0938011562 號令第 3 點與第 4 點「…三、金融控股公司應與授權得運用資</p> |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|--|---|
| 5.3 | (三)對於客戶資料庫之運用、維護及系統使用人員權限設定等之管理事宜，是否訂定書面管理政策？是否與使用及管理資料庫資料之員工，簽訂保密協定切結書？對資料庫之存取授權管理，是否建立適足之控管程序？ | <p>料庫之員工，簽訂保密協定切結書。四、金融控股公司應確保資料傳輸之安全性，並對於資料庫之運用、維護、系統使用人員權限設定及產出表報之管理等事宜，訂定妥適之書面管理政策…」</p> <p>1. 本會 93.9.13 金管銀（一）字第 0938011562 號令第 4 點「金融控股公司應確保資料傳輸之安全性，並對於資料庫之運用、維護、系統使用人員權限設定及產出表報之管理等事宜，訂定妥適之書面管理政策…」</p> <p>2. 本會 94.11.9 金管銀（六）</p> |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|--|--|
| 5.4 | (四)金控公司與各子公司間資訊共享(用)作業平台系統查核。 | 字第 0946000937 號函第 2 點「為有效統一控管對客戶個人資料使用之作業，應設置專人負責控管各子公司客戶不同意公司繼續使用其個人資料之資訊…」 |
| 5.4.1 | 1. 是否開發金控公司與各子公司間資訊共享(用)作業平台系統？系統開發、建置是否有由業務、稽核、會計、企畫等有關單位參與，以求操作、管理、查核各方面之考慮周全？ | |
| 5.4.2 | 2. 資訊共享(用)作業平台運作，是否制定妥適且周延之管理規範？如：資訊傳輸安全機制、資料庫之運用、維護及系統使用人員權限設定、產出表報之管理、資料及程式異動 | |

| 項 目 編 號 | 查 核 事 項 | 法 令 規 章 |
|---------|---|---------|
| 5.4.3 | 控管程序、緊急備援措施等。 | |
| 5.4.4 | 3. 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？ | |
| 5.4.5 | 4. 若有對客戶個人資料使用之作業，是否設置專人負責控管各子公司客戶不同意公司繼續使用其個人資料之資訊？ | |
| | 5. 金融控股公司與其子公司及各子公司間進行共同行銷，於揭露、轉介或交互運用客戶基本資料時，其身分證統一編號及出生日除供作為電腦程式交叉比對之工具外，系統是否設計不得顯示於使用者端任何產出資訊，包含畫面查詢、畫面顯示、產出表報等？ | |