柒、電腦作業與資訊提供：AC-20000

一、資訊部之功能及職責劃分 AC-21000

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AC-21000	資訊部之功能及職責劃分之稽核 目的： 確定上述作業是否符合規定辦理	每半年一次	一、資訊部之組織功能，是否明確訂定。 二、資訊部內各單位之職掌設計，是否未與不同單位權責重疊。 三、資訊部與業務單位之權責，是否明確劃分。 四、資訊作業人員是否皆填具保密切結書；離職時是否取消其識別碼，並收繳其通行證、卡及相關證件。	

二、應用系統維護管理之稽核：AC-22000

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AC-22000	應用系統維護管理之稽核 目的： 確定上述作業是否符合規定辦理	每半年一次	一、已認可之系統開發計畫是否包含下列項目： 計劃之目的及範圍是否定義完成。 針對各種可行方案是否合理估計成本效益並作比較分析。 二、是否依系統開發階段訂定合理的進度表。 三、新系統開發時、是否依現況調查、系統分析規劃、概要設計、程式撰寫、單元設計、整體測試、及系統轉換、併行測試之標準發展階段進行。 四、依系統分析規劃階段所完成之需求分析報告，是否與相關業務單位充分討論。 五、系統分析報告是否包含下列項目： 現行系統之問題點及其改善方式。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
			新系統之成本效益比較分析。 新系統之輸入、輸出及內部流程之明確列出。 六、所引進之套裝軟體是否具有合法之版權。 七、委外作業是否簽訂契約。 八、委外人員之電腦通行使用權，是否設有適當之控管程序，委外期間結束後，是否立即收回該項權利。 九、已完成之程式因故需維護時，是否依據經過正式核准之程序辦理。 十、各項文件與手冊是否經適當維護與控制。	

三、電腦系統管理之稽核：AC-23000

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AC-23000	電腦系統管理之稽核 目的： 確定上述作業是否符合規定辦理	每半年一次	一、電腦設備之購置與管理： 電腦機房硬體設備之運轉及故障情況是否存有紀錄，並向資訊單位負責人報告。 各硬體設備故障之原因經分析後，是否採取適當之措施，並將處理情形列入紀錄。 為確定維護內容，是否與廠商訂有書面維護契約。做完維護時是否留存維護紀錄，並由資訊部派人會同廠商維護人員共同檢查。 是否訂定設備報廢作業程序，報廢前是否將機密性、敏感性資料及授權軟體予以移除、實施安全性覆寫或實體破壞，是否確保報廢電腦硬碟資料不可還原，並留存報廢紀錄，若委託第三者銷毀時，是否簽訂保密合約。 二、電腦作業系統環境設定及使用權限設定：	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
			電腦作業系統環境設定及使用權限設定是否經有關主管核示，並由系統管理人員執行。 電腦系統檔案異動前後是否皆有完善之備份處理措施。 密碼是否以亂碼方式儲存。 三、系統使用者管理： 對於程式及檔案之存取使用，是否應按權限區分並有詳細的書面管制說明。 使用者第一次使用系統時，是否於變更初始密碼後方可繼續作業。 人員異動時，是否及時更新其使用權限。 四、應用系統異動管理： 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。 程式經修改其相關文件是否及時更新。	

四、電腦作業管理之稽核：AC-24000

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AC-24000	電腦作業管理之稽核 目的： 確定上述作業是否符合規定辦理	每週一次	一、實體安全管理： 電腦機房是否有門禁管制(例如：刷卡)。 機房內是否有防火設施，並定期檢驗，且將地震、水災等天然災害因素列入考量。 電腦設備是否有獨立之電源供應系統，其電源供應系統是否含不斷電設備及發電機。 二、資料輸入管理： 安全性或重要性較高之資料，是否由權責單位主管授權後才執行輸入或修改。 所輸入或修改之資料及其執行人員姓名、職稱是否皆留存記錄。 對隱密性高之重要資料是否以亂碼後之資料形式存放。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
			為業務需要以電腦所處理或蒐集之個人資料，是否依「電腦處理個人資料保護法」之規定向主管機關登記。 三、資料輸出管理： 報表是否按時產生並分送各使用單位。 機密性、敏感性之報表列印或瀏覽是否有適當之管制程序。 四、儲存媒體管理： 重要軟體及其文件、清冊是否抄錄備份，存於另一安全處所。 重要之備份檔案及軟體若儲存於與電腦中心同一建築物內，是否鎖存於防火之房間或防火且防震之防火櫃中。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
			存放備份資料之儲存媒體，是否於其標籤上註明存放資料之名稱及保存期限。 對客戶經由網際網路等電子式交易型態所為之交易委託及查詢，其電腦稽核紀錄(log)是否至少保留五年，但買賣委託有爭議者保留至爭議消除為止。 五、電腦操作管理： 操作人員是否確實依規定操作程序執行。 操作日誌是否詳實記載並逐日經主管核驗。 操作疏失是否已檢討改進。 系統主控台所留下之紀錄，是否經專人檢查訊息內容且定期呈主管核驗。	

五、備援及回復作業之稽核：AC-25000

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AC-25000	備援及回復作業之稽核 目的： 確定上述作業是否符合規定辦理	每半年一次	一、故障復原程序是否明確訂定，並製成文件。 二、故障復原程序是否週期性測試，測試後是否召開檢討會議，針對測試缺失謀求改進。	

六、資訊提供作業之稽核：AC-26000

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AC-26000	資訊提供作業之稽核 目的： 確定上述作業是否符合規定辦理	每半年一次	一、期貨交易資訊設備是否依規定設置及使用。 二、除有依「電腦處理個人資料保護法施行細則」第 39 條規定得不公告之事項(有關期貨經理事業之人事、勤務、薪給、衛生、福利或其他相關事項者；專供試驗性電腦處理者；將於依法所為之公告前刪除者；其他法律特別規定者)，或有妨礙職務執行、妨害第三人重大利益之虞者外，對於客戶就其個人資料向期貨經理事業查詢、閱覽或製給複製本之請求，是否依相關規定辦理。	

七、網路安全管理作業之稽核：AC-27000

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AC-27000	網路安全管理作業之稽核 目的： 確定上述作業是否符合規定辦理	每月一次	一、網路系統安全評估： 是否定期評估自身網路系統安全，並留存相關紀錄。 是否適時修補網路運作環境之安全漏洞，並留存相關文件。 有關電腦網路安全之事項，是否隨時公告。 各電腦主機、重要軟硬體設備是否有專人負責。 二、防火牆之安全管理： 是否建立防火牆。 防火牆是否有專人管理。 防火牆進出紀錄及其備份是否至少保存兩個月。 重要網站及伺服器系統(如網路下單系統等)是否以防火牆與外部網際網路隔離。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
			防火牆系統之設定是否經權責主管之核准。 三、網路系統備援與設備備援： 交易主機是否備援。 網路下單主機是否備援。 其他重要網路設備(例如：防火牆、路由器及線路等)是否有備援措施。 四、網路使用者帳號管理： 初始密碼是否隨機產生，並與使用者身分無關。 密碼輸入錯誤次數達五次者，是否中斷連線。 五、電腦病毒及惡意軟體之防範： 是否安裝防毒軟體，並及時更新程式及病毒碼。 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄(含電子郵件)。 防毒是否涵蓋個人端及網路伺服器端電腦。	