柒、電腦作業與資訊提供之稽核：AC-10000

目　　錄

一、 資訊處理部門之功能及職責劃分之稽核：AC-10100

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-10100	資訊處理部門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	不定期：每半年至少查核乙次	一、資訊單位之組織及功能： (一).資訊處理單位之組織功能是否基於職能適當分工，訂定權責分工及職務說明，並規劃適當之職務代理人。 (二).資訊處理單位內各單位職掌設計，是否避免不同單位權責重疊現象。 二、資訊單位人員工作執掌說明 (一).資訊處理單位與業務單位之權責是否明確劃分。 (二).資訊作業人員是否填具保密切結書；並於離職時取消其識別碼且收繳其通行證、卡及相關證件。 三、資訊單位人員之聘用與教育訓練 (一).是否定期(每年至少一次)對全公司員工辦理資訊安全宣導講習（例如：防毒、資料備份、使用合法軟體及電子郵件使用規定等），並留存紀錄。	法令規章： 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 使用表單： 無

二、 系統開發及程式修改之控制作業之稽核：AC-10200

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-10200	系統開發及程式修改之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	**一、**系統開發控制作業： (一).資訊單位是否評估使用單位實際作業需求，確認可行且有開發新系統必要，簽呈送請相關主管會簽，判定是否執行系統開發作業。 (二).資訊單位辦理委外開發之採購作業時，是否根據使用者需求邀集相關單位共同規劃解決方案，實際查詢廠商的成功案例，評選有能力按需求完成系統開發工作的最佳廠商。 (三).合約內容是否包含委外時程表、完成時間、維護方式、付款方式、版權、軟硬體需求、交付文件、相關賠償方式及規定所有必要之安全要求等，委外作業合約內容應完備嚴密。資訊單位人員是否根據合約內容控管該委外案件之執行。 **二、**程式修改控制作業： (一).資訊單位權責主管是否核准系統開發/程式變更申請單，以確認程式修改需求係經相關權責人員充分考量程式變更的必要性及其風險。 (二).系統開發人員是否編製系統規格需求說明書，與使用單位進行討論瞭解細部需求，是否除留存各階段會議紀錄外，並由使用單位確認。 (三).資訊人員是否建置有獨立之開發及測試環境，以維護正式環境之資料。系統開發及程式修改作業是否皆於開發及測試環境執行。 (四).資訊單位是否會同申請單位於測試環境測試開發或修改完成之系	**法令規章：** 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期稽字第 09600018150 號 3.金管證期七字第 0950160204 號函 4.台期（稽）字第 09300034210 號 5.台財證字第 0930115938 號函 **使用表單：** 1.系統開發/程式修改申請單 2.系統規格需求說明書 3.系統上線申請單

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			統或程式，將測試結果記錄於系統開發/程式變更申請單，並檢附相關報表及畫面。 (五).系統負責人是否進行上線變更申請程序並填寫系統上線申請單，經資訊單位主管簽核並確認預定上線日期，由經資訊單位主管授權之執行人員負責將系統上線至系統正式環境。 (六).系統上線至系統正式環境，資訊人員是否建立軟體更新的版本控制機制。 (七).上線完成後，資訊單位應用系統管理組人員是否將系統開發/程式變更申請單、系統規格需求說明書及系統上線申請單編號歸檔後留存。	

三、 編製系統文書之控制作業之稽核：AC-10300

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-10300	編製系統文書之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、 新資訊系統之開發，資訊單位人員或委外廠商是否編寫完整之系統文件，包含：系統規格書、系統文件、使用者操作說明書、系統測試記錄、驗收文件等。 二、 資訊單位人員編寫、維護系統程式時，是否於程式中適當註解，並依程式異動內容，適時修改與更新相關系統文件，並記錄更新人員、範圍、時間以及版本，資訊單位權責主管是否定期檢視系統文書之編製與管理作業。 三、 各項系統文件與使用手冊，是否設專人保管，避免未授權之存取；系統文書之出借或發送，電腦軟體／書籍借用記錄表是否經資訊單位之權責主管允許並授權後，由保管人員負責執行。 四、 保管人員離職時，主管是否指派交接之保管人員。 五、 若確定舊版本之系統文件、使用手冊已無須再使用，保管人是否於資訊單位主管核准後將其報廢。	**法令規章：** 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.系統文件 2.電腦軟體／書籍借用記錄表 3.系統規格書 4.使用者操作說明書 5.系統測試紀錄 6.驗收文件

四、 程式及資料存取之控制作業之稽核：AC-10400

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-10400	程式及資料存取之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、程式及資料存取之控制作業(含作業及應用系統)： (一).使用者權限之設定，是否依其業務職責以及職能分工原則設定權限，每位系統使用者是否皆擁有個別之使用者帳號，並使用密碼設定，以確保程式及資料存取之安全。 (二).授權使用者存取系統資源前，是否依系統別填寫帳號密碼新增/異動申請單，並經由申請單位主管核准後始予開放。 二、主機資源控制作業： (一).機房系統作業之執行是否由專人負責，於事前經系統負責人核准並由主管覆核。 (二).置於危險場所或登入系統風險等級極高之終端機，於閒置時是否於一定時間後自動關機或登出，避免未經授權之存取。 (三).重要之系統公用程式、工具及指令是否依其使用者職權限制其存取權限，是否僅系統管理者帳號具執行權限，由系統管理人員持用並於負責人員調、離職時列入移交項目。 (四).一般應用系統之使用者除執行應用系統外，是否無存取系統主機公用程式、工具及指令權限。 (五).系統開發及程式撰寫人員對於上線系統之程式與資料檔案是否無存取權限。 (六).系統主機是否設置電腦工作日誌，供系統操作員記載系統作業之情狀，並定期由主管覆核。	法令規章： 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.帳號密碼新增/異動申請單 2.電腦工作日誌 3.稽核日誌 4.委外合約

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			(七).電腦主機之作業系統、應用系統及資料庫管理系統中是否設置稽核日誌，以記錄任何可能危害系統安全事件。 (八).公司外部人員（包含維護廠商）之帳號是否妥善監控，並於非使用時期取消其存取權限。 三、密碼及權限管控作業 (一).對於公司之重要系統，是否建立適當之密碼控管原則，包含錯誤登入次數、密碼最短長度、複雜性以及變更週期等。 (二).使用者第一次使用系統時，是否立即更新初始密碼後方可繼續作業。 (三).密碼是否以亂碼方式儲存，對因忘記密碼而無法登入系統之使用者重新申請核發密碼時，是否採取嚴格確認其身分及核發程序後，方可開放其使用系統。 (四).使用者於離職前，或因職務調動需異動帳號時，是否以帳號密碼新增/異動申請單通知資訊組人員辦理帳號刪除事宜，並將該帳號密碼新增/異動申請單編號歸檔備查。 (五).使用者帳號及權限是否由相關主管與系統負責人，定期依使用者職責及職能分工原則覆核，並檢查及取消閒置帳號。	

五、 資料輸出入之控制作業之稽核：AC-10500

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-10500	資料輸出入之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、資料輸入管理 (一).資料之輸入及修改是否經授權，並於輸入前查驗資料輸入之正確性，依相關之原始資料輸入。 (二).原始相關資料及憑證，是否由各單位專人負責保管，並存於安全處所。 (三).各項輸入資料是否配合原始相關資料及憑證編製序號，資料輸入控制是否配合序號控管，遇有漏號或單據遺失，是否立即追蹤，以確保資料之完整性。 (四).在輸入之資料轉換為電腦可閱讀之形式時，須嚴加控制，是否適當併用自動化與人工之控制程序，以確保資料輸入正確。 (五).系統是否建立作業流程以確保輸入之資料係經過驗證和編輯且盡可能符合交易實質內容，程式化之輸入格式可確保資料係依正確之格式輸入正確之欄位。 二、資料輸出管理 (一).輸出資料是否分發予適當授權之人，機密性及敏感性之資料輸出設計有適當管控程序，由專人負責輸出、分送、保管，並建立分發清單及簽收紀錄。 (二).系統是否產生重要資料鍵入、主檔變更及系統自動產生交易之審計軌跡報告（如交易明細報告），以供核對及調節原始輸入憑證。 三、更正例外或異常輸出項目： (一).發現資料錯誤是否會同相關人員查明原因，並填寫電腦系統資料異動	**法令規章：** 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.電腦系統資料異動申請單 2.分發清單及簽收記錄 3.審計軌跡報告

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			申請單報請權責主管核准修正後，更正資料並將申請單與相關文件妥善保存備查。 (二).更正例外或異常項目之再輸入是否調節至原例外或異常項目。	

六、 資料處理之控制作業之稽核：AC-10600

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-10600	資料處理之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、電腦主機作業 (一).資料處理之相關資訊設備是否由資訊人員於購入時與廠商簽訂維護合約。 (二).機器運轉中如發生異常狀況，是否判斷是否會影響進行中之工作，如需立即停機時，是否立刻通知使用者暫停作業，由資訊人員依據故障之訊息作初步處理，待修復完畢並運轉正常後，再行通知使用者重新使用，並是否將處理情形記錄於機房工作紀錄表中。如無法自行排除時，是否立即通知維護廠商派員前來處理，並留下服務紀錄。 二、應用系統軟體 (一).應用系統是否設計適當之功能、控制流程，以確保處理資料之完整性、正確性。 (二).系統是否針對重要資料、重要批次作業，分別設計產生自動檢核序號、處理參數的複查機制之控制。 (三).應用系統之交易紀錄是否登錄於正確之會計期間。 (四).系統是否提供使用者作業處理中各項錯誤或作業失敗之訊息，並產生錯誤報表以利追蹤更正。 (五).資訊人員是否及時追蹤並更正例外或異常之訊息，並由專人覆核、更正並定期追蹤處理情形。	法令規章： 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.機房工作記錄表 2.維護合約 3.使用者操作說明書

七、 檔案及設備之安全控制作業之稽核：AC-10700

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-10700	檔案及設備之安全控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、資料檔案之安全控制 (一).應用程式及資料檔，是否依其重要性執行日、週、月、年等不同週期之備份作業。 (二).備份之資料媒體是否適當記錄於備份紀錄表中，並於備份儲存媒體貼上內外標籤以利辨識備份內容。 (三).備份資料是否定期執行測試作業，以確保備份資料之可用性。 (四).備份資料是否異地存放，媒體存放處所環境應合於電腦機房安全標準。 二、電腦設備之安全控制 (一).是否建立系統自動偵測病毒之機制，並要求所有人員定期更新病毒碼。 (二).購入資訊設備資訊組是否會同使用單位驗收，並登記於資訊設備清單列冊管理。 (三).移轉資訊設備是否填具設備移轉紀錄單，經移出與移入單位經辦人員與主管簽核後送交資訊組存查。 (四)是否訂定電腦設備報廢作業程序；電腦設備報廢前是否將機密性、敏感性資料及授權軟體予以移除，是否實施安全性覆寫或實體破壞，是否確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，是否留存報廢紀錄；若委託第三者銷毀時，是否簽訂保密合約。	法令規章： 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.備份記錄表 2.備份資料測試紀錄表 3.備份磁帶異地存放紀錄表 4.資訊設備清單 5.設備移轉記錄單 6.資訊設備報廢申請單 7.設備借用記錄表 8.電腦機房進出管制登記表

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			(五)電腦設備及其存放之資料於報廢時是否填具資訊設備報廢申請單，申請進行報廢程序，以避免機密資料流失。 (六)行動式電腦設備之攜出攜入是否填寫設備借用紀錄表。 三、通訊設備管理 (一).通信網路是否加強安全防禦，以防止資料遭截取，並於必要時採取加密措施。 (二).若設備線路發生故障時，資訊組是否派員立即檢查，以瞭解線路故障原因，必要時通知廠商或電信單位進行維修。 四、電腦機房之管制 (一).電腦機房是否設有適當之門禁管制；資訊單位人員對非作業人員進出電腦機房，是否請其登記於電腦主機房進出管制登記表，並於資訊組人員陪同下方可進入，嚴禁未經許可人員擅入機房。 (二).資訊單位主管是否定期覆核授權進出機房人員，並檢視門禁管制紀錄。 (三).機房內是否設置獨立之空調設備、高架地板、自動電壓穩定裝置、不斷電系統 (UPS)及電源供應器、自動火警偵測及緊急照明設備等機房防護設備。 (四).各項支援防護設備及週邊設備是否定期檢查與維護，以測試其堪用性。 (五)機房內是否放置其他易燃或危險物品。	

八、 硬體及系統軟體之購置、使用及維護之控制作業之稽核：AC-10800

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-10800	硬體及系統軟體之購置、使用及維護之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、電腦硬體及系統軟體之購置 (一).使用單位是否填寫電腦軟/硬體設備申請單經主管覆核後送交資訊單位。 (二).資訊單位是否評估相容性、擴充性、業務特性及成本效益後，開立符合需求之硬體設備。 (三).資訊單位人員填寫之請購單，是否經資訊單位權責主管覆核後送交採購單位採購。 (四).是否由資訊單位執行驗收作業，確認驗收完成交付使用單位保管使用，並登記於資訊設備清單列冊管理。 (五).資訊軟、硬體設備及作業管理委外管理之辦理，是否遵循內部控制制度之採購及付款循環之規定。 二、電腦硬體及系統軟體之使用 使用單位對於電腦硬體及系統軟體之使用及維護是否依照操作手冊之說明進行操作。 三、軟、硬體設備維護 (一).資訊單位人員是否定期維護重要系統主機，若經資訊單位評估須由委外廠商提供維護服務者，是否與委外廠商簽訂維護合約。 (二).資訊單位人員是否於合約到期前提出續約申請，經相關權責主管核准後進行採購作業。 (三).與委外廠商簽訂維護合約，是否訂定適當之資訊安全協定，規範	法令規章： 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 4.台期稽字第 09600018150 號 5.金管證期七字第 0950160204 號函 **使用表單：** 1.電腦軟/硬體設備申請單 2.請購單 3.資訊設備清單 4.設備借用記錄表 5.電腦軟體／書籍借用記錄

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			委外廠商系統維護所接觸資料之安全管理。 (四).主機系統維護工作，是否避免停機並干擾使用者，儘可能安排在夜間、假日或無人使用狀態下進行停機作業之處理。 (五).電腦軟硬體定期維護是否留下紀錄。如維護作業由委外廠商執行是否確認維護程序皆依照維護合約所述進行，並留下服務紀錄。 (六).一般事務性電腦設備於發生故障時，使用者是否填寫電腦硬體設備故障送修申請單通知資訊單位派員維修，並記錄機器故障原因及維修狀況。 (七).經資訊單位人員確認硬體設備故障需送交廠商維修者，是否填寫服務聯絡單，經申請單位主管核准後由資訊單位辦理。	表 6.電腦硬體設備故障送修申請單 7.服務聯絡單

九、 系統復原計畫制度及測試程序之控制作業之稽核：AC-10900

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-10900	系統復原計畫制度及測試程序之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、系統復原計畫之規劃 (一).重要主機是否制定有系統故障或緊急應變措施與辦法。 (二).系統復原計畫是否涵括各層級負責人員工作事項。 (三).系統復原計畫中是否列示公司中重要的業務及電腦系統及其相關復原程序。 (四).系統復原計畫中是否列示復原之地點及備援之電腦設備、系統軟、硬體。 二、系統復原計劃之測試及演練 (一).公司(期貨信託事業)之交易主機是否有備援措施。 (二).系統復原計畫是否安排定期演練，並於內部教育訓練中執行系統復原計畫之訓練及宣導。 (三).系統復原計畫是否安排定期測試，以驗證計畫是否完整。 (四)系統復原計畫是否定期測試應邀請各相關單位參與，並於測試後驗證與檢討。 (五)系統復原計畫是否有專人負責與相關單位進行檢討。 三、系統復原計劃之更新 (一).系統復原計畫是否定期更新問題偵測及控制技術、人員組織調整變動、人員聯絡資料變動、業務流程的變動或實務作業的變更等相關事項。 (二).系統復原計畫的更新是否呈報主管核准，並將相關的訊息告知相	法令規章： 1.證券暨期貨市場各服務事業建立內部控制制度處理準則 第 10 條 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 **使用表單：** 1.系統復原計畫 2.測試紀錄表

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			關人員。	

十、 資通安全檢查之控制作業之稽核：AC-11000

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-11000	資通安全檢查之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、 資訊安全政策 (一).是否依據相關法令規定及公司業務需求，訂定資訊安全政策。 (二).所訂定之資訊安全政策，是否經管理階層核准，並正式發布要求所有員工共同遵守。 (三).訂定之資訊安全政策，是否至少每年評估乙次，並留存相關紀錄。 (四).公司每年是否將前一年度資訊安全整體執行情形，由資訊安全長或負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具「證券暨期貨市場各服務事業建立內部控制制度處理準則」第二十四條規定之內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過，並將該聲明書內容揭露於主管機關指定之申報網站。 二、 建立資訊安全組織 (一).是否指定副總經理或高層主管人員成立跨單位組織負責規劃、執行及推動資訊安全管理事項、風險評估、及安全分級。 (二).公司是否視資訊安全管理需要及所屬資安分級，指定專人或專責單位負責規劃與執行資訊安全工作，且資訊安全專責人員及專責主管每年是否定期參加十五小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年是否至少接受三小時以上資訊安全宣導課程。 三、 人員安全與管理 (一).員工皆是否填具保密切結書；離職時應取消其識別碼，並收繳其	法令規章： 1.證券暨期貨市場各服務事業建立內部控制制度處理準則第 10 條、第 36 條之 2 2.台期（稽）字第 09300034210 號 3.台財證字第 0930115938 號函 4.台期（稽）字第 09600018150 號 5.金管證期七字第 0950160204 號函 使用表單： 無

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			通行證、卡及相關證件。 (二).是否依員工職務層級施予適當的資訊安全教育訓練，每年並達內部所定之訓練時數，並留存紀錄。 (三).是否落實個人資訊設備之控管。 四、 資產分類與控管 (一).是否製作所有與每一資訊系統相關之重要資產清冊並隨時更新。 (二).是否制定一套與組織採用之分類方式相符之資訊標示與處理流程。 (三).是否訂定資訊安全分級標準，並對各類資產做相對之控管。 五、 內部稽核及其他 (一).稽核人員是否受過適當之稽核訓練。 (二).是否依照內部控制制度之電腦作業與資訊提供循環排定內部稽核計畫，並按計畫執行查核。 (三).是否建立完整之軟體使用清冊。 (四).內部稽核計畫是否涵蓋合法軟體之應用及個人資料保護法等相關規定。	

十一、 向主管機關指定網站進行公開資訊申報控制作業之稽核：AC-11100

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-11100	依規定向主管機關指定網站進行公開資訊申報者,其相關作業之控制作業之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每半年至少查核乙次	一、 總窗口是否負責掌控所有輸入之資訊依相關規範如期完成申報作業。 二、 權責主管是否覆核申報之書面資料，經核對無誤後，方由總窗口執行資料確認。 三、 負責申報人員遇職務異動時，是否清楚交接公開資訊申報應注意事項。 四、 是否依「個人資料保護法」,妥善處理客戶資料。 五、 於所設網站上提供股市即時交易資訊，是否經由與期交所簽約之資訊公司提供。 六、 使用電子憑證ＩＣ卡、其他類型憑證晶片卡或其他憑證載具等代表公司簽署之作業（例如：期信基金資訊觀測站申報系統、公文電子交換系統等)，該等憑證載具是否由專人負責保管並設簿登記，且應訂定相關帳號、密碼保管及使用程序，並據以執行，並定期執行備份。 七、 使用代表公司憑證載具簽署之作業系統端若屬期貨信託事業應用系統者（例如：電子對帳單系統)，是否留存電腦稽核紀錄（log)，其保存年限比照各作業資料應保存年限。 八、 登入密碼是否依主管機關規定之期限內定期變更之。 九、 初次取得之電子憑證金鑰是否立即變更密碼，其後是否亦定期變更之。	法令規章： 1.證券暨期貨市場各服務事業建立內部控制制度處理準則第 10 條 使用表單： 無

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			十、 電子憑證金鑰是否確實於到期前申請展期，以免影響申報作業。 十一、 最高使用權限人員設定使用者之帳號及權限，是否依各業務範圍及權責設定。 十二、 權責主管是否覆核定期或不定期申報公開資訊之正確性。 十三、 公司是否定期或不定期稽核依電腦處理個人資料保護法定義之個人資檔案管理情形。 十四、 是否定期檢查網站內對外提供之資訊，對具機密性、敏感性之資訊內容，是否立即移除。 十五、 各種重要法令規章及通知是否立即張貼於公布欄。 十六、 個人資料檔案之資料，其更新、更正或註銷是否報經核准，並將更新、更正、註銷內容、作業人員及時間詳實記錄。	

十二、新興科技應用之稽核：AC-11200

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
AC-11200	新興科技應用之稽核 目的： 確定上述作業是否符合規定辦理	不定期：每年至少查核乙次	一、雲端服務(涉及關鍵性系統、資料或服務者需符合以下要求) (一)公司為雲端服務使用者時，是否訂定雲端運算服務運作安全規範，內含雲端提供者之遴選機制、查核措施、備援機制、服務水準(含資訊安全防護)與復原時間要求等，如有不符需求之虞，是否有其他補償性措施。 (二)公司為雲端服務提供者時，是否訂定雲端運算服務安全控管措施，內容是否包含法律遵循、權限控管、權責歸屬及資訊安全防護等項目。如涉及敏感性資料之傳遞，是否使用超文字傳輸安全協定(HTTPS)、安全檔案傳輸協定(SFTP)等加密之網路協定。 二、社群媒體： (一)是否訂定社群媒體相關資訊安全規範與運用社群媒體管理辦法，並包含下列項目： 1.界定可於公務用社群媒體上分享之業務相關資料。 2.界定私人與公務用社群媒體之區別與應注意事項。 (二)是否針對開放員工使用社群媒體評估其風險程度，包含：資料外洩、社交工程、惡意程式攻擊等，並採行適當的安全控管措施。 (三)是否訂定經營官方社群媒體資訊安全規範與管理辦法，並包含下列項目：	法令規章： 1.中華民國期貨業商業同業公會「新興科技資訊安全自律規範」 2.證券期貨市場相關公會新興科技資訊安全管控指引 使用表單： 無

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			1.是否事先了解所經營之社群媒體隱私政策，並定期檢視其隱私政策之異動及評估其風險。 2.於官方網站提供連結供使用者連至公司外之社群媒體時，是否出現提示視窗告知使用者該連結非公司本身之網站。 3.對經營之社群媒體是否標示期貨商名稱、聯絡方式，以區別為官方經營之社群媒體。 4.是否建立帳號權限管理機制，對發布內容進行控管與監視，並針對不適當言論及異常事件，進行必要之通報或處置。 三、行動裝置 是否訂定行動裝置之資訊安全規範與管理辦法，並包含以下項目： (一)公務用行動裝置設備管理辦法： 1.公務用行動裝置管理辦法對於申請、使用、更新、繳回與審核是否訂有相關規範。 2.人員異動時，是否進行重新配置或清除配置程序，以確保行動裝置環境安全性。 3.對公務用之行動裝置是否避免安裝非官方發布之行動應用程式，或僅安裝由公司列出通過檢測可安裝之行動應用程式。 (二)員工自攜行動裝置管理辦法，是否包含以下項目： 1.是否要求員工自攜行動裝置使用用途。 2.是否與持有人簽署員工自攜行動裝置使用協議，含：使用限	

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			制及雙方責任等。 3.是否限制內部資訊設備透過員工自攜行動裝置私接存取網際網路(Internet)之行為。 (三)是否訂定行動應用程式之發布規範與管理辦法，並包含下列要點： 1.應用程式發布前，是否確認程式碼或程序庫符合以下安全事項： (1)通過內容安全或驗證程序，如：程式原始碼檢測或掃描，確認未含惡意程式碼與有敏感性資料。 (2)行動應用程式是否完整定義特殊符號篩選機制。 2.無法取得行動應用程式原始碼時，是否要求行動應用程式提供者符合前項安全事項。 (四)是否訂定行動應用程式安全控管規範與管理辦法，須包含以下項目： 1.是否針對交易或帳務等敏感性資料設計行動應用程式存取驗證機制，並僅供經授權之行動應用程式使用該敏感性資料。 2.透過行動應用程式發送簡訊或其他訊息通知方式告知使用者敏感性資料時，是否進行適當去識別化。 3.透過行動應用程式傳送帳號、密碼及其他敏感性資料時，是否以憑證驗證或加密機制確保傳送安全。	

編　號	作業項目	作業週期	作　業　程　序（方　法）及　稽　核　重　點	依據資料
			4.透過行動應用程式儲存密碼、憑證、交易或帳務等敏感性資料時，是否對儲存之資料進行雜湊(Hash)或加密控管保護。 5.透過行動應用程式處理交易或金流作業時，是否留存存取日誌，且存取日誌是否予以保護以防止未經授權存取。 四、物聯網 是否訂定物聯網相關資訊安全規範與管理辦法，須包含下列項目： (一)是否建立物聯網設備管理清冊並至少每年更新一次，且應變更前開設備之初始密碼。 (二)物聯網設備是否具備安全性更新機制且定期更新，如存在已知弱點無法更新時，是否建立補償性管控機制。 (三)是否關閉物聯網設備不必要之網路連線及服務，避免使用對外公開的網際網路位置。	