證券商內部控制制度標準規範—內部稽核實施細則修訂對照表(112 年)

編號	作業項目	修 訂 後 內 容	修 訂 前 內 容	修訂說明
AC-11000	風險評鑑與管理之稽核目的：確定上述作業是否符合規定辦理	(一)~(三)略 (四) 公司是否評估核心系統可容忍中斷時間、復原時間目標(RTO)、資料復原點目標(RPO)。	(一)~(三)略 (四) 核心系統是否評估可容忍中斷時間。	配合內部控制制度 CC-11000 之修訂，並同時修訂查核明細表(FC-11000-M)。

AC-17000 17010 網路安全管理（適用網際網路下單證券商，另1~7、9、13~15、20~26項並適用於所有證券商）	網路安全管理之稽核目的：確定上述作業是否符合規定辦理	(一)、網路安全管理 1、~3、略。 4、是否使用生命週期終止(End of Service, EOS/End of Life, EOL)之網路設備，並針對 EOS/EOL 之網路設備擬定汰除相關計畫。 5、是否建立防火牆，並設專人管理，且防火牆進出紀錄及其備份是否至少保存三年。 6、防火牆系統之設定是否經權責主管之核准。 7、公司建立網路設備規則是否以最小授權及正面表列為原則。 8、網路下單畫面是否採加密方式(例如：SSL)處理且網路下單是否全面使用認證機制。 9、公司使用多因子驗證是否具下列三項之任兩項技術：(1)公司所約定之資訊，且無	(一)、網路安全管理 1、~3、略。 (新增) 1、是否建立防火牆，並設專人管理，且防火牆進出紀錄及其備份是否至少保存三年。 2、防火牆系統之設定是否經權責主管之核准。 (新增) 3、網路下單畫面是否採加密方式(例如：SSL)處理且網路下單是否全面使用認證機制。 (新增)	配合內部控制制度 CC-17000之修訂，並同時修訂查核明細表(FC-17000-M)。

		第三人知悉（如固定密碼、圖形鎖或手勢等）。(2)客戶所持有之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等），公司應確認該設備為客戶與公司所約定持有之設備。(3)客戶提供給公司其所擁有之生物特徵（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），公司應直接或間接驗證該生物特徵。 10、網路下單是否訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，是否採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及 SIM 認證等)驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。 11、公司是否於伺服器端驗證客戶交易身分及使用者帳號。 12、公司對電子交易身分之申請、交付、使用、更新與驗證是否訂定相關規範。	4、網路下單是否訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，是否採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及 SIM 認證等)驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。 (新增) (新增)	

		13、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)。 14、防毒是否涵蓋個人端（含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦。 15、公司是否訂定電子郵件使用安全政策及建立郵件過濾機制，以防範電腦病毒擴散，影響電腦安全。 16、是否定期檢查網路下單系統提供之功能，並留存紀錄。 17、公司提供客戶使用應用程式介面(API)服務，是否於首次下單前就相關傳輸設定進行連線測試，並留存相關測試紀錄。 18、公司提供網際網路下單業務時，兼顧客戶服務品質，是否訂定網際網路下單服務品質相關標準，並包含下列重點如：交易之安全性、交易之穩定及系統可用性、提供客戶服務。	5、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)。 6、防毒是否涵蓋個人端(含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦。 7、公司是否訂定電子郵件使用安全政策及建立郵件過濾機制，以防範電腦病毒擴散，影響電腦安全。 8、是否定期檢查網路下單系統提供之功能，並留存紀錄。 9、公司提供客戶使用應用程式介面(API)服務，是否於首次下單前就相關傳輸設定進行連線測試，並留存相關測試紀錄。 10、公司提供網際網路下單業務時，兼顧客戶服務品質，是否訂定網際網路下單服務品質相關標準，並包含下列重點如：交易之安全性、交易之穩定及系統可用性、提供客戶服務。	

		19、是否就提供外部連線使用網路系統偵測網頁與程式異動、記錄並通知相關人員處理。 20、公司網路是否依用途區分為 DMZ、營運環境、測試環境及其他環境，並有適當區隔機制(如防火牆、虛擬區域網路、實體隔離等)。 21、個人資料及機敏資料是否存放於安全的網路區域，不得存放於網際網路等區域。 22、系統是否僅開啟必要之服務及程式，未使用之服務功能是否關閉。 23、公司是否建立遠端連線管理辦法，對使用外部網路遠端連線至公司內部作業進行控管及身分認證，留存相關維護紀錄並由權責主管定期覆核。 24、公司是否每年定期檢視並維護防火牆存取控管設定，並留存相關檢視紀錄。	11、是否就提供外部連線使用網路系統偵測網頁與程式異動、記錄並通知相關人員處理。 12、公司網路是否依用途區分為 DMZ、營運環境、測試環境及其他環境，並有適當區隔機制(如防火牆、虛擬區域網路、實體隔離等)。 13、個人資料及機敏資料是否存放於安全的網路區域，不得存放於網際網路等區域。 14、系統是否僅開啟必要之服務及程式，未使用之服務功能是否關閉。 15、公司是否建立遠端連線管理辦法，對使用外部網路遠端連線至公司內部作業進行控管，留存相關維護紀錄並由權責主管定期覆核。 16、公司是否每年定期檢視並維護防火牆存取控管設定，並留存相關檢視紀錄。	

		25、公司是否至少每年檢視一次對外網路設備規則，並留存相關紀錄。 26、公司是否建立上網管制措施，以避免下載惡意程式。 27、公司是否偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。 28、公司是否依其所屬資安分級定期對提供網際網路服務之核心系統辦理滲透測試，並依測試結果進行改善。 29、公司是否依其所屬資安分級定期辦理資通安全健診。 30、公司是否依其所屬資安分級建立資通安全威脅偵測管理機制(應含括異常分析、事件收集、偵測攻擊)。 31、公司是否依其所屬資安分級建立入侵偵測及防禦機制。 32、公司是否依其所屬資安分級設置應用程式防火牆。	(新增) 17、公司是否建立上網管制措施，以避免下載惡意程式。 18、公司是否偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。 19、公司是否依其所屬資安分級定期對提供網際網路服務之核心系統辦理滲透測試，並依測試結果進行改善。 20、公司是否依其所屬資安分級定期辦理資通安全健診。 21、公司是否依其所屬資安分級建立資通安全威脅偵測管理機制(應含括異常分析、事件收集、偵測攻擊) 22、公司是否依其所屬資安分級建立入侵偵測及防禦機制。 23、公司是否依其所屬資安分級設置應用程式防火牆。	

		33、公司是否依其所屬資安分級辦理進階持續性威脅攻擊防禦措施。	24、公司是否依其所屬資安分級辦理進階持續性威脅攻擊防禦措施。	
		34、核心系統身分驗證機制是否有防範自動化程式之登入或密碼更換嘗試。	(新增)	
		35、公司是否每日針對核心系統之帳號登入失敗紀錄、非客戶帳號嘗試登入紀錄等進行監控及分析，發現有帳號登入異常情事(如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、帳戶申請或更新憑證下載異常)，是否即時了解異常原因，並留存相關紀錄。	25、公司是否每日針對核心系統之帳號登入失敗紀錄、非客戶帳號嘗試登入紀錄等進行監控及分析，發現有帳號登入異常情事(如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、帳戶申請或更新憑證下載異常)，是否即時了解異常原因，並留存相關紀錄。	
		36、公司提供網路下單服務，是否於網路下單登入時採多因子認證方式(例如：固定密碼、圖形鎖、下單憑證、綁定裝置、OTP、生物辨識等機制)，以確保為客戶本人登入。	26、公司提供網路下單服務，是否於網路下單登入時採多因子認證方式(例如:下單憑證、綁定裝置、OTP、生物辨識等機制)，以確保為客戶本人登入。	
		37、公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣是否即通知客戶，並留存紀錄，避免非客戶本人登入情	27、公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣是否即通知客戶，並留存紀錄，避免非客戶本人登入	

		事：(1) 密碼輸入錯誤或帳戶被鎖定；(2)申請或更新憑證；(3)變更基本資料；(4)異常來源或行為嘗試登入等;(5)密碼申請異動或補發時。 38、公司是否依其所屬資安分級對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，並定期檢視以確認機制有效運作：(1)同一來源 IP 登入不同帳號達一定次數以上；(2) 同一帳號在一定時間內由不同國家登入；(3) 異常來源 (如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單或國外 IP)嘗試登入。	情事：(1) 密碼輸入錯誤或帳戶被鎖定；(2)申請或更新憑證；(3)變更基本資料；(4)異常來源或行為嘗試登入等；(5)密碼申請異動或補發時。 28、公司是否依其所屬資安分級對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，並定期檢視以確認機制有效運作：(1) 同一來源 IP 登入不同帳號達一定次數以上；(2) 同一帳號在一定時間內由不同國家登入；(3) 異常來源 (如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單或國外 IP)嘗試登入。	

17020 電腦系統及作業安全管理	電腦系統及作業安全管理之稽核目的： 確定上述作業是否符合規定辦理	(二)、電腦系統及作業安全管理 1、電腦設備之購置是否參閱採購及付款循環及固定資產循環等規定辦理。 2、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。 3、電腦系統檔案異動前後皆是否有完善之備份處理措施。 4、資通系統內部時鐘是否定期與基準時間源進行同步。 5、公司是否依其所屬資安分級對核心系統重要組態設定檔案及其他具保護需求之資訊進行加密或以其他適當方式儲存。 6、公司是否依其所屬資安分級訂定對核心系統之閒置時間或可使用期限與核心系統之使用情況及條件(如：帳號類型與功能限制、操作時段限制、來源位址限制、連線	(二)、電腦系統及作業安全管理 1、電腦設備之購置是否參閱採購及付款循環及固定資產循環等規定辦理。 2、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。 3、電腦系統檔案異動前後皆是否有完善之備份處理措施。 (新增) (新增) (新增)	

		數量及可存取資源等)。 7、重要軟體及其文件、清冊是否抄錄備份，存於另一安全處所。 8、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。 9、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。 10、公司是否依據系統特性與資料復原點目標（RPO），考量備份頻率、儲存媒體類型（光碟、外接硬碟、磁帶）、資料類型（虛擬機映像檔、系統源碼、資料庫與組態設定檔等）、備份類型（完整備份、增量備份與差異備份）、備份方式（網路同步寫入、網路非同步寫入與離線備份）等，制定適當之資料備份機制，如採離線備份是否依備份類型建立適當的備份基準(baseline)，以確保資料可正確回存。	4、重要軟體及其文件、清冊是否抄錄備份，存於另一安全處所。 5、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。 6、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。 (新增)	

		11、操作人員是否確實依規定操作程序執行。 12、是否建立機密性及敏感性資料媒體之相關處理程序，防止資料洩露或不當使用。 13、電腦系統軟、硬體發生異常操作人員是否及時通知相關人員，並將異常情形詳實記載於操作日誌。 14、操作日誌是否詳實記載並逐日經主管核驗，操作人員不可與主管為同一人。 15、操作疏失是否檢討改進。 16、系統主控台所留存之紀錄，是否經專人檢查訊息內容且定期呈主管核驗。 17、公司（證券經紀商）是否配備經營業務所需、且有適足容量之電腦系統。 18、公司（證券經紀商）之電腦系統是否訂定定期（每年至少乙次）由內部或委託外部專業機構評估電腦系統容量及安全措施之機制與程序，定期對系統容量進行壓力測試，並留存紀錄。	7、操作人員是否確實依規定操作程序執行。 8、是否建立機密性及敏感性資料媒體之相關處理程序，防止資料洩露或不當使用。 9、電腦系統軟、硬體發生異常操作人員是否及時通知相關人員，並將異常情形詳實記載於操作日誌。 10、操作日誌是否詳實記載並逐日經主管核驗，操作人員不可與主管為同一人。 11、操作疏失是否檢討改進。 12、系統主控台所留存之紀錄，是否經專人檢查訊息內容且定期呈主管核驗。 13、公司（證券經紀商）是否配備經營業務所需、且有適足容量之電腦系統。 14、公司（證券經紀商）之電腦系統是否訂定定期（每年至少乙次）由內部或委託外部專業機構評估電腦系統容量及安全措施之機制與程序，定期對系統容量進行壓力測試，並留存紀錄。	

		19、為正確且安全運轉資訊系統，是否訂定日常各種作業處理程序手冊。	15、為正確且安全運轉資訊系統，是否訂定日常各種作業處理程序手冊。	
		20、為確定電腦設備維護內容，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單位派人會同廠商維護人員共同檢查。	16、為確定電腦設備維護內容，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單位派人會同廠商維護人員共同檢查。	
		21、是否建立回存測試機制，以驗證備份之完整性及儲存環境的適當性。	17、是否建立回存測試機制，以驗證備份之完整性及儲存環境的適當性。	
		22、公司是否建立系統最高權限帳號管理辦法(含作業系統及應用系統)，如需使用最高權限帳號時須取得權責主管同意，並留存相關紀錄。	18、公司是否建立系統最高權限帳號管理辦法(含作業系統及應用系統)，如需使用最高權限帳號時須取得權責主管同意，並留存相關紀錄。	
		23、公司是否建立並落實個人電腦、伺服器及網路通訊設備之安全性組態基準(如密碼長度、更新期限等)。	19、公司是否建立並落實個人電腦、伺服器及網路通訊設備之安全性組態基準(如密碼長度、更新期限等)	
		24、公司透過網際網路使用帳號登入系統時，是否採用多因子認證機制。	20、公司透過網際網路使用帳號登入系統時，是否採用多因子認證機制。	

AC-18000	存取控制之稽核目的：確定上述作業是否符合規定辦理	(一)、~(五)、略。 (六)、是否定期(至少每半年一次)審查資通系統帳號及權限之適切性，並視審查結果停用資通系統閒置帳號(~~使用者為客戶者~~客戶帳號除外)。 (七)、公司是否建立資通系統帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 (八)、資通系統帳號是否定義人員角色及責任，授權是否採最小權限原則，僅允許使用者(或代表使用者行為之程序)依公司部門權責及業務功能，完成作業所需之授權存取。 (九)、使用者第一次使用系統時，是否更新初始密碼後方可繼續作業。 (十)、密碼是否使用公開安全且未遭破解之演算法(例如：雜湊演算法等不可逆運算式)產生亂碼並加密儲存。；初始密碼是否隨機產生，並與使用者或客戶身分	(一)、~(五)、略。 (六)、是否定期(至少每半年一次)審查並檢討久未使用之使用者權限(使用者為客戶者除外)。 (新增) (新增) (七)、使用者第一次使用系統時，是否更新初始密碼後方可繼續作業。 (八)、密碼是否使用公開安全且未遭破解之演算法(例如：雜湊演算法等不可逆運算式)產生亂碼並加密儲存。；初始密碼是否隨機產生，並與使用者或客戶身分無	配合內部控制制度 CC-18000之修訂，並同時修訂查核明細表(FC-18000-M)。

		無關。(本項不適用採自行訂定交付電子式交易密碼條之方式)。 (十一)、 密碼輸入錯誤次數達三次者，是否予中斷連線且鎖定該帳號，並留存紀錄。公司於接獲客戶聯繫申請解除鎖定時，是否確實辨認身分(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，並留存相關紀錄後，始得辦理之。 (十二)、 對於使用者及客戶忘記密碼之處理，公司是否有嚴格的身分確認程序(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可再次使用系統。 (十三)、 除語音按鍵下單，公司是否使用優質密碼設定(長度六個字元(含)以上，且具有文數字或符號)並進行管控。 (十四)、 客戶密碼超過一年未變更或變更密碼與前一代相同，公司是否做妥善處理。除客戶外，公司其他使用者之密碼是否至少每三個月變更一次。	關。(本項不適用採自行訂定交付電子式交易密碼條之方式)。 (九)、密碼輸入錯誤次數達三次者，是否予中斷連線且鎖定該帳號，並留存紀錄。公司於接獲客戶聯繫申請解除鎖定時，是否確實辨認身分(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，並留存相關紀錄後，始得辦理之。 (十)、對於使用者及客戶忘記密碼之處理，公司是否有嚴格的身分確認程序(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可再次使用系統。 (十一)、除語音按鍵下單，公司是否使用優質密碼設定(長度六個字元(含)以上，且具有文數字或符號)並進行管控。 (十二)、客戶密碼超過一年未變更或變更密碼與前一代相同，公司是否做妥善處理。除客戶外，公司其他使用者之密碼是否至少每三個月變更一次。	

		(十五)、 檢查公司現有之網站、伺服器、網路芳鄰、路由器、交換器、作業系統及資料庫等軟硬體設備是否設定使用密碼，且避免使用預設(如administrator、root、sa)或簡易(如 1234)之帳號密碼及未設管理者存取權限。 (十六)、 為防止密碼洩漏，是否採取不顯示、不印錄等措施。 (十七)、 客戶申請採電子式交易型態者，公司以電子方式交付電子密碼條時，是否傳送 OTP(One Time Password)密碼至客戶開戶留存之手機號碼，及將加密後之電子密碼條以電子方式傳送至客戶留存之電子信箱，此流程相關系統紀錄是否留存。 (十八)、 公司是否對客戶申請電子式交易型態者採自訂交付電子密碼條訂有電子交易密碼之作業程序。 (十九)、 公司是否對客戶申請電子式交易型態者採自訂交付電子密碼條訂定電子式	(十三)、檢查公司現有之網站、伺服器、網路芳鄰、路由器、交換器、作業系統及資料庫等軟硬體設備是否設定使用密碼，且避免使用預設(如administrator、root、sa)或簡易(如 1234)之帳號密碼及未設管理者存取權限。 (十四)、為防止密碼洩漏，是否採取不顯示、不印錄等措施。 (十五)、客戶申請採電子式交易型態者，公司以電子方式交付電子密碼條時，是否傳送 OTP(One Time Password)密碼至客戶開戶留存之手機號碼，及將加密後之電子密碼條以電子方式傳送至客戶留存之電子信箱，此流程相關系統紀錄是否留存。 (十六)、公司是否對客戶申請電子式交易型態者採自訂交付電子密碼條訂有電子交易密碼之作業程序。 (十七)、公司是否對客戶申請電子式交易型態	

		交易密碼交付流程與安全控管機制相關內部控制制度。 (二十)、 對重要系統（如主機連線系統、網路下單系統等）之稽核日誌紀錄內容是否包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項，並由專人定期檢視。 (二十一)、 核心系統電腦稽核紀錄(日誌)是否建立監控機制，處理失效時，是否採取適當之行動。 (二十二)、 安全性或重要性較高之資料，是否由權責主管人員核可後始得執行輸入或修改。 (二十三)、 所輸入或修改之資料及其執行人員姓名、職稱皆是否留存紀錄。 (二十四)、 對重要及機密性檔案其存取使用是否依規定之作業程序辦理。 (二十五)、 對隱密性高之重要資料（例如：密碼檔）是否以亂碼後之資料形式存	者採自訂交付電子密碼條訂定電子式交易密碼交付流程與安全控管機制相關內部控制制度。 （十八）、對重要系統（如主機連線系統、網路下單系統等）之稽核日誌紀錄內容是否包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項，並由專人定期檢視。 （新增） （十九）、安全性或重要性較高之資料，是否由權責主管人員核可後始得執行輸入或修改。 （二十）、所輸入或修改之資料及其執行人員姓名、職稱皆是否留存紀錄。 （二十一）、對重要及機密性檔案其存取使用是否依規定之作業程序辦理。 （二十二）、對隱密性高之重要資料（例如：	

		放。 (二十六)、公司如屬公開發行公司者，是否於內部控制制度納入「公開發行公司網路申報公開資訊應注意事項」，並據以辦理相關申報事宜。 (二十七)、公司是否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。 (二十八)、使用電子憑證ＩＣ卡或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：「公開資訊觀測站」、「證券商申報單一窗口」、「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。 (二十九)、使用前揭代表公司憑證載具簽	密碼檔）是否以亂碼後之資料形式存放。 （二十三）、公司如屬公開發行公司者，是否於內部控制制度納入「公開發行公司網路申報公開資訊應注意事項」，並據以辦理相關申報事宜。 （新增） （二十四）、使用電子憑證ＩＣ卡或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：「公開資訊觀測站」、「證券商申報單一窗口」、「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。 （二十五）、使用前揭代表公司憑證載具	

		署之作業系統端（server 端）若屬證券商應用系統者(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。	簽署之作業系統端(server 端)若屬證券商應用系統者（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。	
		(三十)、 是否依「個人資料保護法」,妥善處理客戶及公司內部人個人資料。	（二十六)、是否依「個人資料保護法」,妥善處理客戶及公司內部人個人資料。	
		(三十一)、 公司是否依「個人資料保護法」妥善處理公司保有之個人資料，並定期或不定期稽核依「個人資料保護法」定義之個人資料管理情形。	（二十七)、公司是否定期或不定期稽核依「個人資料保護法」定義之個人資料管理情形。	
		(三十二)、 前揭個人資料，其更新、更正或註銷均是否報經備查，並將更新、更正、註銷內容、作業人員及時間詳實記錄	（二十八)、前揭個人資料，其更新、更正或註銷均是否報經備查，並將更新、更正、註銷內容、作業人員及時間詳實記錄	
		(三十三)、 因經營業務需要而為個人資料之蒐集、處理或國際傳輸及利用，是否訂定「與軟硬體廠商機密維護及損害賠償等雙方權責劃分」。	（二十九）因經營業務需要而為個人資料之蒐集、處理或國際傳輸及利用，是否訂定「與軟硬體廠商機密維護及損害賠償等雙方權責劃分」。	
		(三十四)、 報表是否按時產生並分送各使	（三十）報表是否按時產生並分送各使	

		用單位。 (三十五)、機密性或敏感性報表列印或瀏覽是否有適當管制程序。 (三十六)、投資人於公司網站查詢個人資料是否具有加密傳輸機制(例如：SSL)。 (三十七)、電子式及非電子式交易型態以電子郵件執行成交回報之傳輸，公司對姓名、帳號及信用帳號等機敏資訊，是否依「機敏資訊類型及隱匿之具體作法原則」辦理。 (三十八)、相關留存紀錄是否確保數位證據之收集、保護與適當管理程序，且是否至少留存三年。 (一)、～（八）略。 （九） 資訊軟、硬體設備及作業管理有委外	用單位。 （三十一）機密性或敏感性報表列印或瀏覽是否有適當管制程序。 （三十二）投資人於公司網站查詢個人資料是否具有加密傳輸機制(例如：SSL)。 （三十三）電子式及非電子式交易型態以電子郵件執行成交回報之傳輸，公司對姓名、帳號及信用帳號等機敏資訊，是否依「機敏資訊類型及隱匿之具體作法原則」辦理。 （三十四）相關留存紀錄是否確保數位證據之收集、保護與適當管理程序，且是否至少留存三年。 （一）～（八）略 （九）資訊軟、硬體設備及作業管理有委外	

AC-19000	系統開發及維護之稽核 目的： 確定上述作業是否符合規定辦理	管理情形者，是否符合下列事項： 1、委外作業是否簽訂契約，且委外作業契約內容是否包含~~資訊安全協定與對委外廠商資安稽核權等條款~~以下內容：合約期限、服務範圍、服務交付日期、服務水準要求、服務變更規範、服務驗收之標準、資通安全事件通報及應變處理作業程序、對資訊服務供應商之稽核權條款、合約轉讓或同意分包之規範、保密義務條款、罰則與損害賠償條款、爭議處理程序、違約處理條款、合約終止規範、合約終止後之處理、保固、權利及責任。 2、略。 3、公司是否評估資訊服務供應商之集中度，包括評估資訊服務供應商作業能力，採取適當風險管控措施，確保作業委外處理之品質，並注意作	管理情形者，是否符合下列事項： 1、委外作業是否簽訂契約，且委外作業契約內容是否包含資訊安全協定與對委外廠商資安稽核權等條款。 2、略。 (新增)	配合內部控制制度 CC-19000之修訂，並同時修訂查核明細表(FC-19000-M)。

		業委託資訊服務供應商之適度分散以控管作業風險。		
		4、資訊服務供應商是否提供安全性檢測證明（如行動應用程式資安檢測、源碼檢測、弱點掃描等），並確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式是否通過程式碼掃描或黑箱測試。	(新增)	
		5、公司應訂定相關規範管控，與資訊服務供應商資訊委外關係於終止、解除或結束後之相關作業。	(新增)	
		6、委外資訊服務供應商是否揭露第三方程式元件之來源與授權證明。	(新增)	
		7、公司是否管控資訊服務供應商存取權限，對於電腦通行使用權利進行適當控管。	(新增)	
		8、公司是否對資訊服務供應商服務內容變更進行風險評估。	(新增)	

		9、公司對於委外資訊服務供應商於委外關係所涉及公司資訊資產，是否於委外關係終止、解除或結束時完整歸還、確保銷毀或轉交予其他資訊服務供應商，並要求資訊服務供應商持續遵守保密承諾。 (十)、 ～（四十五）略。 (四十六)、 涉及投資人使用之行動應用程式於初次上架前及每年是否委由經財團法人全國認證基金會(TAF)認證合格之第三方檢測實驗室進行並完成通過資安檢測，檢測範圍以目的事業主管機關~~經濟部工業局委託執行單位~~「行動應用App~~資安式基本資安檢測基準項目~~」進行檢測。（適用網際網路下單證券商） (四十七)、 ～（五十）略 （五十一）核心系統是否針對風險評估使用者頁面僅顯示簡短錯誤訊息及代碼，不包含	（十）～（四十五）略。 （四十六） 涉及投資人使用之行動應用程式於初次上架前及每年是否委由經財團法人全國認證基金會(TAF)認證合格之第三方檢測實驗室進行並完成通過資安檢測，檢測範圍以經濟部工業局委託執行單位「行動應用資安式基本資安檢測基準項目進行檢測。（適用網際網路下單證券商） （四十七） ～（五十）略。 新增	

		詳細之錯誤訊息。 (五十二)提供網際網路下單服務之核心系統上架前及系統更新時是否執行「源碼掃描」安全檢測。 (一)、～（二）略	(新增) （一） ～（二）略。 （三）公司（證券經紀商）之交易主機是否	

AC-20000	營運持續管理之稽核 目的： 確定上述作業是否符合規定辦理	（三）、公司（證券經紀商）之交易主機是否有備援措施，並依所屬資安分級建置異地備援機房。 （四）、公司是否擬訂營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之維護，並擬訂關鍵性業務及其衝擊影響分析，評估核心系統中斷造成之衝擊程度，並依核心系統之復原時間目標(RTO)、資料復原點目標(RPO)，作為恢復核心系統、備份備援規劃及執行復原作業之依據，再依其所屬資安分級定期辦理業務持續運作演練。 （五）略。 （六）公司針對與資訊系統有關之資訊安全或服務異常事件，是否依「證券期貨市場資通安全事件通報應變作業注意事項」及「證券商通報重大資安事件之	有備援措施。 （四）公司是否擬訂營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之維護，並擬訂關鍵性業務及其衝擊影響分析，再依其所屬資安分級定期辦理業務持續運作演練。 （五）略。 （六）公司針對與資訊系統有關之資訊安全或服務異常事件，是否依「證券期貨市場資通安全事件通報應變作業注意事項」辦理，並採取適當矯正程序，留存紀錄。	配合內部控制制度 CC-20000之修訂，並同時修訂查核明細表(FC-20000-M)。

		範圍申報程序及其他應遵循事項」辦理，並採取適當矯正程序，留存紀錄。		
		（七）～（九）略。	（七）～（九）略	
		（十） 公司是否辨識風險情境，就各項風險情境當災害發生造成資訊作業異常或中斷時，擬定各系統之應變、減災或復原措施 相關作業流程。	（新增）	
		（十一） 核心系統原服務中斷時，是否於可容忍時間內，由備援設備或其他方式取代並提供服務。	（新增）	
		（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）雲端服務(涉及關鍵性系統、資料或服務者需符合以下要求)	

AC-21100	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	證券商是否事先評估使用雲端運算服務之風險，若雲端運算服務涉及關鍵性系統、資料或服務者，是否訂定雲端運算服務相關運作安全規範。 1. 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~~服務提供者之遴選機制、查核措施、備援機制、服務水準(含資訊安全防護)與復原時間及服務終止措施要求等，如有不符需求之處，需有其它補償性措施。 2. 略。 （二）社群媒體 1. ~2略。 3.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。 (1) ~(2)略。 (3) 對經營之社群媒體是否標示證券商名稱、聯絡方式、許可證字號、客戶申	(新增) 1. 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，如有不符需求之處，需有其它補償性措施。 2. 略。 （二）社群媒體 1.~2.略。 3.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。 (1) ~(2)略。 (3) 對經營之社群媒體是否標示證券商名稱、聯絡方式，以區別為官方經營之	配合內部控制制度 CC-21100之修訂，並同時修訂查核明細表(FC-21100-M)。

		訴聯繫方式及處理窗口，以區別為官方經營之社群媒體。 (4) 略。 （三）略。 （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： 1. 略。 2. 略。 3. 略。 4. 公司採購物聯網設備時，是否宜優先採購取得資安標章之物聯網設備。 5. 公司是否定期辦理物聯網設備使用及管理人員資安教育訓練。 6. 公司是否建立物聯網設備存取權限控管措施。 （五）略 （六）深度偽造(Deepfake)	社群媒體。 (4) 略 （三）略。 （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： 1. 略。 2. 略。 3. 略。 4. 公司採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。 5. 公司是否定期辦理物聯網設備使用及管理人員資安教育訓練。 (新增) (五)略 (新增)	

		1.使用影像視訊方式進行身分驗證時是否強化驗證並搭配其他驗證因子(如上傳身分證件、手機簡訊OTP)。 2.是否定期辦理涵蓋深度偽造認知及防範議題之資訊安全教育訓練。		