證券商內部控制制度標準規範—內部稽核實施細則修正對照表

編號	作業項目	修正後內容	修正前內容	修正說明
AC-17010（適用網際網路下單證券商，另1~7、13~15、20~28、40、41~~、4、5、6、7、8、9、10、11、17、18、20、21、22、23、24、25、26、~~	通訊與作業管理－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	作業週期：不定期（每月至少查核乙次） (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)之軟體及網路設備，且於到期前擬定汰除計畫，並視情況建立補償性措施~~並針對 EOS／EOL 之網路設備擬定汰除相關計畫~~。 5~12(略) 13、是否定期對~~電腦~~資通系統及資料儲存媒體進行病毒掃~~瞄~~描(含電子郵件)。 14~22(略) 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多因子身分認證，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	作業週期：不定期（每月至少查核乙次） (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。 3~12(略) 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)。 14~22(略) 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	配合內部控制制度 CC-17010 調整，同時修正查核明細表。

~~27、34、~~項並適用於所有證券商）		控管設定，每半年檢視 DMZ 區之防火牆規則，是否包含評估高風險設定及六個月內無流量之防火牆之必要性，及針對已下線資通系統於六個月內是否調整或停用該規則，並留存相關檢視紀錄。 25(略) 26、公司是否建立軟體白名單控管機制~~上網管制措施，以避免下載惡意程式~~。 27(略) 28、公司是否每年定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。 29、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。 30、公司是否依其所屬資安分級定期辦理資通安全健診。 31、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)	控管設定，每半年檢視 DMZ 區之防火牆規則，並留存相關檢視紀錄。 25(略) 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。 (新增) 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)	

		32、公司是否依其所屬資安分級建立入侵偵測及防禦機制。 33、公司是否依其所屬資安分級設置應用程式防火牆。 34、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。 35、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。 36、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。 37、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)，以確保為式(客戶本人登入。 38、公司對於客戶帳號登入時宜進行通知，如	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。 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。 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。 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。 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。 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。 39、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。 40、公司設置無線網路是否採用現行公開資訊已認可且無弱點之安全協定。 41、公司提供內部無線網路使用是否限內部人員公務用或資訊服務供應商是否於申請核准後使用。	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。 (新增) (新增)	

AC-17020	作業管理－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	作業週期:不定期(每半年至少查核乙次) (以下略)	作業週期:不定期(每半年至少查核乙次) (以下略)	