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（109年度）

編號	作業項目	修訂後內容	修訂前內容	修訂說明
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	作業週期：不定期（每半年至少查核乙次） (一)~(四十)略 (四十一)、行動應用程式是否於可信任來源之行動應用程式商店或網站發布，且是否於發布時說明欲存取之敏感性資料、行動裝置資源及宣告之權限用途。（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商） (四十二)、是否於官網上提供行動應用程式之名稱、版本與下載位置。（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商） (四十三)、是否建立偽冒行動應用程式偵測機制，以維護客戶權益。（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商） (四十四)、啟動行動應用程式時，如偵測行動裝置疑似遭破解（如root、jailbreak、USB debugging 等），是否提示使用者注意風險。（適用網際網路下單證券商，不適用語音下單及傳統下單	作業週期：不定期（每半年至少查核乙次） (一)~(四十)略 (新增)	為強化證券商行動應用程式(APP)資安標準及配合資通安全檢查機制之修訂，增訂系統開發及維護（CC-19000）之行動應用程式安全管理項次。

		之證券商） (四十五)、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「行動應用資安聯盟」公布之行動應用程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，不適用語音下單及傳統下單之證券商） (四十六)、如通過實驗室檢測後一年內有更新上架之需要，是否於每次上架前就重大更新項目進行委外或自行檢測；所謂重大更新項目為與「下單交易」、「帳務查詢」、「身份辨識」及「客戶權益有重大相關項目」有關之功能異動。檢測範圍是否以OWASP MOBILE TOP 10 之標準為依據，並留存相關檢測紀錄。(適用網際網路下單證券商，不適用語音下單及傳統下單之證券商) (四十七)、對第三方檢測實驗室所提交之行動應用程式檢測報告，是否建立覆核		為確保行動應用程式更新上架時安全性，避免因更新頻繁存有資安空窗期之虞及確保檢測項目與內容一致，修訂相關規範。

		機制，以確保檢測項目及內容一致，並留存覆核紀錄。(適用網際網路下單證券商，不適用語音下單及傳統下單之證券商） (四十八)、是否於發布前檢視行動應用程式所需權限與提供服務相當，首次發布或權限變動應經資安、法遵單位同意，並留有紀錄，以利綜合評估是否符合個人資料保護法之告知義務」。(適用網際網路下單證券商，不適用語音下單及傳統下單之證券商)		為控管行動應用程式發布時所需權限與提供服務相當，參酌銀行公會規範修訂相關內容。