建立證券商資通安全檢查機制修訂對照表（109 年度）

修　訂　後　內　容	修　訂　前　內　容	修訂說明
1.-8.略 9.系統開發及維護（CC-19000，半年查核） (1)-(9)略	1.-8.略 9.系統開發及維護（CC-19000，半年查核） (1)-(9)略	
(10) 程式原始碼安全規範（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）： a.程式應避免含有惡意程式等資訊安全漏洞。 b.程式應使用適當且有效之完整性驗證機制，以確保其完整性。 c.程式於引用之函式庫有更新時，應備妥對應之更新版本。 d.程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。 e.無法取得程式原始碼時，應要求程式提供者符合上開前四項(a、b、c、d)安全事項。	(10)新增	調整 12.新興科技應用之(3)行動裝置項下 c 與 d 項至 9.系統開發及維護之(10)程式原始碼安全規範與(11)行動應用程式安全管理項下
(11)行動應用程式安全管理（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）： a. 行動應用程式發布： (a) 行動應用程式應於可信任來源之行動應用程式商店或網站發布，且應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。 (b) 應於官網上提供行動應用程式之名稱、版本與下載位置。 (c) 應建立偽冒行動應用程式偵測機制，	(11)新增	為強化證券商行動應用程式(APP)資安標準，經參考銀行及保險業行動應用程式相關規範，於系統開發及維護（CC-19000）增

以維護客戶權益。 (d) 應於發布前檢視行動應用程式所需權限應與提供服務相當，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」。 b. 敏感性資料保護： (a) 行動應用程式傳送及儲存敏感性資料時應透過憑證、雜湊（Hash）或加密等機制以確保資料傳送及儲存安全，並於使用時應進行適當去識別化，相關存取日誌應予以保護以防止未經授權存取。 (b) 啟動行動應用程式時，如偵測行動裝置疑似遭破解（如 root、jailbreak、USBdebugging 等），應提示使用者注意風險。 c. 行動應用程式檢測： (a) 涉及投資人使用之行動應用程式於初次上架前及每年應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。如通過實驗室檢測後一年		訂行動應用程式安全管理項次。 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。 為確保行動應用程式更新上架時安全性及避免因更新頻繁存有資安空窗期之虞及確保檢測項目與

內有更新上架之需要，應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。檢測範圍以 OWASP MOBILE TOP 10 之標準為依據，並留存相關檢測紀錄。 (b) 公司對第三方檢測實驗室所提交之檢測報告，應建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄。 10~11 略 12.新興科技應用（CC-21100，年度查核） (1)~(2)略 (3)行動裝置： a.(略) b.(略)	12.新興科技應用（CC-21100，年度查核） (1)~(2)略 (3)行動裝置： a.(略) b.(略) ~~c.公司應訂定行動應用程式之發佈規範與管理辦法，須包含以下內容：~~ ~~(a).應用程式發佈前，應確認程式碼或程序庫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。~~ ~~(b).行動應用程式宜完整定義特殊符號篩選機制。~~ ~~(c).無法取得行動應用程式原始碼時，應要求行動應用程式提供者符合前項安全事項。~~	內容一致，修訂相關規範。 調整 c 項至 9.系統開發及維護之(10)程式原始碼安全規範項下

以下略	~~d.公司應訂定行動應用程式安全控管規範與管理辦法，須包含以下內容：~~ ~~(a).應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。~~ ~~(b).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，應進行適當去識別化。~~ ~~(c).透過行動應用程式傳送帳號、密碼及其他敏感性資料時，應以憑證驗證或加密機制確保傳送安全。~~ ~~(d).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，應對儲存之資料進行雜湊（Hash）或加密控管保護。~~ ~~(e).透過行動應用程式處理交易或金流作業時，宜留存存取日誌，且存取日誌應予以保護以防止未經授權存取。~~ 以下略	調整 d 項至 9.系統開發及維護之(10)程式原始碼安全規範項下