證券股份有限公司

電腦作業與資訊提供：系統開發及維護

作業週期：（每半年至少查核乙次）　　查核明細表

項　　目	查　　核　　程　　序	查核結果			底稿索引
		是	否	不適用	
(FC-19000-S) 系統開發及維護	一、應用系統在規劃分析時是否將資訊安全需求納入分析及規格。 二、輸入資料是否作檢查，以確認其正確性。 三、是否使用具有合法版權之軟體。 四、委外廠商管理： (一)與委外資訊服務供應商提供服務是否訂定合約，合約所含內容是否包含以下內容：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。 (二)是否針對資訊委外業務項目之資通安全風險與委外作業可行性，及資訊服務供應商作業能力及集中度，由相關資訊單位共同執行風險評估，評估結果是否提報適當管理層級並取得同意。 (三)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~~掃描、弱點掃描等)，並應確保交付之 系統或程式無惡意程式及後門程式，其放置於網際網路之 程式應通過源碼掃描或黑箱測試。 (四)公司是否就與資訊服務供應商之資訊委外關係於終止、解除或結束後之相關作業，訂定相關規範。 (五)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。 (六)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。 (七)是否對資訊服務供應商服務內容變更進行風險評估。 (八)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				

項　　目	查　　核　　程　　序	查核結果			底稿索引
		是	否	不適用	
	供應商持續遵守保密承諾。 (九)公司是否載明資訊服務供應商配合進行壓力測試及調整服務負載量之義務，並是否於市場交易量、業務變化及客戶屬性等發生顯著異動時發動辦理。 (十)於資訊服務委外期間是否定期對資訊服務供應商進行稽核，並是否要求資訊服務供應商定期提交服務水準報告，相關結果是否提報適當管理層級審查。 五、資訊軟、硬體設備及作業管理有委外管理情形者，是否符合下列事項： (一)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。 (二)委外契約是否明確訂定雙方之責任區分及雙方之資訊人員管理規範。 六、已完成之程式因故需維護時，是否依據經過正式核准之程序辦理。 七、各項文件與手冊是否經適當維護與控制。 八、應用系統之維護是否指派專人負責。 九、應用系統異動管理： (一)正式作業與測試作業之程式、資料、工作控制指令等檔案是否分開存放。 (二)程序經修改其相關文件是否及時更新。 (三)~~系統~~程式變更上線前是否進行完整測試，變更完成後是否檢核與申請內容是否相符，並進行必要驗證以確認變更作業之可用性及正確性。 十、資通系統弱點掃描：(適用網際網路下單證券商) (一)各資通系統是否定期(至少每半年一次)進行弱點掃描。 (二)弱點掃描所辨識出之潛在系統弱點，是否評估其相關風險或安裝修補程式，並留存紀錄。 十一、核心系統~~是否~~發生錯誤時，針對~~風險評估~~使用者頁面是否僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 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。 十三、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，且於發布時是否				

項　　目	查　　核　　程　　序	查核結果			底稿索引
		是	否	不適用	
	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） 十四、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） 十五、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） 十六、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） 十七、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） 十八、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；並留存相關檢測紀錄（適用網際網路下單證券商）。 十九、對第三方檢測實驗室所提交之檢測報告，是否建立覆核機制，以確保檢測項目及內容一致，並留存覆核紀錄（適用網際網路下單證券商）。 二十、是否於發布前檢視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」（適用網際網路下單證券商）。 二十一、委外開發之行動應用程式如涉及機敏性資料傳送(如：客戶帳號密碼或交易資料等)是否自行或委外檢視驗證傳遞對象之妥適性並留存相關紀錄。 二十二、與資訊公司異業合作平台，是否無提供或介接未經金融監督管理委員會許可之證券期貨業者所提供之證券期貨業務（如證券期貨業務有關之開戶及下單功能）。				
備　註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員 _____ 日 期 _____