證券商內部控制制度標準規範—內部控制制度修正對照表

編號	作業項目	修正後內容	修正前內容	修正說明
CC-19000	系統開發及維護	作業程序及控制重點： (一)系統分析： 1.依資訊作業發展計畫，確定欲開發系統之預定作業方式、作業項目、作業內容及作業時程。 2.依規定呈權責主管核示，以確定作業方式係採用委託開發、直接引用現成系統或自行開發。 3.作業方式如採委託開發則依採購程序辦理委託開發，作業方式如採直接引用現成系統則依程序向被引進系統之著作權所有人引進應用系統。 4.與業務單位共同研討、評估業務需求，確定電腦化後之作業方式並完成需求分析報告 5.評估系統引進、開發、維護等過程中所需之各項軟硬體資源後，提出環境評估報告。 6.將需求分析及環境評估等報告依規定呈有關主管核示後確認作業方式。 (二)環境評估報告： 1.環境評估報告於系統分析完成後提出。 2.環境評估報告內容至少包含下列項目： (1)所開發系統或被引進系統之簡介。 (2)所開發系統或被引進系統之作業所需軟、硬體環境。	作業程序及控制重點： (一)系統分析： 1.依資訊作業發展計畫，確定欲開發系統之預定作業方式、作業項目、作業內容及作業時程。 2.依規定呈權責主管核示，以確定作業方式係採用委託開發、直接引用現成系統或自行開發。 3.作業方式如採委託開發則依採購程序辦理委託開發，作業方式如採直接引用現成系統則依程序向被引進系統之著作權所有人引進應用系統。 4.與業務單位共同研討、評估業務需求，確定電腦化後之作業方式並完成需求分析報告 5.評估系統引進、開發、維護等過程中所需之各項軟硬體資源後，提出環境評估報告。 6.將需求分析及環境評估等報告依規定呈有關主管核示後確認作業方式。 (二)環境評估報告： 1.環境評估報告於系統分析完成後提出。 2.環境評估報告內容至少包含下列項目： (1)所開發系統或被引進系統之簡介。 (2)所開發系統或被引進系統之作業所需軟、硬體環境。	1.調整用字一致性；2.增訂程式更版上線前驗證之規定；3.調整文字，以清楚規範適用範圍。

編號	作業項目	修正後內容	修正前內容	修正說明
		(三)系統引進： 1.依系統分析後之決定按規定程序引進有合法版權之套裝軟體。 2.如應用系統委託專業機構辦理者，應注意下列重點： (1)委外作業應簽訂契約，委外作業契約內容應包含資訊安全協定與對委外廠商資安稽核權等條款。 (2)委外作業之開發、設計、程式撰寫、測試、驗收等各階段依合約規定程序進行，並備妥各階段之相關文件。 (3)資訊軟、硬體設備及作業管理有委外管理情形者，應於委外契約（至少應含委外管理範圍、委外管理期間、委外管理費用、委外管理責任、智慧財產權協議、保密義務、查核條款等）中明確訂定雙方電腦資訊作業管理之安全性規範、業務（含內部稽核）之責任區分及雙方之資訊人員管理規範，以達成明確區分公司與接受委外管理公司權責之目的。 (4)資訊軟、硬體設備及作業管理有委外管理情形者，內部稽核人員仍應依內部控制制度之電腦作業與資訊提供循環所規定之週期，確實執行相關稽核作業。 (四)委外廠商管理： 1.公司與委外資訊服務供應商提供服務應	(三)系統引進： 1.依系統分析後之決定按規定程序引進有合法版權之套裝軟體。 2.如應用系統委託專業機構辦理者，應注意下列重點： (1)委外作業應簽訂契約，委外作業契約內容應包含資訊安全協定與對委外廠商資安稽核權等條款。 (2)委外作業之開發、設計、程式撰寫、測試、驗收等各階段依合約規定程序進行，並備妥各階段之相關文件。 (3)資訊軟、硬體設備及作業管理有委外管理情形者，應於委外契約（至少應含委外管理範圍、委外管理期間、委外管理費用、委外管理責任、智慧財產權協議、保密義務、查核條款等）中明確訂定雙方電腦資訊作業管理之安全性規範、業務（含內部稽核）之責任區分及雙方之資訊人員管理規範，以達成明確區分公司與接受委外管理公司權責之目的。 (4)資訊軟、硬體設備及作業管理有委外管理情形者，內部稽核人員仍應依內部控制制度之電腦作業與資訊提供循環所規定之週期，確實執行相關稽核作業。 (四)委外廠商管理： 1.公司與委外資訊服務供應商提供服務應	

編號	作業項目	修正後內容	修正前內容	修正說明
		訂定合約，合約所含內容應包含以下內容：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。 2.公司應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，評估結果應提報適當管理層級並取得同意。 3.資訊服務供應商應提供安全性檢測證明(如行動應用程式資安檢測、源碼**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。 4.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。 5.委外資訊服務供應商應揭露第三方程式元件之來源與授權證明。 6.公司應管控資訊服務供應商存取權限，對	訂定合約，合約所含內容應包含以下內容：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。 2.公司應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，評估結果應提報適當管理層級並取得同意。 3.資訊服務供應商應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。 4.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。 5.委外資訊服務供應商應揭露第三方程式元件之來源與授權證明。 6.公司應管控資訊服務供應商存取權限，對	

編號	作業項目	修正後內容	修正前內容	修正說明
		於電腦通行使用權利進行適當控管。 7.公司應對資訊服務供應商服務內容變更進行風險評估。 8.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，應於委外關係終止、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。 9.委外資訊服務供應商如自行發現程式漏洞、版本老舊，或於使用相同服務之其他證券商應用系統發生故障或異常時，應儘速瞭解原因，並主動轉知及提供因應措施。 10.委外資通系統之服務規格書應包括硬體規格、軟體版本、作業環境變動、作業系統底層架構及系統程式相容性等，並包含維持委外廠商服務水準之要求與橫向溝通機制。 11.公司應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，俾憑評估系統資源調配或擴增。 12.公司於資訊服務委外期間應定期對資訊服務供應商進行稽核，並應要求資訊服務供應商定期提交服務水準報告，相關結果應提報適當管理層級審查。	於電腦通行使用權利進行適當控管。 7.公司應對資訊服務供應商服務內容變更進行風險評估。 8.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，應於委外關係終止、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。 9.委外資訊服務供應商如自行發現程式漏洞、版本老舊，或於使用相同服務之其他證券商應用系統發生故障或異常時，應儘速瞭解原因，並主動轉知及提供因應措施。 10.委外資通系統之服務規格書應包括硬體規格、軟體版本、作業環境變動、作業系統底層架構及系統程式相容性等，並包含維持委外廠商服務水準之要求與橫向溝通機制。 11.公司應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，俾憑評估系統資源調配或擴增。 12.公司於資訊服務委外期間應定期對資訊服務供應商進行稽核，並應要求資訊服務供應商定期提交服務水準報告，相關結果應提報適當管理層級審查。	

編號	作業項目	修正後內容	修正前內容	修正說明
		(五)系統設計： 1.資料庫設計。 2.系統流程設計。 3.系統輸入設計。 4.系統輸出設計。 5.處理設計。 6.控制設計。 7.與有關單位研討上述系統規格並修訂。 8.依規定呈相關權責主管核定後確認。 9.訂定程式設計工作方法。 (六)程式撰寫及單元測試： 1.邏輯設計。 2.依規定編定程式代號。 3.依規定撰寫程式說明。 4.依規定語言及方式撰寫程式。 5.程式編譯、測試及修改。 (七)系統測試： 1.訂定測試計畫，其內容至少包含下列項目： (1)測試目的。 (2)測試完成標準。 (3)測試方法。 (4)測試記錄格式。 2.依測試計畫請應用系統使用單位共同測試，記錄所有測試經過及結果。 3.修改測試過程中之錯誤,並將所有設計上相關之改變配合修訂。	(五)系統設計： 1.資料庫設計。 2.系統流程設計。 3.系統輸入設計。 4.系統輸出設計。 5.處理設計。 6.控制設計。 7.與有關單位研討上述系統規格並修訂。 8.依規定呈相關權責主管核定後確認。 9.訂定程式設計工作方法。 (六)程式撰寫及單元測試： 1.邏輯設計。 2.依規定編定程式代號。 3.依規定撰寫程式說明。 4.依規定語言及方式撰寫程式。 5.程式編譯、測試及修改。 (七)系統測試： 1.訂定測試計畫，其內容至少包含下列項目： (1)測試目的。 (2)測試完成標準。 (3)測試方法。 (4)測試記錄格式。 2.依測試計畫請應用系統使用單位共同測試，記錄所有測試經過及結果。 3.修改測試過程中之錯誤,並將所有設計上相關之改變配合修訂。	

編號	作業項目	修正後內容	修正前內容	修正說明
		4.製作測試報告其內容至少需包含下列項目： (1)測試目的。 (2)測試方法。 (3)測試記錄。 (4)測試結果總評及建議。 (八)系統設置計畫： 1.應用系統上線前系統負責人需訂定應用系統設置計畫，其內容含下列項目： (1)應用系統概述。 (2)容量規劃。 (3)程式及檔案之設定權限。 (4)使用者及使用權限與使用環境之設定。 2.應用系統設置計畫由操作管理人員依據核定之文件執行之。 (九)應用系統操作訓練： 1.訂定應用系統操作手冊分送使用單位。 2.訓練使用單位人員使用新系統。 (十)資料轉換： 1.訂定資料轉換計畫,其內容至少包含下列項目： (1)轉換時機及負責轉換人員。 (2)轉換方式。 2.資料轉換計畫應呈相關權責主管核定後執行之。 3.進行資料轉換作業前應保留備份資料。 4.比較資料轉換前後新舊系統之執行結果	4.製作測試報告其內容至少需包含下列項目： (1)測試目的。 (2)測試方法。 (3)測試記錄。 (4)測試結果總評及建議。 (八)系統設置計畫： 1.應用系統上線前系統負責人需訂定應用系統設置計畫，其內容含下列項目： (1)應用系統概述。 (2)容量規劃。 (3)程式及檔案之設定權限。 (4)使用者及使用權限與使用環境之設定。 2.應用系統設置計畫由操作管理人員依據核定之文件執行之。 (九)應用系統操作訓練： 1.訂定應用系統操作手冊分送使用單位。 2.訓練使用單位人員使用新系統。 (十)資料轉換： 1.訂定資料轉換計畫,其內容至少包含下列項目： (1)轉換時機及負責轉換人員。 (2)轉換方式。 2.資料轉換計畫應呈相關權責主管核定後執行之。 3.進行資料轉換作業前應保留備份資料。 4.比較資料轉換前後新舊系統之執行結果	

編號	作業項目	修正後內容	修正前內容	修正說明
		並適時修正錯誤。 5.轉換後併行作業。 (十一)併行測試： 1.於資料轉換作業完成後進行。 2.正式作業資料同時輸入新舊系統。 3.比較新舊系統輸出結果，如有錯誤應即時修正。 4.併行測試正常經相關權責主管核准後正式上線。 (十二)文件整理： 1.新開發之應用系統正式實施前應備妥下列各項說明文件： (1)系統概述。 (2)系統流程圖。 (3)系統代碼表。 (4)系統功能表。 (5)程式規格書。 (6)操作手冊。 2.系統有關之文件應設專人負責保管。 3.系統說明文件限於相關業務人員借閱。 4.應用系統維護完成後，應於限期內完成相關文件及手冊之維護。 (十三)系統維護： 1.應用系統之維護應指派專人負責。 2.應用系統之程式、作業方式或其他內容需更動時由提出需求人員填具書面申請資料，交應用系統維護人員表示意見。	並適時修正錯誤。 5.轉換後併行作業。 (十一)併行測試： 1.於資料轉換作業完成後進行。 2.正式作業資料同時輸入新舊系統。 3.比較新舊系統輸出結果，如有錯誤應即時修正。 4.併行測試正常經相關權責主管核准後正式上線。 (十二)文件整理： 1.新開發之應用系統正式實施前應備妥下列各項說明文件： (1)系統概述。 (2)系統流程圖。 (3)系統代碼表。 (4)系統功能表。 (5)程式規格書。 (6)操作手冊。 2.系統有關之文件應設專人負責保管。 3.系統說明文件限於相關業務人員借閱。 4.應用系統維護完成後，應於限期內完成相關文件及手冊之維護。 (十三)系統維護： 1.應用系統之維護應指派專人負責。 2.應用系統之程式、作業方式或其他內容需更動時由提出需求人員填具書面申請資料，交應用系統維護人員表示意見。	

編號	作業項目	修正後內容	修正前內容	修正說明
		3.呈相關權責主管核定後由應用系統維護人員負責辦理。 4.需求經修改測試正常後,依上線應用系統異動管理程序修訂上線應用系統之內容。 5.系統修訂後應將所有設計上相關之改變及時配合修訂，屬於文件修訂部分送文件管理人員配合更新。 (十四)應用系統異動管理： 1.應用系統開發前應由應用系統負責人以書面通知系統管理人員所需之軟硬體資源及使用權限。 2.應用系統上線前系統負責人需訂定應用系統設置計畫，內容含下列項目： (1)應用系統目的。 (2)容量規劃及測試。 (3)程式及檔案之設定權限。 (4)使用者及使用權限與使用環境之設定。 3.應用系統設置計畫由系統管理人員依據核定後文件執行之。 4.為便於管理及安全因素的考慮,在一個系統內，應將「原始程式」「目的程式」及「使用者資料」分別以獨立的「資料館」存放，並將登錄之程式或資料名稱呈核列管。 5.上線系統之執行程序或資料等之新增、修改、刪除等處理除經由正式程式為之	3.呈相關權責主管核定後由應用系統維護人員負責辦理。 4.需求經修改測試正常後,依上線應用系統異動管理程序修訂上線應用系統之內容。 5.系統修訂後應將所有設計上相關之改變及時配合修訂，屬於文件修訂部分送文件管理人員配合更新。 (十四)應用系統異動管理： 1.應用系統開發前應由應用系統負責人以書面通知系統管理人員所需之軟硬體資源及使用權限。 2.應用系統上線前系統負責人需訂定應用系統設置計畫，內容含下列項目： (1)應用系統目的。 (2)容量規劃及測試。 (3)程式及檔案之設定權限。 (4)使用者及使用權限與使用環境之設定。 3.應用系統設置計畫由系統管理人員依據核定後文件執行之。 4.為便於管理及安全因素的考慮,在一個系統內，應將「原始程式」「目的程式」及「使用者資料」分別以獨立的「資料館」存放，並將登錄之程式或資料名稱呈核列管。 5.上線系統之執行程序或資料等之新增、修改、刪除等處理除經由正式程式為之	

編號	作業項目	修正後內容	修正前內容	修正說明
		外，只能由系統負責人依核定後結果執行之。 6.上線系統變更時其設計上相關之改變應及時配合更新。 7.程式變更上線前應進行完整測試，變更完成後須檢核與申請內容是否相符，並進行驗證以確認變更作業之可用性及正確性。 (十五)資通系統弱點掃描：(適用網際網路下單證券商) 1.各資通系統應定期(至少每半年一次)進行弱點掃描。 2.針對系統弱點其相關風險撰寫說明與安裝修補方式文件，並留存記錄以供參考。 (十六)程式源碼安全規範（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)： 1.程式應避免含有惡意程式等資訊安全漏洞。 2.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。 3.程式於引用之函式庫有更新時，應備妥對應之更新版本。 4.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。 5.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	外，只能由系統負責人依核定後結果執行之。 6.上線系統變更時其設計上相關之改變應及時配合更新。 7.系統變更完成後須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正確性。 (十五)資通系統弱點掃描：(適用網際網路下單證券商) 1.各資通系統應定期(至少每半年一次)進行弱點掃描。 2.針對系統弱點其相關風險撰寫說明與安裝修補方式文件，並留存記錄以供參考。 (十六)程式源碼安全規範（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)： 1.程式應避免含有惡意程式等資訊安全漏洞。 2.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。 3.程式於引用之函式庫有更新時，應備妥對應之更新版本。 4.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。 5.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	

編號	作業項目	修正後內容	修正前內容	修正說明
		等)應自行或委外檢視驗證傳遞對象是否適當並留存相關紀錄。 6.公司應依上開安全事項檢驗程式源碼並符合安全事項之要求；無法取得程式源碼時，應要求程式提供者符合上開前五項安全事項之佐證。 (十七)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）： 1.行動應用程式發布： (1)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。 (2)應於官網上提供行動應用程式之名稱、版本與下載位置。 (3)應建立偽冒行動應用程式偵測機制，以維護客戶權益。 (4)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」。 2.敏感性資料保護： (1)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	等)應自行或委外檢視驗證傳遞對象是否適當並留存相關紀錄。 6.公司應依上開安全事項檢驗程式源碼並符合安全事項之要求；無法取得程式源碼時，應要求程式提供者符合上開前五項安全事項之佐證。 (十七)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）： 1.行動應用程式發布： (1)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。 (2)應於官網上提供行動應用程式之名稱、版本與下載位置。 (3)應建立偽冒行動應用程式偵測機制，以維護客戶權益。 (4)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」。 2.敏感性資料保護： (1)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	

編號	作業項目	修正後內容	修正前內容	修正說明
		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。 (2)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），應提示使用者注意風險。 3.行動應用程式檢測： (1)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。如通過實驗室檢測後一年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。 (2)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。 (十八)核心系統**發生錯誤時，**使用者頁面**應**僅顯示簡短錯誤訊息及代碼，不包含詳細	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。 (2)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），應提示使用者注意風險。 3.行動應用程式檢測： (1)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。如通過實驗室檢測後一年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。 (2)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。 (十八)核心系統**應針對風險評估**使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細	

編號	作業項目	修正後內容	修正前內容	修正說明
		之錯誤訊息。 (十九)提供網際網路下單服務之核心系統上架前及系統更新時應執行「源碼掃描」安全檢測。 (二十)與資訊公司異業合作平台，不得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）。	之錯誤訊息。 (十九)提供網際網路下單服務之核心系統上架前及系統更新時應執行「源碼掃描」安全檢測。 (二十)與資訊公司異業合作平台，不得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）。	