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-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	不定期（每半年至少查核乙次） (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)提出之資訊作業發展計畫，是否確定欲開發系統之作業方式。 (四)需求分析報告是否與相關業務單位充分討論。 (五)已認可之系統開發計畫是否包含下列項目： 1.計劃之目的及範圍皆有周詳之定義。 2.針對各種可行方案合理估計成本效益並作比較分析。 3.依系統開發階段訂定合理的進度表。 (六)系統分析報告是否包含下列項目： 1.現行系統之問題點及其改善方式。 2.新系統之成本效益比較分析。 3.新系統之輸入、輸出及內部流程之明確列出。 (七)環境評估報告是否依規定製作。 (八)是否使用具有合法版權之軟體。 (九)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： 1.委外作業是否簽訂契約，且委外作業契約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、	不定期（每半年至少查核乙次） (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)提出之資訊作業發展計畫，是否確定欲開發系統之作業方式。 (四)需求分析報告是否與相關業務單位充分討論。 (五)已認可之系統開發計畫是否包含下列項目： 1.計劃之目的及範圍皆有周詳之定義。 2.針對各種可行方案合理估計成本效益並作比較分析。 3.依系統開發階段訂定合理的進度表。 (六)系統分析報告是否包含下列項目： 1.現行系統之問題點及其改善方式。 2.新系統之成本效益比較分析。 3.新系統之輸入、輸出及內部流程之明確列出。 (七)環境評估報告是否依規定製作。 (八)是否使用具有合法版權之軟體。 (九)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： 1.委外作業是否簽訂契約，且委外作業契約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、	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
		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.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。 3.公司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。 4.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**掃描**、弱點掃描等)，並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是否通過源碼掃描或黑箱測試。 5.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。 6.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 7.公司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	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.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。 3.公司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。 4.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**、弱點掃描等)，並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是否通過源碼掃描或黑箱測試。 5.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。 6.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 7.公司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	

編號	作業項目	修正後內容	修正前內容	修正說明
		管。 8.公司是否對資訊服務供應商服務內容變更進行風險評估。 9.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，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，並要求資訊服務供應商持續遵守保密承諾。 10.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。 11.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。 (十)資料庫設計之欄位是否滿足業務需求。 (十一)資料庫設計是否預留擴充彈性。 (十二)系統作業流程設計是否考慮錯誤處理程序。 (十三)處理過程之控制設計是否適切 (十四)對於交易時間、地點、作業人員及作業內容等事項是否記錄足夠供查詢之資訊 (十五)系統規格是否與有關單位充分討論 (十六)系統規格應經相關權責主管核示。 (十七)是否依規定編定程式代號。	管。 8.公司是否對資訊服務供應商服務內容變更進行風險評估。 9.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，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，並要求資訊服務供應商持續遵守保密承諾。 10.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。 11.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。 (十)資料庫設計之欄位是否滿足業務需求。 (十一)資料庫設計是否預留擴充彈性。 (十二)系統作業流程設計是否考慮錯誤處理程序。 (十三)處理過程之控制設計是否適切 (十四)對於交易時間、地點、作業人員及作業內容等事項是否記錄足夠供查詢之資訊 (十五)系統規格是否與有關單位充分討論 (十六)系統規格應經相關權責主管核示。 (十七)是否依規定編定程式代號。	

編號	作業項目	修正後內容	修正前內容	修正說明
		(十八)是否依規定撰寫程式說明。 (十九)是否依規定語言及方式撰寫程式。 (二十)程式測試是否經由不同人員再行驗證。 (二十一)測試經過及結果是否留有完整紀錄。 (二十二)測試所發現錯誤經修改後，是否將所有設計上相關之改變配合修訂更新。 (二十三)系統設置計畫之訂定與執行是否確實依作業程序辦理。 (二十四)是否訂定應用系統操作手冊，並訓練使用人員熟悉操作。 (二十五)轉換是否挑選恰當之時機。 (二十六)轉換前資料是否留存備份。 (二十七)是否事先考慮新舊系統間無法轉換時資料應如何處理。 (二十八)正式作業資料是否確實輸入新舊系統。 (二十九)新舊系統併行作業測試無誤正式上線前是否經相關權責主管核准。 (三十)各項說明文件是否齊全。 (三十一)各項文件與手冊是否經適當維護與控制；是否由專人保管，且僅限於相關業務人員借閱。 (三十二)整理後之文件是否與系統保持一致。 (三十三)應用系統之維護是否指派專人辦理。 (三十四)系統修訂後是否將所有設計上相關之改變配合修訂、更新。 (三十五)已完成之程式因故需維護時，是否依	(十八)是否依規定撰寫程式說明。 (十九)是否依規定語言及方式撰寫程式。 (二十)程式測試是否經由不同人員再行驗證。 (二十一)測試經過及結果是否留有完整紀錄。 (二十二)測試所發現錯誤經修改後，是否將所有設計上相關之改變配合修訂更新。 (二十三)系統設置計畫之訂定與執行是否確實依作業程序辦理。 (二十四)是否訂定應用系統操作手冊，並訓練使用人員熟悉操作。 (二十五)轉換是否挑選恰當之時機。 (二十六)轉換前資料是否留存備份。 (二十七)是否事先考慮新舊系統間無法轉換時資料應如何處理。 (二十八)正式作業資料是否確實輸入新舊系統。 (二十九)新舊系統併行作業測試無誤正式上線前是否經相關權責主管核准。 (三十)各項說明文件是否齊全。 (三十一)各項文件與手冊是否經適當維護與控制；是否由專人保管，且僅限於相關業務人員借閱。 (三十二)整理後之文件是否與系統保持一致。 (三十三)應用系統之維護是否指派專人辦理。 (三十四)系統修訂後是否將所有設計上相關之改變配合修訂、更新。 (三十五)已完成之程式因故需維護時，是否依	

編號	作業項目	修正後內容	修正前內容	修正說明
		據經過正式核准之程序辦理。 (三十六)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。 (三十七)應用程式文件是否與異動程式相符，正式作業環境之程式是否與所異動程式時間相符，且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，並進行驗證以確認變更作業之可用性及正確性。 (三十八)程式經修改其相關文件是否及時更新。 (三十九)各資通系統是否定期(至少每半年一次)進行弱點掃描。(適用網際網路下單證券商) (四十)弱點掃描所辨識出之潛在系統弱點，應評估其相關風險或安裝修補程式，並留存紀錄。(適用網際網路下單證券商) (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) (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) (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	據經過正式核准之程序辦理。 (三十六)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。 (三十七)應用程式文件是否與異動程式相符，正式作業環境之程式是否與所異動程式時間相符且系統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正確性。 (三十八)程式經修改其相關文件是否及時更新。 (三十九)各資通系統是否定期(至少每半年一次)進行弱點掃描。(適用網際網路下單證券商) (四十)弱點掃描所辨識出之潛在系統弱點，應評估其相關風險或安裝修補程式，並留存紀錄。(適用網際網路下單證券商) (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) (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) (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	

編號	作業項目	修正後內容	修正前內容	修正說明
		單證券商） (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） (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，檢測範圍以目的事業主管機關「行動應用 APP 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） (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」及「身份辨識」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) (四十七)對第三方檢測實驗室所提交之 APP 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） (四十八)是否於發布前檢視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，	單證券商） (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） (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，檢測範圍以目的事業主管機關「行動應用 APP 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） (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」及「身份辨識」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) (四十七)對第三方檢測實驗室所提交之 APP 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） (四十八)是否於發布前檢視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，	

編號	作業項目	修正後內容	修正前內容	修正說明
		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) (四十九)委外系統如涉及機敏性資料傳送(如:客戶帳號密碼或交易資料等)是否檢驗相關資料流，傳遞對象之妥適性並留存相關紀錄。 (五十)核心系統發生錯誤時，針對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。 (五十一)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。 (五十二)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）。	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) (四十九)委外系統如涉及機敏性資料傳送(如:客戶帳號密碼或交易資料等)是否檢驗相關資料流，傳遞對象之妥適性並留存相關紀錄。 (五十)核心系統是否針對風險評估使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 (五十一)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。 (五十二)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）。	