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)~(三)略 (四)、委外廠商管理： 1(略) 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。~~評估資訊服務供應商之集中度，包括評估資訊服務供應商作業能力，採取適當風險管控措施，確保作業委外處理之品質，並注意作業委託資訊服務供應商之適度分散以控管作業風險。~~ 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~~程式~~源碼掃描或黑箱	作業程序及控制重點： (一)~(三)略 (四)、委外廠商管理： 1(略) 2、公司應評估資訊服務供應商之集中度，包括評估資訊服務供應商作業能力，採取適當風險管控措施，確保作業委外處理之品質，並注意作業委託資訊服務供應商之適度分散以控管作業風險。 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程式碼掃描或黑箱測	參酌「證券商資通系統與服務供應鏈風險管理自律規範」第三條第一項供應商遴選原則修訂。 調整用字一致性。

		測試。 4~9(略) 10、委外資~~訊~~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。	試。 4~9(略) 10、委外資訊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。	調整用字一致性。
		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。	(新增)	增訂委外服務壓力測試之要求，說明資訊服務供應商應配合組織因應內外在環境變化執行壓力測試。
		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。	(新增)	參酌「證券商資通系統與服務供應鏈風險管理自律規範」第七條

				第一項及第二項審核資訊服務供應商服務修訂。
		(五)~(十三)略 (十四)、應用系統異動管理： 1~6(略) 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。	(五)~(十三)略 (十四)、應用系統異動管理： 1~6(略) (新增)	增訂程式變更正確性管理之條款，說明程式上線後應確認變更正確性。
		(十五)、資~~訊~~通系統弱點掃~~瞄~~描：（適用網際網路下單證券商） 1、各資~~訊~~通系統應定期(至少每半年一次)進行弱點掃~~瞄~~描。 2(略) (十六)、程式~~原始~~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）：	(十五)、資訊系統弱點掃瞄：（適用網際網路下單證券商） 1、各資訊系統應定期(至少每半年一次)進行弱點掃瞄。 2(略) (十六)、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）：	調整用字一致性。 調整用字一致性。 調整用字一致性。

		1~5(略) 6、公司應依上開安全事項檢驗程式~~原始~~源碼並符合安全事項之要求；無法取得程式~~原始~~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。 (以下略)	1~5(略) 6、公司應依上開安全事項檢驗程式原始碼並符合安全事項之要求；無法取得程式原始碼時，應要求程式提供者符合上開前五項安全事項之佐證。 (以下略)	調整用字一致性。