

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	<p>作業週期：不定期(每半年至少查核乙次)</p> <p>(一)~(八)略</p> <p>(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：</p> <p>1~2(略)</p> <p>3、公司是否<u>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。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。</u></p> <p>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</p>	<p>作業週期：不定期(每半年至少查核乙次)</p> <p>(一)~(八)略</p> <p>(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：</p> <p>1~2(略)</p> <p>3、公司是否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。</p> <p>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</p>	<p><u>配合內部控制制度 CC-19000 調整，同時修正查核明細表。</u></p>

	<p>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<u>程式源碼</u>掃描或黑箱測試。</p> <p>5~9 略</p> <p><u>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。</u></p> <p><u>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。</u></p> <p>(十)~(三十六)略</p> <p>(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<u>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。</u></p> <p>(三十八)略</p> <p>(三十九)、各資<u>訊通</u>系統應<u>是否</u>定期(至少</p>	<p>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程式碼掃描或黑箱測試。</p> <p>5~9 略</p> <p>(新增)</p> <p>(新增)</p> <p>(十)~(三十六)略</p> <p>(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。</p> <p>(三十八)略</p> <p>(三十九)、各資訊系統應定期(至少每半年</p>	
--	---	---	--

		<p>每半年一次)進行弱點掃瞄。 (適用網際網路下單證券商)</p> <p>(四十)、弱點掃瞄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)</p> <p>(以下略)</p>	<p>一次)進行弱點掃瞄。(適用網際網路下單證券商)</p> <p>(四十)、弱點掃瞄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)</p> <p>(以下略)</p>	
--	--	---	---	--