

票券金融公司檢查手冊(異動版)

一、內部管理 (共 39 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.20.6	(6)是否建立「消費爭議處理制度」，並納入下列事項：		本會銀行局 113.8.5 銀局 (合)字第 1130220584 號 函	配合新增函令增列查核事項
2.20.6.1	①對於消費爭議案件之處理，建立以風險為導向之升級陳報機制，並確認申訴態樣之根本原因，適時提出因應作為。		本會銀行局 113.8.5 銀局 (合)字第 1130220584 號 函	修正理由同上
2.20.6.2	②指定專責部門或人員處理消費爭議案件，並提升督導層級至副總經理。		本會銀行局 113.8.5 銀局 (合)字第 1130220584 號 函	修正理由同上
2.20.6.3	③明定受理爭議案件之回應方式，並提供金融消費者查詢爭議案件處理進度之管道。		本會銀行局 113.8.5 銀局 (合)字第 1130220584 號 函	修正理由同上
3.2.5	(5)供應商管理	(5)協力廠商管理	票券金融公司資通系統與服務供應鏈風險管理規範	配合公會訂定規範，修正查核事項
3.2.5.1	(刪除)	①軟硬體買賣合約或委外維護合約內容是		配合公會訂定規

項目編號	查核事項		法令規章	說明
	修正後	修正前		
		否包括作業安全、委託內容、機密維護、損害賠償等雙方權責之劃分？		範，刪除查核事項
3.2.5.2	(刪除)	②是否建立適當控管程序以確保委外維護程式係屬適當？並指定專人負責監控廠商維護活動及服務？		修正理由同上
3.2.5.3	(刪除)	③若廠商可撥接至受檢單位電腦診斷及維護系統，受檢單位是否建立適當程序以控制廠商存取範圍？		修正理由同上
<u>3.2.5.1</u>	<u>①資通系統與服務委外前，是否分析及規劃下列供應鏈資訊安全事項：</u>		<u>票券金融公司資通系統與服務供應鏈風險管理規範第 4 條</u>	配合公會訂定規範，新增查核事項
<u>3.2.5.1.1</u>	<u>I.是否分析委外項目之資訊安全風險(如：可能受影響之資訊資產、流程及作業環境)與委外可行性，並依據分析結果擬訂資訊安全要求？</u>		<u>票券金融公司資通系統與服務供應鏈風險管理規範第 4 條</u>	修正理由同上
<u>3.2.5.1.2</u>	<u>II.屬核心資通系統，或屬非核心資通系統，且供應商於契約存續期間得存取公司</u>		<u>票券金融公司資通系統與服</u>	修正理由同上

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>機敏資料之委外開發項目，其專案成員是否有資訊安全人員參與？</u>		<u>票券金融公司資通系統與服務供應鏈風險管理規範第 4 條</u>	
<u>3.2.5.2</u>	<u>②選擇供應商前，是否執行下列事項：</u>		<u>票券金融公司資通系統與服務供應鏈風險管理規範第 5 條</u>	修正理由同上
<u>3.2.5.2.1</u>	<u>I.是否依據委外項目之性質訂定供應商需求建議書？內容是否明列供應商需符合之專業資格與資訊安全要求及服務水準？</u>		<u>票券金融公司資通系統與服務供應鏈風險管理規範第 5 條</u>	修正理由同上
<u>3.2.5.2.2</u>	<u>II.選擇供應商過程，如涉及公司資訊交換，是否於資訊交換前簽署保密協議書？</u>		<u>票券金融公司資通系統與服務供應鏈風險管理規範第 5 條</u>	修正理由同上
<u>3.2.5.2.3</u>	<u>III. 是否執行安全評估以選任合適之供應商，包括是否評估供應商對公司服務集中度之適度分散（如存在集中度過高之疑慮，應依評估結果擬訂對應之風險處理措施）？是否評估供應商對所委託項目之資訊安全管理機制？是否評估供應商與其提供產品或服務位置？</u>		<u>票券金融公司資通系統與服務供應鏈風險管理規範第 5 條</u>	修正理由同上

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.2.5.3	③供應商之委託契約或相關文件中，是否明確約定下列事項：		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.3.1	I.是否要求供應商遵守相關法令法規及其他適當資訊安全標準要求，並訂定供應商未符合資訊安全要求或服務水準時之罰責標準？		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.3.2	II.是否定義公司與供應商之資訊安全權責，規範供應商應實施之資訊安全要求，應包含人員管理、資訊存取與傳輸安全管控機制等，以落實資通系統供應鏈邊際防護？		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.3.3	III.是否約定非經公司書面同意，不得將作業複委託他人？是否定義委託業務得否複委託、得複委託之範圍與對象，及複委託受託者應具備之資訊安全措施？		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.3.4	IV.是否依據資料之機密等級、資料處理流程與傳輸方式，要求供應商實施資料安全管控？		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上

項目編號	查核事項		法令規章	說明
	修正後	修正前		
			條	
3.2.5.3.5	<u>V.是否與供應商約定服務品質、水準、效能、供應商資訊安全事件應變與通報程序、資訊安全事件損害賠償責任、系統或程式定期檢測與修復要求、保固服務、異常管理等各項服務要求？</u>		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.3.6	<u>VI.是否保留對供應商之稽核權？若供應商發生可能影響受託業務之資通安全事件時，是否確保其本身、本會及中央銀行，或其指定之人能取得供應商辦理受託業務之相關資訊，包括資通安全控管機制及相關系統之查核報告，及實地查核權力？</u>		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.3.7	<u>VII.是否訂定資通系統功能需求或資訊建置要求，並包含資訊安全要求或控制措施？是否訂定產品或服務之交付驗收程序和標準？</u>		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.3.8	<u>VIII.是否明確約定供應商交付之產品及其服務組件來源為合法取得或經合法授權使用？</u>		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.2.5.3.9	IX.是否要求供應商確保交付之資通系統或程式，包含供應商提供之產品及其服務組件，無惡意程式及後門程式，並取得相關安全性測試結果或供應商安全性承諾？		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.3.10	X.是否訂定供應商契約終止時，資訊資產與資料返還、移交、刪除或銷毀之要求？		票券金融公司資通系統與服務供應鏈風險管理規範第 6 條	修正理由同上
3.2.5.4	④於供應商契約存續期間，是否注意以下原則：		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上
3.2.5.4.1	I.公司與供應商是否分別指定專人，負責督導及辦理各項資訊安全要求事項？		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上
3.2.5.4.2	II.與供應商間如涉個人資料交換，是否確認符合我國個人資料保護法相關規定，並確保僅授權者可存取資料及保留資料使用稽核軌跡，以利追蹤資料使用狀況？		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上
3.2.5.4.3	III.是否識別供應商涉及之關鍵資訊資		票券金融公司資通系統與服	修正理由同上

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	<u>產，以加強風險管理？</u>		務供應鏈風險管理規範第 7 條	
3.2.5.4.4	<u>IV.是否訂定供應商存取權限管理規範，妥善管理供應商之實體與邏輯存取權限，以落實資通系統供應鏈邊際防護？</u>		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上
3.2.5.4.5	<u>V.是否定期對具邏輯存取權限之供應商辦理供應鏈資訊安全風險評估，依據供應鏈資訊安全風險評估結果採取適當之資訊安全控管措施或提報適當主管層級核准可接受之風險等級？</u>		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上
3.2.5.4.6	<u>VI.是否建立對核心資通系統及於契約存續期間得存取公司機敏資料之非核心資通系統供應商資訊安全稽核之程序（含稽核結果之改善追蹤機制）？是否依據供應鏈資訊安全風險評估結果選擇合適之資訊安全稽核之方式與頻率（含自行辦理或委託獨立第三方執行資訊安全訪視作業，或由供應商提供公正第三方之驗證報告）？</u>		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.2.5.4.7	VII.是否審查供應商針對其專案執行人員辦理資訊安全教育訓練之紀錄？		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上
3.2.5.4.8	VIII.是否依契約要求審查供應商所交付之系統或程式（含供應商提供之產品及其服務組件之安全性測試結果或供應商安全性承諾）？		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上
3.2.5.4.9	IX.是否依據與供應商約定各項服務要求定期審查供應鏈服務之品質？		票券金融公司資通系統與服務供應鏈風險管理規範第 7 條	修正理由同上
3.2.5.5	⑤供應商服務變更與契約終止時，是否符合下列事項：		票券金融公司資通系統與服務供應鏈風險管理規範第 8 條	修正理由同上
3.2.5.5.1	I. 供應商提供之服務變更前(包含契約變更、供應商組織重大調整、業務重大異動或契約提前終止相關事宜)，公司是否執行供應鏈資訊安全風險評估，並依評估結果擬訂對應之風險處理措施？		票券金融公司資通系統與服務供應鏈風險管理規範第 8 條	修正理由同上

項目編號	查核事項		法令規章	說明
	修正後	修正前		
3.2.5.5.2	II. 供應商契約終止時，公司是否於供應商		票券金融公司資通系統與服	修正理由同上
	依約完成產品或服務之移轉、交付驗收程		務供應鏈風險管理規範第 8	
	序後，監督其完成資訊資產與資料返還、		條	
	移交、刪除或銷毀，並移除供應商於服務 期間所取得之實體與邏輯存取權限？			