信用合作社檢查手冊(異動版)

一、財務狀況與經營績效之查核(共3項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.6.1.1	①信用合作社社股每股金額為新臺幣一百元，每一社員至少是否認購二十股，至多是否未超過實收股金總額百分之五?	①信用合作社社股每股金額為新台幣一百元，每一社員至少是否認購二十股，至多是否未超過實收股金總額百分之五。	~~財政部88.11.11台財融字第88769064號書函「違反信用合作社社員最低認購股數應無除名程序之適用釋疑」。~~	配合法規下架，刪除引用之參考法令。
4.7	7.在所收受之定期性存款資金中，依規定以定期性存款方式轉存於行庫之存款，稱為「轉存款」。	7.在所收受之定期性存款資金中，依規定以定期性存款方式轉存於行庫之存款，稱為「轉存款」。	~~中央銀行110.12.1台央業字第1100046374號函修正「基層金融機構轉存款準備金提存作業要點」第5、6及8點。~~ 中央銀行110.12.1台央業字第1100046374號函修正「基層金融機構轉存款準備金提存作業要點」第2點。	修正引用之參考法規。
4.8	8.信用合作社轉存於合作金庫商業銀行之「轉存款」信用合作社免提法定準備金。	8.信用合作社轉存於合作金庫商業銀行之「轉存款」信用合作社免提法定準備金。	~~前項處理要點第2點。~~ 前項處理要點第3點。	修正引用之參考法規。

資料基準日：112年6月30日

二、存款業務之查核(共9項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.2.1	(1)有無上網查詢遺失身分證領補換紀錄，以確認客戶身分?	(1)有無上網查詢遺失身分證領補換紀錄，以確認客戶身分?	~~財政部90.2.8台財融(一)字第90900581號函「預防及打擊以金融卡及人頭帳戶從事犯罪金融機構應配合辦理事項」。~~	配合法規下架，刪除引用之參考法令。
1.2.7.1.5	V.「開戶檢核表」有無漏未填寫、填寫或檢核是否確實？對有異常情形者是否已依「存款帳戶及其疑似不法或顯屬異常交易管理辦法」第13條第2項、「信用合作社防制洗錢及打擊資助恐怖主義注意事項範本」第4條第1款及「防杜人頭帳戶範本」第一(四)條規定妥適處理？是否拒絕其開戶或其他申請類交易之申請，對冒用或偽變造身分證開戶者，是否通知警調處理及通報聯徵中心？	V.「開戶檢核表」有無漏未填寫、填寫或檢核是否確實？對有異常情形者是否已依「存款帳戶及其疑似不法或顯屬異常交易管理辦法」第13條第2項、「信用合作社防制洗錢及打擊資助恐怖主義注意事項範本」第4條第1款及「防杜人頭帳戶範本」第一(四)條規定妥適處理？是否拒絕其開戶，對冒用或偽變造身分證開戶者，是否通知警調處理及通報聯徵中心？	1.~~本會105.2.19金管銀法字第10500029440號函准予備查「~~中華民國銀行公會「金融機構開戶作業審核程序暨異常帳戶風險控管之作業範本」第2條。 2.~~本會103.8.20金管銀法字第10310004610號令~~「存款帳戶及其疑似不法或顯屬異常交易管理辦法」第13條第2項。 3.~~本會108.8.5金管銀合字第10801302000號函同意備查~~「信用合作社防制洗錢及	配合法令修正，修正查核事項內容。

資料基準日：112年6月30日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
			打擊資恐注意事項範本」第4條第1款。 4.~~本會106.3.31金管銀法字第10600061570號函同意備查~~中華民國銀行公會~~之~~「防杜人頭帳戶範本」及「開戶作業檢核表範本」。 5.~~本會111.9.29金管銀法字第1110146309號函准予備查「~~中華民國銀行公會「銀行受理客戶以網路方式開立數位存款帳戶作業範本」。	
1.2.10	(10)受理自然人開立活期性存款帳戶（支票存款除外），除下列情況外，是否採錄影或拍照方式建立影像檔案？	(10)受理自然人開立活期性存款帳戶（支票存款除外），除下列情況外，是否採錄影或拍照方式建立影像檔案？	~~2.財政部92.12.10台財融(二)字第0922001638號函。~~	配合法規下架，刪除引用之參考法令。
1.4.3	(3)有無不法集團利用金融機構，以不實資金或暫借頭寸方式，循環提供大量存戶充作存款資金證明?	(3)有無不法集團利用金融機構，以不實資金或暫借頭寸方式，循環提供大量存戶充作存款資金證明。	~~財政部88.9.13台財融字第88737515號函「金融機構核發存款餘額證明應注意事項」。~~	配合法規下架，刪除引用之參考法令。

資料基準日：112年6月30日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.7.6	(6)辦理客戶開戶時錄影機錄攝之資料是否保存至少六個月，俾保存證據備供檢警調機關日後之偵辦?	(6)辦理客戶開戶時錄影機錄攝之資料是否保存至少六個月，俾保存證據備供檢警調機關日後之偵辦。	~~1.財政部90.2.8台財融(一)字第90000581號函「預防及打擊不法份子以金融卡及人頭帳戶從事犯罪所列事項」。~~ ~~2.財政部90.4.3台財融(一)字第90733071號函「『金融機構於辦理客戶開戶時應注意防範歹徒以人頭或持偽變造身分證開立存款帳戶情事』之補充說明」。~~ ~~3.~~1.財政部 92.10.16 台財融（二）字第 0922001401 號函「金融機構自動櫃員機及週遭監視錄影帶應暫行保存六個月以上」。 ~~4.財政部93.4.28台財融(一)字第0931000318號函『研商防制利用自動櫃員機詐財案件』會議紀錄」。~~	配合法規下架，刪除引用之參考法令。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
			~~5.~~2.本會93.12.10銀局(一)字第0931000716號函「重申金融機構應落實執行自動櫃員機及週遭監視錄影帶至少保存六個月，及加強查驗開戶證明文件」。	
2.2.1	(刪除)	~~(1)支票或擔當付款本票背面為轉帳指示是否以書面約定，所轉入帳戶是否以存戶本人在該金融機構之支票存款帳戶為限。~~	2.~~財政部93.4.1台財融(二)字第0938010454號令「授權轉帳指示之支票存款戶不以個人帳戶為限」。~~ ~~3.本會93.11.30金管銀(一)字第0938011028號令「銀行法第七條有關活期存款依約定方式提取存款之規範」。~~	配合法規下架，刪除查核事項並調整項目編號。
2.4	4.利息計算是否正確？起息點及計息單位是否符合規定？	4.利息計算是否正確？起息點及計息單位是否符合規定？	~~中華民國銀行商業同業公會全國聯合會83.5.26全授字1152號函「新台幣存放款計息方式」。~~ 中華民國銀行公會102年8月22日第10屆30次理監事聯席	修正引用之參考法規。

資料基準日：112年6月30日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
			會議通過「中華民國銀行公會會員辦理新臺幣存放款計息方式」。	
3.3.1	(1)支票存款戶基本資料之新增、異動、結清是否確實?	(1)支票存款戶基本資料之新增、異動、結清是否確實。	~~1. 中央銀行業務局84.4.24(84)台央業字第475號函「建立支票存款戶基本資料檔處理要點」。~~ ~~2. 中央銀行業務局80.1.10(80)台央業字第0200044號函「依『建立支票存款戶基本資料檔處理要點』填報支票存款戶資料」。~~ ~~3. 中央銀行業務局80.2.14(80)台央業字第0200290號函「為提昇支票存款戶基本資料檔正確性並加強建檔時效應辦理事項」。~~ ~~4. 中央銀行業務局89.4.21(89)台央業字第020012060號函「『如何提昇~~	配合法規下架，刪除引用之參考法規。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
			~~全國支票存款戶基本資料檔之正確性』會商結論」。~~	
4.3	3.定期性存款有否按存款銀行牌告利率給付利息?	3.定期性存款有否按存款銀行牌告利率給付利息。	2.~~中華民國銀行商業同業公會全國聯合會 83.5.26 全授字 1152 號函「新台幣存放款計息方式」。~~ 中華民國銀行公會 102 年 8 月 22 日第 10 屆 30 次理監事聯席會議通過「中華民國銀行公會會員辦理新臺幣存放款計息方式」。	修正引用之參考法規。

三、授信業務之查核(共 2 項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
5.3.2	(2)辦理授信覆審,其覆審人員是否未覆審本身經辦之授信案件,每一授信案件經辦理覆審後,是否編製覆審報告?	(2)辦理授信覆審,其覆審人員是否未覆審本身經辦之授信案件,每一授信案件經辦理覆審後,是否編製覆審報告。	同上規定 33 條第 ~~2~~ 3項。	配合法規修訂,修正引用參考法規之條文項次。

資料基準日:112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
6.7.3	(3)社員社辦理授信，收取手續費、規費、開辦費、承諾費或貸款提前清償違約金等有關費用，是否於書面中明定收費方式，且上開手續費是否未按月隨利息收取?	(3)社員社辦理授信，收取手續費、規費、開辦費、承諾費或貸款提前清償違約金等有關費用，是否於書面中明定收費方式，且上開手續費是否未按月隨利息收取。	1.~~財政部91.8.20台財融(一)字第0911000443號令「銀行辦理消費性貸款如向客戶收取手續費時，不得按月隨利息收取」。~~ ~~2.~~「中華民國信用合作社聯合社社員社授信規範」第9條第2項。	配合法規下架，刪除引用之參考法規。

四、內部管理之查核(共34項)

項目編號	查核事項		法令規章	說明
	修正後	修正前		
2.9	9.金融機構之安全設施（包括警報、報警系統、閉路電視錄影監視系統、金庫、運鈔車安全設備、營業櫃台及大出納區、防火設備、保全防盜系統及防衛器材）是否適當；錄影檔是否保存二個月（新開戶櫃檯、自動櫃員機及其週遭部分應至	9.金融機構之安全設施（包括警報、報警系統、閉路電視錄影監視系統、金庫、運鈔車安全設備、營業櫃台及大出納區、防火設備、保全防盜系統及防衛器材）是否適當；錄影帶是否保存二個月（新開戶櫃檯、自動櫃員機及其週遭部份應至	~~2.財政部89.12.6台財融第(六)字第89764495號函「金融機構應提高警覺，加強金庫及運鈔安全防範措施，落實內部控制制度」。~~ 2.「金融機構安全維護注意要點」。	配合法規下架，刪除引用之參考法規。

資料基準日：112年6月30日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	少保存六個月)，標示錄影日期，並妥適保管備查。	少保存六個月)，標示錄影日期，並妥適保管備查。	3.本會 95.6.13 金管銀（二）字第 09500234510 號令「金融機構之營業單位得免僱用駐衛警、保全人員或其他警衛人員專責擔任警戒工作之規定」。 4.本會 101.10.19 金管銀國字第 10120005240 號令修正「金融機構安全維護管理辦法」。	
3.2.1	(1)庫房是否裝置保全防盜系統、自動報警、自動定時鎖等，安全措施是否嚴密妥善，庫房內是否裝置全天候錄影監視系統，進出金庫是否設簿登記?	(1)庫房是否裝置保全防盜系統、自動報警、自動定時鎖等，安全措施是否嚴密妥善，庫房內是否裝置全天侯錄影監視系統，進出金庫是否設簿登記。	3.~~財政部 89.12.6 台財融(六)字第 89764495 號函。~~ ~~4.~~「金融機構安全維護管理辦法」第 6 條。	配合法規下架，刪除引用之參考法規。
3.2.10	(10)有無加強員工自衛編組，實施防護區制，定期演練，確立「安全維護人人有責」觀念?	(10)有無加強員工自衛編組，實施防護區制，定期演練，確立「安全維護人人有責」觀念。	~~財政部 90.6.14 台財融(六)字第 90744540 號函「加強安全防範措施並落實員工自衛安全維護教育」。~~	配合法規下架，刪除引用之參考法規。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
5.1	1.資訊安全政策、內部組織及資產管理	1.組織與管理		1.參考銀行公會所訂之「金融機構資通安全防護基準」調整查核事項。 2.原項目編號5.14移至5.1.7.8。
		(1)內部組織與權責劃分		
5.1.1	(1)資訊安全政策是否經理事會決議或經其授權之經理部門核定？	①資訊單位在組織系統圖中之地位，是否獨立於其他相互制衡部門？		
5.1.2	(2)資訊安全相關要求是否對所有員工及供應商公布或傳達？	②資訊單位組織與各科(組)職掌是否有明確訂出？管制性功能之職掌與一般作業功能(如操作、資料輸出入、程式設計等)之職掌是否分別由不同單位擔任，並避免不同科（組）擁有同一權責之現象？		
5.1.3	(3)是否訂定資訊作業相關管理及操作規範？			
5.1.4	(4)是否每年檢討資訊安全政策及前款管理及操作規範，並於發生重大變更（如新頒布法令法規）時審查，以持續確保其合宜性、適切性及有效性？	(2)發展管理與作業規章		
		①是否有高階人員或組織負責審議、核准或督導、協調下列事項？		
5.1.5	(5)是否依據作業流程，識別人員、表單、設備、軟體、系統等資產，建立 資產清冊、網路架構圖、組織架構圖及負責人，並定期清點以維持其正確性？	Ⅰ資訊作業重要規章？		
		Ⅱ資訊作業中、長期計畫？		
		Ⅲ資訊作業安全控管措施？		
5.1.6	(6)是否定義人員角色及責任並區	Ⅳ重要軟硬體系統購置、更新？		

資料基準日：112年6月30日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	隔相互衝突的角色？	Ⅴ資訊作業預算？ ②為健全資訊作業制度，是否分別或綜合、新訂或修訂下列有關規範，以作為資訊作業操作、管理、查核之依據： Ⅰ有關系統文件標準化之規範？ Ⅱ有關系統開發、維護規範？ Ⅲ有關電腦軟硬體系統及其附屬設施之管理規範？ Ⅳ有關系統操作之一般規範？ Ⅴ有關程式及資料檔案管理及維護規範？ Ⅵ有關各項業務處理操作規範？ Ⅶ有關工作之分配及其管理之規範？ Ⅷ有關內部自行查核之規範？ 上述規範之研訂是否洽會有關單位(如資訊、稽核、企劃、會計、業務…等)共同參與，以求操作、管理、查核等各層面之考慮周		

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
		全？ ③前述規範有關操作、管理、查核等各方面之規定是否完整？並憑以建立妥適之標準化作業程序及文件管理制度？ ④規範訂定後是否付諸實施，並適時檢討、修訂俾切合實際？ (3)人員訓練與管理		
		①對資訊作業人員之進用，是否依規定填具保密切結書，並辦理人事查核，隨時督導考核？		
5.1.7	(7)是否依據作業風險及專業能力選擇適當人員擔任其角色並定期提供必要教育訓練？	②是否建立資訊人員代理制度，並視實際需要建立輪調制度，是否有擔任同一項工作（如維護同一項系統）時間過長情形？		
5.1.7.1	①對資訊作業人員之進用，是否依規定填具保密切結書，並辦理人事查核，隨時督導考核？	③是否制定移交制度，對於調離職人員是否點收其保管之文		
5.1.7.2	②是否建立資訊人員代理制度，			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	並視實際需要建立輪調制度，是否有擔任同一項工作（如維護同一項系統）時間過長情形？	物，取銷其使用者代號、密碼並收繳其通行證、卡及相關證件？ ④對預定解僱或已遞出辭呈之人員是否有控制其接近敏感之程式或檔案、並禁止在非正常上班時間使用電腦？		
5.1.7.3	③是否制定移交制度，對於調離職人員是否點收其保管之文物，取銷其使用者代號、密碼並收繳其通行證、卡及相關證件？	⑤如有外雇人員，其管理是否有明確的規範，以確保重要資料無外洩之可能？		
5.1.7.4	④對預定解僱或已遞出辭呈之人員是否有控制其接近敏感之程式或檔案、並禁止在非正常上班時間使用電腦？	⑥是否訂有年度教育訓練計畫並編列預算？教育訓練計畫之擬定及實施是否切合需要？		
5.1.7.5	⑤如有外雇人員，其管理是否有明確的規範，以確保重要資料無外洩之可能？	⑦各級人員是否有充分的在職訓練？是否訂有員工交叉訓練計畫，以期至少有兩人可執行相同的工作互為支援？		
5.1.7.6	⑥是否訂有年度教育訓練計畫並編列預算？教育訓練計畫之擬定及實施是否切合需要？	⑧資訊安全之人力與訓練及管理作業是否符合規定？		
5.1.7.7	⑦各級人員是否有充分的在職訓			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	練？是否訂有員工交叉訓練計畫，以期至少有兩人可執行相同的工作互為支援？			
5.1.7.8	⑧資訊安全之人力與訓練及管理作業是否依「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 38-1 條第 1 項但書所稱主管機關對信用合作社辦理資訊安全相關規定辦理，如：		本會111.7.26金管銀合字第11102102331 號令。	
5.1.7.8.1	Ⅰ是否指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。但屬有限責任中華民國信用合作社聯合社南區聯合資訊中心之會員社，得指派經理以上或職責相當之人兼任?			
5.1.7.8.2	Ⅱ信用合作社是否依下列規定設置適當資訊安全人力資源：			
5.1.7.8.2.1	A.上一會計年度決算後淨值達新臺幣 30 億元以上或放			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	款總餘額達新臺幣200億元以上者，是否設置資訊安全主管及資訊安全人員?			
5.1.7.8.2.2	B.未達上述規模者，是否設置至少1名資訊安全人員?			
5.1.7.8.3	Ⅲ前點資訊安全主管及資訊安全人員除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。			
5.1.7.8.4	Ⅳ信用合作社資訊安全主管或資訊安全人員負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情形，依金融控股公司及銀行業內部控制及稽核制度實施辦法第二十七條第一項規定辦理內部控制制度聲明書之出具、揭露及公告申報，並由資訊安全長聯名出具。			
5.1.7.8.5	Ⅴ信用合作社資訊安全主管及資			

資料基準日：112年6月30日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
5.1.7.8.6	訊安全人員，每年應至少接受15小時以上資訊安全專業課程訓練或職能訓練。總社資訊單位、財務保管單位及其他管理單位之人員，每年至少須接受3小時以上資訊安全宣導課程。 Ⅵ第一點有關配置資訊安全長之規定，信用合作社應於本令生效日後九個月內調整至符合規定。信用合作社應於符合第二點適用條件起六個月內調整。			
5.2.2 ~~5.2.2.1~~	(2)是否建立機房門禁管制，並將營運設備集中於機房內，以確保僅允許經授權人員進出？非授權人員進出是否填寫進出登記，並由內部人員陪同及監督？進出登記紀錄是否定期審查，如有異常應適當處置？	(2)人員進出管理 對進出資訊單位、辦公場所、機房、媒體室及文件保管室之人員與攜帶（搬運）之物品是否加以嚴格管制？ ①進出資訊單位建物、辦公場所、機房、媒體室及文件保管	~~「財政部暨所屬機關（構）資訊安全管理準則」：第十章實~~	參考銀行公會所訂之「金融機構資通安全防護基準」調整查核事項。

資料基準日：112年6月30日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
~~5.2.2.2~~ ~~5.2.2.2.1~~ ~~5.2.2.2.2~~ ~~5.2.2.2.3~~		室之人員是否加以辨識並登記？ ②電腦機房、媒體室、文件保管室之門禁管制是否妥善？ Ⅰ電腦機房及媒體室（庫）及文件保管室（庫）有無指定專人負責管制？ Ⅱ機房進出人員除輪班操作員等機房工作人員外是否皆經核准及登記？媒體室（庫）進出人員除媒體管理員外是否皆經核准或授權，並保存進出紀錄？ Ⅲ機房及其他重要區域是否有門禁管制設備以控制人員進出？	~~體及環境安全管理第二節周邊安全管理二、人員進出管制。~~	
5.3.1.5	⑤若涉及個人資料檔案之應用，其程式之設計及管理有無妥善規劃，以防止資料遭不當使用？測試用之機敏資料，是否先進行資料遮蔽處理或管制保護？	⑤若涉及個人資料檔案之應用，其程式之設計及管理有無妥善規劃，以防止資料遭不當使用？		同上。
5.3.1.6	⑥系統實施前是否訂有測試計	⑥系統實施前是否訂有測試計畫？所		同上。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	畫？所有程式、相關子系統及整體系統是否均經完全的測試？其測試結果是否均經系統分析師的覆核及有關主管核示？是否由使用單位作系統接受性測試？測試環境是否符合下列要求：	有程式、相關子系統及整體系統是否均經完全的測試？其測試結果是否均經系統分析師的覆核及有關主管核示？是否由使用單位作系統接受性測試？		
5.3.1.6.1	I 是否評估並辦理：			
5.3.1.6.1.1	A.應建立病毒偵測機制並定期更新病毒碼或建立白名單管控機制，以避免安裝未授權程式。			
5.3.1.6.1.2	B.應隨時掌握資安事件，針對高風險或重要項目立即進行清查及應變。			
5.3.1.6.1.3	C.應定期進行弱點掃描，並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，填寫評估結果及處理			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	情形，採取適當措施並確保作業系統及軟體安裝經測試且無弱點顧慮之安全修補程式。			
5.3.1.6.1.4	D.應避免採用已停止弱點修補或更新之系統軟體及應用軟體，如有必要 應採用必要防護措施。			
5.3.1.6.2	Ⅱ是否避免同時共用不同環境(如營運環境、測試環境、辦公環境)之設備、憑證金鑰、資源存取帳密及使用者配置檔(User Profiles)？			
5.3.1.6.3	Ⅲ是否限制連接網際網路？如有需要是否遵循銀行公會所訂定之相關電子銀行相關自律規範辦理？			
5.3.1.11	⑪第一類電腦系統上線前及針對異動程式是否至少每半年辦理程式碼掃描或黑箱測試作業，並針對掃描或			同上。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	測試結果執行風險評估，依據不同風險訂定適當措施及完成時間，執行矯正、記錄處理情形並追蹤改善？			
5.3.4 5.3.4.1 5.3.4.1.1 5.3.4.1.2	(4)供應鏈風險管理 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： 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？ Ⅱ屬核心資通系統與第一類電腦系統之委外開發項目，其專案成員是否有資訊安全人員參與？			參考本會 112.3.29 金管銀國字第 1120270185 號函洽悉銀行公會新增「金融機構資通系統與服務供應鏈風險管理規範」，新增查核事項。
5.3.4.2 5.3.4.2.1	②選擇供應商前，是否執行下列事項： 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、資訊安全要求，以及資訊安全要求之			同上。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	服務水準?			
5.3.4.2.2	Ⅱ選擇供應商過程，如涉及銀行資訊交換，是否於資訊交換前簽署保密協議書?			
5.3.4.2.3	Ⅲ是否執行安全評估以選任合適之供應商：			
5.3.4.2.3.1	A.是否注意作業委託供應商對銀行服務集中度之適度分散?如存在集中度過高之疑慮，是否依評估結果擬訂對應之風險處理措施?			
5.3.4.2.3.2	B.是否評估供應商對所委託項目之資訊安全管理機制?			
5.3.4.2.3.3	C.是否評估供應商與其提供產品或服務位置?			
5.3.4.3	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：			同上。
5.3.4.3.1	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國際標準要求，並訂定供應商未符合資訊			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	安全要求或服務水準時之罰責標準?			
5.3.4.3.2	Ⅱ是否定義銀行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，包含人員管理、資訊存取與傳輸安全管控機制等?			
5.3.4.3.3	Ⅲ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?			
5.3.4.3.4	Ⅳ是否與供應商約定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、異常管理等服務要求?			
5.3.4.3.5	Ⅴ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、金融監督管理委員會及中央銀行，或其指定之人能取得供應			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	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?			
5.3.4.3.6	Ⅵ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?			
5.3.4.3.7	Ⅶ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?			
5.3.4.4	④於供應商契約存續期間，是否注意下列原則：			同上。
5.3.4.4.1	Ⅰ銀行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？			
5.3.4.4.2	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			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	跡？			
5.3.4.4.3	Ⅲ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？			
5.3.4.4.4	Ⅵ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，並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？			
5.3.4.4.5	Ⅴ是否建立對核心資通系統與第一類電腦系統供應商資訊安全稽核之程序，包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，包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？			
5.3.4.4.6	Ⅵ是否監督供應商針對其專案執行			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	人員辦理資訊安全教育訓練？			
5.3.4.4.7	Ⅶ是否依契約要求審查供應商所交付之系統或程式，包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？			
5.3.4.4.8	Ⅷ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？			
5.3.4.5	⑤供應商服務變更與契約終止時，是否符合下列事項：			同上。
5.3.4.5.1	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)，銀行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？			
5.3.4.5.2	Ⅱ供應商契約終止時，銀行是否於供應商依約完成產品或服務之移轉、交付驗收程序後，監督其完成資訊資產與資料返還、移交、			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	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？			
5.3.4.6	⑥系統之開發或維護外包時，對軟體開發或維護規範之訂定，軟體設計或修改之督導、核定及驗收等是否比照自行開發設計準則及控管程序辦理？	②系統之開發或維護外包時，對軟體開發或維護規範之訂定，軟體設計或修改之督導、核定及驗收等是否比照自行開發設計準則及控管程序辦理？		調整項目編號。
~~5.3.4~~ ~~5.3.4.1~~ ~~5.3.4.1.1~~ ~~5.3.4.1.2~~ ~~5.3.4.1.3~~ ~~5.3.4.1.4~~	(刪除)	(4)外包業務管理 ①外包契約是否依理事會核准之委外內部作業準則適當訂定，包括： Ⅰ具體之委外事項內容，對涉及機密性、敏感性或是關鍵性的應用系統項目是否予納入？ Ⅱ廠商之資訊安全責任及保密規定，是否要求廠商遵守？ Ⅲ廠商是否建立內部控制及考核機制？ Ⅳ金融機構於必要時是否得事前通知廠商後解約？	~~「金融機構作業委託他人處理內部作業制度及程序辦法」。~~	參考本會 112.3.29 金管銀國字第 1120270185 號函洽悉銀行公會新增「金融機構資通系統與服務供應鏈風險管理規範」，原查核事項「外包業務管理」修正為「供應鏈風險管理」，爰刪除原查核事項。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
~~5.3.4.1.5~~		Ⅴ就委外事項之範圍，是否同意主管機關得取得相關資料或報告，及進行金融檢查，或得命令期於期限內提供相關資料或報告？		
~~5.3.4.1.6~~		Ⅵ廠商處理及通報資訊安全事件的責任及作業程序？		
~~5.3.4.3~~		③上述業務之外包，其開發、維護之預定進度及作業安全、委託內容、機密維護、損害賠償等雙方權責之劃分，是否明定於外包契約內？		
~~5.3.4.4~~		④外包業務是否有專人管理，並控制進度？		
~~5.3.4.5~~		⑤對委外事項是否指定專責單位加強控管，定期與不定期稽核，並留存紀錄以供查核？		
~~5.3.4.6~~		⑥是否建立適當程序以確保外包廠商依合約維護程式，且程式更新程序係屬適當？並指定專人負責監控廠商維護活動及服務？		
~~5.3.4.7~~		⑦若廠商得撥接至受檢單位電腦以診		

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
~~5.3.4.8~~		斷及維護系統，受檢單位是否建立適當程序以控制廠商活動範圍？ ⑧網路銀行業務系統委外開發或維運，是否於委外契約要求委外廠商提供之交易安全設計符合銀行公會所訂安控基準？		
5.4.1.5 5.4.1.5.1 5.4.1.5.2	⑤對各式主機系統之使用者帳號及其存取權限(含最高權限使用者帳號)之建置管理是否妥適，並遵循下列程序： Ⅰ除代登系統外於登入作業系統進行系統異動或資料庫存取時，是否留存人為操作紀錄，並於使用後儘速變更密碼?因故無法變更密碼者，是否建立監控機制，避免未授權變更，並於使用後覆核其操作紀錄? Ⅱ帳號是否採一人一號管理，避免多人共用同一個帳號為原則?如有共用需求，申請及使用是否有			參考銀行公會所訂之「金融機構資通安全防護基準」新增查核事項。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	其他補強管控方式(如使用後更換密碼、代登入機制、密碼拆分保管等)?是否留存操作紀錄?是否能區分人員身分?			
5.4.1.5.3	Ⅲ最高權限帳號使用時是否先取得權責主管或授權人員同意並保留稽核軌跡?			
5.4.1.5.4	Ⅳ具最高權限帳號、特殊功能(如程式或軟體異動、參數或組態變更權限等)權限帳號是否和日常維運用帳號區隔，並定期抽查使用結果，以防範未經授權使用?如為核心資通系統，是否於該等帳號被使用時，每日覆核使用結果?			
5.4.1.5.5	Ⅴ提供網際網路服務之伺服器及AD(網域服務)主機，對於最高權限帳號及特殊功能權限帳號，是否採雙因子認證?			
5.4.1.5.6	Ⅵ是否針對核心資通系統、第一類及第二類電腦系統依最小權限			

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	(least privilege)及僅知原則(need-to-know)配發權限予人員使用並定期審查帳號及權限之合理性，以符合職務分工及牽制原則?			
5.4.3.6	⑥有機敏資料儲存於使用者端操作環境、機敏資料於網際網路上傳輸、使用者身分確認資料（如固定密碼、設備資訊、生物特徵）儲存於系統內等情形者，是否建立隱密性機制？			同上。
5.4.8.2.1	I 是否區分網際網路、非武裝區（DMZ)、營運環境及其他（如內部辦公區）等區域，並使用防火牆進行彼此間之存取控管？機敏資料是否僅存放於安全的網路區域，未存放於網際網路及 DMZ 等區域？對外網際網路服務是否僅透過 DMZ 進行，再由 DMZ 連線至其他網路區域？對聯外網站與內部網路或電腦	I 對聯外網站與內部網路或電腦系統間之路徑是否加以控管？		同上。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	系統間之路徑是否加以控管？			
5.4.8.2.7	Ⅶ是否建立病毒偵測及預防程序，並定期辦理病毒碼更新或建立白名單管控機制？對重大電腦中毒事件是否確實釐清原因及研議防制對策？	Ⅶ對可能藉由網路侵入系統之病毒控管是否建置適當之偵測及預防程序？		參考銀行公會所訂之「金融機構資通安全防護基準」調整查核事項。
5.4.8.2.12	(刪除)	XII 是否建立防毒機制並定期更新病毒碼，對重大電腦中毒事件是否確實釐清原因及研議防制對策？		原查核事項移至5.4.8.2.7，爰刪除本項。
5.4.8.7	⑦是否定期進行弱點掃描？並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，填寫評估結果及處理情形，採取適當措施並確保作業系統及軟體安裝經測試且無弱點顧慮之安全修補程式？	⑦是否定期進行網路弱點掃描？針對網路弱點是否依據風險等級進行漏洞修補？		參考銀行公會所訂之「金融機構資通安全防護基準」調整查核事項。
5.4.8.8	⑧是否避免採用已停止弱點修補或更新之系統軟體及應用軟體？如有必要是否採用必要防護措施？	⑧是否定期進行系統修補更新？有無針對各類網路系統修補發布重大警訊？		同上。
5.4.8.9.4	Ⅳ防火牆系統軟體是否定期配合版本更新進行新、舊版本差異及對現行	Ⅳ防火牆是否定期強化，測試與升級之資訊與補強程式之下載？防火牆		同上。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	作業影響等之評估分析，並辦理後續處理？	維護管理是否包含這些項目？		
5.4.8.9.11 5.4.8.9.11.1 5.4.8.9.11.2 5.4.8.9.11.3 5.4.8.9.11.4 5.4.8.9.11.5	XI防火牆及具存取控制（Access control list，ACL）網路設備，是否遵循下列措施： A.是否定期檢視防火牆及具存取控制(ACL)網路設備參數設定？ B.是否檢視所開啟的通訊埠與業務需求相符？ C.是否定期檢視高風險設定及六個月內無流量之防火牆規則評估其必要性及風險？ D.是否針對已下線系統於半年內調整或停用防火牆規則？ E.是否每半年檢視DMZ之防火牆規則？			參考銀行公會所訂之「金融機構資通安全防護基準」新增查核事項。
5.4.8.14	⑭對全社員工上網行為管理是否建立妥適之管控措施，限制連結非業務相關網站，以避免下載惡意程式？			同上。
5.4.8.15	⑮經由網際網路連接至內部網路進行			同上。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	遠距之系統維護管理工作，是否遵循下列措施：			
5.4.8.15.1	Ⅰ是否建立授權機制，依據其申請項目提供必要授權？			
5.4.8.15.2	Ⅱ是否定義允許可連結之遠端設備，並確保已安裝必要資訊安全防護？			
5.4.8.15.3	Ⅲ是否加強變更作業之身分認證，於每次登入時得採用照會或二項以上安全設計並取得主管授權，惟緊急故障排除仍須於事後向主管核備？			
5.4.8.15.4	Ⅳ是否建立監控機制，留存操作紀錄，並由主管或獨立單位定期覆核？			
5.4.8.16	⑯提供員工經由外部網際網路連線使用之應用系統，是否遵循下列措施：			同上。
5.4.8.16.1	Ⅰ是否定期執行弱點掃描、滲透測試及程式原始碼掃描並儘速完成弱點修補？			

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
5.4.8.16.2 5.4.8.16.3	Ⅱ是否建立網頁防竄改機制並將該等系統納入監控範圍？ Ⅲ是否確保委外廠商交付之系統或程式無惡意程式及後門程式？			
5.4.8.17	⑰有機敏資料儲存於使用者端操作環境、機敏資料於網際網路上傳輸、使用者身分確認資料（如固定密碼、設備資訊、生物特徵）儲存於系統內等情形者，是否建立隱密性機制？			同上。
5.4.8.18	⑱透過網際網路傳輸途徑辦理電子銀行之業務，其客戶身分確認資料如為固定密碼者，其固定密碼是否於儲存時應先進行不可逆運算（如雜湊演算法）？另為防止透過預先產製雜湊值推測密碼，是否進行加密保護或加入不可得知之資料運算？採用加密演算法者，其金鑰是否儲存於經第三方認證並符合NIST FIPS 140-2 L3之硬體安全模			同上。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	組內並限制明文匯出功能？			
5.5.3 5.5.3.1 5.5.3.2 5.5.3.3	(3)故障復原及災害應變管理 ①是否建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源以處理各種可能之意外（狀況），俾能在最短時間內，恢復電腦作業功能？應變程序是否包括電腦軟硬體系統故障時之復原程序、資料檔案遭毀損或入侵破壞之復原程序、使用備援系統之轉換程序或故障期間之權宜作業方式？ ②是否每年驗證及演練其營運持續性控制措施？演練週期、範圍及項目是否妥適？是否保留相關演練紀錄及召開檢討會議？ ③應變計畫是否經最高主管批准？有關人員是否確知在災害中應扮演之角色及責任？	(3)故障復原及災害應變管理 ①是否分別或綜合訂定資訊安全事件緊急處理應變計畫，如：電腦軟硬體系統故障時之復原程序、資料檔案遭毀損或侵犯破壞之復原程序、使用備援系統之轉換程序或故障期間之權宜作業方式？ ②前述故障復原程序，使用備援系統之轉換程序，或權宜應變之作業方式，是否定期或不定期舉行個別或整體之測試、演練及調整更新計畫？ ③是否訂有災害應變計畫以處理各種可能之意外(狀況)，俾能在最短時間內，恢復電腦作業功能？ ④應變計畫是否經最高主管批准？有無每年定期演練？有關人員是否確知在災害中應扮演之角色及責任？	~~「財政部暨所屬機關（構）資訊安全管理準則」第十一章、第一節、三。~~	參考銀行公會所訂之「金融機構資通安全防護基準」調整查核事項，並刪除原引用法條。

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
~~5.7.2.2~~	(刪除)	②是否建立防毒機制並定期更新病毒碼，對重大電腦中毒事件是否確實釐清原因及研議防制對策？		已併入其他查核事項5.4.8.2.7，爰刪除本項。
5.7.2.2	②是否研擬南資中心無法提供服務時之應變計畫並辦理演練？	③是否研擬南資中心無法提供服務時之應變計畫並辦理演練？		調整項目編號。
~~5.13~~	(刪除)	13.辦理資通系統防護是否依「金融機構資通安全防護基準」之規定辦理?	~~銀行公會「金融機構資通安全防護基準」~~	已參考銀行公會所訂「金融機構資通安全防護基準」調整查核事項，併入其他查核項目，爰刪除本項。
~~5.14~~ ~~5.14.1~~	(刪除)	14.信用合作社是否依「金融控股公司及銀行業內部控制及稽核制度實施辦法」第38-1條第1項但書所稱主管機關對信用合作社辦理資訊安全相關規定辦理，如： (1)是否指派副總經理以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務。但屬有限責任中華民國信	~~本會111.7.26金管銀合字第11102102331號令。~~	原查核事項移至5.1.7.8，爰刪除本項。

資料基準日：112年6月30日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
		用合作社聯合社南區聯合資訊中心之會員社，得指派經理以上或職責相當之人兼任?		
~~5.14.2~~		(2)信用合作社是否依下列規定設置適當資訊安全人力資源：		
~~5.14.2.1~~		①上一會計年度決算後淨值達新臺幣30億元以上或放款總餘額達新臺幣 200 億元以上者，是否設置資訊安全主管及資訊安全人員?		
~~5.14.2.2~~		②未達上述規模者，是否設置至少 1 名資訊安全人員?		
~~5.14.3~~		(3)前點資訊安全主管及資訊安全人員除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。		
~~5.14.4~~		(4)信用合作社資訊安全主管或資訊安全人員負責規劃、監控及執行資訊安全管理作業，每年應將前一年度資訊安全整體執行情		

資料基準日：112 年 6 月 30 日

項目編號	查核事項		法令規章	說明
	修正後	修正前		
		形，依金融控股公司及銀行業內部控制及稽核制度實施辦法第二十七條第一項規定辦理內部控制制度聲明書之出具、揭露及公告申報，並由資訊安全長聯名出具。		
~~5.14.5~~		(5)信用合作社資訊安全主管及資訊安全人員，每年應至少接受15小時以上資訊安全專業課程訓練或職能訓練。總社資訊單位、財務保管單位及其他管理單位之人員，每年至少須接受3小時以上資訊安全宣導課程。		
~~5.14.6~~		(6)第一點有關配置資訊安全長之規定，信用合作社應於本令生效日後九個月內調整至符合規定。信用合作社應於符合第二點適用條件起六個月內調整。		

資料基準日：112年6月30日