本國銀行檢查手冊(異動版)

一、財務狀況之查核（共 2 項）

項目編號	查核事項		法令規章	說明	評核項目編號
	修正後	修正前			
1.3.5.3 ~~1.3.5.4~~	⑶銀行證券部門因兼營證券及期貨業務者，截至 99 年 12 月底已提列之「買賣損失準備」及「違約損失準備」金額，是否轉列「特別盈餘公積」並依規定之用途使用?	⑶銀行證券部門經營自行買賣有價證券業務者，其自行買賣有價證券利益額超過損失額時，是否按月就超過部分提列百分之十，作為買賣損失準備？ ⑷銀行證券部門經營受託買賣有價證券業務者，是否按月就受託買賣有價證券成交金額提列萬分之零點二八，作為違約損失準備？	~~證券商管理規則第 11 及 12 條~~ 本會 112.4.24 金管銀法字第 11202709871 號令	配合函令發布修正引用之參考法令	20
6.1	(一)銀行年報之記載事項，有無依規定辦理?	(一)銀行年報之記載事項，有無依規定辦理?	1.「公開發行銀行財務報告編製準則」 2.本會 112.3.3 金管銀法字第 11202705771 號令	配合函令發布修正引用之參考法令	24

二、存款業務之查核（共 1 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	評核項目編號
	修正後	修正前			
5.1.2.1.4	④「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、「銀行防制洗錢及打擊資助恐怖主義注意事項範本」第 4 條第 5 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？	④「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、「銀行防制洗錢及打擊資助恐怖主義注意事項範本」第 4 條第 5 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.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.「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.中華民國銀行公會『銀行防制洗錢及打擊資助恐怖主義注意事項範本』」第 4 條第 5 款 4.中華民國銀行公會『防杜人頭帳戶範本』及『開戶作業檢核表範本』 5.中華民國銀行公會『銀行受理客戶以網路方式開立儲值支付帳戶作業範本』 6.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」	配合法令修正，修正查核事項內容。	27

三、投資業務之查核(計 1 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	評核項目編號
	修正後	修正前			
6.9	㈨短期票券得以債票或登記形式發行;除國庫券外,以債票形式發行者,是否送集中保管機構保管,以登記形式發行者,是否由集中保管機構辦理發行登記?由集中保管或登記之短期票券,其買賣之交割,是否以帳簿劃撥方式為之?	㈨出售債票形式發行之短期票券,是否於交易當日,將債票交付買受人,或將其交由買受人委託之其他銀行或集中保管機構保管?	~~1.~~票券金融管理法第 26 條 ~~2.財政部 90.12.19 台財融(四)字第 0908010329 號函~~	配合法令修正及函令廢止,修正查核事項及引用之參考法令	20

四、信託業務之查核(計 1 項)

項目編號	查核事項		法令規章	說明	評核項目編號
	修正後	修正前			
4.3.8	8.金融機構辦理特定金錢信託資金投資有價證券業務,信託人為經許可來台之大陸地區人民,其投資是否符合規定?	8.金融機構辦理特定金錢信託資金投資國內外有價證券業務,信託人為經許可來台之大陸地區人民,其投資是否符合規定?	~~財政部 92.2.11 台財融(一)字第 0928010165 號令~~ 「銀行業辦理外匯業務作業規範」	配合函令廢止,修正引用之參考法令	22

五、內部管理之查核(共 6 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	評核項目編號
	修正後	修正前			
3.2.2.2	⑵庫房消防安全設備、保全設備、自動警報器、自動定時鎖等系統是否齊全，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營業時間，除必要人員進出時外，庫房內柵門是否上鎖關閉？	⑵庫房消防安全設備、保全設備、自動警報器、自動定時鎖等系統是否齊全，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營業時間，除必要人員進出時外，庫房內柵門是否上鎖關閉？	1.「金融機構安全維護管理辦法」 2.財政部 87.9.7 台財融第87744246 號函 ~~3.財政部 89.12.6 台財融(六)字第 89764495 號函~~	配合法規停止適用，刪除引用之參考法規	27
3.2.2.10	⑽是否加強員工自衛編組，實施防護區制，定期演練，確立「安全維護人人有責」觀念？	⑽是否加強員工自衛編組，實施防護區制，定期演練，確立「安全維護人人有責」觀念？	1.「金融機構安全維護注意要點」 ~~2.財政部 90.6.14 台財融(六)第 90744540 號函~~	配合法規停止適用，刪除引用之參考法規	27
3.2.4.12	⑿執行金融交易，是否嚴格規定各經辦人員不得以自己名義代客戶從事金融交易?是否留存交易紀錄憑證，以確保交易之真實性與完整性。	⑿執行金融交易，是否嚴格規定各經辦人員不得以自己名義代客戶從事金融交易?是否留存交易紀錄憑證，以確保交易之真實性與完整性。	~~89.5.1 台財融字第 89710787 號函~~	配合法規停止適用，刪除引用之參考法規	27
~~3.3.9~~	(刪除)	9.銀行辦理電子票證業務時，是否依規定辦理？	~~電子票證發行管理條例第 20 條~~	配合法規停止適用，刪除有關電子票證相關查核事項及引用之規定	20
~~3.3.10~~	(刪除)	10.簽訂電子票證特約機構時，是否於契約中載明特約機構不得將交易手續費轉嫁予持卡人負擔？	~~本會 98.8.31 金管銀票字第 09840006210 號函~~	配合法規停止適用，刪除有關電子票證相關查核事項及引用之規定	22

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	評核項目編號
	修正後	修正前			
4.5.9 4.5.9.1 4.5.9.2 4.5.9.3 4.5.9.4 4.5.9.5 4.5.9.6 	9.採行風險導向內部稽核制度： (1)內部稽核是否建立風險評估之程序與方法，以辨識並評估各受查主體所面臨之風險？ (2)對受查主體之固有風險、控制措施有效性，依風險評估模型評估結果，有無欠合理之情形？是否建立風險評估因子或指標有效性之定期驗證機制？ (3)是否訂定受查主體之綜合風險評估結果與查核頻率連結之標準？查核方式、查核範圍、查核頻率與查核次數是否符合相關規範？ (4)是否依據所訂定之評估方法，每年至少執行一次風險評估？是否留存紀錄並至少保存五年？ (5)是否訂定內部稽核品質評核機制？ (6)是否依據評核結果，就可能影響內部稽核整體運作事項擬訂改善計畫，由總稽核負責督	9.採行風險導向內部稽核制度： (1)內部稽核是否建立風險評估之程序與方法，以辨識並評估各受查主體所面臨之風險？ (2)對受查主體之固有風險、控制措施有效性，依風險評估模型評估結果，有無欠合理之情形？是否建立風險評估因子或指標有效性之定期驗證機制？ (3)是否訂定受查主體之綜合風險評估結果與查核頻率連結之標準？查核方式、查核範圍、查核頻率與查核次數是否符合相關規範？ (4)是否依據所訂定之評估方法，每年至少執行一次風險評估？是否留存紀錄並至少保存五年？ (5)是否訂定內部稽核品質評核機制？ (6)是否依據評核結果，就可能影響內部稽核整體運作事項擬訂改善計畫，由總稽核負責督	1.「金融控股公司及銀行業內部控制及稽核制度實施辦法」第 15 條之 1 2.銀行公會「銀行業建立風險導向內部稽核制度實務守則」 ~~3.本會 107.4.12 金管檢制字第 10706001130 號令~~ 3.本會 112.1.17 金管檢制字第 11206000101 號令 4.採行風險導向內部稽核制度作業問答集 5.本會 109.2.13 金管檢銀字第 1090604016 號函	配合函令更新，新增並刪除引用之參考法規	24

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	評核項目編號
	修正後	修正前			
	導改善計畫之確實執行？	導改善計畫之確實執行？			
4.5.9.7	(7)對受查主體縮減或整併及風險評估方法論等有大幅變更者，屬整體風險導向內部稽核制度之重大改變，是否報本會檢查局備查？	(7)對受查主體縮減或整併及風險評估方法論等有大幅變更者，屬整體風險導向內部稽核制度之重大改變，是否報本會檢查局備查？			
4.5.9.8	(8)採行風險導向內部稽核制度，是否報本會核准？子公司經評估有未予納入風險導向內部稽核制度實施者，是否提供評估文件，報本會核准？	(8)採行風險導向內部稽核制度，是否報本會核准？子公司經評估有未予納入風險導向內部稽核制度實施者，是否提供評估文件，報本會核准？			

六、資訊業務之查核（共 20 項）

項目編號	查核事項		法令規章	說明	評核項目編號
	修正後	修正前			
2.1.3.6.10	J.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：	J.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：	「金融機構資通安全防護基準」第 13 條第 3 款	新增查核事項	28
2.1.3.6.10.1	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？	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？			
2.1.3.6.10.2					
2.1.3.6.10.3	b.是否檢視所開啟的通訊埠與業務需求相符？	b.是否檢視所開啟的通訊埠與業務需求相符？			

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	評核項目編號
	修正後	修正前			
2.1.3.6.10.4 2.1.3.6.10.5	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？	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？			
2.1.6	6.是否將各作業系統、網路設備、資安設備之日誌，及稽核軌跡集中管理，進行異常紀錄分析，設定合適告警指標並定期檢討修訂？	6.是否將各作業系統、網路設備、資安設備之日誌，及稽核軌跡集中管理，進行異常紀錄分析，設定合適告警指標並定期檢討修訂？	「金融機構資通安全防護基準」第 16 條第 1 款 ~~「金融機構辦理電子銀行業務安全控管作業基準」~~	刪除法令規章	28
2.1.17	17.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	17.使用者身分確認資料如為固定密碼者，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 之硬體安全模組內並限制明文匯出功能？	「金融機構資通安全防護基準」第 6 條 2 款	修正查核事項	28

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	評核項目編號
	修正後	修正前			
	L3 之硬體安全模組內並限制明文匯出功能？				
2.1.18 2.1.18.1 2.1.18.2 2.1.18.3	18.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： (1)是否定期執行弱點掃描、滲透測試及程式原始碼掃描並盡速完成弱點修補？ (2)是否建立網頁防竄改機制並將該等系統納入監控範圍？ (3)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？		「金融機構資通安全防護基準」13 條 6 款	新增查核事項	28
2.2.3 2.2.3.1	3.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： (1)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，應留存人為操作紀錄，並於使用後儘速變更密碼；但因故無法變更密碼者，應建立監	3.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： (1)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，應留存人為操作紀錄，並於使用後儘速變更密碼；但因故無法變更密碼者，應建立監	「金融機構資通安全防護基準」第 4 條第 5、6 及 9~12 款	修正查核事項	28

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	評核項目編號
	修正後	修正前			
2.2.3.2	控機制，避免未授權變更，並於使用後覆核其操作紀錄。	控機制，避免未授權變更，並於使用後覆核其操作紀錄。			
2.2.3.3	(2)帳號應採一人一號管理，避免多人共用同一個帳號為原則，如有共用需求，申請及使用須有其他補強管控方式(如使用後更換密碼、代登入機制、密碼拆分保管等)，並留存操作紀錄且應能區分人員身分。 (3)最高權限帳號使用時應先取得權責主管或授權人員同意並保留稽核軌跡。	(2)帳號應採一人一號管理，避免多人共用同一個帳號為原則，如有共用需求，申請及使用須有其他補強管控方式(如使用後更換密碼、代登入機制、密碼拆分保管等)，並留存操作紀錄且應能區分人員身分。 (3)最高權限帳號使用時應先取得權責主管或授權人員同意並保留稽核軌跡。			
2.2.3.4	(4)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)權限帳號應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，應於該等帳號被使用時，每日覆核使用結果。	(4)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)權限帳號應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，應於該等帳號被使用時，每日覆核使用結果。			
2.2.3.5	(5)提供網際網路服務之伺服器及AD(網域服務)主機，對於最高	(5)提供網際網路服務之伺服器及AD(網域服務)主機，對於最高			

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	評核項目編號
	修正後	修正前			
	權限帳號及特殊功能權限帳號，應採雙因子認證。	權限帳號及特殊功能權限帳號，應採雙因子認證。			
2.2.3.6	(6)應針對核心資通系統、第一類及第二類電腦系統依最小權限(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、權限之合理性及異常存取紀錄，以符合職務分工及牽制原則。	(6)應針對核心資通系統、第一類及第二類電腦系統依最小權限(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。			
2.3.2.8 2.3.2.8.1 2.3.2.8.2	(8)系統轉換、架構重大調整或跨版本升級前之準備工作 A.是否建立架構審查機制，從AP、DB、資安、網路、平台、營運等面向進行評估，並評估一次過版或平行運轉可行性？ B.是否檢視相關設備容量，評估營運及業務需求所需備載容量(如跨行交易平台、企業應用系統整合EAI、企業服務匯流排 ESB 等)。是否建置擬真測試環境，測試新系統或功能	(8)系統轉換前之準備工作 A.是否建立架構審查機制，從AP、DB、資安、網路、平台、營運等面向進行評估，並評估一次過版或平行運轉可行性？ B.是否檢視相關設備容量，評估營運及業務需求所需備載容量(如跨行交易平台、企業應用系統整合EAI、企業服務匯流排 ESB 等)。是否建置擬真測試環境，測試新系統或功能相容於既有營運環境之架構、設備及參數？	「金融機構資通安全防護基準」第15條第1款	修正及新增查核事項	28

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	評核項目編號
	修正後	修正前			
2.3.2.8.3	相容於既有營運環境之架構、設備及參數？ C.是否檢視各項測試個案，依據影響範圍進行功能測試(如單元、整合、迴歸等) 及非功能測試(如壓力、相容等)，並進行整體性演練？	C.是否檢視各項測試個案，依據影響範圍進行功能測試(如單元、整合、迴歸等) 及非功能測試(如壓力、相容等)，並進行整體性演練？			
2.3.2.8.4	D.是否建立上線及復原計畫，並建立多個檢核點及啟動復原之決策條件？	D.是否建立上線及復原計畫，並建立多個檢核點及啟動復原之決策條件？			
2.3.2.8.5	E.是否進行上線變更審查及風險評估，辨識複雜度及影響範圍，檢視測試個案及上線復原計畫之完整性？	E.是否進行上線變更審查及風險評估，辨識複雜度及影響範圍，檢視測試個案及上線復原計畫之完整性？			
2.3.2.8.6	F.是否要求廠商上線支援，並能緊急提供備品、更高容量設備、問題查找及修改人力？	F.是否要求廠商上線支援，並能緊急提供備品、更高容量設備、問題查找及修改人力？			
2.3.2.8.7	G.是否預留復原作業及上線驗證時間？	G.是否預留復原作業及上線驗證時間？			
2.3.2.8.8	H.是否召開上線協調會議，安排工作項目並確保各項準備到位？	H.是否召開上線協調會議，安排工作項目並確保各項準備到位？			
2.3.2.8.9		I.是否提前公告並進行教育訓練(含異常話術)？			

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	評核項目編號
	修正後	修正前			
2.3.2.8.10	I.是否提前公告並進行教育訓練(含異常話術)？ J.轉換前關鍵準備工作，如：架構審查、上線變更審查及風險評估、上線協調會議等具資安控制性之事項，是否請資安專責單位參與，並由資安長發揮統籌資安政策推動與資源調度之工作？				
2.3.2.12	(12)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？	(12)系統或新功能首次上線前及至少每半年是否針對異動程式辦理程式碼掃描或黑箱測試作業，並針對掃描或測試結果執行風險評估及漏洞(或弱點)修補？	~~「金融機構辦理電子銀行業務安全控管作業基準」~~ 「金融機構資通安全防護基準」第 10 條第 13 款	修正查核事項及法令規章	28
2.5.2 2.5.2.1 2.5.2.2	2.開放網際網路連線使用之視訊會議使用管理 (1)是否適時更換視訊會議代碼或密碼，避免重複使用？ (2)機敏性會議是否採用高強度密碼或多因子進行身分驗證？	2.開放網際網路連線使用之視訊會議使用管理 (1)是否適時更換視訊會議代碼，避免重複使用？ (2)機敏性會議是否採用高強度密碼或多因子進行身分驗證？	「金融機構資通安全防護基準」第 12 條	修正查核事項	28

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	評核項目編號
	修正後	修正前			
2.5.2.3 2.5.2.4 2.5.2.5	(3)是否確認與會者身分後再進行會議，以確保會議內容不外流？ (4)是否評估使用線上紀錄功能，避免會議內容外洩風險？ (5)參加會議時，是否關閉非必要功能，注意發送及分享資訊，避免機敏資料外洩？	(3)是否確認與會者身分後再進行會議，以確保會議內容不外流？ (4)是否評估使用線上紀錄功能，避免會議內容外洩風險？ (5)參加會議時，是否關閉非必要功能，注意發送及分享資訊，避免機敏資料外洩？			
5.1.1 5.1.1.1 5.1.1.2	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： (1)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？ (2)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？	1.對主要核心業務是否於委外前辦理評估分析，並將法規遵循、營運風險、法律風險及維持業務營運不中斷的應變能力等項目納入評估？	「金融機構資通系統與服務供應鏈風險管理規範」第 4 條	新增查核事項及法令規章	28
5.1.2	2.辦理受託機構遴選作業，是否建立妥適之遴選程序(包括設置評選小組、研訂評選標準、評	2.辦理受託機構遴選作業，是否建立妥適之遴選程序(包括設置評選小組、研訂評選標準、評	「金融機構資通系統與服務供應鏈風險管理規範」第 5 條	新增查核事項及法令規章	28

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	評核項目編號
	修正後	修正前			
	選作業、議價程序及呈報遴選結果等)，並執行下列事項：	選作業、議價程序及呈報遴選結果等)，並落實執行？			
5.1.2.1	(1)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服務水準？				
5.1.2.2	(2)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？				
5.1.2.3	(3)是否執行安全評估以選任合適之供應商：				
5.1.2.3.1	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？				
5.1.2.3.2	B.是否評估供應商對所委託項目之資訊安全管理機制？				
5.1.2.3.3	C.是否評估供應商與其提供產品或服務位置？				
5.1.3 ~~5.1.4~~	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：	4.核心資通系統及第一類電腦系統之委託契約或相關文件中，	~~「金融機構資通安全防護基準」第16條第2款~~	修正項目編號、查核事項項次、查核事項、法令規	28

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	評核項目編號
	修正後	修正前			
5.1.3.1 ~~5.1.4.1~~	(1)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安全要求或服務水準時之罰責標準？ (2)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？ (3)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？ (4)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)是否保留對供應商之稽核權?	是否明確約定下列內容： (1)是否要求受託廠商遵守本基準及其他適當資訊安全國際標準要求？ (2)是否與受託廠商就服務品質、水準、效能等方面訂定服務要求？ (3)是否依本基準內容對受託廠商進行適當監督？ (4)當發生資安事故時，受託廠商是否主動、即時通知委託人？ (5)是否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程式碼掃描或黑箱測試？	「金融機構資通系統與服務供應鏈風險管理規範」第 6 條	章，及新增查核事項	
5.1.3.2 ~~5.1.4.2~~					
5.1.3.3 ~~5.1.4.3~~					
5.1.3.4 ~~5.1.4.4~~					
5.1.3.5 ~~5.1.4.5~~	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				

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	評核項目編號
	修正後	修正前			
5.1.3.6 5.1.3.7	員會及中央銀行，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？ (6)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？ (7)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？				
5.1.4 ~~5.1.3~~ 5.1.4.1	4.供應商服務變更與契約終止時，是否符合下列事項： (1)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？	3.法規規定之應記載事項是否均已納入合約載明？其他重要應注意事項，如委外服務品質保證、終止委託之通知時程及配合移轉程序等事項，是否明訂，相關條款是否妥適明確？	~~「金融機構作業委託他人處理內部作業制度及程序辦法」~~「金融機構資通系統與服務供應鏈風險管理規範」第 8 條	修正項目編號、查核事項項次、查核事項、法令規章，及新增查核事項	28

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	評核項目編號
	修正後	修正前			
5.1.4.2	(2)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、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？				
5.2.1.3 5.2.1.3.1 5.2.1.3.2 5.2.1.3.3	(3)核心資通系統及各類電腦系統是否具備以下管理機制： A.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？ B.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？ C.當委外廠商或相關管理員工職務調動或離職時，網路系統相關的權限與設定是否刪除以避免未經授權之存取？	(3)核心資通系統及各類電腦系統是否具備以下管理機制： A.是否先對受託廠商進行適當之安全評估，並依據最小權限及資訊最小揭露原則進行安全管控設計？ B.是否定期針對可存取銀行內部網路之駐點廠商人員，辦理電子郵件社交工程教育訓練？	~~「金融機構資通安全防護基準」第16條第1款~~ 「金融機構資通系統與服務供應鏈風險管理規範」第7條	修正查核事項及法令規章及合併原5.2.2	28

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	評核項目編號
	修正後	修正前			
5.2.1.4	(4)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？對異常狀況是否能即時掌握並確實追蹤控管後續處理情形，重大異常事項是否提報高階管理階層？		「金融機構資通系統與服務供應鏈風險管理規範」第 7 條	新增查核事項及合併原 5.2.3	28
5.2.1.5	(5)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？		「金融機構資通系統與服務供應鏈風險管理規範」第 7 條	新增查核事項	28
5.2.1.6	(6)是否監督供應商針對其專案執行人員辦理資訊安全教育訓練？		「金融機構資通系統與服務供應鏈風險管理規範」第 7 條	新增查核事項	28
5.2.1.7	(7)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？		「金融機構資通系統與服務供應鏈風險管理規範」第 7 條	新增查核事項	28
~~5.2.2~~	(刪除)	2.當委外廠商或相關管理員工職務調動或離職時，網路系統相		已併入其他查核事項(5.2.1.3.3)，爰刪除本項	28

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	評核項目編號
	修正後	修正前			
		關的權限與設定是否刪除以避免未經授權之存取？			
~~5.2.3~~	(刪除)	3.對異常狀況是否能即時掌握並確實追蹤控管後續處理情形，重大異常事項是否提報高階管理階層？	「金融機構作業委託他人處理內部作業制度及程序辦法」	已併入其他查核事項(5.2.1.4)，爰刪除本項	28
5.2.2 ~~5.2.4~~ 5.2.2.1 5.2.2.2	2.對受託機構是否建立妥適之查核機制： (1)是否訂定查核計畫、查核範圍(含人員職務分工、作業處理、媒體管理、資料檔案及程式變更、受託機構之自行查核情形、災變因應計畫演練等)、查核單位、抽樣標準，及查核結果之呈報與後續改善情形追蹤等，並落實執行？ (2)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	4.對受託機構是否建立妥適之查核機制，包括訂定查核計畫、查核範圍(含人員職務分工、作業處理、媒體管理、資料檔案及程式變更、受託機構之自行查核情形、災變因應計畫演練等)、查核單位、抽樣標準，及查核結果之呈報與後續改善情形追蹤等，並落實執行？核心資通系統是否定期針對供應商辦理資訊安全訪視，或委由第三方提出報告(如 ISO/CNS 27001 有效證書)？	~~「金融機構資通安全防護基準」第 16 條第 3 款~~ 「金融機構作業委託他人處理內部作業制度及程序辦法」 「金融機構資通系統與服務供應鏈風險管理規範」第 7 條	修正項目編號、查核事項項次、查核事項及法令規章	28

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	評核項目編號
	修正後	修正前			
	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?				

七、 其他事項之查核（共 10 項）

項目編號	查核事項		法令規章	說明	評核項目編號
	修正後	修正前			
1.3.3.8	(8)承作結構型商品交易，是否針對弱勢族群客戶，訂定強化商品交易控管機制？對帳單或相關重要資訊提供方式，是否視委託人個別特殊需求，採行掛號、雙掛號或其他合適告知方式提供?	(8)承作結構型商品交易，是否針對弱勢族群客戶，訂定強化商品交易控管機制？	1.本會 105.7.21 金管銀控字第 10560001510 號函 2.「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」第 29 條之 1 3.本會 112.2.13 金管銀票字第 1120270361 號函	配合新增函示增列參考法令	22
2.20	(二十)發卡機構於申請書之申請人聲明及同意事項中，是否載明下列事項，並經申請人以簽名或其他得以辨識申請人同一性及確定申請人意思表示之方式確認： 1.所收取之利率及各項費用，並詳列計收標準及收取條件。	(二十)發卡機構於申請書之申請人聲明及同意事項中，是否載明下列事項，並經申請人以簽名或其他得以辨識申請人同一性及確定申請人意思表示之方式確認： 1.所收取之利率及各項費用，並詳列計收標準及收取條件。	1.「信用卡業務機構管理辦法」第 42 條 2.本會 112.2.24 金管銀合字第 11102741631 號函	配合新增函示增列參考法令	20

資料基準日：112 年 6 月 30 日

	2.持卡人未按時依約繳款之紀錄，將登錄聯徵中心，而影響未來申辦其他貸款之權利。 3.發卡機構與第三人合作，如涉及持卡人資料之使用，應設計欄位供申請人自行勾選是否同意提供個人資料予該第三人，並明列其使用範圍。	2.持卡人未按時依約繳款之紀錄，將登錄聯徵中心，而影響未來申辦其他貸款之權利。 3.發卡機構與第三人合作，如涉及持卡人資料之使用，應設計欄位供申請人自行勾選是否同意提供個人資料予該第三人，並明列其使用範圍。			
2.82.3 2.82.3.1 2.82.3.2	3.第三方服務提供者管理 (1)與第三方服務提供者合作是否簽訂契約?契約是否明訂權利及義務關係、並建立相關徵信審核、風險控管及定期查核等管理機制？ (2)與第三方服務提供者進行相關業務合作時，是否有以廣宣費用以外，其他變動費用或獎金給付方式鼓勵第三方服務業者推銷其線上信用卡業務(變相委外)，惟未向本會申請及核准？	3.第三方服務提供者管理 (1)與第三方服務提供者合作是否簽訂契約?契約是否明訂權利及義務關係、並建立相關徵信審核、風險控管及定期查核等管理機制？ (2)與第三方服務提供者進行相關業務合作時，是否有以廣宣費用以外，其他變動費用或獎金給付方式鼓勵第三方服務業者推銷其線上信用卡業務(變相委外)，惟未向本會申請及核准？	1.銀行公會「金融機構辦理電子銀行業務安全控管作業基準」第 8 及 11~~14~~條 2.金融機構作業委託他人處理內部作業制度及程序辦法第 11 條第 1 項	配合法令修正更新參考法令規章	27
6.2.3.3	⑶資訊相互運用及客戶權益保護	⑶資訊相互運用及客戶權益保護	1.「金融控股公司子公司間共同行銷管理辦法」 2.本會 112.1.9 金管銀法字第 11102253601 號令	配合函令更新，新增並刪除引用之參考法規	20

資料基準日：112 年 6 月 30 日

			~~2.本會93.9.13金管銀(一)字第0938011562號函~~ 3.金融控股公司子公司間共同行銷問答集		
6.2.3.3.1	①金控公司與其子公司及各子公司間相互揭露客戶資料，是否訂定保密協定，並維護客戶資料之機密性或限制其用途？收受並運用資料之其他子公司是否再向其他第三人揭露該等資料？	①金控公司與其子公司及各子公司間相互揭露客戶資料，是否訂定保密協定，並維護客戶資料之機密性或限制其用途？收受並運用資料之其他子公司是否再向其他第三人揭露該等資料？	1.「金融控股公司子公司間共同行銷管理辦法」 2.本會 112.1.9 金管銀法字第11102253601號令 ~~2.本會93.9.13金管銀(一)字第0938011562號函~~ 3.金融控股公司子公司間共同行銷問答集	配合函令更新，新增並刪除引用之參考法規	20
6.2.3.3.2	②金控公司銀行子公司是否向客戶揭露交互運用客戶資料之子公司名稱及其保密措施？該名稱及措施內容是否於公司網頁公告，並以書面、電子郵件方式通知客戶或於營業處所內明顯位置公告？	②金控公司銀行子公司是否向客戶揭露交互運用客戶資料之子公司名稱及其保密措施？該名稱及措施內容是否於公司網頁公告，並以書面、電子郵件方式通知客戶或於營業處所內明顯位置公告？	1.「金融控股公司子公司間共同行銷管理辦法」 2.本會 112.1.9 金管銀法字第11102253601號令 ~~2.本會93.9.13金管銀(一)字第0938011562號函~~ 3.金融控股公司子公司間共同行銷問答集	配合函令更新，新增並刪除引用之參考法規	20
7.8.1.2	⑵對如何確認申請人身分，是否有明訂確認之程序，以防止冒名申請？辦理跨機構間之客戶快速身分識別機制(簡稱金融FIDO)之安全控管，是否依安全	⑵對如何確認申請人身分，是否有明訂確認之程序，以防止冒名申請？	「金融機構辦理快速身分識別機制安全控管作業指引」	配合法令增列查核事項	28

資料基準日：112 年 6 月 30 日

	控管作業指引辦理?				
10.1.5	5.是否參照「臨櫃作業關懷客戶提問參考範本」、「銀行服務失智者或疑似失智者之實務參考做法」等規定，制定櫃台人員對高齡客戶、失智者或疑似失智者異常金融交易行為之應對保護措施？	5.是否參照「臨櫃作業關懷客戶提問參考範本」規定，制定櫃台人員對高齡客戶異常金融交易行為之應對保護措施？	1.「銀行業公平對待高齡客戶自律規範」第 12 條 2.「臨櫃作業關懷客戶提問參考範本」 3.「銀行服務失智者或疑似失智者之實務參考做法」	配合法令增列查核事項	22
10.6.4	4.招攬保險業務之行員及督導本項業務之主管是否依規定接受教育訓練?	4.招攬保險業務之行員及督導本項業務之主管是否依規定接受教育訓練?	1.「銀行、保險公司、保險代理人或保險經紀人辦理銀行保險業務應注意事項」第 7 點 2.「保險業務員管理規則」第 12 條 3.本會 107.12.11 金管保壽字第 10704549750 號函 4.「個人執業代理人、受代理人公司或銀行任用之代理人參加公平對待六十五歲以上客戶教育訓練課程完訓通報作業要點」	配合新增法令，增列引用之參考法規	22
11.1	㈠ 定型化契約內容有無與定型化契約範本內容相抵觸或意旨不符者？	㈠ 定型化契約內容有無與定型化契約範本內容相抵觸或意旨不符者？	1.「個人網路銀行業務服務定型化契約範本」 2.「金融機構保管箱出租定型化契約範本」	配合法規停止適用，刪除引用之參考法規	22

資料基準日：112 年 6 月 30 日

			3.「個人購車及購屋貸款定型化契約範本」 4.「信用卡定型化契約範本」 5.「活期（儲蓄）存款契約附屬金融卡定型化約款範本」 ~~6.「電子票證定型化契約範本」~~ 7.「消費性無擔保貸款定型化契約範本」		

資料基準日：112 年 6 月 30 日