檢查局115年度各業別金融檢查重點

壹、前言

本局經參酌國內外政經環境變化及外界關注議題，並考量本會監理重點、114年度所發布金融法規及應加強檢查事項等，擬定115年度金融檢查重點，合計113項。

鑑於近年國內金融投資詐騙案件頻傳，詐騙手法不斷更新，詐騙款項亦多有匯出至境外及疑似利用虛擬帳號從事洗錢之情事，理專或業務人員不當銷售行為仍時有所聞，金融業資通安全仍存有潛在風險，爰擬將「防制詐騙」、「防制洗錢」、「金融消費者權益保護」及「資通安全韌性」等列為115年度檢查特別關注領域。

貳、115年度各業別金融檢查重點

一、金融控股公司

(一)防制洗錢、打擊資恐及反武器擴散落實情形：建立集團整體性防制洗錢及打擊資恐計畫，包括在符合國外分公司（或子公司）當地法令下，以防制洗錢及打擊資恐為目的之集團內資訊分享政策及程序，並檢討落實情形。

(二)法令遵循制度實施情形：金控公司法令遵循制度設計及運作情形之有效性。

(三)轉投資事業管理：

1.金控公司應建立適當之投資暨併購管理規範及控管機制並落實執行，包括：保密與內線交易控管機制、投資前評估、審核及核決程序、公告申報、法令遵循、投資後效益追蹤與風險管理、建立利益衝突或不當交易防範之具體控管程序及稽核機制。

2.對海外重大轉投資公司(含參股投資)之投資管理規範，應包括確保海外重大轉投資公司營運之健全性及符合法令要求，建立相應監督控管機制。

3.金控公司應建立經營風險督導管理機制，定期確認子公司營運之健全性並符合法令要求(包括利益衝突防範及利害關係人交易與管理作業控管機制等)，並督導子公司下列事項：

(1)法令遵循：子公司法令遵循制度之有效性，並落實執行相關內部規範之導入、建置與實施(包括對防制洗錢法令規範之瞭解及遵循情形，及相關檢查缺失改善)，並建立完善檢舉制度。

(2)風險管理：子公司落實轉投資事業(含海外及大陸地區)之風險管理(包括防制洗錢、信用風險、市場風險及作業風險等)，並陳報金控公司必要資訊。

(3)資訊安全與個資保護：子公司系統更新之妥適性、網路及資安偵測防護、異常應變復原、客戶資料庫之資安管控、個資保護措施及個資外洩應變演練機制等。

(四)公司治理情形：

1.強化董事會及功能性委員會職能運作，如：董事會組織及職能、審計委員會、風險管理委員會與其他功能性委員會之設置與運作、董事會議事規則、決策程序與議事執行情形是否符合相關法規及公司內部規範(如：董事會召集程序、列席董事會之利害關係人對議案迴避情形、董事或其他人就董事會運作事項所提疑義之後續溝通處理情形、董事會議事錄相關發言摘要之正確性與完整性)、董事之忠實注意義務與責任、公

司治理主管及人員之設置等。

2.負責人兼職及分層負責之管理機制：建立負責人兼職行為之內部管理機制，已兼職者是否符合法令規定及內部規範，是否有除董事長及總經理外具首長權限者，內部分層負責機制是否權責相符。

3.大股東持股申報機制：建立瞭解大股東實質受益人之機制，包括：瞭解大股東是否確實依規定將實質受益人列入申報範圍、發現大股東未依規定辦理之處理程序。

4.利害關係人資料建檔及交易控管：

(1)建置利害關係人資料庫，是否確實建檔並定期確認利害關係人資料之正確性。

(2)利害關係人交易之作業控管機制及法規遵循情形，包括實質利害關係人交易及管理。

5.建立檢舉制度，並落實執行：檢舉制度是否具獨立性、有效性，並確實保障檢舉人權益。

6.所定內部聘用顧問之相關作業，是否包括：

(1)聘用顧問之遴選或續聘，有無綜合評估其資格條件、專業能力、負面新聞及任職其他機構之工作經驗與表現等事項。

(2)顧問執行業務之範圍是否具體明確及權責相符。

(3)顧問之報酬給付及考核評估機制，是否建立量化與質化評估標準。

(五)風險管理機制：

1.集團是否因應區域型風險建立妥適之風險管理機制(含對參股他國金融機構之管理)。

2.對國際金融情勢變化，是否預擬因應對策及建立集團風險管理機制，如：營運持續管理計畫、壓力測試等。

3.集團暴險(含海外及大陸地區)之管理機制，是否適時檢討整體暴險之風險胃納控管措施；是否建構風險預警及處置機制，並滾動調整監控指標等。

(六)共同行銷與資料共享：金控公司及其子公司共同行銷之安全維護措施及法令遵循情形、辦理金融機構間資料共享，是否依循個人資料保護法及金融機構間資料共享指引等規定辦理，建立妥適內部控制規範及資訊安全落實情形。

(七)內部稽核：

1.內部稽核之統籌規劃與督導執行，及人力妥適性暨單位獨立性。

2.內部稽核單位在查核對象及重點上已適度分工，確保已對全體子公司辦理有效之查核，建立並落實稽核督導機制(含海外分支機構之委外稽核)，並加強查核作業之執行與管理，確保查核品質及督促改善缺失。

3.採風險導向稽核制度子公司執行成效之確認、考核及督導。

4.對子公司之查核範圍涵蓋重點業務事項。

二、本國銀行

(一)防制洗錢、打擊資恐及反武器擴散落實情形(含國際金融業務分行)：

1.機構風險評估與內控架構：機構風險評估之完整性及合理性、整體內控架構之適當性及有效性、依風險基礎原則執行洗錢防制相關措施落實情形。

2.開戶審查措施與持續性審查及風險等級評估：實質受益人之辨識與身分之確認、開戶之地緣性及目的之合理性、法人客戶營運地點之確認及其真實性與合理性、瞭解高風險客戶之財富來源、辦理持續性審查時瞭解客戶所進行之交易與其身分背景、業務及開戶目的是否相符，及以風險導向方式瞭解客戶資金來源之合理性、客戶風險評估方法論之完整性與合理性暨採取與客戶風險相稱之審查(含與提供虛擬資產服務之事業或人員或經評為高風險之第三方支付業者建立業務關係及持續往來期間之強化措施)。

3.帳戶及交易之持續監控與對可疑交易警示之調查：交易監控型態及金額門檻設定之合理性、對於符合疑似洗錢態樣之交易或客戶及其交易對象疑似符合制裁名單與高風險外籍人士之檢核及查證情形、監控作業之獨立性及有效性暨國際間制裁相關管控措施執行情形、瞭解資金來源去向與客戶之身分背景、業務及交易目的是否相符及合理。

4.可疑交易申報流程：對疑似洗錢、資恐及資助武擴交易之處理作業(含申報、保密作業及資料保存)。

5.組織與人員：專責主管及人員之專業性及適足性、資源配置之適足性、教育訓練與行為管理、內部稽核單

位及會計師對防制洗錢、打擊資恐及反武器擴散制度有效性之獨立性測試品質及確信度。

(二)法令遵循制度及執行情形：

1.法令遵循制度及執行：法遵主管及法遵人員之資格條件及訓練、法令遵循風險管理及監督架構等法遵功能落實情形(含法遵諮詢溝通管道之建立、對法遵重大缺失或弊端之分析及提報、對新種業務或商品提供法遵意見、對法遵作業之考核)。

2.重要法令遵循情形：個人資料保護(含客戶資料之保管運用、資通安全機制等)、信託業務相關之消費者保護(含銷售商品適合度、受託辦理預售屋履約擔保機制之不動產開發信託及價金信託等)、財富管理業務（含接受客戶標準、客戶整體投資組合適配性、高風險集中度控管）、自有資本與風險性資產之計算(含不動產暴險計提方式採貸放比率法辦理者)、流動性風險管理、流動性壓力測試及緊急應變計畫相關政策與執行。

(三)海外暴險管理：

1.海外分支機構管理：如董事會監督管理、總行之督導管理暨對海外法遵之投入資源、防制洗錢作業、信用風險集中度、資產品質、徵授信及貸後管理暨備抵呆帳提列情形、作業風險、重大事件通報機制、與當地主管機關之溝通機制、法令遵循情形(含法遵主管及人員之獨立性暨適格性、海外分支機構遵守其所在地國家法令及其建立法令遵循風險自行評估及監控機制)、行員法治教育及品德操守考核及內部稽核查核品質暨追蹤缺失改善情形。

2.海外有價證券投資、新南向國家及大陸地區授信、投

資及資金拆存等業務之風險管理(含暴險額度控管與計算、授信業務之徵審作業及貸後管理、對所參股他國金融機構之管理)及對大陸地區金融相關事業管理機制。

3.對國際金融情勢變化採取相對應之風險控管措施。

(四)衍生性金融商品業務：

1.客戶信用風險控管制度：對於客戶避險與非避險額度之核給、控管及客戶風險集中度控管機制、徵提期初保證金及追繳保證金之內部作業制度及程序，如收取期初保證金之種類範圍(含得以有價證券抵繳之標的範圍、折扣比率與評價價值計算方式等法令遵循情形)。

2.衍生性金融商品及結構型商品銷售作業之妥適性：如認識客戶程序、專業投資人客戶認定程序及其覆核機制、商品風險分級、商品適合度評估、銷售人員資格、商品風險告知方式、揭露內容及紀錄留存之完整性與妥適性等。

3.衍生性金融商品評價及控管機制：如依連結標的資產種類及商品類別(高風險商品及非高風險商品)，建置高風險商品評價系統辦理商品報價及計算商品市價評估損益，並規範評價系統驗證程序；針對未建有評價系統並採詢價方式辦理之非高風險商品，訂定價格合理性檢核標準之內部作業程序。

(五)有價證券投資及交易室之風險控管：

1.有價證券投資控管：風險限額訂定及控管、停損限額訂定及執行暨避險策略之妥適性。

2.交易室內部控制管理：交易限額及授權之妥適性、前中後台內部控制機制(含股權投資人員利益衝突之防範)、交易室內部稽核及自行查核範圍之完整性與確實性。

(六)金融消費者保護作業(含身心障礙者權益保障措施執行情形)：

1.認識客戶作業、商品適合度評估、契約條款之公平合理性、銷售過程控管(含電話行銷、是否有不當搭售或勸誘客戶購買房貸壽險或以擴張信用方式投資金融商品情形)、新商品上架審查程序、業務人員酬金制度、消費爭議之處理機制、金融服務業公平待客原則(含信用卡違約金及循環利息之計收)、金融友善文化暨服務措施(含視障者網路銀行及行動應用程式 APP 等)之建立及執行情形(如董事會之作為、內部督導機制等)、個人資料保護(如涉及個人資料蒐集、處理及利用之安全維護措施、信用卡發卡機構將持卡人或申請人個人資料提供予第三人之資料保護、金融機構間資料共享指引之遵循情形及個資外洩應變演練機制)。

2.防範理財專員挪用客戶款項相關內部控管措施之落實執行情形：對帳單實務作業、對客戶電子信箱正確性及真實性之檢核、疑似挪用客戶款項態樣監控機制(包含疑似態樣之訂定、調查程序之執行)、薪酬制度與業績目標之關聯合理性及有無銷售未經本會核准之金融商品。

3.兼營保險經紀人保險代理人業務(含保險商品招攬作業、確認要保人親簽之控管機制、客戶購買保險商品之保費來源控管檢核機制等)。

4.以自動化工具提供證券投資顧問服務之執行情形：如對演算法運用之監管、瞭解客戶作業與建議投資組合、系統公平客觀執行、投資組合再平衡、專責委員會監督、告知客戶使用前注意事項。

(七)數位金融業務之辦理情形：

1.提供線上開戶及申辦相關服務，對使用者個資或交易安全機制、身分確認、異常交易監控機制、對警示帳戶數及遭偽冒開戶數之申報及監控管理、消費者資訊查詢【對於客戶資料所有權、消費者個資保護、顧客權益保障、爭議處理機制及第三方服務提供者(TSP 業者)管理方式之控管機制】。

2.電子銀行交易面安全設計(如：憑證簽章、一次性密碼、生物特徵、行動裝置儲存金鑰)、應用程式介面(API)安全管理(含開放銀行服務之客戶資料安全)、行動應用程式(APP)安全檢測。

3.使用電子簽名機制：身分核驗安全設計、簽名作業安全設計及電子簽名平臺之管理。

(八)公司治理制度運作落實情形：

1.董事會職能發揮：如董事會組織及職能、審計委員會及督導風險管理委員會之設置與運作、督導各項業務政策及管理機制情形與對陳報重大事件(如重大違反法令、重大暴險危及財業務狀況)之處置因應等職權行使之妥適性。

2.負責人兼職行為之內部管理機制、法令及內部規範遵循情形、公司治理主管及人員之設置。

3.利害關係人(含實質利害關係人)交易(含授信、不動

產、勞務或物品之採購及其他交易等)與管理作業控管機制(含實質利害關係人之自律性控管機制)、集團內或與主要股東、董監事等有實質關係者之交易決策、對象及價格是否異常或涉及利益衝突等法規遵循情形、費用支付之合理性。

4.與有控制能力股東之溝通聯繫機制(含溝通聯繫原則與管理規範、溝通議題、經理人陪同溝通程序、溝通作業控管流程與紀錄)。

5.檢舉制度之獨立性及有效性(含內、外部人員檢舉管道、檢舉人保護措施等內部作業程序及控管機制)。

(九)資通安全管理：防範主機系統(含容器)及程式異常控管措施(如系統架構重大變更之資安控管、完整測試、程式源碼檢視)、金融機構資訊作業韌性規範執行情形(含核心資訊系統中斷對銀行營運之衝擊評估及備援措施妥適性等)、個資檔案之儲存、傳遞與存取控管機制【含數位服務個人化(MyData)服務平台之資訊安全管控機制】、網路安全措施(如零信任、防火牆與入侵偵測、弱點掃描及滲透測試等資安防禦措施暨漏洞修補改善、物聯網設備管理、資安事件監控與通報處理)、供應鏈風險管理(如對供應商遴選之資訊安全評估、受委託廠商之監督、交付系統與元件之安全檢測、合約妥適性)、雲端服務資安控管(如：加密及金鑰管理、身分識別與存取、組態安全管理、稽核軌跡與監控)及雲端備份機制。

(十)業務操作制度：

1.銀行業防杜貸款詐騙之內部控制機制(含貸前審核流程、徵授信審查作業程序及貸後管理機制)、虛擬資產

保管業務之作業流程安全及風險管理是否依計畫書執行、營運持續管理機制及人員流動率情形。

2.委外作業之法令遵循情形：辨識及評估具重大性標準之妥適性、修正內規之充足性、依風險基礎方法管理之妥適性及有效性(含決策評估、受託機構盡職調查、風險評估、日常監督機制、客戶資訊保護、緊急應變及終止委託)、跨境委外及使用雲端服務管理之妥適性暨申報資料完整性等。

(十一)防制詐騙相關措施：

1.金融機構及提供虛擬資產服務之事業或人員防制詐欺犯罪危害應遵循事項辦法執行情形(含存款機構間及信用卡業務機構對異常存款帳戶與異常信用卡或交易之認定基準及對該等帳戶及信用卡持有人之持續審查措施、存款機構間及信用卡業務機構間之照會、資料交易紀錄保存及通報與帳戶帳號控管作業、聯防通報機制及圈存作業及剩餘款項之發還)。

2.疑似不法或顯屬異常交易預警指標建置與執行情形。

3.臨櫃關懷提問措施落實情形。

4.灰名單機制運作情形。

5.企業戶開立帳戶之審查作業。

6.高風險外籍人士開戶作業流程及帳戶控管情形。

7.警示帳戶觀察指標與督促改善機制之申報扣除數。

8.提供虛擬帳號服務之情形。

(十二)授信業務風險控管及法令遵循情形：如授信業務【如應收帳款融資承購業務、購屋貸款、餘屋貸款、土地(含工業區與閒置工業區土地)及建築貸款、專案融

資等聯貸案】徵信制度、風險評估分析、風險定價、授信審查、核貸程序、貸放後管理、禁止受理貸款代辦業務控管機制、辦理中小企業放款禁止授信回存、建商週轉金貸款移作建築使用之合理性、餘屋貸款資金用途與流向之控管及銀行法第 72 條之 2 之遵循情形。

(十三)內部稽核運作情形：

1.稽核單位之獨立性、稽核人力之妥適性、主管機關要求列入內稽查核事項之法遵情形、重大事件陳報及因應處理機制、對海外分支機構查核作業之落實情形(含總行對國外分支機構內部稽核作業管理)、督導缺失追蹤改善情形、採行風險導向者之執行成效。

2.稽核單位就防範理財專員挪用客戶款項，強化查核篩選原則、頻率及查核重點(含理專與客戶往來關係及理專與其關聯戶往來情形)。

3.兼營保險經紀人保險代理人業務之查核作業落實情形。

(十四)轉投資事業管理：如督導子公司訂定及落實作業與風險控管規章(含利害關係人交易相關控管機制)、實際營運項目與原申請設立營運計畫之一致性暨建立子公司重大業務計畫、交易、業務經營績效及暴險情形等之定期陳報機制與相應之管理措施，及銀行所轄創業投資相關事業，對於辦理創業投資基金籌集業務之管理機制。

(十五)銀行兼營債券、受益證券、資產基礎證券承銷及自行買賣業務：辦理本項業務之額度控管、承銷所屬同一集團關係企業發行債券之控管程序，及辦理本

業務之風險管理及商品適合度制度。

(十六)兼營電子支付業務操作管理(如身分驗證及交易限額控管機制)。

三、外國銀行在臺分行

(一)防制洗錢、打擊資恐及反武器擴散落實情形(含國際金融業務分行)：

1.機構風險評估與內控架構：機構風險評估之完整性及合理性、整體內控架構之適當性及有效性、依風險基礎原則執行洗錢防制相關措施落實情形。

2.開戶審查措施與持續性審查及風險等級評估：實質受益人之辨識與身分之確認、開戶之地緣性及目的之合理性、法人客戶營運地點之確認及其真實性與合理性、瞭解高風險客戶之財富來源、辦理持續性審查時瞭解客戶所進行之交易與其身分背景、業務及開戶目的是否相符，及以風險導向方式瞭解客戶資金來源之合理性、客戶風險評估方法論之完整性與合理性暨採取與客戶風險相稱之審查(含與提供虛擬資產服務之事業或人員或經評為高風險之第三方支付業者建立業務關係及持續往來期間之強化措施)。

3.帳戶及交易之持續監控與對可疑交易警示之調查：交易監控型態及金額門檻設定之合理性、對於符合疑似洗錢態樣之交易或客戶及其交易對象疑似符合制裁名單與高風險外籍人士之檢核及查證情形、監控作業之獨立性及有效性暨國際間制裁相關管控措施執行情形、瞭解資金來源去向與客戶之身分背景、業務及交易目的是否相符及合理。

4.可疑交易申報流程：對疑似洗錢、資恐及資助武擴交易之處理作業(含申報、保密作業及資料保存)。

5.組織與人員：專責主管及人員之專業性及適足性、資源配置之適足性、教育訓練與行為管理、內部稽核單

位及會計師對防制洗錢、打擊資恐及反武器擴散制度有效性之獨立性測試品質及確信度。

(二)銀行提供境外衍生性金融商品資訊及諮詢服務之辦理情形：如提供服務對象、商品範圍、服務內容、報價情形、分潤收入之法令遵循情形。

(三)財富管理業務：如接受客戶標準、瞭解客戶程序、客戶整體投資組合適配性、高風險集中度控管、商品審查程序、銷售過程控管、業務人員酬金制度、爭議處理機制。

(四)衍生性金融商品業務：

1.客戶信用風險控管制。

2.衍生性金融商品與結構型商品銷售作業之妥適性(含專業投資人客戶認定程序及其覆核機制)。

3.衍生性金融商品評價及控管機制。

(五)法令遵循制度及執行情形：如法遵人員之教育訓練、法遵功能之落實情形(含法遵諮詢溝通系統之建置、對法遵重大缺失或弊端之分析及提報、對新種業務或商品提供法遵意見、對法遵自行評估作業之考核)、資安作業之執行。

(六)法定限額遵循情形及資金運用之風險管理：

1.對大陸地區授信限額之控管。

2.存款總餘額核算基準之控管計算機制。

3.授信及投資之資金來源及運用、資產負債期限配置與流動性風險控管。

(七)作業委託他人事項之管理：辨識及評估具重大性標準之妥適性、修正內規之充足性、依風險基礎方法管理

之妥適性及有效性(含決策評估、受託機構盡職調查、風險評估、日常監督機制、客戶資訊保護、緊急應變及終止委託)、跨境委外及使用雲端服務管理之妥適性、申報資料完整性、專責單位與總機構或經其授權之區域總部間之權責分工妥適性等。

(八)個人資料保護及資通安全管理。

(九)銀行兼營債券、受益證券、資產基礎證券承銷及自行買賣業務：辦理本項業務之額度控管、承銷所屬同一集團關係企業發行債券之控管程序，及辦理本業務之風險管理及商品適合度制度。

(十)專案融資之管理情形：如風險評估分析、強化債權確保、貸後管理機制。

(十一)防範理專挪用客戶款項相關內部控管措施之落實執行情形：如對帳單作業之控管機制、疑似理專挪用客戶款項態樣之監控機制(含疑似態樣之訂定、調查程序之執行)。

(十二)使用電子簽名機制：身分核驗安全設計、簽名作業安全設計及電子簽名平臺之管理。

四、信用合作社

(一)防制洗錢、打擊資恐及反武器擴散落實情形：

1.機構風險評估與內控架構：機構風險評估之完整性及合理性、整體內控架構之適當性及有效性、依風險基礎原則執行防制洗錢相關措施落實情形。

2.客戶審查措施及風險等級評估：實質受益人之辨識與身分之確認、客戶風險評估方法論及客戶審查內容之完整性與合理性(與風險相稱)。

3.帳戶及交易之持續監控：交易監控型態及金額門檻設定之合理性、對於符合疑似洗錢態樣之交易或客戶及其交易對象疑似符合制裁名單或高風險外籍人士之檢核及查證情形、監控作業之獨立性及有效性。

4.可疑交易申報流程：對疑似洗錢、資恐及資助武擴交易之處理作業(含申報、保密作業及資料保存)。

5.組織與人員：專責主管及人員之專業性及適足性、資源配置之適足性、教育訓練、內部稽核單位及會計師對防制洗錢、打擊資恐及反武器擴散制度有效性之獨立性測試品質及確信度。

(二)授信風險管理：

1.授信審議委員會運作情形。

2.同一關係關聯戶授信及大額授信之風險管理。

3.不動產授信風險控管(含利率定價、貸後管理等)、法規遵循情形及申報作業執行情形：如建築貸款、購置住宅貸款、房屋修繕貸款、餘屋貸款、購地貸款(含工業區閒置土地)、建商週轉金貸款移作建築使用之合理性、餘屋貸款資金用途與流向之控管等。

4.負責人或職員暨其利害關係人與客戶之異常資金往來(含以他人名義辦理貸款)。

5.辦理中小企業放款禁止授信回存情形。

(三)金融消費者保護作業：

1.契約條款之公平合理性、業務人員酬金制度、消費爭議之處理機制、金融服務業公平待客原則、金融友善文化暨服務措施(含身心障礙者權益保護)之建立及執行情形(如理事會之作為、內部督導機制等)、消費者貸款費用之告知與揭露及利率依約調整作業情形。

2.個人資料保護：客戶資料之蒐集、處理及利用之安全維護措施、金融機構間資料共享指引之遵循情形、個資事故應變機制、個資保護與管理之認知宣導及教育訓練。

3.與他業合作推廣金融商品或保險業務相關內部控管措施之落實執行情形：如認識客戶作業、商品適合度評估、銷售過程控管、推廣保險業務涉授信及存款端之控管機制、建立防範房貸搭售金融商品或於貸款過程中不當勸誘之控管機制。

4 防範員工挪用客戶款項相關內部控管措施之落實執行情形：如防範員工與客戶私下資金往來及代客戶辦理交易之控管機制、主管卡(密碼)使用及控管機制、網路銀行交易之控管機制、對帳單控管機制。

(四)防制詐騙相關措施

1.金融機構及提供虛擬資產服務之事業或人員防制詐欺犯罪危害應遵循事項辦法執行情形(含存款機構

間及信用卡業務機構對異常存款帳戶與異常信用卡或交易之認定基準及對該等帳戶及信用卡持有人之持續審查措施、存款機構間及信用卡業務機構間之照會、資料交易紀錄保存及通報與帳戶帳號控管作業、聯防通報機制及圈存作業及剩餘款項之發還)。

2.疑似不法或顯屬異常交易預警指標建置與執行情形。

3.臨櫃關懷提問措施落實情形。

4.灰名單機制運作情形。

5.企業戶開立帳戶之審查作業。

6.高風險外籍人士開戶作業流程及帳戶控管情形。

(五)流動性控管措施：如訂定流動性風險管理政策、建置適當之資訊系統以衡量及監控流動性風險、定期揭露流動性風險管理之質化及量化資訊、建立並定期檢視流動性風險限額及警示標準之妥適性、定期檢視大額資金來源與運用及其集中度風險、訂定緊急應變計畫及緊急取得資金之處理流程。

(六)資通安全管理：如資訊安全之人力與訓練及管理作業、網路金融業務(含線上金融服務)之系統安控、交易安全設計、網路安全措施(如防火牆與入侵偵測、弱點掃描、電子郵件社交工程演練及滲透測試等資安防禦措施暨漏洞修補、物聯網設備管理、資安事件監控與通報處理)、應用程式介面(API)安全管理、個資檔案之儲存、傳遞與存取控管機制、資安情資之蒐集與評估處理程序，以及資通系統與服務供應鏈風險管理(如對受託廠商監督、交付系統及元件安全檢測、合約妥適性)。

(七)社務治理制度運作落實情形：

1.理監事會職能發揮：如理監事會組織及職能、督導各項業務政策及管理機制等職權行使之妥適性。

2.利害關係人授信與交易之作業控管機制及法規遵循情形。

3.建立檢舉制度，並落實執行：如檢舉制度具獨立性、有效性，並確實保障檢舉人權益。

(八)法令遵循及風險管理制度實施情形：

1.法令規章適時更新、法令遵循教育訓練及法令遵循報告內容之妥適性等。

2.風險管理委員會設置及運作情形。

(九)內部稽核運作情形：如稽核單位以獨立超然之精神，執行稽核業務。

五、票券金融公司

(一)防制洗錢、打擊資恐及反武器擴散落實情形：機構風險評估與內控架構、客戶審查措施及風險等級評估、帳戶及交易之持續監控、可疑交易申報流程、教育訓練、內部稽核單位及會計師有效性之獨立性測試品質及確信度。

(二)公司治理及營運持續管理機制：如保障股東權益、強化董事職能、發揮監察人功能、尊重利害關係人權益(內部檢舉人保護措施)、提升資訊透明度、營運持續管理機制之建立及執行情形、與有控制能力股東溝通聯繫原則之遵循情形。

(三)對利害關係人(含實質利害關係人)辦理授信或授信以外交易之內部控制、法規遵循等機制落實情形。

(四)辦理永續發展票券執行情形(含「辦理永續發展票券自律規範」法令遵循情形)。

(五)對免保證商業本票業務風險控管及自律規範遵循情形(含對個別發行人及同一產業之免保票承銷限額訂定之妥適性、發行人免保證商業本票發行餘額占該發行人淨值倍數之控管情形，及公司持有同一關係人及同一集團之免保證商業本票控管情形)。

(六)辦理保證及背書作業：

1.對產業(如不動產業等)保證業務之集中度及相關風險控管措施。

2.依「中央銀行對金融機構辦理不動產抵押貸款業務規定」所訂之內部控制與內部稽核機制及執行情形。

3.建商週轉金貸款移作建築使用之合理性、餘屋貸款

資金用途與流向之控管情形。

(七)辦理保證及承銷商業本票業務之利率定價作業情形(含是否考量市場利率、本身資金成本、營運成本、預期風險損失及合理利潤等因素)。

(八)票債券投資及持有部位之風險控管機制及執行情形(如投資評估、價格檢核、因應利率波動之風險管理、投資部位及其信用評級之控管機制)及辦理外幣債券經紀、自營及投資業務之外幣風險上限遵循情形。

(九)流動性風險管理機制及執行情形(含「票券金融公司流動性風險管理自律規範」法令遵循情形)。

(十)資通安全管理之執行情形：

1.資訊系統防護：資訊系統弱點掃描及滲透測試等辦理情形暨漏洞修補改善措施。

2.網路安全防護：公司網站之程式版本控管及防火牆機制、資安監控與事件通報應變機制。

3.個人資料保護：個人資料檔案儲存、處理及傳遞之安全維護措施。

六、證券商

(一)防制洗錢、打擊資恐及反武器擴散落實情形(含國際證券業務分公司)：

1.機構風險評估與內控架構：機構風險評估之完整性及合理性、整體內控架構之適當性及有效性、依風險基礎原則執行洗錢防制相關措施落實情形。

2.客戶審查措施及風險等級評估：實質受益人之辨識與身分之確認、客戶風險評估方法論及客戶審查內容之完整性與合理性(與風險相稱)。

3.帳戶及交易之持續監控：交易監控指標設定之合理性、對於符合疑似洗錢表徵交易或客戶及其交易對象疑似符合制裁名單之檢核及查證情形、監控作業之獨立性以及時效性。

4.可疑交易申報流程：對疑似洗錢、資恐及資助武擴交易之處理作業(含申報、保密作業及資料保存)。

5.組織與人員：專責主管及人員之專業性及適足性、資源配置之適足性、教育訓練、內部稽核單位對防制洗錢、打擊資恐及反武器擴散制度有效性之獨立性測試品質及確信度。

(二)法令遵循制度執行情形：建立法遵風險管理架構、獨立法令遵循之權責、落實法令遵循效能報告及監督、確認各項作業及管理規章適時更新、法令遵循自行評估執行情形。

(三)受託買賣國內有價證券之經紀業務及辦理不限用途款項借貸業務：開戶、KYC 程序及徵信與額度管理、受理客戶委託下單及交易對帳單送交、受託買賣錯帳與

更正帳號及違約處理、內部人員利益衝突檢核等作業是否妥適。

(四)財富管理業務：辦理開戶及銷售商品是否建立並落實內部控制制度；以複委託、財富管理信託或於營業處所自行買賣等方式提供客戶之服務或商品範圍、客戶是否符合相關資格條件、證券商是否已善盡資訊揭露與申報義務及建立商品適合度制度及商品審查標準等；辦理信託業務是否依信託契約之約定事項為受益人之利益或特定目的之管理、運用該有價證券及辦理信託利益分配。

(五)受託買賣外國有價證券業務：投資人屬性分級管理、KYC 作業、專業投資人客戶認定程序及其覆核機制、受託投資之標的按投資人區隔、接受委託人以定期定額方式委託買進外國有價證券及接受專業投資人委託買賣外國虛擬資產 ETF，是否就標的風險及流動性訂定標的選定標準、成交價格計算方式和手續費率是否依所訂收費標準計收等，及相關資訊揭露是否妥適、提供銀行業者通路獎勵或禮券、複委託業務資產保管等之管理機制。

(六)辦理衍生性金融商品業務：證券商辦理衍生性商品業務與客戶訂立契約之程序、商品適合度制度(KYC 及 KYP 作業)、專業投資人客戶認定程序及其覆核機制、行銷過程控制、客戶申訴處理、解約及結算作業、商品評價及報價、風險管理、避險操作情形等。

(七)數位金融業務辦理情形：提供線上開戶及申辦相關服務(如申請 API 及 DMA 電子下單等)，對使用者個資、身分確認、異常交易之控管機制。

(八)風險管理機制：對全球政經情勢變化所產生市場風險是否擬定因應對策；是否訂定持續營運管理規範並落實執行；審視風險管理機制運作是否妥適，如董事會與經營層監督管理、風險管理委員會、風險之衡量(模型驗證、敏感度分析及壓力測試等)、限額管理、停損管理及例外處理機制等。

(九)海外子公司之監督與管理：訂定對子公司必要之控制作業規範、督促其子公司建立內部控制制度情形及客戶投資國內有價證券是否符合國內法令(包括對客戶KYC之查核作業程序、客戶資金未源自我國或大陸地區、客戶未具陸籍身分等)之審核機制、對其子公司之監督與管理(包括經營管理、財務、業務、法令遵循及內部稽核管理)應含括之控制作業項目。

(十)證券商作業委託他人處理：是否應依風險基礎方法評估委外風險、訂定委外內部作業規範及委外契約應載明相關事項。

(十一)公司治理落實情形：證券商落實公司治理，強化董事職能之辦理情形，如是否建置內部檢舉制度與落實情形、設置公司治理主管及應遵循事項辦理情形及獨立董事不得連任逾3屆等，與關係企業間人員、財務及費用核銷之管理機制。

(十二)金融消費者保護作業辦理情形：如金融友善文化暨服務措施(含身心障礙者權益保護)之建立及執行情形(如董事會之作為、內部督導機制等)、防範金融投資詐騙(員工教育宣導、設置反詐騙專區、持續關懷客戶)、基金銷售之KYC與KYP執行情形、商品適合度評估、風險揭露、業務人員酬金制度、是否有勸

誘客戶以擴張信用方式投資金融商品；收取手續費及收受佣金是否充分揭露，業務獎金發放是否妥適、消費者爭議之處理情形，及 MyData 平臺與個人資料蒐集、處理及利用是否妥適、辦理金融機構間資料共享，是否依循個人資料保護法及金融機構間資料共享指引等規定辦理，建立妥適內部控制規範。

(十三)公平待客原則：證券商辦理金融服務業公平待客原則之落實情形。

七、證券投資信託公司

(一)防制洗錢、打擊資恐及反武器擴散落實情形：

1.機構風險評估與內控架構：機構風險評估之完整性及合理性、整體內控架構之適當性及有效性、依風險基礎原則執行洗錢防制相關措施落實情形。

2.客戶審查措施及風險等級評估：實質受益人之辨識、客戶風險評估方法論及客戶審查內容之完整性與合理性(與風險相稱)。

3.帳戶及交易之持續監控：交易監控型態及金額門檻設定之合理性、對於符合疑似洗錢態樣交易或客戶及其交易對象疑似符合制裁名單之檢核及查證情形、監控作業之獨立性以及有效性。

4.可疑交易申報流程：對疑似洗錢、資恐及資助武擴交易之處理作業(含申報、保密作業及資料保存)。

5.組織與人員：專責主管及人員之專業性及適足性、教育訓練、內部稽核單位對防制洗錢、打擊資恐及反武器擴散制度有效性之獨立性測試。

(二)境內外基金資訊揭露、KYC 及 KYP 之執行情形：

1.境內外基金配息揭露、非投資等級債券基金風險揭露、基金投資警語、目標到期債券基金之廣告及行銷文件、辦理客戶基金適合度評估、基金銷售業務之認識客戶(KYC)及認識產品(KYP)之執行。

2.境外基金投資人須知揭露之正確性，總代理人代理境外基金之財報資訊、應申請核准或申報等公告事項之辦理情形：

(1)境外基金投資人須知揭露是否與公會所訂範本相

符，且依範本列示相關投資風險警語，並以粗體字揭露主要風險或警語、及投資人須知是否與公開說明書及 Fund Factsheet 相符；ESG 相關主題境外基金之投資人須知應載明事項、投資組合及銷售文件向投資人說明事項有無誤導投資人疑慮等。

(2)總代理人所代理之境外基金年度及半年度財務報告併同其中文簡譯本之公告時間、境外基金應公告及申報事項是否符合境外基金管理辦法等相關規定，及公告財報內容是否與該檔境外基金相符。

3.對防範金融投資詐騙(員工教育宣導、反詐騙提醒)及金融消費者之保護措施。

(三)投信基金及全權委託投資帳戶(含政府基金代操)之利益衝突防範及投資流程控管：

1.經理人及其配偶、未成年子女及利用他人名義買賣與投信基金及全權委託投資帳戶所持有相同標的之情形。

2.投信基金及全權委託投資帳戶(含政府基金代操)之投資或交易，其分析、決定、執行及檢討之內控制度規範及其執行情形。

(四)ETF(含期貨 ETF)之募集銷售、廣告行銷、配息政策(含收益平準金使用原則)、配息時間、配息組成占比揭露、折溢價管理、追蹤指數及強化 ETF 資訊揭露之辦理情形。

(五)發行環境、社會與治理(ESG)相關主題基金之資訊揭露事項情形：包括新成立基金之發行計畫及公開說明書

等書件應揭露內容，及已成立基金應改善事項。

(六)資通安全管理之執行情形：

1.個人資料保護：如個人資料檔案儲存、處理及傳遞之安全維護措施及金融機構間資料共享辦理情形。

2.對金融資安資訊分享與分析中心(F-ISAC)所公布之資安情資或警訊來源之處理情形。

(七)對銷售機構之管理查核及支付通路報酬之情形：對銷售機構之遴選與訪查作業、選派教育訓練參訓人員之參訓標準、教育訓練搭配旅遊之適當性及基金相關專業課程是否具一定比重、訂定通路報酬之事前評估與事後審核機制並落實辦理、及通路報酬支付之合理性(含手續費後收型與前收型基金之通路報酬是否具合理性，有無以通路報酬誘導銷售特定類型基金等)。

(八)公司治理、法令遵循制度實施情形及營運持續管理機制執行情形：如強化董事職能、利害關係人交易及對內部檢舉人保護措施、聘任顧問之服務內容是否有變相執行內部職務之行為、執行「機構投資人盡職治理守則」是否符合自訂內部控制規範、是否訂定持續營運管理規範並落實執行，及法令遵循制度設計與運作情形。

(九)以自動化工具提供證券投資顧問服務之執行情形：如對演算法運用之監管、瞭解客戶作業與建議投資組合、系統公平客觀執行、投資組合再平衡、專責委員會監督、告知客戶使用前注意事項。

八、壽險公司

(一)防制洗錢、打擊資恐及反武器擴散落實情形(含國際保險業務分公司)：

1.機構風險評估與內控架構：機構風險評估之完整性及合理性、整體內控架構之適當性及有效性、依風險基礎原則執行洗錢防制相關措施落實情形。

2.客戶審查措施及風險等級評估：實質受益人之辨識與身分之確認、客戶風險評估方法論及客戶審查內容之完整性與合理性(與風險相稱)。

3.帳戶及交易之持續監控：交易監控型態及金額門檻設定之合理性、對於符合疑似洗錢態樣之交易或客戶及其交易對象疑似符合制裁名單之檢核及查證情形、監控作業之獨立性及有效性。

4.可疑交易申報流程：對疑似洗錢、資恐及資助武擴交易之處理作業(含申報、保密作業及資料保存)。

5.組織與人員：專責主管及人員之專業性及適足性、資源配置之適足性、教育訓練、內部稽核單位及會計師對防制洗錢、打擊資恐及反武器擴散制度有效性之獨立性測試品質及確信度。

(二)法令遵循制度執行情形：

1.法遵單位對法令規章傳達與溝通之執行情形。

2.對新種服務、商品或進行特定或重大資金運用前之出具法遵意見之情形。

3.對各單位法令遵循重大缺失或弊端之處理程序及落實情形。

4.法令遵循之教育訓練、自行評估作業落實情形及對

海外分支機構法遵之督導與查核情形。

5.辦理金融資產重分類相關特別盈餘公積之提列及迴轉之法令遵循情形。

(三)金融消費者保護作業：

1.保險消費者訂約前資訊保障執行情形(如：審閱期間之提供、契約重要內容及風險之揭露)。

2.保全(含投資型保險商品連結標的之異動申請)、理賠、申訴管理制度之建立與執行。

3.外幣保單、投資型保險及房貸壽險商品招攬方式妥適性。

4.對身心障礙者權益之維護(如：對於身心障礙者之招攬、核保作業是否無歧視性對待、核保評估程序及相關人員教育訓練之建立與執行)。

5.金融友善措施及金融服務業公平待客原則之推動情形。

(四)保險商品之行銷及管理情形：

1.對所屬業務員管理情形，如：督導業務員確實填寫招攬報告書及不得勸誘客戶解舊買新、防範保險業務員挪用及重大偶發通報之落實、侵占保戶款項內控作業之建立及執行。

2.利率變動型商品宣告利率運作方式、區隔資產管理及佣金結構制度之合理性。

3.保險商品管理小組會議之召開及檢視商品於法令遵循、定價合理性及商品銷售額度控管等執行情形。

4.保險商品銷售風險控管機制，及向董事會提報商品銷售後對公司財務、業務及清償能力影響之整體評

估報告之辦理情形。

5.與保經代業務往來之管理(包括電話行銷業務、防範保經代業務員不當勸誘客戶解舊買新、通路獎勵措施制度之合理性)。

6.分紅保單之管理(包括商品區隔帳戶管理、商品設計及銷售後管理、資訊揭露及銷售行為規範、相關人員職責、招攬人員教育訓練)。

(五)公司治理情形：如董事會及風險管理委員會等功能性委員會之職能發揮、與大股東溝通機制、利害關係人交易之法令遵循及控管程序、檢舉制度之建立與執行情形、與關係企業間人員、資產及財務之管理機制。

(六)國外投資之辦理情形：

1.投資國外主次順位公司債、次順位金融債券、國際板債券等有價證券之投資條件、風險管理及法令遵循情形。

2.對國外保險相關事業及大陸參股保險相關機構之投資前、後管理機制及法令遵循情形(包括被投資事業有違反防制洗錢及打擊資恐重大事件、內控不良之重大舞弊案件、重大變更向主管機關申請投資計畫及其他足以影響其信譽、正常營運之重大事件處理機制等)。

3.對國際政經情勢變化所發生之風險事件，及就海外及大陸地區授信或投資涉當地政府政策或受政策高度補助產業之風險控管機制。

4.國外資產之保管情形、保管機構資格條件及保管合約之適法性。

5.資金全權委託投資之作業程序及管理制度。

6.國外投資限額之控管作業。

7.設立或投資國外籌資事業之法令遵循情形。

(七)國內有價證券投資內部控制制度之執行情形，如：投資政策與程序、投資後之檢討機制、前台、中台及後台作業權責之控管、資金全權委託投資之作業程序及管理制度、股權投資人員之利益衝突防範及其辦公處所資訊與通訊設備使用管理。

(八)不動產投資之辦理情形，如：不動產投資之投資程序及內部控制機制、即時利用並有收益規定之遵循情形、帳列投資性不動產後續衡量之處理程序。

(九)辦理專案運用及投資私募基金、創業投資事業之風險管理、內部控制機制及法令遵循情形。

(十)自我風險及清償能力評估機制(ORSA)之辦理情形：

1.定期執行及檢視 ORSA 機制之有效及合理性，並採取適當策略及落實情形。

2.風險管理機制之落實及資本適足率之計提情形，如：風險管理實務守則執行情形、自有資本分層架構之劃分、投資國外保險相關事業屬關係人者之自有資本扣除情形、投資國內外 REITs 及債券之風險資本計提情形。

3.持有之國外籌資事業於國外發行具資本性質債券之法令遵循情形。

(十一)數位金融業務之辦理情形：辦理電子商務之法令遵循情形、行動應用程式(APP)開發及發布(含定期安全檢測)之管理機制、電子保單作業、行動投保及網

路投保業務之保戶身分驗證(含行動身分識別)、投保意願確認、核保及通報等作業控管機制。

(十二)資通安全及個人資料管理機制：

1.個人資料蒐集、處理及利用之法令遵循、管理機制項目及安全維護措施(包括對作業委外機構落實保戶個資保護之監督管理、辦理金融機構間資料共享，是否依循個人資料保護法及金融機構間資料共享指引等規定辦理，建立妥適內部控制規範及資訊安全落實情形)。

2.營運持續管理機制、資訊系統安全控管、個資外洩應變演練機制、應用程式介面(API)安全管理、資通系統與服務供應鏈風險管理(如對受託廠商監督、交付系統及元件安全檢測、合約妥適性)。

3.雲端服務資安控管(如：加密及金鑰管理、身分識別與存取、組態安全管理、稽核軌跡與監控)及雲端備份機制。

九、產險公司

(一)防制洗錢、打擊資恐及反武器擴散落實情形(含國際保險業務分公司)：防制洗錢及打擊資恐內控制度、風險評估及降低風險措施之執行、確認客戶身分、姓名檢核、帳戶與交易之持續監控、資訊系統建置整合、疑似洗錢交易檢核與申報及洗錢防制教育訓練。

(二)法令遵循制度執行情形：

1.法遵單位對法令規章傳達與溝通之執行情形。

2.對新種服務、商品或進行特定或重大資金運用前之出具法遵意見之情形。

3.對各單位法令遵循重大缺失或弊端之處理程序及落實情形。

4.法令遵循之教育訓練、自行評估作業落實情形及對海外分支機構法遵之督導與查核情形。

(三)金融消費者保護作業：如客戶投保保險商品之招攬與核保作業程序之建立，及身心障礙者投保權利之維護(例如：對於身心障礙者之招攬、核保作業是否無歧視性對待、核保評估程序及相關人員教育訓練之建立與執行)、金融友善措施及金融服務業公平待客原則之推動情形。

(四)保險商品之開發設計、行銷管理及費率檢測調整情形：

1.保險商品評議小組及保險商品管理小組辦理商品設計之評估、銷售前之查核作業、銷售後之檢視追蹤(包含商品定價及費率調整合理性)，及向董事會提報商品銷售後對公司財務、業務及清償能力影響之整體評估報告等作業之執行情形。

2.商業火災保險、自用小客車汽車車體損失保險及第三人責任保險之費率檢測及調整執行情形。

3.商業火災保險商品對各通路招攬佣金訂定與執行管理。

4.與保經代業務往來之管理。

(五)保險招攬、收費、核保及理賠處理作業之執行情形：如汽車保險、火災保險、傷害及健康保險之保費核算、承保評估及理賠處理之辦理情形，及授權代收現金保費之控管情形。

(六)資金運用風險管理機制：有價證券投資與國外投資之法令遵循、交易控管機制及風險控管措施、股權投資人員之利益衝突防範機制及其辦公處所資訊與通訊設備使用管理機制之建立與執行、資金全權委託投資之作業程序及管理制度。

(七)自我風險及清償能力評估機制(ORSA)之辦理情形：

1.定期執行及檢視 ORSA 機制之有效及合理性，並採取適當策略及落實情形。

2.風險管理機制之落實及資本適足率之計提情形，如：風險管理實務守則執行情形、自有資本分層架構之劃分、投資國外保險相關事業屬關係人者之自有資本扣除情形、投資國內外 REITs 及債券之風險資本計提情形。

(八)數位金融業務之辦理情形：辦理電子商務之法令遵循情形、行動應用程式(APP)開發及發布(含定期安全檢測)之管理機制、電子保單作業、行動投保及網路投保業務之保戶身分驗證、投保意願確認、核保及通報等

作業控管機制。

(九)資通安全及個人資料管理機制：

1.個人資料蒐集、處理及利用之法令遵循、管理機制項目及安全維護措施(包括對作業委外機構落實保戶個資保護之監督管理、辦理金融機構間資料共享，是否依循個人資料保護法及金融機構間資料共享指引等規定辦理，建立妥適內部控制規範及資訊安全落實情形)。

2.營運持續管理機制、資訊系統安全控管、個資外洩應變演練機制、應用程式介面(API)安全管理、資通系統與服務供應鏈風險管理(如對受託廠商監督、交付系統及元件安全檢測、合約妥適性)。

3.雲端服務資安控管(如：加密及金鑰管理、身分識別與存取、組態安全管理、稽核軌跡與監控)及雲端備份機制。

(十)公司治理情形：如董事會及風險管理委員會等功能性委員會之職能發揮、與大股東溝通機制、利害關係人交易之法令遵循及控管程序、檢舉制度之建立與執行情形、與關係企業間人員、資產及財務之管理機制。

(十一)再保險分出業務之管理機制：取得再保險人確認認受文件及再保險契約文件之管理機制、對再保險人及保險經紀人所委任之國外保險經紀人等之適格條件、再保險安排及原保險單承保條件之檢核機制。

十、提供虛擬資產服務之事業或人員 (VASP)

(一)防制洗錢、打擊資恐及反武器擴散落實情形：

1.機構風險評估與內控架構：機構風險評估之完整性及合理性、整體內控架構之適當性及有效性、依風險基礎方法執行洗錢防制相關措施落實情形。

2.客戶審查措施及風險等級評估：客戶風險評估方法論之合理性，暨採取與客戶風險相稱之審查、辨識實質受益人。

3.帳戶及交易之持續監控：依風險基礎方法，建立之交易監控政策與程序，及設定警示交易金額門檻等參數之合理性、對於符合疑似洗錢態樣之交易或客戶及其交易對象疑似符合制裁名單(含錢包地址)與高風險外籍人士之檢核及查證情形、監控作業之獨立性及有效性暨國際間制裁相關管控措施。

4.可疑交易申報流程：對疑似洗錢、資恐及資助武擴交易之處理作業(含申報、保密作業及資料保存)。

5.組織與人員：專責人員之專業性及適足性、資源配置之適足性、教育訓練、內部稽核單位對控制措施有效性之獨立性測試品質。

(二)資訊安全管理制度：建置與所營事業規模與性質相符之穩定與安全之資訊系統，並採取適當措施與程序以確保資料及其傳輸、交換或處理之可得性、正確性、隱密性及安全性。

(三)消費者保護：

1.虛擬資產保管商為客戶保管之資產，與其自有財產，應分別獨立;收受客戶之虛擬資產，應與其自有之虛

擬資產分離保管，不得與客戶約定與其自有之虛擬資產混合保管。

2. VASP 保管客戶虛擬資產，於冷熱錢包之部位比例。

3.應將客戶留存之法定貨幣交付信託或取得銀行十足之履約保證。

4.為客戶辦理虛擬資產服務相關紀錄，自服務關係終止時起，至少保存五年。但遇有爭議者，應保存至爭議消除為止。

5.應建立客戶申訴處理程序，並公平及迅速處理爭議。

(四)交易平台管理：虛擬資產交易平台商所訂虛擬資產上下架之審查標準及審查程序，及建置防止市場交易不公正之機制及偵測價量異常警示等措施。

(五)防制詐騙措施：

1.對疑似涉及詐欺犯罪之異常虛擬資產帳號，應強化確認客戶身分，並得採取對客戶身分持續審查、暫停存入或提領、匯出虛擬資產或款項、暫停全部或部分交易功能、拒絕建立業務關係或提供服務等控管措施，並得向司法警察機關通報。

2.疑似涉及詐欺犯罪之異常虛擬資產帳號或警示虛擬資產帳號、銀行通報之虛擬存款帳號、警政署告誡名單、165 存款帳號、165 錢包地址及自建黑名單與黑錢包地址等資料之審查、管控、通報及法令遵循情形。

3.防制詐欺犯罪「同業聯防」通報辦理情形。

4.防制詐欺犯罪「異業聯防」通報辦理情形。

5.客戶剩餘款項或虛擬資產之發還管理政策、處置及結清程序，與實際執行情形。

十一、專營電子支付機構

(一) 防制洗錢、打擊資恐及反武器擴散落實情形：

1.確認客戶身分措施及持續監控機制，以風險基礎方法決定其執行強度。

2.依國家風險評估結果訂定疑似洗錢或資恐交易態樣表徵，瞭解高威脅形態犯罪態樣，並與業務連結，訂定相對應之控管措施。

(二)業務管理：

1.與銷售遞延性商品或服務之特約機構簽約時，應於契約中約定依相關規定辦理履約保證或交付信託，並揭露該履約保證或交付信託資訊予使用者知悉。

2.提供使用者事先約定不特定金額代理收付實質交易款項業務，所訂特約機構交易安全機制及交易爭議處理流程確認程序之妥適性。

3.辦理代理收付實質交易款項業務，特約機構以最終收款方為原則，非屬最終收款方之特約機構如為外送平臺業者、計程車客運服務平臺業者及停車服務平臺業者時，應訂定妥適之遴選原則。

(三)防制詐騙相關措施：

1.金融機構及提供虛擬資產服務之事業或人員防制詐欺犯罪危害應遵循事項辦法執行情形。

2.所訂疑似不法或顯屬異常交易之電子支付帳戶及記名式儲值卡之認定及相關內部作業準則之妥適性。

3.接獲前一受款機構傳真聯防機制通報單時，應立即查詢受款電支帳戶交易，並將移轉資料傳真通報下一受款機構之通報窗口。

4.經確認通報原因屬詐財案件，且該帳戶中尚有被害人匯(轉)入之款項未被提領者，應妥適處理發還剩餘款項事宜。

(四)金融消費者保護機制：

1.所訂電子支付定型化契約條款內容，應遵守本會所定定型化契約應記載及不得記載事項，並於官網公布使用者相關權利義務、各項申請及作業程序。

2.應建立申訴處理及交易紛爭之解決機制，並明確告知消費者各項作業程序。

3.業務之資訊系統故障或其他原因，致無法執行使用者支付指示時，應及時通知使用者。

4.對涉及個資之系統功能、報表、文件或電子檔編製個資檔案清冊，應建立納管機制，並定期進行清查及留存相關作業紀錄，對傳遞個資應建立妥適之加密及監控機制，並留存完整稽核軌跡。

(五)資訊系統安全控管：

1.資訊安全人力：資產總額或使用者人數達一定條件以上者，應設置資訊安全專責單位及主管，不得兼辦資訊或其他與職務有利益衝突之業務，並配置適當人力資源及設備。前項資訊安全專責單位如隸屬於資訊組織架構，應與資訊單位分別設置，以符合獨立運作之管理機制。

2.網路安全：防火牆、弱點掃描、入侵偵測及滲透測試等網路安全防禦機制之運作情形、系統安全設定管制程序之妥適性及漏洞修補改善。

3.系統運作管理：特權帳號及高權限帳號應建立控管

措施及作業軌跡覆核機制，依職務分工及最小授權原則授予人員必要之操作權限，對個人資料檔案及資料庫應建立妥適之存取控制與監控措施、核心系統架構重大變更應建立資安控管、完整測試及資料驗證機制。

4.災害應變管理及資安事件管理：應妥適訂定資安事件及緊急處理應變計畫，並依所定計畫辦理演練及檢討。

5.電子支付平臺管理：強化應用程式介面(API)安全管理及行動應用程式(APP)安全檢測。

(六)委外作業管理：

1.將電子支付機構業務之一部委由他人辦理時，須先報經主管機關核准或核備，委外事項範圍應確保符合規定。

2.受託機構人員到機構提供服務時，應建立門禁、攜入設備、作業區網段區隔、系統及資料存取權限等監控措施。

3.建立雲端服務資安控管機制(如：加密及金鑰管理、存取控制及緊急應變計畫)。

(七)法令遵循作業：

1.應建立清楚適當之法令規章傳達、諮詢、協調及溝通系統，並確認各項作業及管理規章均配合相關法規適時更新，使各項營運活動符合法令規定。

2.應訂定法令遵循之評估內容與程序，及督導各單位定期自行評估執行情形，並對各單位法令遵循自行評估作業成效加以考核。

(八)內部稽核：

1.設立隸屬董事會之內部稽核單位，並向董事會及監察人報告稽核業務，稽核主管不得兼任與稽核工作有相互衝突或牽制之職務。

2.內部稽核單位所訂內部稽核計畫、稽核工作手冊及工作底稿之妥適性、查核頻率及查核項目之適足性、辦理內部稽核作業執行情形及落實追蹤改善缺失。

(九)公司治理：

1.董事會職能發揮：如董事會組織及職能、審計委員會及督導風險管理委員會之設置與運作、督導各項業務政策及管理機制情形與對陳報重大事件(如重大違反法令、重大暴險危及財業務狀況)之處置因應等職權行使之妥適性。

2.負責人兼職行為之內部管理機制、法令及內部規範遵循情形、公司治理主管及人員之設置。

3.利害關係人(含實質利害關係人)交易(含不動產、勞務或物品之採購及其他交易等)與管理作業控管機制(含實質利害關係人之自律性控管機制)、集團內或與主要股東、董監事等有實質關係者之交易決策、對象及價格是否異常或涉及利益衝突等法規遵循情形、費用支付之合理性。

4.與有控制能力股東之溝通聯繫機制(含溝通聯繫原則與管理規範、溝通議題、經理人陪同溝通程序、溝通作業控管流程與紀錄)。

5.檢舉制度之獨立性及有效性(含內、外部人員檢舉管道、檢舉人保護措施等內部作業程序及控管機制)。