檢查局113年度各業別金融檢查重點

一、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、112年度所發布金融法規及應加強檢查事項等，擬定113年度檢查重點。

配合本會循序納管虛擬資產平台及交易業務事業(VASP)之政策，113年度新增「虛擬資產平台及交易業務事業(VASP)」一項業別，辦理對VASP業者之防制洗錢相關檢查事項。

二、113年度各業別金融檢查重點

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：督導子公司對防制洗錢法令規範之瞭解及遵循情形(如：審查子公司 IRA 評估方法論一致性及評估結果，集團層次及各子公司風險胃納合理性)，督導受檢子公司就防制洗錢檢查缺失辦理改善及其他非受檢子公司配合檢視調整。

(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，及督導子公司(含轉投資事業)法令遵循主管落實執行相關內部規範之導入、建置與實施，確保法令遵循制度之有效性。

(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.定期確認主體(如：銀行、保險及證券)以外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)，建立經營風險督導管理機制(含完善檢舉制度)，如：

(1)創投子公司：資金運用合理性、減損評估與追蹤管理妥適性、辦理創業投資基金籌集業務之管理機制、訂定集團對創投相關事業總暴險限額、再投資其他創投事業之風險控管規範等。

(2)資產管理子公司：訂定集團對資產管理子公司風險管理指標及限額、每半年檢視營運狀況及業務發展情形、建立明確內部控制制度等。

(3)租賃子公司：依風險承擔能力訂定財務監控指標、適足之資產評估及損失準備提列處理原則並覈實提列各項準備、建立具專業注意之徵授信管理措施、辦理不動產抵押貸款業務應落實法令遵循等。

(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、費用報支及分層負責之管理機制：建立負責人兼職行為、費用報支及核銷作業之內部管理機制，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性質者，費用報支及核銷是否覈實且與所屬職務相關，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.有控制能力股東之溝通機制：建立與有控制能力股東之溝通聯繫與控管機制，包括：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等。

5.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。

6.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。

7.金融機構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.金控公司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.督促子公司落實轉投資事業(含海外)之風險管理，並陳報金控必要資訊，以掌握集團風險。

3.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。

4.金控公司集團轉投資(含海外)之風險管理機制，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。

5.金控公司集團對大陸轉投資之風險承擔總額控管及對被投資事業之管理機制是否妥適。

(六)督導並檢視各子公司對更新資訊系統相關規劃作業之妥適性(如：系統轉換穩定性及測試作業)、網路系統安全控管及資訊安全維護，建立有效之偵測及防護措施，及建置網路系統發生異常時之緊急應變作業程序、復原計畫及客戶權益保護機制。

(七)個人資料保護：金控公司及其子公司建置客戶資料庫之資訊安全管控及個人資料蒐集、處理及利用之安全

維護措施、個資外洩應變演練機制、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。

(八)內部稽核：

1.金控公司及子公司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.金控公司及子公司之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.金控公司內部稽核單位對銀行、保險及證券以外之子公司查核範圍涵蓋重點業務事項。

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.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之完整性與合理性暨採取與客戶風險相稱之審查(含與虛擬資產平台及交易業務事業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：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.可疑交易申報流程及品質：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)法令遵循制度及執行情形：如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)、個人資料保護遵循情形(含客戶資料之保管運用、資通安全機制等)、對信託業務相關消費者保護規範之遵法情形(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辦理情形等)、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之法令遵循情形)。

(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、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(含身心障礙者及高齡客戶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)、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.高資產客戶財富管理業務：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。

5.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。

(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：如資安專責單位與專責主管之職能發揮(含指派副總經理以上或職責相當之人兼任資訊安全長)、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)、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、受託廠商之監督、交付系統與元件之安全檢測、合約妥適性)。

(十)業務操作制度：如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)、協助民眾防制詐騙相關措施(含開戶作業審查、關懷提問、疑涉詐欺帳戶預警機制、網銀與 ATM 等高風險自動化業務管理、異常交易辨識及虛擬帳號控管等)、營運持續管理機制、委外作業之法令遵循情形、跨境委外作業之定期查核(如對委託雲端服務業者處理之資訊安全及風險管控措施)、流動性壓力測試之執行情形及流動性風險管理政策有效性之控管機制。

(十一)授信業務風險控管及法令遵循情形：如授信業務(含應收帳款融資承購業務、購屋貸款、餘屋貸款、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、

辦理中小企業放款禁止授信回存、工業區土地貸款資金用途與流向之控管、閒置工業區土地之授信作業及銀行法第 72 條之 2 之遵循情形。

(十二)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。

(十三)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。

(十四)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。

(十五)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)。

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.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之完整性與合理性暨採取與客戶風險相稱之審查(含與虛擬資產平台及交易業務事業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：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.可疑交易申報流程及品質：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)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)高資產客戶財富管理業務：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度。

2.衍生性金融商品與結構型商品銷售作業之妥適性。

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：如作業委外之法令遵循情形、跨境委外作業之定期查核、對委託雲端服務業者處理之資訊安全及風險管控措施。

(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)。

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.可疑交易申報流程及品質：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。

(三)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(含利率訂價、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)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。

(四)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、高齡客戶權益保護)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。

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。

5.協助民眾防制詐騙相關措施(含關懷提問、強化網路銀行約定轉帳風險控管、疑涉詐欺帳戶預警機制、異常交易辨識及虛擬帳號控管、加強教育宣導等)。

(五)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)、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)。

(六)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、建立流動性風險管理指標及預警機制、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。

(七)社務治理制度運作落實情形：

1.社員代表大會、理監事會及社務會運作情形。

2.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。

3.利害關係人授信與交易之作業控管機制及法規遵循情形、費用支付之合理性。

4.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。

5.興建大樓等營繕工程或購置固定資產等相關作業程序。

(八)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。

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、可疑交易申報流程及品質、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)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)。

(五)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。

(六)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)。

(七)票債券(含外幣債券)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、資金調度作業、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。

(八)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)。

(九)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。

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.可疑交易申報流程及品質：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)受託買賣國內有價證券之經紀業務：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、未成年委託人屆齡成年之委託買賣有價證券作業補正程序等作業是否妥適。

(三)財富管理業務(含高資產客戶)：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。

(四)受託買賣外國有價證券業務：投資人屬性分級管理、KYC 作業、受託投資之標的【如未具證券投資信託基金性質之境外基金及封閉型基金(CEF)】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等之管理機制。

(五)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)、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。

(六)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。

(七)風險管理機制：對全球政經情勢變化及升息環境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、限額管理、停損管理及例外處理機制等)。

(八)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。

(九)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)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。

(十一)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(含身心障礙者及高齡客戶權益保護)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)、對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；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及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。

(十二)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。

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.可疑交易申報流程及品質：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)及高齡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、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、及是否訂定持續營運管理規範並落實執行。

(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。

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.可疑交易申報流程及品質：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.外幣保單及投資型保險商品招攬方式妥適性。

4.分紅保單之銷售作業及資訊揭露辦理情形。

5.對高齡客戶及身心障礙者權益之維護(如：評估保險商品特性對高齡客戶影響之作業程序、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、防範保險業務員挪用、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及區隔資產管理。

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)。

(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(含各國中央銀行之升息政策)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。

(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之防範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。

(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：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。

(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、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.資產總額達新臺幣一兆元以上之保險業設置資訊安全長及具職權行使獨立性之資訊安全專責單位之執行情形。

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：如高齡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。

(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：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。

(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、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)。

(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。

虛擬資產平台及交易業務事業(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：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、實質受益人之辨識與身分之確認。

3.帳戶及交易之持續監控：依風險基礎原則制定之交易監控型態及金額門檻之合理性、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)之檢核及查證情形、監控作業之獨立性及有效性。

4.可疑交易申報流程及品質：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。