

上海商業儲蓄銀行風險管理政策

風險管理處擬定
95.03.11 訂定
99.08.28 修訂
106.03.25 修正
108.11.14 修正
110.03.27 修正
111.06.17 修正
112.11.10 修正

第一章 總則

第一條 本政策係依據『金融控股公司及銀行業內部控制及稽核制度實施辦法』規定，為建立良好之全行風險管理制度，使各單位對風險管理取得共識，有效控制風險，以促進銀行健全發展，提昇全體股東價值，爰制定本政策。

第二條 董事會負責核定整體風險政策，且對於確保建立並維持適當有效之風險控管制度負有最終之責任；風險管理委員會秉於董事會授權，為健全董事會功能及強化風險管理機制而設立；總經理應負責執行董事會核定之經營策略與政策，訂定適當之內部控制政策及監督其有效性與適切性，創造注重風險管理內涵之組織文化，俾使全體行員察覺潛在風險，將風險管理功能運用於每日營運活動。

本政策應根據主管機關法令規章或管理需要，由風險管理處定期檢討及擬訂，呈報總經理核轉，由風險管理委員會審查及董事會核定。

第三條 風險管理處應負責建立與管理全行性風險管理機制¹，以利風險管理之執行；並負責定期出具相關風險管理報告呈報總經理核閱及風險管理委員會審查、董事會核備。各項業務之權責單位應參酌本政策規定，適度規定各項業務風險管理規範。

各項業務風險管理規範應依其業務需求及必要性，分別設定明確風險管理目標與執行風險管理之組織架構與權責，建立風險管理作業流程及管理資訊系統，以利風險管理之執行。

¹ 110.09.23 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 條。

第四條 風險管理機制係以考慮整體暴險，資產配置及計算控管大額暴險，並定期檢視提列備抵損失，和建立資訊安全防護機制為原則。本行風險管理政策、風險限額及各項業務風險管理規定，風險管理處及各權責單位應依營運狀況隨時檢討調整，每年應至少一次定期檢討。

第二章 風險管理組織

第五條 風險管理為本行全體員工之職志，非僅為單一風險管理單位之職責，各權責單位皆應明定其風險管理角色與責任，相互協調配合，以落實整體銀行之風險管理。

第六條 為有效執行風險管理，本行應聘用具備專業能力風險管理人員，授權其獨立行使職權，而執行風險管理之單位及個人應保持獨立性，以確保風險管理制度實行成效。

第七條 風險管理單位與職責

- 一、董事會：為風險管理最高監督單位，承擔本行風險管理最終責任，核定風險管理政策、組織、制度、流程及資訊系統，以確保本行風險管理適當性及有效性。
- 二、風險管理委員會：為健全董事會功能及強化風險管理機制而設立，秉於董事會授權，審查各項風險管理之建議及報告。
- 三、總經理：監控執行董事會核定之風險管理政策，明確指派必要之單位或專業人員並配置必要之資源，執行風險管理工作。
- 四、風險管理處：為專責之風險控管單位，且應獨立行使下列職權：
 - (一) 規劃及制訂全行性之風險管理政策、組織、制度、流程及資訊系統。
 - (二) 擬訂全行性風險限額。
 - (三) 評估及監督本行風險承擔能力、已承受風險現況、決定風險因應策略及風險管理程序遵循情形。

- (四)提供風險管理相關報告，除應送相關單位核備或核閱外，並按各風險管理規章之規定報告。
 - (五)其他經董事會或高階管理層級指派之風險管理相關事務。
 - (六)若發現重大暴險，危及財務或業務狀況或法令遵循者，應立即採取適當措施，並向總經理、風險管理委員會及董事會報告，並提出必要之建議。
- 五、法令遵循處：負責法令遵循制度之規劃、管理及執行，支援和協助各管理階層管理法令遵循風險，包含防制洗錢及打擊資恐風險等。
 - 六、資訊總處：負責依業管單位需求建立全行風險管理相關資訊系統及架構妥適之資訊基礎設施，並確保系統穩定與網路安全；為本行資訊科技風險之執行單位。
 - 七、資訊安全處：負責資訊安全規劃、監控及執行資訊安全維護作業，並建立全行性資訊安全風險管理機制，行使全行資安治理之風險辨識、評估與管理，提供資訊科技風險管理報告及建議；與資訊總處同為本行資訊科技風險之管理單位。
 - 八、稽核處：依風險導向方式不定期查核及評估業務或相關部門之內部控制制度是否妥適及有效運作，並適時提供改進建議。
 - 九、各權責單位：係以各事業部及總經理指派之單位為原則，並得視營運規模、重要性及複雜度設置風險管理人員，執行單位內風險管理流程相關事務，以利該單位與風險管理處間有關風險管理事務之溝通與執行。各單位主管並應督導單位內之風險管理。

第三章 風險管理流程

第八條 風險管理流程應確實落實風險管理政策，配合經營環境作適當調整，訂定適當之書面準則及辦法。風險管理流程包括風險辨識、衡量、監控、報告及因應措施，並應建立風險管理資訊系統，以利風險管理執行。

第九條 風險辨識

本行應辨識風險因子來源，歸納營運活動及金融商品所面臨風險類型，如市場風險、信用風險、作業風險、流動性風險、國家風險、法令遵循風險、資訊科技風險，及氣候風險等。

隨著金融經營環境日益複雜，可能導致風險發生的型態及方式無法預期。為降低營運之衝擊，宜保持彈性之作為以應對新興風險。

第十條 風險衡量

- 一、本行應視實際狀況及需求建立適當之風險量化管理系統。
- 二、風險量化管理不符合成本效益時，宜採質化分析(如文字描述)，以評估風險發生可能性及影響程度。

第十一條 風險監控

風險管理處應配合風險管理組織及制度，制定各項風險之適當監控頻率與報告機制。

第十二條 風險報告及因應措施

風險管理處經由權責單位提供資料或自行蒐集相關資料，以取得可信賴適當之資料經由獨立有效風險評估模式評估，建立風險報告及因應措施制度，依業務性質及產品特性設計內外部之風險報告格式、頻率及因應措施，並定期檢討及更新。

第四章 各類風險管理機制

第十三條 本行所從事業務之市場風險、信用風險、作業風險、流動性風險、國家風險、法令遵循風險、資訊科技風險、氣候風險，及新興風險等之規定，應由各權責單位訂定適當之風險管理規章，並落實執行。

第十四條 市場風險

- 一、市場風險管理制度應包括

- (一)風險管理之組織架構、作業及呈報之內容及流程。
- (二)許可交易範圍。
- (三)市場風險評估及監控方法。
- (四)市場風險限額、有權核定層級及超限處理方式。
- (五)特殊交易及問題交易之處理方式。
- (六)定期就經濟金融情勢之變化，及經營方針之調整，檢討與修正各項風險管理限額，以符合相關政策、內部控制及作業程序。

二、本行所從事業務之市場風險評估頻率，應依照部位性質及業務需要分別訂定。

第十五條 信用風險

一、信用風險管理制度應包括

- (一)風險管理之組織架構、作業手冊及呈報流程。
- (二)事前之信用評估、事後之信用監控。
- (三)擬訂及修訂授信政策含括信用分級管理、有權核定層級及超限處理方式、例外管理。
- (四)考量整體經濟情勢對信用風險影響，並進行適當監督、控管。對於交易對手之產業及風險集中度限額，授信組合之內涵與品質，宜訂定限額控管機制及管理原則，並依循經濟金融情勢之變化及經營方針適時調整之。

二、本行所從事業務之信用風險評估頻率，應依照金融商品性質及業務需要分別訂定。

第十六條 作業風險

一、各權責單位依業務特性，建立完善之控制架構及訂定各層級之內部控制程序，適當之職務分工，員工不應擔任責任相互衝突之工作，以防止不當或錯誤之內部控制程序作業、人員及系統引起直接或間接損失之作業風險。

二、本行應建立資訊安全管理機制，以確保各項業務及客

戶資料之安全。

- 三、本行應建立緊急事件應變計劃，以確保各項業務遇緊急狀況時能正常運作，防止銀行產生重大損失。
- 四、本行應以風險與控制自評(RCSA)作為作業風險辨識、評估之主要管理工具，透過流程分析、風險辨識、風險評估、繪製風險地圖，以釐清全行之作業風險輪廓。
- 五、本行應建置作業風險損失資料庫並制定作業風險事件通報處理程序，以建立內部作業風險事件管理機制，透過內部作業風險事件收集(LDC)及紀錄保存，了解損失事件發生成因及分析可能損失金額，作為改善內部控制程序參考，確保董事會及各管理階層瞭解全行風險概況，進而加以管理，設法降低或移轉作業風險。

第十七條 流動性風險

- 一、流動性風險管理制度應包括
 - (一)風險管理之組織架構、作業及呈報之內容及流程。
 - (二)流動性風險評估及監控方法。
- 二、流動性風險管理執行單位對於異常或緊急狀況之資金調度需求，應擬定應變計劃。

第十八條 國家風險

- 國家風險管理制度應包括
- 一、風險管理之組織架構、作業及呈報之內容及流程。
 - 二、國家風險評估及監控方法。
 - 三、國家風險超限之處理方式。

第十九條 法令遵循風險

- 一、本行各單位法令遵循主管應確實依照本行法令遵循政策及法令遵循制度辦法，遵守與營運活動之相關法規，並據以評估與管理銀行之法令遵循風險。
- 二、本行各單位法令遵循主管應確實監控各單位契約文件及作業規章，以確保交易之適法性。

- 三、本行對法令遵循事宜應建立諮詢溝通管道，以有效傳達法令規章，俾使職員對於法令規章之疑義得以迅速釐清，並落實法令遵循。

第二十條 資訊科技風險

- 一、本行應架構符合業務規模與風險狀況之妥適資訊基礎設施，持續評估與監控各系統風險，確保持續營運及系統穩定與安全。
- 二、本行應建立個資安全維護、網路安全控管、災害應變等風險管理及通報機制。
- 三、本行對於新興科技之運用應進行風險評估。

第二十條之一 氣候風險

氣候風險治理面向應包括：

- 一、風險管理之組織架構、作業及呈報之內容及流程。
- 二、氣候風險評估及監控方法。
- 三、高氣候風險客戶、資產之管理措施。
- 四、氣候風險重大異常或特殊情況之處理。

第二十一條 新興風險

新興風險辨識流程：

- 一、風險管理處每年參考外部機構發佈之研究報告及產業標竿企業之企業社會責任報告，提供風險因子清單及新風險評估表予各相關權責單位。
- 二、各業務管理單位參考風險因子清單，依其發生可能性及衝擊影響程度，透過質化或量化的方法進行評估，辨識營運及業務應關注之新興風險，並研擬該等新興風險之因應、抵減措施或監控機制後，呈送新興風險評估表予風險管理處。
- 三、風險管理處彙整各業務管理單位之新興風險，經提報永續經營執行委員會，及風險管理委員會審議，並呈報董事會核議，據以建立本行之新興風險。

四、持續觀察所識別風險之影響與抵減措施運作情形，併同每年之企業社會責任報告書對外揭露。

第二十二條 風險管理監控及彙報

風險管理處應監控本行之市場風險、利率風險、信用風險、作業風險、流動性風險、國家風險、法令遵循風險、資訊科技風險、氣候風險，及新興風險，並彙報本行新巴賽爾協定有關適足率資本計提相關法規彙整。

第五章 壓力測試

第二十三條 本行壓力測試依主管機關規定與高階管理層級指示執行，評估本行在壓力情境之損失承擔能力與對資本適足性或流動性之影響。壓力測試結果可作為本行風險限額設定之重要依據。

第六章 新種業務或重大投資之風險評估

第二十四條 為確保本行對新種業務或產品之風險管理和內部控制，在拓展新業務或進行重大投資前，由負責部門評估風險及利潤，進行內部審核流程後方可承作。如主管機關對該類新種業務或重大投資之開辦另有規定，則依其規定辦理。

第七章 永續金融發展

第二十五條 本行善盡企業社會責任、注意利害關係人之權益，並落實永續風險管理，將環境、社會與公司治理(ESG)，納入各類風險管理之衡量指標及相關流程，以提升資產品質、健全業務發展，達成獲利成長與永續經營之雙贏目標。

第八章 兼營債券、受益證券、資產基礎證券承銷及自行買賣業務²

第二十六條 本行兼營債券、受益證券、資產基礎證券承銷及自行買賣業務應遵循：

- 一、針對交易範圍、整體及個別部位之風險限額、同一關係集團曝險限額、核定層級等訂定相關規範，風險管理單位應定期檢視曝險情形，並向董事會報告。
- 二、本行應訂定商品適合度政策，至少應包括瞭解客戶、客戶分級、商品審查分級、商品適合度、行銷過程控管、風險告知（如國際金融業務分行不適用金融消費者保護法、最大可能損失等）、銀行風險控管、內部控制及內部稽核制度等規範。

第九章 附則

第二十七條 風險管理處負責協調管理各權責單位依主管機關規定於年報、銀行網頁或其他處所需揭露風險管理相關資訊。

第二十八條 風險管理人員應隨時注意國際與國內風險管理制度之發展情形，並據以檢討改善所建置之風險管理制度，以提昇風險管理執行成效。

第二十九條 為落實風險管理制度之執行，各單位應配合人力資源處，依據個別狀況設計完整之人員訓練制度，以期達成風險管理政策所設定之各項目標。

第三十條 本政策如有未盡事宜，悉依主管機關及本行相關規定辦理。

第三十一條 本政策經提報董事會核定後實施，修正時亦同。

² 112.07.31 金管銀外字第 11202181261 號令第九條