

國泰世華商業銀行風險管理政策

111.11.10 第 17 屆第 2 次董事會核定

權責單位：信用暨作業風管部

第一條 風險管理總綱

一、風險管理目的

為因應漸趨複雜的經營環境及涉險程度的多樣化，在符合國內外相關法令與規範下，落實本行風險管理於日常營運活動，合理制定因應措施，以降低潛在業務風險、創造最大股東價值，並追求企業永續經營，爰依據「公開發行公司建立內部控制制度處理準則」、「金融控股公司及銀行業內部控制及稽核制度實施辦法」，訂定本政策。

二、風險管理範疇

於企業風險管理(Enterprise Risk Management, ERM)架構下，本行營運所涉及之各類風險，如：「市場風險」、「信用風險」、「流動性風險」、「作業風險」、「銀行簿利率風險」、「法遵風險」、「資訊科技風險」、「策略風險」、「聲譽風險」、「環境社會、永續治理與氣候風險」、「防制洗錢及打擊資恐風險」，以及其他新興風險等，均需納入風險管理範疇，審慎評估各類風險間之相互影響，並訂有相關依循之規範。本行亦應維持適當之資本適足率，以確保資本結構之健全。

(一) 市場風險

因市場價格不利之變動，造成資產負債表內及表外部位可能產生之損失；市場價格指利率、股價、匯率及商品價格等。其範圍包括交易簿及銀行簿所有匯率部位與商品部位，以及交易簿內利率部位及權益證券部位。本行訂有「市場風險管理準則」等相關規範以為遵循。

(二) 信用風險

借款人或交易對手因其財務體質惡化或其他因素(如企業與其往來對象之糾紛等)，導致借款人或交易對手不履行其契約義務而產生之違約損失風險。本行訂有「信用風險管理準則」等相關規範以為遵循。

(三) 流動性風險

因部位無法在合理時間內，依最近市價成交，或市場突發狀況致使無法取得預期資金以支應資產增加或償付到期負債，並充分支應資產成長能力之風險。本行訂有「流動性風險管理準則」等相關規範以為遵循。

(四) 作業風險

因內部作業、人員及系統之不當或失誤，或因外部事件所造成損失之風險，包括法律風險，但排除策略及聲譽風險。本行訂有「作業風險管理準則」等相關規範以為遵循。

(五) 銀行簿利率風險

當帳列銀行簿之部位面臨利率波動時，因資產端和負債端之本金與利息現金流量不完全對稱，導致整體收益率及盈餘受到利率波動影響之風險。本行訂有「銀行簿利率風險管理準則」等相關規範以為遵循。

(六) 法遵風險

因未能遵循外部法規及內部準則，而遭受法律制裁或監管機關裁罰，或因此產生重大財務損失或聲譽損失之風險。本行訂有「法令遵循制度實施準則」等相關規範以為遵循。

(七) 資訊科技風險

因資訊科技及處理流程在管理與控制等方面的不足、資訊科技之策略及政策不夠完備，或是重要資訊之存取運用等管理不善，而對收益或資本造成之實質或潛在風險。本行訂有「資訊安全政策」及「資訊服務事故管理規則」等相關規範以為遵循。

(八) 策略風險

因不良之決策、不適當之執行方式，或對行業、經濟、科技變化缺乏反應，導致對收益、資本、聲譽、地位產生實質及潛在影響之風險。訂定相關策略時應秉持風險管理程序，辨識可能風險來源、審慎衡量評估，根據全行風險概況、市場和整體經濟情勢，適時調整方向，並向高階管理階層報告管理狀況。

(九) 聲譽風險

由於本行或子公司(含員工)之不當行為或媒體負面消息，可能導致損害品牌價值與股東權益，對於本行聲譽造成不利影響，而須採取

防禦措施因應之風險。本行訂有「聲譽風險管理準則」等相關規範以為遵循。

(十) 環境社會、永續治理與氣候風險

因借款人或交易對手在建設、生產、運營及投資活動中，未落實健全治理、未意識社會責任、永續發展、或未力求減少損害、降低污染及支持低碳經濟，產生對環境與社會之負面影響或因極端氣候變遷等事件，導致銀行形象受損，或產生實質及潛在損失之風險。本行訂有「ESG 與氣候風險管理準則」等相關規範以為遵循。

(十一) 新興風險

為規避或管理目前尚未顯現但可能隨環境改變而產生之風險，通常起因於政治、法規或市場變化。本行訂有「新興風險管理準則」等相關規範以為遵循。

(十二) 防制洗錢及打擊資恐風險

為避免未能確實遵循國內、外防制洗錢及打擊資恐之相關規範，而遭受監管機關裁罰，或遭不法分子利用本行服務進行非法所得來源之清洗或資助恐怖行為或恐怖組織，而致對本行產生實質或潛在之洗錢或資恐風險。本行訂有「防制洗錢與打擊資恐政策」、「防制洗錢及打擊資恐風險評估準則」及「洗錢及資恐風險胃納管理準則」等相關規範以為遵循。

風險管理政策與準則應視內外部環境變化定期檢視是否修訂。

三、風險管理基本原則

(一) 應根據環境變化進行調整，與當前風險狀況和系統重要性等相互因應並合理配置。

(二) 應當覆蓋所有風險種類及不同風險間之相互影響，包括各類業務範疇、分支機構、附屬機構、部門和人員。

(三) 應當建立專責風險管理組織架構，配置人力資源及其他資源、授予風險管理部門足夠權限，並建立有效的溝通管道，與業務端間形成相互制衡之運行機制。

(四) 應根據全行風險概況、市場和整體經濟情勢，評估資本和流動性之充足性，有效預防所承擔之總體風險和各類風險，並將風險管理結

果應用於經營管理上。

第二條 風險管理治理

一、風險管理文化與意識

董事會及高階管理階層應創造一個注重遵循內部風險管理機制的組織文化，且該文化必須能因應本行營運需求變化調整。

二、組織架構

(一) 董事會

應瞭解全行所承擔之各項風險，並負擔起整體風險管理之最終責任。建立適當的風險管理策略、架構及全行的風險管理文化，核定重大風險管理政策及程序，並將資源做有效配置；除定期檢視風險管理策略、風險組織、風險流程及風險管理資訊外，並得適時檢視各項風險機制以確保妥適性並得有效掌握全行風險狀況。

(二) 高階管理階層

高階管理階層應執行董事會所核准之風險管理策略，及風險管理架構；監督檢視管理流程的適當性，並明確指派必要之專業人員。確認從事各項風險管理之員工，具備專業的條件及能力。確保有效地溝通與協調相關風險管理功能及跨部門間之各項風險。

(三) 功能委員會

各委員會依其組織要點之規範組成，並依負責專長領域，定期召開會議，協助董事會與高階管理階層執行監督及管控功能。各委員會包含如下：

1. 風險管理委員會

管理信用、市場及作業風險之相關事項，進行信用評等(分)、市場評價、風險指標、資本適足率等重要風險管理報告及其他風險管理相關討論事項等。

2. 授信審議委員會

審議各單位簽報之授信案件、管理與授信案件審議或與信用風險有關之事項等。

3. 資產負債管理委員會

管理本行之流動性部位及利率敏感性資產負債結構、分析國內外

金融及經濟情勢，評估預測國內外利率、匯率可能變化，以為資產負債管理決策擬訂之參考等。

4. 資訊安全委員會

督導與協調資訊安全管理相關工作、推展資訊安全管理之制度等。

5. 內部控制聯繫會議

建立內部稽核部門與法令遵循、風險管理、自行查核等單位之溝通機制，以針對銀行內部控制弱點、及其他關注重點進行溝通，並作為稽核單位訂定內部稽核計畫及查核重點之參考。

6. 業務風險內控暨合規(Business, Risk, Control & Compliance Committee, BRCC Committee)聯席會議

強化本行公司治理及內部溝通機制，定期召開 BRCC 聯席會議，架構本行多向溝通之平台，各單位得於 BRCC 聯席會議中討論潛在之業務風險、內控機制、相關挑戰及主要法規問題。

7. 防制洗錢與打擊資恐委員會

強化本行防制洗錢及打擊資恐業務執行，針對全行防制洗錢及打擊資恐事務、相關重大議題及主管機關重要函示等進行討論並作成決策。

三、三道防線運作

(一) 第一道防線

如業務管理單位、產品單位、資訊單位及會計單位等，負責及持續管理營運活動所產生的相關風險，包含辨識、評估、控制及降低風險，並建立及執行內部管理程序。當流程及控制程序不足時，應提出改善計畫。

(二) 第二道防線

如風險管理、法令遵循及其他專職單位，負責訂定整體政策及建立管理制度、監督風險承擔能力及承受風險現況，並將風險管理結果呈報高階管理階層。

(三) 第三道防線

稽核單位，負責查核與評估第一道及第二道防線所設計並執行之內部控制與風險管理制度之有效性，並適時提供改進建議。

各道防線依其功能執行風險控管時，應互相協調並分享資訊，以確保整

體風險管理之順利運作。

第三條 風險管理流程

一、風險辨識

- (一) 由本行內部整體及個別營運活動之角度，有系統地辨識風險，以便充分了解全行的風險概況。
- (二) 當外部的環境改變時，即宜進行風險辨識及後續相關工作，以確保本行風險管理機制之妥適性，並掌握全行風險變動之情形。
- (三) 風險辨識時，應依照不同之風險類型、產品或服務，歸納出各類風險因子，編製全行風險地圖。藉由定期檢視與評估發現潛在風險，擬訂因應措施並適時調整。

二、風險衡量

- (一) 以適當且一致的方法，衡量不同的風險類型、產品或服務之暴險程度，作為風險監控、進行績效評估與資本管理的依據。
- (二) 以特定的指標或標準，分析各項風險之暴險程度。
- (三) 應清楚說明所選擇之風險衡量方法，並規劃風險衡量所需要之風險管理資訊系統，以確實執行風險衡量。依不同類型之風險，訂定量化或其他可行之質化標準，加以衡量。
- (四) 應檢視風險衡量方法的主要假設、數據來源及程序。

三、風險管理執行情序

- (一) 日常風險管理執行情序應與風險政策結合。本行應依日常營運活動所涉之各種風險之處理步驟、呈報流程以及權責劃分方式，擬訂各相關辦法及準則。
- (二) 明訂風險限額制定及管理辦法，並經由董事會或有權授權單位核准後施行。
- (三) 風險管理執行情序需因應市場狀況或業務策略做必要之調整。

四、風險溝通

- (一) 本行應依照適用對象及使用目的之不同，規劃符合需要之風險管理報告之格式與頻率。
- (二) 依本行風險管理組織及職掌，建立適當的風險報告架構，彙整並呈報風險管理之必要的資訊。風險報告內容必須使其使用者瞭解其所欲傳達之風險管理資訊，以協助風險管理決策。
- (三) 為增加對外資訊透明度，及符合主管機關要求，公開揭露原則由董事會核准後，依原則規定對外揭露相關定性與定量資料。

五、風險監控

風險監控程序應配合本行風險管理組織架構，制定各項風險之適當監控方式與逐級呈報機制並與例行營運活動相結合。針對重大之事件，可訂定特殊報告程序，以掌握風險，並為即時因應。每年至少一次向董事會進行風險管理業務執行工作報告，報告內容包括但不限於總體風險和各類風險之整體狀況、風險偏好及風險限額執行情況等。

六、風險對策

依各風險所發生之機率及嚴重性進行分析及評估，以決定其所經營業務之風險對策。風險對策可能採行之方式如下：

1. 高風險發生機率及高損失嚴重性者採用風險迴避；
2. 高風險發生機率及低損失嚴重性者採用風險控制；
3. 低風險發生機率及高損失嚴重性者採用風險抵減/移轉；
4. 低風險發生機率及低損失嚴重性者採用風險承擔。

七、風險管理資訊

建立適當的風險管理資訊架構，以促進有效的管理與控制營運的各種環節。風險管理資訊應依其內容之重要性程度，建立不同的資訊安全等級，以確保資料與資訊之機密性。

第四條 資本適足性管理

為妥善管理全行之資本，以維持適當之資本適足性、確保健全之資本結

構，及促進穩健之業務成長。本行訂有「資本管理政策」及「資本適足性管理準則」等相關規範以為遵循。

第五條 新金融產品與新種業務

推出新金融產品或新種業務前，須檢附新金融產品或新種業務計劃及風險評估報告，並由相關支援單位協助檢視其所衍生之可能風險及相關辨識、衡量、溝通及監控等程序的妥適性。本行訂有「新產品規劃評估規則」等相關規範以為遵循。

第六條 海外分行於執行風險管理時，除符合當地法令規定外，亦須遵循本政策及「Best Practices for Overseas Branch Risk Management Principles」，以確保政策之一致。海外分行得自行增訂風險管理規章，並依照分層負責表授權層級呈核。

第七條 海外子行（子公司）得視其所在地之法令、主管機關要求或實務需要，自行制定適用之風險管理政策或準則。依據各子行（子公司）之分層負責表、「海外子行會簽國泰世華銀行彙整表」、「各公司會簽國泰金控事項彙整表」辦理後，提報子行（子公司）董事會審議。此外，子行（子公司）係指本行單獨持有一銀行已發行有表決權股份總數或資本總額全部。

第八條 政策核准與修訂

本政策經董事會核定後實施，修訂或廢止時亦同。