玉山銀行內部控制制度

2007.11.15 第 6 屆第 15 次董事會訂定
2009.11.12第7屆第9次董事會通過
2012.3.16第8屆第7次董事會修訂
2014.11.14 第 9 屆第 5 次董事會修訂
2015.8.21 第 9 屆第 11 次董事會修訂
2017.3.24 第 9 屆第 23 次董事會修訂
2017.4.28 第 9 屆第 25 次董事會修訂
2018.8.10 第 10 屆第 9 次董事會修訂
2019.11.13 第 10 屆第 17 次董事會修訂
2020.4.24 第 10 屆第 20 次董事會修訂
2021.11.12 第 11 屆第 16 次董事會修訂
2023.11.13 第 12 屆第 7 次董事會修訂
2024.08.16 第 12 屆第 13 次董事會修訂

第一章　總則

第一條　本制度依「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「公開發行公司建立內部控制制度處理準則」、「銀行業公司治理實務守則」及「銀行內部控制三道防線實務守則」訂定之。

第二條　本制度之目的在於促進本行健全經營及永續發展，並由董事會、經營管理階層及所有員工共同遵行，以合理確保達成下列目標：

一、營運之效果及效率。

二、報導具可靠性、及時性、透明性及符合相關規範。

三、相關法令規章之遵循。

前項第一款所稱營運之效果及效率目標，包括獲利、績效、保障資產安全及永續經營等目標。

第一項第二款所稱之報導，包括公司內部與外部財務報導及非財務報導。其中外部財務報導之目標，包括確保對外之財務報表係依照證券發行人財務報告編製準則及一般公認會計原則編製，交易經適當核准等目標。

第二章　原則及範圍

第三條　董事會應核准並每年覆核整體經營策略、永續發展與重大政策，且應認知營運所面臨之風險，監督其營運結果及永續資訊揭露，並對於確保建立及維持適當有效之內部控制制度負有最終之責任。

第四條　本行之控制環境包括誠信與道德價值、董事會及審計委員會治理監督責任、組織結構、權責分派、人力資源政策、績效衡量、獎懲及永續經營目標等。董事會

與經理人應建立內部行為準則，包括訂定董事行為準則、員工行為準則。

第五條　內部控制制度應發揮有效管理，經營管理階層應考量外部環境與商業模式改變及永續發展之影響，以及可能發生之舞弊情事。其風險評估結果，可協助本行及時設計、修正及執行必要之控制作業。

第六條　控制作業為本行依據風險評估結果，採用適當政策與程序之行動，將風險控制在可承受範圍之內。控制作業之執行應包括本行所有層級、業務流程內之各個階段、所有科技環境等範圍、適當之職務分工，且經營管理階層及員工均應避免擔任責任相互衝突之工作。

第七條　內部控制制度須具備產生規劃、執行、監督等所需資訊及提供資訊需求者適時取得資訊之機制，並保有完整之財務、營運及遵循資訊，建立有效之溝通管道。

第八條　本行營業單位及業務管理單位應執行持續性評估，亦即對其營運過程進行例行評估。內部稽核人員應執行個別評估，對於本行所發現之內部控制制度缺失，應向高階管理階層、董事會及審計委員會溝通，並及時改善。

本行稽核人員及法令遵循主管，對內部控制重大缺失或違法違規情事所提改進建議不為管理階層採納，將肇致銀行重大損失者，均應立即作成報告陳核，並通知獨立董事或審計委員會，同時均應立即通報主管機關。

第九條　內部控制制度應涵蓋本行之營運活動及永續相關資訊之管理，遵循所屬產業法令，包括對各種交易循環類型之控制作業，並應訂定適當之政策及作業程序，且應適時修訂。本行之組織規程或業務章則，包括組織系統、部門職掌、業務範圍與分層負責授權辦法等。各部門應訂定下列業務相關之規範及手冊：

一、　出納、存款、匯兌、授信、外匯、信託、保險、新種金融商品。

二、　投資準則及股權管理。

三、　客戶資料保密。

四、　利害關係人交易規範。

五、　董事會議事運作之管理。

六、　財務報表編製流程之管理，包括適用國際財務報導準則之管理、會計專業判斷程序、會計政策與估計變動之流程。

七、　總務、資訊、人事管理(含輪調及休假規定)。

八、　對外資訊揭露作業管理。

九、　委外作業管理。

十、　金融檢查報告之管理。

十一、金融消費者保護之管理。

十二、防制洗錢及打擊資恐機制及相關法令之遵循管理，包括辨識、衡量、監控洗錢及資恐風險之管理機制，以及依據風險評估結果而訂定之防制洗錢

及打擊資恐計畫。

十三、股務作業之管理。

十四、個人資料保護之管理。

十五、審計委員會議事運作之管理。

十六、重大偶發事件之處理機制。

十七、兼營證券商業務內部控制制度之管理。

十八、內部信用評等管理。

十九、其他業務之規範及作業程序。

前項各種作業及管理規章之訂定、修訂或廢止，需配合法規、業務項目及作業流程等之變更至少每年檢討修訂，必要時應有法令遵循、內部稽核及風險管理單位等相關單位之參與。

第十條　辦理內部控制制度自行查核內容應融入內部控制制度有效性判斷項目。

第三章　內部控制三道防線

第十一條　本行應建立內部控制三道防線架構，明確釐清三道防線之權責範圍，以利各單位了解其各自在銀行整體風險及控制架構所扮演之角色功能，加強風險管理及內部控制工作的溝通協調，三道防線各司其職。

第十二條　董事會及經營管理階層應積極協助及指導三道防線之建立，清楚界定各道防線之角色功能及權責，並持續確保組織架構符合三道防線原則，督導該架構之有效運作，並對其有效性負最終之責任。

經營管理階層建立三道防線架構時，應考量各項營運活動的性質、大小、複雜程度及風險狀況進行調整，但其調整需能確保三道防線之有效性。

第一節　第一道防線

第十三條　第一道防線係指本行各單位就其功能及業務範圍，承擔各自日常事務所產生的風險，並應負責辨識及管理風險，針對該風險特性設計並執行有效的內部控制程序以涵蓋所有相關之營運活動。

第十四條　第一道防線負責及持續管理營運活動所產生的相關風險，包含下列各款：

一、辨識、評估、控制及降低營運活動所產生的風險，確保營運活動與本行目標及任務一致。

二、 第一道防線應將風險控制在其單位可承擔之範圍內，依需要向第二道防線報導其曝險狀況。

三、建立內部控制程序。

四、執行風險管理程序並維持有效的內部控制。

五、 當流程及控制程序不足時，應立即提出改善計畫。

第一道防線應定期或不定期就前項內容辦理自我評估，以確保風險有被適當控管。

第二節　第二道防線

第十五條　第二道防線係獨立於第一道防線且非為第三道防線的其他功能及單位，依其特性協助及監督第一道防線辨識及管理風險。第二道防線包含風險管理、法令遵循、資訊安全及其他專職單位(包括但不限於財務控制、人力資源、法務等)，其就各主要風險類別負責銀行整體風險管理政策之訂定、監督整體風險承擔能力及承受風險現況、並向董事會或經營管理階層報告風險控管情形。

第十六條　第二道防線的功能係在訂定整體政策及建立管理制度，協助及監督第一道防線管理風險與自我評估執行情形。依照不同的功能性質，第二道防線之權責包含協助辨識及衡量風險、定義風險管理角色及責任、提供風險管理架構及定期將風險管理結果呈報經營管理階層。

第十七條　為符合法令之遵循，應建立法令遵循制度，由法令遵循單位負責其制度之規劃、管理及執行，訂定法令遵循之評估內容與程序，督導各單位定期辦理法令遵循自行評估；並指派高階主管一人擔任總機構法令遵循主管，綜理法令遵循事務，至少每半年向審計委員會及董事會報告，如發現有重大違反法令或遭金融主管機關調降評等時，應即時通報董事，並就法令遵循事項，提報董事會。

總機構法令遵循主管得兼任防制洗錢及打擊資恐專責單位主管，但不得兼任法務單位主管或內部其他職務。

第十八條　本行應訂定適當之風險管理政策，建立獨立有效之風險管理機制，以評估及監督本行及子公司整體風險承擔能力、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。

前項風險管理政策應經董事會通過並適時檢討修訂。

第十九條　風險管理單位應至少每季向董事會提出風險控管報告，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董事會報告。

第二十條　本行應訂定適當之資訊安全政策，建立獨立有效之資訊安全管理制度，以推動、協調、督導及改善本行資訊安全管理體系之運行情形，有效管控資訊安全風險並符合公司整體營運需求。

本行應設置具職權行使獨立性之資訊安全專責單位，負責規劃、監控及執行資訊安全管理作業，並設置資訊安全專責單位主管，綜理資訊安全事務。

第一項資訊安全政策應經董事會通過並適時檢討修訂。

第三節　第三道防線

第二十一條 第三道防線係內部稽核單位，應以獨立超然之精神，執行稽核業務，協助董事會及經營管理階層查核與評估風險管理及內部控制制度是否有效運作及衡量營運之效率，包含評估第一道及第二道防線進行風險監控之有效性，並適時提供改進建議，以合理確保內部控制制度得以持續有效實施及作為檢討修正內部控制制度之依據。

第二十二條 本行應設置隸屬董事會之內部稽核單位，並訂定內部稽核之組織、編制與職掌，建立總稽核制，以獨立超然之精神，綜理稽核業務，至少每季向審計委員會及董事會報告。

第二十三條 內部稽核單位應編撰內部稽核工作手冊及工作底稿，其內容至少應包括對內部控制制度各項規定與業務流程進行評估，以判斷現行規定、程序是否已具有適當之內部控制，各單位是否切實執行內部控制及執行內部控制之效益是否合理等，隨時提出改進意見。

第二十四條 內部稽核單位對金融檢查機關、會計師、內部稽核單位(含母公司內部稽核單位)與內部單位自行查核所提列檢查意見或查核缺失及內部控制制度聲明書所列應加強辦理改善事項，應持續追蹤覆查，並將其追蹤考核改善情形，以書面提報董事會或審計委員會，並列為對各單位獎懲及績效考核之重要項目。

第二十五條 本行於主管機關或國外分支機構當地主管機關檢查結束或收到檢查報告後，總機構之內部稽核單位應依重大性原則，即時通報董事，並提報最近一次董事會報告。報告事項應包括檢查溝通會議內容、主要檢查缺失、遭金融主管機關調降評等、主管機關要求採行之重大缺失改善方案或可能採行之處分措施。

第二十六條 本行內部稽核人員應秉持超然獨立之精神，以客觀公正之立場，確實執行其職務，並盡專業上應有之注意，除每季向各審計委員會報告稽核業務外，稽核主管並應列席董事會報告。

內部稽核人員執行業務應本誠實信用原則，並不得有下列情事：

一、明知本行之營運活動、報導及相關法令規章遵循情況有直接損害利害關係人之情事，而予以隱飾或作不實、不當之揭露。

二、因職務上之廢弛，致損及本行或利害關係人之權益等情事。

三、逾越稽核職權範圍以外之行為或有其他不正當情事，對於所取得之資訊，對外洩漏或為己圖利或侵害本行之利益。

四、對於以前曾服務之部門，於一年內進行稽核作業。

五、對於以前執行之業務或與自身有利害關係或利益衝突案件未予迴避，而辦理該等案件或業務之稽核工作。

六、直接或間接提供、承諾、要求或收受本行從業人員或客戶不合理禮物、款待或其他任何形式之不正當利益。

七、未依規配合辦理主管機關指示查核事項或提供相關資料。

八、其他違反法令規章或經主管機關規定不得為之行為。

本行應隨時檢查內部稽核人員有無違反前項之規定，如有違反規定者，應於發現之日起一個月內調整其職務。

第四節　三道防線間之協調

第二十七條 各道防線依風險管理及內部控制架構中所扮演之角色功能進行協調，運作之原則如下：

一、風險管理及控制流程的建構應遵循三道防線模式。

二、各道防線均應本於其角色定位及職掌，確實執行及管理相關業務。

三、各道防線應互相協調，以促進效果及效率。

四、各道防線之風險管理及控制功能運作結果，應互相分享知識與資訊，以協助所有功能更有效完成其職責。

第四章　附則

第二十八條 經理人及相關人員違反本制度之規定時，依「玉山銀行員工獎懲要點」進行懲處。

第二十九條 本行應確保金融檢查報告之機密性，負責人或職員除依法令或經主管機關同意者外，不得閱覽或對執行職務無關之人員洩漏、交付或公開與金融檢查報告全部或部分內容。

本行應制定金融檢查報告之相關內部管理規範及作業程序，並提報董事會通過。

第三十條　本制度經董事會通過後施行。