金融控股公司及銀行業內部控制及稽核制度實施辦法修正總說明

金融控股公司及銀行業內部控制及稽核制度實施辦法（以下簡稱本辦法）自九十九年三月二十九日訂定發布以來，期間為強化金融消費者保護、落實薪資報酬委員會之運作、提高金融機構對法令遵循之重視、參考美國 Committee of Sponsoring Organizations (COSO 委員會)於西元二〇一三年所提《內部控制-整體架構》更新報告、強化防制洗錢及打擊資恐機制、建立金融機構內部檢舉制度及建置資安專責制度等需要，歷經七次修正，最近一次修正發布係一百十年九月二十三日。

本辦法前已就前揭議題需要，歷經多次修法。為精進本辦法，本次修正除就架構性酌予調整章節名、次序及相關條次外，亦納入內部控制三道模型精神，並考量國際監理趨勢、國內外銀行實務，暨金融監督管理委員會監理重點等。章節主要調整為將現行第三章-內部控制制度之查核修正為內部控制制度之管理、監督及查核，並按第一、二及三道依序列示，分為第一節自行查核制度、第二節法令遵循制度、第三節風險管理制度、第四節資訊安全制度、第五節內部稽核制度及第六節委託會計師查核制度等。

為強化金融機構內部控制三道間相互協作，修正三道防線為三道模型。另為落實三道之職能，第三道對第一道及第二道進行獨立監督，以及第二道協助與監督第一道，故刪除內部稽核單位督導各單位自行查核執行情形，改由管理階層指定執行法令遵循制度、風險管理制度、資訊安全制度或具第二道功能之單位，督導訂定自行查核執行內容與程序，並整併法令遵循自行查核與自行評估作業程序，及簡化一般及專案自行查核程序。另考量金融環境變遷對稽核人員有不同之需求，放寬金融控股公司及銀行業聘任屬具備曾任會計師事務所查帳員、電腦程式設計師或系統分析師等專業人員資格條件之稽核人員員額比例上限。

配合金融監督管理委員會陸續發布「上市櫃公司永續發展行動方案」、「我國接軌 IFRS 永續揭露準則藍圖」等規定，強化金融機構對永續資訊之管理，促使其落實環境、社會及治理(ESG)之責任。同時為因應嚴重特殊傳染性肺炎、氣候變遷、新型態資安攻擊所帶來經濟環境變化、威脅與

風險，且考量巴塞爾銀行監理委員會及國外金融監理機關亦定有相關營運持續管理指南，均顯示因應環境變化，金融機構營運韌性及新興風險控管之重要性，以及一百十四年銀行施行責任地圖制度，爰增訂內部控制制度相關規範包含永續資訊之管理、營運持續管理機制及銀行業務規範及處理手冊應包含責任地圖制度等。另為專業化、組織化、常態化持續性打擊詐欺，金融監督管理委員會推動金融機構指定或設置專責打詐單位，爰配合修正金融控股公司及銀行業法令遵循長得兼任防制詐欺專責單位主管。

為進一步健全金融控股公司及銀行業風險管理，參考美國 COSO 委員會西元二〇一七年發布《企業風險管理—整合策略與績效》報告及巴塞爾銀行監理委員會西元二〇二四年發布新版《有效銀行監理核心原則》，明定風險管理架構內涵及風險管理專責單位權責，並增訂相關風險管理機制應包含辨識、評估及衡量潛在新興風險；同時參考美、英、香港及新加坡等國外金融監理機關規範及國際銀行實務經驗，增設風險管理長，以綜理風險管理事務。另為確保金融控股公司及銀行業總稽核之獨立性，參酌「公開發行公司建立內部控制制度處理準則」增訂總稽核異動應向金融監督管理委員會函報之規定。

金融機構之法令遵循制度、風險管理制度及資訊安全制度等屬內部控制之第二道，具同等重要性。因應不同時期之金融監理重點，本辦法之法規架構與規範層次分階段發展完備。考量金融機構已逐步建置相關組織架構與制度，爰規定金融控股公司及銀行業均須設置三長(即法令遵循長、風險管理長及資訊安全長)及隸屬於總經理之專責單位，俾利二道功能有效發揮，以健全金融機構內部控制制度與持續穩健經營。

本案為全案修正，現行條文計五十四條，修正後全文共五十五條，修正重點如下：

一、考量現行條文已規定總經理應督導各單位審慎評估及檢討內部控制制度執行情形，且本次修正後法令遵循、風險管理及資訊安全專責單位均隸屬於總經理，爰簡化內部控制制度聲明書應簽署人員相關規定。(修正條文第八條)

二、參考 The Institute of Internal Auditors(IIA，國際內部稽核協會)西元二

◯二◯年發布《國際內部稽核協會三道模型：三道防線的更新版》，修正三道防線為三道模型，以強化三道互相協作。(修正條文第九條)

三、增訂董(理)事會與管理階層應落實公平待客原則，並建立誠信經營守則。(修正條文第十條)

四、增訂內部控制制度相關規範及處理手冊包括永續資訊之管理、營運持續管理機制、銀行、信用合作社及票券商業務規範及處理手冊應包括各業法所定業務，以及銀行業務規範及處理手冊應包括責任地圖制度。(修正條文第十二條)

五、修正由管理階層指定執行法令遵循制度、風險管理制度、資訊安全制度或具第二道功能之單位，督導訂定自行查核內容與程序及覆核執行情形，並整併法令遵循自行查核與自行評估規定。採行風險導向內部稽核制度之銀行業，得依風險評估結果訂定一般及專案自行查核計畫，以簡化作業程序。(修正條文第十四條及第十七條)

六、修正金融控股公司及銀行業均須設置法令遵循專責單位，並得兼辦防制詐欺相關事項，金融控股公司及銀行業法令遵循長得兼任防制詐欺專責單位主管。(修正條文第十六條)

七、修正銀行業均須建立全行之法令遵循風險管理及監督架構，並應於設置法令遵循專責單位起二年內報本會備查。(修正條文第十八條)

八、明定金融控股公司及銀行業風險管理架構內涵。(修正條文第二十條)

九、增訂金融控股公司及銀行業應設置風險管理長，並明定風險管理專責單位權責及其隸屬於總經理。(修正條文第二十一條)

十、增訂金融控股公司及銀行業風險管理機制應包含新興風險之辨識、評估及衡量，並採行風險因應策略。(修正條文第二十二條及第二十三條)

十一、增訂金融控股公司亦應設置資訊安全長及隸屬於總經理之資訊安全專責單位，並明定資訊安全長及資訊安全專責單位權責。(修正條文第二十四條及第二十五條)

十二、增訂金融控股公司及銀行業於總稽核異動時，應向主管機關函報原因及異動內容，並應建立獨立董事、審計委員會或監察人(監事、監事會）與內部稽核單位間之溝通管道與機制。(修正條文第二十

七條)

十三、增列國際電腦稽核師得擔任金融控股公司及銀行業內部稽核人員，及放寬聘任屬具備曾任會計師事務所查帳員、電腦程式設計師或系統分析師等專業人員資格條件之稽核人員員額比例上限。(修正條文第二十九條)

十四、增訂內部稽核單位辦理一般查核之內部稽核報告揭露項目包含資訊安全及永續資訊之管理。(修正條文第三十五條)

十五、明定銀行業委託會計師辦理內部控制制度、個人資料保護與防制洗錢及打擊資恐機制專案審查，應提供合理確信之確信報告。(修正條文第四十四條)

十六、發現金融機構重大弊端或疏失應予獎勵者，不限內部稽核人員。(修正條文第五十條)

十七、明定外國銀行在臺分行適用本辦法之彈性規定。(修正條文第五十三條)

十八、有關金融控股公司及銀行業不符下列規定者給予緩衝期至一百十六年十二月三十一日前調整完成，俾利業者因應調整(修正條文第五十四條)：

(一) 第九條、第十條、第十二條第一項第二款第十三目、第十四條、第十六條、第十七條第四項及第五項、第二十條、第二十一條、第二十四條、第二十五條及第三十一條第二項，有關內部控制三道模型、誠信經營守則、營運持續管理機制之訂定、自行查核制度、整併法令遵循自行查核與自行評估作業、設置三長及隸屬於總經理之法令遵循、風險管理、資訊安全專責單位，與風險管理架構、風險管理及資訊安全專責單位權責等。

(二) 第三十五條有關內部稽核報告內容應揭露項目包含永續資訊之管理，考量信用合作社業務單純、人員編制精簡，爰給予緩衝期。

十九、本辦法除第四十四條至四十七條有關委託會計師查核制度施行日期另定之外，自發布日施行。(修正條文第五十五條)