國立臺灣大學法律學院法律學系

碩士論文

Department of Law

College of Law

National Taiwan University

Master Thesis

金融機構公司治理與內部控制——制度與組織之間

Corporate Governance of Financial Institutions and Internal Control: Perspectives on the System and the Organizational Structure

黃信維

Xin-Wei Huang

指導教授：曾宛如 博士

Advisor: Wang-Ruu Tseng, Ph.D.

中華民國 109 年 4 月

April 2020

doi:10.6342/NTU202000744

doi:10.6342/NTU202000744

Memento Vivere

doi:10.6342/NTU202000744

摘要

有鑒於銀行、金融控股公司、保險公司近期層出不窮之裁罰案件在在顯示金融機構未能有效建置或發揮內控制度應有之機能，故基於落實良好之金融機構公司治理之目的，本文即透過內部控制之制度設計、人事組織等兩道途徑之分析與重新形塑，期能具體描繪金融機構內部自律機制應有之典範架構。

首先，本文回顧內部控制之制度發展脈絡後，析出內部牽制、風險控制及權責劃分等三項基本原則，作為改善現行內控制度本身失靈之核心概念。再者，本文以銀行內控制度三道防線基本架構為示例，分析銀行之日常業務經營、報導之編製與揭露、法令規章之遵循等內部控制三項主要目標後，得出法令遵循係內部控制核心目標之觀點。基於前揭觀點，本文透過探討內控制度、法令遵循及風險管理之意涵與彼此間之互動關係後，確立內部控制運作之 GRC 整合架構，並提內部控制程序應納入 PDCA 動態循環之芻議，作為本文對於內部控制制度設計之具體構想。

本文同時點出內控制度之侷限在於人為執行時所生之不利影響，故金融機構內部應重為合理之人事組織安排與權責分配，方能充分發揮內控制度之實效。抑且，現今金融機構之規模與業務種類漸趨龐雜，為落實妥適之權責劃分與營運活動之分工，其內部監督決策與業務執行兩者之組織結構應重新調整。因此本文主張，董事會應定位為監控機關，俾利其履行建置與確保內控制度運作之監督責任，亦得提升獨立董事制度之成效。再者，經營管理階層除了須負擔業務單位職員日常營運活動之管理責任以外，尚須協助具體落實董事會訂定之政策目標、形塑誠信經營之良好組織文化。本文最終指出，內控制度作為確保金融機構運作係符合組織政策、作業程序、具體目標或規範標準之重要治理機制，須經由內部全體成員之通力配合實施與執行，始能完整發揮其制度機能。

關鍵詞：內部控制、金融機構、公司治理、風險管理、法令遵循、監督型董事會

doi:10.6342/NTU202000744

ABSTRACT

The fact that the Financial Supervisory Commission of Taiwan frequently imposes administrative requirements and enforcement on Taiwan's banks, financial holding companies, insurers and so forth, obviously indicates poor corporate governance in these financial institutions. Therefore, after an in-depth examination of the internal control system of financial institutions in Taiwan, its current approach and organizational structure, this thesis aims at outlining an internal corporate governance paradigm that will address the existing problems.

Through examining the history of internal controls, I firstly identify three main principles for a well-functioning internal control system in financial institutions, which are internal checks, risk control, and the delegation of authorization and duties. Then, taking the "Three Line of Defense" principle in banks for example, the focus of the present research will shift to the analysis of the three basic objectives of internal controls: effectiveness and efficiency of operations, preparation and disclosure of reporting, and compliance with applicable rules and regulations. Subsequently, based on the findings that compliance should be the core objective of internal controls, I will discuss the concept of legal compliance and risk management and their cross-relationship with the internal control system. In this regard, I propose that governance, risk management, and compliance ("GRC") should be an essential foundation of a system designing and the "PDCA Cycle" could serve as a feasible methodology for continuous improvement of internal control systems.

This thesis also identifies the limitations of the current internal control system as a result of imperfect execution and proposes that financial institutions should adopt a strong organizational structure with specified roles to fully reap the effectiveness of the internal control system. Furthermore, considering the large scale of modern financial institutions and the diversity of business activities conducted, supervisory and operational roles should be segregated. After surveying internal control system and related best practices, I will deliver three key proposals for improvement: first, reinforcing the position of the supervisory and monitory board in the financial institutions, which will impose upon the

doi:10.6342/NTU202000744

board of directors the ultimate responsibility of ensuring the establishment and maintenance of an appropriate and effective internal control system, and at the same time improving the function of the independent director system; second, other than managing the businesses' daily operations, the management should also play a main role in reinforcing good culture in financial services and continually educating personnel regarding policies, procedures, and ethical standards in place; lastly, this thesis submits that since an effective internal control system is essential to good corporate governance, the burden of ensuring that it works effectively should not only rest on the shoulders of the management, but also on all employees.

KEYWORDS: *Internal Control, Financial Institutions, Corporate Governance, Risk Management, Legal Compliance, Supervisory Board*

doi:10.6342/NTU202000744

簡目

doi:10.6342/NTU202000744

doi:10.6342/NTU202000744

doi:10.6342/NTU202000744

詳目

doi:10.6342/NTU202000744

doi:10.6342/NTU202000744

doi:10.6342/NTU202000744

doi:10.6342/NTU202000744

doi:10.6342/NTU202000744

表目錄

doi:10.6342/NTU202000744

第一章 緒論

第一節 研究動機

第一項 失靈的內控制度

為期促進金融機構之健全經營，並確保合理達成其營運之效果及效率、報導之忠實與即時及相關法令規章之遵循等目標[1]，銀行、金融控股公司（以下簡稱金控公司）、保險業、證券商、信用合作社、票券金融公司等金融機構，應以董事會與經理人為主軸，於組織內部建置內部控制及稽核制度[2]。茲以銀行與金控公司為例，其內部控制制度（以下簡稱內控制度）具體包括業務自行查核制度、法令遵循制度與風險管理制度及內部稽核制度等「三道防線」[3]，同時董事會並應確保各該制度之建立與維持其適當有效之運作[4]，俾利內控制度得發揮協助組織達成經營目標、降低風險成本、遵循法規命令等興利防弊、公司治理之機能[5]。

抑且，除了健全金融機構業務經營之目的外，為維持金融穩定與金融市場交易秩序，以及促進金融市場發展[6]，銀行、金控公司等金融機構之主管機關，即金融監督管理委員會（以下簡稱金管會）依法具有金融檢查權[7]、緊急處分權、指定輔

---

[1] GEOFFREY PARSONS MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 3 (2014).

[2] 具體而言，證券交易法第 14 條之 1 第一項；銀行法第 45 條之 1 第一項；金融控股公司法第 51 條；保險法第 148 條之 3 第一項；票券金融管理法第 43 條；證券投資信託及顧問法第 17 條之 1 第二項、第 93 條；期貨交易法第 97 條之 1 第一項；信用合作社法第 21 條第一項；信託業法第 42 條第二項；郵政儲金匯兌法第 10 條；電子支付機構管理條例第 30 條及電子票證發行管理條例第 17 條第二項等金融相關法令規範，基本上均要求該法人或金融機構應建立財務、業務相關之內部控制制度。抑且依據各金融業法規定，包括銀行、金融控股公司〔以下簡稱金控公司〕、票券商、保險業、信用合作社、信託業、中華郵政股份有限公司、電子支付機構及電子票證發行機構等金融機構，尚應建立內部稽核制度。

[3] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 6 條。

[4] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1。

[5] *See* MILLER, *supra* note 1, at 4.

[6] 金融監督管理委員會組織法第 1 條〔以下簡稱金管會組織法〕。

[7] 如銀行法第 45 條第一項規定，中央主管機關〔即金融監督管理委員會，以下簡稱金管會〕得隨時派員，或委託適當機關，或令地方主管機關派員，檢查銀行或其他關係人之業務、財務及其他有關事項，或令銀行或其他關係人於限期內據實提報財務報告、財產目錄或其他有關資料及報告。關於金融檢查權之意涵與具體說明，可參考：王志誠（2014），《銀行法》，頁 250-252，臺北市：新學林。

doi:10.6342/NTU202000744

導權[8]等外部監理之行政權限[9]。質言之，銀行若未依規定建立或未確實執行內部控制與稽核制度、內部處理制度與程序、內部作業制度與程序等，金管會除得處銀行以新臺幣二百萬元以上五千萬元以下罰鍰之外[10]，倘若其認為銀行未妥適建立內控制度或核有未確實執行內控制度之缺失，致有礙健全經營之虞時，即得行使緊急處分權，予以糾正或命限期改善，或視情節輕重程度為停止部分業務，或解除董事、監察人、經理人或職員之職務或停止其於一定期限內執行職務等必要之處置[11]，以加強金融紀律化，並保障存款大眾之權益，俾導正銀行健全之經營[12]。

然而，觀諸由金管會所公告之金融機構裁罰案件[13]，金融機構因未妥適建立與確實執行內控制度，或未落實執行內部作業程序等情事，招致金管會處以罰鍰或命解除職務或停止業（職）務等裁罰者，無論各該處分結果係重大裁罰或非重大裁罰[14]案件者，其行為類型均所在多有。詳言之，以重大裁罰案件為例，其行為態樣或有銀行內部未確實建立與執行業務分工與業務文件控管覆核機制等內控制度，致使銀行辦事員濫用執行業務之便，私自挪用客戶款項或偽冒貸款[15]。或有銀行未依個別交易員之授權額度，於交易策略部位設定交易上限與停損機制，同時並無配置覆核人員以檢視交易員額度與設置監控交易等牽制控管機制，且金融交易系統、交易員部位控管平台及中後台作業單位均未能即時以系統化或線上監控方式，有效

[8] 如銀行法第 61 條之 1 第三項規定，為改善銀行之營運缺失而有業務輔導之必要時，主管機關得指定機構辦理之。

[9] 金管會組織法第 2 條、第 3 條。

[10] 銀行法第 129 條第七款。

[11] 銀行法第 61 條之 1。

[12] 周伯翰（2017），《銀行法暨金融控股公司法》，頁 48-49，臺北市：元照；王志誠，前揭註 7，頁 255。

[13] 依據金管會組織法第 11 條授權訂定之《金融監督管理委員會處理違反金融法令重大裁罰措施之對外公布說明辦法》第 2 條規定，金融服務業違反金融法令，經金管會處以命令解除、解任董事、監察人、經理人或受僱人職務、或停止前述之人全部或部分職權等重大裁罰措施者，應依同辦法第 3 條與第 4 條之規定，於處分書發文日當日，應於金管會網站公布包括裁罰時間、受裁罰之對象、裁罰之法令依據、違反事實理由及裁罰結果等裁罰措施之內容。金融監督管理委員會網站，〈裁罰案件〉，https://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2（最後瀏覽日：05/13/2019）。

[14] 金管會銀行局網站，〈非重大裁罰〉，https://www.banking.gov.tw/ch/home.jsp?id=175&parentpath=0,2,54（最後瀏覽日：05/15/2019）。

[15] 行為態樣屬銀行辦事員私自挪用客戶款項之重大裁罰有民國（下同）108 年 3 月 26 日金管銀控字第 10702224341 號處分、107 年 10 月 25 日金管銀控字第 10702002191 號處分、107 年 2 月 1 日金管銀外字第 10702703731 號處分、106 年 12 月 19 日金管銀國字第 10620006841 號處分、106 年 10 月 26 日金管銀票字第 10640004421 號處分、106 年 9 月 27 日金管銀國字第 10620004841 號處分、106 年 7 月 6 日金管銀國字第 10620003161 號處分等。

doi:10.6342/NTU202000744

控管交易員下單等行為，更未能實際發揮警示、揭露或超限通知等內控制度應有之檢核與牽制機能[16]。又或銀行於辦理貸款、專案融資等業務時，除未能落實辦理徵信、授信作業之外，尚有貸後管理機制未臻健全，造成徵信報告未充分揭露、高估鑑價金額及資金往來異常等情事發生，核有未建立與未確實執行內控制度之缺失，致使主管階層未能善盡確實覆核督導等公司治理之責，以有效控制風險於可承受範圍之內[17]。抑或金控公司未於內部建立清楚適當之法令規章傳達、溝通及諮詢管道，法務與法遵主管亦未適時提供專業法令諮詢意見，核有未確實執行法令遵循與內控制度之缺失，致公司曝露於違法之風險，有害公司治理之落實[18]。甚或銀行資安防禦機制未完整建置、系統管理者帳號之使用管理與資安事件緊急應變之處理程序欠當，並未落實執行強化自動櫃員機（ATM）監控管理系統伺服器或 SWIFT 系統安全，以致發生駭客入侵內部伺服器資料庫或植入惡意程式等情事時，未能有效清查數據資料與傳輸途徑，亦不利確認個資是否外洩等個資安全性[19]。職是之故，**吾等似得窺知且無妨大膽假設於實際運作上，內控制度或恐未能有效發揮（或被用於落實）其應有之功能與目的**。

除前述個案性之重大裁罰案件外，包括法令遵循、風險管理及洗錢防制在內之內控制度等公司內部自律機制，以及內控制度對公司治理之重要性逐漸受到關注與討論者，無非肇因於「兆豐國際商業銀行（以下簡稱兆豐商銀）裁罰案」所凸顯

[16] 行為態樣屬內控制度未能發揮內部交易牽制與控管之重大裁罰有 107 年 6 月 27 日金管銀控字第 10701079801 號處分、106 年 10 月 26 日金管銀票字第 10640004421 號處分等。

[17] 行為態樣屬未建置與未落實執行徵信、授信及貸款業務相關內控制度之重大裁罰有 107 年 6 月 26 日金管銀合字第 10702725361 號處分，其中備受矚目者方屬「慶富造船公司獵雷艦聯貸案（106 年）」，該案所涉銀行家數甚多，且均於同年 12 月 29 日由金管會為重大裁罰處分，包括臺灣銀行（金管銀控字第 10660006107 號處分）、高雄銀行（金管銀控字第 10660006105 號處分）、合作金庫（金管銀控字第 1066000610F 號處分）、華南商銀（金管銀控字第 1066000610D 號處分）、中小企業銀行（金管銀控字第 1066000610B 號處分）、兆豐商銀（金管銀控字第 10660006109 號處分）、第一商銀（金管銀控字第 10660006101 號處分）及土地銀行（金管銀控字第 10660006103 號處分）等八家銀行，金管會分別對各銀行作成新臺幣（下同）200 萬至 1,000 萬元罰鍰與解除部分銀行辦事員之職務等處分。

[18] 行為態樣屬未建置與未落實執行法令遵循內控制度之重大裁罰有 106 年 12 月 5 日金管銀控字第 10600291713 號處分、106 年 12 月 5 日金管銀控字第 10600291711 號處分。

[19] 行為態樣屬資安內控制度缺失之重大裁罰有 106 年 12 月 15 日金管銀國字第 10620006681 號處分、106 年 11 月 28 日金管銀控字第 10660003651 號處分、105 年 9 月 12 日金管銀控字第 10560003721 號處分。

doi:10.6342/NTU202000744

出內控制度「失靈」對於金融機構公司治理所帶來之衝擊與負面影響[20]。簡言之，該案係萌發於 2016 年 2 月 9 日，時值美國紐約州金融服務署（New York State Department of Financial Services, hereinafter "DFS"）作成金融檢查報告指出，兆豐商銀紐約分行於 2012 年之匯款交易在法令遵循、洗錢防制及可疑交易申報（Suspicious Activity Report，SAR）上，違反美國銀行保密法與洗錢防制法（BSA/AML）。於同年 8 月 19 日，DFS 即公布合意處分令（Consent Order）裁罰兆豐商銀 1.8 億美元，並要求其應改善包括法令遵循與洗錢防制在內之內控制度[21]。該份文件指出，兆豐銀行的內控制度相當「差勁」(poor)，且各該專責單位之負責人不僅訓練不足，對於美國金融等相關法令規範亦缺乏專業認知，甚至有身兼數職以致權責紊亂、利益衝突等狀況發生，種種因素顯示兆豐商銀內部法令遵循、洗錢防制及風險管理等機制存在諸多闕漏[22]。

依據證券交易法之規定，公開發行公司應建立財務、業務之內控制度[23]。所謂「內控制度」係指由經理人考量公司整體之營運活動後所設計，並經董事會通過，由董事會、經理人及其他員工確實執行之管理過程，其目的在於促進公開發行公司之健全經營，以合理確保營運之效果及效率、相關法令規章之遵循，以及公司報導詳實等目標之達成[24]。抑且，公開發行公司應隨時檢討內控制度，以因應公司內外在環境之變遷，俾確保該制度之設計與執行係持續有效[25]。然而，近期大型上市(櫃)

[20] 蔡昌憲（2018），〈從公司法第一條修正談公司治理之內外部機制——兼論企業社會責任的推動模式〉，《成大法學》，36 期，頁 95-153；郭大維（2017），〈我國銀行法令遵循制度之探討——從兆豐銀行紐約分行遭美國重罰事件談起〉，《存款保險資訊季刊》，30 卷 1 期，頁 1-29；王志誠（2016），〈董事之監督義務——兆豐銀行遭美國紐約州金融服務署裁罰一．八億美元案之省思〉，《月旦法學雜誌》，259 期，頁 5-18；林仁光（2016），〈由兆豐銀案談銀行監理——由銀行治理及銀行保密法之遵循出發〉，《月旦法學雜誌》，259 期，頁 19-33；林志潔（2016），〈兆豐案天價罰款的啟示——美國反洗錢法的重點與金融業應有的作為〉，《月旦法學雜誌》，259 期，頁 34-48。

[21] Press Release, *DFS Fines Mega Bank $180 Million for Violating Anti-Money Laundering Laws: Consent Order Requires Bank to Establish Effective Compliance Controls and to Retain Independent Monitor for Two Years*, N.Y. STATE DEP'T FIN. SERVS. (Aug. 19, 2016), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1608191.

[22] N.Y. STATE DEP'T OF FIN. SERVS., CONSENT ORDER UNDER NEW YORK BANKING LAW §§ 39 AND 44 ¶¶ 6-12 (2016), https://www.dfs.ny.gov/docs/about/ea/ea160819.pdf; *see also* Yi-Chin Ho et al., *New York State Department of Financial Services Fines Mega Bank and Its New York Branch $180 Million for Alleged Violations of State Anti-Money Laundering Laws*, KIRKLAND & ELLIS (Nov. 2016), https://www.kirkland.com/siteFiles/Publications/NYDFS_Fines_MegaBank_Eng.pdf.

[23] 證券交易法第 14 條之 1。

[24] 公開發行公司建立內部控制制度處理準則第 3 條、第 5 條。

[25] 公開發行公司建立內部控制制度處理準則第 5 條。

doi:10.6342/NTU202000744

公司之經營或財務危機案例，主要均係公司未能妥適建置、或維持內控制度整體之有效運作所導致。金管會針對兆豐商銀遭 DFS 裁罰美金 1.8 億元一案作成之處分書即認為，兆豐商銀存在經營管理功能不彰，未落實建立且未確實執行內控制度之缺失，有礙健全經營之虞，再對其核處新臺幣一千萬元罰鍰，並命解除董事、總經理、總稽核及法遵長等人之職務[26]。

銀行之內控制度，乃是其內部公司治理架構下興利與防弊兼容的第一線。內部控制的功能在於透過制度設計，建立自我評估、自我控制、自我稽核等自律機制，從而由內部落實公司治理之目的[27]。惟銀行與其他金融機構作為「高度管制產業」（highly regulated industry），長久仰賴金融主管機關（即金管會）之外部金融監理與管制，其發展因深受不同時期政府的金融發展措施與金融改革之影響，致使金融機構之公司治理並未受到相應充分之重視[28]。復以上述兆豐商銀案為例，董事會未能落實海外分支機構法令遵循與洗錢防制內控制度之建立與督導、董事會與高階管理階層亦未能確實瞭解其所犯之缺失與風險，種種內控制度「失靈」之現象背後所突顯者，實為金融機構之公司治理存在諸多缺失，或有改進之空間。

第二項 堆砌的專責單位

首先基本定義上，內控制度指由董事會、管理階層及所有從業人員共同遵行之管理過程，其目的在於合理確保達成營運之效果及效率、報導符合標準規範、法令規章之遵循等三大目標，據以促進銀行之健全經營[29]。具體而言，適當有效之內控制度應具備「三道防線」（Three Lines of Defense）架構[30]：第一道防線為銀行內各業務單位就其日常營運所生個別風險之自行查核；第二道防線則為風險管理、法令

[26] 105 年 9 月 14 日金管銀控字第 10560003851 號、第 10560003852 號處分。

[27] 林仁光（2004），〈論經營者誠信、內部控制、內部稽核制度與公司治理〉，《月旦法學雜誌》，106 期，頁 40。

[28] 郭大維（2008），〈論我國金融機構公司治理之強化〉，《台灣金融財務季刊》，9 輯 4 期，頁 48。銀行業之發展歷程得作為臺灣金融體系發展與逐步成形之觀察對象，臺灣金融發展階段之變遷概略可分為金融體制形成初期、金融管制期、金融開放期、金融整併期及海外拓展期等五個時期，為求金融體系得維持健全且穩定之狀態，政府的政策措施與金融主管機關的規範管制等外部監理手段，對於金融機構之經營與發展，實際上亦具有主導性的影響。關於臺灣金融體系與銀行業發展歷程之詳細介紹與說明，請參照：楊雅惠、許嘉棟（2014），《台灣金融體制之變遷綜觀》，頁 2-11-2-31，臺北市：財團法人臺灣金融研訓院。

[29] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條。

[30] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 6 條。

doi:10.6342/NTU202000744

遵循及其他專責單位，除了協助與監督第一道防線辨識與管理風險外，各專責單位並應就各主要風險類別整體，負責銀行內風險管理；第三道防線係內部稽核單位，其應獨立執行稽核業務，查核與評估前述兩道防線之有效性，並協助董事會與高階管理階層評估內控制度是否有效運作[31]。

基此，銀行內控制度三道防線之架構實已明確釐清各單位人員之職責與權限範圍，倘若銀行之董事會、經營管理階層及各業務或專責單位均能充分瞭解其等在整體風險控制架構之下，各自所扮演之角色且各司其職，原則上即可合理確保銀行所有營運活動均符合內控制度之制度目的。惟如前述，現行實務運作上仍不乏銀行因內控制度本身「失靈」，抑或未能有效建置或落實，導致業務行為違反相關法令規範或風險管理不佳之案例，造成金融機構本身或投資人之損失。職是之故，內控制度之規範架構是否有所不足或存在應予以調整修正之處，以致於未能充分發揮內控制度本身眾所期盼之功能，本文認為容有重新檢討之必要。

抑且，吾等若進一步觀察內控制度第二道防線之發展，或可察覺該防線於專責單位之設置情形，似有愈發「肥大化」之趨勢。質言之，銀行內控制度第二道防線原則上應設置者，為職司法令遵循與風險管理之專責單位──前者係負責法令遵循制度之規劃、管理及執行，並應設置法令遵循主管以綜理遵循事務[32]；後者則就各主要風險類別整體，專門負責並協助董事會為銀行之風險管理，故其應定期向董事會提出風險控管報告，惟若發現重大曝險，危及財務或業務狀況或法令遵循者，即應立即採取適當措施並向董事會報告[33]。除前述兩專責單位外，第二道防線更逐步囊括洗錢防制與資恐打擊、資訊系統安全及個人資料保護等專門領域之職務與功能，容後分述。

洗錢防制（anti-money laundering，AML）與資恐打擊（combating the financing of terrorism，CFT）係近年國際社會間高度重視之金融法制議題。又臺灣為「亞太洗錢防制組織」（Asia/Pacific Group on Money Laundering, hereinafter “APG”）創始會員，為履行遵守國際標準之承諾，打擊洗錢活動與恐怖主義之融資，並因應 APG 相互評鑑，同時與「防制洗錢金融行動小組」所提之四十項建議充分接軌，法務部、

[31] 銀行內部控制三道防線實務守則第 3 條至第 5 條。

[32] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條。

[33] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 36 條。

doi:10.6342/NTU202000744

金管會及各金融機構自律組織均展開相關法規與自律規範之研擬修訂。此外，前述兆豐商銀遭美國金融主管機關裁罰高額罰款，不僅曝露出金融機構對於洗錢防制規範未充分瞭解，且法令遵循架構規範之標準亦有不足。故於兆豐商銀案發生後，金管會即參酌國際準則與外國立法例修訂相關辦法，規定符合金管會所定資產達特定總額以上者，應設置洗錢防制與資恐打擊之專責單位及主管，辦理相關洗錢與資恐相關事項[34]。

再者，伴隨金融科技（FinTech）、互聯網金融等科技與金融結合之新型態金融模式之起興，運用雲端計算（cloud computing）、社交網絡（social network）、大數據（big data）、數據挖掘（data mining）等技術，提供更為便捷之金融服務成為時下發展趨勢[35]。為因應互聯網金融、科技業者對於傳統金融業所帶來之衝擊與挑戰，傳統金融業之經營與服務模式開始朝向數位化、網路化發展[36]，資訊安全治理（Information Security Governance）議題亦逐漸受到重視。由於資訊係屬公司重要資產之一，資訊安全治理除了在於保護公司內部所有資訊、維持資訊保密性、規範資訊接近使用權限以外，亦在於預防網路駭客攻擊、惡意軟體，以及管理資訊滅失、不當使用或揭露等各種風險[37]。另一方面，由於第一銀行 ATM 盜領案等大型金融機構金融資訊安全事件頻繁發生，金管會為提升銀行業之資訊安全意識，故修訂相關辦法，強制要求銀行內部應設置資訊安全專責單位及主管[38]，專門負責規劃、監控及執行資訊安全相關作業[39]，且基於銀行業務推動與資訊安全控管兩者衡平性之考量，原則上資安專責單位及其主管須獨立行使職權，不得兼辦資訊業務[40]。

附值一提，於永豐金控案件後，金管會為協助銀行建立透明、誠信之企業文化，鼓勵內部員工主動檢舉不法行為，以收防微杜漸、避免擴大損及商譽與保障公共利益之效，復規定銀行內部應建立具獨立性之單位，負責檢舉案件之受理及調查（即吹哨者保護機制）[41]。若循此發展脈絡以觀後效，似可預期歐盟實施「一般個人資

[34] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條。

[35] 王志誠（2017），《互聯網金融之監理機制》，頁 118-119，臺北市：新學林。

[36] 同前註。

[37] IT GOVERN. INST., INFORMATION SECURITY GOVERNANCE: GUIDANCE FOR BOARDS OF DIRECTORS AND EXECUTIVE MANAGEMENT 15 (2d ed. 2006).

[38] 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 條之 1 第 1 項。

[39] 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 條之 1 第 3 項。

[40] 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 條之 1 第 2 項。

[41] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條之 2 及本條立法說明。

doi:10.6342/NTU202000744

料保護規範」（General Data Protection Regulation，GDPR）後，為符合或回應國際間對於個人資料保護愈加重視之潮流，立法者或金管會恐再次制定或修訂相關辦法，要求銀行、金控公司等金融機構應設置個人資料保護相關專責單位或主管[42]，進而促成內控制度第二道防線專責單位之「蓬勃發展」。

第三項 未竟的人事責任

吾等得以內控制度之專責單位（機構）作為探究其發展的其中一個觀察點，惟若由人事面向淺析金融機構內部不同組織階層之成員間，其等在內控制度運作過程中扮演之角色及其影響。本文初步認為就此面向，或存有董事責任愈發「模糊」之趨勢、未能有效制約業務單位職員之行為等兩點疑慮，以下分述之。

第一款 董事會成員

為促進銀行業之健全經營，完善其內部治理機制，銀行之董事會應考量實際營運狀況，決議通過內控制度之建置並確保其有效運作[43]。銀行之內控制度係以自行查核制度、法令遵循制度與風險管理機制及內部稽核制度（以下簡稱內稽制度）等內部控制三道防線為基礎架構[44]，具體包括營運政策及作業程序[45]、法令遵循單位與制度[46]、風險管理政策與程序[47]、內稽制度及業務單位自行查核制度等。基此，銀行之董事會負有建立與維持適當有效之內控制度之責任[48]，應本於善良管理人之注意義務，為銀行量身定作適當之規範基礎架構[49]。再者，銀行之董事會亦應認知營運所面臨之各種風險，監督其營運結果，倘若董事發現銀行有受重大損害之虞時，應儘速妥適處理，立即通知審計委員會成員並應提報董事會且應督導所屬銀行通報主管機關[50]。

---

[42] 聯合報（05/26/2018），〈歐盟 GDPR 上路了 金管會要求銀行落實個資保護〉，https://udn.com/news/story/11316/3162994。

[43] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條。

[44] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 6 條。

[45] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 8 條。

[46] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條。

[47] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 35 條。

[48] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條、第 5 條之 1。

[49] 王志誠（2017），《現代金融法》，三版，頁 96，臺北市：新學林。

[50] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條之 1。

doi:10.6342/NTU202000744

詳之，就風險管理機制而言，銀行內部應設置獨立且直接隸屬於董事會之專責風險控管單位，並由董事會通過訂定適當之風險管理政策與程序，建立獨立有效之風險控管機制，以評估及監督整體風險承擔能力、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[51]。故董事會對風險管理專責單位負有義務與責任，應定期審閱由該單位提出之風險控管報告或針對重大曝險之措施報告[52]。再就法令遵循制度而言，縱然法令遵循單位係隸屬於銀行總機構之總經理，惟綜理法令遵循之法令遵循主管係直接對口於董事會，故董事會亦負有義務與責任定期聽取法遵主管就法令遵循制度之規劃、管理及執行等事項之提報[53]。

抑且，由於金管會強制要求銀行之董事會須建立洗錢防制與資恐打擊之內控制度，且應包括風險相關政策與程序、防制洗錢及打擊資恐計畫、監督控管之標準化作業程序等[54]。董事會即負有最終責任，應建立與維持適當有效之洗錢防制與資恐打擊內控制度[55]。準此，董事會（與高階管理階層）應充分瞭解洗錢與資恐風險，採取相關計畫與措施，以期塑造重視洗錢防制與資恐打擊之金融機構組織文化[56]。另外，由於資訊安全治理實與公司日常營運活動及風險管理息息相關，故董事會對於資訊資產、資訊系統及資訊安全治理等相關內控制度之建立與確保其有效運作，亦應負有相當責任[57]。

綜上所述，吾等得認董事會在內控制度扮演重要角色。首先，董事會負有內控制度及其相關專責單位之建置責任，並應承擔內控制度有效運作之最終責任。再者，董事會應認知營運所面臨之風險，以對於營運結果履行監督責任。惟若有董事發現其所屬銀行受有重大損害之虞時，其除應儘速妥適處理外，亦應立即通知審計委員會並提報至董事會，且應督導該銀行通報金管會。此外，由於內部稽核、法令遵循、風險控管、資訊安全等專責單位，係直接或間接隸屬於董事會，故董事會尚

---

51 金融控股公司及銀行業內部控制及稽核制度實施辦法第 35 條。

52 金融控股公司及銀行業內部控制及稽核制度實施辦法第 36 條第 1 項。

53 金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條第 1 項。

54 銀行業及其他經金融監督管理委員會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法〔以下簡稱銀行業防制洗錢及打擊資恐內部控制與稽核制度實施辦法〕第 6 條第 1 項。（本條立法理由第一點指出：各類金融機構之內控制度，應涵蓋防制洗錢及打擊資恐之相關政策及程序，且該內控制度應經董事會通過。）

55 銀行業防制洗錢及打擊資恐內部控制與稽核制度實施辦法第 6 條第 6 項前段。

56 銀行業防制洗錢及打擊資恐內部控制與稽核制度實施辦法第 6 條第 6 項後段。

57 *See* IT GOVERN. INST., *supra* note 37, at 21 & 45.

doi:10.6342/NTU202000744

負有定期或必要時，聽取各單位提報或審閱其所提交之書面報告之義務。董事長亦須協同總經理、總稽核及法令遵循與資訊安全兩單位之專責主管，簽署並出具「內部控制制度聲明書」與「資訊安全整體執行情形聲明書」等文件予金管會，並應擔負相關法律責任。準此，相較於傳統上咸認為董事會主要應負責公司業務之執行，董事之責任範圍與專業要求，似隨著內控制度之演進或有逐漸加重之趨勢，惟個別董事本身的義務內涵，以及能力得否充分因應其所應履行之內控制度相關責任與義務，即有須重新予以檢視之空間。

第二款　業務單位職員

內部控制或謂係落實公司治理目標之管理過程[58]，故董事會與經理人負責制訂之內部行為準則、風險評估程序、資訊取得機制等內控制度相關政策[59]，均仍須由董事會、經理人及各業務單位職員於銀行內部、自上而下予以具體落實，始竟其功，惟自前述本文所探討之內控制度相關裁罰案件中顯示，銀行業務單位職員未能確實遵循內控制度所設規範，亦屬導致該制度失靈之重要原因。舉例言之，金管會作成重大裁罰案件之事由中，不乏係因銀行辦事員或理財專員於日常業務執行時，利用客戶告知密碼或交付存摺或印鑑之便，或於執行臨櫃交易時，私自盜領或挪用客戶款項[60]。或有銀行金融交易系統之個別交易員未依其所獲授權之下單與成交額度操作策略部位，導致累計交易部位超逾該策略部位之授權額度，抑且銀行內部控管平臺與中後臺作業單位對前述超限交易行為，均未為超限通知或未實際發揮警示等檢核功能[61]。質言之，金管會銀行局於 2019 年 5 月指出，統計自 2012 年開始所作成之重大與非重大裁罰處分當中，銀行辦事員或理財專員不當挪用客戶資金之相關案件即有 24 件，涉及 17 家銀行（佔現有銀行總家數之六成）、共有 24 名銀行職員遭解職處分、裁罰金額總計高達新臺幣 8,600 萬元[62]。

---

[58] *See* COMM. ON SPONSORING ORGS. OF TREADWAY COMMISSION [COSO], INTERNAL CONTROL—INTEGRATED FRAMEWORK 9 (1992).

[59] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條。

[60] 例如：108 年 3 月 26 日金管銀控字第 10702224341 號處分、107 年 10 月 25 日金管銀控字第 10702002191 號處分。

[61] 例如：107 年 6 月 27 日金管銀控字第 10701079801 號處分。

[62] 其中依裁罰件數排名前三之銀行分別為高雄銀行（共 4 件，罰鍰 1,400 萬元）、土地銀行（共 3 件，罰鍰 700 萬元）、渣打銀行（共 2 件，罰鍰 900 萬元）與台北富邦銀行（共 2 件，罰鍰 600 萬元）則並列第三。工商時報（05/10/2019），〈理專頻出包 顧立雄：銀行輕忽就重罰〉，https://www.c

doi:10.6342/NTU202000744

準此，金管會早於 2018 年初即曾發函要求各金融機構均應就存款業務、金融商品銷售業務及授信業務等三種常見金融機構內部舞弊與缺失之態樣，管理階層應負責檢討內控制度是否有所不足、注意內部作業流程是否符合牽制原則，並應確實督導業務單位落實執行各項作業規範[63]。然而，由上揭因業務單位職員未能遵循內控制度而遭到金管會作成各式處分之情形來看，縱謂依據銀行法第 45 條之 1 第一項與其他內控制度相關法令規定，係董事會與經理人負起建置與制定內控制度及其相關政策之責任，惟常言道：「徒法不足以自行」，內控制度仍須銀行內部各該營業與業務單位職員之配合實踐，方能充分發揮制度應有之作用。職是之故，本文析述內控制度於現實運作之結果後認為，銀行內控制度之不彰與失靈，除應予檢討前述董事會、經理人等高階管理階層成員之責任外，諸等位居前線之業務單位各該職員似亦難辭其咎。

第四項 小結

經內部控制之制度與人事兩層面之初步分析，本文認為，目前銀行之內控制度存有制度本身未能充分發揮實效、頻繁增設專責單位、或有過度仰賴董事會之虞等問題。首先，概覽近期凸顯金融機構之公司治理有待強化或改革的案件，多係肇因於內控制度「失靈」，導致未能建置或落實法令遵循制度[64]，或無法有效地偵測及預防可能發生的問題所致[65]，且此問題數見不鮮[66]。作為於外部受到金融主管機關

---

hinatimes.com/newspapers/20190510000324-260205?chdtv；自由時報（05/09/2019），〈銀行理專、行員 A 錢 7 年半共 24 件 這家銀行被罰最多〉，https://ec.ltn.com.tw/article/breakingnews/2785136；經濟日報（05/09/2019），〈理專及行員挪用客戶資金 件數及被罰金額最多是這幾家銀行〉，https://money.udn.com/money/story/5613/3803308；鉅亨網（05/09/2019），〈7 年來 24 名理專監守自盜 金管會共開鍘 8600 萬元 這 4 家銀行罰最多〉，https://news.cnyes.com/news/id/4317442。

[63] 107 年 1 月 23 日金管檢銀字第 1070604007 號函。舉例來說，（一）存款業務為銀行辦事員是否私自將存款戶印鑑預先加蓋於空白取款憑條、或利用代替未臨櫃之客戶為交易之際，伺機挪用客戶之存款或資金。（二）金融商品銷售業務為理財專員是否有以不法方式取得客戶網路銀行帳號與密碼，並於代客戶申請網路銀行業務時，私自挪用客戶資金。抑或銀行內部針對理財專員與客戶於短期間使用相同行外 IP 為網路銀行基金交易之異常情事，並未建立檢核與即時確認或通知機制。（三）授信業務為銀行辦事員盜領債權憑證與抵押權塗銷同意書、盜用分行印信印章，以偽造塗銷與偽為設定銀行抵押權。抑或偽刻客戶印鑑、偽造簽名以偽冒客戶辦理貸款。

[64] 蔡昌憲，前揭註 20，頁 95；中央銀行（2017），《強化我國金融業公司治理並對兆豐案及永豐案後續之調查結果》，https://www.cbc.gov.tw/public/Attachment/710213481271.pdf.

[65] ERIK BANKS, CORPORATE GOVERNANCE: FINANCIAL RESPONSIBILITY, CONTROLS AND ETHICS 8 (2004). (“[I]neffective internal controls that cannot detect or prevent problems.”)

[66] 蔡昌憲，前揭註 20，頁 95。

doi:10.6342/NTU202000744

監管之金融機構，惟因銀行之基本組織型態係屬股份有限公司，故其內部公司治理亦須予以重視。內控制度即公司治理機制下重要之內部自律機制[67]，倘若內控制度未能充分發揮其制度機能，亦難謂得有效達成良好之公司治理。準此，本文期能藉由探究「內部控制」之本質與特性，據以分析內部控制相關制度與規範是否有所缺漏或未臻完備之處，並嘗試提出改革或調整之淺見。

再者，觀察目前金融主管機關對於銀行內控制度規範之發展態勢，通常係遇到特定問題或重大案件時，即要求銀行應設置直接對口至董事會之專責單位。例如：因兆豐商銀案之發生，凸顯銀行內控制度於洗錢防制之不足，金管會即要求董事會應於法令遵循單位下，設置洗錢防制與資恐打擊之專責單位並指派專責主管。復因第一銀行 ATM 盜領案，引起各界對於資訊安全之重視，金管會遂規定銀行應設置資訊安全專責單位，且該單位應獨立行使職權，不得兼辦資訊相關業務。又因永豐金控遭「吹哨者」揭露弊案後，為鼓勵銀行從業人員勇於檢舉內部之不法行為，以督促銀行建立透明、誠信之企業文化及健全經營，保障銀行、員工乃至於社會大眾之公共利益，金管會即要求銀行應於內部具職權行使獨立性之單位，建立內部檢舉制度，並提報董事會通過。惟若進一步分析此脈絡即可略知，金管會均係以相同或類似之規定，重複使用在不同或現時所欲處理的議題之上。然而，如此巡迴往復之手段是否得以有效解決此些問題？又倘若未來再遇到特定的問題時，是否又要依循成立專責單位之慣例，以茲因應[68]？固然專責單位具有相當專業性，得依其專業知識與能力處理特定諸問題，惟本文以為，內控制度本身仍有先天上之限制，尤以內控制度之建置與運作須投入必要之成本與資源，倘若不斷增加設置各式專責單位於內控制度，是否均能夠獲致預期之效益，非謂無疑[69]。

最後，董事之責任範圍亦隨著內控制度不斷演進的過程逐漸加重，惟個別董事本身的能力與專業是否足以充分因應其所應履行之義務，亦須重新予以評估。觀諸內控制度相關規定，除董事負有建置、運作內控制度之責任以外，尚且要求董事應

[67] 廖世昌、郭姿君（2017），〈現行金融業法令遵循制度概況簡介〉，《月旦會計事務所 CPA 雜誌》，創刊號，頁 101。

[68] 例如前述歐盟 GDPR 之實施後，再次喚起對於個人資料保護之重視，金管會後續對此可能的具體作法即值得關注。

[69] *See* STEVEN J. ROOT, BEYOND COSO: INTERNAL CONTROL TO ENHANCE CORPORATE GOVERNANCE 140-41 (1998).

doi:10.6342/NTU202000744

認知營運所面臨之風險，或聽取各單位之業務報告，並應對於內控制度之建立與有效維持，擔負最終責任。然而，從第二道防線不斷設置專責單位之現況顯示，目前金融機構內部風險與內控制度之機構組織呈現愈趨複雜、專業化，董事本身是否具備足夠的專業知能，得以承擔該等責任與義務？抑且，倘若肯認董事對於內控制度負有監督義務，惟所謂監督義務之具體意涵，在目前相關法制與實務案例發展中，於既有之董事忠實義務（或謂受託人責任）體系架構下，似尚未有較為明確之闡釋與判準，故應有予以探究之必要。另查，銀行業務單位之辦事員或理財專員等因違反內部控制相關法規，遭金管會課予罰鍰或作成命銀行解除其職務之處分等情，如何於金融機構內部「由下而上」徹底落實內部控制之制度目的與精神，或如何提升各成員對於遵循與重視內控制度之誘因，均為該制度是否得以有效達成良好金融機構公司治理之重要關鍵，故亦屬本文所欲處理之問題。

第二節　研究目的

第一項 再探內部控制之制度與組織架構

銀行法規定銀行之設立，除法律另有規定或銀行法修正施行前經專案核准者外，應以股份有限公司之法人組織型態為限。抑且，銀行作為金融機構，其公司治理機制概可分為外部監督與內部自律兩者，前者包括金融主管機關之行政監理、立法者規範、司法裁判及市場監督機制等；後者則包括風險管理、法令遵循及內部稽核等。實言之，銀行之內控制度即係為確保內部自律機制有效運作之具體制度設計[70]，故內控制度本身是否經妥善建置並有效運作，或可謂係與銀行公司治理之良好與否息息相關。

此外，內控制度之執行者與監督者間，清楚合理的權限責任分配亦屬內控制度是否得以達成其制度目的之關鍵，例如其是否具備足夠專業能力與客觀判斷，得以有效發現並解決問題。舉例來說，相較於英美立法例係將董事會定位為監督機關，公司法即明文預斷董事會之定位係業務執行機關[71]，然而在此架構下，規範董事會應作為內控制度之監督者，恐招致「球員兼裁判」之質疑。再者，依據證券交易法

[70] 周伯翰，前揭註 12，頁 45-47。

[71] 公司法第 202 條。

doi:10.6342/NTU202000744

規定，由獨立董事所組成之審計委員會具有訂定、修正[72]及考核[73]內控制度有效性之權力，然而在前述以業務執行機關為主的董事會群體中，獨立董事作為審計委員會成員得否充分發揮其監督職能，亦將對於內控制度之有效性產生重大影響[74]。簡言之，嗣經上述針對內控制度現況之分析後本文認為，倘為使內控制度得以有效發揮其目的，達成提升良好金融機構治理之目標，現況下，無論係內控制度本身，抑或其參與者（如董事會、審計委員會）之相關規範與具體職能運作，均容有釐清之空間與必要性。

首先，「工欲善其事，必先利其器」，就內部控制制度本身「失靈」，以及頻繁要求增設專責單位或恐造成內控制度之負擔與成本愈趨沉重等制度層面等問題，本文將透過回顧內部控制之制度發展脈絡，據以析出內控制度之本質與重要特性，進而對於現時內控制度之制度設計與法規範架構，嘗試提出具體之改進芻議。再者，尤因「解鈴還需繫鈴人」，針對實際操作或影響內控制度運作之董事會、獨立董事、稽核人員、專責單位、審計委員會等其他專門委員會等組織，以及其各成員之定位、義務、責任及權限範圍，應如何重新調整或為合理分配，始能在銀行日常業務執行與監督間取得妥適平衡，據以促成內控制度充分發揮其功效，則係本文將特別予以著墨之處。

第二項 確立治理為本、監理為輔之原則

銀行係以資金融通、金融中介（financial intermediary）為主要業務之公司法人，且其自有資金偏低，主要資金係來自民間社會大眾之存款，用於供應政府、企業及個人之資金需求，以促進經濟之活絡。故倘若銀行經營不善導致風險控管不當，或發生舞弊情事等，或恐蔓延成金融系統性風險，減損投資大眾權益，且將產生鉅額社會成本。再者，銀行本身即屬具特殊公共地位之「高度管制產業」（highly regulated industry）[75]，其不僅受特別法律之規範（如銀行法），且亦受金融主管機關之層層監理、管制與牽制[76]，使其公司治理要求相較於一般企業則更為嚴格，據以保障民

[72] 證券交易法第 14 條之 3。

[73] 證券交易法第 14 條之 5。

[74] 方嘉麟（2018），〈從永豐金案看獨立董事制度〉，《月旦法學雜誌》，272 期，頁 9-10。

[75] 王志誠，前揭註 49，頁 86。

[76] 黃銘傑（2007），〈金融機構負責人忠實注意義務加重之理論與實務〉，《月旦法學雜誌》，142 期，頁 151。

doi:10.6342/NTU202000744

間資金提供者[77]。再者，公司治理良好的銀行除了能夠兼顧存款人與投資人之保護外，亦同時提升金融監理機關對於銀行內部作業程序之信賴，使其得有效率地執行符合成本效益之監理措施，並得有效維持金融市場、經濟體系之穩定[78]。職是之故，金融監理機關之監理重點僅須強調各銀行內部應設置適當級別與程度，並符合「制衡原則」（checks and balances）之「問責機制」（accountability）即可，若係於金融機構運作發生任何狀況之際，金融監理機關亦得實質仰賴並要求金融機構內部之董事會或職司控制功能之負責人，應擬具有效之解決對策，並在其監督下執行除錯[79]。

「公司治理」作為現代公司法制之重要議題，係因良好之公司治理為公司健全經營之基石。廣義而言，公司治理主要包含制度結構（institutional structures）、法律規則（legal rules）及最佳典範（best practices）等三者，綜合架構出公司內部主要決策者之成員資格、權限範圍，及其作成決策時所應遵循之各式規範[80]。原則上，公司治理規範得協助建立可茲信賴、透明且問責清楚之經商環境，其除為扶植長期投資、促進金融穩定及維持商業誠信之所需以外，其更能支持公司持續穩健成長，繼而創造包容與和諧之社會[81]。至於公司治理之落實，則端賴公司之董事會與管理階層，以符合公司利益之方式，於運作公司、達成營運目標的同時，提供有效的制衡監控機制，據以激勵企業妥適運用既有資源、提升效率與競爭力，並善盡其社會責任、增進公眾福祉。

然而觀諸實務運作與制度發展現況後發現，「公司治理」概念經常於公司發生重大舞弊事件造成投資大眾之損失，又或對於經濟、政治造成一定衝擊時，始重為政策制定者所關注，或為應社會聲浪要求重新檢討法制，以防止不法行為再次發生。此外，無獨有偶者，公司董事會與經營管理階層亦頻於不法案件發生後強調，其將以加強或改善公司治理作為往後繼續經營公司之首要目標，試圖挽回投資人與市場之信心云云，均在在顯示金融機構之公司治理機制或恐存在結構性之根本

[77] Klaus J. Hopt, *Corporate Governance of Banks After the Financial Crisis*, *in* FINANCIAL REGULATION AND SUPERVISION: A POST-CRISIS ANALYSIS ¶11.03 (Eddy Wymeersch et al. eds., 2012).

[78] BASEL COMM. ON BANKING SUPERVISION, PRINCIPLES FOR ENHANCING CORPORATE GOVERNANCE ¶ 15 (2010), https://www.bis.org/publ/bcbs176.pdf [hereinafter BASEL PRINCIPLES 2010].

[79] *Id.*

[80] STEPHEN M. BAINBRIDGE, CORPORATE GOVERNANCE AFTER THE FINANCIAL CRISIS 2 (2012).

[81] *Corporate Governance*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, http://www.oecd.org/corporate/ (last visited Apr. 1, 2019).

doi:10.6342/NTU202000744

問題，亟待解決。

行文至此，本文須再次強調，由**金融監理機關制定與執行之外部監管措施有其存在之必要係無庸置疑，惟諸等措施絕大多數僅能以場外監控方式為之，監管成效之良窳仍端賴其本體／源頭——即銀行本身是否遵循相關法令規範，或財務業務報導是否完整與忠實等內部行為**。因此本文以為，立法者與金融監理機關之首要任務，應為建構以「內部控制制度」與事前問題預防機制為核心的金融機構公司治理法制架構，蓋因良好之金融機構公司治理除了能夠降低外部監理成本外，亦得有效提升外部監理之效率。準此以言，誠如上述本文對內控制度之現況分析，近期關於金融機構公司治理不彰或有待加強之案件，多係因金融機構之內控制度未能有效發揮其作用所致，故本文之研究目的即在於：希冀分別透過內控制度「制度面」與「組織面」之全盤檢視，提出內控制度相關規範與制度設計之具體調整建議。綜而言之，本文期能建構並確立金融機構應自內部充分落實公司治理之制度架構，方能與外部金融主管機關有效率之監理舉措達到相輔相成之綜效，進而使金融機構與金融監理機關共同攜手合作創造良好金融環境與秩序，俾利金融機構得發揮服務實體經濟、落實普惠金融等其應有之社會機能[82]。

第三節　研究方法

本文主要採取「法律重構」（Recasting Project）研究方法，即透過蒐集與彙整內部控制相關法令規範、學術文獻、研究報告、實務案例及準則等第一手資料，再經由參酌與比較現行制度規範或有不足之處後，據此提出由本文重新形塑、完整之內部控制制度設計與人事組織架構之典範（paradigm）[83]。質言之，本文首先回顧金融機構主管機關作成之各項裁罰案件與法規函釋，初步認為金融機構內控制度作為其內部重要自律機制，於現行實際運作上，無論係制度本身之設計，抑或人事組織之安排與權責分配，兩者均存有不足與不妥適之處。準此，本文為提出於金融

[82] 羅伯・席勒（Robert J. Shiller）（著），林麗冠（譯）（2014），《金融與美好社會》（Finance and the Good Society），頁 33，臺北市：遠見天下文化。

> 金融在美好社會中扮演甚麼樣的角色？做為一門科學、一種行業與一種經濟創新的來源，金融如何幫助人們推動美好社會的目標？金融如何能夠促進自由、繁榮、平等和經濟安全？我們如何能夠使金融民主化，使它進一步造福全人類？

[83] *See* Martha Minow, *Archetypal Legal Scholarship: A Field Guide*, 63(1) J. LEGAL EDUC. 65, 66 (2013).

doi:10.6342/NTU202000744

機構內部有效落實內部控制之芻議，將綜合分析法學、會計學、審計學及管理學（包括風險管理、品質管理、人力資源管理）等跨領域之理論與規範，以重新建構並提出完整內部控制之制度與架構藍圖。

第四節　研究範圍

本文係以金融機構公司治理與內部控制為題，望文生義即可知研究主體應為金融機構之內控制度，至於「金融機構」（financial institution）乙詞具體範圍所指為何，應屬開展本文前須予以釐清與定義者。首先，自中央銀行公布之「金融機構一覽表」探尋，該表對金融機構之分類包括中央銀行、本國銀行、外國及大陸銀行在臺分行、信用合作社、農會信用部、漁會信用部、中華郵政公司儲匯處、人壽保險公司、產物保險公司、中央存款保險公司、票券金融公司、證券金融公司及國際金融業務分行等 13 項[84]。復對照金融控股公司法[85]、金融機構合併法[86]、洗錢防制法[87]及金融機構防制洗錢辦法等法規範當中，有具體定義或類型化金融機構範圍者，概將金融機構分為銀行業、證券業（證券商）、期貨業、保險業（保險公司）、信託業、金控公司等六大類別。此外尚有電子票證發行機構、電子支付機構、期貨信託事業、保險代理人公司、保險經紀人公司等其他經金管會指定之金融機構[88]。

---

[84] 金融機構一覽表，中華民國中央銀行全球資訊網，https://www.cbc.gov.tw/public/data/EBOOKXLS/WLIST.pdf（最後瀏覽日：05/17/2019）。

[85] 金融控股公司法第 4 條第 1 項第三款：（一）銀行包括銀行法所稱之銀行與票券金融公司及其他經主管機關指定之機構。（二）保險公司指依保險法以股份有限公司組織設立之保險業。（三）證券商指綜合經營證券承銷、自營及經紀業務之證券商，與經營證券金融業務之證券金融公司。

[86] 金融機構合併法第 4 條第一款：（一）銀行業包括銀行、信用合作社、票券金融公司、信用卡業務機構。（二）證券及期貨業包括證券商、證券投資信託事業、證券投資顧問事業、證券金融事業、期貨商、槓桿交易商、期貨信託事業、期貨經理事業及期貨顧問事業。（三）保險業包括保險公司與保險合作社。

[87] 洗錢防制法第 5 條第一款列舉其所稱金融機構包括銀行、信託投資公司、信用合作社、農會信用部、漁會信用部、全國農業金庫、辦理儲金匯兌、簡易人壽保險業務之郵政機構、票券金融公司、信用卡公司、保險公司、證券商、證券投資信託事業、證券金融事業、證券投資顧問事業、證券集中保管事業、期貨商、信託業、其他經目的事業主管機關指定之金融機構。

[88] 金融機構防制洗錢辦法第 2 條第一款：（一）銀行業包括銀行、信用合作社、辦理儲金匯兌之郵政機構、票券金融公司、信用卡公司及信託業。（二）證券期貨業包括證券商、證券投資信託事業、證券金融事業、證券投資顧問事業、證券集中保管事業、期貨商。（三）保險業包括保險公司、專業再保險公司及辦理簡易人壽保險業務之郵政機構。（四）其他經本會指定之金融機構：包括電子票證發行機構、電子支付機構、槓桿交易商、期貨信託事業、期貨經理事業，以及保險代理人公司、保險經紀人公司及個人執業之保險代理人、保險經紀人。

doi:10.6342/NTU202000744

再者，依循法源位階體系[89]，由上自下踏查與前述各種類型金融機構內控制度相關之法令，屬法律層級之證券交易法規定，公開發行公司與證券商應建立財務、業務之內控制度，抑且各金融業法亦規定金融機構應建立內部控制及稽核制度，諸如銀行法、金融控股公司法、保險法等[90]。屬命令層級則有「金融控股公司及銀行業內部控制及稽核制度實施辦法」、「證券暨期貨市場各服務事業建立內部控制制度處理準則」、「電子支付機構內部控制及稽核制度實施辦法」、「電子票證發行機構業務管理規則」、「郵政儲金匯兌業務內部控制及稽核制度實施辦法」及「保險業內部控制及稽核制度實施辦法」等規範。細繹之，內控制度相關金融機構具體或包括銀行、金控公司、證券商、期貨商、電子支付機構、電子票證發行機構、中華郵政公司及保險機構。本文且將前述法令與其適用之金融機構主體彙整後於下方以表格方式呈現，俾利後續論述與讀者參照。

法令名稱（部分簡稱）	**適用主體**
證券交易法	公開發行公司、證券交易所、證券商、經營證券金融事業、證券集中保管事業或其他證券服務事業者
金控公司及銀行業內控內稽實施辦法	金融控股公司、銀行機構、信用合作社、票券商、信託業、其他金融業兼營票券與信託業務者
證券暨期貨市場各服務事業建立內控制度處理準則	證券交易所、證券櫃檯買賣中心、期貨交易所、證券集中保管事業、證券商、期貨業、證券金融事業、證券投資信託事業、經營接受客戶全權委託投資業務之證券投資顧問事業、信用評等事業、經金管會指定之證券或期貨市場服務事業
電子支付機構內控內稽實施辦法	電子支付機構、兼營電子支付機構業務之電子票證發行機構
電子票證發行機構業務管理規則	電子票證發行機構[91]
郵政儲金匯兌業務內控內稽實施辦法	中華郵政股份有限公司辦理郵政儲金匯兌業務

[89] 憲法第 171 條、第 172 條；中央法規標準法第 11 條。

[90] 前揭註 2。

[91] 電子票證發行機構業務管理規則第 4 條第 4 項第一款僅就發行機構將電子票證之儲存區塊提供他人運用，規定其應內部控制作業制度及程序，並經董事會通過；第二款並指出訂定內控制度至少應包含在內之項目。內控內稽制度之程序性規範則訂定於同規則第 21 條。

doi:10.6342/NTU202000744

保險業內控內稽實施辦法	保險業[92]

表（一）：內控制度相關法令與適用主體彙整

如上表（一）所示，基本上立法者或主管機關依各金融機構類型或業務性質之異同，分別訂有內控制度與內稽制度相關法規以供遵循。惟本文將以銀行[93]與金控公司[94]為論述中心，並適時參酌證券商與期貨商、保險業之內控內稽制度相關規範，原因有三：第一，學理上金融機構之定義係著眼於其引導、匯集及分配資金之金融中介功能[95]，或謂具備接受資金並使其再度入資本市場功能之機構[96]。雖證券公司、信託投資公司及保險公司均可發揮前述金融中介之功能，惟銀行自始即係以吸收存款、集中社會上閒散資金、核發貸款等資金融通作為主要業務[97]，故可謂金融機構之典型代表。第二，就銀行內控制度與內稽制度相關法規範而言，除前述證券交易法、銀行法、金控公司及銀行業內控內稽實施辦法[98]以外，具體尚有其自律組織（即中華民國銀行商業同業公會全國聯合會）制訂之「銀行內部控制三道防線實務守則」、個別銀行通過之內控制度等規範可茲研析。抑且，現時國際組織（如巴塞

[92] 此處所稱保險業，指依保險法組織登記，以經營保險為業之機構（保險法第 6 條第 1 項）。

[93] 銀行法第 2 條規定，銀行謂依據銀行法組織登記，經營銀行業務之機構。

[94] 為消除銀行數量過多所帶來的競爭壓力、發揮金融機構綜合經營效益、強化金融跨業經營之合併監理、促進金融市場健全發展、並維護公共利益（金控公司法第 1 條），立法者於 2001 年 6 月 27 日完成《金融控股公司法》之立法，並於同年 11 月 1 日開始施行，故亦有稱 2001 年為「金控元年」。所謂金融控股公司（Financial Holding Company，FHC）指對銀行、保險公司或證券商具有控制性持股（金控公司法第 4 條第二款），係以控制他公司為成立目的之公司，其任務主要為持有股份與指揮管理者。目前現有 16 家金融控股公司，按其開業日期先後，依序為華南、富邦、中華開發、國泰、玉山、兆豐、元大（原復華）、日盛、台新、新光、國票、永豐（原建華）、中國信託、第一、臺灣及合作金庫。

[95] 王志誠，前揭註 49，頁 52。

[96] *See* TIM S. CAMPBELL & WILLIAM A. KRACAW, FINANCIAL INSTITUTION AND CAPITAL MARKET 85 (1993).

[97] 王志誠，前揭註 7，頁 3；周伯翰，前揭註 12，頁 3。

[98] 金管會對於金控公司、銀行、信用合作社、票券商及信託業等金融業，原係依各業法之規定，分別訂有適用於各該金融機構之內部控制及稽核制度實施辦法，惟由於各業別內控及內稽實施辦法所規範之內容大致相同，基於監理一致性、法律安定性及修法成本之考量，爰彙整前揭五大金融業之內部控制及內部稽核制度實施辦法內容，並參照「證券暨期貨市場各服務事業建立內部控制制度處理準則」之架構，訂定本辦法，並同時廢止上開各業別之內部控制及內部稽核制度實施辦法。金融控股公司及銀行業內部控制及稽核制度實施辦法總說明（99 年 3 月 29 日訂定）；99 年 3 月 29 日金管銀國字第 09900039294 號命令。

doi:10.6342/NTU202000744

爾銀行監理委員會[99])與政府所頒布、出具公司治理與內控制度之研究或調查報告，多係以銀行為探討之主角。第三，依據金管會組織架構與作成處分之各次級機關，可分為銀行局、證券期貨局及保險局三者[100]，而本文主要係採擇由銀行局所作成之內控制度相關裁罰案件為部分研究素材，且該處分多係以銀行、金控公司為對象。

簡言之，本文題目所指稱之金融機構，係以銀行與金控公司為主要研究範圍，惟必要時，將適時輔以證券商與期貨商、保險業之內控內稽實施辦法作為參考比較之對象，俾具體深入探討內控制度與金融機構公司治理間之互動關係。

第五節　研究架構

誠如前述，本文之研究目的在於透過內部控制「制度面」與「組織面」之全盤檢視，以嘗試提出內控制度相關規範與制度設計之芻議，故依此，本文之研究架構主要即係以金融機構之內部控制為主軸，分別論述內部控制「制度設計」與「人事組織安排」等兩大部分。

本文共有五章。第一章為緒論——初步分析內控制度之運作現狀後本文認為，現行內控制度存有制度本身未能充分發揮實效、頻繁因事涉人增加設置專責單位，以及過度仰賴董事，惟未能有效制約業務單位職員之行為等問題。故以此為動機，本文嘗試透過首先探尋內部控制之發展與制度設計、再行建構運作內控制度應有之組織架構等兩道途徑，期能據此確立金融機構應自內部充分落實其自律機制之公司治理制度架構，方能與外部金融主管機關之監理舉措達成相輔相成之綜效之研究目的。職是之故，本文第二章與第三章即屬內部控制制度設計之範疇，第四章主要為內部控制人事組織架構之論述。

第二章為內部控制之基礎理論——本文藉由爬梳內部控制從內部牽制、會計控制與管理控制、內部控制框架成型再到風險管理導向整合等四大理論發展階段，析出內控制度應包括內部牽制、風險管理及權責劃分等三項基本原則。以此為核心概念，本文即於第三章討論內部控制之具體制度設計——首先以銀行為示例，淺介

[99] *E.g.*, BASEL COMM. ON BANKING SUPERVISION, INTERNAL CONTROL SYSTEMS IN BANKING ORGANISATIONS (1998); BASEL COMM. ON BANKING SUPERVISION, CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION (2012); BASEL COMM. ON BANKING SUPERVISION, GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS (2015).

[100] 金管會組織法第 4 條；裁罰案件，前揭註 13。

doi:10.6342/NTU202000744

內控制度三道防線基本架構，以及內部控制之營運、報導、遵循三大目標，本文並透過對於銀行日常各項業務活動、報導與資訊之編製與定期揭露等方面之觀察，以得出內部控制核心目標應係遵循之結論。再者，本文經由探討內控制度、風險管理及法令遵循之內涵，以及三者間之互動關係，確立內控制度之 GRC 整合架構，並提出內控制度之控制程序應納入 PDCA 動態循環之芻議，作為本文對於內部控制制度設計之具體構想。同時，本文點出內控制度或有無法避免之人為限制因素，以為下一章之鋪墊。

第四章則係延續前述內控制度之具體設計及其人為影響，探討金融機構內部應如何為合理之人事組織安排與權責分配，方能充分發揮內控制度之實效。本文首先根據金融機構內部組織層級劃分，依序檢視業務單位、經營管理階層及董事會之實務運作現況，並提出現有法制設計上於權責分配有所不足之處。再者，本文嘗試辨析並釐清董事會作為內控制度之監控機關，其應如何與經營管理階層達成業務執行與監督之合理分工，共同達成形塑與落實誠信經營之良好組織文化之目標，以利於內控制度之運作。最後，本文採擇人力資源部門、稽核與審計制度、公司治理人員等三項係與內控制度運作高度相關者作為論述對象，期能從而完整建構金融機構內部控制之組織設計。第五章為結論。

doi:10.6342/NTU202000744

第二章 內部控制之理論基礎

第一節　內部控制之演進脈絡

內控制度最初係源自於會計師從事審計工作之一環，於查核公司財務報導或會計資訊之準確性時，倘若該公司係透過適當的內部控制程序，建置會計資訊系統且確保其發揮功能，則該系統之運作情形，即可作為會計師判斷財務數字正確性之依據。質言之，內控制度之初始功能為偵測舞弊，據以確保公司資產、財務資訊之可靠與忠實報導。惟歷經相當期間發展，內控制度本身除作為消極偵查與管理舞弊之防弊措施外，逐漸著重其組織、規劃、指揮、控制、監督等積極興利之管理功能，據以協助公司之董事會與高階管理階層於強化企業內部整體營運效率與效果之時，並得預防內部發生違法行為或缺失，併同追求防弊與興利之目標。具體而言，內部控制理論之發展脈絡可概略劃歸為內部牽制、會計控制與管理控制、內部控制框架成型，以及風險管理導向整合等四大階段，以下分述之。

第一項 內部牽制階段

內部控制之具體意涵係由「內部牽制（Internal Check）原則」發展而來，而內部牽制係指組織內各部門或人員透過專業職責分工，對於各項日常業務或交易行為，於彼此間形成相互檢查、制衡及監督之關係，藉以偵測錯誤、舞弊及避免詐欺等非法行為之發生[1]。為貫徹內部牽制原則，不同部門或各職員之間應透過不相容之「職務分離」（Segregation of Duties，SoD）為內部職務之專業化分工。其概念為：不同人員不得擔任互不相容之職務（incompatible duties），例如「管帳不管錢，管錢不管帳」即係最基本的分工態樣，職司日常業務執行之職員或部門不應兼辦，或具有權限得覆核交易紀錄或檢閱財務報表，據以預防錯誤或詐欺等行為情事，遭到當事人隱匿或自行不當掩飾[2]。質言之，負責執行經授權之資產交易（authorization，AUT）、保管資產（custody，CUS）、編製財務報表（recording，REC）及查核紀錄（verification，VER）等四者，應分別委由不同部門或職員負責執行[3]，以防免侵占

[1] *See* STEVEN J. ROOT, BEYOND COSO: INTERNAL CONTROL TO ENHANCE CORPORATE GOVERNANCE 56 (1998).

[2] *See* Stefano Ferroni, *Implementing Segregation of Duties: A Practical Experience Based on Best Practices*, 3 ISACA J. 1, 1 (2016).

[3] *Id.* at 1-2.

doi:10.6342/NTU202000744

資產、挪用公款、詐欺等風險之發生[4]。

第二項 會計控制與管理控制階段

1936 年，美國會計師協會（American Institute of Accountants）發布之「獨立會計師對財務報告之審查」報告中，曾嘗試定義「內部牽制與控制」（Internal Check and Control）乙詞，其指內部控制係公司為保護其現金與資產，以及帳簿紀錄之準確性，於組織內部採用之各種手段與方法[5]。惟至 1949 年，隸屬於美國會計師公會（American Institute of Certificated Public Accountants，以下簡稱 AICPA）之審計程序委員會（Committee on Auditing Procedure）所提出一份內部控制特別報告中，將內部控制定義之範圍擴大為：企業為保障其資產之安全、檢核會計數據之正確性與可靠性，提升營運效率，以及鼓勵員工遵循既有之管理政策等，於組織內部採行之計劃與其他同等重要之方法與措施[6]。

綜觀前述內部控制之各項定義，均純粹自會計學之角度出發，且於實際操作層面，僅將內部控制應用於會計師或稽核人員對於公司財務報導進行稽核作業、為財務控管之層面。然而，由於 AICPA 的定義為首次賦予內部控制於公司當中，具有其獨立之重要性者[7]，故得認此時是為內部控制理論逐漸開展與演變之濫觴。

隨著公司組織型態愈趨複雜與龐大，管理階層為能在有限的能力範圍內，盡力確保公司業務正常運作，惟同時須防範與監測各部門發生錯誤或舞弊等不法行為，以履行其對公司所負之責任與義務，內控制度對於管理階層之重要性可謂係日益增加[8]。抑且，伴隨內控制度之廣泛應用與調整修正，內控制度能發揮其系統機能之場域，實已遠超過原先的會計與財務範疇[9]，故 AICPA 所屬之審計程序委員會復

---

[4] *Id.* at 3.

[5] AM. INST. OF ACCOUNTANTS, EXAMINATION OF FINANCIAL STATEMENTS BY INDEPENDENT PUBLIC ACCOUNTANTS 8 (1936), http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/colletion/papers/1930/1936_0101_AIAExamination.pdf. 該份報告主要係記載會計師於編製、審核公司資產負債表等財務報表時，其所應遵循之準則、流程及各項建議。

[6] COMM. ON AUDITING PROCEDURE, AM. INST. OF CERTIFIED PUB. ACCOUNTANTS, INTERNAL CONTROL: ELEMENTS OF A COORDINATED SYSTEM AND ITS IMPORTANCE TO MANAGEMENT AND THE INDEPENDENT PUBLIC ACCOUNTANT, SPECIAL REPORT 6 (1949) [hereinafter INTERNAL CONTROL SPECIAL REPORT].

[7] Melvin A. Eisenberg, *The Board of Directors and Internal Control*, 19(2) CARDOZO L. REV. 237, 240 (1997).

[8] INTERNAL CONTROL SPECIAL REPORT, *supra* note 6, at 5-6.

[9] *Id.* at 5-6; The Comm. on Law & Accounting, *"Management" Reports on Internal Control: A Legal Perspective*, 49(2) BUS. LAW. 889, 893 (1994); Eisenberg, *supra* note 7, at 241.

doi:10.6342/NTU202000744

於 1958 年發布第 29 號審計程序公報（Scope of the Independent Auditor's Review of Internal Control, Statement on Auditing Procedure No. 29），繼而將內部控制依其特性，區分為「會計控制」（accounting control）與「管理控制」（administrative control）兩種類型。會計控制之主要目標為保護公司資產與提升財務會計紀錄之可靠性；管理控制則包括「非會計控制」（non-accounting control）者[10]，其關注重點在於如何提升公司經營之效率，並確保管理階層所制定之各項管理政策，均得以於公司內部被有效遵守與確實執行。

直至 1963 年 AICPA 發布第 33 號審計程序公報中，其雖未調整內部控制相關定義，惟此份公報進一步釐清會計控制與管理控制之分野，以及外部審計人員（即會計師）查核財務報表時須予以著重之範圍。該份公報指出，由於會計控制與財務報導之可靠性間，原則上具有「直接且重要之關係」，故外部審計人員（即會計師）的查核重點應為會計控制；反之，由於管理控制與財務報導可靠性間，僅具有「間接關係」，僅於其認為管理控制對於財務報導具有「重要影響」時，始須一併予以評估[11]。換言之，內部稽核人員對於會計控制與管理控制均應予以相同程度之重視，自不待言。

AICPA 接著於 1972 年發布第 54 號審計程序公報，除了沿襲第 29 號與第 33 號公報之分類，將內部控制區別為會計控制與管理控制外，其並微調管理控制之定義，指為制定經管理階層授權作成交易決策的過程，所擬定與程序及紀錄相關之組織計畫。換言之，管理階層授權公司內其他成員作成有效交易決策的同時，各該成員亦須承擔達成組織目標之責任，故其應負有相當責任，確保內控制度之建立與有效運作。會計控制方面，除了既有之資產安全與可靠財務紀錄兩大功能以外，其運作結果應對於公司各項交易決策、或接近公司資產等行為，均係經由或符合管理階層之授權內容，提供合理之保證[12]。

---

[10] The Comm. on Law & Accounting, *supra* note 9, at 893.

[11] *Id.*; 銀行內部控制與內部稽核編撰委員會（民 94）〔以下簡稱銀行內控內稽編撰委員會〕，《銀行內部控制與內部稽核》，頁 6，臺北市：財團法人臺灣金融研訓院；陳耀宗（民 104），《審計學：國際審計與確信準則為架構（上）》，頁 222-223，新北市：滄海圖書資訊。

[12] Eisenberg, *supra* note 7, at 241. 此外，美國為禁止其國內企業或特定群體非法向國外政府或政黨提供不當支付，以獲取商業利益等賄賂行為，故於 1977 年通過位階屬於聯邦法律之《海外反腐敗法》（The Foreign Corrupt Practices Act of 1977，FCPA）。該法包括「反賄賂條款」（anti-bribery provisions）與「會計條款」（accounting provisions）兩大部分，後者係直接將 AICPA 第 54 號審計

doi:10.6342/NTU202000744

1985 年成立，美國國內專門從事財務報導系統研究的民間組織「詐欺財務報導全國委員會」（National Commission on Fraudulent Financial Reporting，以下簡稱 NCFFR）曾於 1987 年發布「詐欺性財務報導之研究報告」（又稱 Treadway Report）強調內部控制對於預防或偵測以財務報導從事詐欺行為之重要性[13]。該報告指出，內控制度不應侷限於財務報導等會計控制之範疇，係因公司部分交易決策須透過管理階層的審慎評估或判斷，故詐欺會發生在此些直接受到管理階層控制的交易行為，惟該「營運上」（operational）作為並非會計控制所能掌握者[14]。因此，內部控制除了前述營運控制（管理控制）與財務報導控制（會計控制）等兩者以外，亦應搭配內部稽核與審計委員會等組織，始能充分發揮其作用[15]。

值得注意者，該報告對建立「公司控制環境」（corporate control environment）此概念多所著墨，所謂公司控制環境係指除了內部會計控制、內部稽核、董事會及其他功能性委員會以外，還包括管理階層的管理哲學、個人經營風格、組織結構、分配權力與責任的溝通與執行方法等；強調建立良好控制環境的重要性在於，其不僅是內控制度順利運作之基礎，更對於公司出具正確可靠的財務報導的過程，具有整體性的影響[16]。基此該報告認為，堅實且有效的內控制度不僅是預防詐欺行為的第一道防線，亦得提升管理階層良好的商業意識，且使控制活動均能符合成本效益[17]。然而，NCFFR 最終並未對於內部控制之定義作成結論，其僅表示內部控制本質上係一複雜、動態且不斷演變之概念，故建議應成立其他專門組織為深入研究[18]。

第三項 內部控制框架成型階段

1988 年 AICPA 發布第 55 號審計準則公報（Statement on Auditing Standards，

程序公報關於會計控制之內容予以明文化，要求所有在美國公開發行股票之公司，均應建置並確保內部會計控制系統有效運作。*Id.* at 242; *see also Foreign Corrupt Practices Act: An Overview*, U.S. DEP'T JUST., https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act (last updated Feb. 3, 2017); the Foreign Corrupt Practices Act of 1977 § 78m(b)(2)(B), 15 U.S.C. §§ 78dd-1 (2004); the Comm. on Law & Accounting, *supra* note 9, at 893-94.

[13] Eisenberg, *supra* note 7, at 243; NAT'L COMM'N ON FRAUDULENT FIN. REPORTING, REPORT OF THE NATIONAL COMMISSION ON FRAUDULENT FINANCIAL REPORTING 33 (1987), https://www.coso.org/Documents/NCFFR.pdf [hereinafter REPORT ON FRAUDULENT FINANCIAL REPORTING].

[14] REPORT ON FRAUDULENT FINANCIAL REPORTING, *supra* note 13, at 34.

[15] *Id.* at 34.

[16] *Id.*

[17] *Id.*

[18] *Id.* at 48.

doi:10.6342/NTU202000744

SAS No. 55: Consideration of Internal Control in a Financial Statement Audit），此號公報首次提出「內部控制結構」概念，並揚棄前述諸公報區別會計控制與管理控制之分類。該公報指出，內部控制結構指企業為合理保證得以達成其組織目標，據此設立之相關政策與程序，具體而言可包含三項組成要素，分別為（一）控制環境（control environment）、（二）會計制度（accounting system）及（三）控制程序（control procedures）。儘管該公報仍係立基於財務報表審計之立場而提出前述內部控制之定義[19]，惟其不再區分會計控制與管理控制，並提出內部控制結構之組成要素，可謂係內控制度理論發展之一大重要突破。

為整合並尋繹內部控制之通用定義，以符合公司、會計師、立法者及監管機關等利害關係人之需，同時在廣泛框架下設定為各方認可與接受之具體要件，使公司得據以評估其內控制度之實際效用[20]，美國國內職司內控制度相關議題研究之民間組織「COSO 委員會」[21]（The Committee of Sponsoring Organizations of the Treadway Commission，以下簡稱 COSO）於 1992 年發表「內部控制——整合架構」（Internal Control－Integrated Framework）研究報告，將內部控制定義為：為能對企業達成其組織目標提供合理保證所設計之流程（process），且該流程將受到企業內部董事會成員、管理階層及其他個人之影響。內部控制三大目標則係指營運之效果與效率、財務報導之可靠性，以及相關法令與規範之遵循。質言之，COSO 報告提出之內部控制整合架構，具有幾點重要概念：第一，內部控制為一道管理過程，且係達成目標之手段，而非目標本身。第二，內部控制並非僅是徒具形式之政策、手冊或指南等規範，該制度需要組織內部各個階層、每位成員之參與運作。第三，組織內部董事會與管理階層僅能期待自內控制度獲致「合理確信」（reasonable assurance），並無法「絕對保證」（absolute assurance）營運、報導及遵循等目標之達成。第四，內部控制係一動態過程，其運作之目的在於達成組織內部一或數個獨立觀察具有個別性、整體觀察卻又彼此間部分重疊之目標。

---

[19] 陳耀宗，前揭註 11，頁 223；銀行內部控制制度編撰委員會（民 90）〔以下簡稱銀行內控編撰委員會〕，《銀行內部控制制度》，頁 8，臺北市：臺灣金融研訓院。

[20] *See* ROOT, *supra* note 1, at 111.

[21] COSO 委員會與 NCFFR 分別為美國國內從事內部控制與財務報導系統議題研究之民間組織，兩者均係由美國會計師公會（AICPA）、美國會計學會（American Accounting Association）、美國財務主管協會（Financial Executives International，FEI）、內部稽核協會（Institute of Internal Auditors，IIA）及美國管理會計師協會（Institute of Management Accountants，IMA）等五個機構贊助成立。

doi:10.6342/NTU202000744

除此之外，COSO 報告當中亦具體指出，良好之內部控制整合架構應具備五項組成要素，分別為：控制環境、風險評估、控制活動、資訊與溝通、監控。唯有具備前述五項構成要素之內部控制架構，方能合理達成前述目標。各項要素之意涵，分述如下。

（一）控制環境（control environment）：作為內控制度組成要素之一，控制環境實為建置與運作內部控制之基礎，其主要目的係於組織內部提供紀律與架構，據以樹立組織基調、塑造組織文化，進而影響組織內部人員之控制意識（control consciousness）。詳言之，控制環境之具體要素包括：組織各成員之道德操守與價值觀、專業能力之承諾、董事會與審計委員會等治理單位之參與、管理階層之經營哲學與風格、適當之組織結構、權限與責任之合理分配、人力資源政策與實務等[22]。

（二）風險評估（risk assessment）：企業日常營運活動無可避免地面臨各式內生或外來之風險，為有效控管風險以達成組織目標，即須建置風險評估流程，以之辨識與分析諸風險，作為決定何種風險應如何管理之基礎。再者，由於內部控制之制度目的係為達成營運、報導及遵循等三大目標，故風險評估之前提係先行確立目標（objectives setting），訂定包括組織整體與各作業階層應分別或共同達成之具體目標。

至於具體風險評估流程，尚可區分為風險辨識（identification）、風險分析（analysis）及策略調整（management change）等三階段，本文茲以銀行為例，簡述如下。首先，銀行依確立之目標擬定與執行具體策略時，應辨識與目標達成攸關或可能衍生之風險[23]，而銀行等金融機構於執行業務過程中常見的風險包括：信用風險、市場風險、流動性風險、利率風險、作業風險、資訊科技風險、法律與遵循風險、環境風險及安全風險等，其中法律與遵循風險因係源於外部之法律與命令等強制規範，故該風險須完全予以控制；惟作業風險（或營運風險）係取決於各銀行根據其交易性質、營業規模所擬定之經營策略，因此，各銀行應先行認知其個別之風險胃納程度，據以有效控管各該風險[24]。再者，當個別風險已被辨認，管理階層

[22] ROOT, *supra* note 1, at 120-21; 陳耀宗，前揭註 11，頁 229-233；銀行內控編撰委員會，前揭註 19，頁 25。

[23] *See* ROOT, *supra* note 1, at 125.

[24] *See id.* at 124; 銀行內控編撰委員會，前揭註 19，頁 26。

doi:10.6342/NTU202000744

即須評估該風險之顯著程度與風險實現之可能性，以及倘若該風險實現後之可控制性，俾利其擬定有效的風險因應對策[25]。於此同時，銀行管理階層須另行制定一道程序或步驟，衡量諸如經濟、產業、監管環境等外在條件因素之變化，以協助其決定最終應採取何種風險控管手段[26]，惟其亦得基於成本效益、已合於風險胃納程度等其他考量，決定不採取任何行動而承擔該風險[27]。

（三）控制活動（control activities）：為使組織內部相關成員獲悉管理階層之指令，並據此落實風險控管措施或採取必要手段，以利達成組織目標，控制活動即指為協助管理階層之指示均能有效傳達至組織各階層，並被確實執行所建立之政策與程序[28]。換言之，亦指由管理階層訂定對於控制環境之基調與預期，並由業務執行階層於個別營運活動中，共同實踐之控制過程[29]。控制活動之具體內容包括授權、核准、驗證、勾稽（reconciliations）、營運績效覆核、資產保全及職責分工等，抑且各該控制活動遍布組織各階層及其所涉之職能。

（四）資訊與溝通（information and communication）：即時且可靠之資訊係組織內部各成員清楚瞭解其所扮演之角色與擔負之責任所不可或缺者[30]，所謂「資訊」係指透過資訊系統所產生、蒐集或辨識，並經由該系統適時傳達予特定成員，與營運、財務、法令遵循相關者。「溝通」則係指為使資訊得有效地傳達至各階層，建置包括自上而下、下情上達、水平橫向，以及對外之資訊流通管道，促使組織內部員工認知其本身於內控制度中扮演之角色，及其相對於他人所位居之地位與作業上之關聯[31]。簡言之，資訊與溝通之主要功能係協助組織內部成員充分瞭解並確實完成管理階層所交付之任務，俾使有效履行職責，據以達成組織與內控制度之各項目標。

（五）監控（monitoring）：監控活動係對於內控制度隨著時間推移，為確保該

[25] *See* ROOT, *supra* note 1, at 125.
[26] *See id.* at 125.
[27] 陳耀宗，前揭註 11，頁 235；銀行內控編撰委員會，前揭註 19，頁 27。
[28] *See* ROOT, *supra* note 1, at 128.
[29] 陳耀宗，前揭註 11，頁 248。
[30] *See* ROOT, *supra* note 1, at 131.
[31] 銀行內控編撰委員會，前揭註 19，頁 29；曾令寧、黃仁德（民 92），《現代銀行監理與風險管理》，頁 178，臺北市：臺灣金融研訓院。

doi:10.6342/NTU202000744

制度有效率地運作，定期或於必要時，評估其執行之品質與成效之過程[32]。監控可分為「持續性監控」（ongoing monitoring）與「個別評估」（separate evaluation），抑或兩者共同執行：前者係於日常業務執行過程中，針對經常性管理與督導行為，以及個人執行職務時所採取之行動等，持續進行監控；後者則係為協助管理階層調查與評估內控制度本身是否有效運作，並適時提供調整建議，至於個別評估的範圍與頻率，即須視組織內部風險變化程度與持續性監控活動之有效性而定[33]。

詳之，由於企業營運與控制環境係不斷變化的動態過程，為能即時因應市場或經濟環境之瞬息萬變與接踵而來的各式風險，企業應持續評估並隨時擬定或調整應對策略，此將致使內控制度之功能或有隨著時間之遞嬗與現時情狀之變化，漸次無法因時制宜或失其效用，故監控活動除了能夠適時評估內控制度之設計與運作以外，亦能針對實務運作現況，採取必要之內控制度修正措施[34]。職是故，為能有效達成內控制度之各項目標，無論係業務執行單位、專責單位或內部稽核單位，若發見內控制度出現缺失時，應有通暢之溝通管道，俾利其即時向相應層級之管理階層報告，惟若屬重大缺失，則應逕向高階管理階層與董事會報告[35]。

綜言之，COSO 認為內部控制係一道目標導向之管理流程，且該流程將受到董事會、管理階層等人為因素影響，同時內控制度亦有其限制，對於營運、報導及遵循等目標，內控制度僅能提供合理（reasonable）程度保證，並無法絕對（absolute）保證各該目標之達成[36]。該整合架構如下頁表（二）所示：

---

[32] *See* ROOT, *supra* note 1, at 132.

[33] 銀行內控編撰委員會，前揭註 19，頁 31；曾令寧、黃仁德，前揭註 31，頁 178。

[34] 銀行內控編撰委員會，前揭註 19，頁 31；曾令寧、黃仁德，前揭註 31，頁 178。

[35] 銀行內控編撰委員會，前揭註 19，頁 31；曾令寧、黃仁德，前揭註 31，頁 178。

[36] ROOT, *supra* note 1, at 118.

doi:10.6342/NTU202000744

1992 年版 COSO 報告			
定義：內部控制是為達成組織目標提供合理保證的流程。			
三大目標			五大組成要素
營運效果與效率	財務報導可靠性	法令與規範遵循	控制環境
			風險評估
			控制活動
			資訊與溝通
			監控

表（二）：1992 年 COSO 內部控制整合架構

COSO 報告之重要貢獻在於提出完整之內部控制整合架構概念，同時至此確立內控制度之三大目標，抑且啟蒙公司董事會積極參與組織內部整體風險監督之意識。縱謂 COSO 之研究成果對於內部控制之發展與應用具有相當重要性，惟 COSO 組織本身僅係一民間組織，實際上該份報告並不具有任何立法或監管上之效力，故無法強制一般民間企業採行或遵循[37]。然而，伴隨企業風險管理意識之逐漸萌芽，COSO 內部控制整合架構實謂係內部控制發展邁入下一重要發展階段之里程碑。

第四項 風險管理導向整合階段

第一款 巴塞爾銀行監理委員會

為有效促進開發中與已開發國家內部銀行體系之健全，維持全球金融環境之穩定[38]，1997 年 9 月，由全球十大工業國家（Group of Ten，G10）[39]中央銀行共同組成之巴塞爾銀行監理委員會（The Basel Committee on Banking Supervision，以下簡稱巴塞爾委員會）首度頒布「有效銀行監理核心原則」（Core Principles of Effective

[37] Peter Ferola, *Internal Controls in the Aftermath of Sarbanes-Oxley: One Size Doesn't Fit All*, 48(1) S. TEX. L. REV. 87, 92 (2006).

[38] BASEL COMM. ON BANKING SUPERVISION, CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION ¶ 1 (1997), https://www.bis.org/publ/bcbs30a.pdf [hereinafter CORE PRINCIPLES 1997].

[39] 所謂「十大工業國」（Group 10，又稱 G10 或十國集團），實際上係指包含比利時、加拿大、法國、德國、義大利、日本、荷蘭、瑞典、瑞士、英國及美國等十一國在內者。*G10*, BANK FOR INT'L SETTLEMENTS, https://www.bis.org/list/g10publications/index.htm (last visited Apr. 16, 2019).

doi:10.6342/NTU202000744

Banking Supervision）25 項，其中原則 14 指出，銀行監管機關須確保銀行業已依其業務性質（nature）與規模（scale）妥善建立適當之內控制度，包括明確的權限責任分配、職能分工及獨立的內外部稽核與遵循機能[40]。惟伴隨新興銀行監管議題逐漸浮現並獲廣泛討論，為期能與時俱進地調整原則內涵以符合現時不同監管需求[41]，巴塞爾委員會復於 2006 年 10 月頒布新版之核心原則，相較於 1997 年版之核心原則，新版核心原則 17 認為，除了業務性質與規模以外，銀行於建置妥適之內控制度時，亦應進一步考量其業務之複雜程度（complexity）[42]。抑且，除了建置內控制度與內部稽核制度以外，銀行亦應訂定適當之政策、實務準則及程序，據以提升金融領域道德與專業標準，同時預防犯罪之發生[43]。

再者，為能有效提升銀行內部公司治理與外部金融監理之效果，巴塞爾委員會於 2010 年提出之「強化公司治理守則」（Principles for Enhancing Corporate Governance）則指出，銀行內部均應建立並實施良好之公司治理機制，即有效之內部控制系統。詳言之，由於內部控制之目的在於辨識與控制銀行之各項風險，故內控制度之設計係為確保銀行於面臨關鍵性風險時，得有相關配套政策、程序或管理方法以妥適因應，抑且此等政策、程序或管理方法，均因內控制度之存在而能有效運作[44]，並有助於銀行履行其應盡之義務、遵循相關法律或規範，以確保上開政策、

---

[40] 原則 14 指出，銀行監管機關須確保銀行業已依其業務性質與規模建立適當的內控制度，該制度應包含明確的權限與責任分配；銀行內部交易行為承諾、資金給付、資產與負債會計處理等職責分離；前述各項程序之勾稽、資產保全等機能，同時應有妥適的獨立內外部稽核與遵循機能，得據以檢驗銀行所為各行為是否均符合控制程序與相關法令規範。*See* CORE PRINCIPLES 1997, *supra* note 38, princ. 14.

[41] *See* BASEL COMM. ON BANKING SUPERVISION, CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION ¶¶ 1-2 (2006), https://www.bis.org/publ/bcbs129.pdf.

[42] *Id.* princ. 17.

[43] 為避免銀行遭不法濫用，巴塞爾有效銀行監理核心原則 1997 年版原則 15 與 2006 年版原則 18 均明文要求銀行監管機關須確保銀行業已制定妥適的政策、實務準則（包括嚴格的確認客戶身分原則）及程序，據以提升金融領域之高道德與專業標準，併同預防銀行招致犯罪份子蓄意或無意地利用。*See id.* princ. 18; CORE PRINCIPLES 1997, *supra* note 38, princ. 15.

[44] BASEL COMM. ON BANKING SUPERVISION, PRINCIPLES FOR ENHANCING CORPORATE GOVERNANCE ¶ 70 (2010), https://www.bis.org/publ/bcbs176.pdf [hereinafter BASEL PRINCIPLES 2010]. 值得注意者為，相較於巴塞爾有效銀行監理核心原則係獨立訂定內部控制與內部稽核制度之原則，巴塞爾強化公司治理守則則將「風險管理」（risk management）與內部控制合併於同一原則中說明。依據巴塞爾強化公司治理守則，風險管理係指包括辨識與評估關鍵風險、衡量與監控銀行之曝險程度、作成與執行經董事會同意之風險承擔與管理政策或決定、彙報各項風險措施於高階管理階層與董事會等，係銀行內部所有風險管理相關程序在內者。再者，該守則亦認知或有部分金融監管者與銀行將**內部控制乙詞視為包括風險管理、內部稽核及法令遵循等機能在內之「傘狀術語」（umbrella term）**，故縱

doi:10.6342/NTU202000744

程序或管理方法之公正實施。除此之外，內部控制中之「四眼原則」（Four Eyes Principle）即要求各項關鍵管理或業務決策均應有合理之覆核程序，據以促使銀行管理階層與各業務單位均能遵循董事會制定之政策與策略，且依其職權作成審慎判斷，並避免未經授權而作成交易決定或為詐欺行為[45]。

綜言之，依據前述巴塞爾委員會兩項銀行治理相關原則，為有效達成銀行內部良好公司治理，並且提升外部金融監理之成效，銀行應依其綜合業務之性質與整體規模，妥善建置適當的內控制度。

第二款 2004 年 COSO 企業風險管理

由於諸如安隆公司（Enron）財務醜聞之爆發，導致其投資人與員工受到嚴重損害等大型企業弊端案件叢生，使企業風險管理意識逐漸抬頭並愈發受到重視[46]，故為能建立有效協助企業辨認、評估及管理風險之堅實機制，COSO 即奠基於前述 1992 年版內部控制整合架構研究報告，復於 2004 年發布新版「企業風險管理——整合架構」（COSO Enterprise Risk Management—Integrated Framework），在既有內部控制基礎架構上，進一步朝風險管理概念與程序拓展，以期企業於積極為其利害關係人創造價值的過程中，亦能同時認知管理風險之重要性[47]。新版內控制度研究報告除了提供公司董事會與管理階層衡量內部風險管理效度之判準以外，更重要者方屬自此確立全面整合風險管理之內部控制整體架構，意即形塑納入風險管理導向型態之內控制度。

所謂「企業風險管理」（Enterprise Risk Management，以下簡稱 ERM），係指遍及於企業內部各層面，用以制定策略，並識別當中可能影響企業之潛在事項，以及在企業風險胃納程度內為風險管理，據以合理保證企業目標之達成，且係由董事

然該守則係將風險管理與內部控制分別予以討論，惟其仍認為內部控制與風險管理兩者實際上係密切關聯，區辨與否尚不影響內控制度目的之達成。*See also id.* ¶ 69 & n.23. 本文據此認為，基於前述關於內控制度演進脈絡之分析，並綜合銀行內控制度「三道防線」（three lines of defense）所確立之制度外觀，內部控制應指包括風險管理、法令遵循及內外部稽核等機能之內部治理機制。至於本文對於內控制度具體意涵之闡釋，將留待後續結論予以說明。

[45] BASEL PRINCIPLES 2010, *supra* note 44, ¶ 70.

[46] COMM. OF SPONSORING ORGS. OF TREADWAY COMM'N, ENTERPRISE RISK MANAGEMENT — INTEGRATED FRAMEWORK: EXECUTIVE SUMMARY, at v (2004) [hereinafter COSO ERM FRAMEWORK 2004].

[47] *Id.*

doi:10.6342/NTU202000744

會、管理階層及各成員所實施，並受其等影響之作業流程[48]。或有謂想像上，企業風險管理係協助公司穩健地前往其所欲抵達之處，並防止其於途中不慎落入陷阱或遭遇意外[49]。基於公司存在最主要之目的係為其股東、員工、債權人等利害關係人創造價值（value），惟過程中其將面臨諸多不確定性（uncertainty），故企業內部需有一套程序足供辨識、預防或回應諸等不確定性，以利達成最終之目標[50]。而「機會」與「風險」則屬企業選擇是否接受該不確定性後，一體兩面之結果：前者蘊含得提升企業所能創造的價值之可能性、後者則係造成企業價值遭受侵蝕之潛在風險，故企業風險管理即係協助管理階層得有效地處理該不確定性及其相關的機會與風險，使管理階層妥適運用現有資源以達成營運與績效表現、有效報導及相關法令之遵循等目標，同時避免損及商譽或造成其他可能後果[51]。

再者，相較早先 COSO 內控制度整合架構研究報告，COSO 於 ERM 版本中揭示，企業風險管理除了得協助公司達成內部控制既有之營運、報導及遵循等三大目標以外，並新增「策略性」（strategic）為第四項目標。公司成立與運作除為其利害關係人創造利潤外，亦係為實踐其所立定之使命與願景，職是之故，管理階層即於該貫串公司整體目標框架下，為公司量身制定較高層次之策略性目標，並採取相應策略以確保公司各該目標之達成[52]。觀諸企業風險管理架構下之內部控制四大目標，報導與法令遵循兩項目標因各有具體準則與法令規章可供依循，且多屬公司應確實遵守之強制規範，故內控制度得提供合理保證予此兩項目標之達成[53]。惟就策略性與營運兩項目標而言，達成與否將受到公司內部或外在所生之事件與風險等影響，係諸多無法全然由公司控制其發生與否之不確定因素，故內控制度於此之目的即在使管理階層與位居監督者角色之董事會，均能及時獲知公司於達成其目標的過程中所生之各種狀況及其程度，並為最終各該目標之實踐提供合理保證[54]。

準此，ERM 版本即細緻化內控制度之組成要素，除既有之風險評估、控制活動、資訊與溝通、監控等四項要素外，並新增內部環境、目標設定、事件識別、風

[48] *Id.* at 2.
[49] *Id.* at 1.
[50] *See, e.g.*, GREGORY MONAHAN, ENTERPRISE RISK MANAGEMENT: A METHODOLOGY FOR ACHIEVING STRATEGIC OBJECTIVES 12 (2008).
[51] COSO ERM FRAMEWORK 2004, *supra* note 46, at 1.
[52] *Id.*
[53] *See id.*
[54] *Id.*

doi:10.6342/NTU202000744

險應對等四項。關於諸要素之具體意涵，分述如下。

（一）內部環境（Internal Environment）：相較 COSO 內控制度整合架構中控制環境此要素，內部環境係進一步將風險管理概念納入內部控制程序，而形塑良好內部環境之關鍵包括：高階管理階層是否具備風險管理思維、組織內部是否訂定合理之風險胃納程度、成員是否建立己身職業操守與道德倫理觀念等，其將影響組織內部各成員係如何看待與評價風險之基調[55]。

（二）目標設定（Objective Setting）：管理階層設定企業營運目標對於內控制度與風險管理運作之重要性在於，內控制度得協助管理階層建立妥適程序，以此辨識或預防各種可能影響目標實踐之風險事件，並將風險控制在合理風險胃納程度內，據以達成管理階層所設定之各項目標[56]。

（三）事件識別（Event Identification）：此要素所稱事件係指企業達成上述管理階層所設定目標之過程中，於內於外或將面臨各種影響目標得否達成之事件，故內控制度須能有效辨識各事件對於達成目標而言，係屬風險抑或為有利之機會，同時回溯檢視管理階層所作成之策略與其設定之目標是否正確[57]。

（四）風險評估（Risk Assessment）：承前要素，倘依循內控制度辨識之結果認為，該事件對於目標之達成係潛在之風險者，即須在「固有」（inherent）[58]與「剩餘」（residual）[59]兩項風險評估基礎之上，分析該風險發生之可能性與影響程度，

---

[55] *See id.* at 3.

[56] *See id.* at 3-4.

[57] *See id.* at 4.

[58] 固有風險（inherent risk，IR）係指管理階層尚未採取任何行動來改變風險發生的可能性或其影響之情況下，達成其所設定目標之風險。另就審計學角度說明，即係指不考慮內部會計控制之情況下，某會計科目餘額或某類交易發生重大錯誤之風險。固有風險與企業之業務性質、經營環境及科目或交易之性質有關，且外部因素或特殊情況下亦可能影響固有風險，例如產業景氣衰退等。審計準則公報第二十四號（重大性與查核風險）第 14 條第一款；銀行業建立風險導向內部稽核制度實務守則第六點。

[59] 剩餘風險（residual risk），又稱偵查風險（detection risk），指管理階層設計與執行目的係為管理風險與達成既定目標等控制措施後，所遺留下造成無法達成組織目標之風險。或係指查核人員執行查核程序後仍未能查出既存重大錯誤之風險。查核人員因選用不當查核程序、執行偏差、誤解查核結果、採用抽查等，均可能造成剩餘風險。審計準則公報第二十四號（重大性與查核風險）第 14 條第三款；銀行業建立風險導向內部稽核制度實務守則第六點。

doi:10.6342/NTU202000744

據以決定應如何管理該風險[60]。

簡言之，上揭風險評估流程於實務運作上，又可分為風險辨認與風險評估兩階段[61]，第一階段風險辨認主要係為辨認風險來源、瞭解風險性質，並據以區分風險類型與判斷其對於固有風險之潛在影響與意涵。第二階段風險評估係指確認每一個經前階段辨認之風險發生的可能性與影響程度，並進一步判斷是否屬顯著風險，據以擬定後續風險應對策略。

（五）風險應對（Risk Response）：管理階層應針對上揭經辨識與確認之風險擬定風險應對策略，其目的係將各種風險控制在企業風險胃納程度或可容忍範圍以內，據此管理階層可單獨或共同採取回應風險之方法包括迴避風險、接受風險、減少風險或分擔風險等[62]。

（六）控制活動（Control Activities）：控制活動係指管理階層應建置與執行相關政策或程序，以此協助確保上述風險應對策略均能有效地落實[63]。

（七）資訊與溝通（Information and Communication）：為使相關成員得獲取充足資訊以採取及時、有效之風險應對措施，組織內部辨識、擷取及傳遞資訊之過程應於合理時限內完成，俾利各該人等履行其達成企業目標與管理風險之責。據此，資訊於企業內部傳遞與有效溝通之形式與範圍即應較廣泛，包括由上而下、由下而上等垂直溝通，以及各部門間之水平橫向傳遞[64]。

（八）監控（Monitoring）：企業內部整體風險管理流程應予以監控，且該流程應於必要時予以修正或調整，其方式包括持續性規劃、執行及監督等管理作業或個別評估，或兩者兼採之[65]。

綜上所述，整合風險管理與內控制度兩者之企業風險管理具體包含四項目標與八項要素，分別為策略性、營運、報導及遵循目標；組成要素則為內部環境、目

---

[60] *See* COSO ERM FRAMEWORK 2004, *supra* note 46, at 4.

[61] 陳耀宗（民 104），《審計學：國際審計與確信準則為架構（上）》，頁 168，新北市：滄海圖書資訊。

[62] *See* COSO ERM FRAMEWORK 2004, *supra* note 46, at 4.

[63] *Id.*

[64] *See id.*

[65] *See id.*

doi:10.6342/NTU202000744

標設定、事件識別、風險評估、風險應對、控制活動、資訊與溝通及監控，抑且前述諸要素於內控制度之運作係多面向（multidirectional）、彼此間均相互影響的（interactive），意即任一要素事實上均能對於其他要素產生影響[66]。整合架構如下表（三）所示：

<table>
<tr><th colspan="5">2004 年版 COSO ERM 整合架構</th></tr>
<tr><td colspan="5">定義：企業風險管理（ERM）係為協助擬定策略、識別事件及管理風險，以合理確保達成組織目標的流程。</td></tr>
<tr><th colspan="4">四大目標</th><th>八項組成要素</th></tr>
<tr><td rowspan="8">高階策略性目標</td><td rowspan="8">營運效果與效率</td><td rowspan="8">財務報導可靠性</td><td rowspan="8">法令與規範遵循</td><td>內部環境</td></tr>
<tr><td>目標設定</td></tr>
<tr><td>事件識別</td></tr>
<tr><td>風險評估</td></tr>
<tr><td>風險回應</td></tr>
<tr><td>控制活動</td></tr>
<tr><td>資訊與溝通</td></tr>
<tr><td>監控</td></tr>
</table>

表（三）：2004 年 COSO 企業風險管理整合架構

COSO 提出此一企業風險管理整合版本對於內控制度理論發展方面最重要之影響在於，其係首次將風險識別、風險胃納等風險管理相關概念與內部控制予以整合，自此喚起企業對於風險管理之意識，以有效達成內控制度之制度目的。質言之，整合風險管理之內控制度架構得促使管理階層為利害關係人創造價值而訂定達成目標所需之策略時，亦須具備辨識與評估風險之思維與能力，俾利協助企業內部各成員於面臨諸多事件所帶來之不確定性時，均能有效判斷該不確定性係屬潛在風險或有利之機會，據以決定應採取何種風險因應策略，進而提升企業創造價值之能力[67]。

再者，COSO 指出企業內部無論係董事會、高階管理階層、經理人、風險管理長（risk officer）、財務長（financial officer）、內部稽核人員或個別員工等，均應共

[66] *See id.*
[67] *See id.* at 1.

doi:10.6342/NTU202000744

同擔負風險管理與內控制度運作之職責。詳之，高階管理階層（此指執行長）負有建置與執行風險管理與內部控制機制之最終責任[68]；其他經理人則須共同支持並於企業內部落實風險管理之哲學思維、遵循企業所訂之風險胃納、且於各人責任範圍內，將風險控制在適當之風險容忍程度；風險管理長、財務長及內部稽核人員等均應協助管理階層具體落實風險管理架構或監督、評估其有效性；個別員工則須依其職責，確實執行管理階層就風險管理與內控制度所為之指示或規定；至於董事會則須對企業風險管理機制負重要之監督責任，例如知悉並同意企業之風險胃納，故董事會成員均應具備相當能力或取得足夠資訊，以瞭解管理階層所為任何風險管理相關之行動或建置之制度與程序[69]。綜言之，企業風險管理架構之有效落實與運作繫諸於企業內部各階層或部門職員之共同參與。

然而，除了前述企業達成其目標之過程中將面臨諸多不確定性與風險以外，企業風險管理架構尚有其制度上無可避免之限制存在，例如：管理階層為風險決策時，人為因素或將導致其作成不盡完善之判斷，或單純的人為錯誤與差池造成內控制度之故障（breakdowns）；控制活動或因內部成員共謀（collusion）而遭到規避，或管理階層藐視或濫用其職能以逾越風險決策；抑或作成風險應對與訂定內部控制相關策略時，尚應考量所付成本是否達成預期利益[70]。綜而言之，基於前述諸等因素之限制，或將使內控制度對於企業或金融機構所欲達成之組織目標，僅能提供其董事會與管理階層合理而非絕對之保證，惟本文認為，此制度上之根本性限制並非得用以作為否定或怠於建置與落實內控制度之理由。探究內控制度之實質仍係金融機構內部治理之重要機制，其主要功能在避免金融機構內部各成員於執行業務過程中疏失或舞弊之發生，同時預防或控管風險，故內控制度仍有其存在之必要性。基此，吾等須思索者應係如何建構有效運作之內控制度，俾使其充分發揮提升良好金融機構公司治理之制度機能。

第三款 英國公司治理守則與指令

英國財務報告委員會（Financial Reporting Council，以下簡稱 FRC）針對「英國公司治理守則」（U.K. Corporate Governance Code）出具之指令即指出，公司於

---

[68] JAMES HAMILTON & PETER RASMUSSEN, GUIDE TO INTERNAL CONTROLS: UNDER SECTION 404 OF THE SARBANES-OXLEY ACT 61 (2d ed. 2007).

[69] *See* COSO ERM FRAMEWORK 2004, *supra* note 46, at 6-7.

[70] *See id.* at 5.

doi:10.6342/NTU202000744

營運以獲利之過程中，須面臨與承擔各式多變之風險，故建立內部控制系統之重要目的即係協助公司妥適地管理與控制風險，俾利達成其商業目標[71]。因此，董事會須負責於公司內部建立與維持良好之內部控制系統，據以保障各該利害關係人之投資與公司所有之資產[72]。

至於所謂「內部控制系統」（Internal Control System）指由控制活動、資訊傳遞與溝通程序，以及為持續監控內控系統有效性所建置之程序所組成[73]，涵括公司所有相關政策、程序、任務及行為，目的在於達成以下事項者。第一，促使公司得妥適因應達成其所訂目標之過程中，可能面臨之重大商業、營運、財務、法令遵循或其他風險（例如防止公司資產致遭不當濫用或滅失或出現詐欺行為，或確保內部各項債權均經妥適辨認與管理等），據以提升公司營運之效果與效率[74]。協助確保公司內部與對外各項報導之品質，包括維持適當紀錄，以及得產生於組織內部與對外流通之即時、相關及可資信賴的資訊之程序，此其二[75]。其三則係為協助確保公司得遵循各該適用法律、命令等規範，以及內部商業行為相關政策[76]。簡言之，英國公司治理守則將內部控制定義為由公司各項政策與執行程序所組成，於公司內部運作之「系統」（system）[77]，其目的在於協助公司妥適地管理與控制（而非消除）風險，據以促進或協助公司達成有效果與效率之營運、確保報導之品質及相關法令規範與政策之遵循等三大目標。

鑑於當時董事因執行風險管理措施不彰造成公司損失之事件頻繁發生，且為促進經濟發展並避免公司未有效控管風險而導致嚴重後果[78]。此外，英國公司治理規範強調，董事會應擔負於公司內部建立審慎且有效之控制架構之主要責任[79]，並以之辨別、評估及控管公司於營運過程中所面臨之各式風險，同時塑造具有風險管

---

71 *See* FIN. REPORTING COUNCIL [hereinafter FRC], INTERNAL CONTROL: REVISED GUIDANCE FOR DIRECTORS ON THE COMBINED CODE ¶¶ 1 & 4 (2005) [hereinafter THE TURNBULL GUIDANCE 2005].

72 *Id.* ¶ 7; FRC, THE COMBINED CODE ON CORPORATE GOVERNANCE princ. C.2 (2008).

73 THE TURNBULL GUIDANCE 2005, *supra* note 71, ¶ 20.

74 *Id.* ¶ 19.

75 *Id.*

76 *Id.*

77 *See* IRIS H-Y CHIU, REGULATING (FROM) THE INSIDE: THE LEGAL FRAMEWORK FOR INTERNAL CONTROL IN BANKS AND FINANCIAL INSTITUTIONS 4-5 (2018).

78 *See* FRC, GUIDANCE ON RISK MANAGEMENT, INTERNAL CONTROL AND RELATED FINANCIAL AND BUSINESS REPORTING ¶ 5, § 1 (2014) [hereinafter THE RISK GUIDANCE 2014].

79 *See* HAMILTON & RASMUSSEN, *supra* note 68, at 61.

doi:10.6342/NTU202000744

理意識之組織文化，期能有效地達成公司各項策略目標[80]。據此，FRC 即分別於 2010 年[81]、2011 年及 2012 年[82]，對英國公司治理守則中，與內部控制相關內容予以修正或補充、並於 2014 年提出最新版本之風險管理與內部控制之指令。

2010 年版之公司治理守則中，首先確立董事會應負責建置與維持風險管理與內部控制系統之運作，以及判定公司於達成策略性目標之過程中，所應與所能承擔之重大風險之種類與程度[83]。英國財務匯報局另於 2011 年，彙集包括公司、投資人及顧問業者等組織之意見與建議，出版「董事與風險（Boards and Risk）」報告[84]，當中除了重申董事會應負責決定公司面對風險時之取徑、塑造風險管理之組織文化，以及監督公司內部風險與危機管理之成效外[85]，更須負責決定公司之風險胃納、容忍及曝險程度，並隨時根據公司內外部之風險變化情形，調整長短期之營運決策與策略方針[86]。詳言之，風險管理與內部控制系統係由政策、文化、組織、行為、程序等公司內部各面向所組成，共同運作以發揮促進公司營運之效果與效率、降低作成錯誤之人為決策的可能性及其影響、確保公司內外部報導之品質，以及協助確保遵循營運相關法令規範與公司內部政策等功能[87]。職是故，風險管理與內部控制系統之設計與運作，並非單純為符合主管機關法規範之要求，抑或僅係董事會執行其監督職務所需之工具而已，應認其係公司內部日常業務管理與公司治理程

[80] *See* THE RISK GUIDANCE 2014, *supra* note 78, ¶ 4-6, § 1.

[81] 2010 年版公司治理守則進一步釐清董事於風險管理與內控制度面向之責任為，除了負責確保健全之風險管理與內部控制系統之建置與運作以外，董事最重要之責任在於制定公司經營之商業模式（Business Model），以及決定在其採擇之商業模式下，公司於達成內部策略性目標時，所能承擔之重大風險種類及其程度。此外，董事至少每年應定期檢視前述風險管理與內部控制系統之有效性（應包括財務控制、營運控制及遵循控制等三大重要控制項目），並應將檢核之結果向公司各利害關係人報告。FRC, THE UK CORPORATE GOVERNANCE CODE §§ C.2 & C.2.1 (2010); THE RISK GUIDANCE 2014, *supra* note 78, ¶ 7.

[82] 2012 年版公司治理守則即強調董事於必要時，應要求審計委員會（Audit Committee）協助其提供忠實報導（fair and balanced）且可理解（understandable）之年度會計報告與資訊，且該財務與業務報告須提供足夠必要之資訊，足使公司各利害關係人得據以判定該公司之營運表現、商業模式及策略目標等。FRC, THE UK CORPORATE GOVERNANCE CODE § C.3.4. (2012); THE RISK GUIDANCE 2014, *supra* note 78, ¶ 8.

[83] 同前註 81。

[84] FRC, BOARDS AND RISK: A SUMMARY OF DISCUSSIONS WITH COMPANIES, INVESTORS AND ADVISORS (2011) [hereinafter BOARDS AND RISK].

[85] *Id.* ¶ 1, at 2.

[86] *See id.* ¶ 5-6, at 2.

[87] THE RISK GUIDANCE 2014, *supra* note 78, ¶ 28.

doi:10.6342/NTU202000744

序之一環[88]。因此，無論係風險管理意識與文化之建立，抑或是內控制度之運作與有效遵行，均應認屬公司日常業務之健全執行與達成良好公司治理目標等所不可或缺之要素。

第二節　小結——內部控制發展之本文觀察

本文爬梳內部控制之概念與制度發展後初步認為，內控制度之具體設計上，應包括「內部牽制」與「風險控制」兩項原則。抑且，組織內部建立與運作內控制度時，尚應落實各階層、單位部門或職員間明確之「權責劃分」。下方將就本文對於內控制度上開三項基本原則之觀察，分別析述之。惟本文將先予彙整本節所述內部控制相關概念與定義，並依其提出之時序排列，以對於內控制度之演進脈絡有一較為宏觀之輪廓，如下表（四）所示：

概念	定義
內部牽制	各部門成員透過專業職責分工，對於各項日常業務或交易行為，於彼此間形成相互檢查、制衡及監督之關係，藉以偵測錯誤、舞弊及避免詐欺等非法行為之發生。
內部牽制與控制	為保護現金與資產安全、檢核會計數據之正確性與可靠性、提升營運效率，以及鼓勵員工遵循既有之管理政策等目的，於組織內部採用之各種計畫與措施。
會計與管理控制	提升財務會計紀錄之可靠性與公司資產之實體控制，以及促進營運效率與確保遵循管理政策之控制。
內部管理控制	為制定內部經管理階層授權作成交易決策之過程，故擬定與程序及紀錄相關之組織計畫。
內部控制結構	企業為獲得合理保證以達成組織目標，據此設立之政策與程序，包括控制環境、會計制度及控制程序等三要素。
內控整合架構	為能對企業達成其組織目標提供合理保證所設計之流程，且該流程或將受到企業內部董事會成員、管理階層及其他個人之影響。
風險管理導向之內控制度	企業內部用以制定策略，並識別當中可能影響目標達成之潛在事項，以及在風險胃納程度內為風險管理，據以合理保證目標之達成，且由董事會、管理階層及各成員所實施，並受其等影響之作業流程。

[88] *Id.* ¶ 11.

doi:10.6342/NTU202000744

表（四）：內控制度概念與定義之變遷

第一項 內部牽制

首先，本文認為內控制度最重要之精神係「內部牽制（internal check）原則」，即透過金融機構內部各成員彼此間形成相互檢查、制衡及監督之關係，以偵測業務執行過程中可能之疏漏或錯誤，或避免詐欺等非法行為之發生[89]。為充分貫徹內部牽制原則，不同部門或各個職員之間應透過專業化與不相容之職務分離，由兩位以上職員或兩個以上部門共同辦理一項業務[90]，其理由在於：第一，假設某位負責保管銀行資金之職員同時負責財務報表之查核，在無其他職員監督或複檢之情況下，該名職員得於會計紀錄上為不實之登載或其他舞弊行為發生之可能性或誘因，或將遠高於職務分離之情形[91]。第二，藉由職務分離、多人經手業務之方式，得使不同部門或職員相互覆核交易紀錄、偵測錯誤，降低個人於無意識狀態下發生疏漏之可能性。第三，倘若確實執行職務分離與覆核程序，亦將增加多人有意識地串通舞弊遭到查知或注意之可能性，從而得以減少舞弊發生之風險。準此，內部牽制作為內部控制之最初形式與概念，於具體制度之設計上，應注意是否落實職務分離與相互覆核之原則，方能達成偵測錯誤、防免舞弊等內控制度之基本功能[92]。

第二項 風險控制

再者，基於認知欲達成各項營運目標，須有效偵測並控管業務執行過程中所生之各項風險，內控制度即有朝向以風險控制為基礎之趨勢發展，且對於組織內部風險管理之成效具有重要影響[93]。正所謂「有風險才有控制」，內部控制之具體制度設計上，除了前述內部牽制、權責分明之基本原則外，尚應具備識別潛在風險，以及在風險胃納程度內為風險管理之功能，以合理確保目標之達成。換言之，為避免管理階層欲達成營運目標而過度追求風險，內控制度即係作為偵測並有效控管風

89 *See* ROOT, *supra* note 1, at 56.

90 *Segregation of Duties*, ASS'N INT'L CERTIFIED PROF. ACCTS. [AICPA], https://www.aicpa.org/content/aicpa/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html (last visited May 29, 2019).

91 *See id.*

92 *See* Ferroni, *supra* note 2, at 8.

93 PAUL HOPKIN, FUNDAMENTALS OF RISK MANAGEMENT: UNDERSTANDING, EVALUATING, AND IMPLEMENTING EFFECTIVE RISK MANAGEMENT 291 (2010).

doi:10.6342/NTU202000744

險之制度或程序，包括協助業務單位辨識與管理日常業務所產生之風險，抑或使董事會獲高階管理階層得清楚掌握組織內部之風險承擔能力與風險承受狀態，俾便隨時檢視風險管理政策是否妥適。

第三項 權責劃分

最後，內控制度係由董事會與高階管理階層所設計與制定，用以達成營運、報導及遵循等目標之作業流程，故該制度本身功能並非係單純為覆核會計數據之準確性或偵測錯誤、預防舞弊，亦包括規範各部門員工之行為、確保遵循與落實公司內部管理政策與規範，據以提升公司內部治理之目的。然而，建置內控制度並非為使董事會或高階管理階層用以對其下級部門或員工進行監控，抑或為自上而下要求無條件執行上位者之各項政策，應係上至董事會、下至一般職員須共同落實者。故於探究內部控制之具體制度設計時，亦應明確釐清董事會、管理階層及一般業務單位諸等內控制度之參與者，各自所扮演之角色與所負之權限與責任範圍，除上述職務分離原則外，亦應避免彼此間具有利益衝突或權責分工不清之情形，例如身兼業務執行與法令遵循單位之職務。

綜上所述，源於內部牽制之概念，內控制度歷經相當之發展與變遷後，現已係董事會與管理階層為落實有效之風險管理，於組織內部所建立，明確劃分董事會、管理階層及各部門個別職員之權限與責任範圍，並須由所有成員共同遵守、運作，據以確保合理達成營運、報導等各項目標之管理流程。

doi:10.6342/NTU202000744

第三章 內部控制之制度設計

第一節　三道防線基本架構

鑑於現代公司內部之組織型態漸趨龐大與部門分工愈發細緻，且其所面臨者係瞬息萬變之經商環境與更為複雜之風險態樣，為順利達成經營目標並有效辨識或控管風險，內控制度之「三道防線」（Three Lines of Defense）即係為了明確劃分不同單位各自於風險管理與內控制度架構之職責範圍[1]。換言之，三道防線架構之設計係有利於個別職員瞭解其所扮演之角色與功能，同時有助每一道防線之單位間進行溝通協調，亦能避免權責不明、逾越職權或利害衝突等情事之發生，以有效落實風險管理與內部控制之制度機能。以下即分別介紹內控制度三道防線之具體架構設計。

第一項 第一道防線

第一道防線係「作業管理」（operational management），即各單位就其日常業務運作範圍，應負責建立並維持內部控制與風險管理程序之有效運作[2]。質言之，為達成高階管理階層所設定之經營目標，同時妥適應對或將面臨之各項風險，各業務單位之職員及其經理人均須具備必要之專業知識與技術，並應可取得作成決策或判斷時所需之資訊，且亦須獲得適當之授權，據以於運作日常業務之過程中，遵行內部建置之風險控制相關政策與程序[3]。基此，作為銀行內部風險管理與控制之第一道防線，各單位或部門之經理人均應依其業務範圍內，評估所有可能產生之風險種類與性質，建置適當之內部控制措施，並應確保單位內職員均能妥適遵循之，且若該內部控制措施或程序有故障或不足等情況發生，經理人即須隨時為必要之調整或修正。理想上，組織內部僅須建置一道防線架構即可達成有效之風險管理與內部控制，惟現實運作結果顯示則不然，故仍須有第二道防線之協助與執行監督方竟其功[4]。

---

[1] *See* INST. OF INTERNAL AUDITORS [IIA], IIA POSITION PAPER: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL 1 (2013).

[2] *Id.* at 3.

[3] *See* CHARTERED INST. OF INTERNAL AUDITORS, POSITION PAPER: THE THREE LINES OF DEFENCE 2 (2019), https://www.iia.org.uk/resources/delivering-internal-audit/position-paper-the-three-lines-of-defence/?downloadPdf=true.

[4] IIA, *supra* note 2, at 4.

doi:10.6342/NTU202000744

第二項 第二道防線

第二道防線則屬有別於第一道防線之「風險管理與遵循」(risk management and compliance),該防線之目的與功能為督導並確保第一道防線有效運作,且就風險與遵循事項建立內部控制框架與訂定整體管理政策[5]。惟第二道防線具體組成單位,依各該建置與適用之組織與產業型態或有不同,然而基本皆包括風險管理與遵循[6]兩者。首先,風險管理單位(或委員會)主要作用在於促進第一道防線各業務單位落實內部風險管理程序、監督整體風險承擔狀況、協助辨識目標風險與曝險程度,並於組織內部報導與有效傳遞風險相關資訊。再者,遵循單位主要係負責法令規章遵循制度之設計、管理及執行,同時應訂定組織內部法令遵循情況之評估內容與程序,依此督導並確保各業務單位妥適遵守外部法規與內部規章,以避免產生法律風險,且遵循單位通常係隸屬於高階管理階層(例如總經理)[7]。

銀行、保險公司等金融機構於內控制度第二道防線設置獨立專責或專職單位之目的,在於促使其能維持內控制度之合理運作,適當辨識與管理特定風險,抑或有效控制營運過程中可能適逢之關鍵風險指標(Key Risk Indicator,KRI),以符合衡量營運目標之關鍵績效指標(Key Performance Indicator,KPI)[8]。因此,除前述風險管理與遵循等兩項專責單位以外,第二道防線獨立專責單位之設置或專責人員之指派,亦逐漸擴大涵納洗錢防制與資恐打擊[9]、資訊安全[10]、乃至於個人資料保

---

[5] *See* CHARTERED INST. OF INTERNAL AUDITORS, *supra* note 3, at 2.

[6] 或有認為將「compliance」乙詞翻譯為「法令遵循」並非妥當,倘以日文解讀,應指「(為了)倫理與法令的協調一致(所需之方法架構)」方為適切;或有依該詞遵從、依從、遵守等原意,譯為「合規」者。平野温郎(著),高志明、林奕延(譯)(2019),〈日系企業全球發展下的遵法風險・危機與對應策略〉,台灣企業法律學會(編),《國際公司治理與企業法遵》,頁 21,臺北市:新學林。惟在此慮及行文之簡潔,本文暫且譯為「法令遵循」,至於「compliance」之意義與具體意涵等相關討論,謹待於後續章節予以詳述。

[7] 此外,部分組織內部亦會針對健康與安全、供應鏈、環境或品質等特定事項分別設置遵循單位。IIA, *supra* note 2, at 4; 黃劭彥、陳俊志(2018),〈台灣銀行業內部控制三道防線之探討〉,《月旦會計實務研究》,2 卷 2 期,頁 57。

[8] 黃劭彥、陳俊志,前揭註 7。

[9] 洗錢防制法第 6 條第一項、金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條、保險公司與辦理簡易人壽保險業務之郵政機構及其他經金融監督管理委員會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法第 6 條。

[10] 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 條之 1、內部控制及稽核制度實施辦法第 6 條之 1。

doi:10.6342/NTU202000744

護、誠信經營[11]等。綜言之，第二道防線之權責應包括協助高階管理階層達成所訂目標、監督第一道業務單位內控制度執行狀況、定義風險管理角色與其職責、須訂風險管理架構或政策、分析組織風險胃納等，並應定期將風險管理成效與未來須為調整之處呈報予高階管理階層，以資因應或修正[12]。

第三項 第三道防線

第三道防線「內部稽核」（internal audit）之主要功能為審酌、評估第一道與第二道防線之實際運作成效，並立基於高度獨立性與客觀性，依其職權主動提供專業查核意見與觀點予董事會與高階管理階層[13]，以協助其等評估風險管理與內部控制相關制度、政策及程序是否均有效運作，且適時給予改進或修正建議[14]。基此，內部稽核單位或人員均應秉持客觀公正之立場，依循國際公認準則之規定獨立執行稽核業務並作成查核報告，以作為高階管理與經營階層檢討修正內控制度之專業意見[15]。

簡言之，內控制度三道防線分別具有風險承擔與管理職能、風險督導職能，以及獨立風險確保職能，抑且為能有效發揮各該防線應有之機能，組織內部之董事會與高階管理階層應負責明確界定與協調不同防線各自應有之義務與職責。至內控制度三道防線彼此間所負之風險管理相關責任，如下表（五）所示：

第一道防線	第二道防線	第三道防線
風險承擔與管理	風險控制與遵循	風險確保
• 業務經營管理	• 有限之獨立性[16] • 主要風險報告對象為高階管理階層	• 內部稽核 • 高度獨立性 • 主要對口董事會、審計委員會等治理單位

[11] 上市上櫃公司誠信經營守則第 14 條。

[12] *See* IIA, *supra* note 2, at 4-5.

[13] 黃劭彥、陳俊志，前揭註 7。

[14] *See id.* at 5; *see also* CHARTERED INST. OF INTERNAL AUDITORS, *supra* note 3, at 2.

[15] *See id.* at 6.

[16] 此處所稱「有限之獨立性」係相對於第三道防線而言，蓋因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，惟其本質仍屬管理單位，與第三道防線係超然獨立之查核單位有所差異。*Id.* at 6.

doi:10.6342/NTU202000744

表（五）：風險管理與三道防線之控制架構

第二節　銀行內控制度實務守則

為協助銀行完善其內控制度，強健企業經營之體質，中華民國銀行商業同業公會依據主管機關金管會之授權辦法訂有「銀行內部控制三道防線實務守則」，據以推動前揭內部控制三道防線架構之落實[17]。銀行業建置與落實執行內部控制「三道防線」主要目的，係為明確釐清每一道防線之權責範圍，俾利銀行內部各單位成員均能瞭解於銀行整體風險與控制架構中所扮演之角色與其功能[18]，同時亦得加強風險管理與內部控制相關工作之溝通協調，據以避免業務執行過程中，發生作業相關之疏失或舞弊，以及預防風險。三道防線之內涵具體分述如下。

第一項 三道防線架構

第一道防線係由銀行內部各個業務單位所組成，其等均應就各自之功能、業務範圍、營運活動與其相關風險特性，設計並執行有效之內部控制程序，並應辦理自行查核[19]，故負有執行其業務範圍內內部控制規範之初始責任，並應持續、確實地自我管控日常業務所生之各種風險，且須視情形向第二道防線報告[20]。

第二道防線則包括風險管理與法令遵循單位及其他專責單位，其主要任務概可化約為「訂定」、「監督」及「呈報」等三項目：一，訂定銀行內部整體風險管理政策與制度架構、二，監督銀行整體風險承擔能力與風險承受狀況、三，定期向銀行董事會或高階管理階層報告其辨識、衡量及執行風險控管之結果[21]。簡之，除了處理銀行內部整體之營運與風險外，第二道防線尚應監督與協助處理第一道防線所疏漏之個別問題[22]。

第三道防線為內部稽核，其應獨立執行稽核業務，查核與評估前述內部控制第一與第二道防線之有效性，並適時提供改進建議，據以協助董事會與高級管理階層

[17] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 6 條；銀行內部控制三道防線實務守則第 1 條。

[18] 銀行內部控制三道防線實務守則第 2 條。

[19] 銀行內部控制三道防線實務守則第 3 條。

[20] 銀行內部控制三道防線實務守則第 7 條。

[21] 銀行內部控制三道防線實務守則第 4 條、第 8 條。

[22] 銀行內部控制三道防線實務守則第 4 條。

doi:10.6342/NTU202000744

確保銀行內控制度之有效運作[23]。析言之，就銀行內部控制三道防線之定位而論：前兩者係屬風險管理之範疇，後者則屬內部之獨立監督機制。銀行內控制度三道防線之意涵，簡要如下表（六）所示：

第一道防線	
自行查核	• 銀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。 • 負責辨識及管理風險，針對該風險特性建置內部控制程序，以涵蓋所有相關營運活動。 • 除確保前開內控程序之有效運作之外，並依需要向第二道防線報告。
第二道防線	
風險管理、法令遵循及其他專責（專職）單位	• 各專責單位就其主要風險類別負責銀行整體風險管理政策之訂定、風險承擔能力之監督，及風險現況之承受。 • 向董事會或高級管理階層報告風險控管情形。 • 依其特性協助及監督第一道防線辨識及管理風險。 • 性質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。
第三道防線	
內部稽核	• 超然、獨立地執行稽核業務，查核與評估第一、二道防線進行風險監控之有效性。 • 協助董事會及高級管理階層評估內控制度是否有效且持續運作，並適時提供改進建議。

表（六）：銀行內控制度之三道防線及其理念

第二項 五項構成要素與原則

為使內控制度得支持銀行達成任務、策略或商業等相關目標，有效內控制度應具備控制環境、風險評估、控制活動、資訊與溝通，以及監督作業等五項重要構成要素[24]。此外，本文細繹前揭內控制度實務守則與該五項內控制度構成要素後認為，建構內控制度之基本原則主要包括董事會與高階管理階層之治理與控制文化、風

[23] 銀行內部控制三道防線實務守則第 5 條、第 9 條。

[24] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條。

doi:10.6342/NTU202000744

險辨識與評估、控制活動與職務分工、資訊與溝通、監督與更正缺失等五項，以下依序述之。

第一款 控制環境下治理與控制文化

「控制環境」係銀行設計與執行內控制度之基礎，包括經營之誠信與道德價值、董事會與審計委員會之治理監督責任、組織結構、權責分派、人力資源政策、績效衡量及獎懲，以及分別針對董事、員工訂立之內部行為準則等[25]。由於控制環境為有效運作內控制度之基石，董事會與高階管理階層除須依其職責，於銀行內部建置內控制度以外，尚應負責提升銀行內部良好經營誠信與道德價值之風氣、建立並展現整體風險意識與控制文化[26]，具體作法例如建立內部行為準則或公司治理準則，並要求所有人員均應確實依循[27]。此外，董事會或審計委員會之各成員均應負起治理與監督責任[28]，自上而下形塑且要求銀行內部具體落實內控制度作為其金融機構文化，避免內控制度與其相關政策或程序淪於形式。

第二款 風險辨識與評估

「風險評估」須由管理階層確立並連結銀行內部不同層級單位之各項營運目標，以及評估其適合性作為先決條件，再行考量外部環境與商業模式改變或將對達成目標之影響，以及可能發生之舞弊情事，據以作成銀行整體風險評估結果，協助銀行得及時設計、修正及執行必要之控制作業[29]。質言之，銀行董事會或高階管理階層於擬定經營、業務或法令遵循等具體目標後，風險管理、法令遵循、財務控制或資訊安全等專責單位（主要係第二道防線）應就銀行主要風險類別，負責制定整體風險管理政策，並持續監督內部控制與風險管理之運作，且定期向董事會或高階管理階層報告風險控管情形[30]。基此，除執行日常業務以外，銀行內部各業務單位（即第一道防線）應就其業務範圍內可能發生或存在之風險，以及對於可能影響前

[25] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條第一款。

[26] DOUGLAS J. ANDERSON & GINA EUBANKS, LEVERAGING COSO ACROSS THE THREE LINES OF DEFENSE 4 (2015).

[27] J. STEPHEN MCNALLY, THE 2013 COSO FRAMEWORK & SOX COMPLIANCE: ONE APPROACH TO AN EFFECTIVE TRANSITION 5 tbl.3 (2013).

[28] ANDERSON & EUBANKS, *supra* note 26, at 4 fig.3; 銀行內部控制三道防線實務守則第 6 條。

[29] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條第二款。

[30] ANDERSON & EUBANKS, *supra* note 26, at 6-7 & fig.5; 銀行內部控制三道防線實務守則第 8 條。

doi:10.6342/NTU202000744

述具體目標之達成之重大風險，均須予以辨識、分析及定義，以利後續弭平、降低或管控該等風險[31]。

第三款 控制活動與職務分工

至於「控制作業」即係指銀行根據前述風險評估結果，於銀行內部所有層級、業務流程之各階段、所有科技環境，以及所屬子公司等範圍，採用並執行之適當政策與程序，例如監督與管理、適當之職務分工，尤應注意管理階層與員工不應擔任責任相衝突之工作或職位[32]。原則上，為期有效控制地達成目標過程中所可能遭遇之各項風險，無論第一道防線之業務單位或第二道防線之各專責單位，均應建立具有風險控制活動機能之內控制度，包括適當政策與管理程序，進而得將整體風險控制於銀行之「風險胃納」（Risk Appetite）程度以內[33]。

再者，銀行於設定控制作業或程序等控制相關活動時，尚須劃定明確之職務分工，亦即執行內部控制活動者應不得兼任監督或評估內控制度執行成效之相關職位，此舉除係為落實內控制度之內部牽制原則外，且為避免因個人之權責不明或混淆所衍生之利害關係或責任衝突，導致減損內控制度其應有制度機能之不利結果。

第四款 資訊與溝通

「資訊與溝通」係用以支持內部控制其他構成要素之持續運作，故此要素可細分為產生、提供及保存等三種功能：首先，銀行之內控制度應得產生符合規劃、執行及監督等目的之所需，無論係來自內部或外部之攸關、具品質之資訊；再者，內控制度亦應具備得提供不同資訊需求者適時取得所需資訊之機制，並應確保所有資訊得經由有效之溝通管道，於銀行內部與外部之間皆能進行有效溝通；抑且，內控制度尚須得以完整保存財務、營運及遵循相關之所有資訊[34]。

銀行內部各業務單位與內控制度三道防線之間，均須依風險管理與內部控制

---

[31] ANDERSON & EUBANKS, *supra* note 26, at 5 & fig.4; 銀行內部控制三道防線實務守則第 7 條。

[32] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條第三款。

[33] ANDERSON & EUBANKS, *supra* note 26, 5 figs.4 & 6; 銀行內部控制三道防線實務守則第 7、8 條。所謂「風險胃納」（Risk Appetite），係指銀行準備所能接受之風險程度，亦即風險發生後，銀行有信心其能夠即時運用現有之相應資源（或謂能夠付出相當成本）以著手應對或有效控制該風險之程度。

[34] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條第四款。

doi:10.6342/NTU202000744

架構建置適當之資訊傳遞與溝通管道，以利各防線成員皆能順利取得於執行內控程序所需之相關資訊，且無論於內或於外均能相互進行充分溝通協調，進而確實執行或管理各人應負之職責[35]。再者，董事會為落實對於內控制度之監督責任，確保並維持內部控制整體架構之運作，除應賦予董事會成員足夠權限，得經由銀行內部系統取得足夠之數據與資訊外，尚應建立與銀行各業務或管理單位間適當之溝通管道，以使董事會各成員得向特定對象或單位，諮詢其對於銀行業務運作有疑慮或不清之處，俾能立於充分資訊之基礎，就重大決策作成正確判斷[36]。

第五款 監督與更正缺失

最後，「監督作業」之目的則為確定前述內控制度之各項組成要素是否均已存在並持續運作，檢驗方式包括持續性評估、個別評估或兩者併行：前者係銀行內部不同層級於營運過程中之例行評估、後者則係由內部稽核人員、審計委員會或董事會等其他人員所進行之評估，惟無論係何者，對於其所發現之內控制度之缺失，均應向適當層級之管理階層、董事會或審計委員會溝通，並及時改善[37]。質言之，由於銀行建置內控制度的目的係為偵測並控制內部各單位日常業務執行時所生之各種風險，惟外部商業環境與可能所面臨之風險態樣均將隨時空之不同而有所改變，故為合理確保內控制度得以持續有效運作，監督作業之另一功能即係偵測內控制度是否仍足以應付現時可能發生之各種風險。基此，倘若經監督或稽核單位獨立評估後認為，內控制度之設計有所缺失或顯有不足之處，即應適時提供改進建議[38]，以為董事會與高階管理階層即時或於日後檢討修正內控制度之依據[39]。

第三節　三大內部控制目標

包括董事會、高階管理階層在內所有銀行業從業人員，均應遵行內部控制相關程序與規範之目的，除係為共同協力促進銀行業之健全經營外[40]，亦係為有效運作

---

35 ANDERSON & EUBANKS, *supra* note 26, 5 figs.4 & 6; 銀行內部控制三道防線實務守則第 10 條。

36 *See* David F. Larcker & Brian Tayan, *Netflix Approach to Governance: Genuine Transparency with the Board* 1 (Rock Ctr. for Corp. Governance, Stanford Univ., Stanford Closer Look Series No. CGRP71, 2018).

37 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條第五款。

38 ANDERSON & EUBANKS, *supra* note 26, 5 figs.4 & 7; fig.5.

39 金融控股公司及銀行業內部控制及稽核制度實施辦法第 9 條。

40 金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條。

doi:10.6342/NTU202000744

內控制度，藉此使董事會與管理階層均得合理確保下述三點事項之落實[41]：充分理解銀行內部營運目標及其達成之進度狀況、編製與出具之各項報導內容均屬正確詳實、業務活動均遵循現行相關法律或命令等規範。簡言之，內控制度之三大目標即為營運、報導及遵循，以下依序析述之。

第一項 營運目標

營運（Operation）目標指銀行業務經營之效果與效率，包括達成營運與財務之獲利與績效指標，以及維護與保障其所有資產之安全[42]。所謂營運之「效果」（effectiveness）指基於「營利」係創設公司最主要之目的[43]；或有謂公司乃營利行為之主體、營利則是公司社會活動之內容[44]，縱使獲利並非公司存在之唯一主張，惟亦無法否認其對於公司長期營運之重要性。再者，營運之「效率」（efficiency）即係確保公司所掌握之各項資源，例如人力、資金、時間及設備等，均能為有效利用以創造最大價值。

質言之，健全的內控制度係為促進金融機構充分運用其所有之資產或資源[45]，執行有效果、具效率之營運活動，同時亦能妥適因應其可能面臨之重大商業、作業、財務或遵循等不同風險，俾利其達成所設定之各項營運目標[46]。例如透過內控制度之運作，得以使公司於判斷現有與潛在之風險後，妥適因應風險及其他重大控制相關闕漏；或降低於決策過程中，錯誤、疏失或規避內控制度等人為因素發生之可能性及其所造成之不利影響[47]；或保障與維護營運時需用之資產，避免不當使用或造成額外損失；或防免業務執行過程中出現詐欺行為；抑或確保金融機構內部成

41 *See* STEVEN J. ROOT, BEYOND COSO: INTERNAL CONTROL TO ENHANCE CORPORATE GOVERNANCE 137-38 (1998).

42 建立內部控制制度核心原則 1.3(1)；金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條第一項第一款。

43 公司法第 1 條第一項。

44 楊岳平（2011），《公司治理與公司社會責任——企業併購下股東、債權人、員工、投資人之保護》，頁 5，臺北市：元照。

45 *See* ROOT, *supra* note 41, at 119.

46 *See* FIN. REPORTING COUNCIL [FRC], GUIDANCE ON RISK MANAGEMENT, INTERNAL CONTROL AND RELATED FINANCIAL AND BUSINESS REPORTING ¶ 28 (2014) [hereinafter FRC'S RISK GUIDANCE]; FRC, INTERNAL CONTROL: REVISED GUIDANCE FOR DIRECTORS ON THE COMBINED CODE ¶ 19 (2005) [hereinafter THE TURNBULL REPORT 2005].

47 FRC'S RISK GUIDANCE, *supra* note 46, ¶ 28.

doi:10.6342/NTU202000744

員間存在明確之權利與責任劃分等，據以提升金融機構整體業務執行之實效[48]。

值得注意者係，由於營運活動與其業務績效乃繫諸於金融機構內部董事會、高階管理階層及所有員工等人為之努力，又如政府機關政策之調整、整體經濟環境之震盪等各式外部不確定性因素，或將對於金融產業之發展產生影響[49]。抑且就不同銀行間而言，基於彼此內部之人力或資金規模、業務種類等多寡有別，各銀行所能投注之經營成本與資源未必均等，造成其所能設定與達成之營運目標亦未必宜等同視之。反觀報導與遵循兩項目標，由於兩者基本上均有明文或既定之外部標準（external standards）可資參考依循，因此有效運作之內控制度原則上得合理保證該兩項目標之達成，惟營運目標則無法形成如此確信[50]。

職是之故，或謂此係內控制度侷限性之所在，然而本文認為，銀行作為有限公司之型態固有營運以獲取利潤之考量，惟銀行業同時作為金融主管機關高度監管產業，更須重視者應屬其充分且正確資訊之揭露、營運合乎金融監理相關規範與標準等效能。換言之，由於動搖銀行健全經營基石之情事通常係肇因於業務單位從事風險性高且違法之行為、抑或內部滋生舞弊或詐欺等弊端，對於達成銀行健全經營之營運目標而言，首應於銀行內部徹底落實與執行者，即係風險管理與法令遵循等內控制度之基本功能（詳後述），故內控制度之妥適建置與有效運作仍屬必要。

第二項 報導目標

報導（Reporting）目標係指確保銀行內部與外部報導之品質[51]，具有可靠性、及時性、透明性或符合相關規範[52]。前述所稱之「報導」包括銀行業內部與外部財務報導與非財務報導，且外部財務報導之目標，涵蓋確保對外出具之財務報表係依照一般公認會計原則編製、交易經適當核准等目標[53]。

---

[48] *See* THE TURNBULL REPORT 2005, *supra* note 46, ¶ 19.

[49] *See* ROOT, *supra* note 41, at 124.

[50] *See id.*

[51] FRC'S RISK GUIDANCE, *supra* note 46, ¶ 28; *see also* THE TURNBULL REPORT 2005, *supra* note 44, ¶ 19.

[52] 建立內部控制制度核心原則 1.3；金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條第一項第二款。

[53] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條第三項。

doi:10.6342/NTU202000744

第一款 財務報導

植基於「強制資訊公開原則」之要求，為使市場、投資者或債權人等利害關係人能獲取充分且正確之資訊，用以作成投資決定（informed decision）[54]，銀行除應於每屆營業年度終了後，編製年度財務報告以外[55]，並應將營業報告書、季度與月度財務報告[56]、盈餘分派或虧損撥補之決議等，分別報請中央主管機關與中央銀行備查[57]。倘若發生對股東權益或證券價格有重大影響之事項，銀行亦須即時揭露並向主管機關申報該事項[58]。再者，鑒於銀行業與一般商業或製造行業特性之不同，並為利各銀行於編製財務報告時能有一合理與一致性之規範，金管會依據證券交易法第 14 條第二項之授權規定訂有《公開發行銀行財務報告編製準則》[59]。該準則表示，銀行財務報告之編製應循序依據本準則、準則有關法令、《證券發行人財

---

[54] 關於「公開原則」之意義及其功能的完整論述與分析，請參閱：曾宛如（2012），《證券交易法原理》，六版，頁 33-47，臺北市：元照。

[55] 銀行法第 49 條第一項前段。依據前條項之授權規定，金管會另訂定《銀行年報應行記載事項準則》。該準則中揭示銀行編製年報之基本原則為：一、所載事項應具有時效性，且不得有虛偽或隱匿之情事。二、內容應力求翔實明確，文字文字敘述應簡明易懂，善用統計圖表、流程圖或其他圖表，必要時得以中、外文對照方式刊載或另行刊印外文版本（第 3 條）。再者，年報編製內容應記載事項包括（第 7 條）：一、致股東報告書（第 8 條）。二、銀行簡介（第 9 條）。三、公司治理報告（第 10 條）。四、募資情形（第 11-17 條，包括資本及股份、金融債券、特別股、海外存託憑證、員工認股權憑證、限制員工權利新股及併購之辦理情形暨資金運用計畫執行情形。）五、營運概況（第 18 條）。六、財務概況（第 19 條）。七、財務狀況與財務績效之檢討分析與風險管理事項（第 20 條）。以及八、其他特別記載事項（第 22 條）。當中「公司治理報告」之應記載事項即涵蓋公司治理運作情形，該準則要求銀行須揭露其「內部控制制度執行狀況」，包括內部控制制度聲明書，以及委託會計師專案審查內部控制制度者，應揭露會計師之審查報告（第 10 條第四款第十目）。此外，倘若於最近二年度及截至年報刊印日止，銀行曾因違反法令經本會（按：金管會，後同）處以罰鍰，抑或經金管會依銀行法第 61 條之 1 規定作成處分事項，即應揭露其違法受處分及主要缺失與改善情形（第 10 條第四款第十一目）。

[56] 銀行法第 49 條第一項前段、證券交易法第 36 條第一項。另外，依據證券交易法第 14 條第二項之授權規定，金管會對於公開發行銀行另訂定發布《公開發行銀行財務報告編製準則》。根據該準則，所謂「財務報告」係指財務報表、重要會計項目明細表及其他有助於使用人決策之揭露事項及說明（第 4 條第一項）。前項所稱之「財務報表」，主要係指資產負債表、綜合損益表、權益變動表及現金流量表等（第二項、第 20 條）。

[57] 銀行法第 49 條第一項後段。

[58] 證券交易法第 36 條第三項第二款。該款所稱具有重大影響應揭露之事項，可參考證券交易法施行細則第 7 條之規定。

[59] 公開發行銀行財務報告編製準則部分條文修正總說明（民國（後同）100 年 12 月 26 日修正）；公開發行銀行財務報告編製準則修正總說明（100 年 8 月 19 日修正）；公開發行銀行財務報告編製準則部分條文修正總說明（96 年 6 月 28 日修正）；公開發行銀行財務報告編製準則修正總說明（94 年 9 月 27 日修正）。

doi:10.6342/NTU202000744

務報告編製準則》及一般公認會計原則辦理[60]。基此，由於財務與業務文件係利害關係人瞭解銀行營運表現與財務狀況之重要資訊來源管道，倘若有不實或錯誤資訊存乎其中，將使投資人或債權人等作成錯誤判斷，以致蒙受損失。故內控制度之目標即包括經由適當的記錄、勾稽及覆核程序，以及精確的會計標準，確保銀行財務報導之忠實。

由於近十年間國際企業舞弊案件頻仍，包括安隆（Enron）、環球電信（Global Crossing）、世界通訊（WorldCom）等大型上市公司相繼爆發財報不實、證券詐欺及會計醜聞事件，除了導致公司破產、投資人利益受損之後果外，更凸顯公司未能有效落實內部控制程序（尤指財務資訊方面）之問題[61]。故為確保公司之財務報導與各項揭露資訊均符合法令規範、提升其正確性與可靠性，以及增加金融市場中投資人之信心，達成投資人保護之目的[62]，美國國會於 2002 年通過《2002 年上市公司會計改革與投資者保護法案》（Public Company Accounting Reform and Investor Protection Act of 2002）[63]，該法案之重要內容即係規範公司財務報告[64]或重大財務資訊揭露[65]相關之內部控制。舉例言之，為確保公司出具之年報或季報係經允當表達、抑或於揭露公司財務狀況與營運結果時，並無隱瞞任何具重大性（material）之事實[66]，公司內部應有職員[67]負責設計、建置及維持財務報告相關內部控制[68]，且須於財務報告發布前相當期間內，定期評估內部控制之有效性[69]，並應將評估結果

---

[60] 公開發行銀行財務報告編製準則第 3 條第一項。所稱「一般公認會計原則」，係指經金管會認可之國際財務報導準則、國際會計準則、解釋及解釋公告（第二項）。另外，依據前述《證券發行人財務報告編製準則》第 3 條第二項，金管會認可之國際財務報導準則、國際會計準則、解釋及解釋公告，係指金管會證券期貨局網站「國際財務報導準則（IFRSs）下載專區」公告之各年度適用之 IFRSs，自 109 年 1 月 1 日生效（108 年 7 月 29 日金管證審字第 1080323028 號令）。

[61] *See* STEPHEN M. BAINBRIDGE, CORPORATE GOVERNANCE AFTER THE FINANCIAL CRISIS 140-41 (2012).

[62] *See* Michael A. Perino, *Enron's Legislative Aftermath: Some Reflections on the Deterrence Aspects of the Sarbanes-Oxley Act of 2002* 2 (Ctr. for Law & Econ. Studies, Columbia Univ. Sch. of Law, Working Paper No. 212, 2002); JAMES HAMILTON & PETER RASMUSSEN, GUIDE TO INTERNAL CONTROLS: UNDER SECTION 404 OF THE SARBANES-OXLEY ACT 11 (2d ed. 2007); *infra* note 63.

[63] An Act to Protect Investors by Improving the Accuracy and Reliability of Corporate Disclosures Made Pursuant to the Securities Laws, and for Other Purposes, Pub. L. No. 107-204, 116 Stat. 745 (2002). 又稱「沙賓法案」（Sarbanes-Oxley Act of 2002, SOX）。

[64] *Id.* § 404.

[65] *Id.* § 302.

[66] *Id.* § 302(a) & 302(a)(2).

[67] 所稱「職員」指首席執行長（Principle Executive Officer）、首席財務長（Principle Financial Officer）或其他執行與前述兩職位類似職務之人（"[P]erson performing similar functions"）。*Id.* § 302(a).

[68] *Id.* § 302(a)(4)(A) & 302(a)(4)(B).

[69] *Id.* § 302(a)(4)(C).

doi:10.6342/NTU202000744

呈現於該財務報告內容當中[70]。準此，財務報導無論對個別投資人或整體金融市場而言，係屬重要之文件或資訊，故內控制度目標之一，即在於合理確保財務報導之忠實、及時及可靠。

第二款 非財務報導

除了前揭財務報導外，非財務性報導之詳實與充分揭露亦具有同等重要性。茲以 2001 年安隆公司案為例，安隆公司曾為全球最大的電力與天然氣等能源業巨擘，其亦大量投資發電廠、輸油管及能源公用設施。然而，在其業務持續成長擴張、財務狀況看似良好之帳面數字背後，實際上卻是由大量舉債所支撐，且同時存在未充分揭露之關係人交易與顯著之利益衝突[71]。由此可知，僅憑財務報導所揭露之數據資料，似不足以充分反映公司財務體質、營運狀況及治理情形，故包括環境、社會及公司治理（Environmental, Social, and Governance，以下簡稱 ESG）等內容，因其往往影響公司所面臨之挑戰、經營策略及營運績效，且結果最終亦將反映於公司之財務面向，該等非財務報導則愈發受到重視。意即，由於 ESG 主要係反應一公司得否為永續發展之重要資訊，故其逐漸作為機構投資人訂定投資決策之標準，甚或成為金融監管者強制要求公司應揭露之內容[72]。舉例言之，金管會對此即建議機構投資人將公司之非財務報導或非財務性因素納入其投資決策，除了能夠提高投資效益以外，亦可健全市場與社會發展、維護環境之永續性，達成「永續經營與社會責任型投資」（Sustainable and Responsible Investment）之目的[73]。

歐盟執行委員會（European Commission，以下簡稱歐盟執委會）於 2011 年即肯認，歐盟成員國均應訂定並要求其境內所有企業須遵守社會與環境等非財務資訊揭露之規範，同時須逐步提升、持續改善該非財務資訊揭露之透明程度[74]。復於 2014 年，歐盟執委會修正第 95 號指令（Directive 2014/95/EU），要求銀行、保險公司，以及其他經主管機關認定具公共利益之法人或上市公司，應揭露包括環境保

---

[70] *Id.* § 302(a)(4)(D).

[71] *See* BAINBRIDGE, *supra* note 61, at 139-40.

[72] *See* Florencio Lopez-de-Silanes et al., *ESG Performance and Disclosure: A Cross-Country Analysis* 3-4 (European Corp. Governance Inst., Working Paper No. 481/2019, 2019).

[73] 103 年 10 月 3 日金管證發字第 1030039119 號函。

[74] Directive 2014/95/EU, of the European Parliament and of the Council of 22 October 2014 Amending Directive 2013/34/EU as Regards Disclosure of Non-Financial and Diversity Information by Certain Large Undertakings and Groups, 2014 O.J. (L 330) 1, 1 [hereinafter Directive 2014/95/EU].

doi:10.6342/NTU202000744

護、社會責任、員工待遇、尊重人權、反貪腐與反賄賂，以及董事會成員多樣性等政策之非財務資訊[75]。歐盟執委會指出，揭露如社會、環境等永續發展相關非財務資訊，得協助企業評估、監控及管理其經營績效及其對於社會之影響，亦有助企業辨識永續性風險（substantiality risk）、增加投資人與消費者對其之信任[76]。再者，由於非財務性資訊係雜糅長期獲利、社會正義及環境保護等重要考量，故該資訊之揭露實為促使全球經濟邁向永續發展之所不可或缺[77]。準此，歐盟議會即要求歐盟執委會應提出企業揭露非財務資訊之法案，藉以創造企業較為彈性之政策擬定與執行空間、抑或透過各式面向踐履其社會責任之選擇多樣性，除了滿足投資人與利害關係人之需求外，就意欲瞭解個別企業對於社會造成何種影響之消費者而言，亦能提供通暢之資訊取得管道[78]。

聯合國環境規畫署（United Nations Environment Programme，UNEP）「金融倡議」（Finance Initiative，FI）研究報告亦指出，倘若將 ESG 概念全面且持續性地納入企業經營或投資決策之考量，除了短期內普遍得獲致較佳之財務表現以外，亦得促使企業或投資人更加重視個人道德價值、社會永續發展等長遠目標[79]。據此，金管會為鼓勵上市上櫃公司積極提升公司治理與社會責任文化，同時加強諸如金融業等所適用之公司治理與內部控制相關法規範標準[80]，其首先推動證券交易所之全資子公司「臺灣指數公司」與英國倫敦證券交易所集團（London Stock Exchange Group，LSEG）所屬「富時羅素」（FTSE Russell）合作編製、針對上市公司於環境（E）、社會（S）及治理（G）三大面向予以評鑑之「臺灣永續指數」（FTSE4Good TIP Taiwan ESG Index），並透過財務指標篩選指數成分股，藉以表揚永續發展指數表現良好之公司[81]。

再者，基於非財務資訊之揭露愈發受到利害關係人重視，為提升非財務資訊內

---

[75] *Non-Financial Reporting*, EUROPEAN COMM'N, https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting/non-financial-reporting_en (last visited Oct. 3, 2019); *id.* at 2.

[76] Directive 2014/95/EU, *supra* note 74.

[77] *Id.*

[78] *Id.*

[79] *See* U.N. ENV'T PROGRAMME FIN. INITIATIVE ASSET MGMT. WORKING GRP., SHOW ME THE MONEY: LINKING ENVIRONMENTAL, SOCIAL AND GOVERNANCE ISSUES TO COMPANY VALUE 4 (2006).

[80] 金融監督管理委員會證券期貨局〔以下簡稱金管會證期局〕（2018），《新版公司治理藍圖（2018-2020）》，頁 6。

[81] 同前註，頁 8。

doi:10.6342/NTU202000744

容之揭露品質、加強包括金融保險業在內之上市、上櫃公司對於企業永續發展之重視，以及引導各產業內良性競爭[82]，金管會規定銀行、金控公司等金融機構，應於其年報之公司治理報告中，記載公司治理運作、履行社會責任、誠信經營等情形[83]。其亦推動將企業社會責任（Corporate Social Responsibility，CSR）、誠信經營、永續發展等非財務資訊內容之揭露及其品質，納入公司治理評鑑指標[84]。所謂履行社會責任情形，係分別從落實公司治理、發展永續環境、維護社會公益、加強具攸關性與可靠性之企業社會責任資訊之揭露等四項內容予以評估[85]。

抑且，金管會於 2014 年 9 月起，即採取類似上揭歐盟第 95 號指令之作法，強制要求包括金融保險業在內之特定產業或公司[86]，應依據全球永續性報告協會（Global Reporting Initiative，以下簡稱 GRI）所制訂之最新「GRI 永續性報導準則」（GRI Sustainability Reporting Standards; GRI Standards，以下簡稱 GRI 準則）版本，編製與申報企業社會責任報告書[87]。GRI 準則主要係由兩部分所構成：第一部分為通用準則，包括基礎報導原則、一般揭露及管理方針。第二部分為特定主題準則，包括經濟、環境及社會等三項重大主題。基此，金融機構於編製企業社會責任報告

---

[82] 同前註，頁 31。

[83] 公開發行公司年報應行記載事項準則第 10 條第四款第三至六目、銀行年報應行記載事項準則第 10 條第四款第四、六、七目、金融控股公司年報應行記載事項準則第 10 條第四款第四、六、七目、票券金融公司年報應行記載事項準則第 10 條第四款第四、六、七目、信用合作社年報應行記載事項準則第 16 條第八款。舉例言之，履行社會責任情形包括金融機構對環保、社區參與、社會貢獻、社會服務、社會公益、消費者權益、人權及安全衛生與其他社會責任活動所採行之制度與措施及履行情形。

[84] 依據「第 6 屆（108 年度）公司治理評鑑指標」第四部分「落實企業社會責任」，具體非財務資訊內容尚包括人權保障與管理政策（編號 4.6）、工會團體協約（編號 4.7）、員工薪酬與績效調整政策（編號 4.8）、員工福利措施與退休制度（編號 4.9）、員工人身安全與工作環境之保護措施（編號 4.10）、二氧化碳與其他溫室氣體年排放量（編號 4.11）、節能減碳、溫室氣體減量、減少用水或其他廢棄物管理政策（編號 4.12）、環境或能源管理系統之國際性驗證（編號 4.13）等。

[85] 上市上櫃公司企業社會責任實務守則第 4 條、公開發行公司年報應行記載事項準則第 10 條第四款第五目（附表二之二之二）、銀行年報應行記載事項準則第 10 條第四款第六目（附表二之二之二）、金融控股公司年報應行記載事項準則第 10 條第四款第六目（附表二之二之二）、票券金融公司年報應行記載事項準則第 10 條第四款第六目（附表二之二之二）、信用合作社年報應行記載事項準則第 16 條第八款（附表十八）。

[86] 依據臺灣證券交易所「上市公司編製與申報企業社會責任報告書作業辦法」第 2 條之規定，除了金融保險業以外，食品工業、化學工業，以及依證券交易法第 36 條規定檢送之最近一會計年度財務報告，餐飲收入占其全部營業收入之比率達 50%以上、抑或股本達新臺幣 50 億元以上者，均應依該作業辦法之規定，編製與申報企業社會責任報告書。

[87] 臺灣證券交易所「上市公司編製與申報企業社會責任報告書作業辦法」第 3 條。

doi:10.6342/NTU202000744

書時，除了須依照 GRI 準則之要求揭露相關資訊以外，亦應加強揭露其在永續金融重大主題之管理方針與揭露項目，以及各項經營業務中，其為創造社會效益或環境效益所設計之產品與服務[88]。

附值一提，金管會除了要求金融保險業應編製揭露環境、社會及公司治理等非財務報導之企業社會責任報告書外，其亦持續推動並要求金融業所編製之企業社會責任報告書應取得第三方驗證之措施，以及篩選投資人較為關注之非財務報導項目，並研議將該資訊揭露於年報之可能性[89]。關於前述 GRI 準則架構，本文簡要彙整如下表（七）所示[90]：

GRI 準則架構	
通用準則 （100 系列）	• 基礎（GRI 101）：或謂「使用 GRI 準則的起點」，定義報告書內容與報告書品質之報導原則，協助組織決定永續性報告書應包含之資訊內容，以及如何確保該內容之品質。
	• 一般標準揭露（GRI 102）：用以報告組織相關之脈絡資訊，包括組織概況、策略、倫理與誠信、治理、利害關係人議合、報導流程實務等資訊。
	• 管理方針（GRI 103）：用以報告組織係如何管理重大主題之資訊。例如解釋組織自身係如何管理重大主題相關之經濟、環境或社會衝擊[91]，以及利害關係人之合理期望與利益，並提供其係如何鑑別、分析及回應實際與潛在性衝擊之描述性資訊或敘述性解釋。
特定主題準則	針對以下三項重大主題，除揭露其管理方針以外，並由組織從中選擇聚焦報告之特定揭露項目。例如報告組織於該主題之影響，且指出組織對於該主題

[88] 臺灣證券交易所「上市公司編製與申報企業社會責任報告書作業辦法」第 3 條、第 4 條第三款。

[89] 金管會證期局，前揭註 80，頁 31-32。

[90] 整理自：Global Reporting Initiative〔以下簡稱 GRI〕（著），吳文雅（等譯）（2017），《GRI 準則》，臺北市：社團法人中華民國企業永續發展協會。

[91] GRI 準則所稱「衝擊」係指組織在經濟、環境及（或）社會的影響，該詞可指為正面的、負面的、實際的、潛在的、直接的、間接的、短期、長期、蓄意、非蓄意的影響。同時亦包括組織對於永續發展之貢獻（正面或負面均屬之）。GRI（著），吳文雅（等譯）（2017），《GRI 準則詞彙表 2016》，頁 9，臺北市：社團法人中華民國企業永續發展協會。

doi:10.6342/NTU202000744

	相關永續發展之貢獻。
	• 經濟的主題（200 系列）：經濟績效、市場地位、間接經濟衝擊、採購實務、反貪腐、反競爭行為。
	• 環境的主題（300 系列）：物料、能源、水、生物多樣性、排放、廢汙水和廢棄物、環保法規遵循、供應商環境評估。
	• 社會的主題（400 系列）：可分為以下四個子題。 1. 勞動實務與尊嚴勞動：勞雇關係、勞／資關係、職業安全衛生、訓練與教育、員工多元化與平等機會、強迫或強制勞動、勞工實務問題申訴機制。 2. 人權政策：不歧視、結社自由與團體協商、童工、原住民權利、保全人員實務、人權評估。 3. 社會：當地社區、供應商社會評估、公共政策（例如政治捐獻）、社會衝擊問題申訴機制。 4. 產品責任：顧客健康與安全、客戶隱私、行銷與產品或服務之資訊與標示、社會與經濟法規遵循。

表（七）：GRI 準則架構

括言之，企業社會責任報告書係以財務報告作為基本內容，涵納其於環境、社會及經濟等非財務資訊之內容，並聚焦於短、中、長期創造價值之能力，據以協助投資人或各利害關係人瞭解其經營風險與機會，以及企業之經營治理策略是否及如何提升公司整體價值[92]。

第三款 小結——多樣化資訊揭露已蔚為趨勢

於 2018 年修正通過時，公司法始有明文規定「公司經營業務，應遵守法令及商業倫理規範，得採行增進公共利益之行為，以善盡其社會責任[93]。」該立法鑒於推動公司履行社會責任已為國際趨勢，故以此導入公司應善盡其社會責任之理念

[92] 陳耀宗（民 105），《審計學：國際審計與確信準則為架構（下）》，頁 442，新北市：滄海圖書資訊。

[93] 公司法第 1 條第二項。

doi:10.6342/NTU202000744

[94]，肯認採取企業社會責任理論或原則之共識[95]。同時，企業社會責任或前揭規定所稱商業倫理之立法規範，應如何內化至公司內部自律機制並成為內部倫理規範，除了內控制度之建置與推動外[96]，亦須配合相關資訊之揭露與評鑑制度，始能有效達成推動企業社會責任、落實公司治理之立法目的。換言之，無論係年報、營業報告書等財務報導，抑或公司治理、社會、環境保護乃至人權、反貪腐、反賄賂等非財務報導之編製與揭露，均係履行公司治理與企業社會責任之重要參考標準。由此可知，銀行所應揭露之報導或資訊之種類著實趨於多樣化且繁雜，故為合理確保銀行內控制度之運作得達成具可靠性、即時性、透明性及符合相關規範之報導目標，銀行內部除了應設計與執行妥適之內控制度以外，亦亟須思考者係——應如何建立得有效率地辨識、記錄、彙整、審閱、揭露、更新、歸檔及保存各項資訊之處理流程，以協助其確實履行報導相關義務。

再者，針對現行銀行內控制度規範要求銀行之報導應符合可靠性、及時性及透明性等標準，本文認為於前述銀行所應揭露之報導或資訊之種類與內容，逐漸呈現多樣化之趨勢下，對於各項報導之內容與品質之要求，其標準或有擴大發展並予以細膩化之空間。例如，參酌由國際審計與確信準則理事會（International Auditing and

---

[94] 公司法第 1 條第二項說明。

[95] 有論者認為已有相當研究成果得顯示，公司法學界普遍係採取企業社會責任理論之共識，其並藉由回顧立法沿革與法院實務案例指出，於本次（2018 年）公司法修正以前，法院實務即已與時俱進引入企業社會責任理論，據以解釋公司負責人責任之具體內涵。故公司法第 1 條第二項規定之增訂非謂創設一全新的公司法秩序，毋寧係確認一既有之法秩序並予以明文化。請參閱：楊岳平（2019），〈新公司法與企業社會責任的過去與未來——我國法下企業社會責任理論的立法架構與法院實務〉，《中正財經法學》，18 期，頁 46-48、82-83。除了公司法第 1 條第二項外，同法第 172 條之 1 第五項與第 282 條亦分別修正股東提案權與重整聲請權人之相關規定，同屬立法植入企業社會責任理念之規定。同前同註，頁 5。

[96] 有論者認為，公司法第 1 條第二項所謂「應遵守法令及商業倫理規範」或可解釋為「公司負責人應推動包括法令遵循機制、內部控制制度、風險管理等內部自律規範、企業內部倫理或行為準則（code of ethics or business conduct），以此落實國內外傳統意義下之法令、軟法（soft law）或商業倫理規範之遵循。」蔡昌憲（2018），〈從公司法第一條修正談公司治理之內外部機制——兼論企業社會責任的推動模式〉，《成大法學》，36 期，頁 135-136。再者，由於內控制度五項要素中（控制環境、風險評估、控制活動、資訊與溝通、監督作業），「控制環境」係公司設計與執行內部控制之基礎，其包含了道德操守與價值觀、管理哲學及經營風格等，屬塑造組織文化與員工意識之重要綜合因素。故有論者建議，董事會與審計委員會須確保公司內部已建立並落實整體一致之道德行為規範，並提供與員工溝通管理哲學與道德堅持等理念之管道，以防範經營者或高階主管因倫理崩壞而向下層員工施壓、或強迫達成過高之營利目標或品質標準，造成其鋌而走險。經濟日報（08/22/2008），〈杜絕造假案 健全吹哨機制〉，https://taipei-tfcc.scu.org.tw/notice/enterprise-honesty-morality-1070918-1.pdf。

doi:10.6342/NTU202000744

Assurance Standards Board，以下簡稱 IAASB）所訂定之「國際確信案件架構（International Framework for Assurance Engagements，IFAE）」，對於用以評估或衡量標的資訊（subject matter information）表達與揭露之適當「基準」（Criteria），其認為應具有以下特徵[97]：關聯性、完整性、可靠性、中立性及可瞭解性。

至於前揭 GRI 準則之報導原則中，則係分別對於報導之「內容」與「品質」提出具體標準原則，故相較於現行內控辦法僅就報導提出三點標準[98]，該準則係更加全面地注重報導本身之內容與品質。抑且，該準則之訂定係以「利害關係人」作為報導讀者之角度出發，具有避免掛一漏萬之效，俾使股東、投資人、債權人、消費者或主管機關等或有不同資訊需求者，均可自各項報導中檢視、擷取或比較不同資訊，繼而以此作成充分判斷與正確決策。關於 GRI 準則之各項報導原則及其內容概述，本文簡要彙整如下表（八）所示[99]：

GRI 準則之報導原則		
內容	利害關係人包容性	編製報導時，應考慮包括員工、股東、廠商、弱勢團體、當地社區及公民社群等組織相關之利害關係人之合理期待與利益，並須一併記錄與之溝通的過程與結果。
	永續性脈絡	分別於行業、區域性及全球觀點，揭露組織係如何達成經濟、環境或社會等方面之永續發展及其績效，及其與組織之長期策略、風險、機會及目標的關係。
	重大性	報導主題之採擇應綜合內外兩個面向。一、衝擊廣度：涉及組織整體、關鍵之任務與競爭策略，反映其經濟、環境或社會等顯著衝擊。二、利害關係人廣度：實質上影響利害關係人之評估與決策，或存在潛在重大性者。簡言之，此係決定報導主題及其揭露優先順序之標準。
	完整性	報導內容除應涵蓋報導期間內所有已發生事件之資訊外，亦應納入基於合理基礎所作成之未來衝擊之預測，足使利害關係人實質評估組織於報導期間內之績效。

[97] INT'L AUDITING & ASSURANCE STANDARDS BOARD [IAASB], INTERNATIONAL FRAMEWORK FOR ASSURANCE ENGAGEMENTS ¶ 36 (2010), https://www.ifac.org/system/files/downloads/b003-2010-iaasb-handbook-framework.pdf [hereinafter IFAE].

[98] 即可靠性、及時性及透明性。金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條第一項第二款、證券暨期貨市場各服務事業建立內部控制制度處理準則第 4 條第一項第二款。

[99] 整理自： GRI（著），吳文雅（等譯）（2017），前揭註 90。

doi:10.6342/NTU202000744

品質	準確性	定性描述之資訊應清晰、詳細且與其他報導或可取得之證據間有一致性；定量資訊則須揭露其量測方法與計算基礎或估計之基本假設，以供評估組織之績效。
	平衡性	報導內容應客觀且無偏見地反映組織整體情況，無論正面負面、有利不利之資訊均應揭露，避免刻意選擇或省略表達方式，俾使各利害關係人皆可作成合理評估。
	清晰性	報導呈現與表達之方式應讓各利害關係人易於取得、理解及應用所需之資訊。
	可比較性	報導應以一致之標準來篩選、衡量、整理及呈現資訊，確保利害關係人得將組織目前經濟、環境或社會相關績效或目標與過去相比較，或與其他組織為比較分析。
	可靠性	報導揭露之資訊與數據均應有內部控制或文件紀錄為來源依據，且基本決策流程應透過資訊系統記錄保存，並提供予外部保證／確信檢驗，以證明報導之真實性。
	時效性	報導提供之時點包括：一、定期：組織應依固定之時程與頻率，規律地發布報導、及時提供資訊，供利害關係人定期檢視。二、持續：組織亦須持續不斷發布最新資訊，致力追求報導所載與事件實際發生之時間點接近，給予利害關係人作成決策時所需之所有資訊。

表（八）：GRI 準則之報導原則

第三項 遵循目標

遵循（Compliance）目標係指以銀行法為首之相關法令規章之遵循[100]，此項可由銀行業之法規範體系加以觀察。基於特別法優於普通法原則[101]，銀行之組織登記

[100] 建立內部控制制度核心原則 1.3(3)；金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條第一項第三款。

[101] 中央法規標準法第 16 條規定：「法規對於其他法規所規定之同一事項而為特別之規定者，應優先適用之，其他法規修正後，仍應優先適用。」此即「特別法優於普通法」適用原則。而法律之所以有普通法與特別法之分，乃有二種以上之法律同時存在，對於同一事件，均有所規定，而其規定不相同者屬之。因此普通法與特別法僅為對立之稱謂，屬於相對性，而非絕對性，同一法律對某種法律原為特別法，而因變更其地位時，對某種法律則為普通法，例如公司法、票據法對民法而言，固為特別法，但對證券交易法而言則為普通法。其認定標準，如同一事件規定之性質為一般性者，為普通法，性質較為特殊者，為特別法；就同一事件規定之事項，較為粗疏簡陋者為普通法，規定較為詳細者，為特別法；就同一事件之規定，範圍廣泛而性質較單純為普通法，規定較狹小而複雜

doi:10.6342/NTU202000744

與業務經營[102]等規範法源係以「銀行法」為主，其立法重點在於保護存款人權益、強化銀行業之財務安全性，以及維護金融秩序等[103]。同時，銀行既屬股份有限公司之法人組織型態[104]，其組織、登記、成立及營利行為，亦須受「公司法」之規範[105]。抑且，倘若銀行成為金融控股公司之銀行子公司，則其於從事授信、或關係人交易相關行為時，除銀行法之規範外，尚須適用「金融控股公司法」之規定[106]。另外，由於銀行之股票均應公開發行[107]，且為維護證券市場[108]與保障其參與者之正當權益，以及發展經濟與維持社會安定等公共利益考量[109]，故屬公開發行公司之銀行同須遵守「證券交易法」之規範。其他對於銀行業之金融法規範尚有「存款保險條例」、「國際金融業務條例」、「洗錢防制法」、「資恐防制法」、「管理外匯條例」、「個人資料保護法」、「金融消費者保護法」等，族繁不及備載。

再者，為維護金融市場穩定、促進經營效率、公平分配資源及保障存款人，立法者與主管機關除了依其職權制定各項金融業法、法規命令或行政規則，以規範銀行業等金融機構之人事、財務及業務，以及建立有效之監控機制外[110]，尚須仰賴銀

詳細者為特別法。104 年 10 月 14 日法務部法律字第 10403512790 號函、102 年 3 月 19 日法務部法律字第 10200042350 號函。

102 銀行法第 2 條。

103 林仁光（2016），〈銀行法總則〉，王文宇（等著），《金融法》，九版，頁 29，臺北市：元照。

104 銀行法第 52 條第一項。

105 公司法第 1 條第一項。相關規定包括公司法第一章總則、第五章股份有限公司，以及第六章之一關係企業。

106 金融控股公司法第 44 條、第 45 條。

107 銀行法第 52 條第二項。

108 若將金融市場（Financial markets）依其業務活動區分，則包括「資本市場」（Capital markets）與「貨幣市場」（Money Market）。前者一般指證券市場（Stock market），其主要功能為擔任儲蓄單位（surplus units）與投資人雙方溝通之管道，或謂提供企業經營者有效率之籌資場所，故理論上，資本市場之發展實與國家經濟發展間具有緊密關聯性。今日倘論及資本市場之管理，其範圍則包括投資人（投資公司、投資銀行）、發行人（發行公司）、證券商、投信與投顧公司、證交所、集中保管結算所、櫃買中心、證金公司、證券金融事業及金融消費評議中心等眾多參與者與服務提供者，此觀諸證券交易法之規範亦復如是。曾宛如，前揭註 54，頁 1。

109 余雪明（2016），《證券交易法：比較證券法》，五版，頁 3-5，臺北市：自刊；賴英照（2017），《股市遊戲規則：最新證券交易法解析》，三版，頁 1-2，臺北市：自刊。

110 王志誠（2017），《現代金融法》，三版，頁 48，臺北市：新學林。茲以銀行業相關之金融法規範為例，有學者將其區分為金融行政法、金融組織法、金融活動法及金融再造法等四大類別：一、金融行政法：涉及主管機關之人事組織與行政權限，包括金管會組織法、金融監督管理委員會銀行局組織法、中央銀行法等。二、金融組織法：規範銀行之組織型態、人事、業務及財務等事項，該內容多以政策性與技術性之強制規定呈現，故其亦有金融活動法之性質，銀行法即屬此類法規。三、金融活動法：與金融組織法相似，均係以組織、人事、業務及財務為規範內容，惟其內容固然多屬

doi:10.6342/NTU202000744

行業周邊單位所訂定、種類繁多之自律規範，作為銀行從事金融業務活動時之行為準則。例如銀行同業公會[111]所制定之業務規章、自律公約及作業基準等管理規範，抑或董事會、經理人或其他管理階層所訂定之章程、內部行為準則等相關規章，皆屬於銀行業應遵循之法令範圍。

職是之故，銀行本身所應遵循之法規命令實則多如牛毛，或謂現行金融法規主要係採取「規則基礎之規範模式」（rules-based regulation），分別對於各種金融機構制定剛性之金融業法，形成較為嚴實之規範密度[112]。惟晚近逐漸納入「機構基礎之規範模式」（institution-based regulation）[113]，即於前述金融業法之授權下，由金管會針對各種金融機構分別訂定法規命令，要求銀行、金控公司及保險業等，均應依其實際狀況，自行量身剪裁設計其內控制度[114]。基此，內控制度即為落實各項法令規範、自律規章之遵循目標所設計與運作者。

第四項 內控目標之本文觀察

金融機構建立內控制度之基本目的固係在於促進其健全之經營，以合理確保達成營運、報導及遵循等三大內部控制目標，惟若論及內控制度目標之核心，或謂有效達成前述各該目標之基礎，本文認為應屬「遵循」目標。基此，本文以下謹就營運目標、報導目標兩者與遵循目標間之關係，茲以銀行為例分別說明之。

強制或禁止規定，亦不乏諸多任意規定，包括信託法、國際金融業務條例、洗錢防制法、管理外匯條例等。四、金融再造法：係為金融機構異業整合、業務內容或組織調整，抑或問題銀行之退場機制等提供規範基礎，包括金融機構合併法、金融控股公司法、企業併購法及行政院金融重建基金設置及管理條例。同前同註，頁 48-49。

111 全名為「中華民國銀行商業同業公會全國聯合會」（The Bankers Association of the Republic of China，簡稱中華民國銀行公會），該組織係以台北市銀行商業公會為基礎，聯合台灣省銀行商業同業公會聯合會與高雄市銀行商業同業公會於 1983 年所成立者，截至 2018 年底止，共有 10 個會員公會。其設立宗旨為：協助政府推行金融政策、促進經濟發展、協調同業關係及增進同業之共同利益；主要任務包括：財經金融政策與商業法令之推行、配合經濟發展研商各業資金之供需調劑、同業各項業務規章之釐訂與編纂、會員單位服務道德自律規章之推行、國際性金融組織會議之參與、接受政府或團體委託辦理與研究建議事項等。中華民國銀行商業同業公會全國聯合會網站，https://www.ba.org.tw/Publicinformation/Index（最後瀏覽日：10/07/2019）。

112 王志誠，前揭註 110，頁 49-50。

113 *See* John H. Walsh, *Institution-Based Financial Regulation: A Third Paradigm*, 49(2) HARV. INT'L L.J. 381, 381-83 (2008).

114 金融控股公司及銀行業內部控制及稽核制度實施辦法、保險業內部控制及稽核制度實施辦法等，即屬示例。

doi:10.6342/NTU202000744

第一款 營運目標與遵循

縱曰銀行得經營之業務種類繁多[115]，惟個別銀行實際經營之業務項目，仍須由中央主管機關於銀行法所定之範圍內分別核定，並載明於營業執照[116]。此外，銀行於執行業務過程中，亦須符合立法者、金融主管機關抑或銀行同業公會等，透過金融法規所制定之各式標準規範與行為準則。由於諸如利害關係人授信或其他交易、投資業務、併購交易等交易型態，其交易金額通常龐大或事涉利益衝突，除前述金融法規所建立之規範架構以外，立法者與主管機關亦針對金融重大交易設有較為嚴格且綿密之程序與實體規範[117]。同時伴隨金融商品或服務不斷創新、多元且趨於高風險、複雜化，為能保障金融消費者權益，銀行須確實履行法定之認識客戶程序[118]、適合度原則[119]，以及說明與揭露等告知義務[120]。抑且，為達成銀行專業經營之目標，故相較公司法對於一般股份有限公司董事與經理人之任職條件，僅要求其須為完全行為能力人且不得有特定消極資格[121]，銀行法對於銀行負責人之積極資格

[115] 銀行法第 3 條。

[116] 銀行法第 4 條。

[117] 王志誠（2007），〈金融重大交易之法律風險及控制〉，《全國律師》，11 卷 2 期，頁 5。銀行法關於利害關係人授信係分為無擔保授信與擔保授信，前者之適用範圍與豁免對象規定於該法第 32 條；後者之意義與授信條件則見於第 12 條與第 33 條之規定。

[118] 金融消費者保護法第 9 條第一項。

[119] 金融服務業確保金融商品或服務適合金融消費者辦法第 6 條。

[120] 金融消費者保護法第 10 條第一項。

[121] 公司法第 30 條；第 192 條第一、五項。

doi:10.6342/NTU202000744

[122]與消極資格[123]、兼職限制[124]、義務及法律責任等，均有更為嚴格之要求。再就法律責任而言，倘若法人、銀行或銀行之負責人或職員，或有違反非銀行禁止收受存款等專業經營、違背其職務、詐欺、收受不當利益、不當關係人交易或違反主管機關接管或勒令停業之處置等行為；又或有違反兼職限制、資本虧損怠於申報、未依限提出或未確實執行資本重建或其他財務業務改善計畫，抑或未建立或未確實執行內部控制與稽核制度或內部作業制度等情形，即須分別依銀行法之規定，擔負起有期徒刑、拘役、罰金或沒收等刑事責任[125]，以及罰鍰等行政責任[126]。

由是觀之，無論係銀行之設立登記、業務經營、財務標準或人事規範等各式營運相關事項，均有立法者與金融主管機關，共同藉由金融法規、命令、辦法等各項密度與寬嚴有別之立法層級，構築出銀行於營運過程中必須確實遵循之行為準則，以及違反各該規定所應承擔之明確之法律責任。職此，倘若由銀行之董事或高階管理階層所設計並由所有人員共同遵行之內控制度，其未能合理確保銀行於日常業

---

[122] 銀行法第 35 條之 2。依據銀行法第 18 條，銀行法所稱銀行負責人，謂依公司法或其他法律或組織章程所定應負責之人，原則上包括銀行之董事、監察人、總經理、副總經理、協理、總行經理、分行經理或與其職責相當之人。銀行負責人之積極資格基本上均應具備良好品德、領導及有效經營銀行之能力（銀行負責人應具備資格條件兼職限制及應遵行事項準則第 4 至 6 條、第 9 條第一項，以下簡稱〔銀行負責人資格條件準則〕）。復以銀行之董事為例，其積極資格尚包括應具備下列條件之一：一、銀行工作經驗五年以上，並曾擔任銀行總行副經理以上或同等職務，成績優良者。二、擔任金融行政或管理工作經驗五年以上，並曾任薦任八職等以上或同等職務，成績優良者。三、銀行工作經驗三年以上，並曾擔任銀行總行經理以上或同職務，成績優良者。四、有其他事實足資證明其具備銀行專業知識或經營銀行之能力，可健全有效經營銀行業務者（銀行負責人資格條件準則第 9 條第一項）。此外，包括銀行董事長、董事及監察人之選任，均應於選任後十日內，檢具有關資格文件，報經主管機關認可；若有資格條件未經主管機關認可者，銀行即須於期限內，依主管機關之命令調整之（銀行負責人資格條件準則第 9 條第五項後段）。

[123] 至於消極資格之部分亦相較於公司法第 30 條有更為嚴格之限制，例如不得有「因違反銀行法或其他金融管理法，受刑之宣告確定」（銀行負責人資格條件準則第 3 條第六款，後同）、「重大喪失債信情事尚未了結（債信條款）」（第十款）或「事實證明從事或涉及其他不誠信或不正當之活動（誠信條款）」（第十三款）等情事。

[124] 基於銀行專職經營之要求與競業禁止之觀點，銀行負責人之兼職行為受有較為嚴格之限制。原則上，銀行之負責人與職員不得兼任其他銀行任何職務。但因投資關係，並經中央主管機關核准者，得兼任被投資銀行之董事或監察人（銀行法第 35 條之 1）。除了其他銀行以外，銀行負責人兼職限制之對象基本上包括所有金融機構在內，例如金融控股公司、信託公司、信用合作社、證券公司、保險業等（銀行負責人資格條件準則第 3 條之 1 第三項）。

[125] 銀行法刑事責任之規定或有第 125 條第一項、第 125 條之 2 第一項、第 125 條之 3、第 127 條第一項、第 127 條之 1、第 127 條之 2 及第 136 條之 1。

[126] 銀行法行政責任之規定或有第 127 條之 3 第一項、第 128 條第一項、第 129 條第七款及第 129 條之 2。

doi:10.6342/NTU202000744

務執行時，充分認知並確實遵循前述各項法令規章，則難謂銀行得合理達成營運之效果與效率。

第二款 報導與遵循——兼論確信案件

誠如本文於前就內部控制報導目標所述，銀行應編製或揭露之報導或資訊之種類皆趨於多樣化且繁雜。然而，無論屬財務報導之財務報告、會計揭露項目，抑或企業社會責任報告書、內控制度聲明書等非財務報導，均須依循法規命令或公認準則等法定規範予以編製或揭露。質言之，內控制度之運作係合理確保銀行之財務報告係依照金管會訂定之準則或有關法令、國際財務報導準則、國際會計準則、解釋或解釋公告等一般公認會計原則編製[127]，且該報導之編製程序係適用會計專業判斷程序、會計政策與估計變動等流程[128]。此外，由於銀行亦有證券交易法規定之適用，為貫徹公開發行公司之繼續公開義務[129]，包括年度財務報告、季財務報告或財務報表，均應經會計師查核簽證或核閱後[130]，公告並向主管機關申報之[131]。倘違反前述申報義務，抑或公告之財務文件有虛偽或隱匿之情事，則須負起行政罰鍰、民事損害賠償，以及刑事有期徒刑或罰金等責任[132]。

再者，基於國際趨勢與金融主管機關對於企業社會責任、永續發展與經營等議題之重視，投資人或銀行之利害關係人對於銀行揭露之報導或資訊，其所關注之重點亦不再僅限於財務表現。為使銀行所有利害關係人均能取得詳實且必要之資訊，銀行內部就非財務報導之編製、揭露及確信（認證），同須遵循法定之標準或準則等規範。準此，除前述編製企業社會責任報告時應遵循之 GRI 準則以外，為提升各項報告或報導之預期使用者對於銀行揭露之非財務績效或狀況、系統與流程，以及行為等非屬財務性標的資訊之信賴水準，報導內之資訊仍須由負責編製方出具聲明，或由第三方執業人員取得足夠且適切之證據後，作成標的資訊符合既定準則

127 公開發行銀行財務報告編製準則第 3 條。

128 金融控股公司及銀行業內部控制及稽核制度實施辦法第 8 條第一項第二款第五目。

129 曾宛如，前揭註 54，頁 177-179；賴英照，前揭註 109，頁 209-210。

130 證券交易法第 37 條第一、二項；會計師查核簽證金融業財務報表規則第 2 條。

131 證券交易法第 36 條第一項。

132 證券交易法第 20 條第二項、第 20 條之 1 第一項、第 171 條第一項、第 174 條第一項第五、六款、第 178 第一項第二款及第 178 條第二項。

doi:10.6342/NTU202000744

之書面結論，是謂「確信案件」（Assurance Engagements）[133]。

IAASB 於「國際確信案件架構」（IFAE）中明確指出，確信案件應包括五項要素[134]：第一，由執業人員（又稱確信方）、負責方（主要為企業）及預期使用者組成之「三方關係」（A Three Party Relationship）[135]。第二，適當標的。第三，基於合適之基準。第四，足夠且適切之證據。第五，書面確信報告。所謂適當之「標的」（Subject Matter）係指依基準衡量或評估之項目[136]，或有財務與非財務之績效或狀況、實體運作表現（例如設備產能）、系統與流程（System and Process，例如內部控制與資訊系統）及行為（Behavior，例如公司治理、法令遵循或人力資源實務）等[137]。其次，標的資訊（Subject Matter Information）或聲明（Assertion）指對上述標的依基準予以衡量或評估之結果[138]，亦屬執業人員作成確信結論與書面報告之基礎[139]。出具該結論或確信報告之目的則在於提升預期使用者對標的資訊之信賴

---

[133] *See* IFAE, *supra* note 97, ¶ 7. 此外，為因應臺灣證券交易所與櫃買中心要求金融保險業在內之上市上櫃公司所編製之企業社會責任報告書應取得第三方確認、確信或保證之規定，金管會爰請財團法人中華民國會計研究發展基金會〔以下簡稱會基會〕訂定確信準則。會基會即參考國際審計與確信準則理事會（International Auditing and Assurance Standards Board，IAASB）所訂定，與非屬歷史性財務資訊查核與核閱確信案件相關之「國際確信案件準則（International Standards on Assurance Engagements，ISAEs）第 3000 號（ISAE 3000）訂定確信準則公報第一號「非屬歷史性財務資訊查核或核閱之確信案件」〔以下簡稱確信準則第一號〕，規範會計師等執業人員於執行確信案件時，應如何取得足夠且適切之證據，據以衡量與評估所確信之資訊（標的）是否存有重大不實表達之風險或情事，並於執行必要程序以降低案件風險後，依據衡量與評估標的之結果（標的資訊），作成取得合理確信或有限確信之結論並出具書面報告。確信準則第一號第 8 條。

[134] IFAE, *supra* note 97, ¶ 20:

> The following elements of an assurance engagement are discussed in this section:
> (a) A three party relationship involving a practitioner, a responsible party, and intended users;
> (b) An appropriate subject matter;
> (c) Suitable criteria;
> (d) Sufficient appropriate evidence; and
> (e) A written assurance report in the form appropriate to a reasonable assurance engagement or a limited assurance engagement.

[135] 確信準則第一號附錄一。

[136] 確信準則第一號第 10 條。「基準」（Criteria）係指用以衡量或評估標的之標準，「適用基準」則指用於特定案件之基準。IFAE, *supra* note 97.

[137] IFAE, *supra* note 97, ¶ 31.

[138] *Id.* ¶ 8; 確信準則第一號第 10 條。

[139] 依據執業人員之確信程度（Level of Assurance），確信案件可分為「合理確信案件（Reasonable Assurance Engagement）」與「有限確信案件（Limited Assurance Engagement）」兩種。前者係執業人員執行必要程序將確信案件風險降低至當時情況下可接受之水準，並作成積極式結論之確信案件；後者亦係執業人員執行必要程序將案件風險降低至當時情況下可接受之水準，惟其可接受之案件

doi:10.6342/NTU202000744

水準，俾便其依據標的資訊作成決策。

具體以內控制度有效性之確信為例，執業人員係依 COSO 架構或銀行內部控制制度實施辦法所述內部控制之五項要素作為適當基準，衡量與評估屬「系統或流程」項目之標的，倘若其認為銀行（責任方）內部內控制度之設計與運作係遵循相關規範且有效運作，即可取得合理確信之結果（即標的資訊），據以作成內部控制有效性聲明之書面報告。復以企業社會責任報告書為例，由於法令強制該報告書之編製須取得第三方驗證，故其屬特定確信案件[140]。執業人員須以法定之 GRI 準則作為適用基準，衡量與評估銀行（責任方）所編製之報告書是否依據該準則編製與揭露，作成合理（或有限）確信之書面報告，據以提供銀行於永續發展績效與利害關係人參與之指引。

綜言之，由銀行所編製與揭露，無論係財務報導或非財務報導，均屬銀行與投資人、利害關係人、金融主管機關乃至社會大眾溝通、說明其業務運作、公司治理、誠信經營、環境保護及社會關懷等永續發展策略之重要管道與工具，俾使前述所有報導與資訊之使用者皆得以之作成正確判斷或決策。基此，銀行內部所有職司報導撰著之人員是否充分瞭解與熟悉相關法令規範與公認準則，並確實依循而為編纂、覆核、揭露及認證，足致確保報導之正確與可靠、達成內部控制之報導目標，實為與遵循具有密切之關聯性。

第三款 小結——內部控制之核心目標係遵循

吾等若觀察現行制度架構或將以為，內控制度應係銀行業財務會計作業程序之延伸，於此亦使主管機關認為內控制度之查核應由會計師為之[141]，惟本文認為無

風險水準係高於合理確信案件，故其作成者為消極式之結論。換言之，相較於合理確信案件，執業人員對於有限確信案件所執行程序之性質、時間及範圍較為有限，但仍須取得依其專業判斷，具有意義之確信程度。至於所謂「具有意義之確信程度」，則指預期使用者之信賴水準得提升至明顯高於微不足道之程度。IFAE, *supra* note 97, ¶¶ 11, 48, 53; 確信準則第一號第 10 條。

[140] 臺灣證券交易所「上市公司編製與申報企業社會責任報告書作業辦法」第 3 條第二項。

[141] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 28 條一項。該條項規定，會計師除了辦理銀行業年度財務報表之查核簽證以外，其應受銀行業之委託辦理內控制度之查核，並對銀行業申報予金管會之報表資料及其正確性、內控制度及法令遵循制度執行情形、備抵呆帳提列政策之妥適性等表示意見。同條第二項規定，金管會亦得請銀行業委託會計師依其規定辦理個人資料保護、洗錢防制與資恐打擊機制之專案查核。**惟基於前揭內部控制報導目標所述，銀行業報導之內容亦逐漸涵蓋、列入非財務報導與資訊，且諸多內容係關於法令規範之遵循，故無論係銀行之內部稽核、外**

doi:10.6342/NTU202000744

論就銀行日常各項業務活動，抑或報導與資訊之編製與定期揭露等方面言之，欲達成內部控制營運與報導等目標，銀行首應履行之任務著實為遵循（或謂法令遵循）。基本上，作為金融主管機關高度監管之特許行業，銀行運作之過程中，其任何行為均受相應之「法定行為規範」約束，上至例如銀行法、公司法、證券交易法、洗錢防制法、管理外匯條例等法律，下至內控制度實施辦法、報導編製準則、金管會或行政機關之法令函釋（行政命令）、銀行同業公會之自律規範等。

再者，於 2019 年修正之銀行法之修法說明亦指出，為敦促銀行確實建立與積極落實內控制度與內部作業程序規範，以及有效執行內部稽核程序，強化銀行之法令遵循，故立法者對於金融主管機關針對違反內控規定之銀行，得處以行政罰鍰之金額上限，即由一千萬元調高至五千萬元，藉此達到嚇阻違法之效果[142]。對於採取擴大金融主管機關權限、大幅提升罰鍰金額以要求銀行落實法令遵循之有效性，本文認為該法之實際效用仍有待後續追蹤關注。縱使此舉果真能夠獲致嚇阻違法之效果，惟重點仍在於銀行內部自發性地發展與落實合適之內控制度，確保其營運或各項業務行為均符合法令遵循之規範要求，抑且時刻關注風險管理機制之執行，方能根本性地改善銀行未決之不良現況。

職此，銀行面對龐雜、細緻且縝密之法令規範，應如何將其於組織內部為有效率地傳達與溝通，確保其日常各項業務活動順利且有效執行，即有賴內控制度之設計與運作，於銀行內外部落實有效之法令遵循機制或法令遵循計畫、提升各組成員之遵法意識。意即，藉由積極追求內部控制之遵循核心目標，以收達成營運與報導等其他目標之效。

第四節　風險管理與內部控制

誠如本文第二章提出就內控制度發展之觀察，內控制度已有朝向以「風險管理」為基礎之發展趨勢，意即銀行內部應建立與執行風險管理機制，避免業務執行單位過度追求風險，同時協助管理階層精確掌握銀行整體之風險狀況。惟若欲更細緻地討論風險管理於內控制度之體現，本文認為可從金融機構公司治理之特色、風

部查核或確信案件等執行人員之資格條件，或不應僅侷限於會計背景者。陳耀宗，前揭註 92，頁 416。

142 銀行法第 129 條修正說明（中華民國 108 年 4 月 17 日總統華總一經字第 10800037891 號令修正公布）。

doi:10.6342/NTU202000744

險管理專責機制及內控制度之實際運作等三種角度分別切入。

第一項 金融機構公司治理之特色

學理上，傳統公司治理議題咸有所謂股東優位理論（shareholder primacy theory）與利害關係人理論（stakeholder theory）之論辯，其爭議係圍繞於公司經營者與代表公司利益主要依歸之「股東治理」[143]。然而，諸如銀行、金控公司及保險業等金融機構，由於其組成份子對於風險承擔之偏好與重視程度，或與一般法人組織不同。故相對於一般企業之公司治理，金融機構則較強調包括存款人、投資者及保戶等債權人利益保護之「債權人治理」。至於強調債權人利益下所體現金融機構公司治理之特殊性，本文將從金融機構特殊之財務結構與主管機關高度金融監理等兩點分別觀察。

第一款 特殊資產負債結構

茲以銀行為例，普遍而言，一般公司企業之資產結構係以股東權益（equity）為大宗，惟金融機構之股東權益占其資產比例相對甚低許多[144]，高達 90%之資金來源係債權人之債權（liability）[145]。換言之，銀行之資產主要係由債權人所持有，且多數債權人，或謂主要資金提供者為持有短期債權之大量存款人（depositors）[146]。再者，觀諸銀行法規範銀行之專屬業務，包括收受存款、受託經理信託資金或

[143] 股東優位理論論者認為，公司股東基於賸餘財產請求權人之地位較能代表公司整體利益，故公司經營者應以極大化整體股東利益為依歸。*See, e.g.*, RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 576-80 (9th ed. 2014); FRANK H. EASTERBROOK & DANIEL R. FISCHEL, THE ECONOMIC STRUCTURE OF CORPORATE LAW 35-39 (1996). 利害關係人理論論者則認為，公司經營者應平衡兼顧股東與員工、債權人、客戶、該公司業務所在地區等其他非股東之利害關係人之利益。*See generally* Einer Elhauge, *Sacrificing Corporate Profits in the Public Interests*, 80(3) N.Y.U. L. REV. 733 (2005); Margaret M. Blair & Lynn A. Stout, *A Team Protection Theory of Corporate Law*, 85(2) VA. L. REV. 247 (1999).

[144] 楊岳平（2019），〈論金融控股公司治理的改革方向：以獨立董事與提名委員會為中心〉，《臺大法學論叢》，48 卷 2 期，頁 690-691。

[145] Jonathan R. Macey & Maureen O'Hara, *The Corporate Governance of Banks*, 9(1) FED. RES. BANK N.Y. ECON. POL'Y REV. 91, 97 (2003).

[146] *Id.* at 93.

doi:10.6342/NTU202000744

公眾財產[147]，以及辦理國內外匯兌[148]等項目，其中所謂收受存款係指銀行向不特定多數人收受款項或吸收資金，並約定返還本金或給付相當或高於本金之行為[149]，或謂收受存款為商業銀行與專業銀行最重要之專屬業務[150]。職是故，銀行既係以吸收與運用大眾資金為核心業務，除了前述相較於非金融機構，金融機構之資產結構主要為債權人之債權，而非由股東權益所支持以外[151]，此特殊資產負債結構亦相當程度地提升債權人利益於銀行內部與金融機構公司治理之重要性[152]。

詳言之，自銀行、金控公司、證券商或保險公司等金融機構內部之資產負債結構以觀，較諸其他非金融機構主要係以股東為組成員或投資者，金融機構最大特色在於眾多利害關係人存乎其中。所謂「利害關係人」除了數量眾多之債權人外，尚包括存款保險公司、金融監理機關，甚或納稅人乃至金融體系。因此，非如一般公司治理制度多觸及股東治理之議題，前述之差異造成金融機構公司治理討論重點傾向聚焦於債權人治理，究其主要原因在於股東與債權人間對於「風險」之偏好與重視程度各異[153]，本文於下述之。

理論上，股東應積極監督公司董事之業務經營，避免董事過度追求風險，確保

---

147 所謂「信託資金」，係指銀行以受託人地位，收受信託款項，依照信託契約約定之條件，為信託人指定之受益人之利益而經營之資金（銀行法第 10 條）；信託投資公司則謂以受託人之地位，按照特定目的，收受、經理及運用信託資金與經營信託財產，或以投資中間人之地位，從事與資本市場有關特定目的投資之金融機構（銀行法第 100 條第一項）。基此，受託經理信託資金、公眾財產應屬信託投資公司之專屬業務，其性質有別於收受存款業務。

148 國內外匯兌業務同屬商業銀行與專業銀行之專屬業務。所謂「匯兌業務」，係指行為人不經由現金之輸送，而藉與在他地之分支機構或特定人間之資金清算，經常為其客戶辦理異地間款項之收付，以清理客戶與第三任間債權債務關係或完成資金移轉之行為（最高法院 108 年度台上字第 24 號刑事判決、最高法院 106 年度台上字第 783 號刑事判決）。「國內外匯兌」則係謂銀行利用與國內異地或國際間同業相互劃撥款項之方式，如電匯、信匯、票匯等，以便利顧客國內異地或國際間交付款項之行為，代替現金輸送，了結國際間財政上、金融上及商務上所發生之債權債務，收取匯費，並可得無息資金運用之一種銀行業務而言（臺灣高等法院 107 年度金上重訴字第 1 號判決）。是凡從事異地間寄款、領款之行為，無論是否賺有匯差，亦不論於國內或國外為此行為，均符合銀行法該條項「匯兌業務」之規定（最高法院 95 年度台上字第 5910 號判決）。

149 銀行法第 5 條之 1

150 王志誠，前揭註 7，頁 58-59。

151 Jonathan Macey & Maureen O'Hara, *Bank Corporate Governance: A Proposal for the Post-Crisis World*, 22(1) FED. RES. BANK N.Y. ECON. POL'Y REV. 85, 87 (2016).

152 *See* Macay & O'Hara, *supra* note 145, at 102-03; Klaus J. Hopt, *Corporate Governance of Banks After the Financial Crisis*, *in* FINANCIAL REGULATION AND SUPERVISION: A POST-CRISIS ANALYSIS 337, 342 (Eddy Wymeersch et al. eds., 2012).

153 楊岳平，前揭註 144，頁 691-692。

doi:10.6342/NTU202000744

其投資得獲取穩定收益，惟實際上股東一方面受到有限責任之保護，抑且立於公司賸餘財產價值最終分配請求權人之地位。因此，股東通常較無誘因持續關注或積極監督董事或經理人之行為，甚或期待經營階層從事短期、高風險行為以獲取較多之盈餘分派，倘公司因犯險投資失敗時，其至多僅須承擔出資額內之損失，不若債權人或恐須承擔公司長期或全額之損害，故於「成功有賺、失敗不賠」之投資模式下，股東之角色係屬風險追求者。相較於股東，債權人所關心者並非投資獲利所生之盈餘分派，蓋其所持有之債權之收益係屬固定收益，將不因董事或經理人成功之投資或風險追求行為而產生額外獲利。實則，諸等所在意者應為其債權是否可長期且穩定地獲得清償，倘若風險性投資失敗且損失超逾股東出資額時，債權人之債權本金即將因此蒙受損失，故於此「成功無關、失敗穩賠」之收益模式下，債權人之角色自然傾向避免風險性投資之風險怯避者。

綜上所述，有鑒於債權人與股東兩者對於風險之偏好與重視程度存在相當之差異性，且本質傾向風險怯避的債權人作為金融機構內部最主要之組成份子與資金提供者，故相對於股東利益，金融機構須特別關注者實為債權人之利益。

第二款 主管機關高度監管

有論者將銀行與電力、鐵路等公司類比，認為其等雖主要係以營利為目的之私部門組織，然其健全經營與運作卻係以公共利益為依歸，故謂銀行實為一珍奇異獸[154]。質言之，銀行落實公司治理除了係為平衡兼顧眾多債權人與股東等利害關係人之利益外，由於金融機構之經營與運作尚涉及服務實體經濟、金融體系之穩定與整體經濟發展等外部效應，故金融業同時受制於金融主管機關之高度監督與管理。至於實施金融監理之目的，或有以下考量[155]：一，維持金融體系穩定，避免金融危機之發生。二，保護金融消費者、存款人或投資人之權益。三，追求金融機構經營之效率，達成資源之公平分配。惟為期能更深刻地體會監理目的與風險間之連結，本文以下將自風險管理之角度，探究主管機關對於金融機構予以高度監管之原因。

---

[154] HAMID MEHRAN & LINDSAY MOLLINEAUX, FEDERAL RESERVE BANK OF NEW YORK STAFF REPORTS: CORPORATE GOVERNANCE OF FINANCIAL INSTITUTIONS 7 (2012). (“Bank are strange beasts.”)

[155] 王志誠，前揭註 49，頁 4。

doi:10.6342/NTU202000744

第一目　風險監理原則

銀行等金融機構作為金融中介者（market-based credit intermediation）之角色，或謂其居於整體經濟體系之樞紐地位，其傳統經濟機能在於吸收存款後，再將所吸收之閒散資金以放款方式貸予資金需求者；或藉由其徵信、授信及資訊蒐集等專業能力，妥適配置市場上資金，解決資金供給者與需求者間資訊不對稱之問題；抑或辦理貨幣結算、收付、兌換及存款轉移等支付業務[156]。此外，銀行之現代機能尚包括提供理財諮詢、財富管理、代收代付等金融服務，抑或其透過授信政策與規模、存放利率及資金投向之操作，得於一定程度內，實現調節經濟與產業結構等功能[157]。由於銀行掌握社會大眾之龐大資金，同時身負服務實體經濟之功能，倘若其經營不善以致金融體系運作凍結，將導致存款人擠兌之流動性風險，或將引發潛在之系統性風險，最終造成整體經濟活動嚴峻且長期之損害[158]。

基此，為使銀行等金融機構得穩定且健全地經營、充分發揮本身應有之經濟機能，現代金融監理機關或國際組織均係以「風險」作為其執行監理或訂定金融相關法制規範之基礎（risk-based supervision）。至於所謂「以風險為基礎之監理」又可分為質性監理（qualitative supervision）與量性監理（quantitative supervision）兩項[159]：前者主要係審視金融機構本身控制風險之品質，再由主管機關加以規劃與評估其所採行之監理措施內容。後者則包含要求金融機構應符合其業別之資本適足率

156 王志誠，前揭註 7，頁 3。

157 同前註，頁 4。

158 *See* Macay & O'Hara, *supra* note 151, at 87; MEHRAN & MOLLINEAUX, *supra* note 154, at 9.

159 阮品嘉（2012），《金融控股公司及其集團之規範與實務》，頁 117，臺北市：元照。

doi:10.6342/NTU202000744

或最低資本要求等標準[160]，抑或透過財務結構比例[161]、特定交易或投資金額之總量管制[162]等法令規範，據以限制金融機構之曝險程度，同時促使金融機構加強其本身之風險評估與風險控管能力。

第二目　立即糾正措施

前述各項監理措施中，金融監理機關以金融機構之資本適足率作為區分風險資本等級之基準，進行分級式風險監理之「立即糾正措施」（Prompt Corrective Action，PCA）制度，尤屬「以風險為基礎之監理措施」之重要體現。巴塞爾委員會於「有效銀行監理核心原則」中指出，銀行監理之首要目標係促進銀行經營與銀行系統之安全與穩健（safety and soundness）[163]，避免銀行於業務執行過程中，不當損及存款人之利益或風險之發生[164]。倘若金融監理機關依其職權判斷後認為，有銀行未能確實遵循法令規範、或業務之執行將有害銀行或銀行系統之安全與穩健時，該機關即有權力（或要求該銀行）採取及時糾正措施[165]。所謂立即糾正措施係

---

[160] 觀諸金融相關法令規範，金融主管機關（即金管會）主要係以金融機構之資本等級為其監理標準，故對於不同業別之金融機構設有資本適足率（自有資本與風險性資產之比率）之最低要求，包括：金控公司（金融控股公司法第 40 條第一項；金融控股公司合併資本適足性管理辦法第 6 條第一、二項）、銀行（銀行法第 44 條；銀行資本適足性及資本等級管理辦法第 5 條、第 6 條）、票券商（票券金融管理法第 41 條；票券金融公司資本適足性管理辦法第 13 條第一項）、保險業（保險法第 143 條之 4；保險業資本適足性管理辦法第 4 條、第 5 條）及證券商（證券商管理規則第 59 條；第 59 條之 1）等。再者，若金融機構之資本適足率或資本等級未達法定標準時，金管會得採取「立即糾正措施」（Prompt Corrective Action，PCA）或為其他必要之監理措施。例如：金管會於審核銀行之資本等級後，其認為該銀行有資本不足、資本顯著不足或資本嚴重不足等情形者，即得採取不得以現金分配盈餘或買回其股份、解除銀行負責人職務，抑或派員接管等措施（銀行法第 44 條之 1、第 44 條之 2；銀行資本適足性及資本等級管理辦法第 15 條第二項）。王志誠（2014），《銀行法》，頁 257-259，臺北市：新學林。

[161] 觀諸金融相關法令規範，金管會於必要時，得單獨依職權或經洽商中央銀行後，得對於金融機構之財務結構設定財務比例之上限或下限者，包括：金控公司（金融控股公司法第 41 條第一、二項）、銀行（銀行法第 36 條第二項；中央銀行法第 25 條）、票券商（票券金融管理法第 33 條第一、二項）、證券商（證券商管理規則第 13 條第一項）及期貨商（期貨商管理規則第 17 條第一項）等。

[162] 觀諸金融相關法令規範，現行法對於若干金融機構之特定交易或投資金額設有總量管制者，包括：金融控股公司（金融控股公司法第 37 條第三至五項、第 44 條準用銀行法第 33 條、第 45 條第四項）、銀行（銀行法第 33 條第一、二項、第 33 條之 3 第一項、第 36 條第一項、第 37 條）、票券商或票券金融公司、信託業、保險業及證券商等。具體規範內容之彙整，請參閱：王志誠，前揭註 110，頁 34-43。

[163] BASEL COMM. ON BANKING SUPERVISION [BCBS], CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION ¶ 2, prin. 1 (2012).

[164] *Id.* ¶ 2, prin. 11.

[165] *Id.* ¶ 6, prin. 1. *See also id.* ¶ 2, prin. 11.

doi:10.6342/NTU202000744

指金融機構因財務與業務惡化或有惡化之虞時，為能及時糾正並控管其經營風險，由主管機關及早介入干預（early intervention）要求其改善，以有效地對於發生問題之金融機構為監督管理，避免金融機構之資本或淨值持續惡化，致衍生為系統性風險之金融監理機制[166]。綜言之，建立以風險資本為基準之監理措施，除了明確揭櫫處理時機與門檻，使銀行在經營危機惡化前，即能自行改善以外，亦使金融主管機關得於符合一定之法制條件下，及早糾正並協助銀行之風險控管。

第三款 小結——首重風險控管

準此，為平衡兼顧債權人與股東之利益，強調「風險管理」於金融機構公司治理之優先性與重要性或可謂允理愜情。再者，金融機構之經營與運作除須充分考量其內部所有債權人與股東等利害關係人之利益以外，基於金融機構作為金融中介之角色，或謂為資本市場之要角，其具有服務實體經濟等社會機能，倘若其經營不善或未能有效為風險控管，所造成之結果不僅將影響金融機構本身之繼續運作，亦將對整體社會造成不利影響，或將衍生為全球性金融危機，故可謂牽連甚廣。因此，風險管理之意識與討論，已然成為金融機構公司治理重點之所在。

第二項 風險管理專責機制之設置

前述對於風險管理議題之諸多重視，其實際作為即反映於金融機構內部治理機制或制度之革新，無論係設置風險管理委員會（Risk Management Committee）或派任風險控制長（Chief Risk Officer，CRO）等方法，均為透過專責風險管理單位與獨立風險管理通報管道等制度設計，強化金融機構內部之風險控管。然而，無論是風險管理委員會或風險控制長，其重點應在於金融機構內部應有一套風險管理專責機制，包括訂定適當之風險管理政策與程序，俾利董事會與高階管理階層據以評估與監督金融機構內部整體風險承擔狀況、決定風險胃納程度、採行必要之風險因應策略，以及掌握風險管理程序之遵循情形[167]。質言之，銀行之風險管理架構係

[166] 李智仁（2009），〈二〇〇八年銀行法修訂後之立即糾正措施法制布局〉，《法學新論》，14 期，頁 18。聯邦存款保險法之規定係按銀行槓桿比率（leverage ratio）與風險性資本要求（risk-based capital requirement）等資本適足率之數值，將監理基準分為資本良好（well capitalized）、資本適足（adequately capitalized）、資本不足（undercapitalized）、資本顯著不足（significantly capitalized），以及資本嚴重不足（critically capitalized）等五個類別，並依其資本等級採取寬嚴有別之監理措施。

[167] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 35 條第一項。

doi:10.6342/NTU202000744

由數程序所組成，包括辨識銀行或將面臨之各項風險、衡量與監控曝險程度、確保建置有效之資本規劃方案、採取控制或降低風險之手段，以及向董事會與高階管理階層報告銀行曝險與資本狀況[168]。

第三項 風險管理作為內控之底蘊

所謂「有風險才有控制」，由於金融機構日常業務活動涉及各式內生或外來之風險，為能有效控制與管理各項風險以達成營運獲利之主要目標，內控制度存在之基本目的係協助金融機構辨識、評估、控管及追蹤風險。質言之，無論銀行、金控公司或保險公司等金融機構之組織型態均為股份有限公司[169]，其等設立主要係以營利為目的[170]，故應如何在金融機構本身營運時，講求業務衝刺、訴諸時效、創造與維持利潤等基本需求，且兼顧風險控管、債權人治理、金融監理效率、服務實體經濟甚或普惠金融等金融機構公司治理目的間之平衡發展，即係內控制度設計上所應關注的重要之點。

準此，COSO 即以其所提出企業風險管理架構（ERM）為基礎，復於 2020 年發布報告，進一步細緻化並強調組織內建立與執行風險管理與分析之舉措或程序，對其達成組織任務與願景、實現核心價值、提升營運績效、創造與維持獲利表現等之重要性[171]。鑑於現今公司營運時將面臨之風險種類項目愈趨多樣且複雜[172]，企業風險管理架構不僅僅是組織整體與各單位部門執行風險管理程序之基礎，更係協助董事會與高階管理階層獲取充分資訊以訂定政策、作成最佳判斷、評估所有業務單位營運表現是否落實策略目標，以及董事會履行其監督職責等所不可獲缺者[173]。然而，縱有認為風險管理單純係特定部門之職責或分布於不同單位間獨立之風險評估程序，惟究其本質毋寧係整合（integrate）組織內部單位部門與營運活動、持續不斷運作、用以達成獲利、策略或特定目標之所有相關作業程序之基礎架構[174]。

---

168 *See* BASEL COMM. ON BANKING SUPERVISION, PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK ¶ 11 (2011).

169 銀行法第 52 條第一項；金融控股公司法第 10 條；保險法第 136 條第一項。

170 公司法第 1 條第一項。

171 *See* COMM. ON SPONSORING ORGS. OF TREADWAY COMMISSION [COSO], CREATING AND PROTECTING VALUE: UNDERSTANDING AND IMPLEMANTING ENTERPRISE RISK MANAGEMENT 2 (2020) [hereinafter COSO ERM FRAMEWORK 2020].

172 KPMG, PROTECTING AND CREATING VALUE THROUGH OPERATIONAL RISK MANAGEMENT 12 (2015).

173 *See* COSO ERM FRAMEWORK 2020, *supra* note 171, at 3.

174 *See id.* at 3-5.

doi:10.6342/NTU202000744

是故於今，風險管理並非只有指涉風險承擔、曝險程度評估或特定風險控管等概念或功能，就董事會與高階管理階層訂定經營策略或方針、提升整體營運績效表現等目的而言，系統性、全面之風險管理運作得提供重要分析資訊，協助其等作成決策判斷，為組織內部帶來正面效益[175]。

職是故，無論係具體組織、角色或機制之設計與配置，風險管理作為內控制度中不可或缺之一環，其除了協助金融機構辨識、評估、控管及追蹤風險等基本功能外，更係董事會與高階管理階層用以評估與發現錯誤策略，即時停損或予以改善，果斷作成判定以提升組織價值之必需工具。由此可知，風險管理實係觀察內控制度發展趨勢之重要焦點，或謂係有效運作內控制度以達成營運、報導及遵循等目標之基本精神。

第五節　法令遵循與內部控制

第一項 「遵循」之概念與功能

理論上，「遵循」（Compliance）乙詞存在三項要素[176]：第一，行為人所為之行為符合特定標準（standard）或規範（norm）。第二，前述標準或規範係由相對於該行為人之外部機關（external authority）所頒訂。第三，通常該行為人不會自發性地依據該標準或規範行事，而係出於某種誘因或外來之強制力。職此，對公司來說，無論其係為營利、實踐其經營理念或企業使命，其成立與運作除須遵守法令與內部規範以外，尚須顧及基於與各利害關係人之社會關係所建立之倫理規範，「遵循」即係指行為符合一切法令與倫理規範[177]。惟現行法規與其蘊含之概念多以「法令」為遵循之客體，故本文以下將進一步說明「法令遵循」之概念與其在內控制度中之功能。

法令遵循係為確保企業得依據法令規範訂定或修正其內部作業與控制程序或規章，且公司整體業務之運作得遵守外部法規範與內部規章，據以落實公司治理之

---

175 Kristin Broughton, *COSO Warns of the Downside of Siloing Risk Managers: New Guidance from the Advisory Group Emphasizes the Role of Risk Management in Maximizing Growth*, WALL STREET J. (Feb. 4, 2020, 5:42 PM), https://www.wsj.com/articles/coso-warns-of-the-downside-of-siloing-risk-managers-11580856142.

176 *See* GEOFFREY PARSONS MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 137 (2014).

177 平野温郎（著），高志明、林奕延（譯），前揭註。

doi:10.6342/NTU202000744

有效性。然而，法令遵循對於企業經營之運作模式具有相當之影響，因此公司應將法令遵循視為優化其內控制度、提升董事表現及加強對外報導內容之「機會」，且由公司內部各成員共同形塑法令遵循之組織文化並具體落實之[178]。舉例言之，法令遵循制度實施之目的係為確保公司業務之執行均符合各項法令規範，意即在公司營運或拓展業務之時，須由法令遵循人員或單位於事前就外部法規、內部作業程序等規範予以辨認，並與有關業務單位進行溝通，據此提出業務執行與內控程序設計之建議，惟諸等法令遵循相關措施存在評估、通報等內部作業之執行成本，或將對於公司營運或業務推動造成一定程度之遲滯或影響，故須有高階管理階層之支持，方能實現法令遵循之目標[179]。職是故，吾等或可將法令遵循落實於業務活動及其相關內控制度當中，視為一動態且持續之過程，其目的在於確保公司之運作係符合各項法令規範，故此實係公司內部所有成員之責任[180]。

現代法令遵循之功能與職責已由被動提供組織內部法規諮詢或顧問之地位，逐漸轉變為主動挑戰、獨立擔負執行法令遵循相關風險管理與監控任務之角色。質言之，法令遵循專責人員或單位不僅須以法律專業作為其基本必備能力，尚須充分瞭解組織內部所有業務活動與管理方法，以及各部門於業務執行過程中可能面臨之各項風險，俾能將相關法令監管規範與要求，妥適地轉譯且協助管理階層設計與執行控制與管理程序[181]。基此，茲以銀行內部之法令遵循人員或單位為例，諸等應具備相當之獨立性，意即無論是法令遵循人員或單位，其均應於銀行內部獲有正式職稱與專責部門之設置[182]，同時其不得執行與法令遵循之職責存在利益衝突之業務[183]，且須被賦予適當與足夠之權限取得充分資訊或資源[184]，方能有效執行「法令遵循功能」（Compliance Function）。

所謂法令遵循功能，主要指為協助管理階層有效地控管銀行內部於業務執行

---

178 DEBBIE TROKLUS & SHERYL VACCA, INTERNATIONAL COMPLIANCE 101: HOW TO BUILD AND MAINTAIN AN EFFECTIVE COMPLIANCE AND ETHICS PROGRAM 49 (2013).

179 林瑞彬、張憲瑋、陳月秀（2017），〈企業如何建置法令遵循計畫〉，《全國律師》，9 月號，頁 24。

180 *See* TROKLUS & VACCA, *supra* note 178, at 32.

181 *See* Piotr Kaminski & Kate Robu, *A Best-Practice Model for Bank Compliance*, MCKINSEY & CO. (Jan. 2016), https://www.mckinsey.com/business-functions/risk/our-insights/a-best-practice-model-for-bank-compliance#.

182 *See* BASEL COMM. ON BANKING SUPERVISION [BCBS], COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS ¶¶ 22-27 (2005) [hereinafter BCBS COMPLIANCE FUNCTION IN BANKS].

183 *See id.* ¶¶ 28-29.

184 *See id.* ¶¶ 30-33.

doi:10.6342/NTU202000744

時，可能發生之法令遵循風險所執行之各項手段。首先，誠如上述，法令遵循之主要作用在於控管銀行業務執行時之各項風險（如法令遵循風險、作業風險等），因此，法令遵循人員或單位除了須熟悉銀行各項營運業務內容以外，亦須與各個業務部門密切合作與充分溝通，據以協助各部門辨識與管理各項風險[185]。再者，法令遵循部門之主要職責尚包括：一、給予管理階層法令規範之諮詢與建議，二、提供法令遵循教育訓練，三、辨識、衡量及評估法令遵循風險，四、監控與測試法令遵循計畫與程序之有效性，以及定期透過獨立通報管道，逕向高階管理階層報告法令遵循功能之執行狀況[186]。綜言之，法令遵循人員或單位不僅須負責提供專業法令規範之諮詢，亦須積極與高階管理階層、風險管理部門及銀行內部所有業務執行單位共同合作，建立內控制度與法令遵循風險管理機制，以避免或降低銀行因違反相關法令所生之風險，達成有效營運獲利之目標。

第二項 法令遵循內控之實務運作

第一款 法令遵循風險評估

誠如本文前述，法令遵循部門（包括法令遵循專責人員或單位）於銀行內部之職務與地位，除了法令遵循制度之規劃、管理及執行，以及負責綜理法令遵循事務之外[187]，尚應負責建立全行之法令遵循風險管理與監督架構[188]。準此，結合了內控制度中，風險管理與法令遵循兩項重要功能、目標之「法令遵循風險評估」（Compliance Risk Assessment，CRA，以下簡稱法遵風險評估）即成為落實法令遵循內部控制之重要環節。然而，縱使主管機關已正視並要求金控公司與銀行等金融機構應建立法遵風險管理與監督架構或機制[189]，惟現行法規範並未對於法遵風險評估之意涵與作法有清楚之說明，故本文以下將先予回顧法遵風險之發展與現況，再透過觀察實務運作，嘗試闡釋法遵風險評估之具體內容。

---

185 *See id.* ¶ 21.

186 *See id.* ¶¶ 34-41.

187 金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條第一項。

188 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條之 1。

189 金融控股公司及銀行業內部控制及稽核制度實施辦法部分條文修正總說明（107 年 3 月 31 日修正）要點五、強化大型銀行業應建立全行之法令遵循風險管理及監督架構，並明定其架構原則及權責規定，包括建立全行法遵風險管理架構、獨立法令遵循組織及權責，以及落實法令遵循效能報告及監督（修正條文第三十四條之一）。

doi:10.6342/NTU202000744

第一目　從「法遵自評與考核」

銀行之法令遵循單位之基本功能包括訂定法令遵循之評估內容與程序，以及督導各業務單位定期自行評估其法令遵循執行情形，並對前述法令遵循評估作業之成效加以考核，以為管理階層執行單位考評之參考依據[190]。意即，法令遵循單位於此階段所擔負之職務僅係被動複查各業務單位作成並提交之「法遵自評報告」，故無論係實際執行法令遵循或撰擬法遵自評報告者，均係各業務單位之人員，法令遵循單位之人員僅能透過閱讀書面報告從事事後之書面考核。是故，法令遵循專責單位於實際執行面上，不僅較難透過其立基於內控制度三道防線中第二道防線之地位，主動辨析並掌控各業務單位法遵風險之所在，倘若業務單位出具之法遵自評報告有隱匿或不實記載之情事，抑或未為充分之資訊揭露，法遵單位之人員在欠缺與業務單位相關資訊之前提下，實存有難以發揮內控制度第二道防線風險管理與法令遵循功能之處[191]。準此，囿於法遵自評與考核無法主動偵測與監控法遵風險之限制，法遵風險評估之發展與落實即逐漸受到重視。

第二目　到「法遵風險評估」

誠如上述，為有效落實內控制度風險管理與法令遵循兩項重要功能，銀行內部除了應設置專責之法令遵循單位，綜理法令遵循業務以外，法令遵循單位尚應確實建立完善且健全之法遵風險評估、管理及監督架構，據以發揮主動偵測與控管法遵風險之職能。詳言之，法令遵循單位應建立辨識、評估、控制、衡量及獨立陳報法令遵循風險之程序、計畫及機制，以全面控制、監督及支援其他部門或營業單位之法令遵循事項[192]。同時，法令遵循單位應定期與不定期評估銀行之主要營運活動、商品或業務專案等是否存在潛在之法遵風險[193]。此外，銀行內部亦應有法遵風險警訊之獨立通報、評估及因應機制[194]。職是之故，銀行如何建立一套完整涵蓋法遵風險辨識、評估、控制、衡量、監控及獨立陳報等六項要素之「主動式」法遵風險管

---

[190] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條第一項第四款。

[191] 孫欣、章友馨，〈金融機構法令遵循風險評估與法規資料庫〉，KPMG，https://home.kpmg/tw/zh/home/insights/2018/01/law-compliance-risk-assessment-and-regulations-database.html（最後瀏覽日：11/21/2019）。

[192] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條之 1 第一項第一款。

[193] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條之 1 第一項第五款。

[194] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條之 1 第一項第四款。

doi:10.6342/NTU202000744

理之內控制度，據以專門執行法遵風險態樣之辨識、評估法遵風險發生之可能性與發生後銀行所能接受之範圍、決定現行與所欲達成風險控制程度，即值得思考。

具體而言，法遵風險評估實務操作流程概有三大步驟：首先為法規盤點，再者係法遵風險辨識、評估及監控，最後則為法遵風險報告。相關流程與內容如下表（九）所示：

法遵風險評估實務操作流程		
步驟	**方法**	**內容**
一、法規盤點	1. 辨識法令遵循義務	法遵單位透過自行盤點銀行應遵循之法規或委外建置之法規資料庫，事先綜覽與辨識所有法規與相應之內控程序，同時剔除無關之法規。
二、法遵風險辨識、評估及監控	2. 風險辨識	透過前述法規盤點之結果辨識法遵風險之所在與行為態樣。
	3. 風險評估	評估所有經辨識之法遵風險之風險發生可能性、頻率及嚴重程度，該結果將作為內控制度設計之指標。
	4. 風險控制	設計風險控制程序與措施，並衡量現行之內控程序得否有效降低相應之法遵風險。
	5. 法遵測試	確保所有經辨識與評估之法遵風險均已獲得控制，且該控制程序係有效且持續運作。
三、法遵報告	6. 法遵風險因應措施及獨立陳報	依據落實法遵風險評估程序之結果，由法遵單位向各個業務單位或部門提供對內控制度、法遵風險因應措施之設計或調整之建議，並將該結果向管理階層報告。

表（九）：法遵風險評估實務操作流程

doi:10.6342/NTU202000744

綜上所述，法令遵循之職責逐漸由傳統書面法令遵循自評報告查核，朝向整合風險導向之法遵風險評估發展。亦即主動偵查與發掘風險，同時為銀行之營運提供具有前瞻性與增值性之專業建議，扮演積極角色為銀行落實法令遵循並為其帶來加值貢獻。因此，為達前述目標，銀行內部法令遵循專責單位得經由操作法遵風險評估流程，以充分知悉銀行內部所有業務於執行時所應遵循之相關法令及其可能所生之風險，再者即須訂定有效之法令遵循計畫，作為銀行內部各成員或部門實際執行法令遵循與法遵風險管理之明確準繩。

第二款 訂定法令遵循計畫

「法令遵循計畫」(Compliance Program)此概念得追溯自美國量刑委員會(U.S. Sentencing Commission）於 1991 年所頒布之「聯邦量刑準則」(Federal Sentencing Guideline）第八章「組織之量刑」(Sentencing of Organizations）[195]。其指出，組織內部應合理地設計與實施有效之執行計畫(program)，據以預防或偵測違法行為之發生[196]，同時明確臚列有效之法令遵循計畫應具備之七項要素。值得注意者為該準則於 2004 年修訂時，將法令遵循風險評估納入有效性之定義，謂組織內部應定期評估違法或犯罪行為發生之風險，且應採取適當措施為設計、實施或修正前述法令遵循執行計畫，據以降低嗣經辨識之法令遵循風險[197]。由此可知，法令遵循與風險管理兩者間之密切互動關係，即唯有事前執行合理之法令遵循風險評估，方能清楚掌握風險之所在，並據以訂定法令遵循計畫與程序、員工訓練及稽核制度，故吾等可謂法令遵循風險評估實係有效執行法令遵循計畫之重要前提[198]。至於法令遵循計畫之具體構成要素，本文於下依序述之。

第一目 行為準則、政策及程序規範

法令遵循計畫之基礎係由董事會與高階管理階層共同依據組織日常業務活動內容，訂定結構性（structural）與實質性（substantive）等兩類型之法令遵循政策，

---

195 U.S. SENTENCING COMM'N [USSC], GUIDELINES MANUAL §3E1.1 (Nov. 1991) [hereinafter USSG].

196 *Id.* USSG §8A1.2, comment. (n.3(k)). ("An 'effective program to prevent and detect violations of law' means a program that has been reasonably designed, implemented, and enforced so that it generally will be effective in preventing and detecting criminal conduct.")

197 USSG §8B2.1.(c) (Nov. 2004).

198 張憲瑋（2018），〈法令遵循新趨勢——從法遵風險評估開始〉，《勤業眾信通訊》，11 月號，頁 15。

doi:10.6342/NTU202000744

前者是為組織內部執行法令遵循計畫之基本架構，包括法令遵循施行目標與任務、法令遵循專責人員或單位、審計與監督程序、內部通報程序等相關規則或其設置辦法；後者則須提供內部成員於執行日常業務活動時，所應遵循之法令規章之具體內容[199]。抑且，高階管理階層均應對法令遵循相關政策表達強烈、明確且具體之支持與承諾，方能確保內控制度、行為準則等內部治理規範之有效性[200]。再者，組織內部各單位主管須依據前述高階管理階層所擘劃之法令遵循政策，訂定明確、清楚且易懂之行為準則，作為內部成員執行日常業務，抑或作成決策時之依歸[201]，以避免或偵測不當行為之發生或風險。惟無論係法令遵循政策、程序規範或行為準則，除了須依照組織內部日常業務性質與內容訂定以外，尚須定期檢視修訂，抑或隨時視外在法令變動或經營環境情況調整之。意即，前述諸規範非僅為徒具形式、象徵性之政策宣示，毋寧係與時俱進地調整之「動態」書面文件[202]。

第二目　法令遵循專責人員或單位

為能有效落實高階管理階層之法令遵循政策目標，組織內部應設置獨立法令遵循單位，且應由董事會選派並賦予完整權限予法令遵循專責人員，由其擔負綜理法令遵循相關業務之主要責任。基於法令遵循職務內容之專業性與特殊地位（focal point），擔任法令遵循長（Compliance Officer）一職者，除須為法律專業之外，尚須對其任職領域之商業活動與產業環境，以及營運過程涉及之所有風險，均有相當程度之瞭解，並具備發現問題與良好溝通能力等條件[203]。換言之，法令遵循長之主要任務在於將組織內外部所有相關法令規範、自律規章等要求，有效地轉譯並納入各單位部門業務執行與管理活動之行為準則或作業程序當中，同時須協助為業務活動之風險控管[204]。基此，法令遵循長應掌握由董事會所授予之適當權限與執行職務時所需之資源，例如：其得依該職權充分獲取組織內部任何與執行法令遵循職務相關之文件或資訊，包括財務報告、會計記錄及供應商契約等[205]。抑且，法令遵循尚包括偵測與糾正內部員工於執行業務時是否存有舞弊行為等監督職責，為避免

199 TROKLUS & VACCA, *supra* note 178, at 10.
200 Org. for Econ. Co-operation & Dev. [OECD], *Good Practice Guidance on Internal Controls, Ethics, and Compliance*, Annex II (Feb. 18, 2010).
201 *See* TROKLUS & VACCA, *supra* note 178, at 8-9.
202 *See id.* at 12.
203 *See id.* at 15.
204 Kaminski & Robu, *supra* note 181.
205 *See* TROKLUS & VACCA, *supra* note 178, at 12.

doi:10.6342/NTU202000744

利益衝突、確保法令遵循部門得充分基於公司利益行事之獨立性，法令遵循部門於組織內部之設置應達一定層級，意即法令遵循部門不得低於且應自外於業務部門、財務部門、法務部門或風險管理部門等[206]。此外，組織內部應設有直接彙報管道（direct reporting line），俾使法令遵循長得循之逕向董事會或高階管理階層（主要為執行長）回報組織內部法令遵循之執行情形與狀況[207]。

第三目　員工教育與訓練

由法令遵循單位與人力資源部門（Human Resources，HR）配合，定期向組織內部所有成員進行法令遵循相關教育或訓練（包括新進人員教育訓練、在職員工之持續進修）係法令遵循計畫得準確落實，同時避免舞弊行為與風險發生之重要關鍵[208]。法令遵循教育訓練可分為一般教育課程與專門訓練課程[209]，前者指向所有員工闡釋前揭董事會與高階管理階層訂定之法令遵循政策與目標，再分別就不同業務單位或部門，個別說明針對其業務內容所設計之法令遵循計畫與執行方法；後者則係特別針對董事會與管理階層提供專業訓練，包括法令遵循執行情況之監督、法令遵循風險之控管方法。抑且，無論係一般或專門之教育訓練，兩者均須定期舉辦且應達基本時數，俾使組織內部所有成員得即時獲取與充分知悉最新之法令規範與法令遵循計畫內容[210]。除了前揭法令遵循相關課程外，教育訓練亦得透過定期發布新聞或出版品以說明最新法令規範，抑或部門會議、線上影音等其他形式為之[211]，惟無論為何種方法，教育訓練之重點係為促使董事、經理人及各業務部門員工在內之所有成員，均能充分瞭解個人於法令遵循活動中所扮演之角色與其職責內容[212]。

第四目　監控與審計

除了訂定法令遵循政策與執行計畫以外，法令遵循單位尚應與風險管理單位

---

[206] *See id.* at 13.

[207] *See id.*; *see also* Scott McCleskey, *The Evolving Role and Expectations of the Chief Ethics and Compliance Officer*, CORP. COUNSEL BUS. J. (Mar. 22, 2012), https://ccbjournal.com/articles/evolving-role-and-expectations-chief-ethics-and-compliance-officer.

[208] *See* MARTIN T. BIEGELMAN & JOEL T. BARTOW, EXECUTIVE ROADMAP TO FRAUD PREVENTION AND INTERNAL CONTROL: CREATING A CULTURE OF COMPLIANCE 98 (2d ed. 2012); *see also* TROKLUS & VACCA, *supra* note 178, at 21.

[209] *See* TROKLUS & VACCA, *supra* note 178, at 17-19.

[210] *Id.* at 18.

[211] *See* GARY DESSLER, A FRAMEWORK FOR HUMAN RESOURCE MANAGEMENT 260-61 (4th ed. 2005).

[212] BIEGELMAN & BARTOW, *supra* note 208, at 98.

doi:10.6342/NTU202000744

合作或向其諮詢，設計一套以風險為基礎之整合型監控與稽核計畫，以評估總體與個別之法令遵循政策與計畫是否有效運作。「監控」（Monitoring）指各業務單位或部門之管理階層，於每日經常性地用以評估其所管理之員工執行日常業務時，是否均依循法令遵循計畫或內部作業規範之程序，以及偵測與辨識內部是否有不當行為或舞弊等風險發生，俾利管理階層及時控管該風險或避免其再次發生[213]。「審計」（Auditing）則係藉由外部獨立監督管道，定期檢視（E.g., Retrospective Audit）或即時追蹤（E.g., Concurrent Audit）法令遵循計畫與內部作業程序規範之有效性，以及確保經查核後，已辨認或可疑之風險均為管理階層所處理或改善[214]。

第五目　獨立之通報與溝通管道

論及協助管理階層於組織內部落實法令遵循政策，以及預防或偵測舞弊行為發生之有效方法，尚包括鼓勵員工勇於向管理階層主動通報或反映，惟欲達成此法之重要前提為董事會與高階管理階層應於組織內部形塑正面積極之法令遵循文化與環境。首先，組織內部應設置對所有員工敞開之通報系統或通暢之溝通管道，並須避免任何員工因主動揭露其他員工未遵循法令之行為，使其招致報復或須承擔不利後果[215]，藉此建立員工對於公司與管理階層之信任、促進兩者間有效且持續之溝通。再者，凡屬經由通報系統、溝通管道或執行調查程序得知，以及員工所通報之任何內容或調查細節，管理階層均應確保其保密性（confidentiality）與匿名性（anonymity）之維持[216]，並不得向當事人或其他第三人洩露該通報員工相關或潛在得識別之資訊，於此同時降低報復行為發生之可能性。抑且，高階管理階層應使全體員工瞭解或知悉其建置之內部通報系統與溝通管道，並且使全體員工認知，對於所察覺之組織內部違反或疑似違反法令遵循之行為，應積極主動透過前述通報系統或管道與高階管理階層為溝通或揭露，係屬組織內部每位成員之責任[217]。

---

213 *See* TROKLUS & VACCA, *supra* note 178, at 22.

214 *See id.* at 23-24.

215 為鼓勵員工主動向其所屬管理階層通報或揭露公司內部其他成員違反法令、政策規範或其他有害、歧視性或不道德之行為，以及協助管理階層對於前述違反法令遵循之行為進行調查或執行法律程序，除訂定內部行為準則或相關管理規範以外，董事會或高階管理階層得訂定「反（防止）報復政策」，藉以控管或避免相關法律風險。*See Retaliation in the Workplace Policy*, WORKABLE TECH. LTD., https://resources.workable.com/no-retaliation-company-policy (last visited Dec. 30, 2019); *see also, e.g.*, TROKLUS & VACCA, *supra* note 178, at 73-75.

216 *See* BIEGELMAN & BARTOW, *supra* note 208, at 99.

217 *See* TROKLUS & VACCA, *supra* note 178, at 29.

doi:10.6342/NTU202000744

質言之，無論係通報系統或溝通管道之建立，主要目的均為促進管理階層與員工間存在開放、順暢且有效之溝通，包括即時更新法令遵循政策或規範、接獲緊急事件之通報並由管理階層及時處理等。職是之故，董事會或高階管理階層得先行由法令遵循文化與環境之形塑、通報系統與溝通管道之建置，以及確立防止報復政策等方式，提升與組織內部每位員工間之互信程度與溝通效率，從而使每位員工積極或無畏於履行其所負之通報義務（Duty to Report），最終達成有效監控或落實組織內部之法令遵循目標。

第六目　強制執行與激勵措施

董事會與高階管理階層訂定之法令遵循政策、程序規範及道德行為準則等，均應於組織內部持續不斷地推動與執行，且為有效落實法令遵循目標，須兼有適當之激勵與紀律或懲戒措施搭配實行[218]。首先，欲落實此項政策或措施之基本前提為，由法令遵循部門與人力資源部門協商或共同合作，透過上述員工教育訓練與溝通管道，定期提供法令遵循政策宣導與訓練課程，確保組織內部所有員工均充分瞭解其所應遵守之法遵循政策與計畫之具體內容[219]。同時，各部門管理階層須對於員工之行為或績效表現予以客觀且公平之定期評估（appraisal），此除係為確保員工於執行業務時所採取之手段方法與其所達成之結果，均符合行為倫理與公平待客等基本原則以外，亦係管理階層為明確於組織內部向各部門或員工傳達其對於員工遵守法令或政策行為之高度重視[220]。

準此，法令遵循單位須以書面擬定詳實且易懂之法令遵循行為標準守則[221]，且透過適當且即時地傳達，俾使每位員工於執行業務時皆能清楚知悉其所應遵循之相關法令或程序規範，同時，使董事會或各管理階層就違反法令或作業規章之行為而懲處相關人員時，均能有所本。職是故，為於組織內部充分貫徹法令遵循政策及其目標，倘若法令遵循單位或管理階層已明確且清楚地傳達法令規章予各該部門與員工，且已向諸位告知於執行法令遵循計畫遇有疑義或困難時所能諮詢或溝通之對象或管道後，個別行為人仍有未妥適執行或違反法令遵循之行為發生時，其等

[218] *See id.* at 31-32; *see also* BIEGELMAN & BARTOW, *supra* note 208, at 99.
[219] *See* TROKLUS & VACCA, *supra* note 178, at 32.
[220] *See* Gary R. Weaver & Linda Klebe Treviño, *The Role of Human Resources in Ethics/Compliance Management: A Fairness Perspective*, 11(1-2) HUM. RESOURCE MGMT. REV. 113, 124 (2001).
[221] *See* TROKLUS & VACCA, *supra* note 178, at 32.

doi:10.6342/NTU202000744

即須對於違反法令遵循者施以適當之懲戒或紀律措施[222]，以端正組織內部之法令遵循文化。

然而，藉由管理階層對於違犯法令遵循規範之員工給予懲戒或其他具有懲罰性質之紀律措施的方式，至多僅能得到暫時或短期之嚇阻效果，尚無法根本性地改變員工之行為態度，或促使員工自發性地遵循法令或內部規範[223]，故正面紀律管理[224]或獎勵（reward）等激勵措施於此逐漸受到重視。管理階層得為個別員工或部門設定法令遵循目標，例如檢視員工或部門之績效表現時，亦須探究其是否確實遵循內部作業程序規範或相關法令，並於達成目標時給予額外薪酬，或提供升遷機會等獎勵[225]。綜言之，無論係漸進式紀律管理、正面紀律管理等強制執行之處置措施，抑或激勵措施等，諸等措施訂定與實施之目的均係管理階層為於組織內部營造或強調其對於法令遵循之重視、形塑有效落實法令遵循之組織文化，俾使個別員工或部門均能確實遵循應有之行為規範，共同創造與維繫全體之利益。

---

[222] 舉例言之，多數組織對於其內部違反法令遵循或其他內部規章之行為人，係以採取「漸進式紀律管理」（Progressive Discipline），即係針對個別員工於執行業務過程中，違犯內部政策或程序規範等不當行為之嚴重程度與發生次數，由管理階層分別、逐步給予其非正式告誡、口頭提醒、書面警示、罰款、行政處分、降級、停職、解僱或交付司法程序等處置。*See* DESSLER, *supra* note 211, at 264-65; TROKLUS & VACCA, *supra* note 178, at 33.

[223] *See* DESSLER, *supra* note 211, at 265.

[224] 所謂「正面紀律管理」（Positive Discipline）或稱「非懲罰性紀律管理」（Nonpunitive Discipline; Discipline Without Punishment），係指管理階層與員工透過個別溝通、討論，對於可能發生之違犯法令遵循規範之行為，訂定合理之監督或解決方案，以鼓勵員工自我檢視其行為、提升員工對於行為規則或準則之接受程度，並願就其個人行為負起責任。該管理措施具體包括四道步驟：第一，會面唔談（oral reminder），管理階層須確保員工同意就已發生或可能發生之不當行為，主動與之討論解決方案或預防方法。第二，擬定書面計畫（written reminder），倘若前述解決方案或預防方法無法有效發揮監督之作用，管理階層即須寄發書面通知與員工再次會唔，共同探究該措施失敗之原因並再次建立新的紀律管理計畫，且會唔結果須以書面記錄之。第三，「一日給薪決策假」（a paid decision-making leave），惟如管理階層與員工雙方再次擬訂之紀律管理計畫亦無法有效阻止員工不當行為之發生，則管理階層即須給予該名員工一日之決策假，強制其暫時離開工作崗位，並自行評估自身狀況是否符合現有之職位或適合執行現有之職務。若該名員工認為其能夠勝任此職，並向管理階層或其監督者提出新的紀律管理計畫且承諾繼續遵守之，則可復歸至其原有之工作崗位。第四，解僱（dismissal），會面唔談或於前述各階段所提出之紀律管理計畫均無法達成預防或糾正員工不當行為之目的時，管理階層則須考量解僱該名員工。*See id.* at 265-66; *see also* David N. Campbell et al., *Discipline Without Punishment—At Last*, HARV. BUS. REV., https://hbr.org/1985/07/discipline-without-punishment-at-last (last visited Nov. 19, 2019).

[225] *See* TROKLUS & VACCA, *supra* note 178, at 33; *see also* Weaver & Treviño, *supra* note 220, at 125-26.

doi:10.6342/NTU202000744

第七目　回應與預防

除了執行前述違反法令遵循之相關處置措施外，管理階層尚應就該行為個案對於組織內部整體之法令遵循政策與計畫，抑或對於組織本身所造成之不利影響與負面衝擊，為後續之追蹤、適當回應及預防，確保其所訂定之政策或程序規範得穩定且持續發揮效用[226]。倘若組織內部員工或部門發生違犯法令遵循之不當行為，管理階層除了追究並要求特定行為人須承擔相當之責任以外，其尚須與法令遵循單位、法務部門及外部顧問等，共同就該事件，於相當期間內為內部調查、釐清事件發生之原因與始末，藉此瞭解組織內部現行之法令遵循政策與程序有何闕漏，或無法有效約束員工行為之不足處，進而採取必要補救措施與適當回應[227]。再者，管理階層應將其對於違犯法令遵循個案為內部調查之執行過程與結果作成書面報告或文件紀錄，該書類須詳細記載個案發生之具體事實、管理階層執行之紀律或處置措施、內部調查之時程、執行方法及最終調查結論[228]，且最重要者係於該個案發生後，對於現行既有之法令遵循計畫內容，管理階層或法令遵循單位應如何重新設計或修正調整之，俾能有效防免類似情形再度發生、充分落實法令遵循之目標。

第三款　建置法令遵循資料庫——兼論洗錢防制

為協助銀行內部各單位運作法令遵循功能與執行法令遵循計畫之義務，法遵單位或部門相關人員除應具備必要之智識、能力及經驗外，尚得獲取足夠之資源以履行其職責[229]。該資源係指銀行內部應定期提供系統化教育與訓練，俾使法遵人員得即時瞭解與掌握最新法令規範[230]，據以制訂或更新法令遵循計畫，並落實於銀行內部各業務單位之實際營運過程。誠如前揭法遵風險評估實務程序所述，法遵部門首須執行之步驟係對於銀行業務相關法令為盤點與彙總，故為協助法令遵循人員蒐集、盤點及即時更新所有法令規範與相關資訊，「法令遵循資料庫」之開發與建置乃應運而生。簡言之，法令遵循資料庫於銀行法令遵循作業程序中具有彙整與更新法令規範、取得與保存法遵資訊等兩項重要功能，以下分述之。

---

226 *See* TROKLUS & VACCA, *supra* note 178, at 34.
227 *See id.* at 34-35; *see also* BIEGELMAN & BARTOW, *supra* note 208, at 99.
228 *See* TROKLUS & VACCA, *supra* note 178, at 35-36.
229 BCBS COMPLIANCE FUNCTION IN BANKS, *supra* note 182, ¶ 33.
230 *See id.*

doi:10.6342/NTU202000744

第一目　法令規範之彙整與更新

法令遵循資料庫作為執行法令遵循作業與風險評估之重要底層架構工具，其首要功能在協助法遵部門得於最短期間內，取得處理金融機構內部各項業務法令遵循相關議題所需之最新法令規範與內部政策，有效降低法令遵循人員搜尋法規與對應內部政策之成本，進而提升管理法遵風險之效率[231]。茲以金融機構之洗錢防制與資恐打擊實務作業為例[232]，倘若將所有須遵循之相關法規依其層級區分：屬法律者包括「洗錢防制法」[233]與「資恐防制法」[234]；屬授權命令者則有「金融機構防制洗錢辦法」[235]、「銀行業防制洗錢及打擊資恐內部控制與稽核制度實施辦法」[236]、「存款帳戶及其疑似不法或顯屬異常交易管理辦法」[237]、「國際金融業務分行管理

[231] 孫欣、章友馨，前揭註 191。

[232] 基於資恐防制與洗錢防制均係以金流為規範重心，以防免金流斷點產生資恐與洗錢風險，故目前各行政法規或自律規範均將資恐防制作業併入洗錢防制作業辦理(資恐防制法第 2 條立法理由)。

[233] 為健全防制洗錢體系、重建與穩定金融秩序、促進金流軌跡之透明及強化國際洗錢防制活動之合作，立法者特訂定《洗錢防制法》作為洗錢防制專法（洗錢防制法第 1 條）。

[234] 近年來，有鑒於恐怖主義對於各國人權已產生極大威脅，各國遂對於資助恐怖主義所伴生之恐怖活動、組織及其成員等資恐行為施以刑罰，並對於資恐與武器擴散行為進行「目標性金融制裁」（Targeted Financial Sanctions）之措施，始能有效防制恐怖主義與武器擴散。故為防止並遏止對恐怖活動、組織或份子之資助恐怖主義行為，以維護國家安全、保障基本人權、強化資恐防制國際合作，立法者參酌聯合國「制止向恐怖主義提供資助國際公約」（International Convention for the Suppression of the Financing of Terrorism，又稱反資恐公約），以及防制洗錢金融行動工作組織（Financial Action Task Force，以下簡稱 FATF）所發布之「防制洗錢及打擊資助恐怖主義與武器擴散國際標準」（International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation，簡稱 FATF 國際標準）40 項建議之第 5 項至第 7 項，決議訂定《資恐防制法》（資恐防制法立法總說明、第 1 條及其立法理由）。

[235] 依據洗錢防制法第 4 條第一項前段、第 8 條第三項、第 9 條第三項及第 10 條第三項等授權規定，中央目的事業主管機關（即金管會）應就確認客戶身分、國內外必要交易紀錄保存、一定金額以上通貨交易之申報及疑似洗錢與資恐等交易之申報義務範圍與內容等事項訂定授權辦法，故其參酌銀行業、證券期貨業及保險業之防制洗錢及打擊資恐注意事項等規定，擬具《金融機構防制洗錢辦法》（金融機構防制洗錢辦法第 1 條）。

[236] 依據洗錢防制法第 6 條第三項之授權規定，金融機構應依洗錢與資恐風險及業務規模，建立洗錢防制內部控制與稽核制度。故金管會經參酌「金融機構防制洗錢辦法」、「銀行業及電子支付機構電子票證發行機構防制洗錢及打擊資恐內部控制要點」（該要點已於 107 年 11 月 9 日由金管銀法字第 10702744680 號法令函釋公告廢止，並於同年 11 月 11 日生效）之規定，以及 FATF 發布之建議及評鑑方法論，訂定本辦法（銀行業防制洗錢及打擊資恐內部控制與稽核制度實施辦法總說明、第 1 條）。

[237] 本辦法係依據銀行法第 45 條之 2 第三項之授權訂定。依本辦法第 4 條第二款第八目，符合中華民國銀行公會「銀行防制洗錢及打擊資恐注意事項範本」所列疑似洗錢表徵之交易者，即屬疑似不法或顯屬異常交易，銀行即須採取同辦法第 5 條第二款所訂之第二類處理措施，包括對該等帳戶進行查證與持續進行監控，並依洗錢防制法等相關法令規定處理等。

doi:10.6342/NTU202000744

辦法」[238]、「金融機構對經指定制裁對象之財物或財產上利益及所在地通報辦法」[239]等；其他尚包括「金融機構辦理國內匯款及無摺存款作業確認客戶身分原則」[240]、「銀行業辦理外匯業務作業規範」，由中華民國銀行公會訂定之「銀行防制洗錢及打擊資恐注意事項範本」與「銀行評估洗錢及資恐風險及訂定相關防制計畫指引」，以及銀行業各項兼營業務應遵循之所屬公會自律規範等。

由此觀之，僅就銀行業防制洗錢與打擊資恐相關法規而言，其所應遵循者包括法律、授權命令、行政規則及自律規範等多種規範態樣。抑且，無論係立法者或金管會等行政機關均持續修正或增訂各項法令規範，故對於任何法規之更新或頒布，法遵部門人員除了須能迅速反應並再次進行法規之盤點外，尚須重新檢視銀行內部相應之業務單位現行之政策或作業程序是否須相應調整，以符合法規範之要求。或謂藉由人工作業仍能完成法規盤點更新與相應內控程序調整之任務，然而考量銀行內部法令遵循部門於人力、資源及時間之有限與業務運作之時效，倘若採用系統化之法令遵循資料庫以協助法遵人員即時執行前述作業內容，即可有效提升達成遵循目標之效果，亦能節省成本與避免不必要之延滯。

---

[238] 依金融控股公司及銀行業內部控制及稽核制度實施辦法第 8 條第一項第二款第十一目規定，銀行業應建立辨識、衡量及監控洗錢與資助恐怖主義風險之管理機制，以及遵循洗錢防制相關法令之標準作業程序。國際金融業務分行業務本即涵括於銀行整體防制洗錢及打擊資恐架構中，但就國際金融業務分行辦理確認客戶身分程序，所應參考與驗證之文件、資料或資訊宜有一致性標準。基此，金管會考量新加坡、香港等鄰近金融中心對於確認客戶身分程序之作法日趨嚴格，乃參考其作法，檢討並修正本辦法。該辦法明定國際金融業務分行應遵循洗錢防制與資恐防制等相關法令與銀行公會之自律規範（例如：「國際金融業務分行接受境外客戶開戶暨受託投資信託商品自律規範」）等規定，確實辦理確認客戶身分程序，並納入內部控制及內部稽核項目。該辦法亦指出，國際金融業務分行得透過中介機構協助其對境外客戶辦理身分確認程序，惟須訂定包括由中介機構協助確認客戶身分程序之範圍，及客戶資料保密及資料保存之內部控制制度等內容之執行方案，並應報金管會備查（國際金融業務分行管理辦法 106 年 5 月 22 日修正總說明、第 10 條及第 11 條）。

[239] 依據資恐防制法第 7 條第四項之授權規定，銀行、信託投資公司、保險公司等金融機構，因業務關係知悉經指定制裁之個人、法人或團體之財物或財產上利益及所在地時，應即通報法務部調查局。故金管會經參酌 FATF 發布之建議與美國財政部「外國資產控制辦公室」（Office of Foreign Assets Control，OFAC）之規定擬具本辦法，明定通報之程序、方式、通報紀錄與交易憑證之保存年限等，並規定金融機構應指派專責主管協調監督本辦法之遵循（金融機構對經指定制裁對象之財物或財產上利益及所在地通報辦法總說明）。

[240] 金管會為使銀行、信用合作社及中華郵政公司等金融機構之洗錢防制作業更趨嚴謹與打擊犯罪，並促使匯款與無摺存款客戶留存資料，以利金融機構認識客戶、保障存款戶之權益及防範詐騙，故訂定本原則，要求前述金融機構辦理現金匯款、轉帳匯款及無摺存款案件，應核對、確認及留存客戶之身分資料（金融機構辦理國內匯款及無摺存款作業確認客戶身分原則第 1 至 5 條）。

doi:10.6342/NTU202000744

第二目　法遵資訊之蒐集與保存

除了上述法規資料之盤點與持續更新外，法令遵循資料庫尚具有留存與保管業務文件、客戶資料及交易紀錄等重要資訊之功能。為使銀行充分瞭解其客戶與金融業務活動，俾利達成有效之風險管理，抑或為於主管機關為金融檢查、稽核單位為定期查核時提交相關文件或衍生紛爭時提供司法機關調查之線索，則各項業務資訊之取得與管理，即屬銀行日常營運活動中所不可或缺者。質言之，參酌防制洗錢金融行動工作組織（Financial Action Task Force，以下簡稱 FATF）發布 40 項標準建議第 11 項內容[241]，銀行應依據法律規定，妥適保存所有國內外必要交易紀錄[242]、因執行客戶盡職調查（Consumer Due Diligence，CDD）措施而取得之紀錄、帳戶檔案、業務往來資訊及其相關分析資料等[243]，抑且無論係客戶盡職調查資訊或交易紀錄，銀行應使權責機關經由適當授權下要求其提供時，均得以取得。基此，法遵部門首先須依前述各項法令規範之要求，訂定對內與對外保存資訊之程序與規則，包括應取得與列入法令遵循資料庫保存之資訊範圍與類型、保存期限、歸檔原則及調閱程序等，並應確保所有資訊均能確實留存記錄或依據最新相關法令規定即時更新、保持其正確性[244]。

再者，為履行其評估銀行主要營運活動、商品、服務或業務專案之法令遵循風險管理情形之職責[245]，抑或執行業務範圍盤點與定位、歸戶、身分辨識與驗證、資料清查等洗錢防制、資恐打擊相關程序[246]，法遵部門須輔以「交易監控系統」即時

---

241 *See* FIN. ACTION TASK FORCE [FATF], INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS ¶ 11 (2019), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf [hereinafter FATF 40 RECOMMENDATIONS]. 此外，本項建議內容已訂入《金融機構防制洗錢辦法》第 12 條。

242 國內外交易之所有必要紀錄應至少保存五年，且該等紀錄應足以重建個別交易，除須於權責機關有需要時由銀行即時提供外，尚須於必要時，作為偵查或認定不法活動之證據。*See* FATF 40 RECOMMENDATIONS, *supra* note 241; 金融機構防制洗錢辦法第 12 條第一、三款。

243 舉例言之，銀行因執行客戶盡職調查措施所取得之客戶紀錄包括護照、身分證、駕照或其他類似之官方證明文件之影本或紀錄；帳戶、電子支付帳戶或卡戶檔案或契約文件檔案；對於複雜、異常或大宗交易進行詢問所取得關於該交易背景或目的之資訊或分析資料。*See* FATF 40 RECOMMENDATIONS, *supra* note 241; 金融機構防制洗錢辦法第 12 條第二款。

244 謝雪妮（2017），〈銀行業防制洗錢及打擊資恐機制實務〉，王文杰（等著），《新洗錢防制法——法令遵循實務分析》，頁 409-411，臺北市：元照。

245 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條之 1 第一項第五款。

246 銀行為落實洗錢防制專案，須採取業務範圍盤點與定位、身分辨識與驗證（Identification and

doi:10.6342/NTU202000744

更新法令遵循資料庫內部保存之所有客戶資訊與交易紀錄。詳之，由於銀行內部業務單位與營業項目眾多、金融商品與服務種類多元、客戶群眾廣大且交易數據資料龐雜，依據風險基礎方法建立之交易監控系統得協助銀行對於客戶資料與各項交易為持續監控，除了確保銀行所蒐集之資訊係屬正確與完備外，尚得就特定業務單位未確實執行相關內控程序，抑或疑似洗錢或資恐等不法交易等法令遵循風險，向法遵部門提出預警[247]。

第三目　法遵資料庫與數據治理

誠如前述，諸如法令規範、業務文件、客戶資料及交易紀錄等「法遵資訊」之蒐集與彙整，對銀行內部執行包括洗錢防制在內之法令遵循相關政策與作業程序而言，具有重要之地位。由於銀行業務項目與商品內容愈趨多元、金融服務或交易之數據資料與金流益發龐雜，抑且洗錢防制等各項法令遵循相關作業流程對於銀行內部所有資訊之整合與流通等要求日益嚴格，故銀行內部所有法遵資訊顯非能僅憑人工作業得處理完成或免於人為之錯誤或疏漏。例如，洗錢防制與資恐打擊之法令遵循計畫與執行架構尚應奠基於風險評估流程[248]，舉凡金融機構風險評估、客戶風險評級、名單比對與過濾、帳戶與交易之持續監控、一定金額以上或可疑之交易申報作業等風險控管相關流程[249]，均須仰賴法遵資訊之快速篩選與運算程序，如何執行良好之業務資訊管理或數據治理（Data Governance），則屬銀行內部須投入相當資源與成本者。

Verification，ID&V）、總歸戶及資料清查等前置作業，執行該流程之目的首先在於整合銀行內部不同業務部門（例如一般存款、信用卡、貸款、信託、保管箱、貿易金融及證券、票券等兼營業務）所持有之客戶資料（包括自然人、法人等一般概念下之客戶；監護人、實質受益人、代理人、保險受益人、貸款保證人等客戶關係人；銀行行舍之出租人、供應商、未核卡或未核貸人、已關戶或已死亡戶或拒絕往來戶等非客戶；關係企業、海外分公司或子公司等），確保每位客戶於銀行內部各業務單位所留存之基本資料均已完備，且足致作成身分係屬正確之判定。再者則係持續對於前述客戶資料與日常各項交易紀錄為清查程序，確保各個交易軌跡或交易對手之資料均可取得及其完整性，俾利後續為風險辨識與風險管理政策之訂定與執行。關於銀行業洗錢防治專案管理與基本架構之完整說明，請參閱：王任翔（2019），《洗錢防制法——銀行業實務挑戰》，二版，頁 45-64，臺北市：元照。

[247] 金融機構防制洗錢辦法第 9 條。

[248] *See BSA/AML Manual: Core Examination Procedures for Assessing the BSA/AML Compliance Program*, FFIEC BANK SECRECY ACT/ANTI-MONEY LAUNDERING INFOBASE, https://bsaaml.ffiec.gov/manual/ComplianceProgram/01 (last visited Dec. 8, 2019).

[249] 陳麗琦、萬幼筠（2017），〈金融業防制洗錢查核專案作業探討〉，王文杰（等著），《新洗錢防制法——法令遵循實務分析》，頁 337-351，臺北市：元照。

doi:10.6342/NTU202000744

質言之，銀行業本身之產業特性與業務複雜度，相較於壽險業或證券業等其他金融機構，具有業務形態多元與內部單位分工縝密、作業流程繁複、客戶數量眾多以及相關契約條款內容細膩等特色，致使銀行各單位或部門於執行業務，抑或提供客戶金融商品或服務等日常營運活動時，取得之數據或資料規模龐大，故需有良好之資訊管理系統協助處理與管理銀行內部 24 小時不間斷所產生之各項交易數據紀錄與動態合約關係[250]。再者，銀行內部不同業務單位尚分別涉及繁複之法令規範與內部政策，且其又與相應內控程序之訂定緊密連結，故法遵資料庫之建置與核心系統之重構或修正，係協助法遵部門以迅速、確實盤點與更新法規、有效達成內部控制之遵循目標所不可或缺者。舉例來說，除為符合金融主管機關之監管要求，銀行內部應盤點與彙整所有業務執行相關法規外，法遵部門須進一步確保各該業務單位內部訂定與執行之內控制度作業程序均符合法規要求；抑或透過搜尋取得法遵資料庫所儲存之資訊，法遵部門得履行協助控管銀行整體法令遵循風險、定期向董事會或高階管理階層報告內控制度執行情形等職責。

第四款 小結——法令遵循之兩點觀察

鑑於現行金融機構法令遵循之實務發展漸趨迅速與多樣，其規範體系亦愈趨嚴格，尤以兆豐商銀因洗錢防制法令遵循之缺失，致遭美國紐約金融服務署裁罰後，並為因應亞太防制洗錢組織（Asia/Pacific Group on Money Laundering，APG）年度相互評鑑，洗錢防制與資恐打擊遂為銀行法令遵循實務之首要議題。準此，本文依據上述分析認為，金融機構內部執行法令遵循仍有其基本架構可循：參考美國聯邦金融機構檢查委員會（Federal Financial Institutions Examination Council，以下簡稱 FFIEC）針對「銀行保密法」（Bank Secrecy Act，BSA）與洗錢防制法等要求，其指出法令遵循之基本架構至少須涵蓋風險評估、法令遵循計畫、可疑交易監控與通報系統及自動化系統等[251]。其中，法令遵循計畫須包含「內部控制系統」、「獨立

[250] 李悅嘉（2019），〈系統更新引風暴——南山人壽給金融業寶貴一課〉，《台灣銀行家》，12 月號，頁 72-75。*See also* MARK ALLEN & DALTON CERVO, MULTI-DOMAIN MASTER DATA MANAGEMENT: ADVANCED MDM AND DATA GOVERNANCE IN PRACTICE 4 (2015).

[251] *See BSA/AML Manual: Core Examination Procedures for Assessing the BSA/AML Compliance Program: Examination Procedures: Scoping and Planning*, FFIEC BANK SECRECY ACT/ANTI-MONEY LAUNDERING INFOBASE, https://bsaaml.ffiec.gov/manual/CompliancePrograM/01_ep (last visited Dec. 18, 2019).

doi:10.6342/NTU202000744

測試」（Independent Testing）、「法令遵循專責人員」及「訓練」等四要素[252]，即係銀行欲建立法令遵循架構之基本項目。

再者，前述法令遵循架構於洗錢防制與資恐打擊具體落實後，伴隨國際潮流與主管機關之高度重視，包括銀行在內之金融機構於法令遵循層面之應用亦逐漸擴展至個人資料保護、反貪腐與反舞弊、營業秘密管理、防範內線交易等範疇[253]。諸等實務發展均在在顯示：建置健全之法令遵循架構，以及更重要的法遵意識、文化之形塑與深化，勢必將對於金融機構公司治理之議題產生愈趨重要之影響。準此，以下將分別析述本文對於法令遵循基本架構與實務發展之初步觀察。

第一目　法遵基本架構

FFIEC 首先指出，為達成銀行保密法、洗錢防制法等法令規範遵循之目標，須由董事會與高階管理階層於銀行內部形塑良好之法令遵循文化，並依銀行自身規模、結構、內部各項業務之曝險程度及複雜度等，據以建置包括監控與通報等功能之內控制度，作為達成法令遵循目標之運作基礎[254]。

第二，為協助董事會與高階管理階層得直接獲悉並具體改善內控制度於運作過程中或有不足之處，銀行除須設立專責之內部稽核單位定期就內控制度為查核評估外，尚須聘任外部審計人員或顧問等具備專業查核資格者，定期就銀行所有業務活動與管理資訊系統（Management Information Systems，MIS），執行以風險為基礎之獨立且客觀之查核程序（即獨立測試），由此辨認內部控制缺失，並進一步評估與瞭解內控制度設計之良窳及其執行之有效性[255]。

---

[252] FED. FIN. INSTS. EXAMINATION COUNCIL [FFIEC], BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL 28-30 (2014) [hereinafter FFIEC BSA/AML EXAMINATION MANUAL].

[253] 林瑞彬、張憲瑋、劉家全（2018），〈法令遵循管理的回顧與展望〉，《勤業眾信通訊》，元月號，頁 28。

[254] *See* FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 252, at 29. 舉例言之，內控制度應具備之功能包括：辨識銀行內部各項業務活動相關風險（例如產品、服務、自然人與法人客戶等）、確立銀行內部負責訂立風險管理或法令遵循之人並定期向董事會與管理階層彙報各項制度與程序之執行狀況、實施以風險為基礎之客戶盡職調查措施、確保銀行各項紀錄與報導等資訊內容均符合最新法令規範等。

[255] *See id.* at 30-31. 內控制度之獨立測試內容包括銀行法令遵循政策與程序是否符合法令規範之基本要求及其適足性與有效性；對於內部各項業務活動（包括產品、服務、自然人與法人客戶等）執行風險評估之合理性；以風險為基礎之交易風險測試之揭露是否符合紀錄與報導相關之法令規範要求；員工訓練之適足性、準確性及完整性；可疑交易活動監控系統與管理資訊系統運作之有效性；

doi:10.6342/NTU202000744

第三，基於董事會之職責包括應訂定銀行內部法令遵循目標與政策，抑且其須對於法令遵循相關事務之執行負起最終責任，故其應聘任或於銀行內部指派一或數名具備專業智識與能力者擔任法令遵循專責人員，授與適當層級與權限、提供充分資源予該專責人員，以委由其負責綜理銀行整體法令遵循業務，協調、確保及監控各業務單位日常執行法令遵循程序之具體情形[256]。此外，董事會應建立與法令遵循專責人員間良好溝通橋樑與資訊傳遞管道，俾利法令遵循專責人員得定期或隨時將法令遵循執行狀況向董事會或其他管理階層報告，以及利於董事會得憑藉法令遵循人員所提供之資訊作成適當決策[257]。

第四，銀行內部應對於包括董事、經理人等在內之所有職員，依各人之職務權限與責任範圍，定期提供完善且即時之教育訓練，以利其充分獲悉各自執行之業務所須遵循之相關法令內容與最新動態[258]。質言之，法令遵循人員原則上除應具備專業智識與能力外，尚須定期受訓以吸收最新法令規範；銀行內部各業務單位之職員除了須於入職時，接受新進員工教育訓練，瞭解其執行之所有業務內容與相關法規外，亦應定期進修以掌握業務最新發展；至於董事會與各管理階層則須深入瞭解所有業務內容與其風險、具體法令規範及相應罰則，俾利其執行訂定銀行整體法令遵循目標與政策、擔負法令遵循與內部控制之最終責任等職責[259]。最後，銀行內部過往曾經執行之法令遵循相關教育訓練內容、時程及執行情形等，均應由各業務部門與法令遵循單位人員作成紀錄並應妥予文件化與留存，以作為內部稽核或外部查核評估銀行內控制度執行成效之重要參考依據[260]。

第二目　實務發展趨勢

觀諸銀行之基本業務包括收受存款、信託資金及辦理匯兌業務等[261]，即作為資金供給者與資金需求者之中介機構角色，銀行之運作須能有效促成資金融通、妥適

以及董事會與管理階層是否具有足夠之專業能力得改善或修正內控制度之不足或內部人員違反之情事等。再者，內部稽核單位執行獨立測試所使用之工作底稿，及其測試完畢獲致之評估結論、意見及建議等應作成紀錄或報告，並應將該等文件即時提供予董事會與管理階層作為修正與改善之參考。

256 *See id.* at 32.

257 *Id.*

258 *See id.* at 32-33.

259 *See id.*

260 *Id.*

261 銀行法第 3 條。

doi:10.6342/NTU202000744

將資金導入生產事業，以符合經濟活動之成本效益，或謂銀行掌握「金流」之融通與保管。此外，銀行於金融市場中尚具有創造「信用」之功能，意即金融市場交易之標的多為無形資產，且該交易架構之所以能夠運作係基於金融消費者對於該金融機構之信任所致[262]，故銀行之經營者、職員等是否秉持誠實信用原則作為執行業務之準繩，即係金融市場與交易能否有效且安全運作之基礎。再者，銀行本身型態為「金融服務業」[263]，其所能提供之金融商品或服務種類繁多，為能依據金融消費者之實際需求，作成妥適之財務規劃與資產負債配置，銀行須充分瞭解金融消費者，以完成客戶之需求與風險屬性分析，或可謂銀行得蒐集與持有大量自然人或法人與金融機構為金融交易而提供之非公開資料，包括基本資料、帳務資料、信用資料、投資資料、保險資料等財務與其他「個人資料」。抑且，基於國際金融監理之趨勢與司法（如法務部調查局）、行政（如金管會）機關之高度重視，金融機構應執行嚴格之以風險為基礎之客戶審查程序，以及履行交易紀錄保存與可疑交易通報等義務，以建立透明化之金流軌跡、杜絕重大犯罪集團利用金融機構等管道洗錢，故銀行尚得掌握種類與內容豐富之「資訊流」。準此，除前述洗錢防制與資恐打擊之法令規範以外，本文觀察銀行法令遵循之實際應用或趨勢尚包括「個人資料保護」、「資訊系統安全」及「反賄賂」等，以下分述之。

（一）個人資料保護——首先，內控制度與個人資料保護之關係主要以「個人資料保護法」之遵循與「金融隱私權」之保護為中軸，前者就個人資料之使用原則設有規定，且因金融控股公司、銀行業（存款機構）、保險業、證券業等金融機構係該法所稱之「非公務機關」[264]，故其對金融消費者個人資料之蒐集、處理及利用

[262] 王文宇（2016），〈金融法制與金融監理〉，王文宇（等著），《金融法》，九版，頁 6，臺北市：元照。

[263] 所謂「金融服務業」係指包括金融控股公司；金融重建基金；中央存款保險公司；銀行機構、信用合作社、票券金融公司、信用卡公司、信託業、郵政機構之郵政儲金匯兌業務及其他銀行服務業；證券交易所、證券櫃檯買賣中心、證券商、證券投資信託事業、證券金融事業、證券投資顧問事業、證券集中保管事業、都市更新投資信託事業及其他證券服務業；期貨交易所、期貨商、槓桿交易商、期貨信託事業、期貨顧問事業及其他期貨服務業；保險公司、保險合作社、保險代理人、保險經紀人、保險公證人、郵政機構之簡易人壽保險業務及其他保險服務業；以及電子金融交易業等在內者（金管會組織法第 2 條）。

[264] 個人資料保護法第 2 條第八款；中華民國法務部網站，〈個人資料保護法非公務機關之中央目的事業主管機關列表〉，https://www.moj.gov.tw/cp-793-47377-1acb3-001.html（最後瀏覽日：01/06/2020）。

doi:10.6342/NTU202000744

[265]，均應遵循該法與相關金融業法之規定；後者則係金融消費者對抗金融機構不法蒐集、處理、傳遞、利用及揭露其個人資料之自主性權利，且金融機構同時負有維護個人資料安全之義務，即須採取適當之安全措施防止其所取得之資料遭竊取、竄改、毀損、滅失或洩露等[266]。準此，董事會與管理階層應評估銀行內部各業務單位涉及個人資料蒐集、處理、利用之流程所可能產生之個人資料風險，並根據評估結果訂定與實施適當之個人資料管理程序與措施，以及個人資料之安全稽核、紀錄保存及持續改善機制，並應將前述相關機制納入內控制度與稽核項目[267]。抑且，法律亦明文規定，金融機構對於金融消費者或其本身就個人資料保護方面，應履行保密、告知、揭露、確保安全及申報與通報等義務。準此，倘金融機構未能確實遵循各該金融業法所規定之諸項個人資料保護相關之責任與義務，即屬未落實執行內控制度之缺失，得由金管會作成行政處分課予罰鍰等行政處罰[268]。

（二）資訊系統安全——世界經濟論壇（World Economic Form）發布之「2020年全球風險報告」指出，數據資料之詐欺或竊盜（Data fraud or theft）、網路攻擊（Cyberattacks）、資訊基礎設施故障（Information infrastructure breakdown）等在內

[265] 所謂個人資料指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務狀況、社會活動及其他得以直接或間接方式識別該個人之資料，例如金融消費者買賣有價證券之融資融券交易資料，即係關於財務狀況之個人資料（個人資料保護法第 2 條第一款）。再者，倘金融機構係透過系統建立而得以自動化機器或其他非自動化方式檢索、整理者，亦屬之（個人資料保護法第 2 條第二款）。

[266] 王志誠（2017），《現代金融法》，三版，頁 275，臺北市：新學林；個人資料保護法第 27 條第一項。

[267] 金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法第 5 條、第 13 條。依據「個人資料保護法非公務機關之中央目的事業主管機關」列表，金管會係存款機構、金融控股業、票券金融業、證券金融業、人身保險業、財產保險業等金融機構之中央目的事業主管機關，故其考量諸等金融業者保有大量且重要之個人資料檔案，所負之安全維護責任應較一般行業為重，即依個人資料保護法第 27 條第二項、第三項之授權規定訂定「金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法」，要求該等金融機構須訂定個人資料檔案安全維護計畫與業務終止後個人資料處理方法，以加強管理與確保金融消費者個人資料安全之維護（金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法總說明）。

[268] 個人資料保護法第 25 條第一項、第 47 條至第 49 條。例如中國信託商業銀行辦理網路銀行業務時，將網站索引檔案上傳予網路搜尋引擎業者，惟其內部對於網站索引檔案產出程式之設計未臻嚴謹，對相關檔案驗證方法與程序亦有欠周延，未對內部目錄網頁之讀取權限作嚴謹控管，致使一般網路使用者均能進入並瀏覽其內部目錄網頁所留存之客戶資料，且亦未能有效發現外部人士瀏覽內部網頁之情形，造成客戶個人資料外洩，核有為落實執行內控制度之缺失，違反銀行法第 45 條之 1 第一項規定，依同法第 129 條第七款規定，核處新臺幣 400 萬元罰鍰（102 年 8 月 22 日金管銀控字第 10200181601 號處分）。

doi:10.6342/NTU202000744

之科技風險已為環境風險外，「最可能發生」且「衝擊影響最大」之風險議題[269]。故鑑於銀行、證券商等金融機構係屬「關鍵基礎設施」（critical infrastructure）提供者[270]，其所具備或建置之實體或虛擬資產、系統或網路之功能一旦停止運作或效能降低，對於國民生活、經濟活動、公眾利益或國家安全將有重大影響之虞[271]，金管會即依職權要求金融機構應訂定與實施資通安全維護計畫[272]，且各金融機構並應定期向金管會提出前開計畫之實施情形[273]，同時應接受金管會擇定辦理資通安全計畫實施情形之現場實地稽核[274]。再者，除了上述銀行就其執行業務所需而取得之個人資料，應建置個人資料檔案之管理程序、措施及安全稽核機制外，有鑒於銀行之現代金融商品交易型態愈趨複雜與多元、電子或網路服務內容亦不斷提升等產業特性，從而本身即蒐集、處理及利用可謂鉅量之資訊（流）。因此，銀行與金控公司基於法令規範或補充性行政函釋，於內部建置「利害關係人資料庫」[275]、「子公司業務及客戶資料庫」[276]，或取得同一關係人之授信資料[277]等各式交易資訊，均凸顯銀行除了掌握大量資訊之外，其內部資訊儲存與揭露之載體並不再僅侷限於紙質或書面，而係逐漸擴展於資訊系統、網路或數位載體。

基此，在金融結合科技之發展趨勢下，銀行應如何避免相應而生之駭客攻擊、網路金融詐騙、資料外洩、電腦系統病毒等「資訊安全風險」[278]，據以避免違反現行法令規範或與客戶間之契約條款，亦屬內控制度之法令遵循發展趨勢。鑑於近年

---

269 WORLD ECON. FORUM [WEF], THE GLOBAL RISKS REPORT 2020 fig.II (15th ed. 2020).

270 行政院國土安全政策會報「國家關鍵基礎設施安全防護指導綱要」附件一、國家關鍵基礎設施領域分類（107 年 7 月 30 日訂正），https://ohs.ey.gov.tw/File/79A79307409FF32C。

271 資通安全管理法第 3 條第七、八款。

272 金融監督管理委員會所管特定非公務機關資通安全管理作業辦法第 3 條、第 4 條。「資通安全維護計畫」之內容應包括資通安全政策與目標、機構內部推動資通安全事務之單位或組織、專責單位之人力與經費等資源之配置、資訊與資通系統之盤點與標示核心資通系統與相關資產、資通安全風險評估、資通安全防護與控制措施、資通安全事件通報、應變及演練相關機制、資通安全情資之評估及因應機制、資通安全維護計畫與實施情形之持續精進及績效管理機制等項目（資通安全管理法施行細則第 6 條第一項）。

273 金融監督管理委員會所管特定非公務機關資通安全管理作業辦法第 5 條。

274 金融監督管理委員會所管特定非公務機關資通安全管理作業辦法第三章。

275 銀行法第 32 條、第 33 條；金融控股公司法第 44 條、第 45 條；財政部 82 年 7 月 12 日台財融字第 821165024 號函、金管會 99 年 9 月 28 日金管銀法字第 09910004570 號函。

276 金融控股公司法第 36 條第一項、第 42 條、第 46 條、第 55 條及第 56 條；金融控股公司法第 46 條申報與揭露辦法第 2 條；金管會 93 年 9 月 13 日金管銀（一）字第 0938011562 號令。

277 銀行法第 33 條之 3；銀行法第 33 條之 3 授權規定事項辦法。

278 王志誠（2017），《互聯網金融之監理機制》，頁 132-133，臺北市：新學林。

doi:10.6342/NTU202000744

金融機構之服務方式已由傳統臨櫃作業轉為數位線上分散處理，惟有遭駭客以植入惡意程式控制自動櫃員機（ATM）循非正常程序盜領現金[279]或進行分散式阻斷服務攻擊（DDoS）[280]，導致地區分行網路連線中斷、遭惡意攻擊端點增多、受害稽核軌跡留存不周全等金融資安事件頻繁發生，資訊安全之內控制度即逐漸受到重視[281]。申言之，銀行內部資訊安全專責單位應負責建置與運作「資安三道防線」，以之確保資訊安全計畫與防護工作之有效執行：第一道防線係由各資訊部門配合執行資訊安全工作，例如網路管理單位負責網路安全、程式與系統開發單位負責程式碼安全；第二道防線則為資安專責單位，由其負責評估銀行之資安風險、制訂銀行整體資安政策與程序，並應確保各單位妥適執行；第三道防線即由內部稽核與外部審計共同檢視其成效。

（三）反賄賂（反貪腐與反舞弊）——最後一項值得關注之法令遵循發展趨勢則係與銀行創造信用之功能或誠信經營相關之「反賄賂（Anti-Bribery）」管理機制。申言之，過往跨國企業為取得海外貿易地之經營優勢或換取各類商業利益，均會將賄賂當地政府官員視為「入境隨俗」之表現[282]。惟自二十世紀晚期以降該風氣則日漸猖獗，加以美國公司爆發層出不窮之弊案，美國國會即認知企業行賄外國政府之行為除係違反道德觀念外，亦將阻礙經濟發展，更使其於拓展國際外交關係時遭逢諸多困難[283]。準此，美國國會即於 1977 年制定通過「海外反貪腐法」（Foreign Corrupt Practices Act，FCPA），該法不僅係為達成遏止企業之貪污犯罪、強化財務公開及重塑外交關係等目的[284]，其更逐漸提高全球反貪腐之風潮，同時增強跨國企業對於各國之法令遵循、企業法律風險管理及公司治理等方面之重視，以謹慎追求誠信企

[279] 105 年 9 月 12 日金管銀控字第 10560003721 號處分。

[280] 金管會網站（02/03/2017），〈新聞稿：證券商近期遭網路攻擊事件之說明〉，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201702030004&toolsflag=Y&dtable=News。

[281] 為此，金管會要求銀行、金控公司、保險業等金融機構內部應設置獨立之資訊安全專責單位及主管（Chief Information Security Officer，CISO）負責規劃、監控及執行資訊安全管理作業，以提升金融業對於資訊安全防護能力之重視（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 條之 1）。

[282] *See* JULIE R. O'SULLIVAN, FEDERAL WHITE COLLAR CRIME: CASES AND MATERIALS 538 (2012); 林志潔（2015），〈反制跨國行賄與強化企業法令遵循——以美國海外反貪腐法（FCPA）為例〉，《月旦法學雜誌》，242 期，頁 6-7。

[283] O'SULLIVAN, *supra* note 282.

[284] 15 U.S.C. §§ 78dd-1-3.

doi:10.6342/NTU202000744

業、廉潔經商之理念[285]。再者，有鑒「聯合國反貪腐公約施行法」已於 2015 年 5 月 20 日經總統令公布，並於同年 12 月 9 日生效施行，故該公約之規定即具有國內法之效力[286]。該公約第 12 條即揭示締約國應依據其法律基本原則，對於私部門（private sector）採取加強會計與審計之標準，抑或制定有效、適度且具警惕性質之民事、刑事或行政處罰等措施，以防止私部門涉及貪腐[287]，包括訂定維護商業活動良好操守之標準與程序、識別設立與管理公司之自然人或法人身分以提升公司透明度之措施、防止公職人員任職於私人企業存在利益衝突之合理適當限制、以及確保私人企業依其結構與規模訂定並實施有助於預防與發現貪腐行為之充分的內部稽核控制[288]。「國際標準組織」（International Organization for Standardization，以下簡稱 ISO）即據此發布「ISO 37001 反賄賂管理機制（Anti-Bribery Management Systems，以下簡稱 ABMS）」，以作為國際間實施或加強反賄賂管理系統與內部控制，以及建立企業誠信經營文化之認證標準[289]。質言之，ABMS 係於組織內部建立包括由董事會與高階管理階層訂定之政策與作業程序所組成之反賄賂管理系統，並透過反賄賂遵循專責單位或人員運作該系統，藉以控管反賄賂之風險、達成組織營運或策略等目標[290]。

臺灣證券交易所為協助上市與上櫃公司建立誠信經營之企業文化與健全其發展、提供良好商業運作之參考架構所訂定之「上市上櫃公司誠信經營守則」，即作為金融機構實施與優化有助於其預防或發現賄賂、貪腐或舞弊等風險之內控制度之重要標準。申言之，為塑造永續發展之經營環境，該守則首先要求董事會本於廉

---

[285] 林志潔，前揭註 282，頁 23-24。

[286] 聯合國反貪腐公約施行法第 2 條第一項。

[287] United Nations Convention Against Corruption art. 12, G.A. Res. 58/4, annex (Oct. 13, 2003):

> Each State Party shall take measures, in accordance with the fundamental principles of its domestic law, to prevent corruption involving the private sector, enhance accounting and auditing standards in the private sector and, where appropriate, provide effective, proportionate and dissuasive civil, administrative or criminal penalties for failure to comply with such measures.

[288] *Id.*

[289] *Popular Standards: ISO 37001 Anti-Bribery Management Systems*, INT'L ORG. FOR STANDARDIZATION (ISO), https://www.iso.org/iso-37001-anti-bribery-management.html (last visited Jan. 7, 2020).

[290] *See ISO 37001:2016(en): Anti-Bribery Management Systems — Requirements with Guidance for Use*, INT'L ORG. FOR STANDARDIZATION (ISO), https://www.iso.org/obp/ui#iso:std:iso:37001:ed-1:v1:en:term:3.11 (last visited Jan. 7, 2020).

doi:10.6342/NTU202000744

潔、透明及負責之經營理念，制定以誠信為基礎之政策與建立良好之公司治理與風險控管機制[291]，並應時刻於金融機構內部傳達誠信之重要性[292]。同時，金融機構內部應設置隸屬於董事會之專責單位，並由董事會聘用適任人員與配置充足資源，負責誠信經營政策與不誠信行為風險防範方案[293]之訂定與監督執行，其應定期向董事會報告[294]。基於法令遵循係作為落實誠信經營之基本前提，上市上櫃公司及其董事、監察人、經理人、受僱人、受任人或具有實質控制能力者於執行業務時，均應遵循公司法、證券交易法、政治獻金法、貪污治罪條例、政府採購法等商業行為相關法令、規章及防範方案[295]。此外，為能有效達成董事會之誠信經營政策，金融機構內部除了應訂定具體作業程序與行為指南，作為內部人執行業務時之參考外[296]，亦應定期舉辦員工教育訓練、宣導及績效考核，使全體員工均能充分瞭解各項法令規範與內部作業程序[297]。最後，就誠信經營專責單位評估與分析之不誠信行為風險發生率較高之營業活動，董事會應與高階管理階層共同建立有效之會計制度與內控制度，並應由內部稽核單位定期查核防範方案與內控制度之執行情形[298]，抑且前揭各項政策、程序、制度等規範均應隨時檢討或修正改進，據以提升金融機構誠信經營之落實成效[299]。除此之外，金融機構推動誠信經營之量化數據、採行情形及推動成效等資訊，則均須於其網站、公開資訊觀測站、年報及公開說明書等處詳實且充分揭露相關內容[300]。

由是觀之，反賄賂管理機制之本質亦係建立於「風險基礎方法（Risk Based Approach，RBA）」之內控制度，意即透過瞭解銀行內部各項業務活動，辨識與評估賄賂風險、訂定賄賂風險控管作業程序與措施、定期執行有效性查核與持續改善

[291] 上市上櫃公司誠信經營守則第 5 條。
[292] 上市上櫃公司誠信經營守則第 22 條第一項。
[293] 上市上櫃公司誠信經營守則第 7 條。防範方案係為控管不誠信行為風險所訂定之措施，所謂不誠信行為包括行賄、收賄、提供非法政治獻金、不當慈善捐贈、提供或收受不正當利益、侵害營業秘密或智慧財產權、從事不公平競爭行為、產品或研發損害消費者之權益、健康及安全（上市上櫃公司誠信經營守則第 10 至 16 條）。
[294] 上市上櫃公司誠信經營守則第 17 條第二項。
[295] 上市上櫃公司誠信經營守則第 4 條、第 18 條。
[296] 上市上櫃公司誠信經營守則第 21 條。
[297] 上市上櫃公司誠信經營守則第 22 條第二、三項。
[298] 上市上櫃公司誠信經營守則第 20 條。
[299] 上市上櫃公司誠信經營守則第 26 條。
[300] 上市上櫃公司誠信經營守則第 25 條。

doi:10.6342/NTU202000744

方案內容，最終達成風險管理與法令遵循之目標。基此，縱使前揭上市上櫃公司誠信經營守則尚非屬法律層級之制度規範，惟鑑於反賄賂、反舞弊或反貪腐等議題日漸受重視，或謂「誠信」、「廉潔」實係銀行等金融機構經營之重要核心原則，不可不慎，其未來發展應值得觀察。

第六節　小結——內控制度之本文分析

第一項 內部控制 GRC 整合架構

綜合第二章與本章之觀察與分析後，本文認為「內控制度」係促進金融機構公司治理、風險管理及法令遵循（Governance, Risk Management, and Compliance，GRC）等三種機制或功能順利運作之基礎系統架構。抑且，公司治理、風險管理及法令遵循等三者機能或目標並非各自獨立，唯有三者共同運作，方能達成確保金融機構之管理階層得有效經營、降低風險發生，同時兼顧社會福利提升與永續經營等目標[301]。本文續以銀行為例說明之。

由於銀行日常業務活動涉及各項內生或外來之風險，具體或為信用風險、市場風險、作業風險、流動性風險、策略風險、利率風險、信譽風險、外匯風險、科技風險、主權或國家風險、破產風險[302]及法律風險等，為有效控制與管理風險胃納、達成營運獲利之目標，內控制度存在之目的即係協助金融機構辨識、評估、控管及追蹤前述各項風險。再者，伴隨金融科技之發展，銀行所能提供之金融商品或服務愈發多元、部門組織分工漸趨細緻，網路銀行與數位化之運作亦打破時空限制，使內部單位間亟需橫向整合架構作為風險管理之運作基礎，避免不同部門各自為政、無法有效控管風險。除此之外，銀行作為受制高度行政監管之金融服務業，無論係設立或各項業務之經營，其所須遵循之法令規範體系既龐雜且細緻，為全面檢視與盤點各項法規，並具體落實又不至於與內部各項不同業務之順暢執行產生扞格或影響業務之發展，以及避免因違反法令規範而招致主管機關裁罰等法令遵循風險發生，內控制度與相關標準作業程序之合理訂定與有效運作，亦與達成風險管理、營運目標等息息相關。

---

[301] *See* ADOLF A. BERLE & GARDINER C. MEANS, THE MODERN CORPORATION AND PRIVATE PROPERTY (1932).

[302] ANTHONY SAUNDERS & MARICA MILLON CORNETT, FINANCIAL INSTITUTIONS MANAGEMENT: A RISK MANAGEMENT APPROACH 181-82 (7th ed. 2011).

doi:10.6342/NTU202000744

一言以敝之，銀行之業務經營應不得凌駕於風險之上、提供之金融商品或服務不得逾越於法令規範之上。因此本文認為，「內部控制」即係銀行之董事會與高階管理階層為限縮與控制內部各業務單位或部門於營運過程中，所可能面臨之各項風險，並藉以達成法令遵循目標所設計之政策與作業程序[303]。惟具體操作上，由於內部控制不僅是銀行內部訂定之作業程序，除了「三道防線」之建置與運作以外，為能有效發揮「內控制度」達成銀行之業務經營、風險管理、法令遵循、稽核審計，乃至洗錢防制與資恐打擊、個人資料保護、資訊系統安全、反賄賂等各項目標或功能，同時促進不同附屬單位間之聯繫，即應於現有之內控制度中，導入 GRC 概念，根本性地落實內部控制之基礎建設與系統架構整合。換言之，金融機構內部應建立完善且有效之內控制度，方得達成保障資產安全與營運獲利等目標，並進而使金融機構出具可靠、及時且透明之財務與非財務性報導。準此，倘若金融機構之董事會與高階管理階層之經營理念在於追求長遠營利目的、承諾永續發展，則如何針對其產業特性與企業文化，設計一套有效之內控制度並落實執行，是為公司之經營管理階層於執行日常業務程序以外，亟須重視之環節。

第二項 控制程序之 PDCA 循環

奠基於上揭內部控制 GRC 整合架構，本文認為現行金融機構之內控制度相關法令規範對於內控制度仍停留於「靜態制度」之想像與觀察角度，實則內控制度應為不斷變化之「動態程序」，方能真正達成其「控制」功能。換言之，內控制度之實施係為經由對於金融機構內部各項經營與管理作業之不斷檢驗，以察覺與組織政策或既定目標、作業程序或其他預期標準乖離之事實，將其透過內控制度之監控與回饋系統，適當反映於管理階層，並針對現有之問題或未來可能所生之風險採取必要之修正或改善措施，同時藉由內控制度之內部牽制原則與手段達勾稽之目的，以防止作業弊端或風險之發生，據此確保金融機構得依循董事會與高階管理階層所規劃之政策或目標方向運行[304]。準此，以下本文將依循前述就內控制度之觀察與研究，初步解構內控制度之基本型態與流程，據此嘗試將「PDCA 循環」具體應用於現行內控制度，作為本文提出建置良好有效運作之內控制度之芻議。

質言之，為有效達成經營之效果與效率、多樣化資訊揭露之即時與正確性，以

303 *See* FFIEC BSA/AML EXAMINATION MANUAL, *supra* note 252, at 29.

304 中華民國期貨業商業同業公會期貨信託事業內部控制制度標準規範第 1 條第九款。

doi:10.6342/NTU202000744

及遵循法令規範等目標，或謂為使管理階層能有效掌握轄下個別業務單位職員之行為，避免異常、錯誤或舞弊等風險之發生，多數金融機構等組織內部均依其組織規模、經營模式、企業文化或業務型態，訂有所謂「標準作業流程」（Standard Operating Procedure，SOP）。內控制度即係環環相扣於不同部門、各項作業程序之總和，故其實係攏絡組織運作與經營之各種面向。至於各項作業程序（或稱內控程序）訂定之標準或依據，則包括：董事會與管理階層所訂定之經營政策、績效目標及風險胃納、外部具強制性法令規範或組織章程、個別業務執行程序與作業方法、特定業務運作過程中可能發生之風險來源等，換言之，建置內控制度之前提步驟為盤點與確認各項政策目標、法規、業務內容及風險等，並以之作為設計內控程序之要件。然而誠如本文於前所述，現代金融機構無論係經營型態、業務種類或提供之商品或服務等呈現多元且多變之姿，造成風險之種類態樣瞬息萬變、外部監管法規不斷推陳出新或修正變遷。是故，為提升內控制度之嚴謹與可靠、得以即時且有效地因應業務內容、風險及法令規範之快速更迭，應於各項內控程序注入彈性調整與修正之動能，即「PDCA 循環」，使其能符合現時環境之需求。

由精研企業管理領域之品質管理（quality management）之美國學者愛德華茲·戴明（Edwards Deming）於 1950 年提出，且至今仍為日本豐田汽車公司（Toyota）採用，作為公司內部強化品質管理與有效解決問題之核心概念[305]，「PDCA 循環（Cycle）」、又稱「戴明環」，係指透過規劃（Plan）、執行（Do）、查核（Check）及行動（Action）等四道步驟之交互運作，確保產品之製造程序、標準及品質等均得持續且有效地改善，同時提升執行者之智識與職能，達成較為長遠之經營與績效目標[306]。簡言之，PDCA 循環運作目的在於藉由反復、持續地修正與改進，以優化組織內部各項作業或製造「程序」（process），確保其所提供或製造之產品、服務之內容得不斷拉高其依循標準[307]，除了維持應有之品質與達成既定之目標外，理想上更在於協助組織整體運作達成終極之完美狀態。準此，鑑於銀行內部個別業務部門與專責單位訂定內控程序之標準——即風險與法令規範，例如科技風險、資訊安全

[305] *See* DURWARD K. SOBEK II & ART SMALLEY, UNDERSTANDING A3 THINKING: A CRITICAL COMPONENT OF TOYOTA'S PDCA MANAGEMENT SYSTEM 3-4 (2008).

[306] *See* RAFAEL AGUAYO, DR. DEMING: THE AMERICAN WHO TAUGHT THE JAPANESE ABOUT QUALITY 114-15 (1990).

[307] Rr. Sri Kartikowati, *The Technique of "Plan Do Check and Act" to Improve Trainee Teacher's Skills*, 9(12) ASIAN SOC. SCI. 268, 270 (2013).

doi:10.6342/NTU202000744

風險等新型態之風險，又或洗錢防制與資恐打擊、個人資料保護、反貪腐等各式金融法令之要求，均係不斷變化或新增，故個別執行之內控程序與整體之內控制度應如何即時、動態調整以符合商業運作之需求、達成營運、報導及遵循等內控制度目標，即有賴於 PDCA 循環方法論之運用。

換言之，吾等倘若將內控制度中各項「控制程序」視為金融機構用以製造、提供良好金融產品或服務之程序，則應如何透過納入「PDCA 循環」，逐步漸次提升與優化該「程序」之品質與執行成效，或得謂係有效改善現行內控制度運作失靈、不甚健全等情形之可能解方。至於具體作法，本文參考由 ISO 所發布之品質管理系統與能源管理系統管理之架構與步驟[308]，作為以下實際操作、應用於金融機構之基礎。

第一款 規劃（Plan）

作為金融機構建置有效良好之內控制度系統之重要基礎步驟，董事會與高階管理階層正式訂定金融機構之經營方針與建置內控制度前，須先行確認各項內控程序運作之邊界範圍與權責分配，俾能對各業務單位之經營活動與績效訂定明確且有效之目標。同時掌握政策與程序實施過程中，各項可能發生之風險與待改善之處，以利於持續針對問題提出修正與解決方法[309]。

第一目 前置作業安排

所謂前置作業包括組織邊界確定、管理權責界定及政策目標訂定等三部分。首先，實際建置一套內控制度前，董事會須先予確認並揭露該套控制系統適用之邊界與組織範圍，例如係適用於銀行整體、特定地區分行，抑或係特定業務單位或法令遵循部門等，同時瞭解該套控制系統可能涉及之人員與所需之資源，作為訂定相關政策與選任最高管理階層、界定管理權責之基礎。再者，董事會應明確劃定各業務單位或部門之管理權責，意即派任並賦予高階管理階層足夠之權限與所需之資源，使其得依職權組織管理團隊，共同帶領其所負責之業務單位執行日常業務與運作

[308] *Popular Standards: ISO 9000 Family — Quality Management*, INT'L ORG. FOR STANDARDIZATION (ISO), https://www.iso.org/iso-9001-quality-management.html (last visited Jan. 8, 2020); *Popular Standards: ISO 5001 Energy Management*, INT'L ORG. FOR STANDARDIZATION (ISO), https://www.iso.org/iso-50001-energy-management.html (last visited Jan. 8, 2020).

[309] *See* SOBEK & SMALLEY, *supra* note 305, at 4.

doi:10.6342/NTU202000744

內控制度，且對於該業務單位之績效或行為表現承擔管理與監督之責任。此外，為能提供銀行整體一明確之行動框架、以及內部各業務單位或部門訂定其內部作業控制程序時所得依循之最高指導原則、同時亦激勵全體職員確實遵循內部治理政策與規範，董事會應與高階管理階層共同擬定管理與經營政策作為正式聲明，以此向內部所有成員宣示其推行良好公司治理之決心。政策內容得包括組織營運之具體目標、提供達成組織目標之具體架構、致力於推動內控制度與其他內部治理程序之承諾、積極推動持續改善計畫與策略、確保充足之資源與資訊文件之取得、定期提供相關教育訓練、強化組織內部各階層之有效溝通等，均在於彰顯董事會與高階管理階層對於持續推動並改善治理架構與制度之正面態度，以形塑內部良好之組織與治理文化。

第二目　內控制度規劃

奠基於上揭由董事會主導訂定之治理政策與架構，高階管理階層與銀行內部各業務單位之管理階層即須據此規劃、實施與該政策內容一致之內控制度，包括業務作業流程風險評估與持續監控、改善內部控制活動之機制。為確保內控制度之訂定係符合金融監管要求，銀行法令遵循專責單位須負責執行法規鑑別，事先就銀行經營相關所有法規與契約條款等內容予以綜覽與盤點，並剔除無關法規，作為銀行建置內控制度之重要標準。此外，風險管理專責單位須負責就銀行整體與內部各項業務之主要風險類別進行辨識與評估，尤須確認可能產生重大風險之業務活動、程序、負責人員及單位。各項風險相關數據與資訊除係用以作為訂定風險管理政策之指標外，亦係所有管理階層訂定單位內部作業流程與控制程序之重要依據。

職是故，內控制度或謂係銀行內部各項業務執行之行動準則，其規劃與訂定須能有效控管與預防營運過程中可能發生之各種風險，同時符合現行相關法令之規定，據以達成營運以外，包括風險管理與法令遵循在內等政策與目標。再者，為有效落實或激勵銀行內部所有成員共同遵循或達成由董事會擘劃之政策內容，以及上揭作業程序與內控制度，董事會與管理階層應依據政策願景與可行性，於銀行內部訂定內控制度之落實目標與績效指標。最後，無論政策願景、管理權責分配、作業流程與控制程序、各項目標與績效指標諸等內控制度規劃相關內容，均應予文件化。所謂「文件化」得以書面、電子或任何其他媒介或載體為之，其目的在於明確敘述內控制度之具體內容，並將所有文件與資訊予以記錄、保存，俾供銀行內部所

doi:10.6342/NTU202000744

有成員參照遵循，同時得定期檢視與調整。

第二款 執行（Do）

待內控制度相關政策與程序訂定完畢後，即須於銀行內部具體實施運作，或謂執行階段，包括教育訓練、溝通及管制等三部分。首先，銀行之人力資源部門應與董事會、高階管理階層、風險管理部門、法令遵循部門及內部所有業務單位共同協作，由其負責於銀行內部提供適當、適時之教育訓練，確保所有職員均能掌握內控制度所有作業程序規定，以及各自於內部控制程序中扮演之角色、責任及職權。再者，為確保管理階層得隨時掌握內控制度之運作狀況，抑或個別業務單位之職員執行內控制度時所面臨之疑慮或障礙等可即時獲得釋疑或有效解決，銀行內部應建置通暢之溝通管道，用以對內或對外傳遞各項意見或建議等資訊。此外，各業務單位應自行鑑別與規劃內部控制相關之運作與維護活動，確保內部業務或作業活動內容與前揭政策、目標及行動準則之一致性，是為作業管制。質言之，除了內部作業控制程序以外，業務單位之管理階層須設定並建立使該控制程序得有效運作與維持之行為準則，避免職員之恣意行為導致內控制度之有效性產生重大偏離。

第三款 查核（Check）

為確保內控制度有效且持續運作以達成政策與相關目標，銀行內部應有內控制度之查核機制，定期或隨時檢查、監督及分析內控制度之執行情形。詳言之，查核之目的在於檢視現行內控制度是否得以落實董事會訂定之政策與目標，抑或有效為風險管理、業務之執行是否均符合現行法令規範等，或謂辨識已經存在與具有發生之潛在可能性之問題或風險，以及該等情形之發生對於內控制度之執行績效產生不良後果之嚴重程度。倘若根據查核與分析之結果顯示，現行內控制度或其他相關行為規範準則等容有調整與改進之處，包括相關業務單位之管理階層與銀行高階管理階層、董事會等在內者，則須就查核結果，決定採取矯正或預防等適宜措施，對於現行內部機制即時為必要之修正。再者，無論該查核機制係由各業務單位之管理階層、內部稽核、外部審計或其他具備專業智識、客觀且公正之第三方所為，所有查核結果應建立與維持易於閱讀、可識別及可追溯相關業務活動之紀錄，俾利董事會與高階管理階層得鑑別與檢索相關查核資訊，作為日後訂定管理政策與目標之參考。

doi:10.6342/NTU202000744

第四款 行動（Action）

依據上揭內控制度之查核內容，以及事關業務單位據以進行必要調整之成效等結果，高階管理階層與董事會應進行管理審查，確保內控制度之建置與內容得持續適用、適切及有效運作。誠如前述，內控制度係由所有作業或製造程序組成者，且 PDCA 循環運作目的則在於持續與反覆修正、優化各項內控程序，故在此階段，銀行內部負責監督與管理之職務者，須檢視現行之內控制度得否充分落實董事會訂定之政策內容與目標。質言之，倘若依據查核結果與矯正改善措施執行之結果顯示，現有內控制度仍有瑕疵存在或尚無法有效達成政策與目標，董事會與高階管理階層則須提出政策與目標之變更、具體之改善建議等，作為下一階段訂定或調整政策與目標之依據；惟若現有或部分內控程序係運作良好者，則得由董事會與高階管理階層援引作為銀行內部訂定內控制度之標準。綜言之，「行動」作為 PDCA 循環之最終階段，其目的在於充分檢視內控制度與相關政策、目標之執行結果，並根據所有查核結果提出有效改善或解決方法，以為董事會與高階管理階層後續更新與修正內控制度之依歸，最終目的在於確保內控制度呈現持續改善之動作狀態，藉此展現該制度之績效。

第三項 內控制度之先天限制因素

基於上述內控制度發展脈絡之介紹可知，內控制度多僅能「合理確保」銀行與金控公司等金融機構達成營運、報導及法令遵循等三大主要目標，尚無法保證金融機構內部建置內控制度後，即可百分之百達成預期之效果，此係內控制度就其本質仍屬內部管理流程之不得不然。換言之，健全之內控制度運作至極致僅能減少、尚無法完全消除制度本身之闕漏或人為因素對於內控制度所生之負面影響[310]。關於內控制度之先天限制因素，本文認為可分別從人為影響與成本效益觀點等兩方面觀察。

詳言之，內控制度本身因具有若干先天性限制，造成無論內控制度建置與運作之有效程度如何，其至多僅能對於相關目標之達成，提供合理確信。人為因素相關之諸等限制包括：一、制度設計須考量其成本與效益，且將造成內控制度之設計，

[310] *See* FIN. REPORTING COUNCIL [FRC], INTERNAL CONTROL: REVISED GUIDANCE FOR DIRECTORS ON THE COMBINED CODE ¶¶ 22 (2005) [hereinafter THE TURNBULL GUIDANCE 2005].

doi:10.6342/NTU202000744

通常僅能針對預定或一般之交易事項，並未考慮特殊之交易事項；二、因外在情況改變，導致原先設計之控制程序無法順勢因應[311]；三、無法完全排除於決策制定過程中，人為之疏忽、判斷錯誤或誤解[312]，抑或相關人員未採取適當行動或措施以因應前揭之疏漏等人為所造成之因素[313]；四、內控制度無法完全排除兩人以上共謀或串通舞弊，或管理階層踰越內部控制程序、濫權或監督不周，以致其失效之可能性[314]；五、管理階層於設計控制程序，以及將其付諸實行時，若未具備足夠能力對其所選擇之控制與所選擇承擔之風險二者之性質與範圍作成準確判斷，亦將影響內控制度之實效[315]；六、內控制度之遵行或恐有因日久而鬆懈之可能[316]。職是故，內控制度之設計上因具有上開諸等限制，致使內控制度僅能協助銀行或金融機構獲取所需之必要資訊，同時指出錯誤或缺失，據以達成原先制度設計時所預期之營運目標。惟尚無法保證必然成功，例如並非所有缺失或風險均能被全面有效預防或即時偵測，或完全杜絕問題之發生[317]。

再者，內控制度之建置與運作尚須盱衡成本與效益（cost/benefit tradeoffs），此係前述判斷偏誤、控制程序故障、管理階層踰越及舞弊等人為因素以外，致使內控制度最終落實僅能提供「合理保證」並非「絕對保證」達成各項目標之限制因素，亦即若投注過量成本致累積過多的控制活動，其效果恐漸趨有限甚或造成預期效益逐漸遞減[318]。換言之，衡量內控制度之成本與效益不應僅就可量化之數據資訊為判斷標準，尚應考量前述諸項人為等無法量化之質性因素[319]。再者，不同組織規模或型態之公司建置內控制度所需之成本有別，且內控制度係運作於充斥各種不確定因素之商業環境，業務執行或管理過程中出現的各項變數，均將直接或間接地對

311 審計準則公報第二十三號「內部控制之考量」第 15 條（已廢止）。

312 *See* THE TURNBULL GUIDANCE 2005, *supra* note 310, ¶ 22.

313 *AU 319: Consideration of Internal Control in a Financial Statement Audit*, PUB. CO. ACCT. OVERSIGHT BD. [PCAOB], https://pcaobus.org/Standards/Archived/Pages/AU319.aspx#ps-pcaob_0b41793f-1d94-4a6f-8a01-8e483324399e (last visited June 3, 2019) [hereinafter *AU 319*]; 審計準則公報第四十八號「瞭解受查者及其環境以辨認並評估重大不實表達風險」第 75 條。

314 THE TURNBULL GUIDANCE 2005, *supra* note 310, ¶ 22; *AU 319*, *supra* note 313, ¶ 22; 審計準則公報第四十八號「瞭解受查者及其環境以辨認並評估重大不實表達風險」第 76 條。

315 審計準則公報第四十八號「瞭解受查者及其環境以辨認並評估重大不實表達風險」第 77 條。

316 審計準則公報第二十三號「內部控制之考量」第 15 條（已廢止）。

317 黃劭彥、陳俊志，前揭註 7，頁 58-59。

318 *See* STEVEN J. ROOT, BEYOND COSO: INTERNAL CONTROL TO ENHANCE CORPORATE GOVERNANCE 140, 141 fig.5.4 (1998).

319 吳琮璠（2009），《審計學：實務應用與法律觀點》，四版，頁 232，臺北市：吳琮璠。

doi:10.6342/NTU202000744

內控制度功能之有效性產生實質影響。惟縱採取自上而下（Top-Down）立法模式，強制要求公司應設置內控制度之法令規範，仍應考量制度本身之先天性限制或該限制將對內部控制之效能造成折損之可能[320]。因此即有論者建議，董事會與經營管理階層或得採取「3C 原則」作為內控制度設計與運作之權衡標準，意即綜合考量控制（control）、便利性（convenience）及成本（cost）等三項要素，作為判斷是否採行特定內控制度之依據[321]。

綜上所述，若欲使內控制度得有效發揮其制度目的與功能，吾等於制度之設計與實踐上，首應將前述內控制度本身之諸多先天性限制因素充分納入考量。此外，因內控制度本質上仍屬公司內部自發性、自主性之管理模式[322]，故本文認為，仍須重視人為因素對於內控制度之影響：經營階層對於公司治理目標之主觀態度與其是否具有誠信經營之理念[323]、管理階層是否具有足夠之誘因與工具，落實運作內控制度之責任、內部之監督或稽核單位是否具有足夠專業能力與權限以確實執行其對於管理階層之監督義務等。因此，唯有降低或消除人為相關之不利因素，抑或對於內控制度運作所生之人為負面影響，方屬內控制度於組織內部是否將受到所有成員之重視、以及是否能夠有效落實之重要關鍵。

320 廖大穎（2019），〈檢析法令遵循與我國公司治理之內部控制模式〉，台灣企業法律學會（編），《國際公司治理與企業法遵》，頁 125-126，臺北市：新學林。

321 吳琮璠，前揭註 319，頁 232-233。

322 廖大穎，前揭註 320，頁 125。

323 同前註，頁 125；林仁光（2004），〈論經營者誠信、內部控制、內部稽核制度與公司治理〉，《月旦法學雜誌》，106 期，頁 55。

doi:10.6342/NTU202000744

第四章 內控制度之人事組織

本章將延續前述內部控制之具體架構設計，探討金融機構內部應如何為合理之人事組織安排與權責分配，方能充分發揮內控制度之實效。銀行內部組織層級或稱其組成份子，依據各該成員之權限劃分，概為股東、利害關係人、董事會、經營管理階層，以及各業務單位之職員等。所謂銀行之股東，通常係指持有銀行已發行股份總數達百分之一以上之主要股東；且主要股東為自然人時，本人之配偶與其未成年子女之持股應計入本人之持股[1]。利害關係人主要包括有銀行之存款人、投資人及保戶等債權人。負責人則指依公司法或其他法律，或其組織章程所定應負責者[2]，原則上為銀行董事、監察人、總經理、副總經理、協理、總行經理、分行經理或與其職責相當之人等[3]，或謂係銀行內部之經營管理階層。再者，除了由董事長與全體董事所組成之董事會外[4]，銀行、金控公司、保險公司等金融機構內部尚有由獨立董事[5]所組成之審計委員會[6]、薪資報酬委員會[7]等其他功能性委員會。

基此，為明確釐清銀行內部董事會、經營管理階層、業務單位職員等組成員之權責範圍，俾使各人均能瞭解其在銀行整體風險與控制架構中所扮演之角色及其功能[8]，同時加強溝通協調，避免業務執行過程中發生作業相關之疏失或舞弊，以及預防風險，達成強健銀行經營之體質、權衡保障債權人與股東利益等目的，內部控制或謂係落實公司治理目標之管理過程[9]。再者，內控制度相關法令規範均開宗明義地指出，為促進銀行業之健全經營、完善其內部治理機制，董事會應考量銀行實際營運狀況，決議通過內控制度之建置並確保其有效運作[10]，故得認董事會係在內控制度扮演重要角色。

---

[1] 銀行法第 32 條第三項。

[2] 銀行法第 18 條。

[3] 公司法第 8 條第二項；銀行負責人應具備資格條件兼職限制及應遵行事項準則第 3 條之 1、第 3 條之 3、第 4 條、第 5 條及第 6 條。

[4] 公司法第 192 條第一項。

[5] 證券交易法第 14 條之 2；107 年 12 月 19 日金管證發字第 1070345233 號令。

[6] 證券交易法第 14 條之 4；107 年 12 月 19 日金管證發字第 10703452331 號令。

[7] 證券交易法第 14 條之 6；股票上市或於證券商營業處所買賣公司薪資報酬委員會設置及行使職權辦法第 2 條。

[8] 銀行內部控制三道防線實務守則第 2 條。

[9] *See* COMM. ON SPONSORING ORGS. OF TREADWAY COMMISSION [COSO], INTERNAL CONTROL—INTEGRATED FRAMEWORK 9 (1992).

[10] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條。

doi:10.6342/NTU202000744

若從銀行內部經營管理組織與內控制度「三道防線」架構觀察，實際執行日常業務，以及現狀下因未能遵循內控制度或法令規範而使金管會作成裁罰處分之行為人，通常係隸屬於內控制度第一道防線之人，或謂多係銀行「分行」之職員。惟董事會或高階管理階層等均係隸屬於「總機構」或「總行」之內控制度第三道防線監督管理單位，其面對內控制度第一道防線所生之風險與弊端，在此些對於董事會成員來說恐屬鞭長莫及之限制下，吾等應如何期待僅透過賦予董事會重要責任與加重其監督義務等方法，即可收即時且妥適地管理風險之效？抑且，誠如本文前章小結所指出，內控制度本質為公司治理機制下重要之內部自律機制，其運作之有效與否（或謂其先天限制）在於人為因素，意即銀行內部各該營業與業務單位須自發性地配合實踐，方能充分發揮內控制度應有之作用。職是之故，如何於銀行內部「由下而上」徹底落實內部控制之制度目的與精神，或如何提升各成員對於遵循與重視內控制度之誘因，方屬該制度有效達成良好金融機構公司治理之重要關鍵。

為求根本性地解決現行銀行內控制度之不彰與失靈等問題，本文認為不應僅頻頻將眼光聚焦於董事會、經理人等經營管理階層之人事責任或義務，就該「錯誤連結」（misconnection）造成無法遏止人為因素對內控制度所生之不利影響，似可換位思考與關注之事實係自始即失守之第一道防線，即分行或業務單位職員未能確實遵循內控制度所設程序與業務活動相關規範，將對於內部控制、風險管理及法令遵循等目標之成效造成極大耗損之事實。因此，本章內容在於經由內控制度實際執行層面之角度出發，從「組織層級」之角度觀察、檢視銀行內部之人事組織或其成員，其各自於內控制度中所應扮演之角色與權責、義務，調控人為因素對於內控制度之影響，期能達成充分、有效落實銀行內部控制制度機能之最終目的。

第一節　內控制度之兩種觀察視角

銀行內部最能發現或即時控管風險者，必然係業務執行單位，即內控制度之第一道防線，再者為法令遵循、風險管理等專責單位，最後則是董事會、稽核部門等獨立監督單位，故原則上獨立董事須仰賴內控制度偵查並防範弊端[11]。抑且，內控制度作為落實公司治理與營運、遵循等相關目標之管理過程，並非單純僅具備政策或程序之形式外觀，尚須金融機構內部各成員通力配合實施，方得有效發揮其制度

[11] 方嘉麟（2018），〈從永豐金案看獨立董事制度〉，《月旦法學雜誌》，272 期，頁 6。

doi:10.6342/NTU202000744

功能。惟若就內控制度本身於銀行內部治理架構之定位及其實際執行之成效而言，本文認為或可分別從內控制度之決策與執行兩層面觀察論斷。

第一項 Top-Down：決策層面

首先係內控制度之決策層面。依據銀行法、金融控股公司及銀行業內部控制及稽核制度實施辦法等法令之規定，銀行內控制度之決策流程概係由董事會決議通過[12]，且董事會應同時認知銀行營運時所面臨之風險，監督營運結果，並對於確保建立與維持適當有效之內控制度負有最終責任[13]。詳言之，與內控制度架構諸要素相關之董事與員工內部行為準則、風險評估程序、控制作業政策與程序、完整資訊取得機制、溝通管道及監督評估程序等程序與政策[14]，主要係由董事會、經理人等高階管理階層負責制訂或建立。然而，高階管理階層之定位主要係職司監督內控制度是否有效運作，故前述與銀行經營與風險管理相關之各項決策，仍須由銀行內部各業務單位職員於銀行內部予以具體落實，始竟其功。意即，內控制度應由董事會、管理階層及所有從業人員共同遵守執行，方能合理確保銀行得達成營運、報導及法令遵循等三大目標[15]。

第二項 Bottom-Up：執行層面

再者係內控制度之執行層面。依據前述相關法令之規定，董事會與經理人應擔負起建置與制定內控制度及其相關政策之責任，惟常言：「徒法不足以自行」，內控制度仍須經銀行內部各成員之行動配合，方能充分發揮該制度應有之作用。亦即，內控制度之實施並非僅屬於董事會、高階經理階層或任何特定單位或部門之責任，而在於銀行內部所有組成員持續不斷地推動與執行，始能竟其功。

質言之，內控制度運作或落實之起點為銀行內部所有業務經營單位，包括但不限於出納業務、存款匯兌業務、徵、授信業務、外匯業務、投資業務、信託業務、信用卡業務、保證業務、會計業務及資訊業務等[16]，故為預防或管理前述諸項業務

[12] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條。
[13] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1。
[14] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條。
[15] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條。
[16] 由於商業銀行係屬特許金融機構，故其得經營之業務內容限於銀行法所定之範圍，且須經中央主管機關（即金管會）核定或中央銀行之許可，始得經營（銀行法第 3 條、第 4 條及第 71 條）。

doi:10.6342/NTU202000744

營運活動所產生或可能發生之各項風險，確保營運活動與銀行經營目標與任務之一致，包括銀行之總機構（總行）與分支機構（分行）在內之所有業務單位，均應針對業務風險特性，設計並執行有效之內部控制程序，負責辨識與管理風險[17]。除就實施內控程序之各項內容辦理自我評估以外，各業務部門或單位尚應建立自行查核制度，以定期辦理一般自行查核與專案自行查核[18]，據此確認內控制度第一道防線之有效運作。抑且，銀行總機構應設置直接隸屬於董事會或總經理之法令遵循、風險管理及資訊安全等專責單位[19]，負責銀行內部整體風險控管，同時協助與監督第一道防線之執行情形，是為第二道防線。最後則係由內部稽核單位、外部審計人員、董事會及其功能性委員會（通常係審計委員會）所組成之第三道防線，負責查核與評估銀行內部所有內控制度與相關程序之有效性。

第三項 小結——基層業務至為關鍵

由此觀之，關於銀行內控制度基本架構與政策方向之擬定，縱謂係由董事會、經理人等高階管理階層負責規劃設計與建置，於銀行內部自上而下地形成一細緻之層級區分。惟就內控制度之具體落實與相關目標之達成而言，須由業務單位共同配合執行，或謂內控制度所欲控制之風險主要來源，抑或評估一家銀行之內控制度是否有效運作之指標，即係第一道防線之銀行職員之行為表現。然而，前揭本文所臚列金融機構內控制度相關裁罰案顯示，無論係銀行辦事員或理財專員挪用或私自盜領客戶款項等舞弊案件、抑或係交易員未依其所獲授權限額操作下單交易以致超逾策略部位、辦理貸款時因未落實徵、授信作業造成報告未充分揭露、高估鑑價金額及發生異常資金往來等情事，均凸顯了業務單位職員倘未能確實遵循內控制度所設程序與業務活動相關規範，將對於內部控制與風險管理之成效造成極大耗損之事實。準此，本文以下首先將試圖從第一道防線作業風險管理之角度，探討應如何從銀行內部根本、基礎性地落實內控制度應有之機能。

[17] 銀行內部控制三道防線實務守則第 7 條。

[18] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 25 條。

[19] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條、第 36 條及第 38 條之 1。

doi:10.6342/NTU202000744

第二節　業務單位

第一項 實務運作現況概述

初步觀察金管會作成之裁罰公告可略知，屬內控制度第一道防線之金融機構內部業務單位職員，其未能確實依循內部程序與遵守相關規範而致遭裁罰者——尤以銀行職員不當挪用客戶資產或資金等行為——無論係發生次數或裁罰金額實可謂層見疊出且長惡靡悛[20]。詳言之，銀行之前臺辦事員或理財專員[21]（以下簡稱理專）挪用客戶款項之行為態樣，概有下述類型[22]。第一，不當收受或使用客戶之物件：包括私自取得並留存客戶之存摺或印鑑，或客戶已簽名或蓋印之空白取款憑條或交易單據，抑或誘騙客戶交付前述物件[23]。第二，與客戶間有私人借貸關係、或私下有不當資金往來之情事[24]。第三，利用客戶未審慎查明或其不知情之情況下，擅自代理客戶進行交易：包括違反客戶指示，不當處分或侵占客戶財產等與客戶間有利益衝突之交易活動[25]。其他尚有：私下與客戶約定提供特定利益、對價或負擔

---

[20] 舉例言之，於 2019 年 7 月底，經客戶向銀行反映、或金管會實施金融檢查後經銀行自行查核、或離職銀行辦事員檢舉等原因，金管會發現共有高達七家銀行之理財專員或銀行辦事員涉及挪用客戶款項、或與客戶間有異常資金往來等情事。金管會網站（07/30/2019），〈金管會對華南商業銀行等 7 家銀行行員涉挪用客戶款項或與客戶間有異常資金往來所涉缺失之行政處分〉，https://www.fsc.gov.tw/ch/home.jsp?id=96&parentpath=0,2&mcustomize=news_view.jsp&dataserno=201907300003&aplistdn=ou=news,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&dtable=News（最後瀏覽日：09/05/2019）。

[21] 此處所稱「理財專員」，係指於銀行專職辦理對客戶解說、推介、銷售或受託投資基金（含指數股票型基金）、債券、股票、保險、衍生性金融商品、結構型商品、證券化商品或其他投資型商品之業務人員（銀行防範理財專員挪用客戶款項相關內控作業原則第 2 條）。

[22] 本文於此主要係根據上揭金管會於 2019 年 7 月底，針對七家銀行之理財專員或銀行辦事員涉嫌挪用客戶款項之處分案為例。前述七家銀行分別為華南商業銀行、國泰世華商業銀行、匯豐（臺灣）商業銀行、新光商業銀行、聯邦商業銀行、中國信託商業銀行及台新國際商業銀行，相關裁罰案件則依序為 108 年 8 月 7 日（後同）金管銀控字第 10802721961 號處分、第 1080272196D 號處分、第 10802721967 號處分、第 1080272196B 號處分、第 10802721963 號處分、第 10802721969 號處分及第 10802721965 號處分。

[23] 例如：以投資特定商品名義，誘騙客戶交付存摺或已用印之取款憑條（金管銀控字第 10802721961 號處分）。利用其他銀行辦事員未妥善保管物件之際取得客戶章戳後，蓋印於收據並提供予客戶（金管銀控字第 1080272196D 號處分）。利用保管客戶印鑑與蓋妥印鑑章之取款憑條提領現金或用以購買外幣現鈔（金管銀控字第 10802721965 號處分）。

[24] 例如：擅自利用客戶之財務狀況資料並私自向高資產客戶為借貸行為（金管銀控字第 10802721961 號處分）。利用客戶已簽章之表單與其自動化服務之密碼，將其關聯戶私自新增為客戶之自動化服務約定轉入帳號，藉此多次移轉客戶存款（金管銀控字第 1080272196B 號處分）。

[25] 例如：利用客戶親臨分行換匯或為基金交易時，於客戶應簽名之交易相關書類中夾帶非依客戶指示辦理之匯款交易指示書，藉此將其帳戶內款項匯出至第三方帳戶（金管銀控字第 10802721967

doi:10.6342/NTU202000744

損失，推介其投資特定商品，抑或對於影響客戶權益之事項為不實之說明等行為。

第二項 作業風險管理與內部控制

誠如本文上述分析，現行銀行或其他金融機構內部建置之內控制度無法有效運作之重要原因，或為內部控制第一道防線之業務單位人員未確實遵循內部程序與相關規範所致。論及內控制度之制度目的，主要為控管銀行各業務單位或部門執行業務過程中，所生或可能發生之各項風險，以達成營運與法令遵循等政策或目標。惟基於銀行內部係由多種業務單位或部門組成之情形，除了內部整體控制政策與程序之建置與運作係由董事會與高階管理階層負責外，不同業務單位尚須自行依據其業務之風險特性，設計並執行內部控制作業程序，以負責其日常事務所生風險之辨識與管理，同時及早發見業務上缺失或疏漏。故本文初步認為，若欲解決上揭所述，諸如理專挪用客戶資金、與客戶有不當資金往來，抑或交易監控系統無法即時發揮警示功能等屬內控制度第一道防線失靈之情事，即須思考銀行應如何透過內控制度之建置與運作，有效管控作業風險[26]之風險管理機能，進而達成營運與遵守法令規範之目標。因此，本文於下將逐步分析作業風險之態樣，並探討應如何藉由妥適地建立與運作內控制度，據以達成有效控管銀行內部諸等位居前線之各業務單位職員人為之疏失、錯誤或詐欺等不當行為，或謂控制內部程序失靈所衍生之作業風險之目的。

第一款 作業風險之定義與分析

第一目 銀行內部作業風險

依據巴塞爾委員會對於「作業風險」（operational risk）之定義，該詞指銀行內部所有程序、人員或系統之瑕疵或缺失，抑或外部事件等原因，致使銀行遭受損失之風險，其中包括法律風險（legal risk）[27]，惟排除策略風險（strategic risk）與聲

號處分）。於代客戶臨櫃轉帳時，將客戶款項轉入其友人帳戶後挪用（金管銀控字第 10802721969 號處分）。將開戶申請書及印鑑卡併同借款約據請客戶簽名，偽冒開戶並保有存摺，以及將客戶委託用以清償房貸與申購基金之款項逕予挪用；抑或利用保管客戶交付之印鑑、存摺及現金，偽造存摺交易與基金對帳單（金管銀控字第 10802721963 號處分）。

[26] 關於「作業風險」（Operational Risk）之定義與具體意涵，本文將於後詳述之。

[27] 法律風險係指銀行曝露於遭金融監理機關課予罰鍰、罰金，或給付因私人間糾紛所生之懲罰性賠償金等風險。MICHEL CROUHY ET AL., THE ESSENTIALS OF RISK MANAGEMENT 326 (2006).

doi:10.6342/NTU202000744

譽風險（reputational risk）[28]。具體來說，作業風險可分為程序、人員、技術及外部事件等四種態樣：程序風險係指組織內部經營相關作業程序[29]之失其效用或效率不彰所導致之風險；人員風險包括受雇職員之錯誤或違法行為、抑或缺乏堪用之能力等風險；技術（或系統）風險則係指故障所造成之系統失靈、數據或資訊品質不佳等之風險；至於因外部事件而致生損失之風險，或包括競爭對手之行為、詐欺、以及金融監管方面、整體經濟或社會經濟情狀等之變化[30]。

對於前述作業風險之定義與態樣，本文認為，造成目前銀行內控制度之失靈與金管會頻繁作成相關裁罰案件之可能原因，即係銀行未確實執行有效之作業風險管理。觀察以下兩種案件類型，即凸顯出銀行內部之程序、人員、技術或系統等三大作業風險態樣均未能獲致有效之管理：其一，或有銀行內部未對於客戶資料庫之使用建立監控程序，或對於交易資訊未能清楚揭露，致理財專員得於日常業務執行過程中，得以不當取得客戶之資訊，再透過人頭帳戶交易、私自使用客戶印鑑蓋印於空白取款單等方式挪用客戶存款。其二，或有交易員未依其個別交易授權額度操作外匯交易，致累計交易部位超逾該策略部位之授權額度，且金融交易系統與交易員部位控管平台均未有效發揮警示等內部牽制功能。

質言之，「人員風險」之發生即為銀行之辦事員、理財專員或交易員均未確實依其所應遵循之程序或法令規範執行日常業務；「程序風險」即發生於存摺印鑑登載與保管，抑或交易部位與額度之監控等內部作業程序，均未能有效規範前揭各該受雇職員之行為，甚或自始即未於內部建立作業或檢核制度或規範；「技術或系統風險」之發生則與前項之程序風險攸關，即謂銀行縱已訂有內部控制程序或建置金融交易系統與交易員部位控管平臺，惟於交易員實際操作交易或執行日常業務過程中，各項系統竟無法發揮交易資訊揭露、授權額度超逾通知與警示等應有功能。

---

[28] BASEL COMM. ON BANKING SUPERVISION [hereinafter BCBS], PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK, ¶ 11 n.5 (2011) [hereinafter BCBS PRINCIPLES FOR OPERATIONAL RISK MANAGEMENT]; BCBS, INTERNATIONAL CONVERGENCE OF CAPITAL MEASUREMENT AND CAPITAL STANDARDS: A REVISED FRAMEWORK ¶ 644 (2004) [hereinafter BASEL II].

[29] 舉例來說，包括銷售、行銷、產品發展及消費者支持等利益驅動（value-driving）程序，抑或資訊、人力資源及營運等目的在於支持營利（value-supporting）程序。Peyman Mestchian, *Operational Risk Management: The Solution Is in the Problem*, *in* ADVANCES IN OPERATIONAL RISK: FIRM-WIDE ISSUES FOR FINANCIAL INSTITUTIONS 3 (2005), http://www.risknet.de/fileadmin/eLibrary/OpRisk-Mestchian-2005.pdf.

[30] *Id.* at 3-4; CROUHY ET AL., *supra* note 27, at 327 tbl.13-1.

doi:10.6342/NTU202000744

第二目　作業風險之新型態——不當行為風險

無論人員風險、程序風險或技術（系統）風險等何種作業風險型態，其發生之主要原因概係銀行內部員工提供不適當之金融服務，且該不當行為對其客戶、金融消費者與金融市場秩序等均將造成不良影響。基此，國際組織或各國之監理機關遂將因內部成員之不當行為造成金融機構蒙受損失之當前或潛在風險視為獨立之風險類別，或謂「行為風險」（conduct risk）或「不當行為風險」（misconduct risk）。例如英國金融行為監理總署（Financial Conduct Authority，FCA）即泛指行為風險為金融機構或其內部個人所為而導致消費者受有損害，抑或對金融市場之穩定或競爭效率造成負面影響之任何行為[31]。歐洲系統性風險委員會（European Systemic Risk Board，ESRB）則指出，不當行為風險係指金融機構或其內部員工之行為所生之風險，包括：不當對待消費者或投資人、不當銷售金融產品或違反法令與操縱市場等行為，且對於金融體系之使用者、甚或社會整體均將產生外部成本[32]。簡言之，行為風險與不當行為風險兩者僅係相同概念之不同表述[33]，均指銀行及其內部員工因故意或過失，不公平對待消費者，並對於消費者、金融機構、金融體系甚或整體經濟造成不良影響之風險[34]。

尤其於 2008 年金融危機發生後，各國金融監理機關對於銀行業之風險監理與金融消費者權益之保護日趨嚴格，包括管理階層失能、作業系統缺陷、詐欺舞弊、未確實遵循作業規範、人為失誤、執行不良商業模式等作業風險或不當行為風險之控管即普遍受到重視[35]，即係為避免銀行因缺乏良好風險管理文化、未落實內部控制等所導致之內部舞弊事件再次發生[36]。職是之故，本文認為須思考者係如何對於

---

[31] Lucas Ocelewicz & James Lewis, *Conduct Risk: Delivering an Effective Framework*, KPMG (Sept. 26, 2017), https://home.kpmg/uk/en/home/insights/2017/09/conduct-risk-delivering-an-effective-framework.html.

[32] EUROPEAN SYSTEMIC RISK BD., REPORT ON MISCONDUCT RISK IN THE BANKING SECTOR 3 (2015).

[33] 沈大白、黃追（2019），〈理專案件頻傳——銀行作業風險之未來〉，《會計研究月刊》，403 期，頁 85。

[34] 具體來說，行為風險或不當行為風險包含以下三種內涵：一、係源自於金融機構及其內部員工之故意或過失行為。二、不當行為之客體係消費者，包括金融消費者、法人客戶或交易對手。三、該風險所引起者係一連串之負面外部效應，影響或損害層面涉及消費者、金融市場誠信、公平競爭秩序或公共利益等。同前註，頁 86。

[35] Stephen M. Bainbridge, Caremark *and Enterprise Risk Management*, 34(4) J. CORP. L. 967, 969 (2009); MICHEL CROUHY ET AL., THE ESSENTIALS OF RISK MANAGEMENT 30 (2006).

[36] 沈大白、黃追，前揭註 33，頁 84。

doi:10.6342/NTU202000744

作業風險之主要來源為有效之風險管理舉措，以及應如何建置與運作有效之內控制度第一道防線，同時要求位於該第一道防線中所有營業與業務單位職員之配合實踐，據以避免與管控銀行內部職員之違法或不當行為。

第二款 作業風險管理構成要素

銀行內部風險管理架構主要係由辨識風險、衡量與監控曝險程度、確保建置有效之資本規劃方案、採取控制或降低風險手段、以及向董事會與高階管理階層報告銀行曝險與資本狀況等數項程序所構成；內部控制之設計則須以銀行日常之業務活動為基礎，方能確保銀行營運之效果與效率、資訊之可靠、即時及完整性、以及符合相關法令規範等目標[37]。就作業風險管理與內部控制兩者間關係而言，內控制度係組成作業風險管理架構之基礎[38]，意即風險管理實係建置與運作內控制度之底蘊，故有效作業風險管理活動須經由內控制度之妥適運行，始竟其功。基此，本文將於以下簡析作業風險管理諸要素，並以之檢視現有內控制度規範應如何調整或修正其闕漏，方能有效落實內控制度之作業風險管理之機能。

第一目 風險政策與環境

由於銀行內部各單位人員執行相關業務時須有所本，銀行之董事會或高階管理階層首先應負責制定具體作業風險管理政策，包括明確之作業風險管理指令或實務守則[39]。例如，投資銀行執行金融商品交易業務時，應有前台交易與後台管控之區分等職務分工（segregation）、場外交易、法律文件審批等政策或程序，供各單位成員遵循[40]。此外，為確保銀行內相關成員於執行日常業務時，均能確實遵守前述各項風險管理政策，董事會與高階管理階層等應負責於銀行內部，從上而下形塑良好之作業風險管理文化[41]，據以促進董事會、經理人、乃至業務單位每位職員將風險管理意識內化為組織文化，進而善盡己身之專業職責。

第二目 作業風險管理程序

待董事會與高階管理階層訂定風險管理政策，同時形塑良好風險管理意識與

---

[37] BCBS PRINCIPLES FOR OPERATIONAL RISK MANAGEMENT, *supra* note 28, ¶ 11.

[38] *Id.* ¶ 12.

[39] *See* CROUHY ET AL., *supra* note 27, at 330.

[40] *Id.*

[41] *See* BCBS PRINCIPLES FOR OPERATIONAL RISK MANAGEMENT, *supra* note 28, princ. 1.

doi:10.6342/NTU202000744

文化，即須於銀行內部實際執行與落實作業風險管理程序。具體而言，作業風險管理程序可包括風險辨識、風險評估與衡量、以及選擇採取風險控制策略等三大步驟，以下分別述之。

（一）風險辨識——為使業務單位各職員有效捕捉並管理作業風險，風險管理政策中應具體定義與臚列作業風險各類別之通用語彙（common language），俾使每位職員均得辨認其所應避免或控制之風險行為，例如人員風險包括專業職員之不當部署、程序風險包括內部作業程序或規範之錯誤執行、技術或系統風險包括交易監控系統故障等[42]。再者，風險辨識應始於嚴格之風險自我評估程序，亦即銀行內部業務單位應評估其日常各項業務活動將曝露於人員、程序及技術等不同種類之作業風險之可能性，逐項識別並依其發生之頻率（frequency）與嚴重性（severity）予以評估[43]，方能根據事前辨識與評估之結果為有效之風險管理[44]。

（二）風險評估與衡量——一旦辨識出可能發生之作業風險後，即須透過風險評估與衡量之方法與程序，判斷銀行曝險之重大程度，據以決定應採取何種態樣之風險控制程序[45]。惟須注意者為，因並非所有作業風險之態樣均能以風險衡量方法為具體量化（be measured quantitatively），故須輔以風險評估程序對於不易量化之作業風險類別為質性評估（qualitative assessment）[46]。

關於上述作業風險之量化方法，巴塞爾委員會首先於 2004 年 6 月所公布之「新巴塞爾資本協定」[47]（Basel II）第一支柱「最低資本要求」[48]中，提供三種衡量作業風險以提列法定資本之計算方法。依各計算方法之複雜性與風險敏感度，由簡至繁分別為基本指標法、標準法及進階衡量法。其一，「基本指標法」係以銀行

---

[42] *See* CROUHY ET AL., *supra* note 27, at 330.

[43] *See* IMAD A. MOOSA, OPERATIONAL RISK MANAGEMENT 204-5 (2007).

[44] 據此，高階管理階層須依其職責，確保銀行所有金融商品、營運活動、程序及系統內潛在之作業風險，均得為有效辨識與評估，且作業風險之評估結果係符合銀行整體之風險胃納與承受範圍。*See* BCBS PRINCIPLES FOR OPERATIONAL RISK MANAGEMENT, *supra* note 28, princs. 5 & 6.

[45] *See* MOOSA, *supra* note 43, at 206.

[46] *See id.* at 209.

[47] 新版巴塞爾資本協定（Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework）訂定之主要目的係促進金融監管機關對於國際大型銀行之資本適足率等監管規定得貼近銀行之具體風險，並鼓勵銀行建立風險管理制度，以加強對於信用、授信及作業等風險之評估與管理能力。王志誠（2017），《現代金融法》，三版，頁 25，臺北市：新學林。

[48] 所謂「最低資本需求」（Minimum Capital Requirements）係指銀行承擔信用、授信、作業及市場等風險所需之最低法定資本，又謂銀行自有資本與風險性資產之比率。同前註。

doi:10.6342/NTU202000744

前三年之平均營業毛利作為單一計提指標，依固定比例計算作業風險應計提之法定資本額[49]。其二，「標準法」則係將銀行內部業務歸類為八項業務別，並事先對各業務別設定相應之計提指標，復依據各業務別固定之資本計提權數，分別提列各業務別作業風險之法定資本額[50]。其三，「進階衡量法」須以銀行歷年之作業風險損失資料紀錄作為作業風險法定提列資本之計算基礎，經由分析銀行過去損失經驗之數據資訊，評估其未來發生特定作業風險損失事件之可能性及其損失比率，並將該預期損失納入法定計提資本[51]。

又於 2007-09 年爆發全球金融危機後，巴塞爾委員會為加強金融主管機關對於

---

[49] 基本指標法係以單一計提指標（single indicator）之固定比例（α 值）計算作業風險應計提之法定資本額（K_{BIA}），其計算公式如下：

$$K_{BIA}=[(GI_{1\cdots n}\times\alpha)]/n。$$

單一計提指標為銀行前三年之平均營業毛利（gross income，GI，包括淨利息與非利息收入）之正值，亦即倘任一年營業毛利為負值或為零時，則不列入計算；固定比例則按作業風險應計提之適足資本佔現行最低法定資本計提額之比例加以推算而得。BASEL II, *supra* note 28, ¶649; CROUHY ET AL., *supra* note 27, at 336.

此法之優點在於排除複雜之數學公式與省去作業風險損失資料蒐集過程，惟該選定之單一計提指標與銀行作業風險實際曝險程度間關聯性則較為不足，且亦無法將各業務單位落實作業風險管理之成效充分反映於法定計提資本。張修齊（2003），〈從新巴塞爾資本協定看作業風險管理〉，《台灣金融財務季刊》，4 輯 1 期，頁 63。

[50] 標準法（Standardised Approach，SA）係將銀行內部業務單位歸納為八項業務別後，依業務別事先設定相應之計提指標（GI），再按各業務別固定之資本計提權數（β 值），分別提列各業務別作業風險之法定資本額。其計算公式為：

$$K_{TSA}=\{\Sigma_{years1\text{-}3}\ \max[\Sigma(GI_{1\text{-}8}\times\beta_{1\text{-}8}),0]\}/3。$$

前述業務別共分為企業金融（corporate finance）、交易與銷售（trading & sales）、零售銀行（retail banking）、商業銀行（commercial banking）、支付與清算（payment & settlement）、代理業務（agency service）、資產管理（asset management）及零售經濟（retail brokerage）。八項業務類別之計提指標為各自前三年之平均營業毛利（$GI_{1\text{-}8}$）；資本計提權數則依據各業務別屬性與曝險程度高低，分別設定其資本計提權數（β 值，區間介於 12-18%）。BASEL II, *supra* note 28, ¶¶652-54; CROUHY ET AL., *supra* note 27, at 336-37.

相對於基本指標法，標準法較能充分反映不同業務別之屬性與作業風險之曝險程度，惟前述之八項業務類別是否得一體適用於所有銀行非無疑義，且此法仍無法將採用作業風險管理後之效益直接反映於法定計提資本，或將降低銀行改善其內控環境、落實作業風險管理之誘因。張修齊，前揭註 49，頁 63。

[51] 進階衡量法（Advanced Measurement Approaches，AMA）係以銀行過往之作業風險損失資料紀錄（loss data）作為計算作業風險資本法定提列資本之分析基礎，具體包含內部衡量法、損失分配法及計分卡法等三種方法。簡言之，進階衡量法除採用量化方法計算銀行作業風險資本計提額以外，尚透過銀行過去損失經驗之數據分析，評估銀行未來發生特定作業風險損失事件之機率與損失比率，將預期損失納入法定計提資本。此法之優點在於將銀行致力於作業風險管理所帶來之效益直接反映於作業風險資本計提之數額，得提升銀行妥適為風險管理之誘因，惟關鍵在於作業風險損失歷史資料之蒐集與量化模型之建立。張修齊，前揭註 49，頁 62-64。

doi:10.6342/NTU202000744

銀行體系之規範與監理、提升銀行之風險管理能力[52]，其於 2010 年曾發布「巴塞爾資本協定 III」[53]（Basel III）。惟 2010 年版本內容，基本上係沿用 Basel II 關於銀行衡量作業風險所需資本計提額之三種主要計算方法[54]。直至 2017 年，巴塞爾委員會為提升作業風險衡量方法之實務性與可比較性，並採用更具風險敏感度之曝險指標，據以落實國際一致性之監理標準[55]，故決議定案最新 Basel III[56]。最新 Basel III 係以「新標準法」取代 Basel II 架構中所有作業風險衡量與資本計提方法[57]。新標準法之計算方式係於財務報表擷取「營運指標」作為衡量作業風險之曝險基礎[58]，依曝險程度所對應之邊際係數計算出營運指標因子[59]，再與納入損失因子

---

[52] *Basel III: International Regulatory Framework for Banks*, BIS, https://www.bis.org/bcbs/basel3.htm?m=3%7C14%7C572 (last visited July 8, 2019).

[53] 巴塞爾資本協定 III（Basel III: A Global Regulatory Framework for More Resilient Banks and Banking Systems）係 2007 年全球金融危機後，巴塞爾委員會為改善銀行之風險管理與承擔經濟與金融層面衝擊之能力，提升銀行體系之穩定性等目的所訂定者。相較於 Basel II，Basel III 則修正銀行自有資本之組成項目，並逐年提高資本適足率要求、引入槓桿比率及授權各國金融主管機關訂定抗景氣循環資本、加強流動性風險管理等措施。王志誠，前揭註 47，頁 26。現行最新 Basel III 為 2017 年發布之版本：BASEL III: FINALISING POST-CRISIS REFORMS.

[54] 銀行得選擇其部分業務採取基本指標法或標準法，其餘符合特定要件之業務則採行進階衡量法。原則上，除經主管機關之許可，抑或其認為銀行不符合採行較複雜之風險衡量方法所需之適用要件，而有強制回復採行簡易者以外，若銀行已採行較複雜之風險衡量方法（例如標準法或進階衡量法），即不得再採行較為簡易者（例如基本指標法）。*See* BASEL II, *supra* note 28, ¶¶ 647-48.

[55] 沈大白、黃追（2016），〈BCBS 調整資本計提方法之最新發展——以作業風險為例〉，《貨幣觀測與信用評等》，119 期，頁 78。

[56] 協定指出該版本之核心目的在於解決金融危機前監理架構之闕漏，以及為服務實體經濟之彈性銀行體系提供監理基礎。BCBS, BASEL III: FINALISING POST-CRISIS REFORMS ¶ 1, at 1 (2017) [hereinafter BASEL III 2017].

[57] *Id.* ¶ 2, at 128; 沈大白、黃追（2018），〈修訂後『Basel III：危機後之改革』及作業風險新標準法〉，《貨幣觀測與信用評等》，130 期，頁 108、114。此處所稱新標準法（Standardised Approach，SA）與前述 Basel II 之標準法（Standardised Approach，SA）兩種計算方法之相似處在於，新標準法營運指標因子之計算項目中，分為 12%、15%、18%三級之邊際係數（αi，詳如後註 59 之說明），其性質與標準法八項業務類別之資本計提權數（β 值）相當，均係用以反應風險敏感度。故為區別兩者，有學者將修訂後 Basel III 架構之標準法稱為新標準法，以資辨別，本文後續亦將以「新標準法」稱之。同前註，頁 108、110。

[58] BASEL III 2017, *supra* note 56, ¶¶ 5-6, at 128. 營運指標（Business Indicator，BI）包括以下三項要素：一、利息、租賃及股息因子（interest, leases and dividend component，ILDC）。二、服務因子（services component，SC）。三、財務因子（financial component，FC）。其計算公式為：

$$BI=ILDC+SC+FC。$$

[59] *Id.* ¶ 8, at 129. 營運指標因子（Business Indicator Component，BIC）則係根據各銀行其營運指標之級別（共三級）乘上對應之邊際係數（marginal coefficients，α_i）計算而得，該邊際係數係隨營運指標大小遞增。營運指標與邊際係數之關係，如下表所示：

doi:10.6342/NTU202000744

之「內部損失乘數」[60]，計算銀行最低所須計提之作業風險法定資本[61]。

然而，無論銀行選擇何種風險評估或衡量方法，其均須仰賴通暢之資訊獲取管道，蒐集充分之歷史資訊或模擬資訊作為風險衡量之基礎，始得作成準確判斷[62]。銀行內部用於作業風險管理之資訊除了得透過「風險與控制自我評估」（Risk & Control Self-Assessment，RCSA），即各業務單位之風險自我評估、質性問卷或訪談之方式取得外[63]，尚可藉由建立「數據模型」（data model），取得包括控制環境要素（Control Environment Factors，CEF）、關鍵風險指標（Key Risk Indicators，KRI）及作業風險損失資料（operational loss data）等量化或質性之風險數據或資訊[64]。

巴塞爾委員會指出，採用前述新標準法計算作業風險資本時所需之內部損失資料，應為高品質之年度損失資料[65]，因健全之內部損失資料蒐集程序、資料本身之品質與完整性，對於銀行提列符合其作業損失曝險之資本額係至關重要[66]。準此，銀行應建立適當之程序與流程，據以辨識、蒐集及處理內部作業風險損失資料，抑

級別	BI 範圍（10 億歐元）	BI 邊際係數（α_i）
一	BI≤1	12%
二	1<BI≤30	15%
三	BI>30	18%

對於營運指標屬第一級之銀行而言，其營運指標因子即為 BI×12%。惟營運指標每超逾一個級別範圍時，即須合併計算各級別對應之邊際係數，例如：營運指標為 350 億歐元之銀行（第三級），其營運指標因子為：（10×12%）+（300-10）×15%+（350-300）×18%=53.7 億歐元。*Id.*; 沈大白、黃追，前揭註 57，頁 109。

[60] BASEL III 2017, *supra* note 56, ¶ 9, at 129. 內部損失乘數（Internal Loss Multiplier，ILM）係將銀行過去內部作業風險損失事件所生之影響，納入作業風險資本之計算範圍內。其計算公式為：

$$\mathrm{ILM} = \mathrm{Ln}\left(\exp(1) - 1 + \left(\frac{\mathrm{LC}}{\mathrm{BIC}}\right)^{0.8}\right)$$

損失因子（Loss Component，LC）係相當於銀行前十年內，因作業風險所生損失之年平均之十五倍。基此，當銀行之損失因子大於營運指標因子（即內部損失乘數大於 1）時，其須提列較高之作業風險資本；反之（即內部損失成數小於 1），銀行須計提之作業風險資本則較低。

[61] BASEL III 2017, *supra* note 56, ¶ 9, at 129. 銀行所須計提最低作業風險資本（Operational Risk Capital，ORC）係上述之營運指標因子（BIC）與內部損失乘數（ILM）之積。其計算公式為：

ORC=BIC×ILM。

[62] *See* PAUL HOPKIN, FUNDAMENTALS OF RISK MANAGEMENT: UNDERSTANDING, EVALUATING, AND IMPLEMENTING EFFECTIVE RISK MANAGEMENT 208 (2010); 張修齊，前揭註 49，頁 66。

[63] *See* MOOSA, *supra* note 43, at 209; JOHN HULL, RISK MANAGEMENT AND FINANCIAL INSTITUTIONS 333 (2007).

[64] *See* MARCELO G. CRUZ, MODELING, MEASURING AND HEDGING OPERATIONAL RISK 15-17 (2002).

[65] BASEL III 2017, *supra* note 56, ¶ 10, at 129.

[66] *See id.* ¶ 17, at 130.

doi:10.6342/NTU202000744

且該內部資料除應具備全面性與完整性以外，尚須得與銀行現有之業務活動、技術流程及風險管理程序間，產生明確之連結性[67]。

（三）風險控制策略——待作業風險確經辨識並為具體評估或衡量，銀行則須採取必要之行動以控制或減緩該風險之發生對其所產生之影響，其所得採取者包括風險規避（risk avoidance）、風險降低（risk reduction）、風險轉移（risk transfer）及風險承擔（risk assumption; risk taking）等四種控制作業風險之策略。

首先，對於發生頻率較高且發生後損失程度較大之作業風險，銀行通常採取風險規避或風險終止（risk termination）策略，係因不採取任何行為或執行任何交易屬「最有效」避免產生任何風險之方式[68]。惟風險與報酬互為一體兩面，且尚須考量銀行之業務經營與吸納風險乃金融機構主要機能之一，惟如何選擇妥適之風險規避策略實存有相當之困難度[69]，故原則上銀行須先行求諸於其他可能之風險控制策略，以求其日常業務之持續運作[70]。再者，針對發生頻率較高但發生後損失程度較小之作業風險，銀行得採取降低風險之方式，例如：作業流程再造、人員培訓或技術改良等風險控制策略[71]，抑或透過建立風險呈報制度，掌握銀行內部各業務單位作業風險之實際曝險狀況、及時察覺潛在之作業風險，同時檢視現有作業風險相關管理政策或程序上之不當或不足處，俾憑採取適當之風險管理措施，以降低作業風險損失事件發生之機率與影響[72]。至於針對發生頻率較低，惟發生後損失程度較大之作業風險，銀行得採取風險移轉或沖抵之方式——例如透過保險、委外作業（outsourcing）等外部管道控制之[73]——將銀行內部之作業風險有效分散，達成控制該風險之目的[74]。最後，對於發生頻率低且發生後損失程度輕微之作業風險，銀行得主動採取事前擬定之營運計畫或風險預防措施而加以承擔該作業風險，抑或

---

[67] *See id.* ¶ 19(b).

[68] *See* MOOSA, *supra* note 43, at 210.

[69] *See id.*

[70] *See* HOPKIN, *supra* note 62, at 250.

[71] *See* MOOSA, *supra* note 43, at 210.

[72] 沈大白、黃追（2004），〈簡介 COSO 之企業風險管理（草案）及 BIS 之作業風險管理暨監督準則〉，《管理會計》，67 期，頁 60。

[73] Mestchian, *supra* note 29, at 13-14.

[74] 對於將作業風險發生之損失移轉由保險承擔，有論者認為此舉並非係屬「控制風險」之方式，蓋因於保險事故發生時，銀行始能獲得保險給付以填補其損失。換言之，銀行並未主動採取控制或避免作業風險之手段，而係被動等待作業風險實現後，獲取保險公司之財務性償付（financial cover）以填補該風險所造成之損失。*See* MOOSA, *supra* note 43, at 212.

doi:10.6342/NTU202000744

容認其發生，並藉由預先（如前述 Basel II 或金管會依其職權制訂之標準）提列之法定資本來吸納該作業風險[75]。

實務上，銀行通常係根據特定作業風險發生之經常性（frequency）、該作業風險發生後，其所造成的損失之嚴重性（severity），綜合選擇採取上述風險規避、風險降低、風險轉移或風險承擔等四項之任一或數個風險控制策略[76]。

第三項 小結——作業風險控制之實踐

經由上揭對於作業風險管理程序、作業風險衡量與法定資本提列、銀行內部損失資料之蒐集、風險主要來源等層面之析述，本文認為，作業風險之控制應從內控制度第一道防線伊始，確實執行作業風險資訊之傳遞與溝通，抑且業務執行單位與監督管理單位兩者應有明確之權責劃分，並應於銀行內部「自下而上」（Bottom-Up）貫徹銀行從業人員之道德行為操守、增強其作業風險管理之意識，始能追本溯源地控制風險。具體作法茲分述如下。

第一款 即時且正確之資訊流通

「資訊與溝通」係支持內控制度與風險管理有效運作所不可或缺者，因此，內控制度應得產生或保存符合規劃、執行及監督等目的所需之財務、營運及遵循相關之所有資訊，抑且應具備提供不同資訊需求者適時取得所需資訊之機制，且資訊須於銀行內順暢流通並得協助各部門之成員間為有效溝通。銀行內部資訊之流通或分享之「資訊流」之體現，可分別從董事之內控制度監督義務與作業風險事件資訊之運用等兩方面觀察。

第一目 董事之內控制度監督責任

銀行之董事負有確保建立並維持銀行內部適當有效之控制與稽核制度之責任[77]，亦即銀行之董事對於內控制度之建立與有效運作負有最終責任[78]。縱依公司法

---

[75] *Id.* at 213.

[76] *Id.* at 213-14.

[77] 郭大維（2017），〈企業法令遵循與董事監督義務〉，《月旦法學教室》，179 期，頁 22；臺北地方法院 96 年度重訴字第 1054 號民事判決、臺灣高等法院 97 年度上字第 1036 號民事判決。

[78] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1。

doi:10.6342/NTU202000744

之規定，董事會或為業務執行機關[79]，惟其角色定位應更似或積極作為業務執行政策之擬定者與妥善建置公司內部治理與執行機制者，前述內控制度之建立與執行即屬示例[80]。

（一）資訊之文件化記錄與保存——然正所謂「無資訊，等同無法監督。[81]」董事會應於銀行內部建置一獨立管道，以獲取監督與治理相關資訊，確保內控制度整體架構之維持與運作。因此「資訊與溝通」作為內控制度建置要素之一，同時亦係內控制度運作之基本前提，故金融機構內部無論就內部控制作業程序、行為規範準則、法令遵循政策、員工教育訓練內容等資訊，均應透過書面文件化之處理方式予以妥適記錄與保存，抑且，任何作業程序或法令規範等尚須依據內在營運策略或外在法令與經濟環境等情況變動，定期檢視與修訂之。

（二）個別董事之資訊權——為使董事會得有效履行其對於內控制度之監督責任，應賦予董事會個別成員足夠之權限，得經由銀行內部系統取得足夠且正確之數據與資訊[82]；抑或經由適當之溝通管道，得與銀行內部之各管理階層或業務單位間，進行諮詢或釐清銀行各項業務運作之細節或疑問，俾使董事會係基於充分資訊，就重大決策作成正確判斷[83]。個別董事雖依公司法第 8 條第一項與第 23 條第一項，於其執行業務時，對公司負有忠實義務並應盡善良管理人之注意義務，惟現行法制是否賦予使其知悉、獲得與執行之事務相關之各種資訊，或謂賦予個別董事明確且足夠之董事資訊權或董事資訊請求權等取得公司內部相關資訊之權限，非無疑義。觀諸現行公司法制規範，對於公司股東、監察人及檢查人等三者，縱使範圍與限制有別，均明文賦予諸等得查閱、抄錄或複製公司簿冊或文件等資訊之權限[84]，惟就董事之資訊權則尚未有足夠之權限規範。

---

[79] 公司法第 202 條。

[80] 曾宛如（2017），《公司法制基礎理論之再建構》，頁 192，臺北市：元照。

[81] 劉連煜、杜怡靜、林郁馨、陳肇鴻（2013），《選任獨立董事與公司治理》，頁 16，臺北市：元照。

[82] 蔡昌憲（2015），〈從內控失靈個案談企業社會責任與公司治理：兼論金融體系之市場監督力量〉，《台灣法學雜誌》，285 期，頁 196。

[83] *See* David F. Larcker & Brian Tayan, *Netflix Approach to Governance: Genuine Transparency with the Board* 1 (Rock Ctr. for Corp. Governance, Stanford Univ., Stanford Closer Look Series No. CGRP71, 2018).

[84] 公司股東、檢查人及監察人之資訊權係分別規定於公司法第 210 條第一、二項、第 245 條第一項及第 218 條第一項。首先，公司股東與債權人得檢具利害關係證明文件，指定範圍，隨時請求查閱、抄錄或複製董事會備置於本公司或股務代理機構之章程、歷屆股東會議事錄、財務報表、股東

doi:10.6342/NTU202000744

首先，獨立董事作為金融機構內部協助董事會作成決策、健全董事會監督功能及強化管理機能之制度設計，其引進主要係某種程度為取代監察人以享有公司之監察權限，故依據證券交易法承認上市公司得設置由全體獨立董事之審計委員會取代並準用監察人之規定[85]，獨立董事之資訊權得認已有立法賦予之。然而，由於一般董事不若前述獨立董事已於證券交易法有明文規定，即須另尋出路以探求之。觀諸主管機關之行政函釋，經濟部於民國 76 年始即指出「董事乃董事會之成員，且董事會就其權限言，對公司有內部監察權，為使內部監察權奏效，身為董事會成員之董事，如為執行業務上需要，依其權責自有查閱、抄錄公司法第 210 條第一項章程、簿冊之權。[86]」且基於「公司係由董事組成董事會執行公司業務，公司法第 8 條第一項乃規定，董事為股份有限公司之負責人。而非僅以董事長為公司負責人，董事得查閱、抄錄股東名簿，自不待言。[87]」因此，「董事為執行業務上需要，依其權責查閱、抄錄公司法第 210 條第一項章程、簿冊時，得個別為之，毋庸經董事會決議。[88]」此外，個別董事「所得查閱、抄錄或複製簿冊文件的範圍，當大於股東及債權人所得查閱、抄錄或複製之範圍，原則上不宜有過多的限制。[89]」且其行使

名簿及公司債存根簿等。再者，繼續六個月以上，持有已發行股份總數百分之一以上之股東，得檢附理由、事證及說明其必要性，聲請法院選派檢查人，於必要範圍內，檢查公司業務帳目、財產情形、特定事項、特定交易文件及紀錄。最後，監察人基於監督公司業務執行之職權，得隨時調查公司業務與財務狀況，查核、抄錄或複製簿冊文件，並得請求董事會報告。值得注意者係，公司法第 210 條與第 218 條雖均以「簿冊」二字為規定，惟主管機關（按：經濟部）認為「按公司法第 210 條是針對股東及債權人查閱或抄錄公司股東名簿表冊所設計；而同法第 218 條則是因應公司監察人行使監察權之職權而為規範，其文字解釋上，第 218 條的範圍大於第 210 條，原則上可查閱或抄錄之範圍不宜有過多的限制。」（經濟部 104 年 3 月 10 日經商字第 10402404610 號函）法院實務判決對此亦指出，為落實股份有限公司監察人之監察權，自應認其得請求公司提出各項憑證、會計帳簿、財務報表等，以利檢視公司之財務、業務狀況或發現端倪（臺灣高等法院 102 年度上字第 636 號民事判決），且監察人「業務檢查權之行使範圍，並不以公司所有之各項會計表冊或公司與他人簽訂之契約書或來往信件等各種文件為限。」（板橋地方法院 100 年度訴字第 1997 號民事判決）另外值得注意者，相較於前述股東、檢查人二者資訊權之規定，係分別以具有利害關係、聲請須檢附理由或限於指定之必要範圍內等為前提，法條文字對於監察人資訊權之行使則未有任何限制，故檢查人基於其監察權之行使，不僅得請求查核各項財務、業務文件，「董事會或經理人無從加以拒絕、或自行決定提供何等文件供監察人查核。」（新竹地方法院 102 年度訴字第 263 號民事判決）。

[85] 證券交易法第 14 條之 4 第一項至第四項。

[86] 經濟部 76 年 4 月 18 日商字第 17612 號函釋。

[87] 經濟部 105 年 5 月 27 日經商字第 10502415500 號函。

[88] 經濟部 102 年 6 月 13 日經商字第 10200063220 號函。

[89] 經濟部 108 年 1 月 29 日經商字第 10800002120 號函。

doi:10.6342/NTU202000744

該資訊查閱權限時，「公司尚不得拒絕之。[90]」惟因董事應忠實執行業務並對公司應盡善良管理人之注意義務[91]，其「查閱或抄錄應負保密義務。[92]」

前述經濟部之見解固無不當，惟就個別董事資訊權之定位與意涵非無值得再為斟酌或商榷之處。第一為主體：縱其肯認董事應具有資訊權，然經濟部係迂迴地認為因董事會具有一定之監察權，進而賦予個別董事公司法第 210 條第二項股東或債權人之資訊權。惟其若認為董事應享有監察權，則何不直接援引同法第 218 條第一項監察人之資訊權作為條文依據？第二則為客體：縱經濟部於最新函釋指出，董事請求資訊之範圍應當大於股東與債權人，且公司不宜對該範圍有過多限制[93]，實則個別董事所得查閱之範圍，仍限於該條項條文文義之「章程、歷屆股東會議事錄、財務報表、股東名簿及公司債存根簿」[94]，對公司之財務帳目、業務簿冊文件、原始憑證，甚或公司內部特定事項、交易文件及紀錄等事涉董事經營、業務內容之資訊之取得，其權限範圍尚不若監察人或檢查人等，或有違肯認並賦予董事資訊權之目的[95]，且殊難肯認此係與前述要求董事對於公司應負忠實義務與善良管理人之注意義務等達成權責相符之操作模式。

準此，法院實務判決即有認為「董事得類推適用公司法第 218 條第一項關於監察人之規定，具有得查閱公司資產負債表、綜合損益表、股東權益變動表、現金流量表、收入與支出明細帳（總分類帳）、傳票簿、進銷項原始憑證（如發票、收據等）等相關業務及財產簿冊資料之董事資訊請求權、董事之內部監察權等權限。[96]」理由概如：第一，董事為公司之負責人，於執行職務時，對公司負有忠實義務與注意義務，而要求董事善盡此等法定義務，自應令董事能知悉、獲得與執行業務相關事務及各種資訊。第二，董事會為公司之權力中樞，為充分確認權力之合法、合理運作，及其決定之內容最符合所有董事及股東之權益，應嚴格要求董事會之召集程序、決議內容均須符合法律之規定，如有違反，應認為當然無效，故勿促召集

[90] 經濟部 94 年 7 月 5 日經商字第 09409012260 號函。此外，如公司係將股東名簿備置於股務代理機構者，董事查閱亦比照辦理（經濟部 97 年 6 月 6 日經商字第 09702069420 號函）。

[91] 公司法第 8 條第一項、第 23 條第一項。

[92] 前揭註 90。

[93] 前揭註 89。

[94] 公司法第 210 條第一項、第二項。

[95] 王文宇（2009），〈董事之資訊請求權〉，《月旦法學教室》，86 期，頁 19。

[96] 彰化地方法院 106 年度訴字第 764 號民事判決。

doi:10.6342/NTU202000744

董事會之決議無效，而未能事前獲悉董事會決議之相關資訊，更甚於此，益徵董事有權自公司取得與執行職務相關之資訊。第三，觀諸民國 106 年 5 月 8 日公告之公司法第 193 條之 1 第一項條文修正草案[97]，該項立法理由略以「董事為股份有限公司之負責人，應忠實執行業務並盡善良管理人之注意義務，如有違反致公司受有損害者，負賠償責任；董事如為執行業務上之需要，依其權責自有查閱、抄錄第 210 條第一項章程、簿冊之權，公司尚不得拒絕之。董事本有查閱、抄錄或複製簿冊文件之權，爰將經濟部函釋明文化，並參照第 218 條有關監察人調查權之範圍，將董事查閱、抄錄或複製簿冊文件之範圍擴大。」是故，草案修正條文認為董事查閱、抄錄或複製簿冊文件範圍，不以第 210 條者為限，肯認董事之內部監察權，應得查閱公司相關業務及財產簿冊資料。第四，監察人應監督公司業務之執行，並得隨時調查公司業務及財務狀況，查核簿冊文件，並得請求董事會或經理人提出報告；另繼續一年以上，持有已發行股份總數百分之三以上之股東，得聲請法院選派檢查人，檢查公司業務帳目及財產情形[98]。此等規定乃股份有限公司對公司行使查閱財產文件、帳簿、表冊之檢查業務權，為對公司行使監督權。而如前述，董事為盡其前述法定義務，避免擔負相關責任，自須先自公司取得與執行職務相關之資訊，非對公司實施監督權；監察人不得兼任公司董事，縱董事與監察人查閱之標的同一，因兩者目的不同，不能謂董事查閱即破壞公司監督制衡機制。公司法賦予股東及監察人對於公司之特定文件有查閱之權限，但未明文賦予參與決定公司業務執行之董事有此類似權限，應屬董事執行職務所必然附隨內涵。

職是之故，無論係現行行政主管機關抑或法院實務判決，均已肯認董事為執行職務與履行其所負忠實義務、善良管理人之注意義務等職責，故應賦予個別董事一合理之董事資訊權。為有效解決前述條文依據不明確、資訊請求範圍不一致等董事資訊權定位不清之諸項問題或爭議，正本清源之道為藉由修訂公司法，以明文獨立肯認個別董事均得作為請求公司資訊之主體，並適度規範或限制所得請求之資訊範圍[99]。例如得比照股東或檢查人之資訊權行使之規定，對於董事加以「職務範圍」

[97] 民國 107 年 7 月通過之公司法修正中，行政院所提出之草案本有第 193 條之 1 關於董事資訊權之規定，該條第一項原謂：「董事為執行業務，得隨時查閱、抄錄或複製公司業務、財務狀況及簿冊文件，公司不得規避、妨礙或拒絕。」惟此一草案規定遭逢朝野立法委員之強大阻力，最終並未修正通過。

[98] 公司法第 218 條、第 219 條及第 246 條。

[99] 王文宇，前揭註 95。

doi:10.6342/NTU202000744

或「正當目的」作為資訊權行使之必要限制[100]，抑或參考美國法制，於肯認董事得查閱、檢視與公司法令遵循、內部控制、財務報告、揭露資訊或資產相關之簿冊、紀錄及文件之虞，其資訊權之行使仍須以「與董事執行職務之事項具有合理關聯」為限縮要件[101]。簡言之，為使銀行內控制度等內部自律機制發揮實效，應透過健全內部監督機關（董事、獨立董事及審計委員會）決策過程之方式，例如於法制規範上，應明文獨立賦予董事資訊權，以強化董事取得資訊之管道或系統，提供利於其執行監督之工具[102]，始竟其功。

第二目　作業風險事件資訊之運用

對於銀行而言，作業風險損失事件之資訊（loss data）蒐集與運用之重要性，係實際體現於兩層面：第一，作業風險損失事件之歷史資訊係銀行內部衡量作業風險與計提法定資本所不可或缺之素材。第二，作業風險或損失發生時，資訊之即時流通或傳達，係經營管理階層得即刻處理業務單位成員所為不當行為或舞弊案件等危機事件所仰賴者。

首先，作業風險之衡量與法定資本計提方法概可分為自上而下（top-down）與自下而上（bottom-up）兩種類型：前者係基於金融機構整體觀點，計算作業風險之法定提列資本總額，再透過擬定之計提指標將作業風險資本分別配置於內部各業

---

[100] 邵慶平（2019），〈論公司資訊權的規範：以董事資訊權的增訂爭議為中心〉，《東吳法律學報》，30 卷 4 期，頁 23。學者同時指出，現行公司法第 219 條係賦予監察人具有堪稱「超級資訊權」之資訊權限，惟該規定是否妥適，且是否應比照股東與檢查人之規定，對於監察人資訊權之行使加諸「利害關係」或「必要範圍內」等明確限制，或有納入思考之高度必要。

[101] MALVIN ARON EISENBERG, CORPORATIONS AND OTHER BUSINESS ORGANIZATIONS: CASES AND MATERIALS 793 (9th ed. 2005); MODEL BUS. CORP. ACT § 8.01(b) (1984) (AM. BAR ASS'N, amended 2016):

> A director of a corporation is entitled to inspect and copy the books, records and documents of the corporation at any reasonable time **to the extent reasonably related to the performance of the director's duties as a director**, including duties as a member of a committee, but not for any other purpose or in any manner that would violate any duty to the corporation (emphasis added.)

8 Del. C. § 220(d), https://delcode.delaware.gov/title8/c001/sc04/index.shtml (last visited Feb. 4, 2020): "Any director shall have the right to examine the corporation's stock ledger, a list of its stockholders and its other books and records **for a purpose reasonably related to the director's position as a director**" (emphasis added.)

[102] 蔡昌憲（2018），〈從公司法第一條修正談公司治理之內外部機制——兼論企業社會責任的推動模式〉，《成大法學》，36 期，頁 103-104；蔡昌憲（2015），〈省思公司治理下之內部監督機制——以獨立資訊管道的強化為核心〉，《政大法學評論》，141 期，頁 248-249。

doi:10.6342/NTU202000744

務類別或產品別；至於後者則須先行分析銀行內部各業務單位每一作業流程中，作業風險發生之機率與嚴重程度，再將各項數據整合至金融機構之層次，故作業風險損失資料之蒐集與分析，係落實此類型計提方法所不可或缺者[103]。誠如前述，計算作業風險提列資本時，無論係採用最新 Basel III 之新標準法或 Basel II 之進階衡量法，首應突破之瓶頸均係銀行內部損失資料之缺乏或闕漏[104]，抑或現有損失資料無法忠實呈現內部作業風險之曝險程度，故關鍵在於如何建置完善之資料系統，並透過明確化資料蒐集與追蹤程序，以取得合理、完整、可驗證，同時符合銀行作業損失曝險實況之內部損失資料。

再者，除了上述作業風險損失資料蒐集系統與程序之建置以外，應由內控制度確保作業風險事件相關資料或資訊能即時傳達至經營管理階層，俾使管理單位得於第一時間處理業務單位成員所為之不當行為。質言之，觀諸銀行理財專員挪用客戶資金之內部舞弊案件，除了有數家銀行於七年期間內（2012 年至 2018 年）發生多起類似案件，顯示其疏於落實內控制度致出現累犯紀錄外[105]，部分個案係同一行為人利用職務之便，長時間為舞弊行為，惟竟未能為有效察覺者[106]。此外，尚有法國興業銀行（Société Générale）交易員 Jérôme Kerviel 利用銀行內控制度風險控管系統之漏洞為越權交易，不法操作大量詐欺性部位，惟銀行監督與管理階層竟未能及時察覺該名員工之舞弊行為，導致銀行最終須承擔高達 49 億歐元之鉅額虧損[107]。職是故，針對前述理專不法挪用客戶存款、交易員濫用交易系統等作業風險事件，銀行應於各業務單位確實建立內控制度，偵測內部員工之不法或可疑行為，並應於舞弊案件發生時，即時將該作業風險事件之資訊有效傳遞至負責監督之管理階層，俾利其迅速進行調查、評估或為任何適當之應變措施。

---

[103] 張修齊，前揭註 49，頁 64、66；BCBS, WORKING PAPER ON THE REGULATORY TREATMENT OF OPERATIONAL RISK 2-3 (2001).

[104] *See* HULL, *supra* note 63, at 328-29.

[105] 沈大白、黃追（2019），〈理專弊案頻傳——銀行作業風險之未來〉，《會計研究月刊》，403 期，頁 82。

[106] 例如：108 年 3 月 26 日金管銀控字第 10702224341 號處分、106 年 12 月 19 日金管銀國字第 10620006841 號處分、106 年 9 月 27 日金管銀國字第 10620004841 號處分。各裁罰案件中，理財專員涉嫌為挪用客戶存款之不法行為期間有長達 9 至 13 年不等。

[107] *See* C. Richard Baker et al., *Breakdowns in Internal Controls in Bank Trading Information Systems: The Case of Fraud at Société Générale*, 26 INT'L J. ACCT. INFO. SYS. 20, 20-21 (2017).

doi:10.6342/NTU202000744

第二款 內部各成員之行為操守

完美之內控制度及其相關之任何程序規範至多僅能「合理確保」銀行得達成營運、報導及法令遵循等目標，尚無法保證銀行建置並運作內控制度後，即可收風險降低至零或徹底杜絕舞弊發生之效，此係因內控制度就其本質屬自發性、自主性之內部管理流程之不得不然[108]。至於就作業風險、行為風險等主要係由人為所致之風險發生之原因而論，美國社會學家 Donald Ray Cressey 所提出之「舞弊三角理論」（The Fraud Triangle）或可作為落實有效作業風險管理之參考[109]。詳言之，構成舞弊犯罪之成因包括三項要素：壓力（pressure）、機會（opportunity）及自我合理化（rationalization）。壓力係指舞弊者因面臨某種財務需求，惟其無力透過正常管道解決而萌生舞弊之動機；機會則係指舞弊者意識其居於違犯舞弊且不易被察覺之地位或在免於遭受懲罰之前提下，觸發其實際執行不當行為；自我合理化則係舞弊者對於本身所為舞弊行為之自我評價，使其得跨越或修正自身既有之行為準則或道德觀念之鴻溝，繼而認同其所為之舞弊行為，或將無視任何行為規範[110]。因此，倘若銀行之理財專員、交易員或任何於第一線單位執行業務之前臺員工蓄意凌駕內控制度及其相關規範，抑或利用內控制度之漏洞，故意為不法或舞弊行為時，內部控制之有效性即會遭受極大減損。

基於健全之內控制度運作至極致時僅能減少，尚無法完全消除人為因素對於內控制度所生負面影響，故若為根本性地解決或控管作業風險、行為風險之發生，首須重視者係銀行內部各業務單位員工之行為規範。誠如本文於第二章對於內控制度理論發展脈絡之觀察所述，銀行內控制度之具體設計上最重要之原則與精神係「內部牽制」，即透過銀行內部各單位之成員間專業化與不相容之職務分離，就其各自業務之執行，形成相互檢查、覆核、制衡及監督關係，除藉此偵測業務執行過程中可能產生之疏漏或錯誤以外，尚可避免詐欺、舞弊等違法行為之發生。例如前述銀行理財專員利用職務之便，長期不法挪用客戶資金，以及交易員濫用內控風險管理之漏洞執行越權交易導致銀行蒙受龐大損失等案件均顯示，銀行本身除了

---

108 廖大穎（2019），〈檢析法令遵循與我國公司治理之內部控制模式〉，台灣企業法律學會（編），《國際公司治理與企業法遵》，頁 125-126，臺北市：元照。

109 DONALD R. CRESSEY, OTHER PEOPLE'S MONEY: A STUDY IN THE SOCIAL PSYCHOLOGY OF EMBEZZLEMENT (1953).

110 *The Fraud Triangle*, ASS'N CERTIFIED FRAUD EXAMINERS, https://www.acfe.com/fraud-triangle.aspx (last visited July 11, 2019).

doi:10.6342/NTU202000744

內控制度之設計與建置有所不足外，即係肇因於未充分落實內部牽制與覆核機制，導致單一員工得於相當期間內，數次實施不法行為卻無法為其他員工或管理階層即時察覺。

內控制度之建立與落實或謂係立基於經營者之誠信，透過規範程序之設計，於銀行內部落實自我控制、自我稽核及自我評估之機制[111]，惟本文認為，「誠信」並非僅須存在於經營管理階層，應係銀行內部所有從業人員均應具備之基本要件，因無論係內控制度與作業風險之評估或管理、作業風險損失事件或舞弊行為之發生等，均涉及銀行內部每一位成員之人為判斷，亦即作業風險實與「人」此一因素息息相關。準此，唯有於銀行內部自下而上落實良好風險管理與遵循舞弊防治政策，方能根本性地控制內部成員從事作業風險相關行為之誘因。

第三節　經營管理階層

誠如前述，多數不法或舞弊行為等作業風險係發生於銀行之分行或謂行為人多為分行之職員，為有效地自源頭控管作業風險或於發現不法行為時，及時採取相應措施以避免作業風險持續擴大或累積，各業務單位或部門之經營管理階層實具有重要之角色與功能。再者，因銀行內部業務單位多樣且部門分工細緻，若由較為熟悉該業務單位且具備專業知識之資深管理階層作為確保內控制度第一道防線有效運作者，除了能夠有效且即時查核風險、防止舞弊行為以外，尚可協助董事會評估銀行之營運目標與各項業務投資。然而在現行公司法制規範架構下，經營管理階層於內控制度運作過程中，恐存在與董事會間權責定位未明之根本性問題。故本節首先將嘗試重新定位銀行內部之決策監督與經營管理之機關分責，再行聚焦經營管理階層主體範圍之認定，據此析述經營管理階層於內控制度所應扮演之角色與其職責。

第一項 決策監督與經營管理之辨析

包括金融機構在內之上市、上（興）櫃及已辦理公開發行之股份有限公司等大型企業，雖其家數相較於中小企業或謂有限，惟基於其營業額、員工數及實收資本

[111] 林仁光（2004），〈論經營者誠信、內部控制、內部稽核制度與公司治理〉，《月旦法學雜誌》，106期，頁 40。

doi:10.6342/NTU202000744

額等規模龐大[112]，在總體經濟中實扮演重要角色，公司治理架構亦有其特色。質言之，現代大型公司鑑於規模龐大，故其公司治理架構呈現管理階層化與專業分工之特徵，即於公司內部設置不同管理機關，並賦予各部門或單位成員相應之權責，以求共同有效率且順暢運作多樣且繁雜之日常業務活動[113]。傳統學理上將股東會定位為公司內部最高意思決定機關，惟現實上為考量維護公司正常經營與平衡股東權益之保障，股東會本身所得決議之事項仍須以法律或章程明文規定者為限[114]。則依現行公司法規定，即可認為董事會於公司內部扮演業務決策與業務執行之重要角色，或謂董事會作為公司經營者，握有業務訂定與執行之經營權，此係現今公司法立法例中，企業所有與經營分離原則之體現[115]。

縱謂現行公司法制主要係將公司經營權限交付予董事會行使之，惟對於營業額龐大、業務內容繁雜、單位部門林立及員工數量眾多之大型公司而言，董事會於實務運作上或將囿於種種限制，較難期待其凡事均須親力親為，遂有建構董事會與經營管理階層之組織階層分工、權責劃分之必要性[116]。舉例來說，公司法規定董事

---

112 經濟部訂定之「中小企業認定標準」指出，所謂中小企業與大型企業之認定、辨別基準主要有實收資本額、經常僱用員工數及營業額等。首先，製造業、營造業、礦業及土石採取業實收資本額在新臺幣八千萬元以下，或經常僱用員工數未滿二百人者，即屬中小企業。再者，前述規定外之其他行業前一年營業額在新臺幣一億元以下，或經常僱用員工數未滿一百人者，亦屬之。準此，所謂大型企業之定義則為營業額新臺幣一億元以上，或經常僱用員工數一百人以上者（中小企業認定標準第 2 條）。

113 王文宇（2012），〈論大型企業之公司治理法制〉，《月旦法學雜誌》，200 期，頁 283。

114 林仁光(2006)，〈董事會功能性分工之法制課題——經營權功能之強化與內部監控機制之設計〉，《臺大法學論叢》，35 卷 1 期，頁 175-176。

115 公司法第 202 條；劉連煜（2010），《現代公司法》，六版，頁 449，臺北市：元照。2016 年美國模範商業公司法（Model Business Corporation Act）第 8 章第 8.01 條第(b)項即指出：公司所有權力應由董事會行使或於經董事會授權後行使。公司業務之經營，除章程或協議另有限制外，應受董事會之管理與監督。MODEL BUS. CORP. ACT § 8.01(b) (1984) (AM. BAR ASS'N, amended 2016):

> All corporate powers shall be exercised by or under the authority of the board of directors of the corporation, and the business and affairs of the corporation shall be managed by or under the direction, and subject to the oversight, of its board of directors, subject to any limitation set forth in the articles of incorporation or in an agreement . . . .

此外，德拉瓦州公司法亦指出，除本法或公司之章程另有規定外，公司業務之經營均應由董事會管理或依其指示為之。8 Del. C. § 141(a), https://delcode.delaware.gov/title8/c001/sc04/index.shtml (last visited Feb. 4, 2020): "The business and affairs of every corporation organized under this chapter shall be managed by or under the direction of a board of directors, except as may be otherwise provided in this chapter or in its certificate of incorporation."

116 *See* EISENBERG, *supra* note 101, 198-200; 王文宇（2019），〈論董事會與執行長的權責區分〉，王

doi:10.6342/NTU202000744

會為公司業務執行機關，且董事長一職除對內為董事會主席外、對外尚由其代表公司[117]，惟觀察現行公司法或證券交易法等法規，並未就公開發行公司召開董事會之次數或頻率有強制規定，僅有證交所與櫃買中心建議上市、上櫃公司宜維持每季至少召開一次之最低開會頻率[118]。又或如前述，除公司法或章程規定應由股東會決議之事項外，均應由董事會決議之規定，但實際上該條文除了未明確界定董事會與股東會之權限劃分外，公司法本身明定須經董事會決議之事項並不多，董事會召開與否或恐繫諸於董事長一人[119]。因此，就大型公司而言，由其董事會之集會頻率、成員權力結構、以及董事會成員對於公司內部眾日常業務活動之熟悉與實際參與程度等面向觀察，公司業務之運作除係由董事長單獨決行外，現行趨勢係由董事長授權予其選任之經理人、甚或由經營管理階層負責決策與推動[120]。

公司組織作為一持續運作之有機體（going concern），若其本身部門或單位之規模係持續擴張、業務範圍與種類逐漸增加，僅由董事會作為主要業務執行機關，或將於人力資源配置上有不足之處，故董事會須委由經營管理團隊依其專業能力，實際推行與運作董事會決議之政策目標與業務活動[121]。雖然現行公司法將董事會定性為業務執行機關，惟就業務權限內容而言，其尚可分為業務決策權與業務執行權，意即大型公司董事會至多僅負責重大政策或目標之訂定或議決，至於日常業務之執行則多授權予專業經營管理階層為之[122]，故經理人（或經營管理階層）於執行職務範圍內，亦屬公司負責人。因此，基於實務發展趨勢與有效運作之考量，現行法制似有改革之必要。

文宇（等著），《「落實獨立董事制度，提升公司治理價值」建言集》，頁 22，臺北市：社團法人中華公司治理協會。

117 公司法第 208 條第三項。

118 上市上櫃公司治理實務守則第 31 條。現實運作上，公司鮮少召開董事會，縱有設置常務董事會，至多亦係一個月甚或數個月始召開會議。

119 公司法第 208 條第五項；方嘉麟（2019），〈公司管理之權力結構〉，方嘉麟（等著），《變動中的公司法制：17 堂案例學會《公司法》》，二版，頁 135、141，臺北市：元照。

120 曾宛如，前揭註 80，頁 14-15。就未經董事會或常務董事會決議事項之效力問題，除非面臨訟爭，否則實務基本係採得過且過之態度。惟有學者認為，為免滋生不必要之爭議，公司法應將董事長與董事會之關係，及其可得授權之範圍予以明確釐清，俾使法律規範與實務運作兩者得以協調。同前註，頁 15。

121 曾宛如、林國彬（2019），〈管理者之義務與責任〉，方嘉麟（等著），《變動中的公司法制：17 堂案例學會《公司法》》，二版，頁 182，臺北市：元照。

122 王文宇，前揭註 116，頁 25。

doi:10.6342/NTU202000744

現行公司法以董事會作為業務執行機關之解釋適用於一般中小型公司似無窒礙難行處，惟對於金融機構等較大型之公開發行公司而言，實際運作或組織上需求則應有彈性調整之空間，除避免徒增中小型公司法令遵循成本外，亦有助於法制設計有效運作與發展。質言之，內控制度規範首先即明確指出，金控公司或銀行之董事會，對於確保內控制度之有效建立與維持該制度適當有效運作，以及營運風險之控管，應負起監督之最終責任[123]。再者，現行證券交易法已引進獨立董事制度，金管會並擴大強制要求上市、上櫃及公開發行之金融機構等大型公司，應於董事會下設置審計委員會、薪酬委員會等功能性委員會[124]，且各功能性委員會成員應由獨立董事或具備獨立董事資格者擔任[125]，並直接對董事會負責[126]。吾等若探究功能性委員會存在之目的即可知，其係藉由專業分工與獨立超然之立場，依其專業知識，就公司各項事務提供獨立、客觀之意見，協助董事會作成決策、健全董事會之監督功能及強化管理機能[127]。

承前所述，董事會與經營管理階層兩者間功能定位、職務劃分及責任歸屬，或有重新思考與解釋之空間。歐盟執委會於「歐盟公司治理架構綠皮書（Green Paper）」即曾指出，董事長（董事會）與執行長彼此間明確之權限與責任劃分，係有助董事會落實其監督義務、扮演確保公司運作與發展之重要角色[128]；銀行法相關規範原則上亦限制銀行之董事長不得兼任總經理[129]。準此，本文綜合前述就制度架構、實務運作及相關法制設計等面向之觀察後認為，由於現今銀行規模與業務種類日趨龐

123 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1。

124 證券交易法第 14 條之 2 第一項、第 14 條之 4 第一項及第 14 條之 6 第一項；107 年 12 月 19 日金管證發字第 10703452331 號令、107 年 12 月 19 日金管證發字第 1070345233 號令。

125 證券交易法第 14 條之 4 第二項、第 14 條之 6 第一項；股票上市或於證券商營業處所買賣公司薪資報酬委員會設置及行使職權辦法第 5 條、第 6 條。

126 銀行業公司治理實務守則第 35 條第二項；金融控股公司治理實務守則第 35 條第二項；上市上櫃公司治理實務守則第 27 條第二項。

127 曾宛如（2020），《證券交易法原理》，七版，頁 165、167，臺北市：元照。證券交易所與櫃檯買賣中心於「上市上櫃公司治理實務守則」中亦指出，上市、上櫃公司之董事會得考量公司規模、業務性質、董事會人數，設置審計、薪資報酬、提名、風險管理或其他各類功能性委員會，並得基於企業社會責任與永續經營之理念，設置環保、企業社會責任或其他委員會，並明定於章程（上市上櫃公司治理實務守則第 27 條第一項）。類似規定如銀行公會頒布之銀行業公司治理實務守則第 35 條、金融控股公司治理實務守則第 35 條。

128 *European Commission Green Paper: The EU Corporate Governance Framework*, at 5, COM (2011) 164 final (Apr. 5, 2011).

129 銀行負責人應具備資格條件兼職限制及應遵行事項準則第 3 條之 1 第一項本文。

doi:10.6342/NTU202000744

雜，為達成合理且有效之權責分配，其內部決策監督與經營管理之權限與責任應重新予以詮釋。意即董事會應定位為「監督（監控）型機關」，專司重大政策目標之擬定與經營管理階層之監督；日常業務之執行與管理則交予經營管理階層，即「業務執行型機關」為之[130]，藉此釐清業務「決策」與「執行」權責之分際。惟若然，董事應負之忠實義務（受任人義務）則須為細緻化歸納[131]，故關於董事忠實義務之意義與內涵，本文將留待後續論述。

第二項 經營管理階層之認定與職權

有鑒相對於董事會，大型公司諸如銀行、金控公司、保險公司等金融機構之經理人或經營管理階層，係職司公司日常業務活動之策略擬定與執行，其於內控制度運作過程中所扮演之角色亦漸趨重要。惟就如何認定經理人或界定經營管理階層非無疑義，本文在此謹扼要探討經理人之認定與其權責，俾利聚焦後續論述經營管理階層於內控制度之主體範圍。

首先，自前述大型公司內部逐漸區分業務決策權與業務執行權之趨勢觀察，其公司治理架構係採取由董事會負責重大政策之議決，再由董事會決議或依章程規定選任、設置經理人[132]，將日常業務經營權限授予專業之經營管理階層，同時公司法並未強制規定經理人之法定職稱[133]。然而銀行、金控公司等金融機構作為特許行

---

130 曾宛如（2011），〈董事會與經理人是否真為公司之業務執行機關及業務執行之輔助機關？——從臺灣高等法院臺中分院九十九年度重上字第一七四號判決及九十九年度重上字第一六四號判決所凸顯之亂象論起〉，《月旦法學雜誌》，199 期，頁 181。

131 同前註。

132 公司法第 29 條第一項第三款，類似規定例如 MODEL BUS. CORP. ACT, *supra* note 115, § 8.40(a) (“A corporation has the offices described in its bylaws or designated by the board of directors in accordance with the bylaws.”); 8 Del. C., *supra* note 115, § 142(a) (“Every corporation organized under this chapter shall have such officers with such titles and duties as shall be stated in the bylaws or in a resolution of the board of directors which is not inconsistent with the bylaws . . . .”) 公司法該款明定股份有限公司就經理人之委任、解任及報酬，除公司章程有較高規定者外，應由董事會以董事過半數之出席、出席董事過半數同意之決議（即普通決議）行之，故此類事項原則上應不得授權董事長或由其單獨為之。惟現實上公司選任經理人鮮有經董事會決議者，因而產生經理人之選任有效與否之爭議。曾宛如，前揭註 80，頁 15，註 16。

133 故對於一般股份有限公司而言，經理人之認定方式成有形式認定說與實質認定說之兩種不同見解：前者認為公司之經理人係指依公司法第 29 條規定依章程設置、董事會普通決議任免，並依「公司登記辦法」之規定向主管機關辦理登記者，始為經理人（例如：臺灣臺北地方法院 102 年度訴字第 561 號刑事判決、臺灣高等行政法院 101 年度簡字第 119 號簡易判決）；後者則係依公司法第 31 條第二項規定，認為凡有於公司章程或契約規定授權範圍內，對內有管理公司事務、對外有簽名代表權限之人，方屬經理人，以求名實相符，故實際上若該經理人已有為公司處理事務並簽名之權限，

doi:10.6342/NTU202000744

業，為避免金融機構經營者因毋須擔負確實控管風險之責任，或因政府對金融機構係採取「過大不能倒」（non-failure; too big to fail）政策，以致不當提高經營者道德風險，主管機關對於金融機構之經營者應進行較諸一般公司為縝密之「適格性審查」（“fit and proper” test）[134]。質言之，美國金融監理機關即認為，銀行或其他金融機構本身之經營架構與管理階層是否健全，係著實攸關風險控管有效性與廣大存戶之權益[135]，故基於適格性審查之目的，其應有權限事前評估或審查銀行之董事會與經營管理階層等成員，是否皆具備有效管理或監督銀行所有業務活動之專業能力與技術、從業經驗、道德品性及個人特質等資格[136]。抑且，金融監理機關除了能夠否決銀行報請審酌之人員外，倘其認為銀行之個別董事或經營管理階層人員有不符資格條件之虞者，亦得依職權命銀行重新選任或以行政處分解除特定人之職務[137]。

相較於公司法對於公司之經營管理者（即負責人）主要係採取二分法之立法模式，區分為當然負責人與職務負責人[138]，金融機構之經營管理階層之成員及其名稱，依相關金融業法與主管機關之規定，除了董事、監察人外，明確指出包括總經理、副總經理、協理、總行（總公司）經理、分行（分公司）經理或與其職責相當

為保障交易安全，並使公司承擔經理人制度為其帶來交易之便利與所衍生之風險，即屬實質上之經理人；又或經理人之姓名已明確載於其所任職上市公司之內部控制說明書、年度財務報告、董事會議事錄、營業報告書等文件，且有該經理人簽名或蓋章，即足認公司董事會已實質上決議通過認可聘任該經理人，從而自應發生公司法上經理人之委任關係（例如：最高法院 102 年度台上字第 360 號民事判決、臺灣高等法院臺中分院 100 年度重上更（一）字第 27 號民事判決、臺北地方法院 92 年度勞訴字第 10 號民事判決、臺中地方法院 97 年度重訴字第 515 號民事判決）。

134 *See* Mamiko Yokoi-Arai, *The Evolving Concept of Operational Risk and Its Regulatory Treatment*, 9(1) LAW & BUS. REV. AMS. 103, 110 (2003).

135 *See* Catharine M. Lemieux, *Conglomerates, Connected Lending and Prudential Standards: Lessons Learned*, 4(1) UCLA J. INT'L L. & FOREIGN AFFS. 149, 149 (1999).

136 *See id.* at 150.

137 *Id.*

138 以股份有限公司為例，公司法第 8 條第一項規定，名稱董事者即為公司之當然負責人，包括一般董事、獨立董事、公益董事、勞工董事、事實上董事、內部董事及外部董事，以及同法第 27 條第一項之政府或法人董事、第二項之政府或法人股東代表人董事等；至於第 8 條第二項規定，包括公司之經理人、清算人或臨時管理人、股份有限公司之發起人、監察人、檢查人、重整人或重整監督人等，於執行職務範圍內，亦屬公司負責人。原則上，銀行、金控公司、保險公司等金融機構亦適用該條項之規定（銀行法第 18 條、保險法第 7 條、信託業法第 5 條），惟金融機構依其主管機關按照各金融業法授權規定訂定之準則內容，就金融機構之負責人有較為明確之名稱與範圍，詳如本文後述。

doi:10.6342/NTU202000744

之人[139]。抑且，銀行本身尚有如總稽核、法令遵循主管（或稱法遵長）、資訊安全專責單位主管[140]等具備一定職務權限且職責達內部一定層級以上者。

第三項 小結——內控制度管理權責

觀諸國際組織與各國金融監理機關之內部控制與風險管理相關規範，均要求董事會對於銀行內控制度之設計與建立、作業風險管理架構、政策及原則之訂定、以及監督內控制度並維持其適當有效之運作、乃至於內部控制與風險管理文化之落實等，均應擔負最終之責任[141]。此外，由於內部稽核、法令遵循、風險控管、資訊安全等內部控制專責單位，係直接或間接隸屬於董事會，故董事會尚應履行定期或於必要時，聽取各專責單位提報或審閱其所提交之書面報告之義務。

惟誠如本文前述，將董事會定位於內控制度監督機關之規範架構，得否於現行公司法制架構下充分發揮作業風險管理之實效，容有再思考之空間。觀諸各國立法例，董事會依其主要功能可分為「監控型」與「業務執行型」：前者例如美國大型企業、臺灣股份有限公司之原型則屬於後者。在此立法架構與定位下，倘若要求董事會（包括獨立董事或審計委員會）應擔負內控制度運作之監督責任，不啻係於執行業務為主、權力高度集中之董事會內部置入監督其自身業務執行之機制，或將形成自己同時經營與監控之矛盾現象，則監控之實際成效難謂可期待[142]。故本文認為，董事會自業務執行機關轉型為監督機關即屬必需。

---

[139] 銀行負責人應具備資格條件兼職限制及應遵行事項準則第 3 條之 3、第 4 條、第 5 條及第 6 條；金融控股公司發起人負責人應具備資格條件負責人兼職限制及應遵行事項準則第 2 條；保險業負責人應具備資格條件準則第 4 條、第 5 條；信託業負責人應具備資格條件暨經營與管理人員應具備信託專門學識或經驗準則第 3 條、第 4 條、第 5 條及第 8 條；證券商負責人與業務人員管理規則第 2 條第一項；期貨商負責人及業務員管理規則第 2 條第一項；票券商負責人及業務人員管理規則第 2 條。

[140] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 10 條第二項、第 32 條第一項、第 38 條之 1 第一項。

[141] *See, e.g.*, BCBS PRINCIPLES FOR OPERATIONAL RISK MANAGEMENT, *supra* note 28, princ. 3, at 8; FIN. REPORTING COUNCIL [FRC], GUIDANCE ON RISK MANAGEMENT, INTERNAL CONTROL AND RELATED FINANCIAL AND BUSINESS REPORTING ¶ 24, § 2 (2014); EUROPEAN SYSTEMIC RISK BD. [ESRB], REPORT ON MISCONDUCT RISK IN THE BANKING SECTOR § 3, at 9 (2015); 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1。

[142] 故有學者建議，董事會之法制設計與定位應調整為監控型機關，同時降低其權力集中度，利於董事得透過功能型委員會（即審計委員會）對於管理階層有更強大且客觀之監督與控制能力。請參考：方嘉麟，前揭註 11，頁 9-10。

doi:10.6342/NTU202000744

抑且，現行規範均係強調董事會與「高階」管理階層之職權，然而應注意者為作業風險之風險源通常係存在於內控制度之第一道防線，意即銀行內部直接面對客戶或提供銷售服務之前臺（the front office），抑或係處理業務結算、編製交易紀錄之後臺（the back office）[143]。因此，若欲透過位居於內控制度第二或第三道防線之董事會、高階管理階層即時處理作業風險，頗有「遠水救不了近火」之感。因此本文認為，銀行內部各業務單位或部門之經營管理階層，均應擔負內控制度與作業風險管理之責任，理由概如下述。

首先，吾等若觀察金管會裁罰案件中與作業風險相關者即可知，多數不法或舞弊行為係發生於銀行之分行或行為人多係分行之職員，故唯有透過加強各業務單位管理階層之監督責任，始能有效地自源頭控管作業風險或於發現不法行為時，即時採取有效措施以避免作業風險逐漸擴大或持續累積。再者，銀行內部之業務單位多樣且部門分工細緻，若由較為熟悉該業務單位且具備專業知識之資深管理階層擔負業務執行之監督責任，基於其對於所負責管理業務單位之深入瞭解與經驗，除了能夠有效且即時查核風險、防止舞弊外，尚可協助評估銀行之營運目標與各項業務投資。最後，透過業務單位管理階層親自監督旗下員工業務執行活動，應落實明確之權責劃分，意即須釐清各自所扮演之角色與所掌握之權限與責任範圍，避免利益衝突或權責分工不清之情形發生，例如身兼業務執行與監督管理之職務，如此方可收除弊興利、監督制衡（checks and balances）之雙重效果。

第四項 就地落實誠信經營組織文化

經營管理階層除了於內控制度架構下，扮演協助董事會確保內部控制與作業風險管理有效運作之角色以外，其主要職責在於管理與監督業務單位之日常營運活動，維持銀行整體良好、健全經營之組織文化，以發揮銀行作為金融機構應有之經濟與社會機能。惟「文化」乙詞本身並無孰高孰低或對錯之分，商業組織依其目的與經營模式之不同，各有符合自身所需之組織文化與行為準則；出現不當行為或發生弊案並不必然表示該公司整體組織文化係屬惡劣，僅能謂該公司內部存在與所欲達成之目標較不一致之要素，造成不適當或不為大眾普遍接受之個案行為出

[143] 詹德恩（2019），〈我國金控公司與銀行法令遵循施行現況及未來〉，台灣企業法律學會（編），《國際公司治理與企業法遵》，頁 328-329，臺北市：新學林。

doi:10.6342/NTU202000744

現[144]。因此，透過法律強制規範組織文化與行為著實不可能亦不實際。惟良好組織文化仍係鼓勵正向行為、防止不當侵害他人權益之基礎，尤其創造銀行內部良好之營運環境、形塑誠信與道德價值之組織文化，不僅是銀行永續經營之關鍵，更與內控制度之控制環境要素得否建立息息相關。

本文以下將以經營管理階層為核心，逐步探討銀行內部形塑強調誠信、正直之組織文化之重要性，以及經營管理階層對該組織文化之形塑，又將如何進一步對於內控制度之運作產生影響。

第一款 形塑良好組織文化

內控制度係透過規範制度設計，旨在要求公司內部建立一套自我控制、自我稽核及自我評估之機制，惟該制度推動成敗之關鍵，相當程度繫諸於「經營者之誠信」[145]。因此，倘若經營管理階層違反其忠實義務、背離誠信原則，或棄股東權益之保障於不顧、為牟取自身利益而恣意規避內控制度之行為規範，不僅將使內部治理機制失其效用，亦將對於公司治理造成負面影響。故為充分且有效落實前述內部控制法令遵循機制功能，須由銀行董事會與高階經營管理階層自上而下（the tone at the top），於組織內部形塑強調以誠信（honesty）與正直（integrity）為標準之文化[146]與行為守則。同時，董事會與經營管理階層均應以身作則，將該行為準則具體落實於日常業務執行過程中，俾使所有員工群起仿效[147]，以建立或持續改善銀行經營文化。

形塑良好文化之重要性在於文化係企業運作之基礎，抑且其所導引出組織之價值取向將深刻影響內部所有層面與人員，缺乏或有缺陷之文化將影響該組織與消費者、投資者及主管機關間的互動關係[148]。文化雖謂係企業運作之基礎，然而其要件與意涵並未有特別定義，普遍之說法或描述為「當無人注意時，人將從事何種

144 GROUP OF THIRTY [G30], BANKING CONDUCT AND CULTURE: A PERMANENT MINDSET CHANGE 2 (2018), https://group30.org/images/uploads/publications/aaG30_Culture2018.pdf [hereinafter G30 BANKING CONDUCT & CULTURE].

145 林仁光，前揭註 111。

146 BCBS, COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS ¶ 2 (2005).

147 *See* MARTIN T. BIEGELMAN & JOEL T. BARTOW, EXECUTIVE ROADMAP TO FRAUD PREVENTION AND INTERNAL CONTROL: CREATING A CULTURE OF COMPLIANCE 106 (2d ed. 2012).

148 *See* Olga Rakhmanina, *Culture Shift: Bank's Roadmap to Survival*, TAIWAN BANKER (Sept. 2019), http://service.tabf.org.tw/TTB/Article/Detail?aID=315.

doi:10.6342/NTU202000744

行為」或「塑造行為與心態之共同價值與規範」[149]，亦即組織內部允許成員如何之行為或從業方式。舉例來說，銀行內部環境文化或價值取向若係默許個別辦事員或業務員為追求利潤得過度追求風險，或達成特定財務目標時即可獲取而外獎勵、無視客戶利益或銀行信譽風險，則將使銀行內部所有成員為相互競逐利潤，恣意規避或無視內控制度等內部管理機制，最終該等不當行為不僅將有損於客戶或社會公眾對於該銀行機構本身，甚或擴及對於銀行業、金融服務業整體之信賴。

誠如美國華爾街著名投資銀行索羅門兄弟（Salomon Brothers）之總裁 Henry Kaufman 於其自傳中所言：「信任是人生中大多數關係之基石，金融機構與市場亦須建立在信任之基礎上。[150]」惟事實是，愛德曼公司於 2019 年發布之「全球信任調查報告」中顯示，金融服務業相較科技業、汽車製造業或食品業等產業，係近五年內最不受顧客信賴之業別[151]。英國國會之銀行標準委員會亦指出，銀行從業人員本應具有強烈之信任義務——至少就對待客戶與共同維持銀行業整體專業之聲譽而言，然而事實上鮮有銀行從業人員認為其應適時約束自身行為，更遑論監督其他同業或勇於舉報業內之不法行為，故銀行文化之特徵或可謂係缺乏對於客戶與維繫銀行業整體聲譽之義務與責任感[152]。不可諱言者，倘欲克服現行銀行根深柢固之思維與行為模式實屬不易，唯有持續自銀行內部各個層級與部門予以改善，方能達成建立強調誠信、正直之銀行組織行為文化之目標。

---

[149] *See id.*

[150] HENRY KAUFMAN, ON MONEY AND MARKETS: A WALL STREET MEMOIR 313 (2001). ("Trust is the cornerstone of most relationships in life. Financial institutions and markets must rest on a foundation of trust as well.").

[151] EDELMAN, 2019 EDELMAN TRUST BAROMETER: GLOBAL REPORT 45-46 (2019), https://www.edelman.com/sites/g/files/aatuss191/files/2019-03/2019_Edelman_Trust_Barometer_Global_Report.pdf?utm_source=website&utm_medium=global_report&utm_campaign=downloads.

[152] PARLIAMENTARY COMM'N ON BANKING STANDARDS, CHANGING BANKING FOR GOOD ¶ 135 (2013), https://www.parliament.uk/documents/banking-commission/Banking-final-report-vol-ii.pdf:

> The professions may not be paragons, but they do at least espouse a strong **duty of trust**, both towards clients and towards upholding the reputation of the profession as a whole. In contrast, bankers appear to have felt few such constraints on their own behaviour. Few bankers felt a **duty to monitor or police** the actions of their colleagues or to report their misdeeds. Banking culture has all too often been characterised by an absence of any sense of duty to the customer and a similar absence of any sense of collective responsibility to uphold the reputation of the industry (emphasis added.)

doi:10.6342/NTU202000744

第二款 聚焦中階經理階層

現行法制或實務守則對於建構、形塑銀行文化通常係採取「由董事會與高階管理階層訂定政策」（“tone from the top”）之模式，即由董事會與高階管理階層本於廉潔、透明及負責之經營理念，制定以誠信與道德價值為基礎之政策與內部行為準則，建立良好之公司治理與風險管理機制，創造永續發展之經營環境[153]。惟科技發展與全球化促使現代公司規模日漸擴張，銀行亦呈現內部業務單位多層分工、廣設國內外分支機構或分行之趨，即有國際金融組織對此表示：若欲徹底落實銀行誠信文化與成員正直行為之理念，則應轉由採取「由業務單位直屬中階經營管理階層訂定政策」（“tone from above”）之模式[154]，故銀行前線之業務單位及其經營管理階層——或謂內控制度第一道防線，著實為關注焦點[155]。質言之，實際執行日常業務，同時須遵循銀行內部相關政策規範者，是為數眾多、廣布於銀行總機構、各地分行或業務單位，並直接受其上級單位管理與監督之業務員、理專、財務顧問、出納或會計等前臺（frontline）受雇職員。抑且，縱然經營政策或行為準則等規範、誠信文化之形塑等，係由董事會與高階管理階層負責訂定，惟董事會或高階管理階層尤其對於分支機構之職員實屬「天高皇帝遠」之存在，其影響力或控制力遠不如中階（middle）管理階層來得更為直接與有效[156]。

作為銀行董事會與高階管理階層、內部業務單位職員兩群體間嫁接之橋樑，中階管理階層負有將董事會訂定之政策內容與期待目標，確實且有效轉化為前臺第一道防線業務單位日常業務行為守則之重要權責[157]。再者，中階管理階層得否依其專業訂定適當之作業程序規範，有效協助業務單位職員達成政策目標，亦將對於銀行內部組織文化與行為模式產生相當影響。質言之，中階管理階層因負責依其職權指揮監督或訓練轄下之業務單位職員，共同達成董事會與高階管理階層訂定之政策或營運目標，惟若有中階管理階層之經理人未妥適訂定作業程序規範且要求其

---

153 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條第一款；上市上櫃公司誠信經營守則第 5 條。

154 G30 BANKING CONDUCT & CULTURE, *supra* note 144, at xi.

155 DEBBIE TROKLUS & SHERYL VACCA, INTERNATIONAL COMPLIANCE 101: HOW TO BUILD AND MAINTAIN AN EFFECTIVE COMPLIANCE AND ETHICS PROGRAM 19 (2013) (“‘Tone in the middle’ cannot be overlooked.”).

156 *See* G30 BANKING CONDUCT & CULTURE, *supra* note 144, at 30.

157 Linda Treviño et al., *The Invisible Role of Middle Management: Unethical Behaviour and Unrealistic Expectations*, *in* TRANSFORMING CULTURE IN FINANCIAL SERVICES 68, 68 (Fin. Conduct Auth. ed., 2018).

doi:10.6342/NTU202000744

業務單位職員均應確實依循，抑或蓄意容認業務單位職員之不當或不法行為，完全以達成績效表現為首要考量，則該等舉措不僅將使董事會與高階管理階層對於營運情形作成錯誤決策判斷，亦將造成無法即時有效遏止職員或經理人等欺瞞或不正行為持續發生之不利後果[158]。茲就前述理專挪用客戶存款事件論，案例事實均顯示銀行理專係長期、持續且多次不當挪用款項，惟究其實質，該等挪用款項行為均係個別透過執行例行性業務作業程序所為，例如保管客戶存摺或印鑑、開立對帳單、收取個人資料文件等。對此，倘中階管理階層未能妥適控管業務單位職員或其自身之行為，則該等「例行性程序」（routines）極有可能成為規避與破壞銀行內控制度等組織內部規範之工具，用以達成掩飾與維持諸等欺瞞或不正行為之目的[159]。

職是故，由於現代銀行之規模龐大、分支機構遍佈全球且個別銀行內部業務單位眾多，對於執行位於總機構之董事會所訂定之政策與目標，便須仰賴分散在各地之中階管理階層，以及由其負責管理與監督之業務單位[160]。故在高度分層、分散且分工之經營模式下，中階管理階層則應依照其所屬銀行之業務性質、日常營運活動、人力資源、地理位置、當地法令、氣候環境等個別條件或限制，分別訂定包括行為準則、作業程序、績效目標等在內之內控制度相關規範，俾使各該業務單位職員得於執行日常業務過程中同時知所遵循，據以落實董事會之政策與目標。換言之，由於董事會訂定之政策內容仍須經營管理階層與業務單位共同執行始可發揮作用，故中階管理階層之角色功能即係充分於銀行內部傳達董事會之經營理念，並依其職權與專業，訂定具體作業程序與規範供業務單位職員充分瞭解、遵循且無礙於職員日常業務之順暢運作，最終方能有效形塑銀行良好組織文化與行為操守[161]。

---

158 *See* Niki A. den Nieuwenboer et al., *Middle Managers and Corruptive Routine Translation: The Social Production of Deceptive Performance*, 28(5) ORG. SCI. 781, 781-82 (2017).

159 有學者將此定義為「腐敗例行性程序之轉譯」（Corruptive Routine Translation），意即中階管理階層先行辨識組織內部結構性制度規範之疏漏，藉由執行前線或層級較低之例行性程序，以掩飾本身或所屬業務單位職員為達成組織目標所為之欺瞞或不正當行為。*Id.* at 782. ("[A] process whereby middle managers identify structural vulnerabilities in the organization that they exploit to create and enforce a lower level routine that enables and sustains deceptive subordinate performance.")

160 *See* G30 BANKING CONDUCT & CULTURE, *supra* note 144, at 30.

161 *See id.* at 17.

doi:10.6342/NTU202000744

第四節　董事會

第一項 董事會作為監控機關

銀行董事會建置與運作內控制度之目的與責任，在於藉由內控制度以認知與有效控管銀行整體於營運時所面臨之風險，確保營運、報導及法令遵循等各項政策目標之有效達成，以履行其監督之最終責任。惟如前述，現行通念係將董事會定位為組織內部之業務執行單位，就該認知與定位，本文認為此不僅將影響內控制度之運作，亦將對於現行獨立董事、審計委員會等制度機能造成相當程度之影響。換言之，無論是內控制度或獨立董事相關制度之運作目的，均為協助或強化董事會之監督功能，倘若未能從本質上調整對於董事會功能之想像與定性，或將使其他制度配套間接失其作用。因此，奠基於前述對於現行決策監督與經營管理之辨析，本文在此將從金融機構內部職務之組織分工、獨立董事制度之運作等兩層面，再次嘗試提出董事會應作為監控機關之芻議。

第一款 業務執行與監督之分工

現今銀行、金控公司、保險公司等金融機構規模與業務種類日趨龐雜，為達成合理且有效之權責配置與營運活動之分工，其內部決策監督與經營管理兩者組織結構應重新予以定位。質言之，對於中小型或組織或分層結構較為簡單之公司而言，其董事會得同時身兼業務決策與業務經營之雙重角色；惟就內部業務單位眾多之大型公司而言，業務經營與執行基於專業分工則應交由經營管理階層，董事會則理應專司業務決策與監督（oversight）之職責[162]。意即，現行公司法下之董事會或認為係公司之業務執行機關，惟其所執掌者應非日常業務之執行，實則係公司整體政策目標之擬定與內部治理機制之妥適建立[163]，如銀行或金控公司董事會應認知營運所面臨之風險，監督其營運結果，並對於確保建立與維持適當且有效之內控制度，即屬示例[164]。

除了建置與確保內控制度之有效性外，董事會尚須對公司之經營策略與計畫、

[162] MELVIN A. EISENBERG, CORPORATIONS AND OTHER BUSINESS ORGANIZATIONS: STATUTES, RULES, MATERIALS, AND FORMS 620 (2014th ed. 2014).

[163] 曾宛如，前揭註 80。

[164] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1。

doi:10.6342/NTU202000744

重大風險與曝險程度、經營管理階層績效表現與薪酬、法令遵循政策與道德行為準則、備置財務報表、即時且充足資訊獲取管道、選任獨立董事、設立功能性委員會等事項，擔負決策與監督之責[165]。值得注意者，此部分權責內容係相當程度與專司監督之獨立董事重疊，因此，在現行主管機關係採取逐漸強化獨立董事與審計委員會制度於金融機構內部運作之態度下[166]，若未能調整以董事會作為業務執行機關之定位，或將造成業務執行與決策監督兩者間之扞格[167]，終有損於獨立董事制度之機能。

第二款 強化獨立董事制度功能

獨立董事（independent director）於現代公司治理範疇中，多數認為其屬不可或缺之要角[168]。惟獨立董事實際上並未經常參與公司日常業務之運作，僅例行地參與董事會、協助作成公司業務相關決策，因此其性質亦屬非執行業務董事（non-executive director），故較難發揮經營管理之職能或作為公司之管理階層[169]，或謂其主要職責在於扮演協助與強化董事會監督功能之角色。因此，本文將嘗試經由獨立董事作為董事會成員與審計委員會成員之兩種角色作為切入點，以分析董事會之功能定性對於獨立董事相關制度將產生何種影響，並再次呼應前述本文對於董事會應作為監控機關之倡議。

首先，獨立董事為董事會成員，須參與董事會之業務決策[170]。即對於公司之營運計畫、財務報告、內控制度、具股權性質有價證券之募集發行或私募、財務會計或內部稽核主管之任免、對關係人之捐贈[171]、涉及董事會自身利害關係之事項、重大業務財務行為之程序、重大資產或衍生性商品之交易、重大之資金貸與背書或提

165 MODEL BUS. CORP. ACT, *supra* note 115, § 8.01(c); EISENBERG, *supra* note 162, at 620-21.

166 107 年 12 月 19 日金管證發字第 1070345233 號令、107 年 12 月 19 日金管證發字第 10703452331 號令。

167 方嘉麟，前揭註 11，頁 10（「獨董或審計委員會於我國，是在一個執行業務為主的董事會，塞進監督業務執行者的機關，格格不入可想而知。」）

168 王文宇、林國全、曾宛如、王志誠、蔡英欣、汪信君（2015），《商事法》，頁 321，臺北市：元照。

169 Melvin A. Eisenberg, *The Board of Directors and Internal Control*, 19(2) CARDOZO L. REV. 237, 237 (1997).

170 證券交易法第 14 之 2 第一項但書；公開發行公司董事會議事辦法第 7 條第五項。

171 公開發行公司董事會議事辦法第 7 條第一項。

doi:10.6342/NTU202000744

供保證、簽證會計師之委任解任或報酬等事項[172]，獨立董事應依其商務、法務、財務、會計及公司業務所需之專業知識[173]，適當表達其專業意見。獨立董事對於前述諸等決議之事項，若有反對或保留意見時，亦應於董事會議事錄中載明[174]。準此，獨立董事不僅須參與董事會業務決策之討論，同時須對於決策事項內容表示其獨立、客觀判斷之專業意見。

再者，獨立董事尚須擔任隸屬於董事會之審計委員會成員[175]，且就設置審計委員會之目的言，在於藉由專業分工與超然獨立之立場，擔任協助董事會決策與監督經營管理階層之角色[176]。因此，審計委員會應就公司之內控制度及其有效性之考核、重大財務業務行為之程序、涉及董事會自身利害關係之事項、重大資產或衍生性商品之交易、重大之資金貸與背書或提供保證、具股權性質有價證券之募集發行或私募、簽證會計師之委任解任或報酬、財務會計或稽核主管之任免、財務報告等重大議案[177]，先行予以審查並決議，始能再行提交由董事會決議，以強化審計委員會獨立決策與輔助董事會之功能[178]。

由是觀之，獨立董事一方面對於董事會決議之重大事項，應明確表達其專業意見，且須善盡其董事相關義務，以謀求公司最大利益為依歸[179]，此係獨立董事作為董事會成員所具有之「興利」功能。惟另一方面，獨立董事應基於其本身之專業資格，於董事會決議前，先行審議前述之重大議案，此係獨立董事作為審計委員會成員所具有之「防弊」功能。抑且，獨立董事於執行業務之範圍與期間內，應保持一定之獨立性[180]，據以落實與強化其在公司治理領域中，達成興利防弊之主要目標。究其本質，董事會得認係與公司內部或與股東間，具有緊密連結關係之組織體，其較能且應代表公司或股東及其他利害關係人，執行監督其他董事與經營管理階層

---

172 證券交易法第 14 之 3。

173 公開發行公司獨立董事設置及應遵循事項辦法第 2 條。

174 證券交易法第 14 之 3。

175 BRUCE F. DRAVIS, THE ROLE OF INDEPENDENT DIRECTORS IN CORPORATE GOVERNANCE: AN UPDATE OF THE ROLE OF INDEPENDENT DIRECTORS AFTER SARBANES-OXLEY 118-19 (2010); 證券交易法第 14 之 4 第二項。

176 曾宛如，前揭註 127，頁 165。

177 證券交易法第 14 條之 5 第一項。

178 曾宛如，前揭註 127，頁 166。

179 公司法第 8 條第一項、第 23 條第一項。

180 公開發行公司獨立董事設置及應遵循事項辦法第 3 條。

doi:10.6342/NTU202000744

之權限，或為公司之監督機關[181]。因此，倘若董事會係以業務執行或經營管理為導向，同時又肩負決策與監督之職責，董事會不啻是權力高度集中，且將形成自為經營與自為監督之窘境，獨立董事即無從有效制衡之。

第二項 外部他律機制之補強

綜觀公司治理之架構或機制，可歸類為內部（internal）治理與外部（external）治理兩者[182]，前者主要係探討董事會與經營管理階層應如何組成、運作及互動，以極大化公司、股東及利害關係人之利益；後者則藉由司法判決、行政監管等法規範系統與市場、政策、文化及社區等外部力量，達成由外監督與強化公司內部治理之目的[183]。質言之，董事會作為公司內部治理單位之最高級別（apex），其職責除了在於選任與監督管理階層之業務執行外，更重要者為負責建置與確保內控制度之有效運作，並透過內控制度即時偵查公司內部之缺失或疏漏，及早將公司之運作「導回正軌」[184]。因此，誠如本文前述，鑑於內控制度係促進公司治理、風險管理及法令遵循等順利運作之內部自律機制，董事會既作為公司內部決策、管理及監督之最終機關，即應職司確保內控制度有效運作之責任。

再者，為解決公司治理上代理成本之問題[185]，公司法學者經由採取適當「法律策略」（legal strategy），即以規則或標準等法令規範，功能性地建構外部他律機制，達成控制或最小化代理成本、保障公司及相關利害關係人權益等目的[186]。法律策略可分為「事前法律策略」（*ex ante* strategy）與「事後法律策略」（*ex post* strategy）

---

[181] Eisenberg, *supra* note 169, at 238.

[182] Stuart L. Gillan, *Recent Developments in Corporate Governance: An Overview*, 12(3) J. CORP. FIN. 381, 382 (2006).

[183] *Id.* at 383-85; Diane K. Denis & John J. McConnell, *International Corporate Governance*, 38(1) J. FIN. & QUANTITATIVE ANALYSIS 1, 2-4 (2003).

[184] *See* Michael C. Jensen, *The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems*, 48(3) J. FIN. 831, 862-63 (1993) ("[T]he very purpose of the internal control mechanism is to provide an early warning system to put the organization back to track before difficulties reach a crisis stage.")

[185] 簡言之，公司治理之代理成本問題（agency problems; principal-agent problems）主要存在於，或謂有三種類型態樣：一，公司所有人（指股東）與經理人；二，控制股東與非控制股東；三，公司本身與員工、債權人、消費者等所有利害關係人。John Armour et al., *What Is Corporate Law?*, *in* THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH 1, 2 (Reinier Kraakman et al. eds., 2d ed. 2017).

[186] *See* John Armour et al., *Agency Problems and Legal Strategies*, *in* THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH, *supra* note 185, 29, 31; Chong-En Bai et al., *Corporate Governance and Market Valuation in China*, 32(4) J. COMP. ECONS. 599, 605 (2004).

doi:10.6342/NTU202000744

兩項：前者係指於公司董事、經理人等代理人為監督或業務經營等行為前，立法者或監管機關即訂定對該代理人發生直接效力，內容係要求其應為或限制其不應為特定行為之事前規則（*ex ante* rule），例如：強制公開揭露規則即要求證券發行人於證券市場籌資前，應先揭露特定資訊予投資者知悉。後者則係代理人為特定行為後，方由授權裁判者依循事後標準（*ex post* standard），對該代理人之事實行為是否違反法令規範作成評價，例如：公司法要求董事應基於善意（good faith）作成決策判斷，抑或董事與公司間自我交易應遵守完全公平（entirely fair）法則[187]。

準此，於近年來強化公司治理之趨勢下，就金融機構之董事會於內部自律機制所扮演之角色及其應具備之權責，立法者或金融主管機關於法律命令或實務守則中，不乏有明文規定。首先，相關實務守則指出，董事會成員應忠實執行業務與盡善良管理人之注意義務，並以高度自律與審慎之態度行使職權[188]，為達成公司治理之目標，董事會之主要任務有訂定有效與適當之內控制度[189]。再者，證券交易法、銀行法或其他金融業法亦規定其組織內部應建立內控與稽核制度[190]，故為促進銀行業之健全經營，完善其內部治理機制，銀行之董事會應考量實際營運狀況，決議通過以三道防線為基礎架構之內控制度[191]。抑且，銀行之董事會應認知營運所面臨各種風險，監督其營運結果，倘若董事發現銀行有受重大損害之虞時，應儘速妥適處理，立即通知審計委員會成員並應提報董事會且應督導所屬銀行通報主管機關[192]。意即，董事會就銀行營運之結果、風險控管及內控制度之建置與維持，應負監督之最終責任[193]。由是觀之，立法者與金融監管機關均已透過外部他律機制之事前法律策略，就董事會應如何有效落實內控制度等內部自律機制，設有明確且縝密之法令規範。

---

187 *See* Armour et al., *supra* note 185, 29, 32-33 & 37.

188 銀行業公司治理實務守則第 45 條第一項；金融控股公司治理實務守則第 45 條第一項；上市上櫃公司治理實務守則第 37 條第一項。

189 銀行業公司治理實務守則第 34 條第一款；金融控股公司治理實務守則第 34 條第一款。

190 證券交易法第 14 條之 1 第一項；銀行法第 45 條之 1 第一項；金融控股公司法第 51 條；保險法第 148 條之 3 第一項；票券金融管理法第 43 條；證券投資信託及顧問法第 17 條之 1 第二項、第 93 條；期貨交易法第 97 條之 1 第一項；信用合作社法第 21 條第一項；信託業法第 42 條第二項；郵政儲金匯兌法第 10 條；電子支付機構管理條例第 30 條及電子票證發行管理條例第 17 條第二項。

191 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條、第 6 條。

192 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條之 1。

193 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1。

doi:10.6342/NTU202000744

值得注意者，董事是否因其負有內控制度之「監督責任」，進而須負擔「監督義務」（Duty to Monitor）之責，基於董事監督義務尚未明文化於現行公司制，容有探討之空間。觀諸前述內控制度建置與確保運作之規定，雖有類似於董事監督義務概念之體現，惟該等規定僅屬事前法律策略之「規則」（rules），其尚且無法於現行公司法或相關法制未有明確規範下，對於監督義務之內涵為明確闡釋。固然，董事應建置與運作內控制度之相關規定經常被視為監督義務之重要內涵[194]，或可謂以該等具體規定來充實抽象董事監督義務之作法，得提供董事一明確之行為準則，使其等知悉應如何履行監督義務，同時有效防免因怠於監督所生之賠償責任，惟此是否係對於英美法下董事監督義務意涵先有正確認知後之作法，非謂無疑[195]。質言之，由於董事監督義務本質應屬事後法律策略之「司法審查標準」（standards），故董事監督義務及其相關民事責任之具體內涵，仍須求諸於或留待法院於民事訴訟程序中終局地澄清之[196]。

誠然董事監督義務尚未明文化於我國立法例中，惟該義務於司法實務判決中已有案例論及相關概念，故本文以下將嘗試藉由探尋既有實務案例，觀察董事監督義務之可能具體意涵與發展。然而須先予指明者，本文之研究對象主要為金融機構公司治理之內部自律機制，即內部控制之制度與組織層面之分析與探討，故就本質係屬外部他律機制事後法律策略之董事監督義務，囿於本文研究目的與研究範圍之設定與篇幅之有限，僅略作觀察後之初步分析。

第一款 初探法院實務案例

遍覽現有司法實務案例對於金融機構之董事所負建置與運作內控制度，甚或對於監督義務有具體論述者雖尚稱不多，僅有「花蓮企銀案」與「幸福人壽案」等兩例，且儘管「鄉林建設案」所涉爭點非為金融機構董事之監督義務，惟各級法院在前述諸項案例中，均對於董事會與內控制度、董事所負善良管理人之注意義務等

194 張心悌（2019），〈員工違法行為之董事監督義務——評臺灣臺北地方法院 105 年度訴字第 4239 號民事判決〉，《月旦裁判時報》，80 期，頁 23；洪秀芬（2006），〈董事會獨立經營權限及董事監督義務〉，《政大法學評論》，94 期，頁 247。

195 邵慶平（2008），〈董事受託義務內涵與類型的再思考——從監督義務與守法義務的比較研究出發〉，《臺北大學法學論叢》，66 期，頁 17-18。

196 蔡昌憲（2018），〈從公司法第一條修正談公司治理之內外部機制——兼論企業社會責任的推動模式〉，《成大法學》，36 期，頁 115。

doi:10.6342/NTU202000744

內涵有相當值得參考之論述。因此，本文以下將先行概述前揭三件之案例事實、主要爭點及各級法院判決理由，最後並提出本文對於現行實務就事後法律策略（即董事監督義務）發展之觀察。

第一目　花蓮企銀案

太平洋證券股份有限公司（以下簡稱太平洋公司）為前花蓮區中小企業銀行股份有限公司（以下簡稱花蓮企銀）[197]之法人股東，甲則係太平洋公司指派以其代表人身分當選為花蓮企銀之董事，再由該行董事會選任之董事長[198]。查甲於擔任花蓮企銀董事長期間，曾兩度以董事長身分支領年度年終獎金[199]，惟花蓮企銀前業已於股東常會議決董監報酬之給付標準，然並無董監事得領取獎金之決議[200]，故花蓮企銀係在銀行無盈餘且未經股東會決議之情形下，不當發放前述兩筆年度獎金。再者，金管會亦認定係違反銀行法第 45 條之 1 第一項規定，兩度發函要求花蓮企銀應追回該不當發放之獎金未果[201]，故作成裁處書，依同法第 129 條第七款規定，核處花蓮企銀新臺幣（下同）400 萬元罰鍰。其指出：花蓮企銀兩度發放董事長、副董事長獎金之行為，係違反該行章程規定與股東會討論事項決議，且該行歷次函復之查核報告均未能查核實情，亦拒絕追回獎金，顯見該行內部控制及稽核制度已無法有效執行，始生該等不當發放獎金之情事[202]。因此，原告中央存款保險公司（以

197 自 96 年 9 月 8 日零時起，即本案訴訟繫屬中，花蓮區中小企業銀行股份有限公司〔以下簡稱花蓮企銀〕之營業及資產負債，已概括讓與由中國信託商業銀行股份有限公司〔以下簡稱中信商銀〕承受。

198 公司法第 27 條第二項。蔡○浩（即本文之甲）係自 93 年 7 月 5 日起至 95 年 1 月 17 日止，當選並擔任花蓮企銀第十屆、第十一屆董事長。迄 95 年 1 月 8 日始，太平洋證券股份有限公司改派劉○海接任花蓮企銀之第十一屆董事長，惟劉○海旋於同年 9 月 26 日請辭董事長職務。

199 第一次係於 94 年 1 月 31 日支領 93 年度年終獎金新臺幣（下同）1,837,500 元（含工作獎金 300,000 元、考績獎金 360,000 元、不休假獎金 37,500 元、特別獎勵金 1,140,000 元）；第二次係於 95 年 1 月 24 日支領 94 年度年終獎金 742,500 元（含工作獎金 300,000 元、考績獎金 360,000 元、特別獎勵金 82,500 元），共計 258 萬元整。

200 花蓮企銀於 93 年 6 月 30 日經股東常會決議該公司董監報酬之給付標準為：「月支酬勞上限標準改為董事長辦公費 20 萬元、副董事長辦公費 15 萬元、董事、監察人月報酬金及專業津貼每月上限為 10 萬元。」對此，原告即主張該股東會決議僅議決公司董監事報酬之給付標準，各董監事並無領取獎金之權利。

201 金管會認定花蓮企銀不當發放之獎金包括：一、93 年年終獎金超額發放；二、92、93 年不當核撥特別獎勵金；三、93、94 年核發予董事長、副董事長之各項獎金（金管會 95 年 9 月 22 日金管銀（四）字第 09500383690 號函）。

202 金管會 95 年 12 月 21 日金管銀（四）字第 09500474741 號裁處書（「以花蓮企銀「93 年、94 年度發放董事長、副董事長獎金 3035 千元，違反貴公司章程第 24 條規定及 93 年臨時股東會討論事

doi:10.6342/NTU202000744

下簡稱存保公司）[203]主張甲作為花蓮企銀之董事長，依法有於其任內建立內控與稽核制度有效執行之義務，惟其未能使該行內控制度有效執行，致生該行因不當溢發獎金，遭金管會科以罰鍰之情事。故請求太平洋公司及其法人代表董事長甲，應對花蓮企銀因受前開金管會裁罰所生之損失，負損害賠償之責。

承前，本案爭點主要有：一、負有確保建立並維持有效內控與稽核制度之義務者，究為「董事個人」或屬合議制之「董事會」？二、被告甲是否須就該不當發放獎金致花蓮企業遭金管會科處罰鍰之情事，負有侵權行為之損害賠償責任？且太平洋公司是否須就法人董事代表人所為之侵權行為，負連帶賠償責任？[204]

對於上開第一項爭點，本案第一審與第二審法院均判決原告（上訴人）敗訴，判決理由概為[205]：首先，法院認定花蓮企銀遭課以罰鍰之原因，係該行內控與稽核制度無法有效執行，未能阻止獎金之不當發放所致。然而，法院非以銀行法第 45

項決議，貴行歷次函復本會之查核報告均未能查核實情，並辯稱於法尚無不合，經本會二度函請貴行追回前揭獎金，貴行亦拒絕辦理，顯然內部控制及稽核制度已無法有效執行」為由，認花蓮企銀違反銀行法第 45 條之 1 第一項規定，依同法第 129 條第七款規定，核處罰 400 萬元。）

[203] 為提供金融業優質之經營環境，且讓經營不善之金融機構得以平順地退出金融市場，以消弭問題金融機構造成之金融風暴於無形，行政院設有「金融重建基金」。且相較美國、日本係於金融機構已發生多起倒閉案件且將引發金融危機後，方由政府編列預算、動用公共基金為事後處理，該金融重建基金之特色係於問題金融機構產生前，政府即先行通過設置金融重建基金，此法除了能彌補存款保險機制或恐無法因應系統性風險之不足以外，重點在使問題金融機構之處理上，因備有足夠之財源而更具效率，得有效消弭金融風險、穩定金融秩序及改善金融體質。中央存款保險公司網站，〈行政院金融重建基金簡介〉，https://www.cdic.gov.tw/main_ch/docdetail.aspx?uid=138&pid=15&docid=83（最後瀏覽日：02/09/2020）。行政院金融重建基金設置及管理條例〔以下簡稱重建基金條例〕第 2 條、第 5 條、第 10 條及第 17 條指出，該基金之主管機關金管會應設置金融重建基金管理會（與金融重建基金評價小組）作為決策單位，並得委託中央存款保險公司〔以下簡稱存保公司〕以賠付方式處理問題金融機構。該基金辦理賠付後，在賠付之限度內，取得該金融機構對其負責人等之損害賠償請求權，且得授予訴訟實施權予存保公司，故得由存保公司以自己之名義，對應負賠償責任之人提起民事訴訟或聲請承當訴訟。本案中，重建基金已分別於 96 年 10 月與同年 11 月 7 日，賠付花蓮企銀之概括受讓人中信商銀 44.9 億元、2.12 億元，且於 97 年 8 月將其依據重建基金條例第 17 條第一項之損害賠償請求權，依同條第二項規定授予存保公司訴訟實施權，故本案原告為存保公司。

[204] 由於本文在此主要為探討董事監督義務、建置內控制度之責任等內容，故關於法人董事是否及如何對其代表人所為之侵權行為負連帶損害賠償責任之判決內容（即爭點二），本文暫且不論。惟相關事實理由與分析，請參見：曾宛如，前揭註 80，頁 192-193；蔡昌憲、陳乃瑜（2012），〈內部控制制度、董事監督義務及薪資報酬委員會——評最高法院九十八年度台上字第一三〇二號民事判決〉，《月旦法學雜誌》，203 期，頁 204-207。

[205] 臺北地方法院 96 年度重訴字第 1054 號民事判決、臺灣高等法院 97 年度上字第 1036 號民事判決。

doi:10.6342/NTU202000744

條之 1 規定[206]為據，而係依前開規定授權訂定之相關辦法（以下簡稱銀行內控辦法）第 4 條第一項[207]認定，負有確保建立並維持銀行內部控制與稽核制度之義務者，為合議制之「董事會」，並非董事長個人。故被告甲不因其曾任該行董事長，即單獨負有建立與維持內控制度有效運作之義務，縱該行內控制度有所缺失，亦難認其對該等義務之違反有故意或過失可言。

然而，最高法院則認為前揭本案第一審與第二審法院之見解，容有再為研求之處[208]。最高法院首先確認花蓮企銀遭課以罰鍰，應係其內控與稽核制度無法有效執行所致。再者，原審法院雖依上開內控辦法之規定[209]認為，負有確保建立並維持銀行內部適當有效內控制度義務者為合議制之董事會。惟花蓮企銀係於董事會議中，由全體出席董事授權董事長決定董事酬勞，且董事會本身無權利能力，故在無法以董事會為求償對象之前提下，則董事長或任何董事就內控與稽核制度無法有效執行之情形，得否認其無共同侵權行為而脫免損害賠償之義務？再者，被上訴人（按：一審被告）甲作為董事長，應瞭解相關股東會決議與章程規定，然其除未健全銀行內控制度外，甚且利用職務之便與內控疏漏自行以簽呈核發年終獎金予己與其他董事，是否均未預見該行將遭主管機關裁罰？倘其得以預見，能否內控制度應由合議制之董事會負責，即謂其個人無故意或過失，而無庸負損害賠償責任，殊值斟酌。故最高法院將本案原判決部分廢棄，發回高等法院為第一次更審。嗣高等法院判決認為本件上訴無理由，故駁回上訴後[210]，一審原告對前揭高等法院判決提起上

---

[206] 原告係以此條規定為依據，主張甲身為該行之董事長，負有使花蓮企銀內部控制及稽核制度有效執行之義務。銀行法第 45 條之 1：「銀行應建立內部控制及稽核制度；其目的、原則、政策、作業程序、內部稽核人員應具備之資格條件、委託會計師辦理內部控制查核之範圍及其他應遵守事項之辦法，由主管機關定之。」

[207] 銀行內部控制及稽核制度實施辦法第 4 條第一項：「董事會應負責核准並定期覆核整體經營策略與重大政策，董事會對於確保建立並維持適當有效之內部控制制度負有最終之責任。」惟現行法已為金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1：「金融控股公司及銀行業董（理）事會應認知營運所面臨之風險，監督其營運結果，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。」

[208] 最高法院 98 年度台上字第 1302 號民事判決。

[209] 前揭註 207。

[210] 臺灣高等法院 98 年度上更（一）字第 97 號民事判決。本審法院認為，金管會係基於其二度發文要求花蓮企銀應追回不當發放之獎金，惟該行函復之查核報告未能查核實情，並辯稱於法尚無不合，拒絕執行金管會追回獎金之要求，故其認為該行顯已無法有效執行內控與稽核制度等情事，始對該行處以罰鍰，並非以該行發放獎金為由處罰之。然而，金管會要求花蓮企銀追回獎金時，被上訴人（按：一審被告）甲已非該行董事長，無權代表該行執行追回獎金任務，金管會對該行之處罰，即與被上訴人甲以該行董事長身分發放獎金之行為無關，故不成立侵權行為。

doi:10.6342/NTU202000744

訴。最高法院則認為本件上訴有理由，廢棄原判決，第二次發回高等法院[211]。惟前開兩審判決理由與本文內容較無關，於茲不贅。

值得注意者係，高等法院於第二次更審之判決理由中，就被上訴人（按：一審被告）甲不當領取前開業績獎金之行為表示[212]，甲為銀行董事長依法應具專業資格，殊難諉為不知公司法、銀行法等相關規定，或不予查悉公司章程與財務年報以瞭解公司財務狀況。高等法院再指出，依據銀行法與相關辦法、該行內部稽核準則等規定，內部稽核制度之目的為查核評估內控制度是否有效運作，並適時提供改進建議，以協助董事會與管理階層確實履行其責任。故銀行應設置隸屬董事會之內部稽核單位，以獨立超然精神執行稽核業務，並應定期向董事會報告。惟花蓮企銀稽核處對董事長領取獎金之異常狀況，均無表示任何稽核意見，則該行並未落實稽核制度，洵無疑義。準此，甲自難諉稱不知公司連續兩年均虧損，故其利用職務之便與內控疏漏、事後稽核制度未能落實之際，違反該行章程與股東會決議發放董事長報酬之上限，領取性質為報酬之各項獎金等行為，與該行因被裁罰而受損害間，顯有相當因果關係。要言之，若非董事長甲溢領各項獎金與內控稽核之疏失，該行當不致被金管會裁罰，其自應就其加害行為負全部賠償責任。對於高等法院就本案為第二次更審之判決理由，最高法院亦認為於法並無不合[213]。

第二目　幸福人壽案

本案事實略為被告甲與被告乙曾分別擔任原告幸福人壽保險股份有限公司（以下簡稱幸福人壽）之董事長與總經理，依據保險業內部控制及稽核制度實施辦法（以下簡稱保險業內控稽核辦法）、幸福人壽之公司章程與業務分層負責表[214]等規定，董事長與總經理應有為幸福人壽建置、健全及監督內控內稽制度、法令遵循

[211] 最高法院 99 年度台上字第 1177 號民事判決。最高法院就前審認定被上訴人（按：一審被告）甲不成立侵權行為之判決理由指出，侵權行為之成立並不以行為人之行為係侵權結果發生之唯一原因為必要。不同侵權行為人之行為，苟係損害發生之共同原因，即可成立共同侵權行為。花蓮企銀遭金管會課處罰鍰，係因被上訴人甲擔任該行董事長期間，於違反該行章程與股東會決議之情況下，以董事長身分決定發放系爭獎金，暨該行未能查核實情並拒絕辦理追回獎金之共同行為所致，兩者間應有因果關係。故前審判決均非無再事斟酌之餘地。

[212] 臺灣高等法院 99 年度上更（二）字第 82 號民事判決。

[213] 最高法院 101 年度台上字第 1342 號民事判決。

[214] 幸福人壽保險股份有限公司之業務分層表規定：「董事長就年度法令遵循計劃之擬定及內稽內控之組織、職掌之調整均具有核決之權，並就總稽核、部室經理及相關人員，甚至各部室主管等之任免亦有核決之權；另總經理就定期辦理法令遵循自行查核亦具有核決之權限。」

doi:10.6342/NTU202000744

相關機制之職責，以確保業務執行不違反法令。基此，原告主張被告二人於任期內有：（一）辦理督導內部稽核作業時，未將主管機關、內部稽核單位及自行查核所提列之檢查意見或查核缺失事項列為營業與管理等各單位考評之重要項目，且未就各單位發生缺失之檢查意見與相關失職人員提供懲處建議等數項缺失，遭金管會核處 60 萬元之罰鍰[215]；（二）辦理一般業務違反保險法相關規定等多項缺失，遭金管會裁罰 120 萬元[216]等情事，顯見被告二人均未盡其前揭健全內控內稽相關機制與確保內控內稽執行有效性之責任，造成幸福人壽遭金管會裁罰共 180 萬元，有違反善良管理人之注意義務。故起訴請求被告二人應連帶賠償 180 萬元含依法定週年利率計算之利息。

對前述兩項裁罰內容與原告之請求，被告二人則依序主張：（一）被告乙係總經理，基於稽核應獨立制衡公司運作之原理，稽核單位之運作係直接對董事會負責，並不隸屬總經理管理，故其完全無權介入稽核單位之人事、設立、運作及所有稽核計畫執行相關事項。抑且該 60 萬元裁罰主要係針對稽核單位依職權辦理稽核事項之缺失，與董事長或總經理負責辦理法令遵循之自行查核顯屬不同之事，亦與兩人無關。（二）依裁處書之內容為形式判斷，金管會裁罰違反內控稽核辦法之主體係幸福人壽負責相關業務之承辦人員，而非被告二人。再者，原告並未逐一證明

[215] 104 年 3 月 20 日金管保財字第 10402502462 號裁處書。具體違反事實與理由為：「該公司辦理內部稽核作業經查有內部稽核人員未能提出實際受訓時數之具體證明，致年度專業訓練時數未達法定規定標準、未將主管機關、會計師、內部稽核單位及自行查核所提列之檢查意見或查核缺失事項列為營業及管理單位等各單位獎懲或績效考評之重要項目，且未就各單位發生缺失之檢查意見及失職人員提供懲處建議、稽核單位未積極督導受檢單位辦理缺失改善，即據以回覆尚依檢查意見辦理、稽核單位未定期評估各營業單位自行查核辦理情形等四項缺失，核與保險法第 148 條之 3 第 1 項授權訂定之保險業內部控制及稽核制度實施辦法第 7 條、第 9 條、第 16 條第 2 項及第 20 條第 1 項規定不符。」

[216] 104 年 3 月 20 日金管保財字第 10402503022 號裁處書。具體違反事實與理由為：「經查該公司有尚未經簽呈授權層級核准即辦理顧問合約事項；辦理董事長公務車購入作業有未依所訂『採購作業管理辦法』辦理詢價及議價比價等採購作業；辦理土地合建開發案未依契約徵提保證本票及合建保證金；未依所訂『上市櫃股票投資風險管理標準作業程序』辦理國內股票停損作業；薪資報酬委員會討論訂定董監事、經理人及專業顧問薪資報酬辦法，未評估相關人員績效目標達成情形或參考同業水準、未考量行業特性及公司業務性質即核發高階經理人短期績效獎金等情事；國外投資避險規劃案未由風險管理部門檢討訂定；未訂定外匯價格變動準備金提存、沖減之相關書面內部控制及作業處理程序；辦理投資用不動產減損作業，未對鑑價報告比較案例選用之妥適性及價格差異之原因詳實評估檢討；未對借、保戶有信用不良情形者予以降低貸款成數或拒絕受理、未於借戶申貸期間一年內辦理覆審作業，致未能瞭解借款用途與資金流向是否相符；有委外事項未向主管機關或其指定機關申報等多項缺失。」

doi:10.6342/NTU202000744

諸等業務事項必須或曾經呈核與被告二人核轉或核定，故無從認定被告二人有任何違反注意義務之過失。抑且，幸福人壽既已建置相關內部控制與稽核制度，以規範公司內部業務執行之程序，且透過分層之方式層層進行監督，被告二人身為有數百名原告公司之董事長與總經理，豈有可能就公司每一職員之每一業務均親自監督。故原告指摘被告二人未善盡監督義務之具體事實已不明確，又未說明內部控制與稽核制度缺失為何，更未交代制度缺失與未善盡監督義務間有任何因果關係存在，其主張顯無足採。

承前原告與被告之分別主張，本案爭點主要有：一、負責確保建立與維持公司內部控制與稽核制度之責任主體為何者？二、董事監督義務之具體內涵與範圍是否包括參與或實施業務單位員工之違法行為？

本案第一審法院判決原告敗訴，不得對被告二人請求損害賠償，其判決理由概為[217]：第一，內控內稽制度相關規範之規範主體為「保險業」，非擔任董事長與總經理之被告二人。法院指出，前揭兩份裁處書係金管會分別針對原告（即保險業）內部稽核執行專案檢查報告與一般業務檢查報告所載之內容，有違反保險業內控稽核辦法相關規定之情事予以裁罰。另參酌保險法第 148 條之 3 第一項規定及其立法理由[218]，該規定係為確保保險業健全經營，要求保險業應建立內部控制與稽核制度，防範財務危機之發生，並以保險業為建立與有效發揮內部控制與稽核制度為裁罰要件，所規範之對象俱為保險業，被告二人既非保險業，自無違反之適格性。第二，被告二人縱擔任原告董事長與總經理之職，惟其等未實際參與或實施裁處書所載之違規業務行為，難認有何未盡忠實義務、善良管理人注意義務之情事。法院先就系爭 60 萬元裁處書表示，該裁處書之裁罰基礎係原告稽核室辦理稽核業務有多項缺失，且參酌原告內部之分層負責表與稽核室稽核辦法等規定，足見原告之稽核業務應由稽核承辦人員先為簽呈及核轉，再經董事長核定、總經理備查。惟原告對該裁處書所載之違規事實，均未能提出相關證據資料，以證明被告二人實際參與該等業務或實施何項行為。再者，系爭 120 萬元裁處書之裁罰基礎則有未經簽呈授權層級核准、契約、公司內部規定及內部控制作業程序等規定，辦理各項業務之

[217] 臺北地方法院 105 年度訴字第 4239 號民事判決。

[218] 保險法第 148 條之 3 第一項：「保險業應建立內部控制及稽核制度；其辦法，由主管機關定之」，其立法理由謂：「內部控制及內部稽核制度係為健全保險業務經營及安全其財務之重要事項，為符法制，俾落實本制度之實施，爰於第一項明定之。」

doi:10.6342/NTU202000744

缺失。且再參酌前揭分層負責表與相關業務部門或單位之規定，各項業務均須由承辦單位先為簽呈與核轉，再經董事長核定或總經理核定、備查等。是被告二人雖分別擔任原告董事長與總經理，惟就該等違規事實，亦未見原告提出相關證據資料，證明其等實際參與該等業務或實施何項行為。綜上，原告既未能舉證證明被告二人有實施或參與前揭兩份裁處書所載違規事實，尚難徒憑被告二人擔任原告董事長與總經理之職，即遽認其等有何未盡忠實義務、善良管理人注意義務之情事。

然而，本案二審法院對於前揭兩爭點則有不同見解[219]。其觀諸保險法第 148 條之 3 第一項、保險業內控稽核辦法第 2 條及第 35 條第二項[220]等規定並指出，上開規定已明確規範保險業董事長與總經理應執行並管理內控稽核制度，以保障保險業及其保戶之權益，內容包括董事長與總經理應確保各項交易均經適當授權、公司資產受到保障、相關法令之遵循、制定風險管理程序及監理、追蹤並內控缺失改善情形。再者，董事之監督義務係屬善良管理人注意義務之一環，且監督義務之內涵不僅有董事會應依法令建置與運作內控稽核制度，尚包括其應適當監控董事長與高階管理階層人員是否確實履行，以確保內控制度之有效性，如此始可證明其已完全善盡監督義務。因此，被上訴人（按：一審被告）二人為上訴人（按：一審原告）依法令應建置與運作內控稽核制度，並應監督內部承辦人員是否已確實履行，以確保內控制度之有效性。抑且，被上訴人二人為上訴人之董事長與總經理，執掌有權指揮、監督內稽單位、公關室及相關業務部門承辦人員，有別於公司獨立董事之權責，則是被上訴人二人基於經理公司一切業務與職當內控執行之責，自不得以內控制度相關承辦人員之缺失，減免其違反公司法上善良管理人注意義務之責任。

---

219 臺灣高等法院 106 年度上字第 1343 號民事判決。

220 前揭註 218；保險業內部控制及稽核制度實施辦法第 2 條：「內部控制制度，指管理階層所設計，董（理）事會通過，並由董（理）事會、管理階層及其他員工執行之管理過程，其目的在於促進保險業之健全經營，以合理確保達成下列目標：一、保險業之營運係以謹慎之態度，依據董（理）事會所制定之政策及策略進行，以達成營運獲利、績效之效果及效率。二、各項交易均經適當之授權。三、資產受到安全保障。四、財務與其他紀錄提供可靠、及時、透明、完整、正確與可供驗證之資訊及符合相關規範。五、管理階層能辨識、評估、管理，及控制營運之風險，並保有適足之資本以因應風險。六、相關法令規章之遵循。」第 35 條第二項：「保險業因內部管理不善、內部控制欠佳、內部稽核制度及法令遵循制度未落實、對金融檢查機關檢查意見覆查追蹤之缺失改善辦理情形或內部稽核單位（含金融控股公司內部稽核單位）對查核結果有隱匿未予揭露，而肇致重大弊端時，相關人員應負失職責任。」

doi:10.6342/NTU202000744

第三目　鄉林建設案

本案事實略為被告鄉林建設股份有限公司（以下簡稱鄉林建設）核有「建設事業部總經理獎金辦法」（以下簡稱獎金辦法），明定總經理得依個案銷售金額按達成銷售目標之比例，請領業績獎金。原告甲依獎金辦法向鄉林建設請求其擔任總經理期間所經手銷售個案之部分業績獎金時，卻不獲鄉林建設之回覆，乃起訴請求鄉林建設應給付該部分業績獎金與因遲延給付所生之法定利息。惟原告甲自始未經鄉林建設依公司法第 29 條第一項第三款規定，經董事會適法決議選任之程序。抑且，該獎金辦法係鄉林建設總管理處長依董事長之指示而負責草擬者，並未經鄉林建設董事會決議予以通過，惟原告甲曾兩度依該獎金辦法之規定，經由鄉林建設之會計部門、財務部門、總管理處、總經理及董事長請領業績獎金。本案爭點主要有：原告甲與鄉林建設間是否具有公司法上經理人之委任關係[221]？該獎金辦法得否認為已經鄉林建設董事會決議通過且對兩造發生效力？[222]

本件訴訟之主要爭點雖非董事監督義務或內控制度，惟歷審法院於判決中，就董事監督義務之具體內涵仍有部分闡述，殊值參考。本案二審與終審法院[223]均指出，公司財務相關文件[224]雖均係由主辦會計人員負責編造，非屬董事會直接參與製作，惟因該等資料事關公司之營運與發展，故須經董事長或經理人簽核後，始得提交董事會，再提出於股東會。職是之故，為於會計人員編製後據實審核該等財務文件，以消弭違反法令或不實之內容，達成保障投資人之權益與監督經營者之目的，除了應由公司經營管理階層於董事會決議前，負責事先準備並提供相關文件予董事會成員參閱以外，董事會應以善良管理人之注意義務，負責監督並全盤兼顧經營管理階層之管理及其思慮未及之處，就提出之各該財務文件詳加審閱，避免怠忽監察之職責，此係董事會督導、事後據實審核之責任。準此，姑不論董事是否全員參與議決，該等財務文件既經董事會審查通過且須提出於股東會，諸位董事均應對內容之真實負責，否則將無以保障股東權益與公司利益。

---

[221] 前揭註 133。

[222] 臺中地方法院 97 年度重訴字第 515 號民事判決。

[223] 臺灣高等法院臺中分院 100 年度重上更（一）字第 27 號民事判決、最高法院 102 年度台上字第 360 號民事判決。

[224] 舉例言之，財務相關文件包括會計表冊、營業報告書、損益表、資產負債表、主要財產目錄、年報、股東權益變動表、現金流量表、盈餘分配表及虧損表等。

doi:10.6342/NTU202000744

第二款 事後法律策略之發展

觀諸既有司法實務判決對於董事監督義務有詳加著墨之案例，縱然結果顯示法院對於董事監督義務之具體內涵與操作，或謂尚在學習的階段，惟其內容仍提供相當豐富之發展素材。

第一目 建置與運作內控制度之主體

關於負有確保建立並維持有效內控與稽核制度者，究為「董事（長）個人」、係採合議制之「董事會」抑或「公司」，以及倘因未能建置或無法有效運作內控與稽核制度致使銀行受有損害時，應由前述何者承擔損害賠償責任之問題，雖未嘗沒有分歧，惟多數見解仍認為諸等應屬「董事個人」之責，意即應以個別董事之行為作為責任判斷之標準。

詳言之，地方法院與高等法院曾以「負有確保建立並維持銀行內部控制與稽核制度之義務者，為合議制之董事會，並非董事長個人。故被告甲不因其曾任該行董事長，即單獨負有建立與維持內控制度有效運作之義務，縱該行內控制度有所缺失，亦難認其對該等義務之違反有故意或過失可言」或「保險業應建立內部控制與稽核制度，防範財務危機之發生，並以保險業為建立與有效發揮內部控制與稽核制度為裁罰要件，所規範之對象俱為保險業，被告二人既非保險業，自無違反之適格性」等理由，認定應以董事會全體作為執行內控制度之主體。然而，誠如學者所言：「公司法雖採董事會集體執行業務制，然董事會之決議終究係出於董事個人義務之履行，故有無過失仍應就個別董事予以認定，不得以董事會之決議推諉之。[225]」最高法院對此亦多次予以指明：「董事會無權利能力，不得以董事會為求償對象之情形下，則董事長或任何董事就內部控制及稽核制度無法有效執行得否認其無共同侵權行為而脫免損害賠償之義務？」此外，最高法院判決亦有支持應以「董事個人」之行為作為歸責標準，是謂：「公司法第 194 條所規定之單獨股東權，旨在強化小股東之股權，使之為保護公司及股東之利益，得對董事會之違法行為，予以制止，藉以防範董事之濫用權限，而董事長或董事為董事會之成員，若董事長或董事恣意侵害公司及股東之利益，而為違法行為，是否仍應拘泥須為董事會之違法行

[225] 曾宛如（2010），〈董事忠實義務於台灣實務上之實踐——相關判決之觀察〉，《月旦民商法雜誌》，29 期，頁 148。

doi:10.6342/NTU202000744

為，始有上開規定之適用，而不得探求法律規定之目的，為法律的補充或類推適用，尚非無疑。[226]」因此，法令規範雖課予公司之權責機關，即董事會應建立內控與稽核制度之義務，惟制度之建立須仰賴人為，董事會之決議係出於董事個人義務之履行，故董事個人始為建置與運作內控制度之主體[227]，要無疑義。

第二目　董事監督義務類型之具體化

基於肯認董事個人應負有義務建置與運作內控制度之前提，法院就銀行、保險公司等金融機構之董事應如何履行該義務亦有闡釋。首先，銀行之董事依法須具備專業之能力與資格，包括其對於公司法、銀行法、內控稽核辦法，抑或公司章程等法令規章，均應有相當程度之瞭解。因此，董事會除了須依據前述法令規章之規定，建置與運作內控稽核制度外，董事因有權指揮與管理內稽單位與所有業務部門承辦人員，故其等均應適當監控管理階層人員是否確實履行，以確保內控與稽核制度之有效性。再者，董事基於其監督之責，對於業務單位人員所提出之財務、業務等相關文件，其應充分詳加審閱並就有疑處予以釐清或核實。意即，董事於董事會議決前，得主動要求各業務單位提供或應仔細審核各業務單位部門所提出之各項資訊，以消弭違反法令或不實之內容、保障股東權益與公司利益，始符已盡其善良管理人之注意義務。

第三目　小結——注意義務內涵之質變

金融機構相關內控內稽辦法均開宗明義指出，金融機構之董事會應認知營運所面臨之風險，監督其營運結果，並對於確保建立與維持適當有效之內控制度負有最終之責任，諸等董事監督內控制度之規定，或謂係呼應公司法下董事善良管理人注意義務內涵之「質變」。觀諸前揭花蓮企銀案、幸福人壽案及鄉林建設案等主體均為金融機構或大型公司[228]之實務案例，法院係逐漸肯認諸等大型公司董事會之個別董事成員應擔負建置與運作內控稽核制度、適當監控管理基層人員是否確實

[226] 最高法院 80 年度台上字第 1127 號民事判決。

[227] 蔡昌憲、陳乃瑜，前揭註 204，頁 218-219；曾宛如，前揭註 225；張心悌，前揭註 194。

[228] 鄉林建設事業股份有限公司之實收資本額約為新臺幣 98 億元，得認屬大型企業（中小企業認定標準第 2 條）。經濟部商業司商工登記公示資料查詢服務網站，https://findbiz.nat.gov.tw/fts/query/QueryCmpyDetail/queryCmpyDetail.do?objectId=SEMyMzY0MTgyMg==&banNo=23641822（最後瀏覽日：03/26/20202）。

doi:10.6342/NTU202000744

履行、充分審閱或要求業務單位人員提出之財務業務相關文件等職責。換言之，董事除了關注日常業務與營運績效以外，注意義務尚課予董事「監督責任」(oversight liability)，要求董事須經常性地監督公司各項業務活動是否符合法律或相關規範。

職是之故，現行公司法雖規範董事會屬公司之業務執行機關，惟吾等若由金融業法或法院判決實務觀察即可知，董事會之角色更似業務經營決策之擬定，抑或係建置與維持內部自律機制運作之監督者——內控制度與稽核之建置與監督執行即為示例。意即，金融機構董事會善良管理人注意義務之內涵，已從「親自執行業務、具體處理事務」，逐漸轉變為「董事會係委諸高階經理人所領導，由經營管理階層與業務單位職員所組成之團隊負責業務之執行，其則須職司訂定與運作一套監控系統（即內控與內稽制度），以此追蹤、檢視其等人員執行業務之情形與結果，並確保過程中沒有錯誤、舞弊或其他違法行為之發生」。基此，前述金融機構之內控內稽辦法關於董事就內控制度監督責任之規定，似即有跡可循。

第三項 輔助機關與配套措施

銀行內控制度之有效運作，除了須由董事會主要負責建置與監督外，尚須各級經營管理階層、內部各該業務單位職員等之通力配合實施，方能竟全功。然而，就董事會之職務內容與範圍而論，其應作成之各項決策往往涉及金融機構內部龐雜且繁複之事項，吾等應無法期待任何一位董事均能具備所有相關專業知識、經驗或獨自應付所有挑戰，故銀行內部即設有具備不同專業功能之輔助機關或配套措施，以協助董事會成員履行其所負內部控制相關責任與義務。對此，本文採擇人力資源部門、稽核與審計制度、公司治理人員等三項係與內控制度運作高度相關者，作為論述對象，並依序探討其等係如何影響：第一，銀行內部所有職員對於內控制度之遵循程度；第二，內控制度之效能評估與持續改善；第三，董事會就內控制度監督責任之效能等層面，期能完整建構金融機構內部控制之組織設計。

第一款 人力資源部門

於前揭諸如階層結構、權責劃分、經營政策及價值文化等較屬宏觀之探討外，正所謂「事在人為」，細究內控制度有效落實之關鍵，則在於佔金融機構組成員額顯著相當比例、或謂金融機構重要人事基礎之全體職員，故金融機構內部尚須設置與執行良好之人力資源相關管理部門與政策。換言之，探究金融機構公司治理議題

doi:10.6342/NTU202000744

時，除了董事會、經營管理階層、股東或其他利害關係人等以外，作為實際且高度參與銀行眾多日常業務運作者，諸如銀行辦事員、理專、外匯人員、徵授信人員、企金與消金專員等勞工[229]，其等之影響力均不容忽視[230]。

觀諸金融業內控制度相關辦法，無論係屬內控制度之組成要素，抑或為判斷內控制度有效性之項目，「人力資源」（Human Resource）均具有相當重要之地位[231]。金管會尚且指出，金融機構設計、執行、自行評估或接受會計師專案審查內控制度有效性時，即應考量包括人力資源在內之判斷項目[232]。人力資源既為內控制度組成子要素之一[233]，金融機構除了應訂定與執行人力資源政策，以延攬、培養及留用有能力之人才外；同時須訂定績效衡量與獎懲政策與制度，要求內部職員具相當能力以履行其各自對於內控制度之責任、達成目標[234]。換言之，內控制度作為促進金融機構健全經營，合理確保達成營運、報導及遵循等目標之機制，須由董事會、管理階層及所有從業人員等共同遵行始能落實[235]，意即內控制度之目標或制度目的之實現，均與人為因素高度且緊密連結。因此，人力資源部門應如何透過職位設計與配置、招募、選任、培育、訓練、考核、薪酬激勵等人力資源政策與管理策略[236]，以促使下至業務單位之所有職員、經營管理階層，上至董事會與高階管理階層其等共同遵循致發揮內控制度之制度機能，達成相關政策與目標，即值得關注。

相較於產品、財務或業務部門主管等性質屬「業務主管」（line manager，或稱直線管理者），其等享有得對於業務經營事項作成決策或命令之職權（authority）、指導其所管理之部署應如何執行職務，職責在於共同達成董事會與高階管理階層

---

229 勞動基準法第 2 條第一款（一、勞工：指受雇主僱用從事工作獲致工資者。）

230 *See* Howard Gospel & Andrew Pendleton, *Corporate Governance and Labour Management: An International Comparision*, *in* CORPORATE GOVERNANCE AND LABOUR MANAGEMENT: AN INTERNATIONAL COMPARISION 1, 30-32 (Howard Gospel & Andrew Pendleton et al. eds., 2005).

231 金融控股公司及銀行業內部控制及稽核制度實施辦法第 7 條第一款；保險業內部控制及稽核制度實施辦法第 4 條第一款；證券暨期貨市場各服務事業建立內部控制制度處理準則第 7 條第一項第一款；公開發行公司建立內部控制制度處理準則第 6 條第一項第一款。

232 103 年 10 月 1 日金管證審字第 1030039132 號令。

233 人力資源政策係屬內控制度五項組成要素中，控制環境之子要素。詳言之，控制環境係銀行業與金控公司設計與執行內控制度之基礎，其包括金融機構之誠信與道德價值、董事會與審計委員會之治理監督責任、組織結構、權責分派、人力資源政策、績效衡量及獎懲等。再者，董事會與經理人應建立包括員工行為準則在內之內部行為準則等事項。前揭註 231。

234 前揭註 232。

235 金融控股公司及銀行業內部控制及稽核制度實施辦法第 4 條第一項。

236 GARY DESSLER, A FRAMEWORK FOR HUMAN RESOURCE MANAGEMENT 16, fig.1.6 (4th ed. 2005).

doi:10.6342/NTU202000744

所訂定之政策或目標內容者，人力資源主管性質則屬「行政主管」（staff manager，或稱幕僚管理者），其定位與權限是為董事會、高階管理階層及各業務單位主管等提供人力資源之專業建議，或謂係業務主管之輔助角色[237]。意即，人力資源主管之重要功能在於協助各業務單位主管透過人事招募與選任等程序，盡可能「將正確的人放到正確的職位上」，並對其等施行適當之指導與訓練、薪酬與晉用等措施，提升職員之能力與品質，以協助各該業務部門或單位、經營管理階層及董事會達成組織策略與目標[238]。人力資源部門（或謂人力資源管理）對於內控制度之重要作用與影響，概有三個面向，包括：事前，職員之招募與聘任；事中，職員之培育與訓練；事後，職員之行為績效考核與薪酬等監督與激勵措施。以下依序述之。

第一目　事前之招募與聘任

唯有聘任適合且品行端正之人選進入銀行任職，始能確保其等於執行各項所負責之業務時，將恪遵銀行相關法令規範，以有效發揮內控制度之制度目的[239]。因此，人力資源部門應根據銀行業務單位或部門之勞動力規劃與現有職缺，依其職權執行招募與選才程序，為業務單位尋找適才且適性者，作為聘用職員之參考[240]。

質言之，此階段由人力資源部門負責謹慎篩選與評估合適之銀行職員，其原因包括提升組織績效、遏止職場上不正與偏差行為，以及控管人事成本等三個面向：第一，本身具有適當技能與適性之職員將對於組織績效產生正面貢獻；反之，缺乏專業能力之職員不僅無法有效率地執行職務，更將對於銀行之營運致生阻礙並使績效受損[241]。第二，據各項調查或統計指出，75%之職員或受訪者有自其雇主處偷竊至少一次之紀錄；33%至 75%曾有竊盜、破壞公物及蓄意曠職等行為；約有 25%知悉其他同事間有使用違禁藥品之情事；7%之受訪者表示其曾受有同事間所為之人身威脅；42%之女性受訪職員則表示其曾遭遇職場上性騷擾等，均顯示職場偏差係現行組織內部普遍發生且嚴重之情形[242]。因此，不適任之職員應於獲聘任職前即

237 *See id.* at 3.

238 *See id.* at 18. (“[P]lacing the right person in the right job.”)

239 *See* GEOFFREY PARSONS MILLER, THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 176 (2014).

240 *See* DESSLER, *supra* note 236, at 70-71.

241 *Id.* at 112-13.

242 Rebecca J. Bennett & Sandra L. Robinson, *Development of a Measure of Workplace Deviance*, 85(3) J. APPLIED PSYCHOL. 349, 349 (2000).

doi:10.6342/NTU202000744

先予以過濾並淘汰，若待其等進入金融機構大門後始察覺「櫥櫃裡的骷髏正在嘎嘎作響」，則為時已晚[243]。第三，招募與聘任職員之各項成本所費不貲，例如：聘僱並訓練一位辦事員之費用至少需五千美元、管理職則需用高達辦事員十倍之成本，該成本包括徵才費用、面試時間、資歷查核、車馬費及其他支出等[244]。除了前述之內部觀點外，金管會亦要求金融機構內部應依其業務性質與規模，依內部牽制原理訂定涵蓋所有營運活動，包括人事管理在內之政策與控制作業程序[245]，若金融機構未確實評估審視聘任人員之適格性，致董事會就人事管理之審查流於形式，金管會即得依職權處以罰鍰[246]。綜言之，謹慎且有效之招募與聘任職員之程序對銀行而言相當重要，不可不慎。

準此，銀行進行招募或錄用職員過程中，應有適當機制或方法執行「員工盡職調查程序」（Know Your Employee），以瞭解求職者之品行素質、專業知識、信用及財務狀況[247]。除了透過篩選履歷、面試約談及使用問卷或測驗等方式招募適任職員外，資歷查核（reference check）或背景調查（background investigation）亦係重要選才方法。原則上，透過履歷或其他由求職者所提供，抑或人力資源部門自行主動查詢或詢問之公開資訊，其得獲悉包括求職者之教育背景與工作經歷、人格特質與人際互動能力、工作能力與具體表現，以及作為雇主，聘用該名求職者之意願等訊息[248]。因此，執行資歷查核之目的即在驗證前揭各項求職者所提供之事實資訊是否為真，以及藉此揭露或發現其他有害於公司之背景資訊，例如犯罪紀錄或負面新聞

---

[243] DESSLER, *supra* note 236, at 112; MILLER, *supra* note 239, at 176-77 (“Afterwards, if skeletons rattle in the closet, the situation can get messy.”) 英美熟語（Idiom）「櫥櫃裡的骷髏」（Skeleton in the closet; Skeleton in the cupbord）係用以形容某人不欲為人知悉的秘密，且該秘密一旦曝光，將使他人對該某人造成極為負面或難堪的觀感，如同打開某人櫥櫃發現裡頭藏有一具骷髏——屍體上原有肉塊因為放置（隱藏）的時間過久，已完全腐爛而僅存一具枯骨。*See* Tim Bowen, *Phrase of the Week: To Have a Skeleton in the Cupboard*, ONE STOP ENGLISH, http://www.onestopenglish.com/community/your-english/phrase-of-the-week/phrase-of-the-week-to-have-a-skeleton-in-the-cupboard/145671.article (last visited Feb. 25, 2020).

[244] *See* DESSLER, *supra* note 236, at 113.

[245] 前揭註 232。金融控股公司及銀行業內部控制及稽核制度實施辦法第 8 條第一項第二款第六目；保險業內部控制及稽核制度實施辦法第 5 條第一項第八款。

[246] 109 年 2 月 14 日金管保產字第 10904520112 號裁處書。

[247] 銀行防範理財專員挪用客戶款項相關內控作業原則第 4 條。前揭銀行內控作業原則係銀行公會為協助同業強化內部控制，杜絕理財專員挪用客戶款項之情事，故依據金管會之指示所訂定者。

[248] WAYNE F. CASCIO, MANAGING HUMAN RESOURCES: PRODUCTIVITY, QUALITY OF WORK LIFE, PROFITS 210 (5th ed. 1998).

doi:10.6342/NTU202000744

[249]。簡言之，包括經理人、銀行辦事員、理財專員等在內之全體職員係為建立內控制度控制環境之基礎，其等專業能力與良好道德品行均係招募與聘任時所應考慮之點，故人力資源部門之職責係事前透過合理且有效之方式，充分瞭解應徵職員相關資訊與背景，作為各業務部門主管選任之參考依據。

第二目　事中之培育與訓練

對於業務單位與基層職員眾多之銀行或其他大型金融機構而言，提供完善且健全之員工訓練與進修發展主要係為提升職員之專業技能與執業素質，同時亦係有效控管人為相關風險、發揮內控制度等內部治理機制之效用所不可或缺者[250]。除了由各業務部門之管理階層，分別針對其員工施以基本業務相關技能與技術指導與訓練外，人力資源部門尚應負責對於銀行內部全體員工執行價值觀、法令遵循及職業道德相關之指示，其重要方法包括新進員工引導訓練（employee orientation）與行為塑模（behavior modeling）兩者，以下分述之。

（一）教育訓練——「新進員工引導訓練」之主要目的為管理階層或雇主提供公司重要背景資訊（例如公司規章、作業規定）予新進員工，確保新進員工得勝任其職務，或謂係新進員工瞭解並持續學習，以落實公司與其所任職之部門所期待之態度、標準、價值觀及行為典範等「社會化」（socialization）過程[251]。因此，該訓練之成功與否，即視人力資源部門得否與銀行內部所有業務部門之管理階層共同合作，達成以下目的：使新進員工得感到其本身係受公司歡迎，並開始建立對組織之認同感；對於組織之歷史背景、結構、文化、未來願景與使命、重要政策、作業程序及準則，均有較宏觀之瞭解；清楚掌握經營管理階層對所有員工在執行業務或其他各項行為表現上之期待等[252]。

再者，自風險管理之角度而論，誠如本文於前一章就法令遵循內控實務運作之內容所述，人力資源部門與法令遵循單位配合、共同向新進人員進行法令遵循相關教育訓練或在職人員之持續進修，係法令遵循得以準確落實、避免舞弊行為或風險

[249] DESSLER, *supra* note 236, at 134.
[250] *See* MILLER, *supra* note 239, at 181.
[251] *See* DESSLER, *supra* note 236, at 151.
[252] *See id* at 152; *see also* Howard J. Klein & Natasha A. Weaver, *The Effectiveness of an Organizational-Level Orientation Training Program in the Socialization of New Hires*, 53(1) PERSONNEL PSYCHOL. 47, 50 (2000).

doi:10.6342/NTU202000744

發生之重要方法。例如，為避免證券交易員過度追求績效，不當利用非公開之重大訊息進行交易，教育訓練之目的即在於提供明確之作業行為規範與指示，同時傳遞正確之價值判斷與誠信之組織文化予員工，以盡可能地減緩其不當逾越內控制度且降低舞弊行為發生之風險[253]。

質言之，銀行法令遵循單位、營業單位、資訊單位、財務保管單位及其他管理單位之法令遵循主管，其等每年皆應參加由金融主管機關或銀行業自行舉辦十五小時，包括各項專業課程、金融相關法律常識與最新修正之法令、風險管理、新種業務或新種金融商品等項目在內之教育訓練[254]。再者，縱謂負責確認銀行內部各項作業與管理規章、營運活動，以及董事會與管理階層建立之內控制度三道防線架構係符合最新法規者[255]；抑或對銀行內部各單位人員進行法規與內控制度相關訓練，主要係由法令遵循單位負責為之[256]。然而，基於金融機構各單位或部門間存在明確之層級與職能劃分，且人力資源部門本身因具備人力資源之訓練與潛能開發、執行員工培訓策略等專業能力，即應由其扮演授課單位與業務單位（被授課者）間溝通之橋樑，負責籌劃教育訓練、聯絡並安排特定單位或部門[257]對業務單位進行授課，如此始符合金融機構內部之組織層級與權責劃分，並得把關與確保訓練之品質。

（二）行為塑模——為確保銀行職員執行各項業務時，均能依循其任職之業務單位所訂定之作業程序規範與內控制度，人力資源部門與業務單位之管理階層得

253 MILLER, *supra* note 239, at 182.

254 金融控股公司及銀行業內部控制及稽核制度實施辦法第 32 條第六項。再者，金管會為執行前條項在職教育訓練之規定，認定辦理金控公司與銀行業內部稽核人員之職前與在職訓練、法令遵循人員在職訓練之訓練機構，並確保訓練之品質，其訂定有「金融控股公司及銀行業訓練機構審核原則」。該原則第 3 條指出，訓練範圍包括：（一）職前訓練：應涵蓋各項專業課程、電腦稽核及金融相關法律常識等；（二）在職訓練：應著重風險管理、新修正之相關法規及新種金融商品。

255 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條第一項第二款。

256 金融控股公司及銀行業內部控制及稽核制度實施辦法第 34 條第一項第五款。

257 除了銀行內部設立之法令遵循單位或風險管理部門外，經金管會依金融控股公司及銀行業訓練機構審核原則指定或核准，現得辦理金控公司與銀行業相關人員教育訓練之外部主管訓練機構有：財團法人台北金融研究發展基金會（105 年 6 月 17 日金管銀國字第 10500127920 號函）、財團法人保險事業發展中心（96 年 7 月 27 日金管銀（二）字第 09600292280 號函）、社團法人中華民國內部稽核協會（96 年 7 月 12 日金管銀（二）字第 09600286440 號函）、財團法人中華民國會計研究發展基金會（96 年 5 月 28 日金管銀（二）字第 09600149690 號函）、財團法人台灣金融研訓院（95 年 8 月 8 日金管銀（二）字第 09500307181 號函）、中華民國電腦稽核協會（95 年 8 月 8 日金管銀（二）字第 09500307182 號函）及財團法人中華民國證券暨期貨市場發展基金會（95 年 8 月 8 日金管銀（二）字第 09500307180 號函）。

doi:10.6342/NTU202000744

透過「行為塑模」此訓練方法，使銀行誠信經營文化、職業道德、內控制度或其他政策之遵循等，具體落實於日常業務活動當中。行為塑模指先向受訓者（即職員）直接演示組織內部認屬正確或標準之作業或行為方式，再由受訓者親自演練前揭示範，最後由受訓者之主管根據受訓者之表現給予回饋之過程[258]，目標在於養成並強化職員遵守作業標準與行為規範之意識，並得具體落實於日常業務之執行過程當中。

無可否認，內控制度之完善建置與充分運作至多僅能合理確保銀行得以達成營運、報導及法令遵循等目標，尚無法完全保證各項業務之執行不會有任何錯誤或疏漏發生，究其原因主要係人員不當僭越或蓄意規避內控程序所導致。職是之故，為使銀行業務單位職員得充分瞭解內部控制實務所涉控制點之疏漏與緣由，俾利其等自我約束與檢視是否有類似行為情狀，以改善並強化內部控管作業[259]，前述之職前或在職訓練內容亦得納入相關案例，藉此具體指明與形塑各職員於執行職務時，其等所應遵循之正確行為模式。抑且對此，主管機關金管會為加強宣導並協助銀行從業人員確實改善其內控缺失，其除了定期依金融業別篩選出重要之制度面或具普遍性質之內控制度相關檢查缺失並公告外[260]，尚且要求各該裁罰案件所涉缺失或現負責案關業務之承辦人員、直屬主管及單位法遵人員等[261]，均應額外參加裁罰案例研習或與系爭受裁罰業務相關之專業課程訓練，據以落實執行教育訓練機制。

綜言之，經由教育訓練與行為塑模等方式指引銀行內部所有員工於執行個人職務時，充分知悉並遵循內控制度與相關作業程序，相較於透過主管機關裁罰方於事後改善員工之違法行為者，前者屬較佳之作法。唯有如此始能促使職員主動積極落實正確且良善之行為準則，而非被動消極行事以免於遭受裁罰或不利後果[262]，以有效達成形塑良好組織文化、約束自身行為等目的。

---

258 *See* DESSLER, *supra* note 236, at 166.

259 銀行防範理財專員挪用客戶款項相關內控作業原則第 3 條。

260 105 年 8 月 11 日金管會檢局（制）字第 1050150280 號函。

261 105 年 12 月 7 日金管會檢局（制）字第 1050150456 號函。

262 *See* G30 BANKING CONDUCT & CULTURE, *supra* note 144, at 41.

doi:10.6342/NTU202000744

第三目　事後之考核與激勵

為提供業務單位職員，甚或銀行內部所有成員確實遵循內控制度與相關作業程序之誘因，人力資源部門須依其職權訂定公正且客觀之績效考核標準與適當之薪酬制度。首先，為避免各該單位職員追求績效表現而過度追求風險，甚至逾越或規避內控制度作業規範以獲取高額報酬，銀行內部之績效評估與管理機制不應僅止於關注職員個人所獲營利數字，尚應考量包括職員行為、消費者回饋、服務品質等非財務性質之表現，以減緩過度激勵措施或將對個別職員所生之負面不利影響[263]。例如於 2016 年，美國富國銀行（Wells Fargo & Co.）之業務單位職員為謀達成銀行內部銷售目標，其等即不當利用客戶個人資料虛設幾近 350 萬筆銀行帳戶與信用卡，惟該銀行之董事會與高階管理階層竟未能察覺諸等情事並迅速導正該行已漸趨扭曲之績效至上組織文化，不僅造成高達 5300 名職員因涉入此類不當行為而遭該行開除，該行甚至招致主管機關課予 1.8 億美元之罰鍰，同時命該行更換其董事會成員[264]。由此可知，銀行內部訂定之績效管理與獎酬等激勵措施應避免使之與量化銷售數額間形成緊密連動關係，避免業務單位職員為達成績效目標致發生行為，此除係為消除前述對於職員不必要之壓力外，亦可協助職員於提供各式金融商品或服務時，均得以滿足消費者或客戶之需求為優先考量[265]。

綜言之，績效評估與管理之功能與目的除了在於提供各級經營管理階層明確資訊，以作為決定業務單位職員調整報酬與晉升之判準以外，經營管理階層尚得就評估結果，判斷是否及如何對於業務單位職員之缺失或不正行為採取糾正或改善措施，確保所有職員均得依據銀行內部作業行為準則或規範行事[266]。最後，自組織與人力資源發展角度而論，因績效評估可顯示並提供個別職員檢視其執行職務時所展現之強項與弱點，進而協助職員作成完善之職涯發展規劃[267]，得有效提升人力資源之整體素質，更能達成組織內部各項目標。

第二款　稽核與審計制度

緣於銀行之董事會與高階管理階層須負責合理確保內控制度持續有效運作、

---

263 *See id.* at 40.
264 *See id.* at 41.
265 *See id.*
266 *See* DESSLER, *supra* note 236, at 186.
267 *See id.*

doi:10.6342/NTU202000744

衡量整體營運之效率，故其等須仰賴稽核與審計單位協助查核與評估且適時提供內控制度之改進建議，作為檢討並修正內控制度之重要依據。誠如本文前述，內控制度作為銀行內部建置用以達成營運、報導及遵循等各項管理目標之動態程序或作業規範，其應具備明確內部控制三道防線架構，基此，為使內控制度得持續有效實施，即須設有相應之查核與監控機制，主要包括三個層面：第一，銀行內部自行查核與內部稽核制度。第二，外部審計與專案審查之委託。第三，金融主管機關之金融檢查。以下分別述之。

第一目　自行查核與內部稽核

細究之，銀行內部稽核稽核制度與組織又可分為自行查核作業與內部稽核。

（一）自行查核——自行查核作業指銀行內部業務、財務、資產保管、資訊等內控制度第一道防線之單位，應由其單位主管指定非原經辦人員，採取事先保密之方式，並在該主管所指定適當負責人之監督執行下，對單位業務與相關作業程序之實際執行情形進行查核[268]。此係俾利管理階層儘早發現業務執行過程是否存在缺失或疏漏，並得即時予以糾正與改善，同時經營管理階層得將各單位辦理業務自行查核與改善之情形，作為內部稽核單位檢查與獎懲、經營績效考核之重點項目[269]。

誠如本文前述，業務單位作為內控制度架構之第一道防線，倘若有理財專員、交易員或任何居於第一線之前臺員工恣意僭越內控制度之規範，內控制度即無從有效控管風險。故為確保內控制度之持續有效運作，業務單位之管理階層應考量其業務之風險特性與各項作業程序之控制重點，負責訂定自行查核內容與程序[270]，並定期執行之[271]。舉例而言，為杜絕金融機構之職員私自代客戶辦理存款、提款，致孳生不當挪用客戶款項之情事，銀行公會除針對銀行理財專員訂有相關內控作業原則以為規範外[272]，就金融機構不定期派員赴外收付款項、接受客戶傳真指示扣款

[268] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 25 條第一、三項。

[269] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 26 條第一項。

[270] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 14 條第一項第二款。

[271] 質言之，各單位之業務自行查核可分為一般自行查核與專案自行查核兩種，前者係指業務單位應依照管理階層訂定之自行查核計畫、工作分配及查核結果登載表等所列項目，至少每半年一次，為全面性之查核；後者則係至少每月一次，查核前述自行查核報告所載內容至少三項目以上。再者，無論係何種性質之自行查核，各該自行查核報告均須作成工作底稿，併同所有相關資料，至少留存五年備查（金融控股公司及銀行業內部控制及稽核制度實施辦法第 25 條第一、四項）。

[272] 同前註 247。

doi:10.6342/NTU202000744

等兩業務訂有內部作業程序範本[273]。因此，為管控職員辦理存款業務之行為，銀行內部應建立包括以下程序或流程：審慎篩選與指定經辦人員、業務執行與記帳人員須分別派任、每日收付款項之當日帳務處理、客戶授權書之簽報與核准、取款憑條或其他扣款憑證於備查簿之登記或電子化記錄、取款憑條與印鑑之驗印與核對程序等，亦須加強對於所屬職員與客戶之宣導。

除了前述存款業務以外，銀行內部尚應就出納、匯兌、授信、外匯及其他新種金融商品等訂定業務規範與作業處理流程[274]，故個別業務單位所定期執行之自行查核制度即係確保諸等內部控制相關規範或程序是否有效且妥適運作所不可或缺者。準此，為利於自行查核功能得有效發揮，其首先應由非原業務單位之經辦人員以事先保密的方式為之，業務單位辦理自行查核須訂定包含全盤業務之自行查核訓練計畫，查核之時程亦應安排於不同月份。再者，由於自行查核時所應考量之項目係以各該業務單位之業務負荷與風險特性分別予以調整者，與內部稽核有別，故自行查核報告與工作底稿應不得沿用內部稽核。綜言之，無論係各業務規範與作業流程或自行查核計畫之訂定、業務單位執行人員與自行查核經辦人員之選任、查核報告與工作底稿之撰擬、查核時程期日之擇定等，均應由個別業務單位之經營管理階層負責籌劃與監督是否已確實執行，並須確實留存各項資訊以備查驗，方得避免各項稽察流於形式，始能有效發揮內控制度控管第一道防線風險之功能。

（二）內部稽核——作為內控制度運行時不可或缺之重要配套措施，設置內部稽核單位之目的與功能即在於協助董事會與經營管理階層檢查與覆核內控制度之缺失、衡量營運之效果與效率，以適時提供修正或改進建議，確保內控制度得持續有效實施[275]。故為協助各級管理階層善盡其責任，內部稽核人員均應維持獨立性與客觀性[276]、本於誠實信用原則執行業務[277]，其主要職責包括：檢查保護資產安全之

[273] 金融機構代客戶辦理存提款作業範本第 1 條。

[274] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 8 條第一、三項。其他由金融機構同業公會所訂定之內控制度相關作業程序之標準範本尚有：中華民國銀行公會金融機構開戶作業審核程序暨異常帳戶風險控管之作業範本、中華民國期貨業商業同業公會期貨信託事業內部控制制度標準規範等。

[275] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 9 條。

[276] 審計準則公報第二十五號「內部稽核工作之採用」第 5 條。

[277] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 13 條第一項。再者，內部稽核人員執行業務尚不得有隱飾或對金融機構之營運、報導或相關法令規章遵循有直接損害利害關係人之情事為不實或不當之揭露；為己圖利而為對外洩露所取得之資訊等逾越稽核職權範圍以外之行為或有

doi:10.6342/NTU202000744

措施是否適當、會計與業務資訊是否可靠與完整、各項資源之運用是否具效率、各項業務運作是否按照既定政策或計畫執行並達成預期目標等[278]。

基於內部稽核執行之頻率與實效係判斷現行內控制度之規定與程序是否適當之關鍵，故銀行內部稽核單位對於國內營業、財務、資產保管與資訊單位每年至少應各辦理一次一般查核與專案查核[279]，且每半年應對於子公司之財務、風險管理及法令遵循辦理一次專案業務查核[280]。除了前揭法令規定之查核事項與時程外，銀行內部尚得針對特定業務單位職員或交易行為建置適當之控管措施並作為內部稽核查核重點事項，例如為防範理財專員不當挪用客戶存款或擅自進行交易或為相關不當行為，銀行內部得建立客戶交易檢核制度[281]。因此，為確保該控管措施得充分落實，內部稽核單位得以月、季、半年或年度為頻率，主動或與管理階層單位配合進行客戶帳戶交易明細與餘額確認機制之抽樣查核。抑或，為避免理財專員與客戶有私下不當之資金往來，銀行內部除得建置帳戶監控機制與異常交易舉報機制外，內部稽核單位亦得定期或不定期抽查各分行理財專員之辦公處所，以防免有理財專員私下保管客戶個人身分證明物件之情事[282]。又為對於業務單位職員進行有效之防弊調控舉措，業務單位內部得訂定職員之休假與輪調機制[283]，前者係利於內部稽核單位得於職員休假期間，抽樣查核檢視職員日常業務執行之紀錄或資訊；後者則係為避免有特定職員因長期服務同一客戶或任職於相同單位，致衍生弊端卻無法即時查覺之情況，故對於長期任職相同單位已達一定年資之職員，內部稽核單位應確保業務單位管理階層已訂定且落實妥適之職務調動程序、調整負責客戶帳戶對象或加強職員與客戶往來情形之查核等防弊措施。

此外，內控制度未能確實建立或未獲徹底落實，除了須檢討內部稽核單位是否未善盡其職責以外，更須留意與關注者為，因內部稽核單位係隸屬於董事會與高階

其他不正當之情事；自身有利害關係案件而未予迴避；直接或間接提供、承諾、要求或收受所屬金融機構從業人員或客戶不合理或不正當利益；未配合辦理主管機關指示查核事項或提供相關必要資料等情事或行為。

[278] 審計準則公報第二十五號「內部稽核工作之採用」第 4 條。

[279] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 15 條第一項。

[280] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 16 條第二項。

[281] 銀行防範理財專員挪用客戶款項相關內控作業原則第 7 條。

[282] 銀行防範理財專員挪用客戶款項相關內控作業原則第 9 條。

[283] 銀行防範理財專員挪用客戶款項相關內控作業原則第 6 條。

doi:10.6342/NTU202000744

管理階層之組織部門，故內部稽核單位是否受到其等控制或影響，導致該單位人員無法以超然獨立之精神執行稽核業務，以充分發揮查核與評估內控制度之職能[284]。詳言之，內部稽核單位於銀行內部係隸屬於董事會之組織層級，其須至少每半年向董事會與審計委員會報告稽核業務[285]。至於負責綜理稽核業務之總稽核之職位係等同於副總經理，其聘任、解聘或調職則須分別經審計委員會與董事會全體成員之同意[286]，且內部稽核人員之任免、升遷、獎懲、輪調及考核等人事相關事項均應由總稽核簽報經董事長核定後辦理[287]，故內部稽核單位於組織中之定位或可謂相當程度繫諸於董事會之決策。換言之，判斷與維持內部稽核單位之客觀性時，除了須視銀行是否訂定禁止內部稽核人員對其本身曾經負責或即將負責、或其親屬擔任重要或敏感性職務之營運活動加以稽核等維持內部稽核客觀性之政策外[288]，尚應考量內部稽核單位於銀行內部之組織地位，包括內部稽核單位是否係直接隸屬於高階主管、得否逕向董事會報告稽核業務執行情形，以及內部稽核主管之任免是否由董事會決定等[289]。

職是之故，為使內部稽核單位得依其職權確保內控制度之有效運作，或須強化董事會或應賦予其監督之功能，促使董事會成員應擔負有效監督內控制度之責任，亦即呼應本文強調董事會應定性為銀行內部監控機關，而非業務執行機關之論述。舉例言之，前揭兆豐商銀紐約分行裁罰案中，經金管會認定其內部稽核單位核有：未能確保內控制度與法令遵循等事項之查核品質、未能將檢查報告之重要缺失及時提報予董事會，以利其督促海外分行即時改善缺失、未能將美國金融主管機關（即紐約州金融服務署，DSF）極有可能採取監理處分行動（Enforcement Action）之重大資訊使董事會即時獲悉等缺失[290]。然而，依據內部稽核單位之職權，其應就內部控制重大缺失或違法違規等情事向管理階層提供改進建議，若該等建議不為管理階層所採納將肇致所屬銀行面臨重大損失時，均應立即作成報告陳核董事會

[284] 蔡昌憲（2012），〈從內控制度及風險管理之國際規範趨勢論我國的公司治理法制：兼論董事監督義務之法律移植〉，《臺大法學論叢》，41 卷 4 期，頁 1835。

[285] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 10 條第一項。

[286] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 10 條第三項。

[287] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 10 條第五項。惟若涉及其他管理、營業單位人事者，則應事先洽商人事單位轉報總經理同意後，再行簽報董事長核定（同條第五項但書）。

[288] 審計準則公報第二十五號「內部稽核工作之採用」第 11 條。

[289] 同前註。

[290] 105 年 9 月 14 日金管銀控字第 10560003851 號處分。

doi:10.6342/NTU202000744

並通知審計委員會[291]，以利於銀行之董事得有效作成決議採取積極作為，抑或另行依據金融主管機關之要求，訂定重大缺失改善方案或可能採行之處分措施[292]。準此，鑑於銀行之董事會所負對於內控制度與營運結果之監督責任[293]，內部稽核單位之重要功能即係作為監督機關之輔助角色，提供內控制度運作之查核結果與改進建議，俾利董事會確保內控制度得持續有效實施，以充分履行其監督責任。

第二目　外部審計與金融檢查

誠如本文前述，金融機構作為主管機關高度監督與管理之業別對象，其經營與運作尚涉及諸如服務實體經濟、金融市場之秩序，以及整體經濟發展之穩定等外部效應。因此，就金融機構內控制度之執行情形等，除經由前述自行查核與內部稽核等制度之檢視以外，尚須透過外部審計（External Auditor）與主管機關所為之金融檢查等外部、公正、客觀第三方，對於內部控制三道防線整體制度面之建立與運作予以查核，並適時提出專業之改善意見。質言之，相較會計師係基於私法契約關係對其客戶提供財務報表查核、簽證等服務，外部審計人員則基於「公眾角色」（public role）之地位，就受查對象之財務報表與控制為獨立審查，故係對於投資者或其他使用經其審閱之財務報表或資訊之利害關係人負有一定義務[294]，使其重要性在致受外部高度行政監管之金融機構即愈發明顯。

質言之，諸如內部會計師或律師作為提供專業會計或法律服務或意見者，係以其當事人之最大利益為首要考量，同時並對該客戶案件負有保密相關義務，惟外部審計人員或獨立簽證會計師於查核驗證公司對外揭露之各項財務狀況相關資訊時，不僅對該公司（即其客戶）負有私法上僱傭關係所生之責任，尚應對於該公司之債權人、股東及投資大眾負有公共責任（public responsibility）與最大忠誠義務[295]。意即，該「公共守門人」（public watchdog）職能要求外部審計人員須隨時維持完全獨立性於其客戶，並應對公眾信賴負完全之忠實義務（complete fidelity）[296]。

原則上，外部審計之功能主要在於發現財務報表是否存在不尋常或詐欺情形，

---

[291] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 42 條。

[292] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 42 條之 1。

[293] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 5 條之 1。

[294] *See* MILLER, *supra* note 239, at 338-39.

[295] United States v. Arthur Young & Co., 465 U.S. 805, 817-18 (1984).

[296] *Id.*

doi:10.6342/NTU202000744

意即由審計人員依據一般公認會計原則，對於銀行業出具之年度財務報表等，基於重大性之考量，查核各項財務性資訊是否允當表達並表示其意見。然而，隨著銀行編製與揭露之資訊愈趨多樣，並不僅侷限於財務性資訊，尚包括環境、社會及公司治理（ESG）與企業社會責任報告書等非財務性資訊，故會計師對於銀行業之外部查核尚有針對內控制度所為者，包括銀行申報予主管機關報表資料之正確性、內控制度與法令遵循執行之情形、備抵呆帳提列政策之妥適性、個人資料保護、洗錢防制與資恐打擊機制等之查核[297]。再者，金融主管機關為確保金融機構均已妥適建立與實施內控制度三道防線、降低金融機構重大經營風險之發生，故須定期以抽查方式實地為金融檢查，評估其資本適足性、資產品質、管理能力、盈利狀況、財務與業務面經營方針、風險管理與法令遵循制度、消費者保護等層面之具體執行情形。惟囿於人力、物力等成本之限制，金融檢查之實施並非在於確保個別金融機構萬無一失，毋寧係著重整體金融市場之秩序與穩定。

準此，無論係外部審計人員或金管會檢查局，對於銀行或其他金融機構依金融業法行使檢查權或資料調閱權時，銀行有提供其所需之財務報表、業務文件、財產報告、交易憑證、帳務簿冊、會議記錄、電子資料檔或其他有關資料與報告之義務[298]，俾利外部查核單位對於銀行之財務、業務及整體營運情形執行檢查、提出修正建議事項。然而，究其實質外部審計或金融檢查均屬外部監管措施，固然該等場外監控之實施有其存在必要性係毋庸置疑，該等措施之成效仍高度仰賴銀行之運作是否遵循相關法令規範，抑或其所出具之財務業務相關報導是否忠實等內部整體行為，或謂內控制度是否有效達成營運、報導及遵循等三大目標。因此，仍須透過加強落實董事會與高階管理階層等對於內控制度之監督責任，敦促其等確實依據由外部審計與金融檢查所提出之檢查意見予以改善並持續追蹤之，始能有效發揮作為配套措施之外部金融監理功能，同時達成降低監理成本、提升監理效率等附隨效果。

[297] 金融控股公司及銀行業內部控制及稽核制度實施辦法第 28 條第一、二項。

[298] 金管會組織法第 5 條第一項；金融控股公司及銀行業內部控制及稽核制度實施辦法第 30 條第一項第一款；金融控股公司法第 52 條第一項；銀行法第 45 條第一項；保險法第 148 條；票券金融管理法第 45 條第一項；信託業法第 42 條第一項；期貨交易法第 98 條第一項；證券交易法第 38 條、第 38 條之 1。

doi:10.6342/NTU202000744

第三款 公司治理人員

為加強公司內部對董事會行使職務之支援、促使董事會發揮其應有之功能，以有效落實公司治理，於 2019 年始，金管會即強制要求金控公司、銀行、票券商、保險公司、上市櫃綜合證券商等金融機構內部應設置「公司治理人員」，作為提供董事與獨立董事取得其等行使監督職務所需資訊或其他必要之協助者[299]。質言之，董事為履行其所負之監督責任，即須於掌握充分資訊之前提下，依其職權作成即時且正確之決策，故董事會應於公司內部建置一套「資訊與報告系統」（information and reporting systems），始能有效獲取各項所需之資訊[300]。意即，董事或高階管理階層等成員履行其義務之前提，即在於獲有充足之「治理資訊」，並以此為判斷並作成有效之監督決策[301]。

是故，銀行等金融機構應依公司規模、業務情況及管理需要，配置適任與適當人數之公司治理人員，並指定公司治理主管[302]一名作為最高主管，負責辦理董事會與股東會之會議事宜、製作董事會與股東會之議事錄、協助董事就任與持續進修、提供董事執行業務所需資料、協助董事遵循法令等公司治理相關事務[303]。簡言之，

---

[299] 金融監督管理委員會證券期貨局（2018），《新版公司治理藍圖（2018-2020）》，頁 17-18。任何公司內部均需有一名得全面掌管內部行政程序事項、確保董事會於執行公司業務時遵循相關法令規範，以及於公司治理環節得發揮重大影響力之人。對此，英國、新加坡、香港、澳洲等英系國家均設計了「公司秘書」（Company Secretary）一職，並立法詳盡規定公司秘書之資格、職務及相關責任，且建立制度完善之協會組織作為培訓公司秘書之重要機構。美國（及其聯邦下由各州訂定之州法）雖未將公司秘書予以法制化（美國則稱公司秘書為 “Corporate Secretary”），惟隨著諸如《2002 年上市公司會計改革與投資者保護法案》（Public Compant Accouting Reform and Investor Protection Act of 2002）與《華爾街改革與消費者保護法案》（Dodd-Frank Wall Street Reform and Consumer Protection Act）等強調公司應改善且加強公司治理結構、應設置熟悉相關法律規範之人員，為公司提供良好公司治理服務之法案相繼出現，公司法學者與實務即正式賦予此職一新名稱，謂為「公司治理長」（Corporate Governance Officer，CGO），據以凸顯其於公司內外所應擔負之重要責任。*See* GERTRUD ERISMANN-PEYER ET AL., THE INSIDER'S VIEW ON CORPORATE GOVERNANCE: THE ROLE OF THE COMPANY SECRETARY 43-44 (2008); Mark R. Gilbert & James Lundy, *Demand Is Growing for a Chief Governance Officer*, GARTNER 1, 1 (2003), https://www.bus.umich.edu/kresgepublic/journals/gartner/research/117400/117465/117465.pdf.

[300] *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 970 (Del. Ch. 1996).

[301] 蔡昌憲（2018），〈從公司法第一條修正談公司治理之內外部機制——兼論企業社會責任的推動模式〉，《成大法學》，36 期，頁 111，註 46。

[302] 臺灣證券交易所股份有限公司上市公司董事會設置及行使職權應遵循事項要點第 21 條；金融控股公司治理實務守則第 49 條之 2；銀行業公司治理實務守則第 44 條之 2；票券金融公司公司治理實務守則第 44 條之 2。

[303] 公司治理主管應取得律師、會計師執業資格或於證券、金融、期貨相關機構或公開發行公司擔任法務、法令遵循、內部稽核、財務、股務或公司治理相關事務單位之主管職務達三年以上（臺灣

doi:10.6342/NTU202000744

公司治理人員之職能主要可包括「守門人」與「橋樑」等兩層面：前者指公司治理人員本身對於公司治理相關法律之專業能力，得有效協助董事會與高階管理階層遵循法令規範，減少爭議案件之發生；後者則係指公司治理人員具備統整公司資訊之功能，除了得聯絡董事會與管理階層；股東、債權人及利害關係人；公司（金融機構）與金融主管機關等群體，抑或促進其等間之溝通以外，亦得協助獨立董事等外部監督人員獲取必要之資訊以行使其職權，有利於強化獨立董事制度[304]。

質言之，設置公司治理人員對於落實內控制度與董事會監督責任之重要因素，或可體現於公司治理人員應具備之專業性與獨立性兩點。第一，參酌外國立法例與實務經驗，公司治理人員之背景多以法律專業居多、其次為財務會計[305]，可知公司治理人員主要職責在於協助確保董事會甚或公司內部各項業務之運作係符合法令規範，以及協助董事會履行審閱與決議通過財報等義務。公司治理人員所具備可謂係綜合性專業能力，包括公司營運發展、內部權責劃分、董事會義務與職能、法令遵循、財務會計與商業決策、策略與風險管理等[306]，故作為公司守門人之角色或稱公司治理之中流砥柱，其得充分協助董事會建立並隨時因應環境之變遷檢討內控制度。第二，縱謂相較獨立董事，公司治理人員係屬公司內部人，須充分瞭解公司內部情況，並與內、外各單位部門間保持良好且密切之合作關係，取得董事會所需之治理資訊，惟作為公司橋樑之角色，公司治理人員仍須具備相當獨立性，始能本於前述專業提供各項治理建議，且防免不當之影響或利益衝突[307]。準此，鑑於金融

證券交易所股份有限公司上市公司董事會設置及行使職權應遵循事項要點第 23 條；金融控股公司治理實務守則第 49 條之 4；銀行業公司治理實務守則第 44 條之 4；票券金融公司公司治理實務守則第 44 條之 4）。

304 獨立董事雖具備公司所需之專業知識或經驗，惟基於對獨立董事應維持獨立性之要求，其等係屬公司之外部人，對於公司實際情況未必能充分瞭解，故其執行監督職務時所需之各項資訊，即須仰賴公司經營者提供，否則就瞭解議案本身即有困難，遑論充分監督其所認為有問題之議案、有效發揮監督、遏止之效果。再者，由於獨立董事通常身兼數項職務，為避免影響其正職之職責，其所能夠投入之時間多半有限，致使其無法盡心投入執行監督，前述諸多因素造成或大幅增加獨立董事執行職務之困難度。劉連煜（2010），〈現行上市上櫃公司獨立董事制度之檢討暨改進方案——從實證面出發〉，《政大法學評論》，114 期，頁 127-128；蔡昌憲（2012），〈從內控制度及風險管理之國際規範趨勢論我國的公司治理法制：兼論董事監督義務之法律移植〉，《臺大法學論叢》，41 卷 4 期，頁 1841。

305 ERISMANN-PEYER ET AL., *supra* note 299, at 48.

306 朱德芳（2019），〈獨立董事不可或缺的工作夥伴——公司治理主管〉，《月旦會計實務研究》，20 期，頁 39。

307 同前註。

doi:10.6342/NTU202000744

主管機關、股東、投資人及其他利害關係人對於金融機構之公司治理、法令遵循及風險管理意識日漸增長，基於前述職能，公司治理人員之重要性或將愈發顯著。

doi:10.6342/NTU202000744

第五章 結論

觀諸近期金管會頻繁研擬諸多政策與法令，以防範金融機構層出不窮之舞弊案件，多數係肇因於金融機構內部未能妥適建置或有效運作其內控制度之缺失，故無法有效控制各項業務執行過程中所生之風險，以致內部職員所為之故意或過失行為，使金融機構本身、金融消費者之利益、金融市場之誠信甚或公平競爭秩序，均受有程度不一之損害。換言之，鑑於金融機構內部因職員眾多、分工層級細緻、業務單位與內容龐雜，故為促進金融事業之健全經營與監督管理之效率，合理達成營運績效、忠實報導及法令規章遵循等目標，應由董事會、高階經理階層、各部門主管、稽核人員等針對金融機構之特定情形與諸項業務之實際需要，個別設計妥適作業流程以供全體職員遵循，是謂內控制度。因此，本文藉由回顧內部控制之發展脈絡，嘗試重新形塑其制度設計與人事組織架構，思索應如何於銀行內部有效落實健全之內部治理機制，達成良好金融公司治理之目標，並有以下結論。

第一節 「工欲善其事，必先利其器」

為探究現行內控制度本身失靈之根本原因，且嘗試重塑內部控制之制度設計應有如何之形貌始謂健全，本文透過回顧內部控制之歷史演進與制度理論，再綜合對於現行實務發展之觀察後，析出內部牽制、風險控制及權責劃分等三項內控制度之重要原則與特性，並提出內部控制 GRC 整合架構之基本概念。

金融機構建立內控制度之基本目的為達成營運、報導及遵循等三項控制目標：營運係指各式經營活動之效果與效率，包括業務與財務之獲利與績效指標、維護與保障金融機構所有資產之安全，並促進金融機構之健全經營；報導即確保金融機構所出具之報導或資訊內容，係符合可靠性、及時性、透明性及其他相關公認準則或規範，包括年度財務報告、營業報告書、盈餘分派或虧損撥補之決議等財務報導，以及涵納環境、社會及經濟、永續發展、企業社會責任報告書等非財務報導；至於遵循則係指金融機構之運作應依循相關法令規章，包括各項金融業法、法規命令及行政規則。準此，本文觀察金融機構因作為受制於金融主管機關高度監督與管理之對象，其無論係設立登記、業務經營、財務標準或人事規範，抑或係應編製或揭露之報導或資訊內容，均由立法者與金融主管機關訂定金融法規、命令、辦法等各項密度與寬嚴有別之立法層級，共同構築出金融機構於運作過程中，其須確實遵循之

doi:10.6342/NTU202000744

行為準則與違反各該規定所應承擔之明確法律責任，故認為法令遵循不僅係內部控制之核心目標，更係內控制度 GRC 整合架構之重要基礎。

第一項 內控制度整合架構

（一）法令遵循（Compliance）——法令遵循除作為前述內部控制之核心目標外，內控制度中各項作業程序與控制重點均須以現行相關法令規章作為訂定基礎與標準，即內控制度之訂定者須充分瞭解金融機構內部所有業務內容與管理方法，以及各業務活動執行過程中可能面臨之風險，始能妥適地將相關法令監管規範與要求，轉譯並訂入作業程序以供業務單位執行。因此，法令遵循專責單位應負責為金融機構進行整體法規盤點、法遵測試、法遵風險評估等，俾使金融機構內部各項業務之執行得有一致之規範標準。再者，倘任何法令有新增或修訂，抑或金融機構內外部情況變遷之情事，法令遵循專責單位須立即配合檢討修正內控制度之相關內容，據以確保內控制度之完整性與有效性。

（二）風險管理（Risk Management）——金融機構相較其他股份有限公司，其公司治理特徵之一為債權人治理，即除了股東以外，尚須平衡兼顧包括存款人、投資者、保戶等廣大債權人之利益。抑且，金融機構作為金融中介角色，具有服務實體經濟之機能，故金融主管機關對其係採取以風險為基礎之高度監理，對於金融機構之曝險程度、風險胃納、法定資本提列等風險管理程序均設有嚴格規範，以防止市場風險、系統性風險等肇因於金融機構內部風險管理不當所引致之外部牽連效應發生。雖謂如此，除了前述「防弊」之考量以外，強調金融機構風險管理尚有立於「興利」之層面者，即事前透過風險辨識、風險評估、風險衡量及風險控制等風險管理程序，俾使董事會與高階管理階層於訂定達成各項目標之策略時，得具備辨識與評估風險之思維與能力，並得準確判斷風險所帶來之不確定性，以採取妥適之風險因應策略，進而提升創造價值之可能性。

（三）公司治理（Governance）——包括前述風險管理與法令遵循機制，以及內部稽核制度在內共同組成之內控制度，係屬達成金融機構公司治理目標所不可或缺之內部自律機制。良好之公司治理除了係為透過內控制度之運作，以達成前述營運、報導及遵循等目標以外，尚包括獲利、債權人、風險控管、金融法令遵循、服務實體經濟及普惠金融等目標，惟無論何者，均應透過金融機構內部自律機制

doi:10.6342/NTU202000744

（即內控制度）之順暢運作始能達成。本文自始認為，縱謂金融機構基於其特性而受有外部監督（或謂他律）機制之高度控管，惟無論係金融監理機關之行政裁罰（例如裁處高額罰鍰、命金融從業人員停止執行職務）、規範縝密之金融立法（例如修法提高內控制度罰鍰上限），甚或司法裁判等等，均僅能透過場外監控或事後補強之方式為之，故若欲根本性地解決既有或可能之治理問題，抑或提升金融機構公司治理之良率，仍須從金融機構內部著手，此亦為內控制度之所以重要之由。

第二項 內控制度設計原則

（一）內部牽制（Internal Check）原則——基於該內控制度最初之核心與本文認屬最重要之精神，金融機構內部各成員間應形成相互檢查、監督及制衡之關係，藉以偵測業務執行過程中可能之疏漏或錯誤，或避免詐欺舞弊等違法行為之發生。因此，個別業務單位或部門特定作業流程之設計，應區分為多階段執行且分別設定內部控制點，交由不同單位或職員執掌或處理。換言之，不同部門或個別職員間應透過專業化分工與不相容之職務分離，由兩位以上職員或兩個以上部門共同辦理一項業務。例如，為避免理財專員利用其所保存客戶之印鑑或已蓋有客戶原留印鑑之取款憑條，私自挪用客戶款項之情事發生[1]，銀行內部應對於客戶之開立戶頭、提存款項，以及客戶存摺、印鑑或已簽章空白交易單據等物品之保管與使用等作業程序，強化內部牽制與職務分離機制。意即，藉由多人經手業務之方式，使不同職員得相互覆核交易紀錄、偵測錯誤，同時得降低個人於無意識之狀態下發生疏漏，抑或提升多人有意識地串通舞弊為他人查知或注意之可能性。

（二）風險控制——正所謂「有風險才有控制」，基於認知欲達成金融機構之營運、報導或其他目標，須能有效偵測並控管業務執行過程中所生之各項風險，故內控制度即有朝向以風險控制為基礎之態勢發展，且對於金融機構內部風險管理之成效具有重要影響。換言之，設計內部作業程序時須著重之控制重點，即係諸如作業風險、法律風險等內生或外來風險發生之熱點，故應透過內控制度之運作隨時

[1] 109 年 2 月 3 日金管銀控字第 10802240082 號處分，本件案例事實為：甲商業銀行北部分行之理財專員 A 於 2013 年至 2019 年間，曾偽冒客戶自行開立帳戶（以下簡稱偽冒帳戶），並使用其客戶蓋具原留印鑑之單據，將客戶定存解約、外幣存款結售與轉帳、基金與海外 ETF 與股票之贖回等款項匯入客戶原始帳戶或偽冒帳戶。事後，A 以臨櫃方式提取原始帳戶或偽冒戶中現金，再將提取之現金存入 A 個人帳戶或以轉帳方式匯入其關係人帳戶，並將款項挪為己用，所涉金額逾新臺幣（下同）3,600 萬元。對此，金管會依銀行法核處該行 1,200 萬元之罰鍰。

doi:10.6342/NTU202000744

檢視每一作業流程或循環中所設定之若干控制點，是否存有錯誤數據資訊、違法或不符合規定之事實發生，並即時予以剔除。例如，針對理財專員與客戶間涉及不當資金往來之情事[2]，銀行內部應建立包括：充分瞭解客戶審查作業程序、客戶資料之歸檔列管與查詢、客戶基本資料與印鑑變更、查對紀錄與對帳單寄送等帳戶管理相關作業程序，並應特別著重諸如：帳戶監控、簽收或交易紀錄保存、調閱或查詢各項資料、使用客戶保存物件應經授權核准與備查等控制重點，方能預防理財專員不當行為風險之發生。

（三）權責劃分——或可謂係衍生自前述內部牽制原則，不同部門或個別職員彼此對於各項業務或交易行為，應採取不相容之職務分離（Segregation of Duties，SoD）機制，於金融機構內部為專業化之分工。因此，組織內部應明確釐清且具體規範董事會、管理階層及一般業務單位或部門諸等內控制度參與者，各自所扮演之角色與所負之權限與責任範圍，且應避免存在利益衝突或有權責分工不清之情形。例如，法令遵循主管主要應負責協助董事會訂定法令遵循制度、監督法令遵循人員任職後之訓練，以及分行職員之當地法令教育訓練等職務，惟有銀行竟令海外分行法令遵循人員於其他非法遵相關之業務活動上有兼職之情事，致生業務執行與法令遵循間之職務衝突，即有違上揭權責劃分原則之要求，難謂為妥[3]。

[2] 109 年 2 月 3 日金管銀控字第 10801362282 號裁處書，本件案例事實為：乙商業銀行北部分行之理財專員 B 於 2016 年起任職該分行達 13 年餘，期間未曾輪調其他分行或安排至其他職位。B 自 2015 年至 2019 年間，於客戶將基金贖回、申購新保單或提前繳清續期保險費時，利用協助客戶填寫相關申購或取款文件之機會，逕將款項匯至其指定帳戶挪為己用，受影響之客戶多達八戶、所涉金額逾 7,000 萬元。此外，於 2012 年至 2019 年間，B 另與客戶成立借貸關係，並利用客戶之帳戶作為挪用款項之入款帳戶。對此，金管會認定 B 核有挪用客戶款項及與客戶有異常資金往來之情事，故依銀行法核處該行 1,200 萬元之罰鍰。

[3] 105 年 9 月 14 日金管銀控字第 10560003851 號處分，本件案例事實為：2016 年，丙商業銀行海外分行因未能充分瞭解當地銀行與洗錢防制相關法令，故就防制洗錢無完整之內部作業手冊、各項業務單位對於防制洗錢均未有一致之規範，致該分行之法遵功能嚴重不足。再者，該分行之法令遵循主管缺乏適任性，不僅未能協助建立完整有效之法令遵循制度、監督法令遵循人員與行員之當地法令遵循訓練，於資金、授信、聯行與同業往來等業務尚有兼職、產生職務衝突之情形。尤有甚者，對前述諸等經當地金融主管機關於其金融檢查報告中列為重大缺失，並預告可能採取監理處分行動此重大事件，不僅該分行內部稽核部門未能及時向董事會提出報告、充分說明重要檢查意見及提出因應處理方式，以致於稽核工作報告流於形式，且該行之董事會亦未能發揮綜理全行業務、有效督導內控內稽等管理制度之建立與執行等功能，導致董事會成員無法即時獲取資訊以知悉該缺失之嚴重性。對此，該分行不僅招致當地金融主管機關處以鉅額罰款，金管會復依銀行法核處 1,000 萬元罰鍰，並命該行須解除總經理、總稽核、法遵長等數名高階經理人職務之處分。

doi:10.6342/NTU202000744

第二節　「事在人為耳，彼朽骨者何知」

內部控制之實施主要係經由對於業務單位依據內控制度所為經營活動之不斷檢查，藉以偵測或發覺金融機構內部是否存在與組織政策、作業程序、既定目標或預期標準等乖離之事實，並藉由回饋系統即時反應至適當之經營管理階層，以針對個案問題採取必要之應對措施，確保金融機構得穩定朝向董事會與高階管理階層所擘劃之藍圖前進，同時透過前述內部牽制原則達到勾稽之目的，防止舞弊或錯誤之發生。質言之，縱謂依據相關法令之規定，應由董事會與高階管理階層負起建置與維持內控制度之責任，惟無論係內控制度或業務活動之實際執行，抑或最能發現或即時控管風險者，應係位居內控制度第一道防線之業務單位。職是故，本文經由逐步檢視金融機構內部之人事組織及其成員，諸等於內控制度中所應扮演之角色、權責與義務後，容有以下結論。

第一項 董事會作為決策監督機關

現今金融機構之規模與業務種類漸趨龐雜，為達成合理且有效之權責劃分與營運活動之分工，其內部決策監督與經營管理兩者之組織結構應有重新予以定位之必要。依據現行公司法制之規定，或有謂董事會主要負責公司業務之執行，惟就營業額龐大、業務內容繁雜、單位部門廣布及員工數量眾多之金融機構而言，董事會於實際運作上或將囿於人力、時間及專業等限制，較難期待其凡事均親力親為。是故內控制度規範即明確指出，金融機構之董事會對於確保內控制度之妥適建置與維持該制度之有效運作、營運等風險之控管，應負起監督之最終責任；同時，董事會尚須就金融機構之經營策略與計畫、重大風險與曝險程度、經營管理階層績效評估、法令遵循政策、備置財務報表等事項，擔負決策與監督之責。

再者，本文觀察現行之證券交易法引進獨立董事制度、設置審計委員會，以及金融機構主管機關對於獨立董事係採取正面且強制採用之態度後認為，除了前述實然之面向，即基於金融機構之規模與組織架構逐漸龐大，愈趨難以期待董事會得親自參與第一線各項日常業務之執行，故董事會須職司訂定重大政策與建制內控制度以確保有效監督金融機構之運作以外，於應然之面向亦有將董事會定位、確立為決策監督機關之態勢。質言之，無論獨立董事或由全體獨立董事組成審計委員會之制度設計，其職權範圍概有訂定與修正內控制度、重大交易之決策、財務會計或

doi:10.6342/NTU202000744

內部稽核等主管之任免等，均係立基於監督角色或機關之地位，主要負責金融機構內部制度與規則之建立或重大事項之決策，且審計委員會之獨立董事成員尚頻繁準用監察人行使監察權限之規定。

觀諸司法實務判決亦可知，法院係逐漸肯認金融機構董事會之個別董事均應負責建置與運作內控內稽制度，並監督管理階層與業務單位是否確實履行，且必要時尚得要求業務單位人員提供財務業務相關文件，俾利其可經常性檢視所有業務活動是否符合法令或相關規範。抑且，現行金融主管機關亦擴大強制金融機構應於董事會下設置由獨立董事所組成之審計委員會、薪酬委員會等功能性委員會，期藉由獨立董事專業分工與獨立超然之立場，就各項事務提供建言或意見，以協助董事會作成決策，並健全董事會之監督與管理機能。由是可知，倘若固守董事會係金融機構內部業務執行或經營管理中樞之定位，則要求業務執行權力高度集中之董事會同時應肩負決策與監督之職責，或將形成自為經營與自為監督之窘境，獨立董事制度是否能夠有效發揮制衡效果，難謂無疑。

綜而言之，現行法制規範與主管機關對於金融機構董事會之定位，均已由傳統業務執行機關，漸朝決策監督機關之方向傾軋，俾利董事會、獨立董事及審計委員會等諸項制度設計得有效發揮其機能。抑且，學說與法院實務判決亦均就個別董事於內控制度所負之責任與義務逐漸展開有別於傳統忠實義務或善良管理人之注意義務等內涵之辨析與論述，即該等義務已由金融機構之董事會應親自執行業務或具體處理各項事務，逐漸肯認董事會應將業務執行委諸高階經理人所領導，由經營管理階層與業務單位職員所組成之團隊主要負責日常業務之實際執行，而個別董事則須共同職司訂定與有效運作內控制度，並以此追蹤、檢視諸等人員執行業務之情形與結果，確保各項業務過程中未有錯誤、舞弊或其他違法行為之風險產生。意即，個別董事作為金融機構內部最高治理單位之成員，不僅係個人所具備之特定領域之專業能力，其等就公司整體業務、財務、法務及內控制度等不同層面之具體運作，於今亦須具備全盤、系統性之基本素養甚或專業職能，始能勝任此職。準此，配合前述現行法制規範與主管機關之函釋見解，法院實務判決亦已開始對於金融機構監控型董事會與個別董事於內控制度所負監督責任有具體化闡釋，例如個別董事應充分瞭解金融機構法令規範、認知不同業務風險、審閱並核實各項文件資訊等見解，或可謂對於尚待細緻化之個別董事於內控制度監督責任，提供穩定且正確

doi:10.6342/NTU202000744

之發展基礎。

第二項 經營管理階層誠信之落實

誠如前揭內控制度之權責劃分原則，既謂董事會係作為金融機構內部之決策監督機關，經營管理階層即須協助管理業務單位職員之日常經營活動，同時須維持金融機構整體健全經營之良好組織文化。本文首先觀察現行裁罰案件之原因事實，多係內控制度第一道防線之職員未能確實遵循內控制度相關程序規範所致，故若欲自源頭控管風險，抑或於發現違犯內控制度之行為時，即時採取有效措施以防範風險持續擴大或累積，則有賴於各業務單位之經營管理階層之管理與監督。此係鑑於銀行內部之業務單位多樣且部門分工細緻，透過較為熟悉各該業務單位且具備專業知識與實務經驗之資深管理階層擔負業務執行之管理責任，除了能夠有效且即時查核風險、防止舞弊行為以外，尚可協助評估金融機構之營運目標與各項業務投資。

再者，基於金融服務事業之經營與內控制度之執行皆係以誠信與正直等道德價值作為運作基礎與行為準則，故不僅須由董事會與高階管理階層本於廉潔、透明及負責之經營理念，訂定以道德價值為核心之政策與目標（是謂 tone from the top 模式），亦應由直接管轄業務單位之中階管理階層將董事會訂定之政策內容與期待目標有效轉化，並以此訂定適當之作業程序規範，且依其職權指揮監督與訓練轄下之業務單位職員共同達成政策目標（是謂 tome from above 模式）。綜言之，良好之金融機構組織文化係鼓勵內部成員為正向行為、防止不當侵害他人權益之基礎，更是金融機構永續經營之重要關鍵，強調管理階層帶領業務單位職員具體落實，不僅得充分傳達與銜接董事會與高階管理階層訂定之政策方向，且能夠確保內控制度作業程序於各該業務單位之運作與風險即時控管之實效。

第三項 當內部控制成為全民運動

探究內控制度之運作係由執行各業務活動或交易循環之作業程序，藉以發覺各項經營與管理作業是否存在與政策目標背離或舞弊等事實，確保金融機構整體運作之健全性與符合法令規範，且該持續性內部控制作業並非屬董事會、高階管理階層或特定單位或部門之責任，毋寧在於全體成員之通力配合推動與執行。意即，基於內控制度之本質係須考量現時金融機構政策、經營環境與狀況、法令規範變遷

doi:10.6342/NTU202000744

等因素，隨時予以檢視之動態性作業程序，故對其之遵循或調整即須高度仰賴金融機構內部所有成員。因此，除了前述董事會與經營管理階層以外，尚須有人力資源部門建立之甄選、任用、培訓等人事制度，據以提升職員對於內部控制之依循意識與效能；內部稽核單位進行評估與查核並提供專業改進建議，以持續優化內控制度之實施；公司治理人員負責提供董事會與管理階層即時且充足之治理資訊，協助其等監督內控制度之執行與作成正確之監督決策；甚或由外部稽核與金融檢查對於金融機構為客觀監督等之參與，共同促進內控制度之持續適用與適切運作。

綜言之，本文嘗試藉由內部控制之制度設計與人事組織架構等兩層面之研析與重塑，初步建構金融機構內控制度應有之完整形貌，並提出上述諸項淺見。儘管囿於智識與能力之限制以致本文或有疏漏或不完整之處，惟吾等若同樣肯認內控制度係達成良好金融機構公司治理目標所不可或缺之重要內部自律機制，則期待本文對於內控制度僅能稱冰山一角之研究，能為往後內控制度之持續發展與優化略盡棉薄之己力。

doi:10.6342/NTU202000744

參考文獻

一、 中文參考文獻

（一）專書

王文宇、林國全、曾宛如、王志誠、蔡英欣、汪信君（2015），《商事法》，臺北市：元照。

王任翔（2019），《洗錢防制法——銀行業實務挑戰》，二版，臺北市：元照。

王志誠（2014），《銀行法》，臺北市：新學林。

王志誠（2017），《互聯網金融之監理機制》，臺北市：新學林。

王志誠（2017），《現代金融法》，三版，臺北市：新學林。

余雪明（2016），《證券交易法：比較證券法》，五版，臺北市：自刊

吳琮璠（2009），《審計學：實務應用與法律觀點》，四版，臺北市：吳琮璠。

阮品嘉（2012），《金融控股公司及其集團之規範與實務》，臺北市：元照。

周伯翰（2017），《銀行法暨金融控股公司法》，臺北市：元照。

陳耀宗（民 104），《審計學：國際審計與確信準則為架構（上）》，新北市：滄海圖書資訊。

陳耀宗（民 105），《審計學：國際審計與確信準則為架構（下）》，新北市：滄海圖書資訊。

曾令寧、黃仁德（民 92），《現代銀行監理與風險管理》，臺北市：臺灣金融研訓院。

曾宛如（2012），《證券交易法原理》，六版，臺北市：元照。

曾宛如（2017），《公司法制基礎理論之再建構》，臺北市：元照。

曾宛如（2020），《證券交易法原理》，七版，臺北市：元照。

楊岳平（2011），《公司治理與公司社會責任——企業併購下股東、債權人、員工、投資人之保護》，臺北市：元照。

楊雅惠、許嘉棟（2014），《台灣金融體制之變遷綜觀》，臺北市：財團法人臺灣金融研訓院。

銀行內部控制制度編撰委員會（民 90），《銀行內部控制制度》，臺北市：台灣金融研訓院。

銀行內部控制與內部稽核編撰委員會（民 94），臺北市：財團法人臺灣金融研訓院。

劉連煜（2010），《現代公司法》，六版，臺北市：元照。

劉連煜、杜怡靜、林郁馨、陳肇鴻（2013），《選任獨立董事與公司治理》，臺北市：元照。

doi:10.6342/NTU202000744

賴英照（2017），《股市遊戲規則：最新證券交易法解析》，三版，臺北市：自刊。

（二）翻譯書籍

Global Reporting Initiative（著），吳文雅（等譯）（2017），《GRI 準則》，臺北市：社團法人中華民國企業永續發展協會。

Global Reporting Initiative（著），吳文雅（等譯）（2017），《GRI 準則詞彙表 2016》，臺北市：社團法人中華民國企業永續發展協會。

羅伯・席勒（Robert J. Shiller）（著），林麗冠（譯）（2014），《金融與美好社會》（Finance and the Good Society），臺北市：遠見天下文化。

（三）書之篇章

方嘉麟（2019），〈公司管理之權力結構〉，方嘉麟（等著），《變動中的公司法制：17 堂案例學會《公司法》》，二版，頁 121-151，臺北市：元照。

王文宇（2016），〈金融法制與金融監理〉，王文宇（等著），《金融法》，九版，頁 1-22，臺北市：元照。

王文宇（2019），〈論董事會與執行長的權責區分〉，王文宇（等著），《「落實獨立董事制度，提升公司治理價值」建言集》，頁 21-27，臺北市：社團法人中華公司治理協會。

林仁光（2016），〈銀行法總則〉，王文宇（等著），《金融法》，九版，頁 23-72，臺北市：元照。

陳麗琦、萬幼筠（2017），〈金融業防制洗錢查核專案作業探討〉，王文杰（等著），《新洗錢防制法——法令遵循實務分析》，頁 319-358，臺北市：元照。

曾宛如、林國彬（2019），〈管理者之義務與責任〉，方嘉麟（等著），《變動中的公司法制：17 堂案例學會《公司法》》，二版，頁 179-213，臺北市：元照。

詹德恩（2019），〈我國金控公司與銀行法令遵循施行現況及未來〉，台灣企業法律學會（編），《國際公司治理與企業法遵》，頁 315-349，臺北市：新學林。

廖大穎（2019），〈檢析法令遵循與我國公司治理之內部控制模式〉，台灣企業法律學會（編），《國際公司治理與企業法遵》，頁 105-151，臺北市：新學林。

謝雪妮（2017），〈銀行業防制洗錢及打擊資恐機制實務〉，王文杰（等著），《新洗錢防制法——法令遵循實務分析》，頁 381-422，臺北市：元照。

（四）期刊論文

方嘉麟（2018），〈從永豐金案看獨立董事制度〉，《月旦法學雜誌》，272 期，頁 5-

doi:10.6342/NTU202000744

12。
王文宇（2009），〈董事之資訊請求權〉，《月旦法學教室》，86 期，頁 18-19。
王文宇（2012），〈論大型企業之公司治理法制〉，《月旦法學雜誌》，200 期，頁 282-301。
王志誠（2007），〈金融重大交易之法律風險及控制〉，《全國律師》，11 卷 2 期，頁 5-13。
王志誠（2016），〈董事之監督義務——兆豐銀行遭美國紐約州金融服務署裁罰一．八億美元案之省思〉，《月旦法學雜誌》，259 期，頁 5-18。
朱德芳（2019），〈獨立董事不可或缺的工作夥伴——公司治理主管〉，《月旦會計實務研究》，20 期，頁 34-43。
李悅嘉（2019），〈系統更新引風暴——南山人壽給金融業寶貴一課〉，《台灣銀行家》，12 月號，頁 72-75。
李智仁（2009），〈二〇〇八年銀行法修訂後之立即糾正措施法制布局〉，《法學新論》，14 期，頁 17-37。
沈大白、黃追（2004），〈簡介 COSO 之企業風險管理（草案）及 BIS 之作業風險管理暨監督準則〉，《管理會計》，67 期，頁 41-62。
沈大白、黃追（2016），〈BCBS 調整資本計提方法之最新發展——以作業風險為例〉，《貨幣觀測與信用評等》，119 期，頁 78-91。
沈大白、黃追（2018），〈修訂後『Basel III：危機後之改革』及作業風險新標準法〉，《貨幣觀測與信用評等》，130 期，頁 105-118。
沈大白、黃追（2019），〈理專案件頻傳 銀行作業風險之未來〉，《會計研究月刊》，403 期，頁 82-87。
林仁光（2004），〈論經營者誠信、內部控制、內部稽核制度與公司治理〉，《月旦法學雜誌》，106 期，頁 39-55。
林仁光（2006），〈董事會功能性分工之法制課題——經營權功能之強化與內部監控機制之設計〉，《臺大法學論叢》，35 卷 1 期，頁 157-266。
林仁光（2016），〈由兆豐銀案談銀行監理——由銀行治理及銀行保密法之遵循出發〉，《月旦法學雜誌》，259 期，頁 19-33。
林志潔（2015），〈反制跨國行賄與強化企業法令遵循——以美國海外反貪腐法（FCPA）為例〉，《月旦法學雜誌》，242 期，頁 5-25。
林志潔（2016），〈兆豐案天價罰款的啟示——美國反洗錢法的重點與金融業應有的作為〉，《月旦法學雜誌》，259 期，頁 34-48。
林瑞彬、張憲瑋、陳月秀（2017），〈企業如何建置法令遵循計畫〉，《全國律師》，9 月號，頁 18-27。

doi:10.6342/NTU202000744

林瑞彬、張憲瑋、劉家全(2018),〈法令遵循管理的回顧與展望〉,《勤業眾信通訊》,元月號,頁 27-30。
邵慶平(2008),〈董事受託義務內涵與類型的再思考——從監督義務與守法義務的比較研究出發〉,《臺北大學法學論叢》,66 期,頁 1-43。
邵慶平(2019),〈論公司資訊權的規範:以董事資訊權的增訂爭議為中心〉,《東吳法律學報》,30 卷 4 期,頁 1-28。
洪秀芬(2006),〈董事會獨立經營權限及董事監督義務〉,《政大法學評論》,94 期,頁 217-266。
張心悌(2019),〈員工違法行為之董事監督義務——評臺灣臺北地方法院 105 年度訴字第 4239 號民事判決〉,《月旦裁判時報》,80 期,頁 19-24。
張修齊(2003),〈從新巴塞爾資本協定看作業風險管理〉,《台灣金融財務季刊》,4 輯 1 期,頁 55-77。
張憲瑋(2018),〈法令遵循新趨勢——從法遵風險評估開始〉,《勤業眾信通訊》,11 月號,頁 15。
郭大維(2008),〈論我國金融機構公司治理之強化〉,《台灣金融財務季刊》,9 輯 4 期,頁 47-64。
郭大維(2017),〈企業法令遵循與董事監督義務〉,《月旦法學教室》,179 期,頁 20-22。
郭大維(2017),〈我國銀行法令遵循制度之探討──從兆豐銀行紐約分行遭美國重罰事件談起〉,《存款保險資訊季刊》,30 卷 1 期,頁 1-29。
曾宛如(2010),〈董事忠實義務於台灣實務上之實踐——相關判決之觀察〉,《月旦民商法雜誌》,29 期,頁 145-156。
曾宛如(2011),〈董事會與經理人是否真為公司之業務執行機關及業務執行之輔助機關?——從臺灣高等法院臺中分院九十九年度重上字第一七四號判決及九十九年度重上字第一六四號判決所凸顯之亂象論起〉,《月旦法學雜誌》,199 期,頁 166-183。
黃劭彥、陳俊志(2018),〈台灣銀行業內部控制三道防線之探討〉,《月旦會計實務研究》,2 卷 2 期,頁 49-55。
黃銘傑(2007),〈金融機構負責人忠實注意義務加重之理論與實務〉,《月旦法學雜誌》,142 期,頁 149-176。
楊岳平(2019),〈新公司法與企業社會責任的過去與未來——我國法下企業社會責任理論的立法架構與法院實務〉,《中正財經法學》,18 期,頁 43-92。
楊岳平(2019),〈論金融控股公司治理的改革方向:以獨立董事與提名委員會為中心〉,《臺大法學論叢》,48 卷 2 期,頁 683-750。

doi:10.6342/NTU202000744

廖世昌、郭姿君（2017），〈現行金融業法令遵循制度概況簡介〉，《月旦會計事務所 CPA 雜誌》，創刊號，頁 101-110。
劉連煜（2010），〈現行上市上櫃公司獨立董事制度之檢討暨改進方案——從實證面出發〉，《政大法學評論》，114 期，頁 53-156。
蔡昌憲（2012），〈從內控制度及風險管理之國際規範趨勢論我國的公司治理法制：兼論董事監督義務之法律移植〉，《臺大法學論叢》，41 卷 4 期，頁 1819-1896。
蔡昌憲（2015），〈省思公司治理下之內部監督機制——以獨立資訊管道的強化為核心〉，《政大法學評論》，141 期，頁 197-276。
蔡昌憲（2015），〈從內控失靈個案談企業社會責任與公司治理：兼論金融體系之市場監督力量〉，《台灣法學雜誌》，285 期，頁 189-205。
蔡昌憲（2018），〈從公司法第一條修正談公司治理之內外部機制——兼論企業社會責任的推動模式〉，《成大法學》，36 期，頁 89-153。
蔡昌憲、陳乃瑜（2012），〈內部控制制度、董事監督義務及薪資報酬委員會——評最高法院九十八年度台上字第一三〇二號民事判決〉，《月旦法學雜誌》，203 期，頁 200-228。

（五）翻譯著作

平野温郎（著），高志明、林奕延（譯）（2019），〈日系企業全球發展下的遵法風險・危機與對應策略〉，台灣企業法律學會（編），《國際公司治理與企業法遵》，頁 19-33，臺北市：新學林。

（六）官方文件

金融監督管理委員會證券期貨局（2018），《新版公司治理藍圖（2018-2020）》。

（七）案例

最高法院 101 年度台上字第 1342 號民事判決。
最高法院 102 年度台上字第 360 號民事判決。
最高法院 106 年度台上字第 783 號刑事判決。
最高法院 108 年度台上字第 24 號刑事判決。
最高法院 95 年度台上字第 5910 號判決。
最高法院 98 年度台上字第 1302 號民事判決。
最高法院 99 年度台上字第 1177 號民事判決。
臺灣高等行政法院 101 年度簡字第 119 號簡易判決。

doi:10.6342/NTU202000744

臺灣高等法院 102 年度上字第 636 號民事判決。
臺灣高等法院 106 年度上字第 1343 號民事判決。
臺灣高等法院 107 年度金上重訴字第 1 號判決。
臺灣高等法院 97 年度上字第 1036 號民事判決。
臺灣高等法院 98 年度上更（一）字第 97 號民事判決。
臺灣高等法院 99 年度上更（二）字第 82 號民事判決。
臺灣高等法院臺中分院 100 年度重上更（一）字第 27 號民事判決。
臺北地方法院 102 年度訴字第 561 號刑事判決。
臺北地方法院 105 年度訴字第 4239 號民事判決。
臺北地方法院 92 年度勞訴字第 10 號民事判決。
臺北地方法院 96 年度重訴字第 1054 號民事判決。
板橋地方法院 100 年度訴字第 1997 號民事判決。
新竹地方法院 102 年度訴字第 263 號民事判決。
臺中地方法院 97 年度重訴字第 515 號民事判決。
彰化地方法院 106 年度訴字第 764 號民事判決。

（八）函釋、函令或函文

1. 法務部

102 年 3 月 19 日法律字第 10200042350 號函。
104 年 10 月 14 日法律字第 10403512790 號函。

2. 金融監督管理委員會

93 年 9 月 13 日金管銀（一）字第 0938011562 號令。
95 年 8 月 8 日金管銀（二）字第 09500307181 號函。
95 年 8 月 8 日金管銀（二）字第 09500307182 號函。
95 年 8 月 8 日金管銀（二）字第 09500307180 號函。
95 年 9 月 22 日金管銀（四）字第 09500383690 號函。
95 年 12 月 21 日金管銀（四）字第 09500474741 號裁處書。
96 年 5 月 28 日金管銀（二）字第 09600149690 號函。
96 年 7 月 12 日金管銀（二）字第 09600286440 號函。
96 年 7 月 27 日金管銀（二）字第 09600292280 號函。
99 年 3 月 29 日金管銀國字第 09900039294 號令。
99 年 9 月 28 日金管銀法字第 09910004570 號函。
102 年 8 月 22 日金管銀控字第 10200181601 號處分。

doi:10.6342/NTU202000744

103 年 10 月 1 日金管證審字第 1030039132 號令。
103 年 10 月 3 日金管證發字第 1030039119 號函。
104 年 3 月 20 日金管保財字第 10402502462 號裁處書。
104 年 3 月 20 日金管保財字第 10402503022 號裁處書。
105 年 6 月 17 日金管銀國字第 10500127920 號函。
105 年 8 月 11 日金管會檢局（制）字第 1050150280 號函。
105 年 9 月 12 日金管銀控字第 10560003721 號處分。
105 年 9 月 14 日金管銀控字第 10560003851 號處分。
105 年 9 月 14 日金管銀控字第 10560003852 號處分。
105 年 12 月 7 日金管會檢局（制）字第 1050150456 號函。
106 年 7 月 6 日金管銀國字第 10620003161 號處分。
106 年 9 月 27 日金管銀國字第 10620004841 號處分。
106 年 10 月 26 日金管銀票字第 10640004421 號處分。
106 年 11 月 28 日金管銀控字第 10660003651 號處分。
106 年 12 月 5 日金管銀控字第 10600291711 號處分。
106 年 12 月 5 日金管銀控字第 10600291713 號處分。
106 年 12 月 15 日金管銀國字第 10620006681 號處分。
106 年 12 月 19 日金管銀國字第 10620006841 號處分。
106 年 12 月 29 日金管銀控字第 10660006101 號處分。
106 年 12 月 29 日金管銀控字第 10660006103 號處分。
106 年 12 月 29 日金管銀控字第 10660006105 號處分。
106 年 12 月 29 日金管銀控字第 10660006107 號處分。
106 年 12 月 29 日金管銀控字第 10660006109 號處分。
106 年 12 月 29 日金管銀控字第 1066000610B 號處分。
106 年 12 月 29 日金管銀控字第 1066000610D 號處分。
106 年 12 月 29 日金管銀控字第 1066000610F 號處分。
107 年 1 月 23 日金管檢銀字第 1070604007 號函。
107 年 2 月 1 日金管銀外字第 10702703731 號處分。
107 年 6 月 26 日金管銀合字第 10702725361 號處分。
107 年 6 月 27 日金管銀控字第 10701079801 號處分。
107 年 10 月 25 日金管銀控字第 10702002191 號處分。
107 年 12 月 19 日金管證發字第 10703452331 號令。
107 年 12 月 19 日金管證發字第 1070345233 號令。
108 年 3 月 26 日金管銀控字第 10702224341 號處分。
108 年 8 月 7 日金管銀控字第 10802721961 號處分。

doi:10.6342/NTU202000744

108 年 8 月 7 日金管銀控字第 10802721963 號處分。
108 年 8 月 7 日金管銀控字第 10802721965 號處分。
108 年 8 月 7 日金管銀控字第 10802721967 號處分。
108 年 8 月 7 日金管銀控字第 10802721969 號處分。
108 年 8 月 7 日金管銀控字第 1080272196B 號處分。
108 年 8 月 7 日金管銀控字第 1080272196D 號處分。
109 年 2 月 3 日金管銀控字第 10801362282 號裁處書。
109 年 2 月 3 日金管銀控字第 10802240082 號處分。
109 年 2 月 14 日金管保產字第 10904520112 號裁處書。

3. 經濟部

76 年 4 月 18 日商字第 17612 號函釋。
94 年 7 月 5 日經商字第 09409012260 號函。
97 年 6 月 6 日經商字第 09702069420 號函。
102 年 6 月 13 日經商字第 10200063220 號函。
104 年 3 月 10 日經商字第 10402404610 號函。
105 年 5 月 27 日經商字第 10502415500 號函。
108 年 1 月 29 日經商字第 10800002120 號函。

4. 財政部

82 年 7 月 12 日台財融字第 821165024 號函。

（九）網路資料

工商時報(2019)，〈理專頻出包 顧立雄：銀行輕忽就重罰〉，https://www.chinatimes.com/newspapers/20190510000324-260205?chdtv。

中央存款保險公司網站，https://www.cdic.gov.tw/main_ch/index.aspx。

中華民國中央銀行全球資訊網，https://www.cbc.gov.tw/tw/mp-1.html。

中華民國法務部網站，https://www.moj.gov.tw/mp-001.html。

中華民國銀行商業同業公會全國聯合會網站，https://www.ba.org.tw/Publicinformation/Index。

自由時報（2019），〈銀行理專、行員 A 錢 7 年半共 24 件 這家銀行被罰最多〉，https://ec.ltn.com.tw/article/breakingnews/2785136。

金融監督管理委員會網站，https://www.fsc.gov.tw/ch/index.jsp。

金融監督管理委員會銀行局網站，https://www.banking.gov.tw/ch/index.jsp。

孫欣、章友馨，〈金融機構法令遵循風險評估與法規資料庫〉，KPMG，https://home.kp

doi:10.6342/NTU202000744

mg/tw/zh/home/insights/2018/01/law-compliance-risk-assessment-and-regulations-database.html。

經濟日報（2019），〈理專及行員挪用客戶資金 件數及被罰金額最多是這幾家銀行〉，https://money.udn.com/money/story/5613/3803308。

經濟部商業司商工登記公示資料查詢服務網站，https://findbiz.nat.gov.tw/fts/query/QueryBar/queryInit.do。

鉅亨網（2019），〈7 年來 24 名理專監守自盜 金管會共開鍘 8600 萬元 這 4 家銀行罰最多〉，https://news.cnyes.com/news/id/4317442。

聯合報（2018），〈歐盟 GDPR 上路了 金管會要求銀行落實個資保護〉，https://udn.com/news/story/11316/3162994。

（十）其他資料

中央銀行（2017），《強化我國金融業公司治理並對兆豐案及永豐案後續之調查結果》，https://www.cbc.gov.tw/public/Attachment/710213481271.pdf。

行政院國土安全政策會報「國家關鍵基礎設施安全防護指導綱要」附件一、國家關鍵基礎設施領域分類（107 年 7 月 30 日訂正），https://ohs.ey.gov.tw/File/79A79307409FF32C。

經濟日報（2008），〈杜絕造假案 健全吹哨機制〉，https://taipei-tfcc.scu.org.tw/notice/enterprise-honesty-morality-1070918-1.pdf。

二、 英文參考文獻

（一）專書

AGUAYO, RAFAEL (1990), DR. DEMING: THE AMERICAN WHO TAUGHT THE JAPANESE ABOUT QUALITY.

ALLEN, MARK & DALTON CERVO (2015), MULTI-DOMAIN MASTER DATA MANAGEMENT: ADVANCED MDM AND DATA GOVERNANCE IN PRACTICE.

ANDERSON, DOUGLAS J. & GINA EUBANKS (2005), LEVERAGING COSO ACROSS THE THREE LINES OF DEFENSE.

BAINBRIDGE, STEPHEN M. (2012), CORPORATE GOVERNANCE AFTER THE FINANCIAL CRISIS.

BANKS, ERIK (2004), CORPORATE GOVERNANCE: FINANCIAL RESPONSIBILITY, CONTROLS AND ETHICS.

doi:10.6342/NTU202000744

BERLE, ADOLF A. & GARDINER C. MEANS (1932), THE MODERN CORPORATION AND PRIVATE PROPERTY.

BIEGELMAN, MARTIN T. & JOEL T. BARTOW (2012), EXECUTIVE ROADMAP TO FRAUD PREVENTION AND INTERNAL CONTROL: CREATING A CULTURE OF COMPLIANCE, 2d ed.

CAMPBELL, TIM S. & WILLIAM A. KRACAW (1993), FINANCIAL INSTITUTION AND CAPITAL MARKET.

CASCIO, WAYNE F. (1998), MANAGING HUMAN RESOURCES: PRODUCTIVITY, QUALITY OF WORK LIFE, PROFITS, 5th ed.

CHIU, IRIS H-Y (2018), REGULATING (FROM) THE INSIDE: THE LEGAL FRAMEWORK FOR INTERNAL CONTROL IN BANKS AND FINANCIAL INSTITUTIONS.

CRESSEY, DONALD R. (1953), OTHER PEOPLE'S MONEY: A STUDY IN THE SOCIAL PSYCHOLOGY OF EMBEZZLEMENT.

CROUHY, MICHEL et al. (2006), THE ESSENTIALS OF RISK MANAGEMENT.

CRUZ, MARCELO G. (2002), MODELING, MEASURING AND HEDGING OPERATIONAL RISK.

DESSLER, GARY (2005), A FRAMEWORK FOR HUMAN RESOURCE MANAGEMENT, 4th ed.

DRAVIS, BRUCE F. (2010), THE ROLE OF INDEPENDENT DIRECTORS IN CORPORATE GOVERNANCE: AN UPDATE OF THE ROLE OF INDEPENDENT DIRECTORS AFTER SARBANES-OXLEY.

EASTERBROOK, FRANK H. & DANIEL R. FISCHEL (1996), THE ECONOMIC STRUCTURE OF CORPORATE LAW.

EISENBERG, MALVIN ARON (2005), CORPORATIONS AND OTHER BUSINESS ORGANIZATIONS: CASES AND MATERIALS, 9th ed.

EISENBERG, MELVIN A. (2014), CORPORATIONS AND OTHER BUSINESS ORGANIZATIONS: STATUTES, RULES, MATERIALS, AND FORMS, 2014th ed.

ERISMANN-PEYER, GERTRUD et al. (2008), THE INSIDER'S VIEW ON CORPORATE GOVERNANCE: THE ROLE OF THE COMPANY SECRETARY.

HAMILTON, JAMES & PETER RASMUSSEN (2007), GUIDE TO INTERNAL CONTROLS: UNDER SECTION 404 OF THE SARBANES-OXLEY ACT, 2d ed.

HOPKIN, PAUL (2010), FUNDAMENTALS OF RISK MANAGEMENT: UNDERSTANDING, EVALUATING, AND IMPLEMENTING EFFECTIVE RISK MANAGEMENT.

HULL, JOHN (2007), RISK MANAGEMENT AND FINANCIAL INSTITUTIONS.

IT GOVERNANCE INSTITUTE (2006), INFORMATION SECURITY GOVERNANCE: GUIDANCE FOR BOARDS OF DIRECTORS AND EXECUTIVE MANAGEMENT, 2d ed.

KAUFMAN, HENRY (2001), ON MONEY AND MARKETS: A WALL STREET MEMOIR.

doi:10.6342/NTU202000744

MILLER, GEOFFREY PARSONS (2014), THE LAW OF GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE.

MONAHAN, GREGORY (2008), ENTERPRISE RISK MANAGEMENT: A METHODOLOGY FOR ACHIEVING STRATEGIC OBJECTIVES.

MOOSA, IMAD A. (2007), OPERATIONAL RISK MANAGEMENT.

O'SULLIVAN, JULIE R. FEDERAL (2012), WHITE COLLAR CRIME: CASES AND MATERIALS.

POSNER, RICHARD A. (2014), ECONOMIC ANALYSIS OF LAW, 9th ed.

ROOT, STEVEN J. (1998), BEYOND COSO: INTERNAL CONTROL TO ENHANCE CORPORATE GOVERNANCE.

SAUNDERS, ANTHONY & MARICA MILLON CORNETT (2011), FINANCIAL INSTITUTIONS MANAGEMENT: A RISK MANAGEMENT APPROACH, 7th ed.

SOBEK, DURWARD K. II & ART SMALLEY (2008), UNDERSTANDING A3 THINKING: A CRITICAL COMPONENT OF TOYOTA'S PDCA MANAGEMENT SYSTEM.

THE COMMITTEE ON SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION [COSO] (1992), INTERNAL CONTROL—INTEGRATED FRAMEWORK.

TROKLUS, DEBBIE & SHERYL VACCA (2013), INTERNATIONAL COMPLIANCE 101: HOW TO BUILD AND MAINTAIN AN EFFECTIVE COMPLIANCE AND ETHICS PROGRAM.

（二）書之篇章

Armour, John et al. (2017), *Agency Problems and Legal Strategies*, *in* THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH 29 (Reinier Kraakman et al. eds., 2d ed.).

Armour, John et al. (2017), *What Is Corporate Law?*, *in* THE ANATOMY OF CORPORATE LAW: A COMPARATIVE AND FUNCTIONAL APPROACH 1 (Reinier Kraakman et al. eds., 2d ed.).

Gospel, Howard & Andrew Pendleton (2005), *Corporate Governance and Labour Management: An International Comparision*, *in* CORPORATE GOVERNANCE AND LABOUR MANAGEMENT: AN INTERNATIONAL COMPARISION 1 (Howard Gospel & Andrew Pendleton et al. eds.).

Hopt, Klaus J. (2012), *Corporate Governance of Banks After the Financial Crisis*, *in* FINANCIAL REGULATION AND SUPERVISION: A POST-CRISIS ANALYSIS (Eddy Wymeersch et al. eds.).

doi:10.6342/NTU202000744

Treviño, Linda et al. (2018), *The Invisible Role of Middle Management: Unethical Behaviour and Unrealistic Expectations*, *in* TRANSFORMING CULTURE IN FINANCIAL SERVICES 68 (Financial Conduct Authority ed.).

（三）期刊論文

Bai, Chong-En et al. (2004), *Corporate Governance and Market Valuation in China*, 32(4) JOURNAL OF COMPARATIVE ECONOMICS 599.

Bainbridge, Stephen M. (2009), Caremark *and Enterprise Risk Management*, 34(4) THE JOURNAL OF CORPORATE LAW 967.

Baker, C. Richard et al. (2017), *Breakdowns in Internal Controls in Bank Trading Information Systems: The Case of Fraud at Société Générale*, 26 INTERNATIONAL JOURNAL OF ACCOUNTING INFORMATION SYSTEMS 20.

Bennett, Rebecca J. & Sandra L. Robinson (2000), *Development of a Measure of Workplace Deviance*, 85(3) JOURNAL OF APPLIED PSYCHOLOGY 349.

Blair, Margaret M. & Lynn A. Stout (1999), *A Team Protection Theory of Corporate Law*, 85(2) VIRGINIA LAW REVIEW 247.

Den Nieuwenboer, Niki A. et al. (2017), *Middle Managers and Corruptive Routine Translation: The Social Production of Deceptive Performance*, 28(5) ORGANIZATION SCIENCE 781.

Denis, Diane K. & John J. McConnell (2003), *International Corporate Governance*, 38(1) THE JOURNAL OF FINANCIAL AND QUANTITATIVE ANALYSIS 1.

Eisenberg, Melvin A. (1997), *The Board of Directors and Internal Control*, 19(2) CARDOZO LAW REVIEW 237.

Elhauge, Einer (2005), *Sacrificing Corporate Profits in the Public Interests*, 80(3) NEW YORK UNIVERSITY LAW REVIEW 733.

Ferola, Peter (2006), *Internal Controls in the Aftermath of Sarbanes-Oxley: One Size Doesn't Fit All*, 48(1) SOUTH TEXAS LAW REVIEW 87.

Ferroni, Stefano (2016), *Implementing Segregation of Duties: A Practical Experience Based on Best Practices*, 3 ISACA JOURNAL 1.

Gillan, Stuart L. (2006), *Recent Developments in Corporate Governance: An Overview*, 12(3) JOURNAL OF CORPORATE FINANCE 381.

Jensen, Michael C. (1993), *The Modern Industrial Revolution, Exit, and the Failure of Internal Control Systems*, 48(3) THE JOURNAL OF FINANCE 831.

doi:10.6342/NTU202000744

Kartikowati, Rr. Sri (2013), *The Technique of "Plan Do Check and Act" to Improve Trainee Teacher's Skills*, 9(12) ASIAN SOCIAL SCIENCE 268.

Klein, Howard J. & Natasha A. Weaver (2000), *The Effectiveness of an Organizational-Level Orientation Training Program in the Socialization of New Hires*, 53(1) PERSONNEL PSYCHOLOGY 47.

Lemieux, Catharine M. (1999), *Conglomerates, Connected Lending and Prudential Standards: Lessons Learned*, 4(1) UCLA JOURNAL OF INTERNATIONAL LAW AND FOREIGN AFFAIRS 149.

Macey, Jonathan & Maureen O'Hara (2016), *Bank Corporate Governance: A Proposal for the Post-Crisis World*, 22(1) FEDERAL RESEARCH BANK OF NEW YORK ECONOMIC POLICY REVIEW 85.

Macey, Jonathan R. & Maureen O'Hara (2003), *The Corporate Governance of Banks*, 9(1) FEDERAL RESEARCH BANK OF NEW YORK ECONOMIC POLICY REVIEW 91.

Minow, Martha (2013), *Archetypal Legal Scholarship: A Field Guide*, 63(1) JOURNAL OF LEGAL EDUCATION 66.

The Committee on Law and Accounting (1994), *"Management" Reports on Internal Control: A Legal Perspective*, 49(2) THE BUSINESS LAWYER 889.

Walsh, John H. (2008), *Institution-Based Financial Regulation: A Third Paradigm*, 49(2) HARVARD INTERNATIONAL LAW JOURNAL 381.

Weaver, Gary R. & Linda Klebe Treviño (2001), *The Role of Human Resources in Ethics/Compliance Management: A Fairness Perspective*, 11(1-2) HUMAN RESOURCE MANAGEMENT REVIEW 113.

Yokoi-Arai, Mamiko (2003), *The Evolving Concept of Operational Risk and Its Regulatory Treatment*, 9(1) LAW AND BUSINESS REVIEW OF THE AMERICAS 103.

（四）官方文件

BASEL COMMITTEE ON BANKING SUPERVISION (1997), CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION, https://www.bis.org/publ/bcbs30a.pdf

BASEL COMMITTEE ON BANKING SUPERVISION (1998), INTERNAL CONTROL SYSTEMS IN BANKING ORGANISATIONS.

BASEL COMMITTEE ON BANKING SUPERVISION (2004), INTERNATIONAL CONVERGENCE OF CAPITAL MEASUREMENT AND CAPITAL STANDARDS: A REVISED FRAMEWORK.

BASEL COMMITTEE ON BANKING SUPERVISION (2005), COMPLIANCE AND THE COMPLIANCE FUNCTION IN BANKS.

doi:10.6342/NTU202000744

BASEL COMMITTEE ON BANKING SUPERVISION (2006), CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION, https://www.bis.org/publ/bcbs129.pdf.

BASEL COMMITTEE ON BANKING SUPERVISION (2010), PRINCIPLES FOR ENHANCING CORPORATE GOVERNANCE, https://www.bis.org/publ/bcbs176.pdf.

BASEL COMMITTEE ON BANKING SUPERVISION (2011), PRINCIPLES FOR THE SOUND MANAGEMENT OF OPERATIONAL RISK.

BASEL COMMITTEE ON BANKING SUPERVISION (2012), CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION.

BASEL COMMITTEE ON BANKING SUPERVISION (2015), GUIDELINES: CORPORATE GOVERNANCE PRINCIPLES FOR BANKS.

BASEL COMMITTEE ON BANKING SUPERVISION (2017), BASEL III: FINALISING POST-CRISIS REFORMS.

Directive 2014/95/EU, of the European Parliament and of the Council of 22 October 2014 Amending Directive 2013/34/EU as Regards Disclosure of Non-Financial and Diversity Information by Certain Large Undertakings and Groups, 2014 O.J. (L 330).

European Commission Green Paper: The EU Corporate Governance Framework, COM (2011) 164 final (April 5, 2011).

EUROPEAN SYSTEMIC RISK BOARD (2015), REPORT ON MISCONDUCT RISK IN THE BANKING SECTOR.

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (2014), BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL.

FINANCIAL REPORTING COUNCIL (2005), INTERNAL CONTROL: REVISED GUIDANCE FOR DIRECTORS ON THE COMBINED CODE.

FINANCIAL REPORTING COUNCIL (2010), THE UK CORPORATE GOVERNANCE CODE.

FINANCIAL REPORTING COUNCIL (2011), BOARDS AND RISK: A SUMMARY OF DISCUSSIONS WITH COMPANIES, INVESTORS AND ADVISORS.

FINANCIAL REPORTING COUNCIL (2014), GUIDANCE ON RISK MANAGEMENT, INTERNAL CONTROL AND RELATED FINANCIAL AND BUSINESS REPORTING.

MEHRAN, HAMID & LINDSAY MOLLINEAUX (2012), FEDERAL RESERVE BANK OF NEW YORK STAFF REPORTS: CORPORATE GOVERNANCE OF FINANCIAL INSTITUTIONS.

NATIONAL COMMISSION ON FRAUDULENT FINANCIAL REPORTING (1987), REPORT OF THE NATIONAL COMMISSION ON FRAUDULENT FINANCIAL REPORTING, https://www.coso.org/Documents/NCFFR.pdf.

doi:10.6342/NTU202000744

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES (2016), CONSENT ORDER UNDER NEW YORK BANKING LAW §§ 39 AND 44, https://www.dfs.ny.gov/docs/about/ea/ea160819.pdf.

Organisation for Economic Co-operation and Development, *Good Practice Guidance on Internal Controls, Ethics, and Compliance* (February 18, 2010).

PARLIAMENTARY COMMISSION ON BANKING STANDARDS (2013), CHANGING BANKING FOR GOOD, https://www.parliament.uk/documents/banking-commission/Banking-final-report-vol-ii.pdf.

THE FINANCIAL ACTION TASK FORCE (2019), INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

UNITED NATIONS ENVIRONMENT PROGRAMME FINANCE INITIATIVE ASSET MANAGEMENT WORKING GROUP (2006), SHOW ME THE MONEY: LINKING ENVIRONMENTAL, SOCIAL AND GOVERNANCE ISSUES TO COMPANY VALUE.

UNITED STATES SENTENCING COMMISSION, GUIDELINES MANUAL (November 1991).

UNITED STATES SENTENCING COMMISSION, GUIDELINES MANUAL (November 2004).

WORLD ECONOMIC FORUM (2020), THE GLOBAL RISKS REPORT 2020, 15th ed.

（五）案例

In re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Court of Chancery of Delaware 1996).

United States v. Arthur Young & Co., 465 U.S. 805 (1984).

（六）法律、法案或條約

An Act to Protect Investors by Improving the Accuracy and Reliability of Corporate Disclosures Made Pursuant to the Securities Laws, and for Other Purposes, Pub. L. No. 107-204, 116 Stat. 745 (2002).

DELAWARE CODE ANNOTATED title 8.

MODEL BUSINESS CORPORATION ACT (1984) (AMERICAN BAR ASSOCIATION, amended 2016).

The Foreign Corrupt Practices Act of 1977 § 78m(b)(2)(B), 15 U.S.C. (2004).

doi:10.6342/NTU202000744

United Nations Convention Against Corruption, G.A. Res. 58/4, annex (October 13, 2003).

（七）網路資料

AU 319: Consideration of Internal Control in a Financial Statement Audit, PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD, https://pcaobus.org/Standards/Archived/Pages/AU319.aspx#ps-pcaob_0b41793f-1d94-4a6f-8a01-8e483324399e.

Basel III: International Regulatory Framework for Banks, BANK FOR INTERNATIONAL SETTLEMENTS, https://www.bis.org/bcbs/basel3.htm?m=3%7C14%7C572.

Bowen, Tim, *Phrase of the Week: To Have a Skeleton in the Cupboard*, ONE STOP ENGLISH, http://www.onestopenglish.com/community/your-english/phrase-of-the-week/phrase-of-the-week-to-have-a-skeleton-in-the-cupboard/145671.article.

Broughton, Kristin, *COSO Warns of the Downside of Siloing Risk Managers: New Guidance from the Advisory Group Emphasizes the Role of Risk Management in Maximizing Growth*, THE WALL STREET JOURNAL (February 4, 2020, 5:42 PM), https://www.wsj.com/articles/coso-warns-of-the-downside-of-siloing-risk-managers-11580856142.

BSA/AML Manual: Core Examination Procedures for Assessing the BSA/AML Compliance Program, FFIEC BANK SECRECY ACT/ANTI-MONEY LAUNDERING INFOBASE, https://bsaaml.ffiec.gov/manual/CompliancePrograM/01.

BSA/AML Manual: Core Examination Procedures for Assessing the BSA/AML Compliance Program: Examination Procedures: Scoping and Planning, FFIEC BANK SECRECY ACT/ANTI-MONEY LAUNDERING INFOBASE, https://bsaaml.ffiec.gov/manual/CompliancePrograM/01_ep.

Campbell, David N. et al., *Discipline Without Punishment—At Last*, HARVARD BUSINESS REVIEW, https://hbr.org/1985/07/discipline-without-punishment-at-last.

Corporate Governance, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, http://www.oecd.org/corporate/.

Foreign Corrupt Practices Act: An Overview, THE UNITED STATES DEPARTMENT OF JUSTICE, https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

G10, BANK FOR INTERNATIONAL SETTLEMENTS, https://www.bis.org/list/g10publications/index.htm.

doi:10.6342/NTU202000744

ISO 37001:2016(en): Anti-Bribery Management Systems — Requirements with Guidance for Use, THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, https://www.iso.org/obp/ui#iso:std:iso:37001:ed-1:v1:en:term:3.11.

Kaminski, Piotr & Kate Robu, *A Best-Practice Model for Bank Compliance*, MCKINSEY & COMPANY (January 2016), https://www.mckinsey.com/business-functions/risk/our-insights/a-best-practice-model-for-bank-compliance#.

McCleskey, Scott, *The Evolving Role and Expectations of the Chief Ethics and Compliance Officer*, CORPORATE COUNSEL BUSINESS JOURNAL (March 22, 2012), https://ccbjournal.com/articles/evolving-role-and-expectations-chief-ethics-and-compliance-officer.

Non-Financial Reporting, EUROPEAN COMMISSION, https://ec.europa.eu/info/business-economy-euro/company-reporting-and-auditing/company-reporting/non-financial-reporting_en.

Ocelewicz, Lucas & James Lewis, *Conduct Risk: Delivering an Effective Framework*, KPMG (September 26, 2017), https://home.kpmg/uk/en/home/insights/2017/09/conduct-risk-delivering-an-effective-framework.html.

Popular Standards: ISO 37001 Anti-Bribery Management Systems, THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, https://www.iso.org/iso-37001-anti-bribery-management.html.

Popular Standards: ISO 5001 Energy Management, THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, https://www.iso.org/iso-50001-energy-management.html.

Popular Standards: ISO 9000 Family — Quality Management, THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, https://www.iso.org/iso-9001-quality-management.html.

Press Release, *DFS Fines Mega Bank $180 Million for Violating Anti-Money Laundering Laws: Consent Order Requires Bank to Establish Effective Compliance Controls and to Retain Independent Monitor for Two Years*, NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES (August 19, 2016), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1608191.

Rakhmanina, Olga, *Culture Shift: Bank's Roadmap to Survival*, TAIWAN BANKER (September 2019), http://service.tabf.org.tw/TTB/Article/Detail?aID=315.

Retaliation in the Workplace Policy, WORKABLE TECHNOLOGY LIMITED, https://resources.workable.com/no-retaliation-company-policy.

doi:10.6342/NTU202000744

Segregation of Duties, ASSOCIATION OF INTERNATIONAL CERTIFIED PROFESSIONAL ACCOUNTANTS, https://www.aicpa.org/content/aicpa/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html.

The Fraud Triangle, ASSOCIATION OF CERTIFIED FRAUD EXAMINERS, https://www.acfe.com/fraud-triangle.aspx.

（八）其他資料

AMERICAN INSTITUTE OF ACCOUNTANTS (1936), EXAMINATION OF FINANCIAL STATEMENTS BY INDEPENDENT PUBLIC ACCOUNTANTS, http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1930/1936_0101_AIAExamination.pdf.

CHARTERED INSTITUTE OF INTERNAL AUDITORS (2019), POSITION PAPER: THE THREE LINES OF DEFENCE, https://www.iia.org.uk/resources/delivering-internal-audit/position-paper-the-three-lines-of-defence/?downloadPdf=true.

COMMITTEE ON AUDITING PROCEDURE, AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS (1949), INTERNAL CONTROL: ELEMENTS OF A COORDINATED SYSTEM AND ITS IMPORTANCE TO MANAGEMENT AND THE INDEPENDENT PUBLIC ACCOUNTANT, SPECIAL REPORT.

EDELMAN (2019), 2019 EDELMAN TRUST BAROMETER: GLOBAL REPORT, https://www.edelman.com/sites/g/files/aatuss191/files/2019-03/2019_Edelman_Trust_Barometer_Global_Report.pdf?utm_source=website&utm_medium=global_report&utm_campaign=downloads.

Gilbert, Mark R. & James Lundy (2003), *Demand Is Growing for a Chief Governance Officer*, GARTNER, https://www.bus.umich.edu/kresgepublic/journals/gartner/research/117400/117465/117465.pdf.

GROUP OF THIRTY (2018), BANKING CONDUCT AND CULTURE: A PERMANENT MINDSET CHANGE, https://group30.org/images/uploads/publications/aaG30_Culture2018.pdf.

Ho, Yi-Chin et al., *New York State Department of Financial Services Fines Mega Bank and Its New York Branch $180 Million for Alleged Violations of State Anti-Money Laundering Laws*, KIRKLAND & ELLIS (November 2016), https://www.kirkland.com/siteFiles/Publications/NYDFS_Fines_MegaBank_Eng.pdf.

KPMG (2015), PROTECTING AND CREATING VALUE THROUGH OPERATIONAL RISK MANAGEMENT.

doi:10.6342/NTU202000744

Larcker, David F. & Brian Tayan (2018), *Netflix Approach to Governance: Genuine Transparency with the Board* (Rock Center for Corporate Governance, Stanford University, Stanford Closer Look Series No. CGRP71).

Lopez-de-Silanes, Florencio et al. (2019), *ESG Performance and Disclosure: A Cross-Country Analysis* (European Corporate Governance Institute, Working Paper No. 481/2019).

MCNALLY, J. STEPHEN (2013), THE 2013 COSO FRAMEWORK & SOX COMPLIANCE: ONE APPROACH TO AN EFFECTIVE TRANSITION.

Mestchian, Peyman (2005), *Operational Risk Management: The Solution Is in the Problem, in* ADVANCES IN OPERATIONAL RISK: FIRM-WIDE ISSUES FOR FINANCIAL INSTITUTIONS, http://www.risknet.de/fileadmin/eLibrary/OpRisk-Mestchian-2005.pdf.

Perino, Michael A. (2002), *Enron's Legislative Aftermath: Some Reflections on the Deterrence Aspects of the Sarbanes-Oxley Act of 2002* (Center for Law & Economic Studies, Columbia University School of Law, Working Paper No. 212).

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (2004), ENTERPRISE RISK MANAGEMENT — INTEGRATED FRAMEWORK: EXECUTIVE SUMMARY.

THE COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION (2020), CREATING AND PROTECTING VALUE: UNDERSTANDING AND IMPLEMANTING ENTERPRISE RISK MANAGEMENT.

THE INSTITUTE OF INTERNAL AUDITORS (2013), IIA POSITION PAPER: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL.

THE INTERNATIONAL AUDITING AND ASSURANCE STANDARDS BOARD (2010), INTERNATIONAL FRAMEWORK FOR ASSURANCE ENGAGEMENTS, https://www.ifac.org/system/files/downloads/b003-2010-iaasb-handbook-framework.pdf.

doi:10.6342/NTU202000744