經 105.6.30 理監事聯席會議決議：修正通過

經 105.9.23 金融監督管理委員會金管銀國字第 10500206730 號函：依說明二修正後洽悉

「銀行內部控制三道防線實務守則」全文說明

條文內容	說明欄	參考資料來源
第一章　總則		
第 1 條 中華民國銀行商業同業公會全國聯合會為有效協助銀行完善內部控制制度及強健企業體質，推動內部控制三道防線理念之落實，特訂定本守則。 銀行關於內部控制三道防線架構之建立，應依本守則辦理。	102 年 4 月 2 日銀行局發文要求金融控股公司及銀行業應強化法令遵循及風險管理等第二道防線功能，以確保內部控制制度之有效性，三道防線各司其職。 此後，103 年 8 月 8 日「金融控股公司及銀行業內部控制及稽核制度實施辦法」落實修正部分條文以強化法令遵循主管之角色功能，並於總說明重申各單位負責第一道防線、內部稽核係第三道防線。惟各銀行風險管理及內部控制作業分散在多個部門及單位，為了有效協調各部門及單位間的運作，特制訂本守則。	「內部控制三道防線實務守則」，係參考下列項目： 1. 金融控股公司及銀行業內部控制及稽核制度實施辦法 2. IIA position paper：The three lines of defense in effective risk management and control 3. Leveraging COSO across the three lines of defense. (The Institute of Internal Auditors) 4. Corporate governance principles for banks (Basel Committee on Banking Supervision)
第 2 條 銀行應建立內部控制三道防線架構，明確釐清三道防線之權責範圍，以利各單位了解其各自在銀行整體風險及控制架構所扮演之角色功能，加強風險管理及內部控制工作的溝通協調，三道防線各司其職。		1. 金融監督管理委員會銀行局於民國 102 年 4 月 2 日發文要求，金融控股公司及銀行業為強化法令遵循及風險管理等第二道防線功能，以確保內部控制制度之有效性，其中第二項中說明：其中自行查核為第一道防線，法令遵循與風險管理為第二道防線，內部稽核為第三道防線，為使內部控制制度能有效及適當的運作，由第一道、第二道防線進行風險監控，第三道防線進行獨立監督，三道防線各司其職。

條文內容	說明欄	參考資料來源
		2. “IIA position paper：The three lines of defense in effective risk management and control”： The Three Lines of Defense model distinguishes among three groups (or lines) involved in effective risk management: ● Functions that own and manage risks. ● Functions that oversee risks. ● Functions that provide independent assurance.
第二章　內部控制三道防線理念		
第3條 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，謂第一道防線，其應該負責辨識及管理風險，針對該風險特性設計並執行有效的內部控制程序以涵蓋所有相關之營運活動。	本條係說明第一道防線的功能及權責範圍。第一道防線應該就其功能區分，其可能包含：業務管理單位(含作業中心)、產品單位、資訊單位及會計單位等。同一單位在某些功能可扮演第一道防線，而在其他功能可扮演第二道防線的角色，釋例說明如下： 釋例一：會計單位在編製財務報表作業時係第一道防線之範圍；但若在執行各業務單位之異常報表監控時，係第二道防線之範圍。 釋例二：資訊單位在研發新商品系統時，在其職責範圍內，係屬第一道防線；但若在監督	1. “IIA position paper：The three lines of defense in effective risk management and control”： ● As the first line of defense, operational managers own and manage risks. They also are responsible for implementing corrective actions to address process and control deficiencies. ● Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives. 2. “Corporate governance principles for banks” (Basel Committee on Banking Supervision) Article 38： ● Business units are the first line of defence. They take risks and are responsible and accountable for the ongoing management of such risks. This includes identifying, assessing and reporting such exposures, taking into account the bank’s risk appetite and its

條文內容	說明欄	參考資料來源
	全行的資訊安全時，係第二道防線之範圍。 釋例三：產品企劃管理單位在設計商品係為第一道防線;但若在管理全行的商品風險時，係第二道防線之範圍。	policies, procedures and controls. The manner in which the business line executes its responsibilities should reflect the bank's existing risk culture. 3. "Leveraging COSO across the three lines of defense" (The Institute of Internal Auditors)： ● The first line of defense lies with the business and process owners whose activities create and/or manage the risks that can facilitate or prevent an organization's objectives from being achieved. This includes taking the right risks. The first line owns the risk, and the design and execution of the organization's controls to respond to those risks. ● The first line of defense in the Model is primarily handled by front-line and mid-line managers who have day-to-day ownership and management of risk and control. Operational managers develop and implement the organization's control and risk management processes. These include internal control processes designed to identify and assess significant risks, execute activities as intended, highlight inadequate processes, address control breakdowns, and communicate to key stakeholders of the activity. Operational managers must be adequately skilled to perform these tasks within their area of operations.
第4條 第二道防線係獨立於第一道防線且非為第三道防線的其他功能及單位，依其特性協助及監督第一道防線辨識及管理風險。第二道防線包含風險管理、法令遵循及其他專職單位，其就各主要風險類別負責銀行整體風險管理政策之訂定、監督整	本條係說明第二道防線的功能及權責範圍。 除風險管理、法令遵循單位外，其他扮演第二道防線之專職單位例如：	1. "IIA position paper：The three lines of defense in effective risk management and control"： ● Management establishes various risk management and compliance functions to help build and/or monitor the first line-of-defense controls. The specific functions will vary by organization and industry, but typical functions in this second line of defense

條文內容	說明欄	參考資料來源
體風險承擔能力及承受風險現況、並向董（理）事會或高階管理階層報告風險控管情形。	1. 資訊單位對於部門本身的功能，例如資訊系統的開發程序扮演第一道防線的角色，但若涉及全行的系統管理應用及資訊安全政策，則為第二道防線。 2. 人力資源單位對於部門本身的功能，例如人員聘雇程序扮演第一道防線的角色，但若涉及全行人事政策制定及管理則為第二道防線。 各主要風險類別包括信用風險、市場風險、作業風險等。	include: (1) A risk management function (and/or committee) that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization. (2) A compliance function to monitor various specific risks such as noncompliance with applicable laws and regulations. In this capacity, the separate function reports directly to senior management, and in some business sectors, directly to the governing body. Multiple compliance functions often exist in a single organization, with responsibility for specific types of compliance monitoring, such as health and safety, supply chain, environmental, or quality monitoring. (3) A controllership function that monitors financial risks and financial reporting issues. ● Management establishes these functions to ensure the first line of defense is properly designed, in place, and operating as intended. Each of these functions has some degree of independence from the first line of defense, but they are by nature management functions. As management functions, they may intervene directly in modifying and developing the internal control and risk systems. 2. “Leveraging COSO across the three lines of defense“ (The Institute of Internal Auditors) ● The second line is put in place to support management by bringing expertise, process excellence, and management monitoring

條文內容	說明欄	參考資料來源
		alongside the first line to help ensure that risk and control are effectively managed. The second line of defense functions are separate from the first line of defense but are still under the control and direction of senior management and typically perform some management functions. The second line is essentially a management and/or oversight function that owns many aspects of the management of risk.
第5條 第三道防線係內部稽核單位，應以獨立超然之精神，執行稽核業務，協助董（理）事會及高階管理階層查核與評估風險管理及內部控制制度是否有效運作，包含評估第一道及第二道防線進行風險監控之有效性，並適時提供改進建議，以合理確保內部控制制度得以持續有效實施及作為檢討修正內部控制制度之依據。	本條係說明第三道防線的功能及權責範圍。	1. 金融監督管理委員會銀行局於民國102年4月2日發文要求，金融控股公司及銀行業為強化法令遵循及風險管理等第二道防線功能，以確保內部控制制度之有效性，其中第二項中說明：其中自行查核為第一道防線，法令遵循與風險管理為第二道防線，內部稽核為第三道防線，為使內部控制制度能有效及適當的運作，由第一道、第二道防線進行風險監控，第三道防線進行獨立監督，三道防線各司其職。 2. 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：內部稽核制度之目的，在於協助董（理）事會及管理階層查核及評估內部控制制度是否有效運作，並適時提供改進建議，以合理確保內部控制制度得以持續有效實施及作為檢討修正內部控制制度之依據。 ● 第10條：金融控股公司及銀行業應設立隸屬董（理）事會之內部稽核單位，以獨立超然之精神，執行稽核業務，並應至少每半年向董（理）事會及監察人（監事、監事會）或審計委員會報告稽核業務。 3. “IIA position paper：The three lines of defense in effective risk management and control”： ● Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the

條文內容	說明欄	參考資料來源
		first and second lines of defense achieve risk management and control objectives. 4. “Corporate governance principles for banks” (Basel Committee on Banking Supervision) Article 41： The third line of defence consists of an independent and effective internal audit function. Among other things, it provides independent review and assurance on the quality and effectiveness of the bank’s risk governance framework including links to organisational culture, as well as strategic and business planning, compensation and decision-making processes. Internal auditors must be competent and appropriately trained and not involved in developing, implementing or operating the risk management function. 5. “Leveraging COSO across the three lines of defense“ (The Institute of Internal Auditors)： ● The third line provides assurance to senior management and the board over both the first and second lines’ efforts consistent with the expectations of the board of directors and senior management. The third line of defense is typically not permitted to perform management functions to protect its objectivity and organizational independence. In addition, the third line has a primary reporting line to the board. As such, the third line is an assurance not a management function, which separates it from the second line of defense. ● Internal auditors serve as an organization’s third line of defense. The IIA defines internal auditing as an “independent, objective assurance and consulting activity designed to add value and improve an organization’s

條文內容	說明欄	參考資料來源
		operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." ● What distinguishes internal audit from the other two lines of defense is its high level of organizational independence and objectivity.
第 6 條 銀行的董（理）事會及高階管理階層應積極協助及指導三道防線之建立，清楚界定各道防線之角色功能及權責。 管理階層建立三道防線架構時，應考量各銀行活動的性質、大小、複雜程度及風險狀況進行調整，但其調整需能確保三道防線之有效性。 董（理）事會及高階管理階層應持續確保組織架構符合三道防線原則，督導該架構之有效運作，並對其有效性負最終之責任。	1. 本條係說明董（理）事會及高階管理階層對三道防線建置的責任。 高階管理階層包括總經理、副總經理等負責銀行最高決策者。 管理階層係指中階管理人員，負責將高階管理階層所訂目標轉化為第一線人員可以執行的明確作業活動。 2. 銀行應就各主要風險類別清楚界定各道防線之角色功能及權責。	1. "IIA position paper：The three lines of defense in effective risk management and control"： ● Governing bodies and senior management are the primary stakeholders served by the "lines," and they are the parties best positioned to help ensure that the Three Lines of Defense model is reflected in the organization's risk management and control processes. ● The Three Lines of Defense model is best implemented with the active support and guidance of the organization's governing body and senior management. 2. "Corporate governance principles for banks" (Basel Committee on Banking Supervision) Article 37： ● Depending on the bank's nature, size and complexity, and the risk profile of its activities, the specifics of how these three lines of defence are structured can vary. Regardless of the structure, responsibilities for each line of defence should be well defined and communicated. 3. "Leveraging COSO across the three lines of defense" (The Institute of Internal Auditors) ● The Model enhances understanding of risk management and control by clarifying roles and duties. Its underlying premise is that, under the oversight and direction of senior

條文內容	說明欄	參考資料來源
		management and the board of directors, three separate groups (or lines of defense) within the organization are necessary for effective management of risk and control. ● The Three Lines of Defense Model is purposely designed to be flexible. Each organization should implement the model in a way that is suitable for their industry, size, operating structure, and approach to risk management. However, the overall governance and control environment normally is strongest when there are three separate and clearly defined lines of defense. Organizations should strive to implement a governance structure that is consistent with the Model such that all three lines exist in some form, regardless of size or complexity of the organization. The “lines” should be distinct, with separate roles and responsibilities, clearly articulated in the appropriate policies and procedures of the organization, and reinforced by a consistent “tone from the top.
第三章　三道防線之角色與功能		
第７條 第一道防線負責及持續管理營運活動所產生的相關風險，包含下列各款： 一、 辨識、評估、控制及降低營運活動所產生的風險，確保營運活動與銀行目標及任務一致。 二、 第一道防線應將風險控制在其單位可承擔之範圍內，依需要向第二道防線報導其曝險狀況。 三、 建立內部控制程序。 四、 執行風險管理程序並維持有效的內部控制。	本條係說明第一道防線負責的角色與功能，及承擔風險後須設立之相關自我評估機制，例如內部控制制度自行查核及法令遵循作業自行查核等。 有關第一道防線需要向第二道防線報導之事項，各銀行應依內部監督需要由第二道防線自行決定。	1. “IIA position paper：The three lines of defense in effective risk management and control”： ● As the first line of defense, operational managers own and manage risks. They also are responsible for implementing corrective actions to address process and control deficiencies. ● Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are

條文內容	說明欄	參考資料來源
五、 當流程及控制程序不足時，應立即提出改善計畫。 第一道防線應定期或不定期就前項內容辦理自我評估，以確保風險有被適當控管。		consistent with goals and objectives. 2. "Corporate governance principles for banks" (Basel Committee on Banking Supervision) Article 11： ● The business line – the first line of defence – has "ownership" of risk whereby it acknowledges and manages the risk that it incurs in conducting its activities. 3. "Corporate governance principles for banks" (Basel Committee on Banking Supervision) Article 38： ● Business units are the first line of defence. They take risks and are responsible and accountable for the ongoing management of such risks. This includes identifying, assessing and reporting such exposures, taking into account the bank's risk appetite and its policies, procedures and controls. The manner in which the business line executes its responsibilities should reflect the bank's existing risk culture. 4. "Leveraging COSO across the three lines of defense" (The Institute of Internal Auditors) ● The first line of defense in the Model is primarily handled by front-line and mid-line managers who have day-to-day ownership and management of risk and control. Operational managers develop and implement the organization's control and risk management processes. These include internal control processes designed to identify and assess significant risks, execute activities as intended, highlight inadequate processes, address control breakdowns, and communicate to key stakeholders of the activity. Operational managers must be adequately skilled to perform these tasks within their area of operations.

條文內容	說明欄	參考資料來源
		5. 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 ● 金融控股公司各單位及子公司每年至少須辦理一次內部控制制度自行查核，以及每半年至少須辦理一次法令遵循作業自行查核。
第 8 條 第二道防線的功能係在訂定整體政策及建立管理制度，協助及監督第一道防線管理風險**與自我評估執行情形**。依照不同的功能性質，第二道防線之權責包含協助辨識及衡量風險、定義風險管理角色及責任、提供風險管理架構及定期將風險管理結果呈報高階管理階層。說明如下： 一、 風險管理單位負責建立獨立有效的風險管理機制，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。 二、 法令遵循單位負責法令遵循制度之規劃、管理及執行，訂定法令遵循之評估內容與程序，並督導各單位定期辦理法令遵循自行評估及綜理法令遵循事務。 三、 其他專職單位，包含但不限於財務控制、人力資源、法務等。	本條係說明第二道防線負責的角色與功能，相關參考資料請詳下列包含下列項目： 1. “Corporate governance principles for banks” (Basel Committee on Banking Supervision) Article 103 2. 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 3. “Leveraging COSO across the three lines of defense ”(The Institute of Internal Auditors)	1. “IIA position paper：The three lines of defense in effective risk management and control”： ● A risk management function (and/or committee) that facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization. ● A compliance function to monitor various specific risks such as noncompliance with applicable laws and regulations. In this capacity, the separate function reports directly to senior management, and in some business sectors, directly to the governing body. Multiple compliance functions often exist in a single organization, with responsibility for specific types of compliance monitoring, such as health and safety, supply chain, environmental, or quality monitoring. ● A controllership function that monitors financial risks and financial reporting issues. ● The responsibilities of these functions vary on their specific nature, but can include: (1) Supporting management policies, defining roles and responsibilities, and setting goals for implementation. (2) Providing risk management frameworks. (3) Identifying known and emerging issues. (4) Identifying shifts in the organization’s implicit risk appetite. (5) Assisting management in developing

條文內容	說明欄	參考資料來源
		processes and controls to manage risks and issues. (6) Providing guidance and training on risk management processes. (7) Facilitating and monitoring implementation of effective risk management practices by operational management. (8) Alerting operational management to emerging issues and changing regulatory and risk scenarios. (9) Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies. 2. "Leveraging COSO across the three lines of defense" (The Institute of Internal Auditors) ● The second line of defense includes various risk management and compliance functions put in place by management to help ensure controls and risk management processes implemented by the first line of defense are designed appropriately and operating as intended. These are management functions; separate from first-line operating management, but still under the control and direction of senior management. Functions in the second line are typically responsible for ongoing monitoring of control and risk. They often work closely with operating management to help define implementation strategy, provide expertise in risk, implement policies and procedures, and collect information to create an enterprise-wide view of risk and control. ● The responsibilities of individuals within the second line of defense vary widely but typically include: (1) Assisting management in design and

條文內容	說明欄	參考資料來源
		development of processes and controls to manage risks. (2) Defining activities to monitor and how to measure success as compared to management expectations. (3) Monitoring the adequacy and effectiveness of internal control activities. (4) Escalating critical issues, emerging risks and outliers (5) Providing risk management frameworks. (6) Identifying and monitoring known and emerging issues affecting the organization's risks and controls. (7) Identifying shifts in the organization's implicit risk appetite and risk tolerance. (8) Providing guidance and training related to risk management and control processes.
第 9 條 內部稽核單位係第三道防線，負責查核與評估第一道及第二道防線所設計並執行之內部控制與風險管理制度之有效性，**並適時提供改進建議**。	此條係說明第三道防線之角色與功能，具體內容應依相關規定辦理。	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： 內部控制之基本目的在於促進金融控股公司及銀行業健全經營，並應由其董（理）事會、管理階層及所有從業人員共同遵行，以合理確保達成下列目標： 一、營運之效果及效率。 二、報導具可靠性、及時性、透明性及符合相關規範。 三、相關法令規章之遵循。 前項第一款所稱營運之效果及效率目標，包括獲利、績效及保障資產安全等目標。 第一項第二款所稱之報導，包括金融控股公司及銀行業內部與外部財務報導及非財務報導。其中外部財務報導之目標，包括確保對外之財務報表係依照一般公認會計原則編製，交易經適當核准等目標。 ● 第 7 條： 金融控股公司（含子公司）與銀行業之內部控制制度應包含下列組成要素：

條文內容	說明欄	參考資料來源
		一、控制環境：係金融控股公司及銀行業設計及執行內部控制制度之基礎。控制環境包括金融控股公司及銀行業之誠信與道德價值、董（理）事會及監察人（監事、監事會）或審計委員會治理監督責任、組織結構、權責分派、人力資源政策、績效衡量及獎懲等。董事會與經理人應建立內部行為準則，包括訂定董事行為準則、員工行為準則等事項。 二、風險評估：風險評估之先決條件為確立各項目標，並與金融控股公司及銀行業不同層級單位相連結，同時需考慮金融控股公司及銀行業目標之適合性。管理階層應考量金融控股公司及銀行業外部環境與商業模式改變之影響，以及可能發生之舞弊情事。其評估結果，可協助金融控股公司及銀行業及時設計、修正及執行必要之控制作業。 三、控制作業：係指金融控股公司及銀行業依據風險評估結果，採用適當政策與程序之行動，將風險控制在可承受範圍之內。控制作業之執行應包括金融控股公司及銀行業所有層級、業務流程內之各個階段、所有科技環境等範圍、對子公司之監督與管理、適當之職務分工，且管理階層及員工不應擔任責任相衝突之工作。 四、資訊與溝通：係指金融控股公司及銀行業蒐集、產生及使用來自內部與外部之攸關、具品質之資訊，以支持內部控制其他組成要素之持續運作，並確保資訊在金融控股公司及銀行業內部與外部之間皆能進行有效溝通。內部控制制度須具備產生規劃、執行、監督等所需資訊及提供資訊需求者適時取得資訊之機制，並保有完整之財務、營運及遵循資訊。有效之內部控制制度應建立有效之溝通管道。 五、監督作業：係指金融控股公司及銀行業進行持續性評估、個別評估或兩者併行，以確定內部控制制度之各組成要素是否已經存在及持續運作。持續性評估係指不同層級營運過程中之例行評估；個別評估係由內部稽核人員、監察人（監事、監事會）或審計委員會、董事會等其他人員進行評估。對於所發現之內部控制制度缺失，應向適當層級之管理階層、董事會及監察人（監事、監事會）或審計委員會溝通，並及時改善。

條文內容	說明欄	參考資料來源
		2. “IIA position paper：The three lines of defense in effective risk management and control”： ● Internal auditors provide the governing body and senior management with comprehensive assurance based on the highest level of independence and objectivity within the organization. This high level of independence is not available in the second line of defense. Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defense achieve risk management and control objectives. The scope of this assurance, which is reported to senior management and to the governing body, usually covers: (1) A broad range of objectives, including efficiency and effectiveness of operations; safeguarding of assets; reliability and integrity of reporting processes; and compliance with laws, regulations, policies, procedures, and contracts. (2) All elements of the risk management and internal control framework, which includes: internal control environment; all elements of an organization’s risk management framework (i.e., risk identification, risk assessment, and response); information and communication; and monitoring. (3) The overall entity, divisions, subsidiaries, operating units, and functions — including business processes, such as sales, production, marketing, safety, customer functions, and operations — as well as supporting functions (e.g., revenue and expenditure

條文內容	說明欄	參考資料來源
		accounting, human resources, purchasing, payroll, budgeting, infrastructure and asset management, inventory, and information technology). 3. "Leveraging COSO across the three lines of defense "(The Institute of Internal Auditors) ● Among other roles, internal audit provides assurance regarding the efficiency and effectiveness of governance, risk management, and internal control. The scope of internal audit work can encompass all aspects of an organization's operations and activities. 4. Corporate governance principles for banks (Basel Committee on Banking Supervision) Article 14： ● Independent validation and verification are components of the third line of defence in the governance structure used to manage operational risk, and serve as a challenge function to the other two lines of defence. ● The depth and extent of the validation and verification efforts should be consistent with the materiality and complexity of the risk being managed.
第四章　三道防線間之協調		
第 10 條 各銀行的組織架構雖然不盡相同，惟仍須依風險管理及控制架構中各道防線所扮演之角色功能進行協調，運作之原則如下： 一、 風險管理及控制流程的建構應遵循三道防線模式。 二、 各道防線均應本於其角色定位及職掌，確實執行及管理相關業務。	本條係說明各道防線依其功能在執行風險控管時，應**互相協調彼此**分享知識及資訊，以協助所有的功能能夠更有效的完成各道防線的角色。	1. "IIA position paper：The three lines of defense in effective risk management and control"： ● Because every organization is unique and specific situations vary, there is no one "right" way to coordinate the Three Lines of Defense. When assigning specific duties and coordinating among risk management functions, however, it can be helpful to keep in mind the underlying role of each group in the risk management process. 2. "Leveraging COSO across the three lines of

條文內容	說明欄	參考資料來源
三、 各道防線應**互相**協調，以促進效果及效率。 四、 各道防線之風險管理及控制功能運作結果，應**互相**分享知識與資訊，以協助所有功能更有效完成其職責。		defense ”(The Institute of Internal Auditors) The Three Lines of Defense Model is purposely designed to be flexible. Each organization should implement the model in a way that is suitable for their industry, size, operating structure, and approach to risk management. However, the overall governance and control environment normally is strongest when there are three separate and clearly defined lines of defense. Organizations should strive to implement a governance structure that is consistent with the Model such that all three lines exist in some form, regardless of size or complexity of the organization. The “lines” should be distinct, with separate roles and responsibilities, clearly articulated in the appropriate policies and procedures of the organization, and reinforced by a consistent “tone from the top. 3. “ IIA position paper ： The three lines of defense in effective risk management and control” ： ● Recommended practices： (1) Risk and control processes should be structured in accordance with the Three Lines of Defense model. (2) Each line of defense should be supported by appropriate policies and role definitions. (3) There should be proper coordination among the separate lines of defense to foster efficiency and effectiveness. (4) Risk and control functions operating at the different lines should appropriately share knowledge and information to assist all functions in better accomplishing their roles in an efficient manner. (5) Lines of defense should not be

條文內容	說明欄	參考資料來源
		combined or coordinated in a manner that compromises their effectiveness. In situations where functions at different lines are combined, the governing body should be advised of the structure and its impact. For organizations that have not established an internal audit activity, management and/or the governing body should be required to explain and disclose to their stakeholders that they have considered how adequate assurance on the effectiveness of the organization's governance, risk management, and control structure will be obtained.
第五章　附則		
第 **11** 條 「本守則經本會理事會通過，並報請金融監督管理委員會核備後施行；修正時亦同。」		