Content

Title：	Regulations Governing Implementation of Internal Control and Auditing System of Insurance Enterprises Ch
Date：	2018.05.29
Legislative：	Amended on 29 May 2018 per Order Ref. Jin-Kuan-Bao-Tsai 10704502401 of the Financial Supervisory Commission.
Content：	Article 6 An insurance enterprise that uses a computerized information processing system shall, in addition to clearly delineating the authority and responsibility of information and user departments, include at least the following control operations in its internal control system and observe the self-regulatory rules established by the trade association it belongs to: 1. Clear division of authority and responsibility of the information processing department; 2. Control of system development and program modification; 3. System documentation control; 4. Program and data access control; 5. Data input/output control; 6. Data processing control; 7. Security control of the entrance of computer room; 8. System, files, computer and communications equipment security control; 9. Control of purchase, usage, and maintenance of hardware and system software; 10. Prevention and control of spread of computer viruses and hacker invasion; 11. Control of system recovery plan, disaster backup plan and testing procedures; 12. Control of outsourcing of core businesses; 13. Confidentiality and security control of classified data of customers and company; and 14. Prevention and control of computer crimes. The Life Insurance Association of the Republic of China and The Non-Life Insurance Association of the Republic of China shall establish and periodically review self-regulatory rules for information security. Article 6-1 An insurance enterprise shall set up a dedicated information security unit and appoint a chief information security officer that may not handle concurrently information operation or other affairs that may pose a conflict of interest, and shall be allocated with proper manpower resources and equipment, except as otherwise provided by the competent authority with respect to insurance cooperatives. An insurance enterprise whose total assets in the previous year as audited by a CPA exceed NTD 1 trillion shall set up a dedicated information security unit with independent function and appoint a person at the level of associate general manager or higher or a person in an equivalent position to be the chief officer of such dedicated information security unit. The dedicated information security unit of an insurance enterprise is in charge of planning, monitoring and implementing information security management operation. The chief information security officer shall, together with the chairmen of the board (council), the general manager, and the chief auditor, jointly issue a Declaration of Overall Information Security Implementation (Attachment 1), specifying the implementation of information security in the previous year, and report same to the board of directors (council) within three months after the end of each fiscal year. The personnel of the dedicated information security unit of an insurance

enterprise shall attend at least 15 hours of professional courses on information security, or on-the-job training every year. The personnel of the head office, domestic and foreign business units, product development management unit, fund utilization unit, information units, asset custody unit, and other management units shall attend at least 3 hours of information security courses every year.
Insurance enterprises governed by Paragraph 2 hereof shall make adjustment to become compliant within six months after it meets the applicable condition set forth therein.

Article 25
The general manager of an insurance enterprise shall supervise all units to carefully assess and review the implementation status of its internal control system. The chairman, general manager, chief auditor and head office chief compliance officer shall jointly issue an internal control system statement (Attachment 2), which shall be submitted to the board of directors for approval, and submitted together with the annual report set forth in Article 148-1 of the Act to the competent authority before the end of March each year.
An insurance enterprise shall disclose its internal control system statement on its website.

Article 30
The head office of an insurance enterprise shall, based on its size, business nature and organizational characteristics, establish a compliance unit directly under the general manager to take charge of the planning, management and implementation of regulatory compliance system.
The compliance unit shall establish the position of head office chief compliance officer who oversees the compliance matters and reports to the board of directors (council) and supervisors or the audit committee at least semiannually, and in case of any major regulatory violation, immediately inform the directors (council members) and supervisors, and report to the board of directors (council) on compliance matters.
The requirements for establishing a compliance unit and the position of head office chief compliance officer under the preceding two paragraphs are as follows:
1. An insurance enterprise whose total assets in the previous year as audited by a CPA exceed NTD 1 trillion shall set up a dedicated compliance unit that may also take charge anti-money laundering and combating terrorist financing (AML/CFT) affairs, but may not take charge of legal affairs unrelated to the planning, management and implementation of legal compliance system or any other affairs that may pose a conflict of interest. The head office chief compliance officer may also serve concurrently as the head of dedicated AML/CFT unit but may not serve concurrently as the chief legal officer or hold other internal posts.
2. For insurance enterprises not governed by the preceding subparagraph, their head office chief compliance officer may not concurrently hold internal positions other than the chief legal officer and the head of dedicated AML/CFT compliance unit.
The head office chief compliance officer of an insurance enterprise shall have a position equivalent to a vice general manager and possess the leadership and the ability to effectively supervise the compliance works.
The qualifications of head office chief compliance officer shall comply with the Regulations Governing Required Qualifications for Responsible Persons of Insurance Enterprises.
The branches of foreign insurance enterprises in Taiwan, reinsurance enterprises and insurance cooperatives may appoint a high level manager to act as the head office chief compliance officer under the preceding paragraph, and insurance cooperatives are not subject to the restriction on head office chief compliance officer holding concurrently other internal positions under Paragraph 3 hereof.
Chief auditor, head of audit unit and internal auditors may not serve as the head office chief compliance officer under Paragraph 2 hereof.
The appointment and dismissal of head office chief compliance officer shall have the consent of at least the majority of all directors and be reported to competent authority for record.

The head office chief compliance officer, the head and personnel of the compliance unit of an insurance enterprise shall attend at least 20 hours of on-the-job training courses a year offered by the competent authority or institutions recognized by the competent authority or held internally by the financial holding company which is the parent company of the insurance enterprise or the insurance enterprise. The training courses shall cover at least the latest regulatory amendments and new insurance products launched.
The compliance officer of the business unit, product development and management unit, fund utilization unit, information unit and asset custody unit and other units of an insurance enterprise shall attend at least 15 hours of on-the-job training a year offered by the competent authority or institutions recognized by the competent authority or held internally by the financial holding company which is the parent company of the insurance enterprise or the insurance enterprise.
The compliance officer of a foreign branch of an insurance enterprise shall attend at least 15 hours of on-the-job training courses on regulatory compliance a year offered by the local competent authority or relevant institutions. If no such training course is available, the officer may attend the training courses offered by the competent authority or institutions recognized by the competent authority or held internally by the financial holding company which is the parent company of the insurance enterprise or the insurance enterprise.
The training methods for on-the-job training set forth in the preceding three paragraphs given by the insurance enterprise itself shall be approved by the board of directors (council), and the head office shall keep the attendance records of relevant personnel for reference.
When a dedicated AML/CFT compliance unit is set up under the compliance unit, the required training for AML/CFT compliance unit personnel before their appointment and the annual required training for them after their appointment shall observe the relevant AML/CFT regulations and is not subject to the provisions of Paragraph 8 of this article and Paragraph 2 of Article 33.
An insurance enterprise shall file the list of head office chief compliance officer, head and personnel of compliance unit and their reward/disciplinary records, qualifications and training records in the past three years with the competent authority via a Web-based information system.

Article 32-1
An insurance enterprise governed by Subparagraph 1, Paragraph 3 of Article 30 shall establish a company-wide compliance risk management and supervision framework. The basis of such framework, functions and responsibilities are as follows:
1. The compliance unit shall establish procedures, plans and mechanisms for identifying, assessing, controlling, measuring, monitoring, and independently reporting any compliance risk in order to fully control, supervise, and support each domestic or foreign department, branch, and subsidiary with respect to individual business unit, cross-department and cross-border regulatory compliance matters.
2. The compliance unit shall set up an adequate number of professional units based on the classification of business or the focus of regulatory compliance to monitor, implement and support the regulatory compliance matters of the domestic or foreign business units related to that business or regulations.
3. The compliance unit may assess the appointment and enhance the independence of compliance officer under respective units using a risk-based approach. Notwithstanding to the requirements in the front section of Paragraph 1 of Article 33, units with lower compliance risk may not need to have a separate compliance officer but may be charged by the head office chief compliance officer.
4. The compliance unit shall establish the mechanism of independent reporting, assessment and response to compliance risk alert.
5. The compliance unit shall evaluate the management of compliance risks with respect to key operating activities, products and services, fund utilization or business projects, and major customer complaints where regulatory violation may be involved on a regular and ad-hoc basis, and

shall establish the horizontal communication mechanism with other second lines of defense.
6. The compliance unit may request each unit to provide relevant information in order to understand the compliance risks across the company.
7. The compliance unit shall include the evaluation of management and department heads into its opinion on their implementation of regulatory compliance program.
8. An insurance enterprise and its compliance unit shall fully understand the compliance requirements applicable to the foreign business units, and the criteria required by the local competent authority, and provide full resources and support.
9. The compliance unit shall specify the weakness of compliance risk management, and supervise the improvement plans and schedules with respect to domestic and foreign operations across the company when reporting compliance affairs to the board of directors (council) and supervisors or audit committee at least semiannually pursuant to Paragraph 2, Article 30. The board of directors (council) shall provide sufficient resources and appropriate mechanism of rewards and disciplines applicable to the business units in order to progressively establish a company-wide culture of compliance.
10. The chief auditor shall include the performance of the compliance office and the assessment opinion of the compliance status across the company when reporting the audit business to the board of directors (council) and supervisors or audit committee at least once every half year pursuant to Paragraph 1 of Article 11.
An insurance enterprise governed by the preceding paragraph shall established a dedicated compliance unit and appoint the chief compliance officer at the head office pursuant to Subparagraph 1, Paragraph 3 of Article 30 within six months after meeting the applicable conditions set forth therein, and report the adjusted company-wide compliance risk management and supervision framework to the competent authority, and file the evaluation reports under Subparagraphs 5 and 9 of the preceding paragraph with the competent authority by the end of every April pursuant to Article 148-1 of the Act.

Article 32-2
In order to promote sound operation, an insurance enterprise shall set up a whistleblower system, and designate a unit at the head office with independent functions to accept and investigate the reported cases.
An insurance enterprise shall protect the whistleblower as follows:
1. The whistleblower’s identity shall be kept confidential; no information that may be used to identify that person shall be disclosed.
2. A whistleblower shall not be terminated, dismissed, downgraded/relocated, given a reduction in pay, impairment to any entitlement under the law, contract or customs, or other unfavorable disposition due to the reported case.
Any person with conflict of interest shall recuse himself/herself from the acceptance and investigation of the reported case.
The whistleblower system under Paragraph 1 shall at least cover the following particulars and be approved by the board of directors (council):
1. The system expressly declares that anyone may file a report when discovering any crime, corruption, or potential legal violation.
2. The types of reported cases that will be accepted.
3. The system establishes and publishes the channels of reporting.
4. The process of investigation and cooperation in investigation, rules of recusal and the standard operating procedure of subsequent disposition mechanism.
5. Whistleblower protection measures.
6. Acceptance of reported case, investigation process, investigation results, records and retention of relevant documentation.
7. The whistleblower shall be given appropriate notice in writing or by other means with respect to the progress of the reported case.
If the alleged perpetrator is a director (council member), supervisor (member of the board of supervisor), or a managerial officer in a position equivalent to a vice general manager or higher, the investigation report shall be reviewed by the supervisors (board of supervisors) or the audit

committee.
An insurance enterprise shall report to or inform relevant authorities any material incident or violation discovered following an investigation.
An insurance enterprise shall regularly introduce the whistleblower system to its employees and provide relevant training.

Article 33
The head office compliance unit, business unit, product development and management unit, fund utilization unit, information unit, asset custody unit, other management units and foreign branches of an insurance enterprise shall assign personnel to act as the compliance officer of the unit to take charge of compliance matters. The position of the compliance officer in the foreign branches shall be arranged in compliance with the local laws and regulations and the requirements by the local authorities, and the compliance officer shall not hold other posts concurrently except in any of the following situations:
1. The compliance officer serves concurrently as the AML/CFT compliance officer.
2. The compliance officer may hold concurrent posts that do not constitute any conflict of interest according to local laws and regulations.
3. Where it is not clearly prescribed in local laws and regulations regarding whether or not compliance officers may hold concurrent posts, the compliance officer may hold other concurrent posts that do not result in any conflict of interest after such matter has been communicated with and confirmed by the local competent authority and reported to the competent authority for recordation.
The head office chief compliance officer and personnel of the compliance unit of an insurance enterprise as well as the compliance officer of the business unit, product development and management unit, fund utilization unit, information unit, asset custody unit, other management units and foreign branches shall meet one of the following qualification requirements prior to his/her appointment or within half a year after appointment:
1. Having worked as a compliance personnel or chief at any financial institution for at least a total of five years.
2. Having attended not less than 30 hours of courses offered by institutions recognized by the competent authority, passed the exams and received completion certificates therefor.
3. The compliance officer of a foreign branch who is employed locally has been evaluated by the insurance enterprise in accordance with its internal evaluation procedure passed by the board of directors (council) or reviewed and recognized by the local competent authority, which suffices to show his/her familiarity with local laws and regulations and his competence in related matters.
4. The compliance officer of the business unit, product development and management unit, fund utilization unit, information unit, asset custody unit and other management units of an insurance enterprise may take relevant training courses and exams not less than 30 hours held by the financial holding company which is the parent company of the insurance enterprise or the insurance enterprise in accordance with the specific training plan developed by the insurance enterprise, which suffices to show his familiarity with laws and regulations applicable to the respective unit and his competence in related matters.
Respective unit should draw up a compliance manual, which will be implemented after being approved by the head office chief compliance officer and the general manager.
The regulatory compliance manual shall contain at least the following particulars:
1. Regulatory compliance procedures to be adopted by each business;
2. Rules and regulations to be complied with by each business;
3. Procedures for handling violation of rules and regulations;
4. Self-evaluation procedure for regulatory compliance operation; and
5. Name list of regulatory compliance officers.
Where an insurance enterprise has a foreign branch, the regulatory compliance unit shall supervise the foreign branch conducting the following matters:
1. Gathering information on local insurance laws and regulations, fully

implementing the self-evaluation of the regulatory compliance business and ensuring the competency of the compliance officer and the adequacy of compliance resources (including personnel, equipment and training), to ensure the compliance with local laws and regulations by the foreign branches.
2. Establishing the self-evaluation and monitoring mechanism for compliance risks; for foreign branches with larger business size, higher business complexity or higher risks involved, they shall commission a local independent expert to verify the effectiveness of their self-evaluation and monitoring mechanism for compliance risks.

Article 38
An insurance enterprise should establish necessary controls for its subsidiaries in its internal control system and urge its subsidiaries to establish internal control system in consideration of local rules and regulations at where each subsidiary is located and the actual nature of the subsidiary's operations.
An insurance enterprise shall establish a group-wide AML/CFT program, including information sharing policies and procedures for the purpose of AML/CFT under the laws and regulations of the jurisdiction where such foreign branch (or subsidiary) is located.
An insurance enterprise shall establish audit plans targeted at each subsidiary in its annual audit plans based on the business risk profile and implementation of internal audits by each subsidiary.
All subsidiaries of an insurance enterprise shall submit to the parent company their board meeting minutes, CPA audit reports, examination reports issued by the financial examination agency, and other relevant materials. For subsidiaries having established an internal audit unit, audit plans and reports on significant deficiencies identified in internal audit and the status of improvements thereof shall also be submitted. The parent company shall review such documents and monitor the improvement actions taken by each subsidiary.
The chief auditor of an insurance enterprise shall periodically evaluate the effectiveness of the internal control activities of a subsidiary, and after having reported to the board of directors, send the evaluation results to the subsidiary's board of directors for their reference in personnel evaluations.

Article 41
These Regulations shall be in force on the date of promulgation.
Except for the part on management of financial consumers' protection which has been in force since December 30, 2011, the provisions of Article 5 amended on February 4, 2012 shall enter into force three months after the date of promulgation.
The provisions of Article 32-2 amended on May 29, 2018 shall take effect six months after promulgation.