


<b>Title :</b>	<a href="#"><u>Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries (2017.03.22 Modified)</u></a> 
----------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Chapter 1 General Principles

- Article 1 These regulations are enacted in accordance with Article 51 of Financial Holding Company Act; Paragraph 1, Article 45-1 of Banking Act; Paragraph 1, Article 21 of Credit Cooperatives Act; Article 43 of Act Governing Bills Finance Business; Paragraph 3, Article 42 of Trust Enterprise Act.
- Article 2 The "banking business" referred to in these regulations include banking institutions, credit cooperatives, bills and trust business. Unless otherwise regulated, the internal control and internal audit system for financial and bills and trust business other than banking business shall also be governed by these regulations.
- Article 3 A financial holding companies or banking business shall establish internal control and internal audit systems and ensure the on-going and effective operation of the system to promote the sound business operation of financial holding companies (including its subsidiary companies) and the banking business.  
Financial holding companies (including its subsidiary companies) and banking business shall organize overall operation strategies, risk management policies and guidelines, draft operation plans, risk management procedure and execution guidelines.
- Article 4 The basic objectives of internal controls of a financial holding company or banking business are to promote sound operations and, through joint compliance by the board of directors, management, and all personnel, to reasonably ensure that the following objectives are achieved:
- A. Effectiveness and efficiency of operations;
  - B. Reliability, timeliness, transparency and compliance of reporting; and
  - C. Compliance with applicable rules and regulations.
- The objective of effectiveness and efficiency of operations referred to in subparagraph 1 of the preceding paragraph includes objectives such as profits, performance, and safeguarding asset

security.

The "reporting" referred to in subparagraph 2, paragraph 1 includes internal and external financial reporting and non-financial reporting of a financial holding company or banking business. The objective of external financial reporting includes ensuring that financial reports presented to external users are prepared in accordance with the generally accepted accounting principles and that all transactions are properly approved.

Article 5 The internal control system of a financial holding company or a banking business should be supported by the board of directors. If the board has opposite opinions or retain their opinions, these opinions and reasons should be notified clearly in meeting minute and sent, together with the internal control system passed by the board, to the auditor (supervisors or the board of supervisors) or to the audit committee. The same procedure should be applied if any revisions are needed.

Article 5-1 The board of directors (or the council) of a financial holding company or a banking business should be aware of the operational risks faced by the company or business, supervise its operating results and bears the ultimate responsibility for ensuring the establishment and maintenance of appropriate and effective internal control system.

## **Chapter 2 The Design and Execution of Internal Control System**

Article 6 A financial holding company or a banking business should establish three lines of defense in internal control system, including self-inspection system, legal compliance system and risk management mechanism, and internal audit system to ensure their on-going and effective operation. The procedure for implementing the code of practice for three lines of defense in internal control system established by banks will be set out by The Bankers Association of The Republic of China and filed with the competent authority for recordation.

Article 7 The internal control system of a financial holding company (including its subsidiary company) and a banking business shall incorporate the following components:

A. Control Environment: Control environment is the basis for the design and implementation of internal control systems across a financial holding company or banking business. It encompasses the integrity and ethical values of a financial holding company or banking business, governance oversight responsibility of its board of directors (or the council) and supervisors (board of supervisors) or audit committee, organizational structure, assignment of authority and responsibility, human resources policy, performance measures, and awards and disciplines. The board of directors (or the council) and management should establish internal code of conduct, including code of conduct for directors and code of conduct for employees.

B. Risk Assessment: A precondition to risk assessment is the identification of objectives, linked at different levels of the financial holding company or banking business, and the suitability of the objectives should also be taken into consideration. The management shall consider the impact of changes in the external environment and within its own business model and possible fraud scenarios. The risk assessment results can assist the financial holding company or banking business in designing, correcting, and implementing necessary controls in a timely manner.

C. Control Operations: Control operations means the actions of adopting proper policies and procedures by a financial holding company or banking business based on the risk assessment results to control risks within a tolerable range. Control operations shall be performed at all levels of a financial holding company or business, at various stages of business processes, and over the technological environment, and shall include supervision and management of subsidiaries, appropriate segregation of duties and that management and employees are not assigned conflicting responsibilities.

D. Information and Communication: Information and communication means relevant and quality information that a financial holding company or banking business obtains, generates, or uses from both internal and external sources to support the continuous functioning of other components of internal control, and to ensure that information can be effectively communicated within and outside the organization. The internal control system

must have mechanisms to generate information necessary for planning, implementation, and supervision and to enable timely access to information by those who need it, and the system should maintain comprehensive internal financial, operational and compliance data. An effective internal control system shall also establish effective channels of communication.

E. Monitoring Operations: Monitoring operations means ongoing evaluations, individual evaluations, or combination of the two undertaken by a financial holding company or banking business to ascertain whether each of the components of internal control is present and continuously functioning. Ongoing evaluations means routine evaluations built into the course of operations at different levels. Individual evaluations are evaluations conducted by different personnel such as internal auditors, supervisors (or board of supervisors) or audit committee, or the board of directors (or the council). Findings of deficiencies of the internal control system shall be communicated to management of appropriate levels, the board of directors (or the council), and supervisors (board of supervisors) or audit committee, and improvements shall be made in a timely manner.

Article 7-1 The code of conduct for directors (council members) mentioned in Subparagraph 1 of the preceding article shall contain at least the rules that when a director (council member) discovers that the financial holding company or banking business is in danger of sustaining material loss or damage, the director (council member) should promptly take appropriate actions and immediately notify the audit committee or independent director members of the audit committee or supervisors (board of supervisors), and report to the board of directors (or the council), and supervise the financial holding company or banking business to report to the competent authority.

Article 8 The internal control system shall cover all business activities, include appropriate policies and procedures as follows, and shall be reviewed and revised in a timely manner:

1. Organizational chart or corporate rules and bylaws, including a clear organizational system, unit functions, scope of operations for each unit, and rules governing authorizations

and hierarchical delegation of responsibilities.

2. Related operational guidelines and procedural manuals, including:

- (1) Investment guidelines.
- (2) Customer data confidentiality.
- (3) Regulation on interested party transactions.
- (4) Shares management.
- (5) Management of the preparation process of financial statements, including management of the application of International Financial Reporting Standards, procedures for professional accounting judgments, and processes for making changes in accounting policies and estimates.
- (6) Management of administration of general affairs, information, and personnel affairs (for banking business, it should contain regulations for regular transfer and vacation).
- (7) Management of operations for disclosing information externally.
- (8) Management of financial examination report.
- (9) Management of protection of financial consumers.
- (10) Mechanism for handling major contingencies.
- (11) Mechanism for anti-money laundering and combating the financing of terrorism (AML/CFT) and management of compliance with relevant laws and regulations, including the management mechanism for identifying, assessing, and monitoring AML/CFT risks.
- (12) Other operational guidelines and operating procedures.

The business regulations and handling guides of a financial holding company shall also include the management and collaborated marketing management of its subsidiary company.

The business regulations and handling guides of a banking business should also include affairs concerning cashier, savings, exchange, loaning, foreign currency, new financial products, and outsourcing task management.

The business regulations and handling guides of a credit cooperative should also include affairs concerning cashier, savings, loaning, exchange, and outsourcing task management.

The business regulations and handling guides of a bills business should also include business such bills, bonds, and new financial

products.

The template for the operation guides of a trust business should be stipulated by the trust association of R.O.C with contents specifying business operation procedure, accounting operation procedure, computer operation procedure, personnel management system, and other items.

A trust business should establish its operation guidelines based on the reference template and make regular revisions in accordance with the alterations in legal regulations, business items, and business procedure.

The internal control system of a financial holding company or banking business whose stock is listed on the stock exchange or traded over the counter shall include the management of the operations of the remuneration committee.

The internal control system of a financial holding company or banking business that has an audit committee set up shall include management of the operation of the audit committee.

A financial holding company or banking business should set up the control tasks on their subsidiary companies in their internal control system.

If the subsidiary company resides in a foreign country, the mother company should consider the local applicable regulations issued by the government where the subsidiary company is in and the actual nature of its operation in order to supervise the subsidiary company to establish its own internal control system.

Financial holding companies and banking businesses shall establish a group-level AML/CFT program, which shall include intra-group information sharing policies and procedures for AML/CFT purposes, based on the laws and regulations of countries or jurisdictions where the foreign branches (or subsidiaries) are located.

For the stipulation, revision, or abolition of all operational and management regulations mentioned in the preceding ten paragraphs, it requires the participation of legal compliance, internal audit, and risk management agencies.

## **Chapter 3 The inspection of internal control system**

### **Section 1 Internal audit**

- Article 9 The purpose of internal audit is to assist the board of directors and the managerial level to verify and evaluate whether the operation of internal control system works effectively and smoothly and provide appropriate suggestions for revision, which can ensure the on-going performance of effective internal control and serve as the basis of internal control system revisions.
- Article 10 A financial holding company or banking business should set up an internal audit unit that is directly subsidiary to the board of directors, which should perform audit business independently and honestly. The unit is required to report its audit business to the board of directors and supervisors (board of supervisors) or audit committee at a minimum period of every six months.
- A financial holding company or banking business should establish a chief auditor system to manage all audit business. The chief auditor should possess sufficient leadership and ability to carry out effective audit work, whose qualification should be equal to the conditions set for the responsible people of each section and has the power as an general co-manager. The auditor is not allowed to take a job that will cause conflicts or limitations to the audit work. The employment, dismissal, or transfer of the chief auditor should have the consent of the majority of audit committee members as well as the consent of more than two-thirds of the board of directors and report to the competent authority for ratification.
- Where the matter in the preceding paragraph did not have the consent of the majority of audit committee members, the resolution adopted by the audit committee shall be recorded in the board meeting minutes. If there is no audit committee but independent directors set up and an independent director objects to or expresses reservations about the matter, it shall be recorded in the board meeting minutes.
- The appointment, dismissal, promotion, reward/ discipline, rotation, and performance review of personnel in the internal audit unit shall become effective after being reported by the chief auditor to chairman of the board. However, if a matter involves personnel of other management or business units, the chief auditor shall first consult the personnel department to refer the matter to the president for approval, and then report to the chairman of the

board for final approval.

The regulations in Paragraph 1 to 5 of this article doesn't apply to a company who operates financial and trust business concurrently other than a banking business.

The chief auditor of a financial holding company is allowed to, if required by business, dispatch the internal auditors of a subsidiary company to conduct the internal audit task on the financial holding company or its subsidiary company. The chief auditor should also take up the final responsibility to ensure appropriate and effective internal audit system in the financial holding company or its subsidiary company.

- Article 11 When any of the following circumstances applies to a chief auditor in overseeing internal audit work, the competent authority may, having regard to the seriousness of the event, issue an official reprimand, order the chief auditor to make improvements within a specified time limit, or otherwise order the financial holding company to release the auditor general from duty.
- A. Has made any improper loan extension, been involved in a material breach of the principles for giving credit, or otherwise engaged in any improper transfer of funds with customers, as established by factual proof.
  - B. Has abused authority of office, there is evidence showing that he or she has carried out improper activities, or he or she has misused power, in an attempt to seek profits for him or herself or for a third party, or to damage the interest of its belonging financial company (including its subsidiary company) or banking business; and therefore, his or her abuse or misuse of power has thus cause losses for its belonging financial company or its subsidiary company or banking business or a third party.
  - C. The auditor disclose, deliver, or publicize all or part of the contents of its financial examination reports to a person not related to such job without the consent from the competent authority.
  - D. Has failed to notify the competent authority of any significant malpractice that due to poor internal management has occurred in the financial holding company (including its subsidiary company) or the banking business.
  - E. Has failed to disclose in an internal audit report any significant



deficiency identified in the financial and business operations of the financial holding company (including its subsidiary company) or the banking business.

F. Has issued a fraudulent internal audit report on internal audit findings.

G. As a result of obviously insufficient staffing or staffing operations by obviously incompetent internal auditors in the financial holding company (including its subsidiary company) or banking business, has failed to identify a serious deficiency in financial and business operations.

H. Has failed to follow the instructions of the competent authority in conducting audit work or in providing relevant information.

I. Has otherwise committed any act that impairs the reputation or interests of the financial holding company (including its subsidiary company) or the banking business.

- Article 12 A financial holding company or banking business shall, after having regard to its investment scale, business condition (the number of its branches and amount of business), management needs, and relevant provisions of rules and regulations, staff competent persons in an appropriate number as full-time internal auditors who shall perform their duties in a detached, independent, objective, and impartial manner. Personnel of the internal audit unit shall be deputy to each other to cover each other's absence. An internal auditor of a financial holding company or banking business shall meet the following qualification requirements:
- A. Have no less than two(2) years of experience in financial examination; or have graduated from a junior college, college, or university or passed a senior civil service examination or an examination equivalent to senior civil service examination and have no less than two(2) years of experience in financial operations; or have no less than five (5) years of experience in financial operations. A person is deemed as meeting such requirements if he or she has worked as a professional, such as an auditor in an accounting firm, or a programmer or system analyst in a computer company for no less than two(2) years, and has received no less than three(3) months of training in financial operations and administration. However, the number of this type of auditor cannot

exceed one-third of the total auditors.

B. Free of any record of demerit or more serious from employer in the last three(3) years, unless the demerit record was a result of joint and several disciplinary action on account of the violation or offense of another person, and the demerit has been offset by other merits; and

C. If a lead auditor, have no less than three(3) years of experience in auditing or financial examination, or have no less than one(1) year of experience in auditing and no less than five(5) years of experience in financial business.

The financial holding company or the banking business shall examine at all time whether the internal auditors have violated the regulations in the preceding two paragraphs. If the auditor has violated the rules, the company should order the auditor to make improvement within two(2) months and should be transferred to other job if he or she fails to make such improvement.

- Article 13 The internal auditors of a financial holding company or banking business shall perform their duties in good faith, and may not do any of the following:
- A. Conceal or make false or inappropriate disclosures of any of the financial holding company's or the banking business's business activities, reporting, or compliance with rules and regulations that they know to directly cause damage to any interested party.
  - B. Act beyond the scope of audit functions or engage in other improper activities, or externally disclose any acquired information, attempt to profit therefrom, or otherwise use the information against the interest of the financial holding company (including its subsidiary company) or banking business.
  - C. Cause losses to the financial holding company (including its subsidiary company) or the banking business or harm the interests of its stakeholders due to negligence.
  - D. Conduct audit work within one (1) year to the department where the auditor used to work at.
  - E. Fail to recuse himself or herself from auditing of cases or business within the scope of his or her past duties or matters in which he or she has a personal interest.

F. Directly or indirectly provide, promise, demand or accept any unreasonable gift, hospitality or other improper benefits of any form to or from employees or customers of the same financial holding company (including its subsidiaries) or the banking business.

G. Fail to audit matters that the competent authority has instructed to him or her to audit or to provide relevant information.

H. Any other violation of rules, regulations or practices prohibited by the competent authority.

The financial holding company or the banking business should examine at all time whether the internal auditors have violated the regulations in the preceding two paragraphs. If the auditor has violated the rules, the company should order the auditor to make improvement within one(1) month and should be transferred to other job if he or she fails to make such improvement.

Article 14

The internal audit unit shall undertake the following tasks:

A. Plan the organization structure, size and duty of the internal audit unit. Prepare internal audit working manuals and working papers, which shall at least include assessing the various rules and operating procedures of the internal control system to determine whether adequate internal controls are already in place in the current rules and procedures, whether each department has realistically carried out the internal controls, and whether the internal controls are carried out in a reasonably effective manner, and from time to time provide recommendations for improvement.

B. Monitor the formulation of rules and procedures for self-inspection and assessments of the internal control system by business and management units, and the implementation of periodic self-inspection by each unit.

C. Formulate annual audit plans and, based on the business risk profile of and implementation of internal audits by each subsidiary or department, determine audit plans targeted at each individual subsidiary or department.

For the purpose of self-inspecting its internal control system, a financial holding company (including its subsidiary companies) or a banking business shall see to it that all of its internal departments and subsidiaries carry out self-inspection, and have its internal

audit unit review the self-inspection reports of each department and subsidiary (including its subsidiary companies if it is a financial holding company); such self-inspection, together with the reports on the correction of any deficiencies and irregularities discovered in the internal control system by the internal audit unit, shall serve as a basis for the board of directors, president, chief auditor, and chief compliance officer to evaluate the overall efficacy of the internal control system and to issue internal control system statements.

Article 15 A banking business shall conduct a routine audit at least annually, and a special audit on its and all its subsidiaries' operation, finance, asset quality and information departments; a special audit at least annually on other management departments; a routine audit at least annually on its all business centers, foreign business units and foreign subsidiary companies. The auditing method for a foreign office can be replaced with a report auditing or adjust the auditing frequency flexibly.

The contents of the routine audit or the special audit, which is performed by the audit unit of a banking business to its business unit, should cover whether there are improper marketing activities when dealing with trust business, financial management, and the sale of financial products; whether the contents of the products are clearly disclosed; whether the risks are well notified; whether the contract is fair and other obligations are performed appropriately following the law or self-regulatory guidelines.

The internal auditing unit of a financial holding company shall conduct a routine audit at least annually; a special audit on its finance, risk management, and compliance with applicable acts and regulations at least semiannually; where the routine business has covered the scope of the special audit and its audit results reveal no significant deficiency, and it expressly states such in the internal audit report, it is not required to conduct a special audit for that current half-year.

The internal audit unit should include the execution status of the regulatory compliance system into the routine audit or special audit of the business and management units.

Article 15-1 A domestic bank may apply to the competent authority for approval to adopt a risk-based internal auditing system. The

competent authority may ask a domestic bank to apply for approval to adopt a risk-based internal auditing system in view of the bank's asset size, business risks and other necessary conditions.

A domestic bank that applies for approval to adopt a risk-based internal auditing system must meet the following criteria:

- 1.The bank's most recently filed ratio of regulatory capital to risk-weighted assets meets the requirements set out in Article 5 of the Regulations Governing the Capital Adequacy and Capital Category of Banks;
- 2.The bank does not show insufficient loan loss provision and reserves based on the most recent financial examination and the most recent CPA-audited and certified financial statements;
- 3.The bank's non-performing loan ratio of the most recent quarter does not exceed 1%; and
- 4.The bank has an effective internal control system.

The provisions on auditing frequency in Paragraph 1 of the preceding article do not apply to domestic banks that have been approved to adopt a risk-based internal auditing system.

Article 16 A financial holding company or a banking business shall formulate annual audit plans and, based on the business risk profile of and implementation of internal audits by each subsidiary, determine audit plans targeted at each individual subsidiary.

The internal audit unit of a financial holding company or a banking business, except those foreign branches of a banking business and other business ratified by the competent authority, conduct a target audit on its subsidiaries' finance, risk management, and compliance with applicable acts and regulations at least semiannually and incorporate the audit results into its annual audit project.

All subsidiaries shall submit to the financial holding company or the banking business their board meeting minutes, CPA audit reports, examination reports issued by the financial examination agency, and other relevant materials, and, for subsidiaries having established an internal audit unit, audit plans and reports on significant deficiencies identified in internal audit reports and the status of improvements thereof; the mother company shall review such documents and monitor the implementation of improvements

by each subsidiary.

The chief auditor of a financial holding company or a banking business shall periodically evaluate the efficacy of the internal control activities of a subsidiary as set forth in the preceding paragraph and, after having reported to the board of directors, send the evaluation results to the relevant subsidiary's board of directors for their reference in personnel evaluations.

Article 17 A financial holding company or the banking business shall disclose at least the following information in its internal audit report for routine business audits.

A. Audit scope; summary commentary; financial status; capital adequacy; operation performance; asset quality; management of shares; management of the operation of board of directors and audit committee; compliance with major acts, regulations, and rules; internal controls; interested party transactions; the control and internal management of all business tasks; protection and management of customers' data; information management; management of customer data confidentiality; protection measures of consumers and investors and the results of self-inspection, and the evaluation to above matters.

B. Opinions for the major illegal errors or faults in all departments, and the suggestions for punishment for employees fail to fulfill their duties.

C. The examination comments or faults listed by the financial examination agency, accountants, internal audit unit (including the internal audit unit of the mother company), and self-inspection people, and the improvement status of items that enlisted as 'need further improvement' by the internal control statement.

The record of the results in working papers shall be preserved together with the self-inspection or internal audit reports and relevant materials for no less than five(5) years.

Article 18 Where a financial holding company or a banking business makes any concealment of poor internal management, unsatisfactory internal controls, inadequate implementation of the internal audit system and regulatory compliance system, or the results of implementation of improvement of any deficiency specified by a financial examination agency in an examination opinion requiring

review and follow-up, or the internal audit unit (including the internal audit unit of parent company) otherwise conceals any audit findings, and where such concealment constitutes significant malpractice, the personnel involved shall be held responsible for negligence in their duties. A financial holding company (including its subsidiaries) or a banking business shall commend an internal auditor who identifies any significant malpractice or negligence and thereby averts material loss to the company.

When a significant deficiency or malpractice arises within the management or business departments of a financial holding company or a banking business, the internal audit unit shall have the power to suggest penalties and shall make a full disclosure of the responsible negligent personnel in an internal audit report.

Article 19 The internal audit report of a financial holding company or banking business shall be delivered to the supervisors (board of supervisors) or audit committee for review and unless it is otherwise provided by the competent authority, shall be submitted to the competent authority within two (2) months following completion of the audit. The audit report shall also be delivered to the independent directors if such positions are set up by the financial holding company or the banking business.

Article 20 Before assuming the following post, the person should enroll in the following trainings held by the institutes recognized by the competent authority and obtain completion certificate from them:

A. When acting as an internal auditor for the first time, the auditor should participate in the audit training course, computer audit training course or billing audit training course for no less than sixty (60) hours. The auditor should also pass the exam and obtain the completion certificate.

B. An internal auditor with leadership duty should participate in the internal auditor leader train course for no less than nineteen (19) hours.

C. The chief auditor and official, deputy managers should participate in audit manager training course for no less than twelve (12) hours. Internal auditors (including the official, deputy managers and chief auditor) of a financial holding company (including its subsidiary companies) or a banking business

(including the parent company) each year shall attend a finance-related professional training held by a competent authority-designated institution or by the financial holding company or a subsidiary thereof. For the minimum number of training hours, the total hour should be no less than twenty(20) for the official, deputy managers and chief auditors; no less than thirty(30) for the other internal auditors. If an auditor has obtained an international internal auditor certificate within the current year, the certificate can be transferred to the training hours. The total hour of a finance-related professional training held by a competent authority-designated institution shall not be less than half of the training hours in the preceding paragraph.

For an auditor stationed overseas, the training hours can be recognized by enrolling with a financial training institute established by the local regulations and acts.

The financial holding company or the banking business should organize self-inspection programs for every year and continue proper training courses for auditors in accordance with the nature of each department.

A financial holding company or a banking business shall verify that its internal auditors meet the qualification requirements set forth herein. The verification documentation and records for such purpose shall be kept on file for future reference.

Article 21 A financial holding company or banking business shall, in a prescribed format and via an Internet-based information system, file with the competent authority for recordation the information on the name and years of service of its internal auditors by the end of January each year.

When preparing the basic information of internal auditors, the financial holding company or the banking business should verify whether these auditors have met the requirements stipulated in Paragraph 2, Article 12 and Article 20. If the auditor fails to meet the requirements, it should be improved within two(2) months, if not, the auditor should be re-assigned to another job.

Article 22 A financial holding company shall, in a prescribed format and via an Internet-based information system, file with the competent authority for recordation its next year's audit plan by the end of



each fiscal year and a report on the execution of its preceding year's annual audit plan within two(2) months from the end of each fiscal year.

By the end of each accounting year, the financial holding company or the banking business shall deliver a written audit plan for the next year to the supervisors (supervisors, board of supervisors) or the audit committee for examination and compilation. If the company doesn't have an audit committee, the report shall be delivered to the independent directors for comments. The annual audit plan and changes thereof shall be approved by the board of directors.

The contents of audit plan mentioned in the preceding paragraph shall at least include: an explanation of the audit plan, annual audit points, units that will receive the audit, nature of audit (routine audit or special audit), and whether the frequency of audit comply with the regulation of the competent authority. If the audit is a special audit, then it is necessary to notify the range of audit.

Article 23 A financial holding company or banking business shall, in a prescribed format and via an Internet-based information system, file with the competent authority for recordation its improvements of deficiencies and irregularities identified in the internal control system in previous year within five (5) months from the end of each fiscal year.

Article 24 For a banking business, officers at various levels with the authority to approve business and transactions shall meet any of the requirements below prior to taking office:

A. Have served as auditors in the internal audit unit and worked for over one(1) year with actual auditing affairs.

B. Have enrolled in the audit training course or computer audit training course held by a competent authority-designated institution and passed the exam and obtained the completion certificate.

C. Obtaining the qualification certificates in banking business internal control and internal audit exam held by a competent authority-designated institution.

The contents of the exam should be similar to the contents mentioned in the preceding paragraph.

For the heads of individual levels at foreign business units that have authorization in business or transactions, they are allowed to enroll in professional audit training held by a foreign professional institute or obtain a similar certificate from a foreign institute to replace the certificate mentioned in Paragraph 1.

When acting as the manager of a local business unit, the manager should meet the conditions listed in Paragraph 1, besides, if the manager qualifies the conditions in Subparagraph 2 or 3 of Paragraph 1, the manager should participate in more than four(4) times of audit practices with the internal audit unit before actually assuming the post or within six(6) months after assuming the post. Each practice should be responsible for as least one(1) item, practicing at least four(4) items, write a report on the practice, and send to the chief auditor for verification. The chief auditor should present a certificate and keep the report for further reference.

For the heads of individual levels in the banks of a foreign bank in Taiwan, if they are responsible for tasks involving the authorization in business or transactions, and they have finished the internal audit trainings requirement by the bank, when the training is higher than the requirements listed in Paragraph 1, then they can be exempt for the regulations in this article.

## **Section 2 The Examination of self-inspection and Statement for Internal Control System**

Article 25 The banking business should establish a self-inspection system. The bank shall conduct a self-inspection on all business, financial, asset safekeeping, information, and foreign business units at least semiannually; a special self-inspection at least every month. However, if the company has conducted a routine self-inspection, an internal audit unit (including the internal audit unit of the mother company) has conducted a routine business audit, a financial examination agency has conducted a routine business audit or self-evaluation on affairs concerning compliance with applicable acts and regulations in that month, a special self-inspection can be exempted in that month.

All departments and the subsidiaries of a financial holding company should conduct a self-inspection on internal control system at least annually; a legal compliance self-inspection at least semiannually.

For the self-inspection affairs mentioned in the preceding two paragraphs, the head of the unit should assign a person of another duty to conduct the audit and be kept secret.

The results of self-inspections mentioned in paragraph 1 and 2 shall be made as working papers and shall be preserved together with the self-inspection or internal audit reports and relevant materials for no less than five(5) years.

Article 26 The internal audit unit (including the internal audit unit of the mother company) shall continually conduct follow-up reviews on any examination opinions or audit deficiencies brought up by the financial examination authority, CPA, or internal audit unit, and on matters specified in the internal control system statement as requiring stronger improvement efforts, and submit a written report on the implementation of improvement of deficiencies to the board of directors, together with a copy to the supervisors (supervisors, the board of supervisors), and list these as an important factor in the relevant department's performance evaluations.

The major points of audit task for a financial holding company or a banking business should be prescribed by the competent authority.

Article 27 A financial holding company or a banking business shall supervise all departments (for the financial holding company, including its subsidiaries) to carefully assess and review the status of the operation of its internal control system, and, separately for self-inspection results and internal audit reports, submit internal control system statements jointly signed and issued by the chairperson, general manager, chief auditor, and compliance officer (as attachment 1) to the board of directors for approval, and subsequently within three (3) months from the end of each fiscal year disclose the information contained therein on the company's website and publish the same on a website designated by the competent authority.

The internal control system statement under the preceding paragraph shall be duly published in the annual report, stock issue prospectuses, and other prospectuses.

The regulations in Paragraph 1 are not applicable to the banking business taken over by the competent authority.

### **Section 3 The Audit of a Banking Business by an Accountant**

- Article 28 If the annual financial report of a banking business is audited and certified by CPA the business should also delegate the CPA to conduct an audit on its internal control system. The CPA should also comment on the correctness of the report submitted to the competent authority for the banking business, the execution status of internal control system and regulatory compliance system, and the appropriateness of policies for loan loss reserves, including those of the foreign business units of the banking business.
- The competent authority may request a banking business to provide the examination report of its personal data protection and AML/CFT mechanism issued by CPA.
- The audit fees for the CPA should be negotiated by the banking business and the CPA. The business should pay the CPA as negotiated.
- The provisions of Paragraph 1 and Paragraph 2 are not applicable to banking business taken over by the competent authority.
- Article 29 When necessary, the competent authority is allowed to invite the banking business and its delegated accountant to conduct further discussion concerning the affairs of such audit. If the competent authority finds the delegated accountant is not competent for the audit affairs delegated by the business, the authority should demand the banking business to alter the delegation to another accountant for another audit.
- Article 30 When an accountant conducts audit affairs following the regulations of Article 28, the accountant should inform the competent authority immediately when the following conditions are found:
- A. During the process of audit, the business fails to provide the required reports, certificates, books of accounts, and meeting minutes for the accountant, or refuses to make further explanation on the queries submitted by the accountant, or there are other objective environment restrictions to cause the accountant unable to continue his or her audit work.
- B. When there are severe false, forged data, or missing in its

accounting or other records.

C. Its assets are insufficient to pay its debts or its financial condition is worsened.

D. There is evidence indicating that its transactions will cause great damage to the bank's net asset.

If an audited banking business has conditions listed in Paragraph 2 to 4, the accountant should submit in advance a summary report to the competent authority based on the auditing results.

Article 31 When a banking business delegates a CPA to conduct audit as provided in Paragraph 1 of Article 28, the business should provide the CPA audit report of the previous year to the competent authority by the end of April each year for recordation. The audit report should at least entail the scope, basis, procedure, and results of the audit.

When a credit cooperative conducts such audit in accordance with the preceding paragraph, the audit report shall be submitted via the finance department of municipal government or the county (city) government.

When the competent authority has queries concerning the contents of the audit report, the CPA should provide relevant information and explanation based on facts.

#### **Section 4 legal compliance System**

Article 32 The head office of a financial holding company or a banking business shall set up a compliance unit under the president to take charge of the planning, management, and execution of the regulatory compliance system. Another high level manager shall also be assigned to act as chief compliance officer for the head office to conduct compliance affairs. The chief compliance officer shall make a report to the board of directors (council), supervisors (board of supervisors) or the audit committee at least semiannually, and in case of major regulatory violation or rating downgrade by the financial competent authority, immediately inform the directors (council members) and supervisors (board of supervisors), and report to the board of directors (or the council) on compliance matters.

The requirements for setting up the foregoing compliance unit and

the chief compliance officer for the head office are as follows:

1. A banking business, if the total assets of the previous year as audited by a CPA have exceeded NTD 1 trillion, shall set up a dedicated compliance office that may be in charge of AML/CFT, but shall not be in charge of legal affairs unrelated to the planning, management, and implementation of the legal compliance system, or any affairs with conflict of interest. The chief compliance officer of its head office may be appointed as the AML/CFT compliance officer but shall not serve as the chief officer of legal affairs or other internal posts.

2. The chief compliance officer at a financial holding company or the head office of a banking business that is not governed by the foregoing paragraph cannot be appointed to internal posts other than chief legal officer or chief AML/CFT compliance officer, except as otherwise provided by the competent authority with respect to the credit cooperatives and bills finance companies.

The chief compliance officer at a financial holding company or the head office of a banking institution shall hold a post comparable to that of vice president and meet the qualification requirements set out respectively in the Regulations Governing Qualification Requirements for the Promoter or Responsible Persons of Financial Holding Companies and Concurrent Serving Restrictions and Matters for Compliance by the Responsible Persons of a Financial Holding Company and in the Regulations Governing Qualification Requirements and Concurrent Serving Restrictions and Matters for Compliance by the Responsible Persons of Banks.

The compliance unit of the head office, domestic and foreign business units, information unit, assets safekeeping unit, and other management units of a financial holding company or a banking business shall each assign the personnel to act as the compliance officer to take charge of related affairs. Arranging the compliance officer position in the foreign business unit shall comply with the local regulations and the requirements of the local authorities and the compliance officer should not hold other posts except in any of the following situations:

1. The compliance officer serves concurrently as the AML/CFT compliance officer.

2. The compliance officer holds concurrent posts that do not

constitute a conflict of interest according to the local regulations.

3.It is not strictly prohibited in the local regulations regarding the holding of concurrent posts, provided the holding of concurrent posts does not result or potentially result in conflict of interest and the matter has been communicated with and confirmed by the local competent authority and reported to the competent authority for recordation.

The chief officer and personnel of the compliance unit of a financial holding company or the head office of a banking business, as well as the compliance officer of its domestic and foreign business units, information department, assets management department, and other management departments shall meet one of the following qualification requirements:

1.Having worked as personnel or chief officer of legal compliance office at any financial institute for five years in aggregate.

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 business unit who is hired locally, has shown his/her familiarity with local regulations and competence in related matters according to the self-assessment of the assessment procedures resolved by the board of directors, or the review and acknowledgement by the local competent authority.

The chief compliance officer and personnel of the compliance unit of a financial holding company or the head office of a banking institution as well as the compliance officer of its domestic and foreign business units, information department, assets safekeeping department, and other management departments shall attend at least fifteen (15) hours of training a year offered by institutions recognized by the competent authority or held internally by the financial holding company (including its subsidiaries) or the banking business (including its parent company), and the training courses shall cover at least the latest regulatory amendments, new businesses or new financial products launched.

The compliance officer of a foreign business unit shall attend at least fifteen (15) hours of on-the-job training courses a year offered by the local competent authority or relevant institutions, or the

training courses offered by the competent authority, the institutions recognized by the competent authority, or held by the employing financial holding company (including its subsidiaries) or the banking business (including the parent company).

The training methods for the on-the-job training as set forth in the foregoing two paragraphs held by the company itself shall be approved by the board of directors. The head office shall keep the attendance records of relevant personnel for review.

When a dedicated AML/CFT compliance unit is set up under the legal compliance unit, the required training for AML/CFT compliance unit personnel before their appointment/assignment and every year shall observe the relevant AML/CFT regulations and is not subject to the provisions of Paragraph 5 and Paragraph 6 hereof.

Financial holding companies and banking businesses shall file the list of head office chief compliance officers, the chief officers and personnel of the compliance unit as well as their training records with the competent authority via an online information system.

- Article 33 The head office and branches of a financial holding company or banking business should establish advisory and communication channels for regulatory compliance matters to keep employees informed of rules and regulations, swiftly clarify any questions of the employees on rules and regulations, and ensure regulatory compliance.
- When the legal compliance unit of a financial holding company or banking business makes a report to the board of directors in accordance with Paragraph 1 of the preceding paragraph, the report should contain at least an analysis of the causes of significant deficiency or malpractice in compliance matters within respective departments as well as recommendations for improvement.

- Article 34 A compliance unit should conduct the following tasks:
1. Establishing a system for clear and adequate conveyance, consultation, coordination and communication of rules and regulations.
  2. Keeping operating and management rules and procedures updated in line with relevant regulations to make sure all business



activities comply with regulatory requirements.

3. Before a banking business introduces a new product or service, or applies to the competent authority for approval to offer a new business, the chief compliance officer shall issue and sign an opinion statement undertaking that the new product, service or business complies with applicable regulations and internal rules.

4. Drafting rules and procedures for evaluating regulatory compliance and overseeing the periodic implementation of self-evaluation by respective units; assessing the compliance self-evaluation operations of respective units and producing a report thereon, which, after being signed off by the president, will be used as reference in the performance evaluation of the unit.

5. Providing pertinent regulatory training to employees.

6. Supervising the introduction, establishment and implementation of relevant internal rules by the compliance officer of respective department.

The internal audit unit may draft the rules and procedures for evaluation of compliance by its subordinate units and perform self-evaluation of compliance by its subordinate units, to which the provisions in Subparagraph D of the preceding paragraph do not apply.

If a banking business has a foreign business unit, the legal compliance unit should supervise the following tasks of the foreign business unit:

1. Collecting data on local financial regulations, conducting self-evaluation of compliance operation, and ensuring the suitability of compliance officer and the adequacy of compliance resources (including personnel, equipment and training) so as to ensure compliance with the laws and regulations of the host country or jurisdiction.

2. Establishing self-evaluation and monitoring mechanism for compliance risks, and for large business operation, highly complex business or business involving higher risk, engaging a local, outside, independent expert to verify the effectiveness of the self-evaluation and monitoring mechanism.

A financial holding company or banking business should perform self-evaluation of compliance at least semiannually. The results should be sent to the compliance unit for further reference. The

head of a unit should designate a specific person to conduct the self-evaluation affair in each unit.

The self-evaluation draft and information for the preceding affairs should be kept at least five (5) years. Article 35

Article 34-1 A banking business governed by subparagraph 1, paragraph 2 of Article 32 shall establish a bank-wide risk-based management and supervision framework for legal compliance. The basis of such framework, functions and responsibilities are specified as follows:

1. The compliance unit shall set up the procedures, plans and mechanisms for identifying, assessing, controlling, measuring, monitoring, and independently reporting any compliance risk in order to generally control, supervise, and support each domestic or foreign department, branch, and subsidiary with respect to individual business unit, cross-department, and cross-territorial legal compliance.

2. The compliance unit shall set up an adequate number of professional units based on the classification or business, or points of legal compliance to monitor, implement and support the legal compliance the local or foreign business units related to that business or legislation.

3. The compliance unit may assess the appointment, and enhances the independence of each chief compliance officer by risk-based approach. Notwithstanding to the requirements in the first part of paragraph 4 of Article 32, an independent chief compliance officer is not required, and the legal compliance office of the head office will be responsible for a unit with lower compliance risk.

4. The compliance unit shall establish the mechanism of independent reporting, assessment and disposition of compliance risk alert.

5. The compliance unit shall assess the risk management of legal compliant for the primary operating activities, products and services, credit or business projects, and critical customer complaints subject to potential legal violation 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 bank.

7. The compliance unit shall consider the evaluation of the management board, and each chief officer of department to form the opinion of their implementation of legal compliance.

8. The banking business and its compliance unit shall fully understand the compliance procedures 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 the compliance risk management, and supervise the improvement plans and schedules with respect to the local and foreign operations across the bank when reporting the legal compliance to the board of directors (or the council), and the supervisors or audit committee at least once every half year pursuant to paragraph 1 of Article 32; the board of directors (or the council) shall provide sufficient resources and appropriate mechanism of rewards and sanctions applicable to the business units in order to progressively establish a bank-wide culture of legal compliance.

10. The internal audit unit shall include the performance of the compliance office, and the assessment opinion of the compliance status across the bank when reporting the audit tasks to the board of directors (or the council), and the supervisors or audit committee at least once every half year pursuant to paragraph 1 of Article 10.

A banking business governed by the foregoing paragraph shall set up the dedicated compliance office and appoint the chief compliance officer at the head office pursuant to subparagraph 1, paragraph 2 of Article 32 within six months upon satisfaction of the applicable conditions, and report the adjusted risk-based management and supervision framework for legal compliance across the bank to the competent authority, and file the assessment reports under subparagraphs 5 and 9 in the foregoing paragraph with the competent authority by the end of every April.

Article 34-2      In order to promote a robust operation, financial holding companies and banking businesses shall set up the whistleblower

system, and designate a unit with independent functions at the head office to accept and investigate the reported issues.

A financial holding company or a banking business shall protect the whistleblower as below:

1. The whistleblower's identity shall be kept confidential; no information that may be used to identify that person shall be disclosed.
2. The 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 interested person shall recuse himself from the acceptance and investigation of the reported case.

The whistleblower system, in paragraph 1, shall at least cover the following procedures, and be resolved by the board of directors (or the council):

1. Expressly specifies that anyone may file the report when discovering any crime, corruption, or potential legal violation.
2. The types of reporting that will be accepted.
3. Establishes and publishes the channel of reporting.
4. The procedures of investigation and collaborative support, 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 document preparation.
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 (or council member), supervisor (or member of the board of supervisor), or a managerial officer of an equivalent level higher than vice president, the investigation report shall be reviewed by the supervisors (or members of the supervisory board, or the supervisory board), or the audit committee.

The financial holding company or the banking business shall report or file the critical incident, or material violation discovered in the

investigation with relevant authorities.

A financial holding company or banking business shall hold regular promotional program and education training of the whistleblower system for its personnel.

## **Section 5 Risk Management Mechanism**

- Article 35 A financial holding company or a banking business shall formulate adequate risk management policies and procedures and establish operationally independent and effective risk management mechanisms, by which to assess and monitor the respective risk-bearing capacity, and current status of risks already incurred, and to determine their compliance with the risk response strategies and risk management procedures.
- The risk management policies and procedures under the preceding paragraph shall be passed by the board of directors and be reviewed and revised in a timely manner.
- Article 36 A financial holding company or a banking business shall establish an independent risk management task force and regularly furnish risk management reports to the board of directors; upon identifying a significant risk exposure that might adversely affect its financial or business status or compliance with applicable acts and regulations, it shall take immediate and adequate countermeasures and submit a report to the board of directors.
- For a credit cooperative, the establishment of the independent risk management task force mentioned in the preceding paragraph can be replaced by a designated management unit in its headquarters.
- Article 37 The risk management mechanisms of a financial holding company shall include the following matters:
- A. Monitoring the capital adequacy of the financial holding company and of all subsidiaries based on their respective business scale, credit, market, and operational risks, and future business trends.
  - B. Adopting adequate long- and short-term financing principles and guidelines, and establishing management mechanisms for measuring and monitoring the liquidity positions of the financial holding company and of all subsidiaries, by which to measure, monitor, and manage the liquidity risks of the financial holding

company and of all subsidiaries.

C. Making various investment allocations after having considered the overall risk exposure, equity capital, and characteristics of liabilities of the financial holding company, and establishing various measures to manage investment risks.

D. Establishing uniform assessment methodologies for rating and classifying the quality of assets of the financial holding company and of all subsidiaries, calculating and controlling large risk exposures of the financial holding company and its subsidiaries, carrying out periodic reviews, and faithfully setting aside allowances or reserves for loss.

E. Building information security mechanisms and contingency plans with respect to business exchanges, transactions, or other activities between the financial holding company and its subsidiaries and between its subsidiaries.

Article 38 The risk management mechanism of a banking business shall include the following principles:

A. Monitoring the capital adequacy based on its business scale, credit, market, and operational risks, and future business trends.

B. Establishing management mechanisms for measuring and monitoring the liquidity positions of the banking business, by which to measure, monitor, and manage the liquidity risks.

C. Making various investment allocations after having considered the overall risk exposure, equity capital, and characteristics of liabilities, and establishing various measures to manage investment risks.

D. Establishing uniform assessment methodologies for rating and classifying the quality of assets, calculating and controlling large risk exposures, carrying out periodic reviews, and faithfully setting aside allowances or reserves for loss.

E. Building information security mechanisms and contingency plans with respect to business, transactions, and information exchanges or other activities.

Article 38-1 Banking businesses shall set up the dedicated information security office, and appoint the chief officer, who shall not be appointed to other posts of information, or tasks with conflict of interest, and shall arrange suitable workforce and equipment except as

otherwise provided by the competent authority with respect to the credit cooperatives and bills finance companies.

A banking business shall set up a dedicated information security office and appoint a person a level higher than associate general manager or equivalent function to be the chief officer of such dedicated information security office if its total assets of the previous year as audited by a CPA have exceeded NTD 1 trillion.

The dedicated information security office is in charge of planning, monitoring and implementing the management processes of information security. The chief officer of the dedicated information security office shall issue the Declaration of Overall Information Security Implementation (as attachment 2), specifying the implementation of information security in the previous year, with the names of the chairmen of the board (or the chairperson of the council), the president, the auditor general shown therein, and report to the board of directors (or the council) within three months after the end of each fiscal year.

The personnel of the dedicated information security office of the banking business shall attend at least fifteen (15) hours of professional courses of information security, or on-the-job training every year. The personnel of the head office, local and foreign business units, information units, financial custody unit, and other managerial units shall attend no less three hours of promotional program of information security every year.

The Bankers Association, the National Federation of Credit Cooperatives, and the Bills Finance Association shall establish and regularly review the self-disciplinary regulations of information security.

Banking businesses governed by paragraph 2 shall implement the adjustments within six months upon satisfaction of the applicable conditions.

#### **Chapter 4 Supplementary Principles**

Article 39 To secure the confidentiality level of the financial examination report of a financial holding company or a banking business, unless consented by the law or the competent authority, the responsible person or the employee are not allowed to read or disclose, deliver, publicize all or part of the contents of the report to another person

irrelevant of the performing of the task.

The financial holding company or the banking business should follow the provisions of the competent authority to prescribe the relating internal management regulations and business procedures of the financial examination reports and submit them to the board of directors for consent.

- Article 40 A financial holding company or a banking business shall set out in its internal control system penalties for violations of these Regulations or its internal control system rules by managers and relevant personnel.
- Article 41 The subsidiary company of a financial holding company referred to in these regulations should be defined as in Article 4 of the Financial Holding Company Act; the subsidiary company of a banking business should follow the provisions of Paragraph 3 of Article 5 of Regulations Governing Establishment of Internal Control Systems by Public Companies.
- Article 42 The internal auditors and compliance officer of a financial holding company or a banking business shall immediately prepare a report for submission, with a notice to the independent directors and supervisors (supervisors, board of supervisors) or the auditing commission and report to the competent authority, when their recommendations for improvements regarding significant deficiencies or noncompliance identified in internal controls are not accepted by management and as a result the financial holding company or the banking business might incur a material loss.
- Article 42- 1 After the end of examination conducted by the competent authority or the local competent authority at where a foreign branch is located or after receiving an examination report, the internal audit unit at a financial holding company or the head office of a banking business should, based on the principle of materiality, promptly inform the directors (council members) and supervisors (board of supervisors), and make a report to the forthcoming board of directors' (or the council) meeting. The report items should include the content of examination communication meeting, major deficiencies found in the examination, the rating downgrade by



the financial competent authority, improvement actions required by the competent authority or possible disciplinary measures to be taken.

Article 43 The competent authority will set forth formats specified in the Rules herein.

Article 44 When a credit cooperative submit relating materials to the competent authority as regulated in these regulations, the cooperative should also report to the finance department of municipality or the finance bureau of county (city) government.

Article 45 The branch of a foreign bank in Taiwan shall carry out internal control and audit in compliance with the Rules herein. However, if the internal control and audit systems of a branch in Taiwan are prescribed based on regulations with higher or equivalent standards for internal control and audit establishment, then the branch is allowed to report its situation to the competent authority for future reference and conduct such systems after a comparison report on the details of the standards that bank adopts and our system, which should also be signed by the responsible person of the branch.

If the headquarters of the branch bank in Taiwan has altered its internal control and auditing systems, which might also apply to the branch in Taiwan, the revisions should be immediately explained and compared to domestic regulations and send to the competent authority for future reference after signed by the responsible person in Taiwan.

If the branch of a foreign bank in Taiwan violates the internal control and audit system accepted by the competent authority in accordance with three preceding paragraphs hereof, it shall be deemed as violating the Rules herein.

Article 46 Financial holding companies and banking businesses that do not meet the provisions in the latter section of Paragraph 4 of Article 32 herein concerning full-time and concurrent posts shall make adjustment to become compliant within six (6) months after the promulgation of the amended Regulations on March 22, 2017. Compliance personnel or officers who took up the post prior to the

promulgation of the amended Regulation on March 22, 2017 but do not meet the provisions in Paragraph 5 of Article 32 herein shall make adjustment to obey the rules within one year.

Article 47 The Rules herein shall be in force on the date of promulgation. The 2nd March 2012 amendments, except Article 8, paragraph 1, subparagraph 2 item 5, the credit cooperatives shall enter into force from 1st January 2014, and Article 8, paragraph 1 subparagraph 2 item 8 shall enter into force from 30 December 2012, shall enter into force three months after the date of issuance. The amended and reinstated provisions of Article 34-2 on March 31, 2018 shall take effect six months after promulgation.