Unofficial Translation

With collaboration between the Bank of Thailand and the Association of International Banks

This translation is for convenience of those unfamiliar with Thai language.

Please refer to the Thai text for the official version.

Bank of Thailand Notification

No. FPG. 19/2560

Re: Regulations on Information Technology Risk of Financial Institutions

---

1. Rationale

Currently, information technology (IT) plays an important role in the business operations of financial institutions, as the financial institutions have used IT as infrastructure to enhance the efficiency of their business operations, reduce operating costs and raise their competitiveness. In addition, financial institutions also use IT to develop financial products and expand the service to cover a wider range of customers, while the service can serve a variety of customers that tends to look for more convenient and responsive services, especially financial services offering through electronic channel and financial technology (FinTech) businesses. Even though IT helps increase the efficiency of the business operations and the financial institutions can provide more responsive services, if there is a lack of proper risk management, the use of IT may lead to IT risks make the financial institutions vulnerable to cyber threats, which may result in financial losses, loss of reputation, or, even, a widespread impact on the payment system and financial system of the country, while the customer trust in financial service is deteriorated.

Therefore, the Bank of Thailand prescribes the supervisory regulations to ensure that financial institutions have sound IT governance, appropriate IT security controls, and IT risk management. The regulations highlight the composition and roles and responsibilities of the board of directors of financial institutions, organizational structure, and staff management. The board of directors and senior managements are expected to have sufficient knowledge and understanding as they must set the directions on IT usage that are appropriate to the business strategies of their financial institution. They are also expected to be aware of risks that rapidly arise from the extensive use of IT, put importance on IT risk management, by integrating it into the enterprise risk management (ERM), and must set out and communicate the relevant policies to all involving staff so that they have been aware of and understood IT risks as well as implement the policies by appropriate approaches, as well as ensure that there are the staff planning and

management, especially the staff responsible for IT functions must have qualifications and knowledge that are appropriate to their assignments, while the number of staff is sufficient to deal with current and future business operations of the financial institution.

Furthermore, the Bank of Thailand also emphasizes that financial institutions must have IT security controls, IT risk management, the supervision of compliance with IT laws and regulations, IT audit, and IT project management that are effective and robust according to the IT risk supervision framework, namely (1) confidentiality; (2) integrity; and (3) availability. Moreover, financial institutions must take care of customer data protection and customer interests. The IT risk management must be commensurate with the nature of business, volume of transactions, IT complexity, and relevant risks, such as operational risk, strategic risk, reputational risk and legal risk.

On this, if any particular financial institution encounters significant IT problems or IT incidents that affect its services, system or reputation, as well as the events where significant IT functions have been attacked or threatened by cyber attacks, and where those problems or incidents are the issues that the financial institution must report to its top executive, the financial institution must report those problems or incidents to the Bank of Thailand immediately or as soon as they are discovered. For usage of any technology for the first time or making any changes to the technology usage, which has a significant impact or risk on business operations, financial institutions must receive approval from the Bank of Thailand before proceeding.

2. Statutory Power

By virtue of Section 41 of the Financial Institution Business Act B.E.2551, the Bank of Thailand hereby issues regulations on Information Technology Risk of Financial Institutions, as specified herein

3. Notification to Be Repealed

The Bank of Thailand Notification No. FPG. 26/2551 Re: Permission for Commercial Banks to Operate E-banking Services dated 3 August 2008 (B.E.2551)

4. Scope of Application

This Notification shall apply to all financial institutions according to the Financial Institution Business Act.

5. Contents

5.1 The provisions under "Clause 5.2 Security controls" and "Clause 5.3 Internal control" of the Bank of Thailand Notification No. FPG. 27/2551 Re: Permission for Finance Companies and Credit Foncier Companies to engage in Electronic Banking (E-Banking) dated 3 August 2008 (B.E.2551) shall be repealed, and finance companies and credit foncier companies shall, accordingly, comply with the regulations as specified in this Notification.

5.2 Definitions

"Information technology risk (IT risk)" means risk that may arise from the used of information technology in business operations, as the risk may lead to an effect on systems or operations of the financial institution, including risk from cyber threats.

"Information technology (IT)" means information technology that has been used in business operations, which includes data, operating system, application system, database system, hardware, and communication system.

"Board of directors" means the board of directors of a locally registered financial institution or the authorized managements of a foreign bank branch.

5.3 Regulations on IT risk supervision

5.3.1 IT governance

(1) Roles and responsibilities of the board of directors

The composition of the board of directors must be in accordance with the Bank of Thailand Notification Re: Corporate Governance of Financial Institutions, where, at least, one member of the board must have IT knowledge or experiences so that the board of directors can set the directions and oversee that its financial institution has used IT appropriate to business strategies, as well as have awareness of changing risks and IT evolution so that the board of directors can effectively oversee IT risk management of its financial institution.

Furthermore, the board of directors must receive sufficient training in IT and relevant risks within an appropriate timeframe so that the board will have knowledge and understanding of IT and its relevant risks, which will benefit the oversight of IT risks of the financial institution. The roles and responsibilities of the board of directors on the oversight of IT risk management shall include, but not limited to, the following:

(1.1) Oversee that the financial institution uses IT that is appropriate to its business strategies and the IT usage is flexible as it can respond to any changes in IT and business operations of the financial institution in the future

(1.2) Oversee that there is IT risk management (as it is one of the key risks) as part of the enterprise risk management (ERM) of the financial institution

(1.3) Oversee that the following policies are formulated:
(1) IT security policy – including IT business continuity plan (IT BCP) policy; and
(2) IT risk management policy – the policy must be commensurate with the nature of business, volume of transactions, complexity of IT, and relevant risks; where the board of directors must approve those policies

(1.4) Oversee that (1) IT security policy and (2) IT risk management policy that have been approved by the board of directors are used in setting out an operating procedure and process on IT security controls and IT risk management; and oversee that those policies are properly implemented, while the effectiveness of those policies must be reviewed at least once a year and when there is any significant change

(1.5) Oversee that there are the appropriate monitoring, auditing and reporting of the following matters to the board of directors, designated committee or senior managements of the financial institution: IT security controls, results of IT BCP testing and implementation, and IT risk management such as the results of the overall IT risk management, IT problems or incidents that led to a widespread impact or affected the reputation of the financial institution

(1.6) Oversee and promote the communication with staffs of financial institutions so that they are aware of IT risks and understand the appropriate use of IT in order to reduce IT risks

(2) Oversight structure

(2.1) Organizational structure

A financial institution must has the organizational structure that promotes appropriate IT risk management and in line with the three lines of defense concept. There must be the clear segregation of duties among those who (1) perform IT operations; (2) manage IT risks; and (3) perform IT audit. In addition, a financial institution must ensure that there is the balance of power, as the IT audit function must be independent from IT operations and IT risk management functions.

On this, a financial institution may appoint senior managements or head of the unit to be responsible for IT security (IT security function), which is independent from IT operations function. The appointed person must have IT knowledge and competence and is capable to deal with cyber threats, such as receiving a relevant certificate according to international standards.

(2.2) IT risk oversight committee

(2.2.1) A financial institution must set up a committee to be responsible for IT management and oversight of IT operations, such as IT Steering Committee.

(2.2.2) A financial institution must set up a committee to be responsible for the oversight of IT risk management according to its IT risk management policy.

(2.2.3) A financial institution must set up a committee to be responsible for the oversight of IT audit, where the auditing process should cover IT operations and IT risk management, as well as the oversight of compliance with relevant IT laws and regulations.

(3) Staff management

A financial institution must have the appropriate management of staff responsible for IT operations, IT risk management and IT audit, as well as staff using IT in their day-to-day operations. The key concerns for the staff management include the knowledge and competence of staff, their workloads, and IT security controls, where the financial institution must carry out, but not limited to, the following:

(3.1) The management of staff responsible for IT operations, IT risk management and IT audit must cover the following:

(3.1.1) Recruitment process – in order to have the staff who have proper qualifications, sufficient knowledge and experiences as necessary for their assignments, the staff may receive a general IT certificate or specific IT certificate that is relevant to their assignments.

(3.1.2) Staff adequacy – in order that the number of staff is appropriate to the volume of IT usage of the financial institution

(3.1.3) Measures to build and raise IT risk awareness – in order that the staff are aware of their roles and responsibilities, including measures to ensure that the staff perform their assigned duties and responsibilities.

(3.2) There must be appropriate training sessions, conducted within an appropriate timeframe, for the board of directors, senior managements and staff responsible for IT operations, IT risk management and IT audit. The training must cover relevant contents, such as IT development, cyber threats, IT risk management or IT regulations, so that the board of directors, senior managements and staff responsible for IT functions will have sufficient knowledge and skills necessary for their relevant responsibilities.

(3.3) Terms and conditions of an employment contract should clearly outline the responsibilities of the employee on IT security controls in order to prevent any data leakage or possible damage to IT assets of the financial institution.

(3.4) The management of access rights of staff responsible for IT functions – the access rights must be regularly updated, especially when there is any change of the assignment or the employment is terminated, such as reviewing the permission to access data. Any changes to the access rights, assignments and responsibilities must be communicated to the related persons.

(4) IT risk awareness

A financial institution must sufficiently and appropriately communicate with and provide knowledge to staff responsible for IT operations, IT risk management and IT audit as well as staff using IT in their day-to-day operations so that the staff have understanding and are aware of IT risk and secure use of IT, such as arranging a staff training session on the secure use of internet-facing devices, carrying out an IT BCP exercise in preparation for cyber attacks.

(5) Policies on IT risk supervision

(5.1) A financial institution must formulate (1) IT security policy; and (2) IT risk management policy in writing, where those policies must meet the CIA principles, namely (1) confidentiality; (2) integrity; and (3) availability. The policies must be in line with the strategies of the financial institution on the use of IT in its business operations and risk management, as well as in line with international standards or generally accepted frameworks on IT risk management and IT security controls.

In addition, those policies must be commensurate with the nature of business, volume of transactions, complexity of IT, and relevant risks including risks from the use of IT within the financial institution and the risks from using the IT outsourcing services.

(5.2) The IT security policy and IT risk management policy must be reviewed at least once a year and when there is any significant change.

5.3.2 IT security

To ensure that a financial institution has efficient IT security controls, the financial institution must use the IT security policy to set out IT security procedures and processes, which must cover, but not limited to, the following:

(1) IT asset management

A financial institution must have appropriate IT asset management, where there must be an IT asset register so that all IT assets can be identified, and it can also be used to set out a practice for IT security controls. IT assets must be regularly maintained to ensure that they are ready to use and can continuously support the business operations.

(2) Information security

A financial institution must have information security controls for data transmitted through communication networks and data stored on IT systems and any storage media. And, to ensure data confidentiality, data must be appropriately classified, kept and disposed depending on its classification, and encrypted by a reliable and generally accepted encryption technique (cryptography).

(3) Access control

A financial institution must have the control of access to its operating systems, systems, and databases, as there must be the management of access rights and authentication. The access rights must be given depending on the need to access any particular system and risk level in order to prevent the access and revision to systems or data by unauthorized persons.

(4) Physical and environmental security

A financial institution must have security controls for its data centers, IT workplaces, as well as the areas of critical IT systems. There must also be a

protection system and maintenance process for computer hardware and facility system connected to IT systems in order to prevent possible attacks or damage from natural disasters and ensure that they can continuously support the business operations.

(5) Communications security

A financial institution must have security controls for its communication systems so that the systems and data transmitted through them are secure and protected from any possible attacks or threats.

(6) IT operations security

A financial institution must have security controls for its IT operations so that the IT operations are secure, which must cover, but not limited to, the following:

(6.1) Capacity management for IT systems and facility systems, such as conducting an assessment of the future demand for IT resources so that the IT resources are properly managed, as they can sufficiently support the business operations, while the financial institution can manage IT resources to deal with its future needs

(6.2) Security controls for the severs and user devices (endpoint devices), such as installing anti-virus or anti-malware software or cyber attack in order to prevent data leakage or unauthorized access

(6.3) Data backup – data must be backed up using an appropriate approach within an appropriate timeframe, such as on a daily basis so that backup data is ready to use whenever the original data is unavailable or damaged

(6.4) Keeping of logs of the servers and important networking hardware, such as keeping and reviewing access logs and activity logs in order to monitor and inspect the access and the use of the system or data; this may be provided to customers as evidence of their electronic transactions

(6.5) Security monitoring – there must be a process or tools for monitoring suspicious incidents or threats that may affect critical IT systems, such as installing a system for monitoring and analyzing cyber threats so that the financial institution can promptly detect, prevent and handle suspicious incidents or threats

(6.6) Management of system vulnerability according to risk level – so that the vulnerabilities are detected and the financial institution can promptly take further actions to prevent possible threats; a vulnerability assessment for critical

IT systems must be conducted at least once a year and when there is any significant change

(6.7) Penetration test, which may be conducted by an independent internal or external expert; the test must cover internet-facing systems and be conducted at least once a year and when there is any significant change in order to detect the vulnerabilities and that the financial institution can promptly make improvements to prevent possible threats

(6.8) Change management – there must be a secure and sufficient process for managing and controlling a change, which may be in form of, such as, system deployment, system configuration, patch installment, in order to ensure that the change correctly and completely reaches the specified objectives and the unauthorized change is prevented

(6.9) System configuration management – there must be a control process for the configuration of production systems, and the configuration must be regularly reviewed in order to prevent operational errors

(6.10) Patch management – there must be a control process for the installment of patch on production systems in order that the important security patch is promptly installed

(7) System acquisition and development

(7.1) System acquisition

A financial institution must set out clear and appropriate criteria for the selection of system and service provider, which should cover, for example, the credibility of system or service provider, certification (according to international standards or generally accepted IT standards), system security, system support and maintenance, to ensure that the system and service provider can respond to business needs of the financial institution. Other key concerns also include the flexibility in the replacement of service provider, technological changes, or future changes in business strategies of the financial institution.

(7.2) System development

A financial institution must carry out the design, development and testing of system to ensure that the system is accurate, secure, reliable, ready to

use, and is flexible enough to accommodate any changes in the future. And, the financial institution must have in place, but not limited to, the following:

- Technical specification, which covers security controls as well as a process for testing, maintaining and monitoring the system security

- Source code version control

- Segregation of duties and responsibilities between those involved in system development, such as those who develop the system must be independent from those who deploy the system into the production environment

- Separation of environments of the system development, testing, and production

- Testing process, such as conducting the unit test, system integration test, user acceptance test, and security test; the tests must be conducted according to a security process as specified in the technical specification

- In developing or making any modifications to a service system or system for electronic transactions - a performance test must be conducted

- A practice for safeguarding and confidentiality of critical data used in the tests

- Preparation of instructions and trainings for users and administrators

(8) IT incident and problem management

A financial institution must properly and promptly manage IT incidents and problems, where the incidents and problems must be recorded, analyzed, and reported, together with the resolutions, to the board of directors, designated committee or senior managements in a timely manner. In addition, the financial institution must figure out the root causes of those problems in order to resolve the actual problems and prevent a recurrence of the incidents.

(9) Preparation of IT business continuity plan

(9.1) A financial institution must set up a working group or appoint a particular unit to be responsible for preparing an IT business continuity plan, which

must be in written and in line with the specified policy. And, the IT business continuity plan must be approved by the board of directors.

(9.2) In preparing an IT business continuity plan, a financial institution must take into consideration the nature of business, volume of transactions, IT complexity, and relevant risks, which include the risk of losses due to any particular events and general risks, such as operational risk, reputational risk, and other risks, such as interdependency risk, concentration risk as well as systemic risk.

(9.3) An IT business continuity plan must be practical as it can effectively be used to mitigate losses, and must be in accordance with the Policy Statement of the Bank of Thailand Re: Business Continuity Management (BCM) and Business Continuity Planning (BCP) of Financial Institutions. The plan must specify the recovery time objective (RTO) and recovery point objective (RPO), which will depend on the materiality of system, as well as the maximum tolerance period of disruption (MTPD) to ensure the continuity of business operations of the financial institution and that the plan can deal with the incidents that may lead to a disruption or damage to the system, such as cyber threats, natural disasters. The plan will also ensure that the financial institution can rapidly recover the system and return to its normal operations.

(9.4) A financial institution must prepare instructions or guidelines for the implementation of IT business continuity plan, while there must be the communication and related training sessions so that those taking part in the plan have understanding and can, accordingly, perform their duties under the plan.

(9.5) An IT business continuity plan must be reviewed and tested at least once a year and when there is any significant change.

(9.6) A financial institution must set up a disaster recovery site that is ready to operate whenever the primary site encounters a disruption. The disaster recovery site should be remote from the primary site to ensure that they do not share the same disruptions or have been affected from the same causes at the same time, such as power outage, natural disasters.

(10) Third party management

As a financial institution enters into an arrangement with third-party service providers or business partners by which there is a system interconnection or those providers/partners can access critical data of the financial institution or customers, the arrangement must be made in form of a contract or service level agreement that

clearly specifies duties, responsibilities and service conditions, such as the service provider must dispose all data of the financial institution and customers when the contract matures or the service is canceled, liability for data leakage if the data is used for other purposes apart from those as specified in the contract or agreement.

In addition, as a financial institution enters into an arrangement with third-party service providers or business partners for joint development or operations of financial services, the financial institution must take into consideration the business continuity, limitations or conditions on the change of service provider or business partner, as well as conditions on the termination or expiration of contract (exit strategy) to ensure that the financial institution can continuously operate its business and can deal with technological changes in the future.

On this, if a financial institution uses IT outsourcing, it must comply with the Bank of Thailand Notification Re: Regulations on IT Outsourcing for Business Operations of Financial Institutions.

5.3.3 IT risk management

To ensure that a financial institution can effectively manage its IT risks, the financial institution must formulate the IT risk management policy that covers the organizational structure, and roles and responsibilities of those involved in IT risk management. The policy must be used to draw up operating procedures and processes on IT risk management of the financial institution, which should cover, but not limited to, the following:

(1) Risk assessment

(1.1) Risk identification

A financial institution must identify its IT risks, which includes cyber threats and vulnerabilities. The IT risks may be caused by the operating process, IT system, personnel, or external factors.

(1.2) Risk analysis

A financial institution must understand and analyze its IT risks in order to set out the appropriate risk management practices.

(1.3) Risk evaluation

A financial institution must assess the possibility that IT risks may arise and the severity of impact on its internal and business operations, and must set out the level of IT risk appetite.

(2) Risk treatment

A financial institution must set out a practice for managing, controlling and preventing risks that is appropriate to the results of IT risk assessment so that the residual risk is controlled within the IT risk appetite. A balance between the potential costs and the benefits that the financial institution is expected to receive should also be considered.

In addition, a financial institution should develop IT key risk indicators for its business operations so that they can be used for monitoring and reviewing IT risks. Those indicators must be consistent with the materiality of each IT function.

(3) Risk monitoring and review

A financial institution should have in place a process that allows it to effectively monitor and review IT risks to ensure that the risks are controlled within the IT risk appetite.

(4) Risk reporting

A financial institution must report the results of IT risk management and the possible IT risks to the board of directors or designated committee within an appropriate timeframe.

On this, a financial institution must review its operating procedures and processes on IT risk management at least once a year and when there is any significant change.

5.3.4 IT compliance

A financial institution must have the supervision of IT compliance, such as the Electronic Transactions Act, Computer Crime Act, Electronic Payment System Act, in order to prevent the offence or incompliance with those laws and regulations.

5.3.5 IT audit

(1) A financial institution must have IT auditors who have knowledge, experiences, and competence in an IT audit. The auditors may be internal auditors, external auditors or specialists, but they must be independent from the IT operations function or IT risk management function.

(2) A financial institution must set out an IT audit plan and scope that reflect the materiality and level of IT risks as well as IT risk management policy of the financial institution. The IT audit plan and scope must be approved by the audit committee and must cover critical IT systems/activities of the financial institution. And, the IT audit plan and scope must be reviewed at least once a year and when there is any significant change.

(3) A financial institution must conduct an IT audit at least once a year, according to the audit plan and scope as specified in (2) and whenever there is a significant IT incident.

(4) A financial institution must arrange for independent external specialists to assess the critical systems or technologies, for which the audit is required but the financial institution has limited resources or the internal IT auditors as specified in (1) are not capable of doing so. The scope of the audit may include an assessment of complex systems or the use of new technology, or an assessment of the adaptability of the system to deal with future business operations of the financial institution within a rapidly evolving technology landscape.

(5) A financial institution must prepare an IT audit report, which must be presented to the audit committee. The report must be kept at the financial institution for examination by the Bank of Thailand when requested.

(6) A financial institution must follow up issues from an IT audit, while the significant issues must be presented to the audit committee and related units.

5.3.6 IT project management

(1) A financial institution must conduct a study to evaluate the necessity and expected benefits of an IT project before commencing the project, where the appropriate technology must be used and there must be an assessment of risks and impact on other units or related systems. The IT projects must be prioritized and presented to the board of directors, or designated committee or senior managements, for approval.

(2) A financial institution must set out a project management framework in writing as it will be used as project management guidelines. The framework must cover key arrangements, namely project commencement, project implementation and control, project completion and project review. And, there must be the clear control and supervision structure of the project (project governance), which should cover, but not limited to, the following:

(2.1) There must be the project commission to be in charge of monitoring the project milestones, giving recommendations and making a decision on critical matters of a project. This will ensure that the project can operate as planned. The project commission should consist of executives or representatives from related units.

(2.2) There must be a unit or work team to be in charge of overseeing the overall operations of a project (which may be in form of "project management office (PMO)". The PMO will be in charge of developing the format, process and tool that will be adopted as standards for project management and the monitoring of project development. The PMO will report the significant development and overview of a project to the board of directors, or designated committee or senior executives, for their acknowledgement to ensure that the project will reach the targets as planned.

(2.3) There must be a project manager to be in charge of managing each individual project according to the project management procedures and delivering each subproject according to the format, process and tool as specified by the PMO. This will ensure that the project can be accurately and completely delivered as planned.

5.4 Submission of reports to the Bank of Thailand

A financial institution must inform the Bank of Thailand of significant IT problems or incidents that affect its services, IT systems or reputation, as well as the events where its critical IT functions have been attacked or been threatened by cyber attacks, where those problems or incidents are the issues that the financial institution must report to its top executive. Those IT problems and incidents shall be reported to the Information System Examination Department, Payment Systems Policy and Financial Technology Group, Bank of Thailand, immediately or as soon as they are discovered, and the causes and resolutions that have been taken may later be reported.

5.5 Submission of an approval request for technology usage or change of technology usage

In case where a financial institution uses any technology for the first time or make any change to its technology usage that may affect or pose significant risks to the business operations, the financial institution shall submit a plan for its new technology usage or change of technology usage, which has been approved by the board of directors or designated committee, to the Financial Institution Business Supervision Department, Financial Institutions Policy Group, Bank of Thailand, before proceeding. The plan must indicate reasons and necessity, details of IT usage, customer protection measures, IT business continuity plan, risk assessment results and risk management framework, which have been considered and signed off by the risk management unit of the financial institution. The Bank of Thailand may ask for any further documents, and will finish its consideration within 30 business days from the day the request and supporting documents have been correctly and completely received.

Should a financial institution have any inquiries about the determination whether any IT usage or change of IT usage will lead to a significant impact or risks to the business operations, the financial institution shall consult the Financial Institution Business Supervision Department, Financial Institutions Policy Group, Bank of Thailand, before proceeding.

5.6 Request for relaxation of the guidelines

If any particular financial institution cannot comply with the regulations as specified in this Notification, the financial institution shall submit a request for relaxation of the regulations to the Financial Institution Business Supervision Department, Financial Institutions Policy Group, Bank of Thailand, on a case-by-case basis, by giving reasons and details of necessity as well as an operating plan for the full compliance with the regulations. The Bank of Thailand will finish its consideration within 30 business days from the day the request and documents have been correctly and completely received.

5.7 Transitory provisions

As this Notification has come into effect, if any particular financial institution cannot comply with the regulations as specified in Clause 5.3.1, the financial institution must manage to fully comply with those regulations within 1 year from the effective date of this Notification by not seeking the relaxation of those regulations.

6. Effective Date

This Notification shall come into effect as from 1 April 2018 (B.E.2561) onwards.

Announced on 20 December 2017 (B.E.2560)

(Mr. Veerathai Santiprabhob)
Governor
Bank of Thailand

Regulatory Policy Department
Tel. 0 2283 6938

Questions and Answers on the Bank of Thailand Notification
Re: Regulations on Information Technology Risk of Financial Institutions
Dated 20 December 2017 (B.E.2560)

No.	Question	Guided Answer
IT governance		
1	In case where the board of directors does not consist of one member who has IT knowledge, but the financial institution has arranged IT training sessions for the board, does this comply with the guidelines as specified in this Notification?	The board of directors must consist of "one member" who has IT knowledge or experiences to ensure that the board can make suggestions for business directions and oversee that the financial institution has the IT usage that is appropriate to its business strategies and has effective IT risk management. That board member may have IT education or working experiences in IT. While, attending IT training sessions may not be sufficient as the sessions only provide supplementary knowledge and awareness of the changing technologies and its relevant risks.
2	As the Bank of Thailand requires that one board member must have IT knowledge or experiences, is it also required that this board member must be an independent director or a non-executive director?	The Bank of Thailand does not specify that the board member who has IT knowledge or experiences must be the "independent", "non-executive" or "executive" director.
3	In case where the board of directors, delegates its authority to oversee and support IT risk management to the designated committee, such as Risk Management Committee, including approval of an IT project or IT supervision policy as well as the implementation of those policies, is it still required that one board member must have IT knowledge or experiences?	The board of directors cannot delegate the designated committee to approve an IT supervision policy, but may delegate the committee to oversee and implement those policies, where the board of directors must be informed of the results of those operations. Therefore, one board member is still required to have IT knowledge and experiences to ensure that the board can effectively perform its duties and

No.	Question	Guided Answer
		responsibilities as specified in the Notification.
4	For a foreign bank branch or a subsidiary of a foreign bank that has committees and IT functions, namely IT operations function (1st line), IT risk management (2nd line) and IT audit function (3rd line) operated abroad, while having an IT operations unit, which is part of 1st of the parent company (head office), in Thailand, is this structure considered in accordance with the regulations as specified by the Bank of Thailand?	In determining if the IT oversight structure is in accordance with the guidelines, the entire structure of the bank will be considered, including units in other countries and those in Thailand. If "the structure" meets the requirement on segregation of duties, as (1) IT operations unit; (2) IT risk management unit; and (3) IT audit unit are independent from each other, while there is the IT risk oversight committee according to the requirements as specified in Clause 5.3.1 (2.1) and (2.2), it is considered that the foreign bank branch or subsidiary has the IT oversight structure in accordance with the regulations as specified by the Bank of Thailand.
5	For a foreign bank branch or a subsidiary of a foreign bank that adopts an IT risk supervision policy as specified by the head office/parent bank abroad, is it still required that the bank must have that policy approved by the relevant management committee of the foreign bank branch or the board of directors of the subsidiary of a foreign bank?	A foreign bank branch or a subsidiary of a foreign bank may adopt an IT risk supervision policy as specified by its head office/parent bank, but it must ensure that such policy comply with the regulations as specified by the Bank of Thailand. However, the relevant management committee of the foreign bank branch or the board of directors of the subsidiary of a foreign bank must approve that policy.
IT security		
6	Can the IT operations unit set out a process for managing data access, or is it required to set out by the unit that is independent from the IT	A financial institution can independently set the structure of a unit responsible for managing data access, as the Bank of Thailand does not require that such

No.	Question	Guided Answer
	operations unit?	responsibility must be of any particular unit and it is left to the discretion of each financial institution. However, that structure must comply with the "segregation of duties" concept.
7	In case where a subsidiary of a foreign bank uses the core banking and related systems of the parent bank abroad, can it use the results of a penetration test of its parent bank?	A subsidiary of a foreign bank may use the results of a penetration test of its parent bank abroad, but the test must cover all critical systems used by the subsidiary.
8	If a financial institution has a primary site and disaster recovery site, is it still required to have another disaster recovery site?	A financial institution must set out a policy on establishment of a disaster recovery site, by considering the necessity, relevant risks and appropriateness of having a secondary disaster recovery site.
IT compliance		
9	Is it required that an IT compliance function must be independent from the compliance unit? What are the qualifications of those responsible for IT compliance?	An IT compliance function may perform by the compliance unit, but those responsible for this function must have knowledge and understanding of laws and regulations concerning the use of IT of the financial institution.
10	Can a foreign bank branch or a subsidiary of a foreign bank use the IT compliance unit of its head office/parent bank abroad? Is it required to set up that unit or compliance team in Thailand?	A foreign bank branch or a subsidiary of a foreign bank may use the IT compliance unit of its head office/parent bank abroad. However, that IT compliance unit must have knowledge and understanding of laws and regulations concerning the use of IT of the branch/subsidiary in Thailand, which may be different from the laws or regulations applied to its head office/parent bank abroad.

No.	Question	Guided Answer
IT audit		
11	What is the unit that is responsible for arranging for external specialists to assess critical systems or technologies according to the Notification?	The Bank of Thailand does not require that such responsibility must be of any particular unit, while a financial institution must set out a policy on entering to an agreement with external specialists for such purposes, and that policy must be in line with other relevant policies of the financial institution.
12	**The Bank of Thailand (BOT) had communicated during the meeting to clarify the draft BOT Notification Re: Regulations on Information Technology Risk of Financial Institutions (IT Risk Notification) on 23 August 2017 that the BOT Notification no. FPG. 26/2551 (2008) Re: Permission for Commercial Banks to Operate E-Banking Services would be repealed after the IT Risk Notification became enforceable. Does this mean that commercial banks can undertake preparation to comply with the IT Risk Notification, without having to have the electronic fund transfer system audited by external auditor for the year 2017 and during January – March 2018 as required under BOT Notification no. FPG. 26/2551?** **(Amended on 30 April 2018)**	**Upon consideration, the Bank of Thailand (BOT) grants permission to commercial banks to undertake IT audit according to the guidelines specified under the IT Risk Notification instead of the audit of electronic fund transfer system under the BOT Notification no. FPG. 26/2551 for the year 2017 – March 2018. The rationale is that commercial banks are already aware of the repeal of the BOT Notification no. FPG. 26/2551 and begin to prepare to comply with the new IT Risk Notification instead. (The IT Risk Notification does not stipulate a specific audit of the electronic fund transfer system but requires commercial banks to prepare a plan and scope for IT audit according to the importance and risk of each commercial bank's reliance of the IT. Whereby the IT auditor, who can be an independent internal, external auditor, or outside expert, must be knowledgeable and has expertise in IT audit) This is to alleviate the burden**

No.	Question	Guided Answer
		and cost of commercial banks in having to conduct an audit of the said fund transfer system.
IT project management		
13	Can a unit/work team that is responsible for monitoring the overall project management (Project Management Office – PMO) be a unit/work team that is responsible for monitoring both “IT” and “Non-IT” project management? Can a foreign bank branch use the PMO of its regional office in place of setting up the new PMO in Thailand?	The PMO may be a unit/work team that is responsible for monitoring both IT and Non-IT project management. And, a foreign bank branch may use the PMO of its regional office in placing of setting up the PMO in Thailand, but that PMO must monitor the progress and overall management of important IT projects of the branch in Thailand and report to the relevant designated committee or executives to ensure that those projects reach the targets as planned.
Change of IT usage		
14	In case where a financial institution uses new technology that may lead to a significant impact on its business operations, but that technology has already used by a company within its group, will the financial institution be required to seek approval for the usage of such technology from the Bank of Thailand?	The financial institution must seek approval from the Bank of Thailand, as the Bank of Thailand must consider risks and impacts on the financial institution from using such technology.
15	What is the scope of “significant” change of technology usage for which prior approval from the Bank of Thailand is required according to the Notification?	In determining if any change of technology usage is “significant”, a financial institution should consider if it meets one of the following criteria: (1) may lead to a bank wide impact, such as the change of a system that involves a wide range of its customers and people

No.	Question	Guided Answer
		(2) may lead to a banking system wide impact, such as the change of a system this connected to the central settlement system Should a financial institution have any inquiries about the determination if any change of technology usage will lead to a significant impact or risks to the business operations, the financial institution shall consult the Financial Institution Business Supervision Department, Financial Institutions Policy Group, Bank of Thailand, before proceeding.