Notification of the Insurance Commission
Re: Criteria for Non-life Insurance Companies' Governance and Management of Information Technology Risks (IT Risks)
B.E. 2563 (2020)

The insurance industry currently faces the challenges of fierce competition and quantum leaps of technological change. Consequently, Companies must adapt to stay abreast of changes and afloat with business continuity. Several Companies have adopted technology in their operations, product development, and customer services, for example: the sale of insurance products via electronic media, customer data storage systems, underwriting systems, finance and accounting systems, systems for payments of indemnity, compensation, and other benefits according to insurance policies. The increasing role of technology in business operations leads to inherent risks in the form of Information Technology and Cyber Threat risks that have escalated substantially, which could harm and impact customer confidence.

Therefore, the Insurance Commission prescribes the criteria and procedures for the governance and management of Information Technology risks, so that insurance Companies shall have in place the appropriate and systematic governance and management of Information Technology risks and Cyber Threats, as well as appropriate control and maintenance of Information Technology security in conformity with international standards, and the supervision and consideration of action plans in introducing Information Technology in their organizations, and the management of Information Technology projects, Information Technology compliance, and Information Technology audit.

By virtue of Section 37 (10) and (12) of the Non-life Insurance Act B.E. 2535 (1992), as amended by the Non-life Insurance Act B.E. 2551 (2008), together with the resolutions of the Insurance Commission Meetings No. 11/2019 on 25 October 2019and No. 6/2020 on 22 May 2020, the Insurance Commission prescribes this Notification as follows:

Clause 1 This Notification shall be called the "Notification of the Insurance Commission Re: Criteria for Non-life Insurance Companies' Governance and Management of Information Technology Risks B.E. 2563 (2020)."

Clause 2 This Notification shall take effect from 1 January 2021 onwards.

Clause 3 In this Notification:

"Information Technology Risk (IT risk)" means risk that may arise from the use of Information Technology in business operations that could have an impact on Companies' system or operations, including any risk that may arise from Cyber Threats;

"Information Technology (IT)" means any information technology that is used in business operations, and includes any data or information, operating system, application system, database system, computer hardware, and communication system;

"Information Technology Assets " means

(1) Information Technology Assets in the form of systems include computer network systems, computer systems, computer application systems, and information systems;

(2) Information Technology Assets in the form of equipment include computer machines, computer hardware, data recording devices, and any other equipment relating to the Information Technology systems;

(3) Information Technology Assets in the form of data include information, electronic data, and computer data;

"Information Technology Security (IT Security)" means the protection of the Information Technology and the Information Technology Assets from unauthorized access, use, disclosure, disruption, alteration, loss, damage, destruction, or becoming known of in any way, and includes information security, that embraces the maintenance of Confidentiality, Integrity, and the Availability of the Information Technology and the Information Technology Assets, as well as other attributes, namely authenticity, accountability, non-repudiation, and reliability;

"Cybersecurity" means any measure or activity that is established with a view to protecting, handling, and mitigating risks from both domestic and international Cyber Threats, in compliance with the law on Cybersecurity;

"Cyber Threat" means any unlawful act or activity through the use of computers or computer systems or malicious programs, with the aim of harming computer systems, computer data, or other related data, and is an imminent danger to the functioning of computers, computer systems, or other related data;

"Cyber" means data and communication arising from the provision of services or the application of computer networks, the Internet, or telecommunication networks, as well as the ordinary provision of services of satellite and similar network system that are generally linked;

"Confidentiality" means the practice of maintaining or reserving for the purpose of the protection of computer network systems, computer systems, computer application systems, information systems, information, electronic data or computer data from any unauthorized person's access, use, or disclosure;

"Integrity" means any arrangement to ensure that information, electronic data, or computer data is valid at the time of use, process, transfer or storage against any unauthorized or unlawful alteration, loss, damage, or destruction;

"Availability" means the practice of ensuring that the Information Technology Assets or the Information Technology is functionable, accessible, and usable whenever needed;

"Company" means a company that has been granted a a non-life insurance business license under the law on non-life insurance, and shall include a foreign non-life insurance company's branch that has been granted a license to operate a non-life insurance business in the Kingdom of Thailand under the law on non-life insurance;

"Board of Directors" means the Board of Directors of a Company under the law on non-life insurance, and shall include the executive board of a foreign non-life insurance company's branch that has been granted a license to operate a non-life insurance business under the law on non-life insurance where, the branch manager also acts as a director;

"Executive" means the manager, the first four persons holding executive positions beneath the manager, every person holding executive positions equivalent to the fourth executive, and shall include any person holding an executive position in the accounting or finance departments at the level of department manager or above;

"Office" means the Office of the Insurance Commission.

Clause 4 The Office shall be empowered to prescribe guidelines in the interest of ensuring compliance with this Notification, or to issue orders for a Company to undertake any act with respect to the management of the Information Technology Risks (IT Risks), including Cyber Threat risks, in conformity with the size, characteristics, complexity, and the level of Information Technology Risks of the Company; and upon having complied with the guidelines or orders, as the case may be, it shall be considered that the Company is in compliance with the relevant provision of this Notification.

Clause 5 A Company must have in place the following criteria for the governance and management of its Information Technology Risks:

(1) Information Technology governance (IT governance);

(2) Information Technology project management (IT project management);

(3) Information Technology Security (IT Security);

(4) Information Technology Risk management (IT risk management);

(5) Information Technology compliance (IT compliance);

(6) Information Technology audit (IT audit);

(7) Governance and management of Cybersecurity;

(8) Reporting of Cyber Threats or threats to the Information Technology system.

Chapter 1
Information Technology Governance
(IT Governance)

Clause 6 A Company must have in place a governance and management of Information Technology and Cyber Threat risks in proportion to the size, characteristics, complexity, and environment of its business operations. Roles and responsibilities of the Board of Directors shall be defined. Governance and the management of Information Technology Risks (IT Risks) shall be properly structured to ensure checks and balances that are independent and conform to the three lines of defense principle. The Company must also establish policies in relation to the governance of Information Technology Risk (IT Risks).

Clause 7 The composition of a Company's Board of Directors must be in accordance with the relevant Notification of the Insurance Commission on good corporate governance of non-life insurance companies. In this regard, the Company should retain at least one director who is knowledgeable and experienced in Information Technology for the purpose of setting its business direction in line with the current situation, overseeing the adoption of technology to accommodate the business operations strategy, and staying abreast of risks and changes in the development of Information Technology. In addition, appropriate training on Information Technology, Cyber Threat trends, and related risks should be provided to the members of the Board of Directors.

Clause 8 A Company's Board of Directors has the responsibility to oversee the Company's compliance with the criteria prescribed in this Notification and has the following duties:

(1) To oversee the application of Information Technology and ensure its conformity with the business operations strategy, its flexibility to adequately accommodate any change

in Information Technology, as well as its attention to any changes in future business operations and its preparedness for dealing with Cyber Threats;

(2) To oversee the maintenance of the management of Information Technology and Cyber Threat risks that may arise from the adoption of Information Technology in the business operations. These risks shall be regarded as major organizational risks and an integral part of enterprise risk management (ERM);

(3) To oversee an establishment of written policies relating to the governance and management of Information Technology and Cyber Threat risks, which contain the following details at a minimum:

(a) Information Technology risk management policy;

(b) Information Technology Security policy that includes action plans or guidelines for the following subjects at a minimum:

1) Information Technology continuity plan;

2) Plan or guideline on the governance and management of Cybersecurity risks under Clause 7;

(4) To oversee the Company's implementation of all approved policies through developing guidelines on the Information Technology risk management and the Information Technology Security, and ensuring due compliance and regular review of such policies and guidelines at least once a year, or upon any material change;

(5) To oversee reporting to the Company's Board of Directors or delegated subcommittee, covering the following subjects at a minimum:

(a) Reporting on the overview of the outcome of the Company's Information Technology risk management, whereby the head of the risk management unit must be delegated to proceed with such reporting to the Company's Board of Directors or delegated subcommittee;

(b) Information with respect to all Information Technology issues or incidents that are significant, or may have a widespread impact on, or may affect the Company's reputation or its Information Technology Security operations and maintenance;

(c) Results of the testing and compliance with the Information Technology continuity plan.

In this regard, the Company's Board of Directors may delegate a subcommittee to oversee the activities described in paragraph one in the following manners:

(1) An Information Technology steering committee (IT steering committee) or other subcommittees shall be tasked to oversee the application of Information Technology and ensure its consistency with business operations strategy as stated in paragraph one (1);

(2) A risk management committee or other subcommittee shall be tasked to oversee the management of Information Technology and Cyber Threat risks pursuant to paragraph one (2), or to oversee an establishment of policies in relation to the governance and management of Information Technology and Cyber Threat risks pursuant to paragraph one (3);

In a case where the Company's Board of Directors tasks a subcommittee with duties to oversee the arrangements required pursuant to paragraph one, the subcommittee so tasked must report the outcome of such arrangements pursuant to paragraph two to the Board of Directors, as prescribed in this Notification.

Clause 9 A Company must establish a written policy in relation to the governance of Information Technology Risk (IT Risks) and ensure its conformity with the application of Information Technology in its business operations, potential risks in connection therewith, as well as risks associated with application of Information Technology internally and externally through the use of services rendered by third-party providers. The policy must be reviewed and approved by the Company's Board of Directors or delegated subcommittee in line with the following:

(1) An Information Technology Risk management policy must be in conformity with the Company's enterprise risk management policy. Said policy must define the organizational structure, the roles and duties of all concerned parties in the Information Technology Risk management, and describe the guideline on risk management that must contain details covering the following matters at a minimum:

(a) Duties and responsibilities in relation to the Information Technology Risk management;

(b) Procedure or steps in assessing and managing risks;

(c) Information Technology risk appetite;

(d) Criteria for risk assessment, which covers the extent of impact and the likelihood of any occurrence of incident, for the purpose of risk management prioritization;

(e) Procedure or tools for managing and handling risks in line with the Information Technology risk appetite;

(f) Defining Information Technology Risk indicators, and ensuring that such Information Technology Risk indicators are monitored and reported to the responsible person for the purpose of managing relevant risks properly and timely;

(g) Risk reporting.

(2) Information Technology Security policy (IT security policy) pursuant to Clause 14.

Chapter 2
Information Technology Project Management
(IT Project Management)

Clause 10 A Company must maintain efficient management of risks associated with the implementation of each Information Technology project to prevent any impact on the implementation of the strategic plan, taking into consideration the project's risks, prioritization, management framework, and supervision.

Clause 11 A Company must assess risks and prioritize each Information Technology project, through the following arrangements at a minimum:

(1) An arrangement of a study on the necessity and the expected benefits from any project that applies Information Technology in the business operations before its commencement, so as to ensure that the application of Information Technology is chosen appropriately;

(2) An arrangement of assessment of potential risks to and impacts on other business units and related systems;

(3) An arrangement of prioritizing projects and proposing them for approval by the Company's Board of Directors, delegated subcommittee, or Executive as having been specified beforehand. In the case of the Company's first application of any technology, or any change of technology that may cause a material impact or risk to the overall business operation, the Company must establish a set of clear requirements for consideration, and ensure an assessment of Information Technology Risks or review of related risks, as well as potential impact on the overall business operations of the Company. The arrangement shall also include tasking the Company's Board of Directors or delegated committee with a review and approval of action plans for the intended application of Information Technology, or any changes in the application of Information Technology.

Clause 12 A Company must clearly establish a written Information Technology project management framework, to serve as a guideline for project management, containing details of the following matters at a minimum:

(1) Commencement of the project;

(2) Implementation of the project;

(3) Control of the project;

(4) Closure of the project;

(5) Audit of the project;

Clause 13 A Company must oversee each Information Technology project by defining a clear project governance structure, appointing a project overseeing committee for supervising and monitoring developments of the project, as well as giving advice, reviewing and making decisions on key implementation of the project in order to ensure its conformity with specified plans.

Chapter 3
Information Technology Security
(IT Security)

Clause 14 A Company must maintain a written Information Technology Security policy in conformity with the intended application of Information Technology in the business operations and all potential risks associated with such application. The policy must be reviewed and approved by the Company's Board of Directors or delegated subcommittee, and undergo a review annually at a minimum, or whenever there is any material change. The policy must also be communicated to all personnel of the Company and contain the details of following matters at a minimum:

(1) Information Technology Assets management;

(2) Access control;

(3) Physical and environmental security;

(4) Information Technology operations security;

(5) Establishment of Information Technology continuity plans;

(6) Guideline on the governance and management of Cybersecurity risk.

Clause 15 A Company must make necessary arrangements for its human resource security management pertaining to Information Technology personnel, by establishing criteria for recruitment and selection of such personnel, rules or regulations applicable to their performance, and their termination.

Clause 16 A Company must make necessary arrangements for its Information Technology Assets management that includes the following arrangements at a minimum:

(1) An arrangement of maintaining a register of Information Technology Assets and ensuring periodic maintenance of the Information Technology Assets, as well as establishing security measures for the use of computer machines and related devices; for example, bring-your-own-device BYOD that are connected to the network of the Company, portable data storage devices (external hard disk/flash drive), etc.

(2) An arrangement of establishing a guideline for information classification appropriately in line with the level of Confidentiality and importance of such corporate information, , a guideline for ensuring security in conformity with information classification, as well as ensuring security of information during its transmission via communication networks, its storage in the system or other data storage media, and its destruction in line with such level of Confidentiality.

Clause 17 A Company must maintain control of access to its system, data, and Information Technology Assets to prevent any prohibited or unauthorized person's access to and modification of such system or data. Such control must include the following arrangements at a minimum:

(1) An arrangement to establish a policy on access to or use of its system, data, and Information Technology Assets including a policy on any use of service of the organizational communication network in conformity with its business operations requirements;

(2) An arrangement to manage relevant right of use and user authentication in accordance with the specified rights, taking into consideration the necessity of use and the level of risk;

(3) An arrangement to review and update the right of use within a specified period;

(4) An arrangement to revoke any person's right of use upon the person's change of duties or employment termination.

Clause 18 A Company must establish a guideline for cryptography for data security in conformity with the information's Confidentiality and importance classification.

Clause 19 A Company must maintain both physical and environmental security of its computer center, Information Technology related work areas, and spaces used in relation to important Information Technology, by making the following arrangements at a minimum:

(1) An arrangement to establish a written set of regulations on access to the computer center;

(2) An arrangement to establish control of an ingress into and an egress from its computer center by placing appropriate restrictions on computer center access rights, as well as maintaining a record and storage of information on such ingress and egress;

(3) An arrangement to establish a system for the protection, preservation, and maintenance of equipment, computer machines, and system facilities relating to Information Technology, such as, a backup power supply for the computer center, an air-conditioning system, a fire prevention or alarm system, closed circuit cameras, etc.

Clause 20 A Company must maintain its network and communication security, by making the following arrangements at a minimum:

(1) An arrangement to establish a segregation of its network and communication zones, through appropriately segregating the network and organizing strict connection controls between various application systems and important application systems.

(2) An arrangement to establish control and limits to right of access to its network system and remote access system, through controlling security in the connection with external networks and requiring appropriate approval of any access thereto.

Clause 21 A Company must maintain Information Technology operations security by ensuring the following management and arrangements at a minimum:

(1) An arrangement of pursuing change management and requiring a written approval of every change;

(2) An arrangement of pursuing capacity management to accommodate the current business operations and planning such management to accommodate all future applications;

(3) An arrangement of maintaining security of its server through system configuration management, patch management, as well as defining the right of access and restriction on the right of use for high privileged users (high privileged ID)***;***

(4) An arrangement of setting a procedure and process for data backup and appropriate frequency of such data backup activities, in conformity with the nature and complexity of its operations;

(5) An arrangement of logging data of its server, application system and important network equipment, with sufficient security to prevent any change, modification, or destruction thereof, and maintaining a regular Information Technology Security audit log;

(6) An arrangement of security monitoring, with a process or tool to detect unusual incidents or threats that have a significant impact on system security, as well as appropriate vulnerability management in conformity with risk levels, and engaging independent experts to perform penetration testing, particularly on the application and network systems that are connected to the public communication network system (internet facing) periodically or upon every material system change.

Clause 22 A Company must establish criteria and procedures for system acquisition and development in line with the following:

(1) For system acquisition, the Company must establish clear criteria for the assessment and selection of vendors or developers, engagement under a sale and purchase agreement, or a hire of work engagement agreement, setting forth clear conditions on system development;

(2) For system development, the Company must arrange for system design, development, and testing, to ensure that the system is accurate, secured, reliable, and available, with the following arrangements at a minimum:

(a) An arrangement of documenting system requirements and detailed technical specifications that cover the security issue and application system testing process;

(b) An arrangement of maintaining a process or tool for source code version control, through limiting any use thereof to an as-needed installer of production systems.

(c) An arrangement of segregating concerned parties in the system development process, with respect to their roles, duties, and responsibilities, for example, segregating developers from administrators;

(d) An arrangement of segregating the environment of the application system used for development and testing from that of the production system;

(e) An arrangement of running system tests prior to actual production, for example, unit tests, system integration tests, user acceptance tests, and security tests, in conformity with the security process specified in relevant technical specification documents, and maintaining security and Confidentiality of important data used in such tests;

(f) An arrangement of running a performance test on systems related to providing services or conducting electronic transactions;

(ฐ) An arrangement of providing all system users and administrators with manuals and training.

Clause 23 In the case that a Company engages third-party management service providers or has business partners, whose systems are connected to its Information Technology system, or accessible to its important information or that of its customers, the Company must arrange to define procedures and criteria for the assessment and selection of such third-party management service providers, as well as their engagement under service agreements, requirements for their compliance with the Company's security policy, terms of their service level agreements (SLA), and periodic inspection and monitoring of their services.

Regarding, Information Technology outsourcing, the Company may consider adopting courses of operations in conformity with the Office of the Insurance Commission's practical guideline on criteria for governing Information Technology outsourcing.

Clause 24 A Company must ensure suitable and timely management of Information Technology incidents and problems, by establishing procedures, processes, or plans for coping with Information Technology incidents and problems arising from the application of Information Technology, which include recording, analyzing and reporting such Information Technology incidents and problems, as well as resolutions of such to its Board of Directors or delegated subcommittee within a reasonable period of time. The Company must arrange a root cause analysis of such problems to identify courses of resolving problems from such root causes and preventing any future reoccurrence thereof.

Clause 25 A Company must conduct Information Technology continuity planning, which include the following arrangements at a minimum:

(1) An arrangement of data backup processes that cover important Information Technology systems, such as, the application system, the operating system, the database, etc., and accommodates data recovery suitable for its business.

(2) An arrangement of secured off-site storage of backup data, with the Company's monitoring of important data backup processes, testing of backup data recovery, and ensuring continuous availability of such backup data;

(3) An arrangement of maintaining a written information system disaster recovery plan, which has been approved and disseminated to the Company's personnel, and ensuring a review of the plan regularly or upon any material amendment or revision;

(4) An arrangement of testing an information system disaster recovery plan annually at a minimum and reporting the test results to the Company's Executive.

Chapter 4
Information Technology Risk Management
(IT Risk Management)

Clause 26 A Company must manage Information Technology Risks efficiently by establishing a policy on Information Technology Risk management which covers aspects of organizational structure and the roles and duties of all concerned parties. Such policy is to be reflected in the guidelines and procedures of Information Technology Risk management.

Clause 27 A Company must establish a guideline on the Information Technology Risk management which specifies the following context, scope, and criteria for risk management, at a minimum:

(1) Consideration of the likelihood of Information Technology Risks by specifying the context and the scope of assessment of risks, including an action plan, routine tasks, and application of Information Technology;

(2) Criteria for risk management with the details of criteria for risk assessment, which defines the severity of impact and the likelihood of the occurrence of Information Technology incidents;

(3) Information Technology risk appetite;

(4) Procedure for risk assessment to be applied for risk identification, analysis, and assessment;

(5) Procedure for risk management to be applied for considering options and measures in managing risks and establishing a risk management plan.

Clause 28 A Company must carry out a process of risk assessment with respect to Information Technology in line with the following criteria and procedures:

(1) Identification of Information Technology Risks, including major Cyber Threats and vulnerabilities, the incidence of which may result from operation process, application system, personnel, or external factors, as well as definition of its current control mechanism and responsible persons or risk owners;

(2) Analysis of Information Technology Risks by assessing the severity of impact and the likelihood of the occurrence of Information Technology incidents for the purpose of risk prioritization;

(3) Evaluation of risks by considering the severity and Information Technology risk appetite for the purpose of risk prioritization and identification of appropriate responsive measures.

Clause 29 A Company must ensure a course of risk treatment to arrange appropriate control and prevention in conformity with the results of Information Technology Risk assessment, for the purpose of keeping any residual risk in line with its risk appetite, by taking into consideration the balance of risk prevention costs and expected benefits, and defining Information Technology key risk indicators for the purpose of risk monitoring and review.

Clause 30: A Company must ensure an efficient Information Technology Risk monitoring and review procedure for the purpose of keeping such risks in line with its risk appetite.

Clause 31 A Company must ensure that a risk reporting, which entails the results of Information Technology Risk management and the trends of potential Information Technology Risks, is timely made by the head of its risk management unit to the Company's Board of Directors or delegated subcommittee.

Chapter 5
Information Technology Compliance
(IT Compliance)

Clause 32 A Company must oversee its compliance with the relevant laws and criteria on Information Technology (IT compliance), such as, the law on electronic transactions, the law on computer-related offenses, the law on Cybersecurity, the law on personal data protection, including the law on anti-money laundering, and other laws of a similar nature, for the purpose of preventing any violation of or non-compliance with the laws and criteria set forth by relevant regulatory authorities.

Chapter 6
Information Technology Audit
(IT Audit)

Clause 33 A Company must ensure a description of the roles, duties and the action plan in relation to the Information Technology audit, which include the following arrangements at a minimum:

(1) An arrangement of retaining an Information Technology auditor with the knowledge, experience, and expertise in Information Technology audit, who may be either an internal or independent auditor;

(2) An arrangement of establishing an action plan and scope of the Information Technology audit that cover its Information Technology Risks, and has been approved by the Company's audit committee and is subject to a review at least once a year or upon any material change.

Clause 34 A Company must arrange for Information Technology audit operations, which include the following arrangements at a minimum:

(1) An arrangement of appropriate Information Technology audits in conformity with its specified action plan and scope, and upon occurrence of any material Information Technology incident;

(2) An arrangement of engaging an independent expert to conduct a required audit in the case that its technology system is complex or involves a new technology, rendering the Company's internal assessment or audit unfeasible.

Clause 35 The Company must ensure a reporting and monitoring of the audit results, which include the following arrangements at a minimum:

(1) An arrangement of reporting the Information Technology audit results to the audit committee, and safekeeping such audit results report at the Company's premises in anticipation of the Office of Insurance Commission's inspection or request;

(2) An arrangement of monitoring issues identified during the Information Technology audit and reporting any critical issues to the Company's audit committee and relevant units.

Chapter 7
Governance and Management of Cybersecurity

Clause 36 A Company must maintain a guideline on the governance of Cyber resilience, entailing an operational framework and courses of actions for the overall

organizational governance and management of Cyber Threat risks, in conformity with the law on Cybersecurity and the size and complexity of its business operations.

Clause 37 A Company must maintain a governance of Cybersecurity and identification of risks, which include the following arrangements at a minimum:

(1) Cybersecurity governance;

(2) Maintaining a register and management of Information Technology Assets;

(3) Defining the scope and procedure for the assessment of Cyber risks in conformity with Information Technology Risk management or Information security;

(4) Establishing a risk management plan, risk management measures, or guideline on the management of Cybersecurity, in conformity with the results of the assessment of Cyber risks;

(5) Ensuring management of supply chain risk, guidelines for managing external service providers, formulating hiring contracts, assessment of appropriateness, monitoring and assessment of performance, and review of performance.

Clause 38: A Company must ensure risk protection, which include the following arrangements at a minimum:

(1) Establishing a guideline on the control and the protection of risks associated with critical information infrastructure, such as, computer systems, network systems, hardware equipment, software, data, application systems, etc., as well as application system configurations, application access management system, management of licenses, data security, application system developments which are safe according to steps or processes in the system development life cycle (SDLC), and management of patches with appropriate technology, for the purpose of putting in place processes, tools, and procedures for the Company's control or mitigation of potential impacts on Cybersecurity;

(2) Maintaining a cybersecurity procedure in conformity with good standards and practices;

(3) Establishing a guideline on the collection and analysis of Cyber Threat data, procedures and channels for data exchange and cooperation in managing and handling Cyber Threats both internally and externally.

Clause 39 A Company must ensure the inspection, detection, and monitoring of Cyber Threats, which include the following arrangements at a minimum:

(1) Providing channels for the reporting of any vulnerabilities, weaknesses, incidents, or situations relating to Cybersecurity, and defining the scope of duties and responsibilities of the relevant units, whether internal or external;

(2) Defining a course of action in searching, testing, and managing Information Technology vulnerabilities for the purpose of detecting, analyzing, monitoring, and alerting the responsible units of any Information Technology incidents or Cyber Threats, and establishing a guideline on communication and initial rectification in a timely manner.

Clause 40 A Company must maintain measures for handling and responding to a detected Cyber Threat, which include the following arrangements at a minimum:

(1) Establishing a guideline on managing and handling unusual incidents or Cyber Threats, so that the Company will be able to respond and handle risks in a timely manner;

(2) Creating, drilling or testing a Cybersecurity incident response plan (CSIRP), emergency plan, investigation and analysis of causes/solutions, and ensuring that a report thereof is made to its Board of Directors or delegated committee;

(3) Establishing a guideline on communications for the purpose of resolving Cyber Threat incidents or situations.

Clause 41 A Company must establish a guideline on the recovery from damage sustained in connection with Cyber Threats, which include the following arrangements at a minimum:

(1) Establishing a guideline and measures for recovery of damage sustained in connection with Cyber Threat incidents, in conformity with the results of the assessment of risks and impacts conducted pursuant to the Company's Cybersecurity operation framework and Information Technology Risk management;

(2) Establishing a guideline on communications for the purpose of recovery of damage sustained in connection with Cyber Threat incidents.

Clause 42 A Company must conduct Cybersecurity risk assessment by assessing risks associated with Cybersecurity and Cyber Threats for the purpose of identifying its risk situations, threats, vulnerabilities, and taking into consideration the following risk factors associated with Cyber Threats:

(1) Criteria for the assessment and classification of the severity and impact of Information Technology incidents or Cyber Threat situations, and the likelihood of the occurrence of Information Technology incidents, as well as the assessment of risk severity

arising from Cyber Threats, whereby the impact of Information Technology incidents shall be considered in accordance with the following aspects:

(a) Confidentiality;

(b) Integrity;

(c) Availability; and

(d) Law & regulation compliance.

(2) Arranging an assessment of risks associated with Cybersecurity or Cyber Threats and reporting the results of the Information Technology Risk management and the trends of potential Information Technology Risks to its Board of Directors or delegated subcommittee in a timely fashion.

Chapter 8
Reporting of Cyber Threats or Information Technology Threats

Clause 43 A Company must report Cyber Threats or Information Technology threats in the following manner:

(1) Reporting to the Office of Insurance Commission promptly upon any occurrence of or acknowledgement of material issues or incidents pertaining to application of Information Technology which impact provision of services, systems, information of insureds, or reputation of the Company, including any attack on the Company's important Information Technology, or any Cyber Threats attacks, as well as issues or incidents that the Company must report to its highest level Executive, with the detailed description and causes of such incidents as well as anticipated impact, action taken to solve issues, the results thereof, the period of issue-solving, and course to prevent future incidents;

(2) In the case of any Cyber Threat attack leading to problems or incidents involving the Company's provision of its major information infrastructure service which is a Cyber Threat of low severity, high severity, or critical severity, the Company must inform the Office of Insurance Commission or an agency as required by law of such breach without delay, within seventy-two hours, and also provide such information to or coordinate with the government agency or any organization established under the law on Cybersecurity for the Cyber Threats response and handling.

Notified on this 1st day of September B.E. 2563

(Mr. Prasong Poontaneat

Permanent Secretary, Ministry of Finance

Chairman of Insurance Commission

Kraithep / drafted/typewritten

[initials] / reviewed