Thai Institute of Directors

Guideline on Board's Role in IT and Data Governance

Content

Introduction

It is undeniable that information technology (IT) and data play important roles in driving business nowadays. They can accommodate companies to enhance operation efficiency, improve quality of products and services, or transform business model to reach new sources of income. Since technology can help companies respond better to social changes and evolving business environment, applying IT in creating business opportunity to support enterprise strategies and goals becomes crucial matter being discussed by the Board.

However, IT and data do not only bring about opportunities but also new form of risks that businesses have never before encountered. Among them are IT risks from system or data crashes and inevitable cyber threats that companies must stand ready to tackle any time. They also lead to the development of corporate governance principles as well as new laws and regulations that aim to encourage companies to consider the benefits of IT and data along with potential impact on stakeholders. Applying IT in business operations is about finding the most efficient way to use IT for value creation and respond to challenges in order to preserve value of the enterprise either via risk management, IT security, and data privacy.

Therefore, understanding principles, guidelines, and roles of the Board concerning IT and data governance would help the Board establish clear governance direction to ensure IT and data management generate utmost benefit to stakeholders and the enterprise.

This guideline has been developed to reflect the significance of this matter. The IOD sincerely hopes the essence of this document will help the Board establish IT governance policy framework and support the Board in performing its duties to create business opportunities and promote sustainable growth of the enterprise.

• Thai Institute of Directors •

Working Committee on ESG

Guidelines for Boards 2021

1. Mr. Kulvech	Janvatanavit	Chief Executive Officer, Thai Institute of Directors (Committee Chairman)
2. Mr. Rapee	Sucharitakul	Former Consultant, Thai Institute of Directors (Committee Consultant)
3. Mr. Veerasak	Kositpaisal	Director, Thai Institute of Directors

4. Representative from the Stock Exchange of Thailand

Ms. Sineenart	Chamsri	Vice President-Head of Corporate Governance Development Department
Mr. Pornchai	Tavaranon	Deputy Head of Corporate Governance Development Department
Mr. Suraphon	Buphakosum	Deputy Head of Corporate Governance Development Department

5. Representative from Government Pension Fund

Mr. Supawit	Chotiwit	Senior Director & Department Head, Investment Research Department

6. Representative from Association of Investment Management Companies

Ms. Voravan	Tarapoom	Honorary Chairman
Ms. Duangkamon	Phisarn	Secretary General

7. Experienced Directors at Listed Companies

Mr. Yuth	Worachattarn	Expert on Corporate Governance and Social Responsibility, The Stock Exchange of Thailand
Ms. Patareeya	Benjapolchai	Expert on Corporate Governance and Social Responsibility, The Stock Exchange of Thailand

8. Experienced Company Secretaries

Ms. Kobboon	Srichai	Company Secretary and Senior Vice President, Charoen Pokphand Foods Public Company Limited
Ms. Siribunchong	Uthayophas	Company Secretary and Executive Vice President, Corporate Office Division, Siam Commercial Bank Public Company Limited
Ms. Boonsiri	Charusiri	Former Company Secretary and Consultant, Banpu Public Company Limited

9. Knowledge Department, Thai Institute of Directors (Secretary of Working Committee)

Ms. Sirinun	Kittiwaytang	Executive Vice President - Knowledge (Research & Development and Curriculum & Facilitators)
Mr. Tanakorn	Pornratananukul	Assistant Vice President - Curriculum & Facilitators
Mr. Apilarp	Phaopinyo	CG Supervisor - Research & Development
Ms. Jaravee	Jeeramakorn	Senior CG Analyst - Curriculum & Facilitators

Section 1

Key Principles

Key Principles

1. The Board should have knowledge and understanding about information technology (IT) and data as well as recognize their significance in value creation and the achievement of enterprise success. It should also encourage the management to apply IT and data in operations and innovation development as well as business opportunity enhancement to support enterprise strategies, goals, and sustainable growth. (*See Guideline 1)*

2. The Board should set IT governance policy framework that aligns with enterprise strategies and goals. The policy framework should cover the application of IT and data for value creation, IT risk management, system and data security, and IT resource allocation and management. *(See Guideline 3.1)*

3. The Board should review Board Composition to ensure appropriateness in performing duties concerning the determination of IT governance direction. *(See Guideline 1.2)*

4. The Board should identify accountable persons and responsible persons for IT operations and ensure the organizational structure matches IT objectives and aligns with three lines of defense mechanism. *(See Guideline 3.1)*

5. The Board should ensure existence of participation, communication, and reporting processes that accommodate stakeholder participation and delivery of essential and necessary information that is accurate, complete, and in timely manner. *(See Guideline 3.1)*

6. The Board should determine IT strategy that supports and aligns with enterprise strategy by considering roles and priorities of IT as well as external and internal factors. *(See Guideline 3.2)*

7. The Board should ensure that data can effectively support value creation and enterprise strategy while stakeholders are taken into account by establishing processes to control and manage data life cycle, data quality, data security, and data privacy. *(See Guideline 3.2)*

8. The Board should ensure IT risk management is part of and in alignment with enterprise risk management. It should also set appropriate IT risk appetite that does not exceed the enterprise level. *(See Guideline 3.3)*

9. The Board should put in place cybersecurity plan that aligns with IT risks so that the enterprise can properly protect and tackle cyber threats. *(See Guideline 3.3)*

10. The Board should see that IT resource allocation and management align with enterprise strategy and requirements to ensure sufficient and appropriate resources for present and future operations. *(See Guideline 3.4)*

11. The Board should drive organizational culture that recognize the significance of IT and data, risk management, and system and data security to enterprise success and achievement of enterprise goals which will accommodate successful IT operations. *(See Guideline 3.5)*

12. The Board should regularly monitor and evaluate performance of IT operations. *(See Guideline 3.6)*

13. The Board should arrange IT audit to ensure IT governance and management are effective and comply with laws, regulations, and industry standard. *(See Guideline 3.6)*

14. The Board should regularly review IT governance and management policies to ensure alignment with enterprise strategy, effective operation framework, and achievement of value creation target. *(See Guideline 3.6)*

Section 2

Guidelines

Guideline 1 | Essence of IT governance

1.1 Definition and significance of IT governance

1.1.1 The application of IT involves with "data" and "information technology". The terms have meanings and linkages as follow:

- Data is something that communicates fact, either in its own form or through any process. Data could be in the form of text, number, statistics, or any other forms. (electronics or non-electronics) Business wise, data can be crucial element in driving enterprise when it is processed or transformed into information that can be used to achieve desirable objectives. For instance, it can be used to comprehend with enterprise operation efficiency, understand ways to respond to demand of customers and stakeholders, and develop innovation. Therefore, data is considered key IT assets of the enterprise. *(See Annex 1)*

- Information Technology (IT) is equipment or computer system that is capable to sort, compile, create, process, store, and distribute data or information. In business sense, IT allows enterprise to manage and utilize information in driving business toward its goals. It can also be used to enhance efficiencies of operations, production of goods or services, decision making, innovation development, and creation of business opportunities. IT also covers application, storage, network, infrastructure, and process relevant to data and information management of the enterprise.

1.1.2 IT governance means ensuring IT and data structure, policy, and management framework are in place so that IT and data application accommodates achievement of objectives and goals, effective IT risk management, appropriate IT security, compliance with laws, rules, and industry standard, trust among stakeholders, competitiveness and long-term growth.

1.1.3 To ensure IT application supports enterprise strategies and achievement of objectives and goals, the Board should stipulate IT governance and management framework that aligns with enterprise requirements and accommodates the application of IT to improve operation efficiency, develop innovation, and create business opportunity.

1.2 IT governance concept and composition

1.2.1 To ensure IT can help enterprise achieve strategic objectives and goals, the Board should see that IT governance and management framework covers key issues as follow:

1.2.1.1 Strategic Alignment

IT application should enhance enterprise potential in strategies implementation and achievement of objectives and goals. IT strategy should align with enterprise strategy, passing business goals to IT goals and transform into IT implementation plan that accommodates successful enterprise strategy.

1.2.1.2 Value Creation

IT investment, either in existing equipment or new ones, should respond to enterprise requirements and accommodate achievement of value creation goal within specific timeframe and appropriate budget. Value creation from IT and data application could mean competitive advantage, operation efficiency, ability to respond to demand of stakeholders, innovation, or new business opportunity.

1.2.1.3 Risk Optimization

IT application can bring about value creation opportunity but they also come with risks such as IT risk from unexpected event, benighted user or ill-intended person, and cyber threat. Such risks could affect operations, system and data security, confidence of stakeholders, and potential violation of law and regulation. Therefore, IT risk management should be included in enterprise risk management to preserve value created by IT application.

1.2.1.4 Resource Optimization

To ensure IT operations run effectively, there should be appropriate investment as well as resource allocation and management to enhance potential of strategic IT operations and respond to current and future enterprise demand. It applies to both technological resource (covering availability of equipment, system, and IT structure) and human resource. (covering knowledge, skill and competency of personnel in IT application)

1.2.1.5 Performance Measurement

To ensure positive progress of IT operations and achievement of goals, enterprise should have monitoring, performance measurement, and reporting processes of IT operations.

1.2.2 Beside aforementioned issues, the Board should also ensure enterprise has following success factors in IT application:

1.2.2.1 Ensure the Board, management, and personnel recognize the significance of IT in value creation and successful enterprise strategies. The Board should allot sufficient time to discuss with the management about strategic IT application regularly and stand ready to support and promote IT application to help achieving enterprise objectives and goals, develop innovation, and business opportunity.

1.2.2.2 Ensure the Board, management, and personnel understand IT opportunities and risks by having a process to educate them about IT development and trend in business operations, IT risks and cyber threats that should be aware of, as well as relevant laws, regulations and industry standard such as electronics transaction law, cybercrime law, cyber security law, personal data protection law, and foreign laws applicable to the enterprise. Such education process will equip them with perspective and initiative to apply IT in creating business opportunity and at the same time prevent potential risks.

1.2.2.3 Review Board Composition to ensure its appropriateness with IT governance. For example, the Board should consider the necessity to recruit director with knowledge or experience in IT, IT governance, or related industries to help the Board determine appropriate IT direction and IT governance. The Board should also ensure senior management have skills and competencies that make them fit to manage IT application of the enterprise.

1.2.2.4 Ensure the IT governance structure clearly indicates accountable persons and responsible persons to divide governance and operating roles which will provide clarity and lead to systematic performance monitoring and reporting.

1.2.2.5 Ensure the enterprise has organizational structure that matches with IT strategy and goals. The Board may consider allowing flexible operating structure and chain of command to accommodate the application of IT in business transformation, innovation development, or creation of business opportunity. The organizational structure should align with the Three Lines of Defense principle to ensure appropriate check and balance as well as division of duties. (See Annex 2)

1.2.2.6 Ensure availability of IT resources for the implementation of IT strategy to achieve pre-determined goals.

1.2.2.7 Ensure IT governance and management also cover stakeholders. Since successful IT application requires understanding, acceptance, and cooperation of stakeholders, it is essential to engage and communicate with stakeholders. It involves communication with internal personnel to recognize the need and create common understanding of IT strategy and goals as well as communication with external relevant parties to create understanding about IT and data management direction of the enterprise which will lead to harmonious implementation. It also includes reporting about IT policy and operations to key stakeholders.

1.2.2.8 Promote organizational culture that accommodates successful IT operations. Organizational culture that recognizes the significance of IT risk management and system and data security toward achievement of enterprise goals and success will help building awareness that will lead to desirable behaviors regarding IT and data application.

Guideline 2 | Board's role in IT governance

2.1 Responsibilities of the Board

As the top responsible group of persons for successful IT operations, the Board is tasked to perform the following roles:

2.1.1 Determine IT governance and management policy as well as IT strategy and goals that align with the enterprise.

2.1.2 Ensure governance structure is in place while IT operating process accommodates strategy and aligns with policy. The Board must also ensure communication with personnel at all levels including key stakeholders.

2.1.3 Oversee the management to ensure IT operations align with enterprise policy.

2.1.4 Support and promote IT application to create value and business opportunity of the enterprise and drive prudent IT organizational culture.

2.1.5 Monitor IT performance to see that it aligns with policy and effectively achieve pre-determined and agreed upon goals while complying with laws, rules, and industry standard.

2.2 Parties involving IT governance

Parties involving IT governance can be divided into two groups comprising internal related parties and external related parties. The Board should aware of roles of the two groups as follow:

Internal related parties including

2.2.1 Management

2.2.1.1 Determine IT strategy and goals together with the Board.

2.2.1.2 Responsible for IT operations to yield results in accordance with direction and policy stipulated and agreed upon with the Board.

2.2.1.3 Design operating process, prepare structure and secure IT resources for strategic implementation in accordance with the policy.

2.2.1.4 Communicate IT strategy, goals, and operating policy with personnel at all levels as well as key stakeholders.

2.2.1.5 Consider value creation and business opportunity from IT and drive positive IT organizational culture.

2.2.1.6 Monitor and evaluate IT performance in accordance with policy to report back to the Board.

2.2.2 Employee

2.2.2.1 Support the success of IT strategy by complying with policy and procedures.

2.2.2.2 Report policy implementation and issues detected to the management on a regular basis.

External related parties including

2.2.3 Service providers and parties conducting businesses with the enterprise and links with the enterprise system and data such as counterparties, trading partners, suppliers, IT service providers, and consultants.

2.2.3.1 Implement IT operations in compliance with enterprise policy, laws, regulations, and industry standard.

2.2.4 Key stakeholders such as customers, investors, regulators.

2.2.4.1 Acknowledge policy and implementation to ensure the enterprise has effective IT governance and management in compliance with laws, regulations, and industry standard.

Guideline 3 | IT governance direction

3.1 Determination of IT governance and management framework

3.1.1 The Board should stipulate IT governance and management policy framework in overseeing IT operations and the management to ensure alignment with enterprise strategy and goals. The policy should cover the application of IT and data to create value, manage IT risk, maintain system and data security, and effective IT resource allocation and management. *(See Annex 3)*

3.1.2 The Board should consider both external and internal factors relevant to business operations in order to determine appropriate IT governance and management framework for the enterprise.

- External factors – e.g. business environment, IT development and trend, IT risk development, laws, regulations, industry standard, and demand of stakeholders.

- Internal factors – e.g. enterprise strategy, objectives, and goals, alignment between IT application and current enterprise strategy, enterprise IT risk, detected problems concerning current IT application and operations, impact on stakeholders from current enterprise IT and data application, demand of internal stakeholders, and enterprise obligations.

3.1.3 The Board should consider indicating roles and priorities of IT in achieving business goals to provide direction in determining appropriate IT strategy, goals, and governance policy. It may consider using framework in the following example: *(See Annex 4)*

3.1.4 To assign IT governance responsibilities, the Board may consider assigning a committee to support the Board by stipulating clear roles and responsibilities in the Board Charter and charter of the committee assigned to perform IT governance roles. The consideration is subject to appropriate roles and priorities of IT to the enterprise, readiness of the enterprise, expertise of the Board, and industry practices. The Board may consider using the following guideline:

In case of defensive IT application	In case of offensive IT application
Assign IT governance roles to existing committees such as Risk Oversight Committee and Audit Committee.	Nominate specific committee such as IT Governance Committee to oversee IT governance issues.
Roles • Oversee IT strategy, investment, and operations to ensure alignment with enterprise strategy. • Stipulate IT and risk management policies. • Ensure compliance with relevant laws, regulations, and industry standard.	Roles • Oversee IT strategy, investment, and operations to ensure alignment with enterprise strategy. • Ensure IT and risk management policies as well as compliance with relevant laws, regulations, and industry standard. • Monitor IT trend to consider opportunity, risk, and recommendation about strategic implementation.
Composition • May have director with IT expertise as a member.	Composition • Have a director with IT expertise as a member. • May have a member of Audit Committee as a member.

3.1.5 To assign persons responsible for IT management and operations, the Board should ensure that senior management with appropriate knowledge and experience with understanding in IT management is nominated. The Board may specifically establish a senior IT executive position or assign competent senior executive with equivalent responsibilities. The consideration is subject to appropriate roles and priorities of IT to the enterprise, resource availability, and industry practices.

Roles of senior management	Designated positions
Responsible for IT management and operations to create value and support enterprise strategy.	• Chief Information Officer / Chief Technology Officer)
Responsible for data management and operations.	• Chief Data Officer or • Senior IT executive
Responsible for IT risk management and operations.	• Chief Risk Officer or • Chief Security Officer / Chief Information Security Officer)
Responsible for system and data management and security.	• Senior IT security executive or • Senior risk executive

3.1.6 The Board should stipulate appropriate IT authorization and principles to be used as guideline in IT decision-making framework in alignment with enterprise policy.

3.1.7 The Board should ensure effective communication and reporting processes to help persons responsible for IT governance, IT decision making, and IT operations receive accurate, complete, and timely information.

3.1.8 The Board should ensure the management indicates internal and external stakeholders relevant to IT and stipulate participation, communication, and reporting direction concerning IT governance in accordance with each stakeholder.

3.2 IT and data governance for value creation

3.2.1 To ensure IT investment is worthwhile, effectively respond to enterprise demand, and has appropriate cost, the Board and management should develop IT strategic plan that aligns with enterprise strategy and set clear IT goals.

3.2.2 The Board should ensure IT strategy and goals take into account internal and external factors such as IT roles and priorities to the enterprise *(See Guideline 3.1.3)*, IT system structure, assets, data, resources, and controls necessary to accommodate enterprise strategy. The Board should also take into account demand of stakeholders, both from business department and IT department, such as level of IT dependence in operations, IT application potential of personnel and enterprise.

3.2.3 The Board should encourage the management to consider potential business opportunity that may arise from the application of existing or emerging IT. The Board should also consider applying IT for innovation development to help the enterprise respond to opportunity or challenge occurred from changing business environment either via innovated product, process, or business model.

3.2.4 The Board should allot sufficient time to discuss IT strategy with the management regularly. The topic should be included as an agenda item of the Board meeting.

3.2.5 The Board should ensure IT strategy and goals are communicated with all personnel within the enterprise to create common understanding about the significance of IT to the enterprise success.

3.2.6 To ensure IT budget is spent effectively and aligns with enterprise strategy, the Board should prioritize IT investment which could be done be considering the significance of investment to enterprise strategies, urgency of usage, cost, expected benefits, and risks involving the investment etc.

3.2.7 The Board should ensure appropriate and well-balanced IT investment portfolio (projects, services, and assets) in various aspects including short- and long-term benefits, expected financial and non-financial benefits, investment with low and high risks. The Board should also evaluate and review investment proportion regularly to ensure IT expenditures create value as expected and support enterprise strategy.

3.2.8 The Board should regularly review IT strategy of the enterprise at least once a year to ensure it aligns with enterprise strategy and achieve value creation target.

3.2.9 To ensure the enterprise receive quality data that accommodates effective operations and create business opportunity, the Board should stipulate data governance and management policy that align with enterprise strategy and also take into account stakeholders who may be affected by enterprise data usage. Data management targets should cover data quality, data security, and data privacy.

3.2.10 The Board should see that data governance and management policy covers control and management processes throughout data life cycle to ensure data quality, data security, and data privacy. The process should have guidelines concerning data quality, data security and data privacy that comply with international standard, laws, regulations, and industry standard. *(See Annex 5)*

Examples of data management targets	
Data Quality	Data must be managed to ensure quality and ability to be used effectively by having the following characteristics: • Accuracy • Completeness • Consistency • Timeliness • Relevancy
Data Security and Data Privacy	Data must be managed to ensure security and privacy in accordance with CIA principle as follow: • Confidentiality • Integrity • Availability

3.3 IT risk management oversight

3.3.1 To ensure enterprise risk management covers IT risk, the Board should stipulate IT risk management policy that align with enterprise risk management policy and see that IT risk assessment is part of the environment being considered in enterprise strategic decision making.

3.3.2 In policy drafting, the Board should ensure the management has effective IT risk management process comprising risk identification, determination of risk appetite and risk tolerance, risk assessment (assess risk likelihood and risk impact of identified risks by risk map creation), create risk profile from risk assessment result to compare and prioritize key risks to manage, and manage risks in accordance to risk appetite.

3.3.3 The Board should see that management comprehensively identify internal and external risks by considering IT risk scenarios and IT risk factors such as IT structure of the enterprise, rules and regulations, IT risk development and trend. The Board should also explore and analyze IT risk factors and events regularly to identify potential new risk.

3.3.4 The Board should control IT risk appetite and IT risk tolerance by communicating with personnel so that they clearly aware of risk appetite and risk tolerance, manage identified and prioritized risks in accordance with risk appetite, and review IT risk appetite annually or when there is any significant change or IT and cyber incident.

3.3.5 The Board should see that management prepares cybersecurity plan in alignment with enterprise IT risk and has guideline in accordance with international standard to help the enterprise prevent, detect, and tackle threat as well as effective loss recovery. *(See Annex 6)*

3.3.6 The Board should see that management stipulate hierarchical reporting when there is any substantial change in IT risk to ensure appropriate reporting to the management and able to respond to change in timely manner. All personnel should also be encouraged to report IT risk issue to department relevant to risk management.

3.3.7 The Board should put in place a mechanism to ensure service providers and those conducting business with the enterprise have IT risk management as well as system and data security controls that align with enterprise policy, laws, regulations, and industry standard. It may also examine system and data security operations of service providers and those conducting business with the enterprise by clearly stipulating as requirement in contracts or business agreements.

3.3.8 The Board should ensure the enterprise has an internal unit responsible for system and data security controls in accordance with relevant regulations or industry standard. It should also see that such controls cover assessment of IT law compliance.

3.3.9 The Board should ensure management arrange training on IT risk, IT security and privacy, relevant laws and regulations, and cyber exercise for the Board, management, staffs, as well as service providers and those conducting business with the enterprise which connect to its system and data. The training is meant to provide sufficient knowledge and understanding to implement controls over IT risks. The frequency of training and exercise should align with IT risk level of the enterprise.

3.3.10 The Board should ensure management stipulate and select appropriate IT risk indicators to monitor current and potential risks. The indicators should be well-balanced between risk performance indicators and enterprise capability indicator in preventing risk incident while indicating linkage between risk incident and causes.

3.4 IT resource allocation and management oversight

3.4.1 To ensure sufficient and appropriate resources for IT operations to accommodate enterprise strategy and achievement of current and future goals, the Board should stipulate IT resource allocation and management policy that covers financial, technology, and human resource aspects.

3.4.2 In policy drafting, the Board should consider enterprise strategy as well as current and future resource requirements, both overall and IT aspects, in order to evaluate and determine alternatives, sources, and ways to develop IT potential that can appropriately accommodate current and future demand of the enterprise.

3.4.3 The Board should stipulate criteria for resource allocation and management to ensure IT operations have sufficient resources and potential to accommodate achievement of enterprise goals in prioritized orders and within appropriate budget. For instance, the Board may set criteria for IT plan prioritization by considering from alignment with strategies, indication of sources for certain IT services, and indication of financial scope for each alternative.

3.4.4 The Board should also stipulate criteria for IT resource protection that include prevention of damage in IT assets and preservation of skillful and competent personnel.

3.4.5 The Board should ensure IT resource allocation and management plan align with enterprise financial and human resource allocation and management plan.

3.4.6 The Board should see that management track IT resource performance to ensure achievement of targets such as efficiency of IT system and equipment, performance of IT personnel, and consider ways to improve in case IT resource performance fail to achieve target.

3.5 Promotion of IT organizational culture

3.5.1 To promote organizational culture that accommodates successful IT application, the Board should stipulate characteristics of expected culture and ensure the characteristics are clearly communicated along other IT policy and targets with personnel at all levels to create common understanding about desirable IT culture and guidelines. Such understanding will eventually turn into knowledge, believe, and attitude that will lead to IT behaviors and decision in alignment with the organizational culture targets.

Example of desirable characteristics of IT organizational culture
• Personnel understand the significance of IT in achieving enterprise goals and recognize the need for cooperation of all units to make IT application align with stipulated direction, not just being "IT department issue".
• Personnel understand type of IT risks that the enterprise is facing or may face and recognize own's roles in preventing risks from affecting the enterprise and stakeholders. They use IT and data prudently in accordance with guidelines and report to relevant parties right away when detecting issue concerning IT risk.
• Personnel recognize the significance of data toward enterprise success and the significance of system and data security and privacy to preserve the quality of data and right of data owner. They comply with guidelines in data usage to prevent data leakage, damage, or being used unethically and unlawfully.

3.5.2 The Board should encourage management to set up mechanism to support IT behaviors that will lead to desirable culture. It may indicate responsibilities in data security and data privacy in the Code of Conduct, grant honors or awards for creative initiation of IT usage in operations or those being role model in handling IT risks, stipulate disciplinary actions against IT behaviors that clearly violate the guidelines.

3.5.3 The Board should see that management conduct training to develop IT knowledge and skills for personnel at all levels including the Board, management, and staffs. IT training may be included in human resource development plan to provide direction in building appropriate knowledge, recognition, and skills for both existing and new personnel.

3.5.4 To build confidence and compliance of personnel, the Board should set tone at the top on IT culture by being role model and participate in IT activities. The Board may publish IT and data application handbook for personnel, mention the significance of IT culture in statements, and participate in IT training and cyber-attack exercise etc.

3.6 IT monitoring and performance evaluation

3.6.1 The Board should stipulate and agree with the management on IT monitoring and performance evaluation process as well as performance indicators. It should also ensure IT governance and management policy, targets, and performance evaluation in each topic are communicated with relevant personnel at all levels to create common understanding.

3.6.2 In IT monitoring and performance evaluation, the Board should ensure both operations and outcome are being evaluated so that the Board can monitor progress and achievement of targets. Performance indicators should cover both financial and non-financial aspects. They comprise of leading indicators that depict results occurred during IT implementation process which reflect efficiency in achieving targets and lagging indicators that demonstrate achievement of IT operations. *(See Annex 7)*

3.6.3 The Board should stipulate reporting timeframe of IT operations in accordance with existing policy. The reporting timeframe should align with the significance or urgency of operations in particular topic to the enterprise. It could be set quarterly, annually, or when any event with significant impact emerge. For instance, finance business may require cyber threat and cyber security reporting every quarter.

3.6.4 The Board should communicate with the management about appropriate form of IT progress and performance report, which will help the Board receive key information for effective decision making. The report should present overall operations of each aspect in easy-to-understand format, use concise wording, avoid "technical terms", demonstrate relationship between IT targets and operations with enterprise targets and operations, and indicate realistic problems and key obstacles.

3.6.5 The Board should monitor and evaluate performance of persons assigned to oversee and manage IT issues in accordance with predetermined and agreed upon targets and performance evaluation process. It should ensure that IT achievement is one factor in considering compensation of the assigned senior management.

3.6.6 The Board should ensure internal audit unit and external independent auditor conduct IT audit. The audit scope should align with the significance and risks of IT to the enterprise. The Audit Committee should review audit scope at least once a year as well as when there is any change or event that yield material impact.

3.6.7 The Board should monitor that issues detected from the audit process are used to improve IT governance and management policy. It should also ensure that audit results are sent to regulators in accordance with relevant laws, regulations, or industry standard.

3.6.8 The Board should reach agreement with the management to immediately report any problem or flaw detected in IT process that could yield material impact on operations. It should also identify responsible persons and set clear direction in fixing problem.

3.6.9 The Board should regularly review IT governance and management issues of the enterprise at least once a year as well as when there is any change or event that yield material impact to ensure effective operations in alignment with enterprise strategy and achievement of value creation target.

3.6.10 The Board should ensure information concerning IT governance policy and policy implementation outcome are reported to external stakeholders in compliance with relevant laws or regulations.

Annex

Annex 1 Key enterprise data and information

Key enterprise data and information usually include

- **Personal Data** includes personal data of past and present customers, employees, contracted personnel, and stakeholders.
- **Financial Data** such as financial statements, sales, and annual results prior to public announcement.
- **Business Information** such as in-depth information about merger and acquisition, business contracts, business deals, information concerning legal cases and law suits.
- **Intellectual Property** such as model or formula that is considered trade secret, operation system developed by the enterprise, patent.

The Personal Data Protection Act (PDPA) defines personal data in section 6 as follow:

> "Personal data" refers to any information relating to a person, which enables the identification of such person, whether directly or indirectly, but not including information of the deceased person in particular.

"Person" hereby refers to a natural living person but excludes juristic person such as company, association, foundation, or any other organization. Person indicated by personal data is called data subject.

The enterprise should manage personal data with discretion should its operations involve receiving, sending, and using personal data in foreign territory because personal data definition and regulations may vary from country to country. For instance, personal data under the definition of EU General Data Protection Regulation does not cover deceased persons but the legislation allows EU member states to apply their own respective laws in this regard. Meanwhile, personal data under Singapore Personal Data Protection Act cover data of those who passed away up to 10 years.

Annex 2 Three Lines of Defense

First Line of Defense: Unit that performs IT operations

This includes personnel or unit conducting IT operations such as IT unit, business units that use IT system, data manager, units that are data owners etc.

Roles of personnel or unit in the first line of defense are to run IT operations under scope of responsibilities in accordance with policy and control guideline as well as evaluate and mitigate IT risks.

Second Line of Defense: Unit that manage IT risks and oversee compliance

This includes personnel or unit that oversee compliance with IT laws and regulations such as risk management unit, IT risk management unit, and compliance unit etc.

Roles of personnel or unit in this line may include

- *Risk management unit* determines IT risk management framework and process, conduct risk assessment in accordance with the framework, monitor IT risk and review relevant controls of units in the first line of defense and of the enterprise to ensure they are at acceptable levels.

- *Compliance unit* determines monitoring framework and process, monitor IT governance and management process to ensure they align with the policy, monitor adequacy and appropriateness of controls and compliance with relevant laws and regulations.

Third Line of Defense: Unit that conducts IT audit

This includes personnel or unit that audit operations of units in the first and second lines of defense as well as other relevant units (such as external IT service providers). They may be internal audit unit or external independent auditor etc.

Roles of personnel or unit in this line are to conduct audit to ensure compliance with policy, laws, regulations, and relevant IT standard.

Annex 3 Example of IT governance and management policy drafting

IT governance and management policy of each enterprise may vary in details but it should fundamentally cover the following topics:

Objectives

Indicate reasons for the drafting of IT governance and management policy and how this policy will accommodate achievement of enterprise strategy, goals, and objectives.

Enforcement scope

Indicate persons, group of persons, and units that must comply with this policy including subsidiaries, service providers, and those conducting businesses with linkage to system and data of the enterprise.

Definition

Indicate definition of terms used in the policy so that relevant parties have common understanding and can comply accordingly.

Structure, roles, duties, and responsibilities.

Indicate governance structure and persons, group of persons, or units related to policy implementation as well as roles and responsibilities of relevant persons.

Policy

Indicate policy and guidelines in

- IT strategy of the enterprise
- Data management
- IT risk management
- System and data security
- IT resource allocation and management

(See details of issues to consider in the drafting of each policy aspect in relevant guidelines.)

Reporting

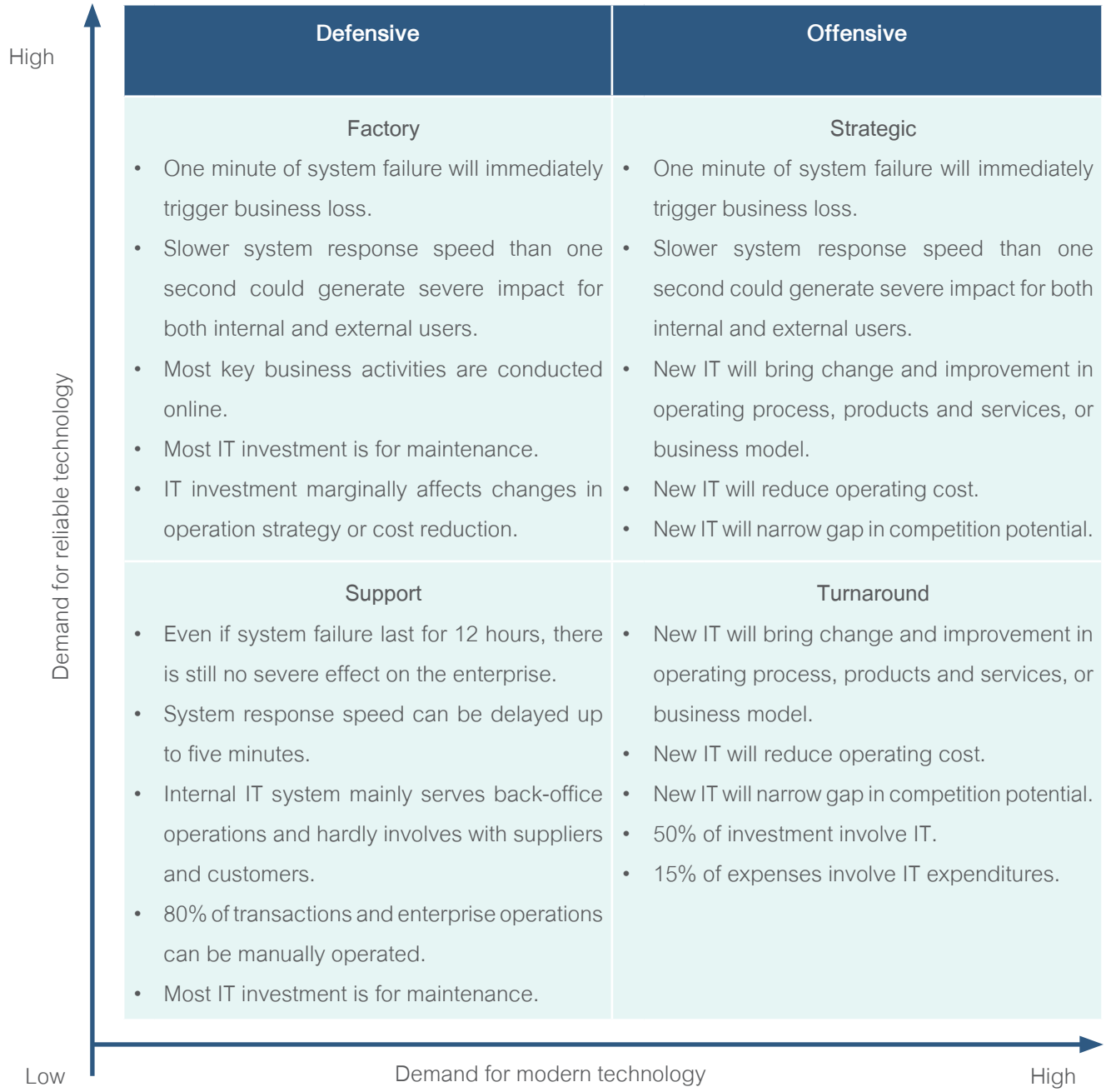
Indicate guidelines in reporting policy implementation to the Board and stakeholders or regulators in accordance with regulations and industry standard.

Policy review

Indicate person responsible for reviewing and approving policy as well as policy review frequency.

Annex 4 Framework for considering roles and significance of IT to enterprise

From example of framework presented in Guideline 3.1.3, the Board may use details indicated in the table below for further consideration:



Defensive	Offensive
Factory • One minute of system failure will immediately trigger business loss. • Slower system response speed than one second could generate severe impact for both internal and external users. • Most key business activities are conducted online. • Most IT investment is for maintenance. • IT investment marginally affects changes in operation strategy or cost reduction.	**Strategic** • One minute of system failure will immediately trigger business loss. • Slower system response speed than one second could generate severe impact for both internal and external users. • New IT will bring change and improvement in operating process, products and services, or business model. • New IT will reduce operating cost. • New IT will narrow gap in competition potential.
Support • Even if system failure last for 12 hours, there is still no severe effect on the enterprise. • System response speed can be delayed up to five minutes. • Internal IT system mainly serves back-office operations and hardly involves with suppliers and customers. • 80% of transactions and enterprise operations can be manually operated. • Most IT investment is for maintenance.	**Turnaround** • New IT will bring change and improvement in operating process, products and services, or business model. • New IT will reduce operating cost. • New IT will narrow gap in competition potential. • 50% of investment involve IT. • 15% of expenses involve IT expenditures.

Annex 5 Key issues in control and management process throughout data life cycle

- **Conduct diagram that demonstrate data linkage throughout data life cycle.** The cycle may consist of processes to create, store, use, publish, archive, and destroy data to depict the relationship between data, activities, and engaged parties (both internal and external) so as to manage data in alignment with data complexity.

- **Clearly indicate data usage objectives.** This will accommodate processes throughout data life cycle to achieve objectives and store only necessary data by taking into account the rights of data owners, contacts, business deals, laws, regulations, and relevant industry standard.

- **Conduct metadata.** This will accommodate users in data sorting and can be used for the preparation of data catalog for effective data storage and retrieval.

- **Data Classification.** Data should be classified in accordance with significance and sensitivity as well as risk levels and impact on the enterprise. Levels of data confidentiality in each operation cycle must be taken into account to ensure data security at all time.

- **Set guideline for access control.** Rights to access data should be regularly reviewed to prevent ineligible person from accessing, using, or fixing data.

- **Set data quality criteria** and operating guideline concerning data to ensure data is trustworthy and can be used effectively. For instance, there should be a mechanism to detect data with poor quality as well as data backup in accordance with data classification that make it available at all time.

- **Have log file** such as in data processing, usage, and exchange to allow possible backtrack.

- **Set guideline for data destruction when it is no longer used** or being stored beyond specified period. A guideline should also be set for destruction of personal data upon request by data owners in alignment with applicable laws and regulations.

Annex 6 Cybersecurity operation framework

Procedures	Example of key issues
1. Identify key elements in cybersecurity.	• Type of risks and cyberthreats. • Key IT assets that need to be protected. • List of service providers, persons conducting businesses with the enterprise, and external parties with linkage to enterprise system and data or accessible to enterprise IT assets. • Responsible persons (such as senior management in IT security), stakeholders, process, system, and required resources for operations.
2. Set guideline to Protect key IT system and assets.	• Manage accessibility to IT system and assets, both tangible and digital, in alignment with relevant risk and significance of such system and assets. • Install and ensure up to date anti-virus and malware protection programs in the system and equipment. • Guideline to maintain data security throughout life cycle in alignment with risk and significance of data type. *(See Annex 4)* • Training program to educate personnel about IT security.
3. Set guideline to Detect threat or irregularity.	• Establish Security Operations Centre. • Put in place mechanism to monitor and detect threat and irregularity in system, network, and equipment.
4. Stipulate clear measures to Respond to incident.	• Set criteria for severity of incident. • Indicate roles of departments and persons involving in each level of severity. • Indicate stakeholders that need to be communicated, both internal and external, when incident occurs and Board reporting guideline. • Stipulate that cyber drill, penetration testing, and vulnerability assessment are conducted by external expert at least once a year. • Appropriately insure against cyber events.

Procedures	Example of key issues
5. Stipulate measures to recover damaged system or assets in accordance with their significance to the enterprise	• Have back up data and system. • Set system recovery period. • Set acceptable disruption period. • Have business continuity plan. • Have plans to learn and improve IT security from incident.

Annex 7 Example of IT performance indicators

Operational issues	Indicators
Using IT and data for value creation	• Percentage of the company's strategic targets supported by IT strategic targets. • Percentage of IT investment that achieved benefits as expected or beyond expectations. • Number of key business operations that benefited from improvement of IT structure and operating system. • Number of new business opportunity that actually create value from IT. • Number of projects/innovations derived from approved IT initiative. • Percentage of senior management that satisfy with the use of innovation and IT application to improve business operations. • Proportion of data that met data quality criteria. • Level of user satisfaction in data quality and availability. • Number of times that problem concerning confidentiality, accuracy, and availability of system and data damage financial, business continuity, or reputation of the enterprise.
IT risk management	• Consistency in risk review. • Alignment between IT risk and enterprise risk. • Number of undesirable IT risk or cyberthreat incident that was not indicate in risk assessment. • Percentage of doubtful IT access or contradict with accessibility level. • Percentage of personnel (Board / management / staffs) victimized by cyberattack. • Number of times that legal issues / policy violation arise from contracts or agreements made with IT service provider.

Operational issues	Indicators
IT resource allocation and management	• Number of projects completed within specified timeframe and budget. • Proportion of IT personnel with business knowledge and competency / business personnel with IT knowledge and competency.
IT Organizational culture	• Proportion of personnel attended IT training as planned. • Number of times that IT issues arise from inadequate knowledge of personnel. • Number of reported incidents concerning IT risk / system and data security / personnel data privacy.

References

1. **20 Questions Directors Should Ask about Cybersecurity,** Chartered Professional Accountants Canada (CPA), 2019
2. **Board Briefing on IT Governance,** IT Governance Institute, 2003
3. **COBIT 2019 Framework,** ISACA, 2018
4. **Data and Privacy Governance,** Australian Institute of Company Directors (AICD), 2020
5. **DGI Data Governance Framework,** The Data Governance Institute, 2018
6. **Framework for Improving Critical Infrastructure Cybersecurity,** National Institute of Standards and Technology (NIST), 2018
7. **General Data Protection Regulation (EU) 2016/679**
8. **Information Technology and the Board of Directors,** Harvard Business Review (October 2005), 2005
9. **Information Technology Governance,** Australian Institute of Company Directors (AICD), 2020
10. **Performance Measurement Metrics for IT Governance,** ISACA Journal (Volume 6), 2016
11. **Thailand Data Protection Guidelines 3.0,**Research Center for Law and Development, Faculty of Law, Chulalongkorn University, 2021
12. **Data Governance Framework,** Government Development Agency, 2561
13. **IT risk management,** Office of the Securities and Exchange Commission (SEC), 2019
14. **IT governance and risk management guideline,** Office of the Securities and Exchange Commission (SEC), 2019
15. **Bank of Thailand policy on data governance,** Bank of Thailand, 2021
16. **BOT announcement at SNC 1/2564 on IT risk governance under payment system law**
17. **SEC announcement at NP 3/2559 on IT system guideline.**
18. **Cybersecurity Act B.E. 2562**
19. **Personal Data Protection Act B.E. 2562**
20. **Corporate governance code for listed companies,** Office of the Securities and Exchange Commission (SEC), 2017

Thai Institute of Directors

Thai Institute of Directors Association

Capital Market Academy Building 2, 2/9 Moo 4 Northpark Project,
Vibhavadi - Rangsit Road, Thung SongHong, Laksi, Bangkok
10210, Thailand

Phone : (66) 2955 1155 Fax: (66) 2955 1156 - 57 www.thai-iod.com