Declaration no. 009/2024

IT GOVERNANCE POLICY
OF
GMO-Z COM SECURITIES (THAILAND) PUBLIC COMPANY LIMITED

Information Technology Governance Policy

GMO-Z COM SECURITIES (THAILAND) PUBLIC COMPANY LIMITED

Table of contents

1. Purpose

This document establishes the principles and standards for the governance of Information Technology (IT) within GMO-Z com Securities (Thailand) Public Company Limited (Company).

IT Governance is the accountability of the Company Board who delegates this task to the Company Risk Committee. The design and management of the IT governance system is delegated to the Head of Information Technology.

2. IT Governance

IT governance is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives.

The objective of IT governance is to direct IT endeavors, to ensure that IT's performance meets the following objectives:

- Alignment of IT with the enterprise and realization of the promised benefits
- Use of IT to enable the enterprise by exploiting opportunities and maximizing benefits
- Responsible use of IT resources
- Appropriate management of IT-related risks

In summary, IT governance ensures that IT goals are met, and IT risks are mitigated such that IT delivers value to sustain and grow the enterprise. IT governance drives strategic alignment between IT and the business and must judiciously measure performance.

3. Key Principles

The IT Governance Policy is guided by the governance principles of COBIT5, aligned to the company's IT governance baseline and complies with Securities and Exchange Commission (SEC) legislation.

Company has adopted 7 Governance baseline principles for the development and implementation of an information technology governance framework. These principles incorporate standards included in SEC notifications, COBIT, ITIL and ISO and starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives.

The 7 Company Governance baseline principles are:

1. **Business alignment and enablement** focuses on ensuring the linkage of business and IT plans, defining, maintaining and validating the IT value proposition, and aligning IT operations with enterprise operations.
2. **Operations Performance** is about ensuring IT is capacitated with the right people who are developed and empowered and ensuring optimal IT processes and measurements are deployed.
3. **Sourcing** requires responsible and adequate procurement of IT hardware and software and the correct selection and vetting of IT partners and suppliers.
4. **Supplier performance management** outlines practices regarding the implementation and monitoring of service level agreements and commercial agreements
5. **Business Continuity / Disaster Recovery** details requirements and practices regarding the processes to ensure IT impacted disruptions
6. **Security** promotes our views regarding data privacy, cybersecurity and user access
7. **Compliance** sets out guidance in respect of internal monitoring and external assurance

4. Information Technology Governance Framework

The governance framework in the use of IT within Company is defined as follows:

- The Company Board has assumed responsibility of IT governance and, as such, has placed it on the Company Risk Committee's Charter ensuring promotion of an ethical IT governance culture and awareness. The Company Governance baseline principles have been adopted to ensure that IT internal controls are adequate. Independent assurance on the effectiveness of the IT internal controls are provided by the Internal and External Auditors.
- The activities and functions of the IT strategy are aligned to the business strategy

and opportunities to improve the use of IT within Company are identified and exploited by the Board.

- The Company Board has delegated to management the responsibility for the implementation of IT governance.
- The optimal investment is made in IT, costs are managed and the return on investment is measured by the relevant divisional boards and oversight committees. Where applicable synergies between IT initiatives are enabled and IT choices are in the best interest of the organization.
- IT risks are identified and adequately addressed in line with Company Risk Management framework. Company ensures that it has adequate business resilience arrangements in place for disaster recovery and assurance has been provided to the Board.
- IT resources are sourced optimally and legitimately, keeping core capabilities in-house.
- Processes and procedures are in place to ensure that Company's IT Assets are managed, maintained, replaced and disposed effectively and in accordance to applicable divisional IT policies.
- Infrastructure, systems and policies are in place for the management of information which includes information security and information privacy.
- The audit committee considers IT as it relates to financial reporting and the going concern of the company by regular and risk-based audit coverage.
- IT use is sustainable with respect to the environment.

5. Responsibilities

Company's board carries out its governance duties through various committees that oversee the governance of IT. IT Governance is applied at three levels: Strategic, Tactical, and Operational. For the purposes of this document, the key committees that oversee IT Governance are:

- The Company Board of Directors, the Company Risk Committee, and the Company Audit Committee at a strategic level
- Management Team, the Company IT forum, and divisional IT forums at a tactical level
- The IT steering Committees and project committees at the operational level.

6. Implementation of Policy

The IT governance policy will be rolled out across the Company. It needs to be embraced by Company and its related processes filtered into the daily IT operations and the way we do business.

Appendix A – IT Strategy

One factor to drive the company profit is to reduce the cost. IT plays an important role to the business by not only generating revenue but also optimizing cost as well. Company's IT strategy is summarized as follows.

1. **Automation** where possible to optimize manual tasks. Repetitive operations should be replaced with automated scripts so that we can utilize staffs in more challenging assignments.
2. **Application Service Provider (ASP) Model** is company's preferred choice for vendors. Infrastructure and maintenance cost should be on their side. Pay per use is preferable.
3. **Growing Together Model** is company's preferred choice for partnerships. If their service is so good that our customers are actively using it, we are not reluctant to share certain amount of commission to them. However, the operation cost should be on their side as per ASP model.

Appendix B – BOD Report

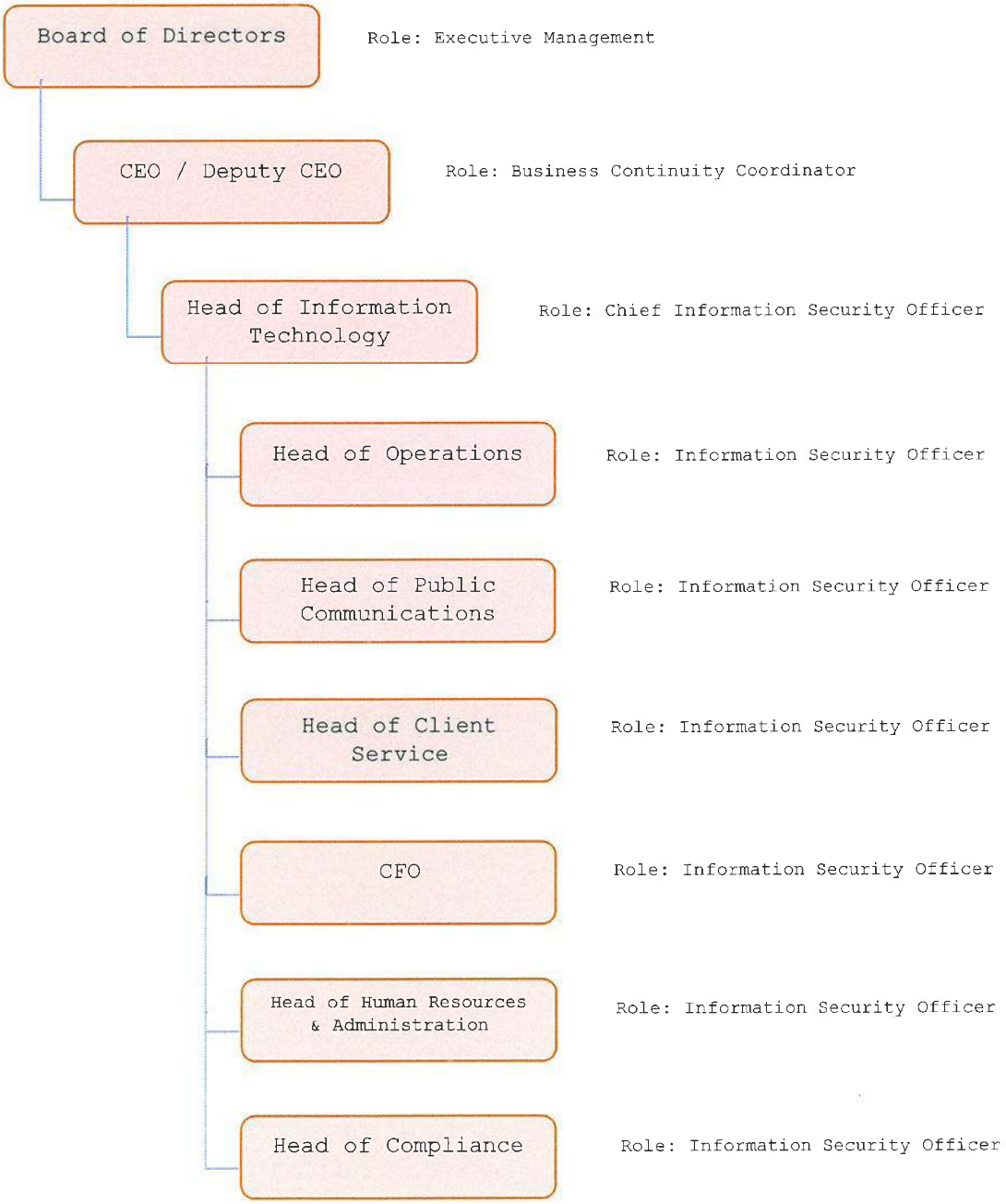
As SEC specified that reporting on the conformance of the information technology governance policy shall be provided to the board of directors of the intermediary at least once a year. And in case of the occurrence of any event which may significantly affect the conformance of such policy, the board of directors of the intermediary shall be informed without delay.

Therefore, the company shall have in place information technology governance to establish procedures of preparation, monitoring, and supervision of reporting to ensure that reporting is complete, accurate, timely, and it shall be provided to the board of directors of the intermediary at least once a year.

Report should include the following significant topics as minimum:

1. Activities relating to the approach of risk management or allocation and management of IT resources, for example, a summary of the risk management or allocation of IT resources in a year, etc.
2. Any progress of the IT project (if any).
3. Any compliance with the regulations, rules or agreement made with external parties and internal parties, for example, submission of incident reports to the SEC Office upon an occurrence of an event that affects the IT systems or monitoring of the service provider to ensure that its operation is in accordance with the terms specified in the service level agreement.
4. Effectiveness for adopting new IT system in business operation. For example, monitoring of the operating time after the technology is applied to improve operating procedures and the accordance of the adopted IT system with the business objectives.
5. Issues and obstacles.

Appendix C – Information Security Committee



Information Security Committee Roles and Responsibilities

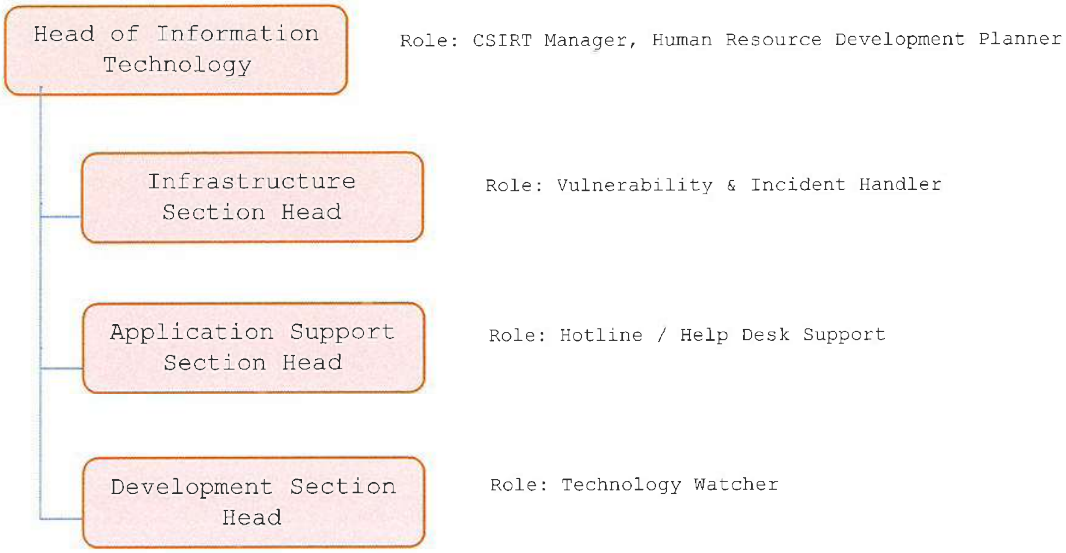
- **Executive Management** is a forum for executive consideration of companywide IT strategy. Specific oversight responsibilities related to implementation of the Information Security Policy include the following:
    a. Reviewing and recommending strategies to implement the Information Security Policy.
    b. Analyzing the business impact of proposed strategies on the company.
    c. Approving proposed strategies.
    d. Serving as a champion for accepted strategies within respective business units.
    e. Overseeing the review and approval of Information Security Policy exceptions.

- **Business Continuity Coordinator** is assigned the overall responsibility for co-coordination of the recovery planning program.
    a. Working closely with critical business units to understand their processes, identify risks, and provide solutions to help manage and minimize those risks.
    b. Reviewing the development and maintenance of business continuity plans done by CISO.
    c. Once an incident occurs, the BCC must communicate, manage, and control activities associated with damage assessments and the recovery of critical business functions.

- **Chief Information Security Officer** is Head of IT of the company who oversees the company's information security program. Responsibilities of the Chief Information Security Officer include the following:
    a. Developing and implementing a companywide information security program.
    b. Documenting and disseminating information security policies and procedures.
    c. Coordinating the development and implementation of a companywide information security training and awareness program.
    d. Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of Customer and Company Data.

- **Information Security Officer** serves as a resource regarding matters of information security and reports the status of ongoing information security activities to the Chief Information Security Officer.
    a. Ensuring appropriate controls are in place for the security of information assets.
    b. Safeguarding information by seeing that security risks are identified, assessed, and accurately reported.
    c. Ensuring local procedures and activities comply with all regulatory requirements and internal policies, procedures, guidelines and standards.
    d. Monitoring the security management status of each part and report monitoring results to the information security committee.

Appendix D – Computer Security Incident Response Team (CSIRT)



CSIRT Roles and Responsibilities

- **CSIRT Manager** is responsible for organizing and directing the CSIRT. Typical duties center on managing incident response processes.
    a. Overseeing and prioritizing actions during the detection, analysis, and containment of an incident.
    b. Conveying the special requirements of high severity incidents to the rest of the company.
    c. Managing policies and procedure updates to deal with future incidents.

- **Human Resource Development Planner** provides information security learning plan for all staffs to ensure they are aware and have latest knowledge of information security.
    a. Working closely HR business units to design and create the information security learning plan.
    b. Regularly evaluate staff's information security awareness.

- **Vulnerability & Incident Handler** is designated to coordinate responses to IT security incidents. All information about incidents must be passed through this person before it leaves the team and is passed on to the organization or the public.
    a. Working directly with the affected system or network to research the time, location, and details of an incident.
    b. Filtering out false positives and watch for potential intrusions (Triage Analysis).
    c. Recovering key artifacts and maintaining integrity of evidence to ensure a forensically sound investigation (Forensic Analysis).

- **Hotline / Help Desk Support** provides fast and useful technical assistance on computer security.
    a. Serving as the first point of contact for staffs seeking computer security assistance over the phone or email.
    b. Directing unresolved issues to the Vulnerability & Incident Handler.
    c. Recording incidents and problems and their resolution in logs.

- **Technology Watcher** complements the CSIRT by providing threat intelligence and context for an incident.
    a. Searching the internet and identifying intelligence that may have been reported externally.
    b. Analyzing the collected information and report it to the meeting.
    c. Building and maintaining a database of internal intelligence.

Appendix E – IT Resource Allocation and Management Policy

Management Team are accountable for assigning a person, for example, Head of IT, who will be responsible for IT resource allocation and management which should be consistent with the corporate strategic objectives to achieve the goals according to the missions, strategies, policies, and operational plans.

Company's IT resource allocation and management policy is summarized as follows.

1. **Prioritization**
   a. Establish criteria and factors for determining priority of IT project roadmap, for example, suitability in accordance with the company's strategic plan, impact to business operations, urgency of use.
2. **Budget Planning**
   a. Prepare and approve information technology budgets which must be in line with company's budget plan and corporate strategic plan.
3. **Human Resourcing**
   a. Ensure the sufficiency of skilled human resources for information technology tasks, for example, provide trainings or skill development plan for IT staffs, outsourcing IT tasks.
4. **Risk Management**
   a. Identify and manage major risks that could occur in the event that sufficient resources are not allocated to IT operations or projects, for example, in the case of key IT staff resigning, insufficient budget, demand exceeding the capacity planed.

Revision History
(Version approved by Board of Directors Meeting)

Date	Declaration No.	Status	Details of Revision
14 August 2018	003/2018	Cancelled	- Newly implemented
12 March 2020	002/2020	Cancelled	- Revise per audit feedback
26 January 2021	002/2021	Cancelled	- Revise Appendix C by changing Head of Finance to CFO.
27 July 2021	009/2021	Cancelled	- Revised following IVL audit feedback.
25 March 2022	013/2022	Cancelled	- Changing Company name
23 March 2023	014/2023	Cancelled	- Revised the part that related to Executive Committee due to the dissolution of Executive Committee by the resolution of BODs Meeting No.2/2023.
30 May 2024	009/2024	Effective	- Revised the detail of "Appendix B – BOD Report" follow SEC regulation.

Effective from 30 May 2024 onwards