Thai Institute of Directors

Guideline on Board's Oversight Role in Risk Management

Content

Introduction

It is rather tough to run business nowadays amid uncertain environment and unpredictable disruption such as technological change, pandemic, natural disaster, management change, competition, new legislation, and trade barrier.

Companies that may achieve sustainable growth in this new era must have solid fundamental while being flexible to changes in strategies and administration techniques under applicable laws and regulations. They must also be equipped with knowledgeable Board and management, who can lead the company and respond well to expectations from various stakeholders. To oversee risk management, the Board must comprehend with existing risk management process from risk indication, assessment, management, and monitoring to ensure that the management prudently assessed risks and managed them well so that the company is not exposed to any risk too big to handle. However, the Board may be obliged with other commitments that make it unable to adequately oversee risk management. In such case, the Board may nominate Risk Management Committee to relieve its burden in this aspect and regularly report any progress to the Board.

In this regard, the Thai Institute of Directors (IOD) has prepared the Guideline on Board's Oversight Role in Risk Management to help the Board recognize the significance, composition, roles and duties, and how to make risk management system effective to ensure viability and continuous growth.

• Thai Institute of Directors (IOD) •

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 apply GRC (Governance, Risk and Compliance) integration concept in governing organization to accommodate advancement and sustainability. *(See Guideline 1)*

2. Risk management is key component of GRC integration because it makes the organization recognize and able to handle potential events that could have adverse effect in achieving strategies, objectives, and expectations of stakeholders. *(See Guideline 1)*

3. The Board should take parts in determining and monitoring the implementation of strategies and determine risk appetite in alignment with the implementation of such strategies. In doing so, the Board should hold discussion with senior management. *(See Guideline 1)*

4. The Board should turn risk management system and internal control into normal daily work process, not making them separate and temporary activities. *(See Guideline 1)*

5. The Board should ensure that risk management is integrated and aligned with sustainability management system, covering Environmental, Social and Governance (ESG) aspects. *(See Guideline 1)*

6. The Board may oversee risk management by itself or assign Risk Management Committee to take charge in governing the company's risk management efficiency and report to the Board. *(See Guideline 2)*

7. Structure of the Risk Management Committee of each company is subject to size, complexity, relevant legislations. It may as well be the same as other committees, such as Audit Committee, or it could be set up separately. *(See Guideline 2)*

8. The Board should assign roles, duties, and responsibilities to Risk Management Committee through written Charter. Key roles of the committee should be to support the Board in performing its duties by ensuring that the organization's risk management and internal controls are efficient, sufficient, and appropriate. *(See Guideline 2.2)*

9 The Board should stipulate that Risk Management meet at least twice a year and regularly report meeting results to the Board so that the Board acknowledge progress, key risk management issues, and recommendations for necessary decision. *(See Guideline 2)*

10 Performance of the Risk Management Committee should be evaluated at least once a year and performance report should be presented to the Board annually. *(See Guideline 2)*

Section 2

Guidelines

Guideline 1 Roles, duties, and responsibilities of Risk Management Committee

1.1 Key governance principles under GRC concept

1.1.1 The Board is responsible to govern the organization towards sustainability and meet expectations of stakeholders. Therefore, the Board must ensure the organization has integrated governance, risks management, and compliance system. (Governance, Risk and Compliance or GRC)

1.1.2 GRC is a continuous process that starts with understanding demand of stakeholders, making strategic plan / business direction in alignment with those demand, assessing risks or future events that may prevent the organization from achieving the strategy in order to seek ways to control or manage (or improve) and regularly monitor efficiency of the process.

1.1.3 To integrate "risk management" into GRC framework, the Board should communicate clearly with the management, especially the CEO, about issues that should be reported to the Board. Key matters that should be reported to the Board include

1.1.3.1 Key risks of the organization.

1.1.3.2 Ways to manage such risks.

1.1.4 After being reported, the Board should consider risks and ways to manage them in comparison with "risk appetite" as well as suggest the management if additional actions should be taken. In contrary, if risk management methods can substantially reduce risks and allow more room to take more risks, the Board may consider adjusting corporate strategy / revising up risk appetite as appropriate. To perform the aforementioned tasks, the Board must ensure that the organization complies with relevant laws, regulations, and policies fully and accurately .

Remark: See further details in The Thai Institute of Directors' "Guideline on Board's Roles in Governance, Risk, and Compliance".

1.2 Determination of risk management framework

1.2.1 The Board has a duty to oversee risk management by the management, emphasizing that risk management must drive/support the organization's strategy to meet expectations of stakeholders and keep the organization's risks in alignment with risk appetite.

1.2.2 The Board should clearly stipulate risk framework / definition and ensure the company has appropriate risk management and controls. It may refer to international practical framework called COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017) (See Annex 1)

1.2.3 The Board should have business knowledge, experience, and good understand of relevant risks while being independence to ask management challenging questions and concur in issues as follow:

- 1.2.3.1 Appropriateness of strategy and risk appetite.
- 1.2.3.2 Harmony of strategy and goals / long-term objectives of the company (vision, mission, value etc.)
- 1.2.3.3 Risk assessment when making key decisions such as merger, capital allocation, dividend utilization etc.
- 1.2.3.4 Ability to respond quickly to key operational volatility or the company's portfolio view of risk.

1.2.4 The Board should monitor, comment, and provide suggestion on how the management manage risks and impose internal controls to mitigate risks or impact. Type of key risks that the Board should consider include:

- 1.2.4.1 Strategic Risk
- 1.2.4.2 Operational Risk
- 1.2.4.3 Financial Risk
- 1.2.4.4 Compliance Risk
- 1.2.4.5 Technology Risk
- 1.2.4.6 Fraud Risk
- 1.2.4.7 Human Resource Risk
- 1.2.4.8 Hazard Risk
- 1.2.4.9 Process Risk
- 1.2.4.10 Other risks (if any)

1.3 Determination of risk appetite

1.3.1 The Board should determine "risk appetite" along with strategic planning. In doing so, the Board should consider business environment, corporate culture, alignment with mission and vision, and expectations of stakeholders.

1.3.2 Risk appetite refers to acceptable level and value of risk determined by the company that can be used to cover overall risks. Good risk appetite will make the company accept appropriate level of risk suitable for achievement of long-term strategic plan as well as enhance and preserve corporate values.

1.3.3 "Risk appetite" can change. During economic crisis, the company may need to be cautious and has marginal risk appetite. Once the economy recovers, the company may increase "risk appetite" by using statement or narrative such as

1.3.3.1 The company will not accept if there is 10% chance that the company will have to register more than Bt10 million loss.

1.3.3.2 The company will use new innovation to improve its services unless the new innovation is exposed to risk of violating law and may cause business disruption.

1.3.4 In determining risk appetite, the Board should provide the management with clear guidelines as follow

1.3.4.1 Method to determine "risk appetite".

1.3.4.2 Issues that will enhance corporate value should also be taken into account when determining risk appetite, not just issues that could cause damage.

1.3.5 The Board and management should discuss to determine "risk appetite" that links with corporate vision, values, and strategy. Among questions that the Board may bring up as discussion topics are

1.3.5.1 Which activity has risk levels beyond "risk appetite" and affect the company's strategy?

1.3.5.2 What are activities that the company bear too little risks to achieve its objectives?

1.3.5.3 Which part of the business bear more or lesser risk appetite than other parts?

1.3.5.4 Which strategy or objective is crucial to the organization's success and whether it has appropriate "risk appetite"?

1.3.5.5 What is the current risk level of the organization? (high, moderate, low)

1.3.5.6 What are risks that should determine "risk appetite"?

1.4 Determination of risk management structure

1.4.1 The determination of risk management structure should be in alignment with the corporate strategy and objectives. The authority and reporting must be clearly assigned in the Board, management, and other levels while human resource and budget must be adequately allocated to perform the tasks. (See Annex 2)

1.4.2 Risk management structure has various formats such as

1.4.2.1 De-centralized risk management structure will help identifying various risks without concentrating on any risk in particular.

1.4.2.2 Centralized risk management structure will point out only a few risks that are relevant to the company.

1.5 Creating risk management culture

1.5.1 The Board should accommodate creation of risk management culture by setting tone from the top and make the management recognize and be accountable for risk management under their respective departments. This can be done by linking risk management with operational targets, which may include the consideration of risk management efficiency in the determination of rewards / incentives.

1.5.2 To evaluate risk management culture, the Board may consider using the following questions:

1.5.2.1 Has the Board and senior management provided direction and communicate the significance of risk management?

1.5.2.2 Does the management understand duties and responsibilities concerning risk management?

1.5.2.3 Has personnel training and performance evaluation been considered together with risk management outcome?

1.5.2.4 Can personnel at all levels of the organization proactively express comments and discuss fully in issues concerning risks?

1.6 Communicating core value in risk management of the organization

1.6.1 The Board should ensure accurate and effective risk management communication with relevant internal and external parties, particularly when there is any sustainability issue concerned by stakeholders.

1.6.2 The Board should acknowledge risk management report on a regular basis. Information received should comprise of key issues such as key risks, methods used by the management to manage such risks, potential emergence of new risks, risk management impact on strategy and operational targets etc.

1.7 Human Resource Development

1.7.1 The Board should accommodate the development of human resource to equip them with knowledge and capability to assess risks and determine methods to manage such risks. With capable human resource, the company may then assign them full authority to implement and make decision because they can collaborate to achieve the company's strategy and objectives.

1.7.2 The Board should provide direction for performance evaluation and determination of incentives, both monetary and non-monetary, such as promotion and commemorative announcement for those helping the company manage risks and effectively achieve its strategy and objectives.

Guideline 2 Nomination of Risk Management Committee

The Board may consider nominating "Risk Management Committee" to help it perform more effectively in overseeing risk management from policy, implementation, monitoring, to reporting levels.

The Risk Management Committee can substantially relieve burden of the Board as the committee can spend time fully to perform duty concerning risk management. However, the Board is still accountable for this duty as it cannot transfer the responsibility of this matter to the Risk Management Committee.

2.1 Determination of necessity to nominate Risk Management Committee

2.1.1 The Board should determine whether it should nominate Risk Management Committee or perform the duties by itself. Issues to be considered are as follow:

2.1.1.1 Do the Board or other committees have adequate time to emphasize on risk management?

2.1.1.2 Does the Board want to have a committee to be the centre in overseeing and monitoring risks in all fronts or all units of the company to ensure transparency in risk management?

2.1.1.3 Does the Board want to communicate with shareholders and stakeholders that the company emphasize especially on risk management?

2.1.1.4 Does the Board want dependent directors (e.g., executive director) to oversee risk management? (In this case, Audit Committee cannot be member of Risk Management Committee)

2.1.1.5 Does the Board concern that the company may not have sufficient capability to identify, assess, and manage risks?

2.1.2 In case the Board nominate Risk Management Committee, it must allot sufficient time to hold meeting with the committee to acknowledge the outcome and problems arise from risk management.

2.1.3 In case the Board nominate Risk Management Committee, there should be a written Risk Management Committee Charter approved by the Board (See Annex 3). The charter should be reviewed annually to ensure its practicality.

2.2 Composition and qualifications of Risk Management Committee

2.2.1 Composition of Risk Management Committee in each company depends on size, business complexity and relevant legislations.

2.2.1.1 In a small enterprise with simple structure, the Board usually acts as Risk Management Committee.

2.2.1.2 In a medium enterprise, Risk Management Committee usually is the Board or other committees such as Audit Committee.

2.2.1.3 In a large enterprise or company with everchanging businesses, a separate "Risk Management Committee" may be nominated.

2.2.2 Members of Risk Management Committee may be "all directors" or "a mix of directors and management", which will report result to the Board.

2.2.3 In case members of the Risk Management Committee are all management, they usually consist of Chief Executive Officer (CEO), Chief Financial Officer (CFO), Chief Operating Officer (COO), Chief Risk Officer (CRO), or other C-Suite executives.

2.2.4 Risk Management Committee must have been equipped with knowledge about business characteristics and industry dynamics, expansive vision, able to analyze and predict future events comprehensively and rationally, have leadership and be decisive as well as knowledge about how to manage risks.

2.3 Roles, duties, and responsibilities of Risk Management Committee

2.3.1 Risk Management Committee is tasked to support and relieve burden of the Board in sustaining effective risk management mechanism of the company from policy, implementation, monitoring, to reporting levels (as mentioned in Guideline 1) such as

2.3.1.1 Screen risk management policy and framework before proposing to the Board for approval.

2.3.1.2 Consider risk assessment result as well as plans to manage such risks and provide suggestions on how to mitigate risks to keep them in alignment with risk appetite to ensure the company has sufficient and appropriate risk management system.

2.3.1.3 Provide advice / recommendation to the Board and management about risk management as well as accommodating continuous development of internal risk management framework/system.

2.3.1.4 See that risk management framework/policy are regularly audited to ensure they align with the company's business context and environment.

2.3.1.5 Report key risks, status, and progress in managing such risks to the Board on a regular basis.

2.4 Terms of office

2.4.1 In case members of the Risk Management Committee are "all directors" or "a mix of directors and management", the Board should clearly stipulate terms of the Risk Management Committee in alignment with terms of the Board.

2.4.2 In case committee member resigns, terminates membership, or has any reason to leave the membership and consequently make the number of Risk Management Governance Committee less than "the minimum", the Board should consider nominating other qualified person to fill in the position.

2.5 Meetings of Risk Management Committee

2.5.1 The company should stipulate that Risk Management Committee meets at least twice a year. (some companies may require quarterly meeting) Chairman of Risk Management Committee may call additional meetings as deem appropriate. However, the Risk Management Committee should set meeting dates in advance in the Annual Board Calendar.

2.5.2 The Risk Management Committee should work with Secretary of the Corporate Governance Committee to set (initial) meeting agenda before proposing to the Board for approval.

2.5.3 The meeting invitation letter should clearly state meeting date, time, venue, agenda, and attached with meeting documents. They should be delivered to the Risk Management Committee members and relevant persons at least seven days ahead of the meeting date. Should additional agenda item arise, more meeting can be arranged as deem appropriate.

2.5.4 Each member of the Risk Management Committee should attend at least 75% of total meetings held each year. The meeting "quorum" should consist of at least half of the Committee at the time.

2.5.5 "Meeting resolution" will base on majority vote of attending committee members. Each member has one equal vote and in case of tie vote, Chairman of the meeting will cast an additional vote to break tie.

2.5.6 In case the Chairman of Risk Management Committee is unable to attend the meeting, committee members may nominate "Vice Chairman of Risk Management Committee" (if any) or one of the committee members to act as "Temporary Chairman" of the meeting.

2.5.7 The Risk Management Committee may invite the management as well as other relevant persons to join the meeting in certain agenda items in order to seek information as necessary.

2.5.8 "Secretary of the Risk Management Committee" must attend all meetings to record and prepare meeting minutes. In case the Secretary of the Risk Management Committee is unable to attend the meeting, the Risk Management Committee may assign other person to assume such roles instead as deem appropriate.

2.6 Report to the Board

2.6.1 The Risk Management Committee should regularly report meeting results to the Board to keep the Board informed about its performance, key risks of the company, and useful recommendations for the Board's decision.

2.6.2 The Risk Management Committee should prepare "Annual performance report of the Risk Management Committee" and submit to the Board annually. The report should be signed by the Chairman of Risk Management Committee and be disclosed in the annual report along with details in other aspects such as

2.6.2.1 Review of risk management framework and direction.

2.6.2.2 Key risks that the company is facing.

2.6.2.3 Factors that could affect future risk status of the company.

2.6.3 Performance of the Risk Management Committee should be evaluated annually to review past direction and indicate any problem or challenge. It should then be reported to the Board to seek ways for improvement and enhance efficiency. (See Annex 4 for example of issues to be used in self-evaluation of Risk Management Committee)

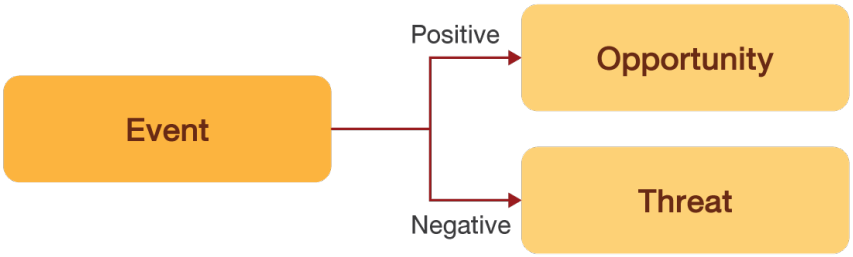
2.6.4 The performance evaluation of Risk Management Committee may apply similar method as the performance evaluation of the Board or it could be conducted and advised by external expert. The evaluation should be conducted at least once a year or in tandem with the performance evaluation frequency of the Board.

Annex

Annex 1 Organizational risk management under COSO ERM Framework

Basic concept

- Risk is event that may occur in the future and affect achievement of business strategy and objectives. Such event could have either positive or negative impact on the organization.



- Organizational risk management under COSO ERM Framework has five elements including

1. **Governance and Culture** means the Board comprehends with the company's risks and risk management as well as build s culture that will drive successful risk management.

2. **Strategy and Objective Setting** refers to harmonization of risk management, strategy, and determination of objectives in strategic planning. The determination of risk appetite must relate with the strategy while objectives will facilitate strategy implementation and will be the fundamental of risk indication, assessment and management.

3. **Performance** refers to risk indication, assessment, and management.

4. **Review and Revision** refers to performance review to see if risk management system needs to be improved and how.

5. **Information, Communication and Reporting** refers to communication to receive and provide continuous information concerning risk management. It consists of internal, external, and inter-department information.

- Robust risk management framework must be part of the performance to achieve the organization's strategy. It must align with expectations of stakeholders and accommodate sustainable growth because the company may see new opportunities after understanding and managing new risks.

Integrating risk management with the company's strategy and operations

- Risk management is not a separate process from others. In contrary, the Board should ensure the management normally develops and applies risk management with other operations. Key integration of risk management should comprise of:

1. Integration with strategic planning

   Strategic planning is choosing the best available alternative for sustainable growth. Since the decision involves both risks and opportunities, the company should apply risk management methods with strategic planning to mitigate potential mistake and select appropriate strategy that fit with the company's risk appetite.

   COSO Enterprise Risk Management – Integrating with Strategy and performance suggests that the company consider three risks as follow

   1.1 Risk that the strategic plan does not synch with the company's mission, vision, and values

   This risk may derive from unclear mission, vision, and values that make them mismatch with the strategic plan. In contrary, clear mission, vision, and values but poor strategic plan may bar achievement.

   1.2 Risk of choosing wrong strategic plan.

   In strategic planning, the company usually have many alternatives and each strategy contains different risk. Therefore, the company should assess risks associated with each alternative whether they fit with the risk appetite.

1.3 Risk of implementation failure.

This kind of risk usually occur from internal and external implementation such as financial risk, operation risk, compliance risk, market risk, technological risk, and human resource risk. Therefore, the company should make all personnel understand and build risk management culture to make it part of normal operation and lead to common desirable targets.

2. Integration with performance evaluation

The company should have a process to link performance evaluation with risk management. It should use performance indicators as targets, let the management assess potential events and potential impact from targets achievement, then let the management determine risk management methods. Once the company achieve the current targets, it may uplift targets while creating and preserving corporate value as well as building new opportunities.

3. Integration with internal controls

Risk management is not just about determining what to do but to design and implement existing processes such as those concerning procurement, revenues, inventory management, financial report, and IT etc. A good process requires adequate and appropriate internal controls to manage risks and achieve objectives.

For instance, companies with revenue risk from new competitors could manage risk by seeking new customers as soon as possible. In this regard, the sales department must define qualifications of targeted new customers but it also need to present to the Board for approval to ensure the qualifications match with the company's strategy and retain its competitiveness.

4. Integration with sustainability

Sustainability is obvious targets of all companies. Events that may threaten sustainability are considered risks. The company must assess events that could occur seek ways to manage such risks.

Risks that threaten sustainability include insufficient governance, rejection by the community, economic crisis, and climate change.

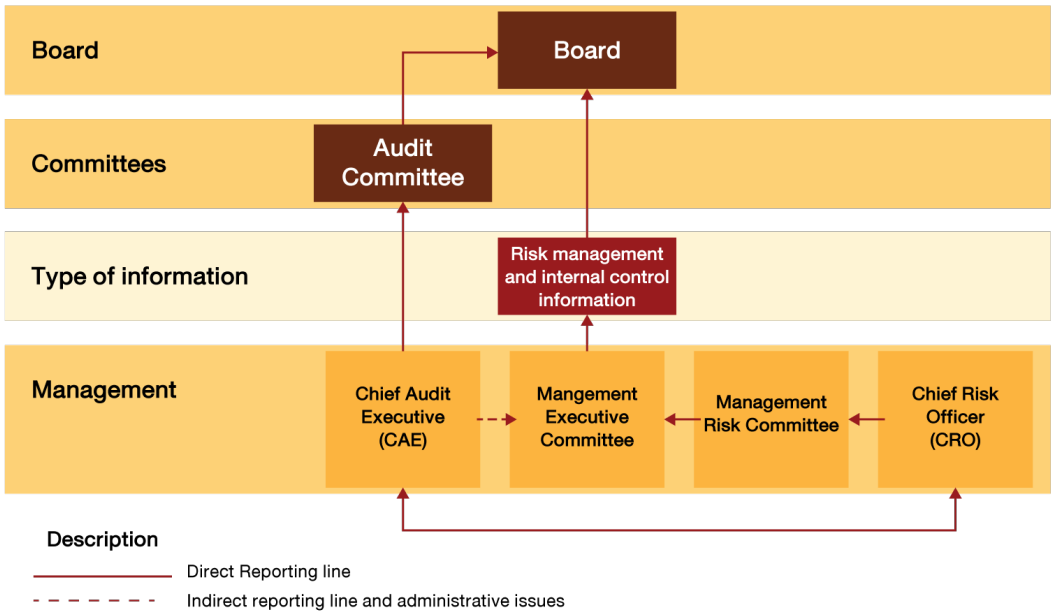
5. Integration with Environmental, Social and Governance (ESG)

The Risk Management Committee should ensure the company applies risk management to evaluate, manage and report ESG risks. It should set collaborative structure between units responsible for risk management and corporate sustainability, arrange for evaluation and prioritization of ESG risks, and communicate ESG risk management outcome to relevant internal and external parties such as investors, suppliers, customers, civil society organizations and the general public.

Annex 2 Types of risk management structure

Structure 1

The "Board" has a duty to oversee risk management and internal controls.

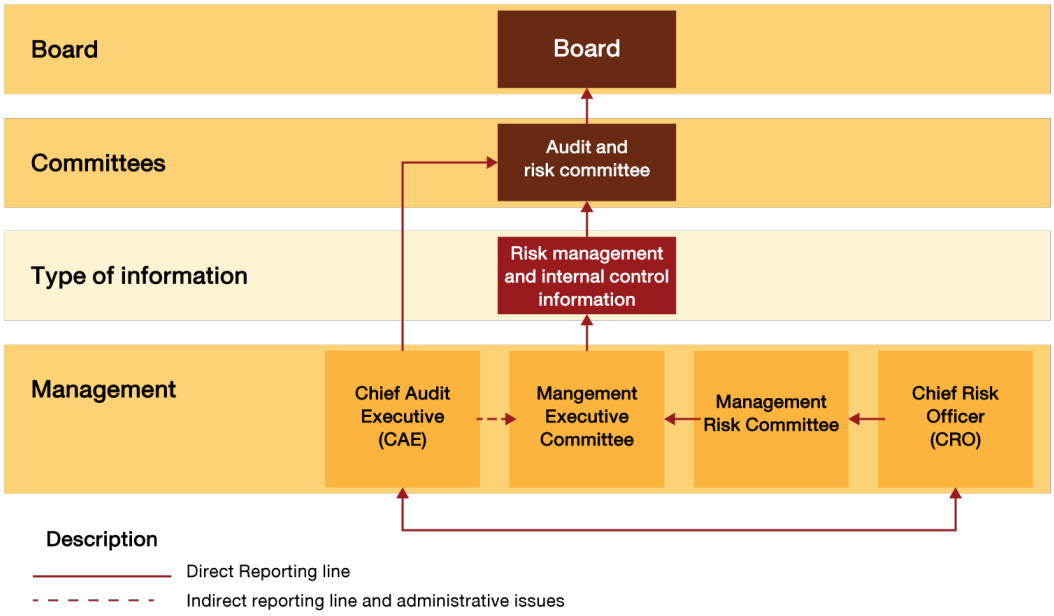


Source : IOD Singapore

Remark: Chief Executive Officer (CEO) is member of Executive Committee

Structure 2

"Audit and Risk Management Committee" oversees risk management and internal controls.

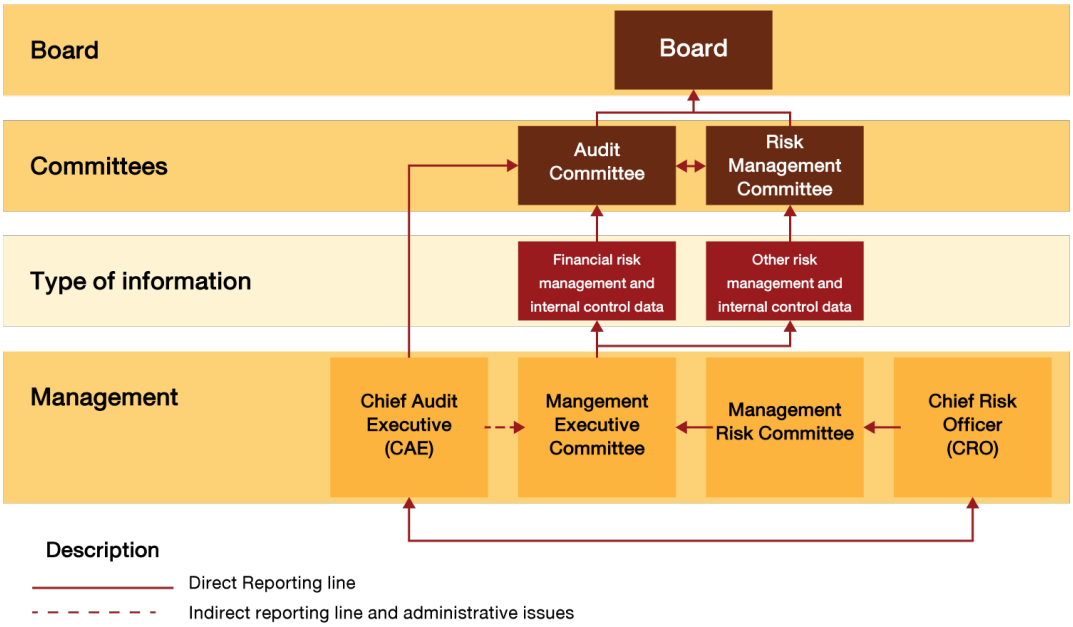


Source : IOD Singapore

Remark: Chief Executive Officer (CEO) is member of Executive Committee

Structure 3

"Risk Management Committee" oversees risk management and internal controls.

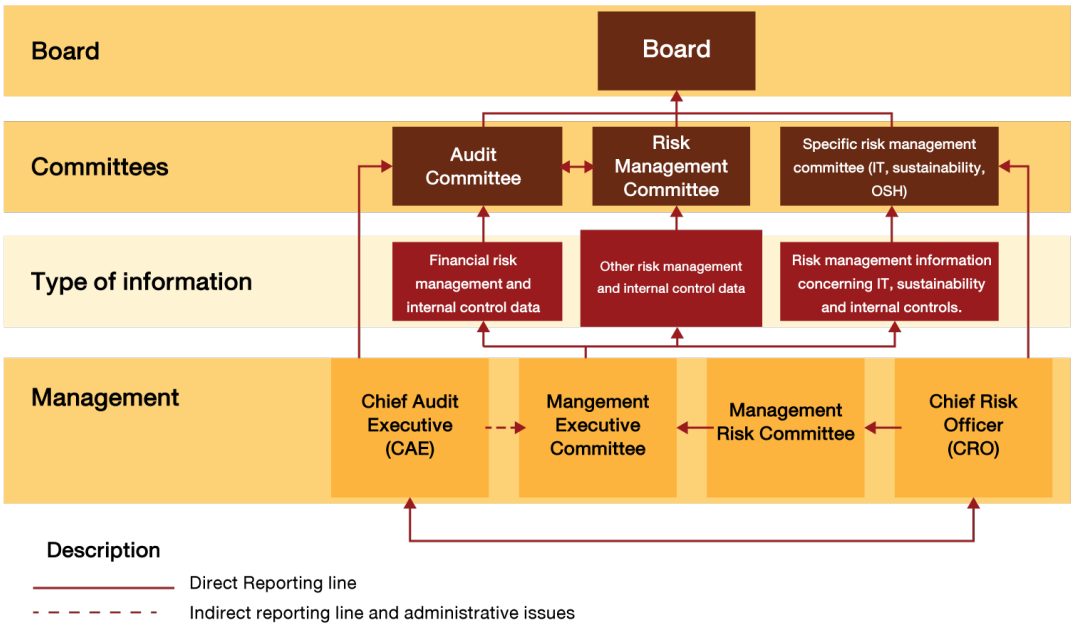


Source : IOD Singapore

Remark: Chief Executive Officer (CEO) is member of Executive Committee

Structure 4

"Risk Management Committee" collaborates with other committees.



Source : IOD Singapore

Remark: Chief Executive Officer (CEO) is member of Executive Committee

Annex 3 Example of Risk Management Committee Charter

1. Objectives

The Board nominates Risk Management Committee, comprising a number of qualified directors/ management to determine risk management policy that covers the whole organization and ensure that risk management system is in place to control risks and mitigate impact of risks, determine preventive measures, and appropriately monitor implementation of such measures. The Charter is meant to help Risk Management Committee understand its roles, duties, and responsibilities as well as to be used as guideline in performing its duties.

2. Nomination

2.1 Risk Management Committee consists of directors/management at no less than .....

2.2 The Board or Risk Management Committee will pick a committee member to be Chairman of Risk Management Committee.

3. Qualifications

3.1 Members of Risk Management Committee must be equipped with knowledge and experience useful for business operations, be honest person, have high ethical standard, and have enough time to contribute fully to the company. In particular, they must have knowledge about relevant and potential risks that may affect the company's business operations.

3.2 Members of Risk Management Committee must be qualified and has no prohibited characteristics under Public Company Act, Securities and Exchange Act, and other relevant legislations concerning the company's business.

4. หน้าที่และความรับผิดชอบ

4.1 Consider and identify key risks concerning the company's business operations such as strategic risk, financial risk, operational risk, regulatory risk, marketing risk, and reputation risk etc. The committee should also suggest ways to prevent such risks and manage the risks to align with the company's risk appetite. It should set policies and suggest ways to manage risks concerning business operations as well as offer recommendations to the management about risk management.

4.2 Determine risk management plan and process for the company.

4.3 Oversee and accommodate risk management by tracking and evaluating overall risk management framework. It must also review sufficiency of risk management policy and system as well as improve operating plan to continuously mitigate risks in accordance with ongoing business conditions.

4.4 Communicate with Audit Committee about significant risks to consider adequacy of internal controls.

4.5 Report risk evaluation and risk mitigation outcome to the Board on a regular basis. Any key issue that significantly affect financial and operating results of the company must be reported to the Board as soon as possible.

4.6 Perform other duties assigned by the Board.

5. Terms of office and nomination of Risk Management Committee

5.1 Risk Management Committee shall vacate office upon

1) Death.
2) Resignation.
3) Lacking of qualification or having prohibited characteristics under Public Company Act or Securities and Exchange Act.
4) Resolution by the Board to vacate office.
5) Ruled out by the Court.
6) Terminated from directorship or company employment.

5.2 Any member of Risk Management Committee who wish to resign must submit resignation in written, effective from the date the letter reached the company.

5.3 In case of vacant Risk Management Committee member, making the Committee unable to meet the quorum, the Board may consider nominating any qualified person to fulfil the position. In other cases, the Board may consider nominating any qualified person to be member of Risk Management Committee as deem appropriate.

5.4 In case all members of Risk Management Committee end their terms altogether, the outgoing Committee members must assume their roles until the new Risk Committee members take office.

6. Meetings

6.1 At least half of the Risk Management Committee is required to present to meet the quorum. In case the Chairman of Risk Management Committee is not presented or unable to perform duties, the Vice Chairman will chair the meeting. If there is no Vice Chairman or the person unable to perform duties, participants may pick a member to act as Chairman of the meeting.

6.2 The decision of Risk Management Committee will base on majority vote. Each member has one equal vote (unless the member has conflict of interest, the member will not be eligible to vote on the agenda item) and in case of tie, Chairman of the meeting will cast an additional vote to break tie.

6.3 The Risk Management Committee may call meetings as deem appropriate, at least quarterly. In case the meeting cannot be held within the quarter, Chairman of the Risk Management Committee may call a meeting. If needed, at least two members may ask the Chairman to call a meeting, which will require the Chairman to call a meeting within 14 days.

6.4 Chairman of the Risk Management Committee or a member assigned by the Chairman may determine meeting date, time, and venue of Risk Management Committee meeting. The venue may be different than the company's head office.

6.5 To call a meeting of the Risk Management Committee, the Chairman of Risk Management Committee or assigned person must send invitation letter, relevant documents, and voting of the committee through registered mail or send directly to the Risk Management Committee. The invitation must indicate meeting time, date, venue, and agenda to Risk Management Committee at least seven days ahead of the meeting date. In case of emergency to preserve the company's interest, the meeting invitation may be informed via other methods or the meeting may be held sooner than scheduled.

7. Authorities

7.1 The Risk Management Committee is authorized to nominate Secretary of the committee to facilitate operations of the committee.

7.2 The Risk Management Committee is authorized to seek comments from other professions as deem appropriate at the company's expenses. The employment must be in accordance with the company's regulations.

7.3 The Risk Management Committee is authorized to seek information from the company's units and subsidiaries.

8. Reporting

Risk Management Committee is a committee appointed by the Board to study and screen relevant issues. Therefore, the Risk Management Committee is responsible to report its performance to the Board on a regular basis.

9. Renumeration

The Risk Management Committee is eligible to receive remuneration approved by the Board after taking into consideration comments and recommendations of the Nomination, Compensation, and Corporate Governance Committees.

At the XX/25XX Board meeting on XXX, the Board approved Risk Management Committee Charter, effective from XXX.

Announced on Date …… Month …… Year ……

Signature ……..

Chairman of the Board

Annex 4 Example of issues for self-evaluation of Risk Management Committee

Issues
Governance and Culture
1. Knowledge and understanding about risk management system. 2. Continuous training to stay up to date with changes in risk management. 3. Relationship and collaboration with the management to understand concept, attitude, and risk management method of the company. 4. Communication ability to make everybody understand and recognize the significance of risk management and become corporate culture.
Strategy and Objective Setting
5. Ensure that risk assessment is in alignment with strategic planning. 6. Determination of appropriate risk appetite of the company and communicate with relevant parties.
Performance
7. Ensure that risk management is part of business as usual and that it accommodates achievement of operational targets.
Review and Revision
8. Monitor and improve risk management methods while regularly assessing new risks.
Information, Communication and Reporting
9. Report risks to the Board in comprehensive, accurate, regular, and timely basis. 10. Apply technology in risk management to ensure complete, accessible, and timely communicated information.

References

1. COSO 3 Lines of Defence
2. COSO ERM Creating and Protecting Value
3. COSO Guidance on Risk Appetite
4. **Developing a Strong Risk Culture**, PwC December 2010
5. **Enterprise Risk Management – Integrating with Strategy and Performance**, Committee of Sponsoring Organizations of The Treadway Commission, 2017
6. **GRC Capability Model version 3.0**, The Open Compliance and Ethics Group
7. **GRC And The Board: What They Really Need To Know**, Forbes, March 2020
8. **G20/OECD Principles of Corporate Governance**, Organization for Economic Co-operation and Development (OECD), 2015
9. **How your Board can influence culture and risk appetite**, PwC, February 2017
10. **How your Board can decide if it needs risk committee**, PwC, March 2017
11. **How your Board can ensure enterprise risk management connects with startegy**, PwC, April 2017
12. **Striking a Balance – Whistleblowing arrangements as part of a speakup strategy**, PwC, January 2011
13. **The Building Blocks of GRC**, The Open Compliance and Ethics Group, April 2016
14. **Guidance on Risk Appetite – a critical to success**, COSO

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