Thai Institute of Directors

Guideline on Board's Role in Governance, Risk, and Compliance (GRC)

Content

Preface

A sustainable company in modern era requires solid fundamental, agility, and ability to manage risks under relevant laws and regulations. Meanwhile, stakeholders also demand growth, business transparency, as well as fast and effective responses to changes. Thus, companies are driven by various forces toward integrated operations.

In this regard, the Board must have the capability to steer the company toward desirable strategy. The Board also has a role to comprehend with the holistic view of Governance, Risk and Compliance (GRC) aspects.

Since mission of each GRC element requires continuous, detailed, and fast actions, Boards of small companies may be able to handle all the necessary tasks by themselves. But for sizable companies, Boards may assign separate committee to help oversee each aspect, such as governance, risk, compliance, and internal controls. However, the appointment of committees only alleviates some of the Board's burden though overall responsibilities still lie with the full Board.

Therefore, the Thai Institute of Directors (IOD) has developed this guideline to help the Board recognize the significance, elements, roles and responsibilities, and conduct effective integration of Governance, Risk, and Compliance.

• 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 — Consultant, Thai Institute of Directors (Committee Consultant)

3. 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

4. Representative from Government Pension Fund

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

5. Representative from Association of Investment Management Companies

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

6. Experienced Directors at Listed Companies

Mr. Yuth	Worachattarn	Expert on Corporate Governance and Social Responsibility The Stock Exchange of Thailand
Mr. Veerasak	Kositpaisal	Chairman Eastern Water Resources Development and Management Public Company Limited
Ms. Patareeya	Benjapolchai	Expert on Corporate Governance and Social Responsibility The Stock Exchange of Thailand

7. 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, Corporate Strategy and Business Development Function Siam Commercial Bank Public Company Limited
Ms. Boonsiri	Charusiri	Former Company Secretary and Consultant Banpu Public Company Limited

8. Corporate Governance Expert

Ms. Varunee	Pridanonda	Partner and Consultant - Governance, Risk, Compliance and Internal Audit Services Pricewaterhouse Coopers ABAS 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

Section 1

Key Principles

Key Principles

1. The Board, as the leader, has roles and responsibilities in sustainable corporate value creation. It should ensure the company has strategy that can accommodate growth while allowing business to be conducted ethically, transparently, taking all stakeholders into account and comply with relevant laws. (See Guideline 1)

2. The Board should apply GRC integration concept as a framework in driving the company to operate in alignment with four key principles of the Office of Compliance and Ethics Group (OCEG). The four key principles include

    2.1 Learn – Study and comprehensively understand business context, corporate culture, and expectations of stakeholders.
    2.2 Align – Use such comprehension to determine the company's objectives and identify potential risks that may derail achievement of such objectives.
    2.3 Perform – Drive the company towards the objectives through effective business process that complies with regulations as well as prudent internal controls.
    2.4 Monitor – Put in place adequate and appropriate monitoring system to ensure objectives are achieved. (See Guideline 1)

3. The Board should ensure the company is driven by a vision and progressive strategy that will allow it to achieve objectives rationally and ethically amidst uncertainties from rapid and severe changes in economic, market, technology, personnel, legal, environment, and social aspects, etc. With such uncertainties, the company must address potential risks and opportunities while seeking to mitigate risks and enhance opportunities to achieve the strategic objectives. (See Guideline 1)

4. The Board should govern and set business direction toward sustainability, taking into account internal and external factors as well as stakeholders' interests. The Board should also communicate strategies, policies, and key principles with the management in order to put them into implementation. They should cover effective, flexible and agile risk management as well as comprehensive compliance with relevant laws and regulations. (See Guideline 2)

5. The Board's roles and responsibilities are not divisible. The Board must ensure the company can connect and interweave Governance, Risk Management, and Compliance into the same picture under ethical, transparent and honest corporate culture. This is called the Governance, Risk and Compliance, or GRC, integration. (See Guideline 2)

6 The Stock Exchange of Thailand has a guideline for the Board to appoint appropriate experts as members of committees with specific tasks to study key issues that regularly occur or need special monitoring to enhance the Board efficiency. (For examples, Audit Committee, Risk Management Committee) However, the Board is still fully accountable for the roles and responsibilities that it assigned to such committees. (See Guideline 3-4)

7 The Risk Management Committee, for example, is assigned by the Board to oversee risk management, work closely with the management, and ensure the Board gets quality risk report in timely manner. (See Guideline 3-4)

Section 2

Guidelines

Guideline 1 | Key Roles of the Board in Corporate Governance

1.1 Definition of Governance, Risk, and Compliance (GRC)

1.1.1 GRC refers to the integrated administration of all units, systems, processes, personnel, and information to ensure the company achieves its strategies, objectives, and goals while taking into account expectations of all stakeholders.

1.1.2 GRC is considered the comprehensive administration of

1.1.2.1 Corporate Governance – Comprehend with the company's context through business environment assessment, industry dynamics, and stakeholders' expectations, etc. and use them as inputs to develop corporate strategy and appropriate business model.

1.1.2.2 Risk Assessment – Identify risks that could derail strategy implementation and seek ways to control / manage such risks.

1.1.2.3 Compliance – Comply with professional ethics and relevant guidelines.

Example of Administration in Accordance with GRC Principles

Business Environment:

- The company had only one distributional channel. (rental space in department store)
- The company found that "online business" accelerated as consumers shifted their behavior from buying goods at traditional stores to "online shopping" which is much easier, more convenient, and time-saving.
- The company faced new competitors with greater variety and more modern distribution channels, leading to continuous declines in its sales/profit.

Direction and Strategic Goals:

- The company set earnings growth target at least 20% YoY.
- The company's strategy was to add new online distribution channels to boost proportion of online sales to at least 30% of total sales.

GRC Administration:

- After assessing risks of launching online distribution channels, the company found that current operating system cannot accommodate the new channels.
- The management formed a task force to study and adjust operating model of sales, marketing and accounting departments to ensure they are in synch and apply new technology into such functions.
- Considered relevant legislations concerning each functions.
- The management reported strategy implementation progress to the Board quarterly.

In the past, most companies did not employ GRC administration concept. They just set targets and went right to implementation without considering potential risks or making plans to tackle such risks. If companies failed to achieve the targets, they simply changed targets or started over again, causing substantial waste of time and budget. Therefore, the Board should push the company and management to apply GRC principle in strategy implementation and general administration.

1.2 Why Should the Board Put Emphasis on GRC?

1.2.1 The Board, as the leader, has a significant role in sustainable value creation for the company. It should take part in strategy and management oversight to ensure the company is competitive and adaptable to changes. The Board is considered a group of key persons who promotes the adoption of GRC principles to ensure the company successfully achieved its strategic objectives.

1.2.2 Should the Board fail to apply GRC principles, the company could face following issues.

1.2.2.1 Lack comprehensive understanding of stakeholders' expectations, making business model lack long-term view and unsustainable.

1.2.2.2 Lose competitiveness due to internal administration issues.

1.2.2.3 Inefficient operations with abnormally high operating costs.

1.2.2.4 Unable to understand risky operations and key weaknesses of relevant controls due to complex, fragmented, and disconnected processes.

1.2.2.5 Have various risk reports from many functions / units but still unable to analyze the big picture of key risks, how the management should tackle, and how will they affect strategy.

1.2.2.6 Absence of timely non-compliance reports could make it difficult to identify and resolve any incident, and undermine the corporate image.

1.2.3 Since GRC is the integration of all operations that link many functions / units within the company, the Board has a key role to demonstrate "tone from the top" in order to make all employees agreed to the need for GRC adoption and ensure collaborated implementation.

1.2.4 The Board may demonstrate "tone from the top" to raise awareness of employees at all levels through the following methods:

1.2.4.1 Set clear agenda or discussion topic at Board meetings to ensure continuous monitoring.

1.2.4.2 Prepare policy to clearly communicate GRC-based guidelines / practices throughout the company.

1.2.4.3 Determine a format of management report that links all elements in accordance with GRC principles to give the Board a holistic view of the company.

1.3 Qualifications of Company with Effective GRC Integration

Companies with effective GRC integration will have confidence in achieving pre-determined strategies, objectives, and goals because they employ efficient methods in process, personnel, data, and IT administrations under ethical and transparent culture. Companies adhering to GRC principles usually have the following characteristics:

1.3.1 The Board is well aware of information necessary for proactive and timely oversight and able to collaborate effectively with the management.

1.3.2 Possess accurate understanding of the company's context, sustainability aspects, and stakeholders' expectations in order to determine appropriate business model / long-term strategy.

1.3.3 Flexible and agile business management with relatively lower cost than industry peers.

1.3.4 Identify new business opportunity and confidently invest in the pursuit.

1.3.5 Agile and simplified business operation without time wasted and internal conflicts between functions / units.

1.3.6 Reduction of losses in key assets.

1.3.7 Able to access information needed to make timely decision by authorized persons.

1.3.8 The execution of strategy follows pre-determined scope / timeframe and yields desirable results.

1.4 Overview of Roles of GRC-focused Board

1.4.1 Since the Board is obliged to perform "Duty of Care" and "Duty of Loyalty", it is necessary for the Board to ensure the company applies GRC approach. The Board should clearly set and comprehend with strategies, objectives, and goals. This will lead to appropriate risk assessment and formation of risk management system, both at corporate and functional levels, as well as evaluation and controls to ensure compliance with relevant laws and regulations. In summary, the Board should be able to understand and monitor management performance in a holistic manner rather than in silos.

1.4.2 Before approving strategic plan, the Board should focus on providing suggestions and ensuring that the management proceeds as follow:

1.4.2.1 Revisit existing business direction / business model to see if they are efficient enough to tackle ongoing challenges and rapid changes in business environment.

1.4.2.2 Propose appropriate strategic plan in conjunction with strategic risk assessment.

1.4.2.3 Consider risk mitigation plans whether they are implementable and how.

1.4.2.4 Consider whether it is necessary to restructure or adjust existing business processes to accommodate such strategy and how.

1.4.2.5 Consider if the execution of proposed strategy has risks of non-compliance.

1.4.3 The Board should consider and take into account the GRC integration of the following activities.

1.4.3.1 Strategy development: The Board has a role to approve strategies proposed by the management. As the management proposes new direction, goals, and strategies, the Board should require the management to present integrated information that covers the new strategic direction, risk assessment and mitigation plans, company's readiness, and work structure that accommodates such strategic direction as well as compliance risk. All these aspects must connect systematically in a non-complex manner and align with each other.

1.4.3.2 Strategy implementation: Following the Board approval of company's direction and strategy, the management must propose implementation plan to the Board, particularly those concerning significant business transactions or investment plans. Therefore, the Board should ensure such plans are in alignment with strategic direction and that the company has concrete risk management, compliance system, and internal controls as well as quality information, personnel and technology to accommodate timely decision-making. In summary, the Board must ensure the stipulated GRC principles are appropriately adopted and accommodate effective implementation. Should there be any part that may not be suitable, the Board must ensure that the management tackle it.

1.4.3.3 Strategy monitoring: The Board must establish a process for the management to report overall implementation result periodically to ensure effective GRC integration.

1.4.4 To perform oversight role, the Board must possess comprehensive understanding of the GRC concept and ready to guide the management properly. The Board may enhance its own GRC readiness through the following aspects.

1.4.4.1 Board Composition:

1.4.4.1.1 The Board should ensure it has appropriate composition. Besides diversity of expertise and experience, all directors should have comprehensive understanding of the company's context and overall linkage of business processes in order to oversee and provide appropriate guidance in GRC development to the management.

1.4.4.1.2 Appropriate Board composition accommodates discussions to exchange, learn, and integrate idea as well as create a balanced view among directors with different expertise in strategy, risk, and compliance, resulting in effective decision-making.

1.4.4.2 Board Leadership:

The Board must have leadership in determining and reviewing strategic direction and other work plans with the management. The Board needs to understand the following issues.

1.4.4.2.1 The Board should understand key factors that the company must take into account to accommodate sustainable growth. Besides disruption issues, the Board should also consider stakeholders' issues / concerns as they will directly affect the company's business operations.

1.4.4.2.2 Understanding these issues allow the Board to make decision and oversee the company in accordance with GRC principles more effectively. They include the determination of company's direction, goals, strategies, risk assessment and management that match with the company's context and relevant compliance issues.

1.4.4.2.3 To understand these issues, the Board needs to engage key stakeholders properly, get management report on sustainability issues and ways to manage them, monitor news, trends and surrounding situations that could, positively or adversely, affect the company.

1.4.4.2.4 The Board must understand business environment, context, and the overview of company's operations. It may seek to gain better understanding by asking for information from the management, arranging business meeting with the management, attending training programs / seminars, etc.

1.4.4.2.5 This is considered key fundamental information that the Board should know prior to and while assuming directorship. Due to ever-changing business environment, directors need to keep up with new information all the time.

1.4.4.2.6 The Board should understand the company's key risks and ways to manage them. Key risks include strategic risk, financial risk, operation risk, and compliance risk, etc. The Board should require regular report and use such information to oversee the management.

1.4.4.3 Board Oversight:

Besides making decision together with the management on company's direction and operating plans in accordance with the GRC principles, the Board also has continuous oversight roles as well. For the Board to fully perform such roles, it should establish a clear framework to oversee implementation as well as provide guidance to the management to enhance the implementation effectiveness in accordance with the GRC principles. The GRC framework should cover the following issues.

1.4.4.3.1 It is imperative that a company must constantly assess its business landscape and environment to see if there is any change and how that change affects its operation. The Board should require the management to take such issues into account and ask it to present this information every time it proposes company's strategic direction / plan, or when it reports implementation progress. This is to ensure all that being proposed or implemented still match the business environment.

1.4.4.3.2 The Board should recognize that rapid changes in business context and environment at present can bring about emerging risks. As such risks are unprecedented, highly uncertain, and difficult to predict the magnitude, these risks may be overlooked by the management. Therefore, the Board should ensure the strategic planning process (in parallel with risk management process) takes these emerging risks into account.

1.4.4.3.3 The Board should ensure that the management reviews the appropriateness of GRC elements and presents them to the Board whenever it proposes new strategic direction / plan or reports implementation progress. The GRC elements include governance structure, risk and control continuum, compliance system, assurance mechanisms, desired behavior and corporate culture, as well as accessible knowledge and data.

1.4.4.3.4 The implementation of the aforementioned tasks may need to be adjusted in accordance with business maturity, relevance, integration and convergence in a wholistic approach. Therefore, the Board should ensure the management presents integrated information that takes into account the company's business environment and maturity.

1.4.4.3.5 Another vital element is that the Board and management takes the leadership, accountability, and assurance roles in driving these issues and making them materialized.

Figure 1: GRC Implementation Framework

Guideline 2 GRC (Governance, Risk, and Compliance) Building Blocks

2.1 GRC Building Blocks

GRC Building Blocks comprise of three key elements including Governance, Risk, and Compliance. To integrate GRC into the company's business operations, the Board should consider the following general principles.

2.1.1 Good GRC implementation requires efficient and effective linkage of Governance, Risk, and Compliance. It starts with the management proposing direction, strategic plan, operating plan or reporting implementation progress together with risk assessment results and ways to tackle such risks to the Board.

2.1.2 Should the Board find that information proposed by the management is appropriate, in line with the company's risk appetite, and the existing corporate governance practices remain intact, the Board may approve the strategic plan or operating plan for the management to implement or develop further. In case of progress report, the Board may acknowledge the progress and allow the management to carry on with the plan.

2.1.3 The Board should ensure that management implements the compliance aspect in parallel with general risk management. There should be regular compliance risk assessment, audit, and periodic report to the Board.

2.1.4 The Board should ensure that management has arrange for internal auditor to audit the efficiency and effectiveness of GRC Building Blocks regularly and submit the audit report to the Board. When the Board finds that strategy, business environment, company size, or stakeholders' expectations have changed, it should be able to advise the management to improve GRC Building Blocks.

2.2 Governance

Considering the governance aspect, the Board must ensure that existing strategic and operating plans or those being proposed by the management match the company's governance structure and key policies. In this regard, the Board must consider the following issues.

2.2.1 Do direction, strategy, and operating plan proposed by the management align with purpose, mission, and vision of the company? Do approved and implemented plans still align with purpose and current company's direction?

2.2.2 Does the existing organizational structure still accommodate direction, strategy, and operating plan of the company? Does the structure need to be amended or resized?

2.2.3 Do direction, strategy, and operating plan align with the organizational culture? (e.g. risk-taking or risk-averse culture) If not, how does the management plan to tackle the matter? For example, the management may form a task force to specifically implement the new strategy. The task force should be separated from the company's conventional structure / hierarchy to ensure faster and more flexible decision making.

2.2.4 Do existing policies accommodate the implementation of direction, strategy, and operating plan? If the existing policies restrict the implementation, how does the management plan to tackle the matter? For example, the management may omit the implementation if it contradicts the company's policy or amend the policy to facilitate appropriate implementation.

2.2.5 Do the implementation of direction, strategy, and operating plan have proper delegation of authorities?

2.2.6 What are performance metrics used to gauge the implementation of direction, strategy, and operating plan? Are they appropriate to be used to measure expected result, impact on culture and employees' behaviour?

In strategy implementation, the management should assess risks at corporate, business, and functional levels. It should report key risks and ways to manage such risks to the Board on a regular basis, at least quarterly. After getting the report, the Board should consider accuracy and completeness of risk listing, appropriateness of risk management plans, and provide comments or suggestions concerning ways to manage them more effectively, or recommend how to improve the strategic plan to match the identified risks. Through consideration of all relevant information, the Board and management may see opportunity to add value to the business. For example, company with low financial and human capital risks have greater opportunity to adopt new technology in business operations.

2.3 Risk Management

Key elements of risk management that the Board should oversee when it considers corporate purpose and strategic direction, makes key decisions, or monitors implementation result include

2.3.1 Does it align with the company's risk appetite? If it exceeds acceptable risk level, how will the management tackle the matter? Should the management cease the action or review the company's risk appetite?

2.3.2 Have key risks arising from the execution of direction, strategy, and operating plan been identified and assessed? Do key risks change along with the situation, time, and business maturity?

2.3.3 What is the company's risk treatment approach? (e.g., reduce risk, accept risk, transfer risk, avoid risk, or pursue risk)

2.3.4 Ensure that report of key risks and ways to manage such risks are presented to the Board on a regular basis or at least quarterly. After receiving the report, the Board should consider the accuracy and completeness of risk listing, appropriateness of risk management plans, and provide comments or suggestions concerning the risks, ways to manage them more effectively, or recommend how to improve the strategic plan to match the identified risks.

After the strategic plan is approved by the Board, the management should assess both "corporate risk" (to identify all key risks of the company) and "business risk" (to identify key risks of each business unit). Latter risks involve operational risk, financial risk, and compliance risk exposed to day-to-day business operations. The management may apply either top-down or bottom-up approaches to assess risks but it must ensure that the assessment of both corporate and business risk will lead to achievement of the company's objectives and strategic goals.

During the phase of strategy execution, the Board should ensure the management also conduct strategic risk assessment. This is particularly important when there is emerging risk that could have substantial impact on the strategic plan and obstruct normal business operations. Therefore, the company needs to mitigate such risks. In case the management detect any risk that could affect the execution of strategy, it must report to the Board so that the Board can consider adjusting strategic plan accordingly.

2.4 Compliance

The Board should ensure the company understand and able to comply correctly and completely with relevant laws, rules, and regulations. Full compliance is considered one of the company's key objectives. Therefore, the management must assess compliance risks, stipulate ways to mitigate such risks, and report the outcome to the Board on a regular basis.

In terms of compliance oversight, the Board should consider the following key issues when the management proposes corporate purpose, strategic direction, or other essential matters for Board consideration.

2.4.1 What are laws, ethics and stakeholder concerns as well as ways to manage them?

2.4.2 Do they align with relevant industry standards or best practices?

2.4.3 How is compliance audit process to ensure the company is meeting relevant laws, rules, and regulations?

2.4.4 What are reporting procedures to inform the Board and key stakeholders on compliance matters?

Guideline 3 | Appointment of Committees

3.1 The Board has oversight roles in GRC which consists of governance, risk management, and compliance systems. With such massive responsibilities, most Boards usually appoint Committees to assist them in performing these duties.

3.2 In general, Committees appointed by the Board to oversee GRC matters include Corporate Governance Committee, Audit Committee (some companies may consider appointing separate Compliance Committee if it fits the business contexts), and Risk Committee.

3.3 Normally, listed companies are required to appoint Audit Committee to help the Board oversee an integrity of financial reporting, corporate governance, risk management and internal controls. Appointment of other Committees depends on appropriateness of each company. Key factor to consider is whether the Board has the capability to oversee these issues by themselves.

3.4 For large-scale companies or those with business complexity, such as financial institutions, the Board may consider appointing more Committees. However, the Board must ensure the appointed Committees are equipped with relevant knowledge and understanding to alleviate burden of the Board.

3.5 Despite appointment of Committees, the Board still have oversight roles and responsibilities for overall operations as it cannot transfer such accountability to the Committees. Therefore, the Board should require all Committees to submit their progress reports to the Board on a regular basis or at least quarterly.

3.6 GRC is the integration of Governance, Risk, and Compliance. Therefore, Committees should work in collaboration and share the same vision. To facilitate integration among Committees, the Board may consider taking the following steps.

3.6.1 Require that each Committee reports to the Board periodically so that the Board obtains a clear picture whether the works of committees are in synch.

3.6.2 Arrange for appropriate overlapping Committee members in a bid to link the Committees and accommodate harmonious work of each Committee. However, other key factors, such as skill, knowledge, and experience of Committee members must also be taken into account.

Guideline 4 | Committees' Roles and Responsibilities Toward GRC

4.1 Corporate Governance Committee

Has following roles

4.1.1 Corporate Governance Committee has a role to set governance framework in accordance with the Stock Exchange of Thailand's corporate governance principles and the Securities and Exchange Commission's corporate governance code. The Committee also has a role to monitor that the implementation of such framework is achieved.

4.1.2 Build and promote good corporate culture and ethics that accommodate achievement of the company's purpose and strategy.

4.1.3 Consider the company's GRC framework and guidelines if they are properly designed and implemented at all levels, starting from the Board, management, to all employees.

4.1.4 Ensure that performance evaluation methodology for the Board and management aligns with GRC framework and guidelines.

4.2 Risk Committee

Has following roles

4.2.1 Oversee the determination of corporate risk appetite for the management to use as operational framework or guidance.

4.2.2 Regularly discuss with the management about risk appetite, especially when surrounding situation changes or new opportunity emerges.

4.2.3 Oversee that the management has prudent risk management process to identify, assess, manage, monitor, and report key risks as well as consider if there is continuous improvement in risk management system.

4.2.4 Provide timely advice on implications of key risks to the management.

4.2.5 Oversee enterprise-wide risk assessment, including the identification and reporting of key risks.

4.2.6 For complex and significant risks, the Board may consider recruiting committee members with specific expertise in such matter.

4.2.7 Monitor risky behaviours that affect the efficiency of risk management system and force the company to take risk beyond appropriate level. For example, inappropriate or excessive remuneration could incentivize employees to accept greater risks to achieve certain financial rewards.

4.3 Compliance Committee

Has following roles

4.3.1 Ensure the Board, management, and employees comply with both internal policies and ethical standards, rules, and regulations.

4.3.2 Arrange for the assessment of regulatory impacts on business operations and consider the adequacy and appropriateness of internal controls to compliance risks.

4.3.3 Ensure all key compliance issues are recognized and integrated in day-to-day operations and ensure there are training, communication, and monitoring processes to ensure proper implementation.

4.3.4 Small- and medium-sized enterprises or those with business contexts that are irrelevant to complex rules and regulations may not need to appoint the Compliance Committee. Instead, the Board may assign such tasks to other Committees, such as Corporate Governance Committee or Audit Committee, etc.

4.4 Audit Committee

Has following roles

4.4.1 Audit corporate governance, risk and compliance practices and get audit report directly from external / internal auditors to ensure the company has effective, adequate, and appropriate internal controls to achieve GRC-related objectives. In summary, the Audit Committee is essential as it provides assurance that the company's operations are accurate, transparent, and accountable.

4.4.2 Given the Audit Committee's duties to monitor and audit overall operations of the company, the Board usually assigns the Committee to also oversee corporate governance, risk, and compliance. This is particularly the case for small- and medium-sized enterprises, and those with non-complex business operations.

Appendix GRC Health Check

Checklist	Issues	Yes	No
Board's Accountability			
1	The Board emphasizes and takes into account stakeholders' expectations in reviewing the appropriateness of long-term goals, strategy, and business model on a regular basis.		
2	The Board has concrete understanding of "risk management" that covers beyond measures to eliminate risks but also as early warning signs which are meant to point out weaknesses within "governance" as well as "compliance" system, and allow the Board to resolve such issues in timely manner.		
3	The Board has concrete understanding of compliance that covers more than mandatory requirements but also the aim to respond fairly to stakeholders' expectations and operate in accordance with ethics, best practices, and international standards.		
4	The Board aims to embed risk-aware culture and encourage the management to concretely adopt an integrated GRC program.		
5	The Board ensures that strategic planning process is conducted in parallel with risk management planning.		
6	The Board continuously monitors the implementation of such plans (specified in checklist no.5) by setting clear agenda in Board meetings.		
Structure / Policy / Business Process			
7	Governance, risk, and compliance structures are well integrated and not working in isolation.		
8	GRC-related roles and responsibilities of the Board and management are clearly defined.		
9	Delegation of GRC-related roles and responsibilities is clear and proper.		

Checklist	Issues	Yes	No
Structure / Policy / Business Process			
10	Management performance evaluation, rewards, and recognition helps promote GRC-related practices.		
11	GRC communication and report are conducted through efficient and effective channels.		
12	Ethical and honest business practices are seriously emphasized.		
13	Risk management system has been developed and implemented efficiently, effectively, and consistently.		
14	Compliance program has been developed and implemented efficiently, effectively, and consistently.		
15	Internal audit system has been developed and implemented efficiently and effectively.		
16	Corruption incident management system has been developed and implemented efficiently and effectively. It covers detection, response, and disciplinary action.		
17	GRC policy has been communicated with employees at all levels while implementation results are constantly monitored and reported.		
18	Information technology has been utilized for GRC integration.		

References

1. **A Maturity Model for Integrated GRC**, The Open Compliance and Ethics Group
2. **Corporate Governance Code**, The Office of Securities and Exchange Commission, 2017
3. **Corporate Governance in the Boardroom – A Practical Perspective**, Pricewaterhouse Coopers, 2015
4. **Corporate Governance Health Check – Increasing the Value of Your Business**, Pricewaterhouse Coopers, 2013
5. **COSO Enterprise Risk Management 2017**
6. **Enterprise Risk Management – Integrating with Strategy and Performance**, Committee of Sponsoring Organizations of the Treadway Commission (COSO), June 2017
7. **Fundamentals of GRC : The Connected Roles of Internal Audit and Compliance**, Thomson Reuters
8. **GRC Capability Model version 3.0**, The Open Compliance and Ethics Group
9. **G20/OECD Principles of Corporate Governance**, Organization for Economic Co-operation and Development (OECD), 2015
10. **Guidance on Board Effectiveness**, Financial Reporting Council (FRC), July 2018
11. **Implement GRC Lines of Defense to Improve Your Business Processes**, The Open Compliance and Ethics Group
12. **Should your Board have a separate Risk Committee**, Harvard Law School Forum, 2012
13. **Striking a Balance – Whistleblowing arrangements as part of a speakup strategy**, PwC, January 2011
14. **The Building Blocks of GRC**, The Open Compliance and Ethics Group, April 2016
15. **The UK Corporate Governance Code**, Financial Reporting Council (FRC), July 2018
16. **The GRC Toolbox – the Use of Integrated Methods to Fight Fraud**, Association of Certified Fraud Examiners, Fraud Magazine, September-October 2011

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