The Institute of
Internal Auditors
Malaysia

SORMIC GUIDE 2025

STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL (SORMIC)

Guidelines for Directors of Listed Companies

FOREWORD

The Statement on Risk Management and Internal Control (also known as the **SORMIC**) is a mandatory declaration, included in the annual reports of listed companies in Malaysia, to provide stakeholders with insights into the state of the risk management and internal control systems within listed companies.

The primary requirement for the SORMIC is set out in Paragraph 15.26(b) of BURSA's Listing Requirements (LR). This requirement is to be read in conjunction with Main Market Practice Note 9 and ACE Market Guidance Note 11, including any updates from time to time.

The SORMIC sets out the obligations of the Board of Directors (the Board) and Management with respect to risk management and internal control and describes the processes that are considered in reviewing its effectiveness. In making the statement, the Board of a listed company is required to explain its governance framework and policies, including any special circumstances that have led it to adopt a particular policy.

The purpose of the **SORMIC Guide** 2025 is to facilitate the Boards of listed companies in preparing the Statement on Risk Management and Internal Control **(SORMIC)** for publication in annual reports.

The SORMIC Guide 2025 provides an approach for the Board of a listed company to establish sound risk management and internal control systems, enhancing governance, transparency, and stakeholder confidence. The Board is responsible for oversight, while Management ensures implementation and effectiveness of the risk Management and internal control measures adopted by the company.

The SORMIC Guide 2025 also aligns with international best practices, as set by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), International Organization for Standardization (ISO), and The Institute of Internal Auditors (IIA). These standards reinforce accountability, strengthen governance frameworks and, enhance business resilience in a dynamic corporate environment.

Evolution of the Guide: The initial Guide for the Statement on Internal Control was introduced in December 2000 by an industry Task Force. It aimed to help directors of listed companies formulate their Statement on Internal Control in compliance with Bursa Malaysia Listing Requirements (Bursa LR).

Over the years, BURSA has taken significant steps to advance regulations, codes, and direction on risk management and internal control. These efforts have reshaped the frameworks underpinning SORMIC, driving transformative changes in industry practices among listed companies.

In 2012, the Guide was updated and renamed "The Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers". This revision reflected the evolving regulatory landscape and growing emphasis on corporate governance, making disclosure a vital aspect of informed investment decision-making.

Since 2012, there have been amendments and impactful changes to the BURSA LR, Malaysian Code on Corporate Governance (MCCG) and related guidelines.

Building on previous versions, the SORMIC Guide 2025 incorporates BURSA current LR, relevant aspects of the MCCG practices, and globally recognised standards. It also integrates insights and data from authoritative sources to provide practical, and actionable guidance for directors of listed companies.

Acknowledgements: The Task Force behind this publication extends its sincere thanks to the regulatory agencies, company directors, professional bodies, and industry experts for their valuable contributions through focus groups and consultations which have enhanced the relevance and applicability of the SORMIC Guide 2025.

We are confident that the SORMIC Guide 2025 will provide the Board of listed companies with the guidance and tools to meet BURSA's disclosure requirements.

Chairman of the Task Force
Date: **26 August 2025**

TASK FORCE MEMBERS

RESEARCH AND TECHNICAL ADVISORY COMMITTEE (RTAC) – IIAM

Mohd Khaidzir Shahari
Task Force Chairman
Former President, IIAM
CEO, Lembaga Zakat Selangor

Ainon Mahat
General Manager of Internal Audit,
Malaysia Airports Holdings Berhad

Prof Dr Susela Devi
Honorary Professor, Faculty of Business and Accountancy, Universiti Selangor (UNISEL)

Steven Kho Chai Huat
Head of Internal Audit
Sarawak Energy Berhad

Assoc. Prof. Dr Eddy Yap Tat Hiung
Founder and Managing Consultant
CONDUCTIVITI Business Advisory Sdn Bhd

Datin Shamita Atputharaja
Director of Internal Audit
Bursa Malaysia Berhad

MEMBERS

Arivintha Raj Anparessu
Director, Ernst & Young Consulting Sdn Bhd.

Chang Ming Chew
Representative, Former ISACA Malaysia Chapter
Managing Director, Axcelasia Sdn Bhd

Dominic Chegne How Kooi
Partner, PwC Malaysia

Dr Ismet Al-Bakri bin Yusoff Al-Bakri
CEO, Minority Shareholders Watch Group ("MSWG")

Seline Goh Sek Lian
Director, Controls Assurance Practice,
Deloitte Asia Pacific

Sujatha Sekhar Naik
Chairman, Malaysian Institute of Corporate Governance ("MICG")

Chan Chee Keong
Partner, KPMG Malaysia

YBhg Dato Billy Goh Soo Wee
Vice President, Federation of Public Listed Companies Bhd ("FPLSB")

Dipa Kaur
Deputy President, The Malaysian Institute of Chartered Secretaries and Administrators ("MAICSA")

Faizatul Farhah Ghazali
Former Chairman, Malaysian Association of Risk and Insurance Management ("MARIM")

Michele Kythe Lim Beng Sze
Founding President & CEO, The Institute of Corporate Directors Malaysia ("ICDM")

Simon Tay Pit Eu
Executive Director, Professional Practices and Technical, Malaysian Institute of Accountants ("MIA")

Assoc. Prof. Dr Sherliza Puat Nelson
Research and Publication Committee
Malaysian Accounting Association ("MyAA")

TASK FORCE MEMBERS

SECRETARIAT

Geetha Kanny
Executive Director, The Institute of Internal Auditors Malaysia (IIA Malaysia)

Hong Kah Ann
Assistant Manager, Technical & Quality Assurance, The Institute of Internal Auditors Malaysia (IIA Malaysia)

Alyssa Hew Li Min
Head, Technical & Quality Assurance, The Institute of Internal Auditors Malaysia (IIA Malaysia)

OBSERVERS

Jimmy Tium Beng Teck
Deputy Director, Internal Audit Department, Securities Commission Malaysia

Mohamad Azhar Mohamad Hamidi
Executive Vice President, Corporate Surveillance & Governance, Bursa Malaysia Berhad

TECHNICAL WRITERS

Devanesan Evanson
Technical Writer

Vanajah Shanmugam
Assistant Technical Writer

CONTENTS

1. CLARIFYING KEY TERMS

GLOSSARY

TERM	DEFINITION
ACE Market	A growth-oriented market within BURSA, designed for companies with high growth prospects. It's a sponsor-driven market, meaning companies seeking to list must have an approved sponsor who assesses their suitability.
Board	The highest-level governing body of a company responsible for setting strategy, overseeing Management, and protecting the interests of shareholders and other stakeholders.
Bursa Malaysia Berhad (BURSA)	The stock exchange in Malaysia, serving as the primary platform for trading securities and derivatives.
Committee of Sponsoring Organizations of the Treadway Commission (COSO)	A private sector initiative that developed a framework for internal control and enterprise risk management. This framework is a widely recognized set of guidelines for organisations to evaluate, design, and implement effective internal controls.
Committee of Sponsoring Organizations (COSO) Enterprise Risk Management (COSO ERM)	A widely recognised model for managing risks across an entire organisation. It helps organisations understand and manage risks related to their strategy, objectives, and overall performance. The framework emphasises the importance of integrating risk management into the organisation's culture, strategy, and operations.
Environmental, Social and Governance (ESG)	A set of standards that is used to evaluate the sustainability and ethical impact of an organisation. Using the ESG framework as a guideline can help you assess risks, and mitigate potential issues that can be costly, if left unaddressed.
Greenhouse gases (GHG)	Atmospheric gases that trap heat, contributing to the greenhouse effect and global warming.
International Organization for Standardisation (ISO)	An independent, non-governmental international body that develops and publishes voluntary global standards to promote quality, safety, efficiency, and interoperability across industries.
International Sustainability Standards Board (ISSB)	A standard-setting body established by the International Financial Reporting Standards (IFRS) Foundation to develop standards that will result in a high quality, comprehensive global baseline of sustainability disclosures focused on the needs of investors and the financial markets.
Listed Companies	Companies whose securities are listed and traded on BURSA Main Market and ACE Market.
Listing Requirements / LR	Collectively, the Main Market Listing Requirements and ACE Market Listing Requirements of BURSA.
Main Market	Main Market is the prime market for established companies that have met the standards in terms of quality, size and operations, listed on BURSA. Potential issuers for the Main Market must demonstrate that they have achieved minimum profit track record or minimum size measured by market capitalisation.

1. CLARIFYING KEY TERMS

GLOSSARY (continued)

TERM	DEFINITION
Malaysian Code on Corporate Governance (MCCG)	A set of principles and practices issued by the Securities Commission Malaysia (SC) to enhance corporate governance of listed companies and promote accountability, transparency, and sustainability.
Minority Shareholders Watch Group (MSWG)	An independent, not-for-profit organisation established to protect the interests of minority shareholders and promote greater transparency and accountability among listed companies in Malaysia.
National Sustainability Reporting Framework (NSRF)	A framework developed by Securities Commission Malaysia (SC) to address the use of the IFRS® Sustainability Disclosure Standards issued by the International Sustainability Standards Board (ISSB), specifically the IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information, and IFRS S2 Climate-related Disclosures (collectively referred to as the ISSB Standards), as the baseline sustainability disclosure standards for companies in Malaysia, as well as the assurance requirements for sustainability reporting.
Other Sustainability Risks	Material risks that fall outside ESG risks but still have a significant ESG dimension and can affect the company's ability to meet its objectives, create value, or maintain compliance.
Task Force on Climate-related Financial Disclosures (TCFD)	A framework established in 2015 by the Financial Stability Board (FSB) to guide organisations in disclosing climate related governance, strategy, risk management, and metrics/targets, enhancing transparency and capital-market alignment.
The EU's Corporate Sustainability Reporting Directive (EU CSRD)	A framework that requires companies to disclose information about their ESG performance.
The IIA's Three Lines Model	The Model helps organisations identify structures and processes that best assist the achievement of objectives and facilitates strong governance and risk management.
The Institute of Internal Auditors (IIA)	A global professional association for internal auditors that establishes the International Standards for the Professional Practice of Internal Auditing (IPPF).
The Institute of Internal Auditors Malaysia (IIAM)	The recognised national institute in Malaysia affiliated with The Institute of Internal Auditors (IIA) globally, established to develop and promote the internal audit profession in Malaysia.
The Taskforce on Nature-related Financial Disclosures (TNFD)	An international, market-led and science-based initiative supported by governments and regulatory bodies, to provide a structured set of recommendations to help organisations disclose and manage dependencies, impacts, risks, and opportunities related to nature, ultimately supporting a global shift from nature-negative to nature-positive financial and business decisions.

2. ALIGNING THE STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL WITH PREVAILING REGULATORY REQUIREMENTS

2.1 Objective of the SORMIC Guide 2025

The primary objective of the SORMIC Guide 2025 is to assist the Board of Directors of listed companies (the Board) in making the Statement on Risk Management and Internal Control, as required by BURSA LR and Main Market Practice Note 9, and ACE Market Guidance Note 11.

2.2 The **SORMIC Guide 2025,** in line with prevailing requirements for the **Statement on Risk Management and Internal Control (Statement)** as outlined in BURSA LR, intends to provide listed companies with **a structured approach** to:

a) communicate the companies' risk management and internal control practices, policies and frameworks in public disclosures, including annual reports and/or corporate governance statements.

b) outline the responsibilities of the Board and Management of a listed company concerning risk management and internal control.

c) identify key elements for maintaining a robust risk management and internal control system.

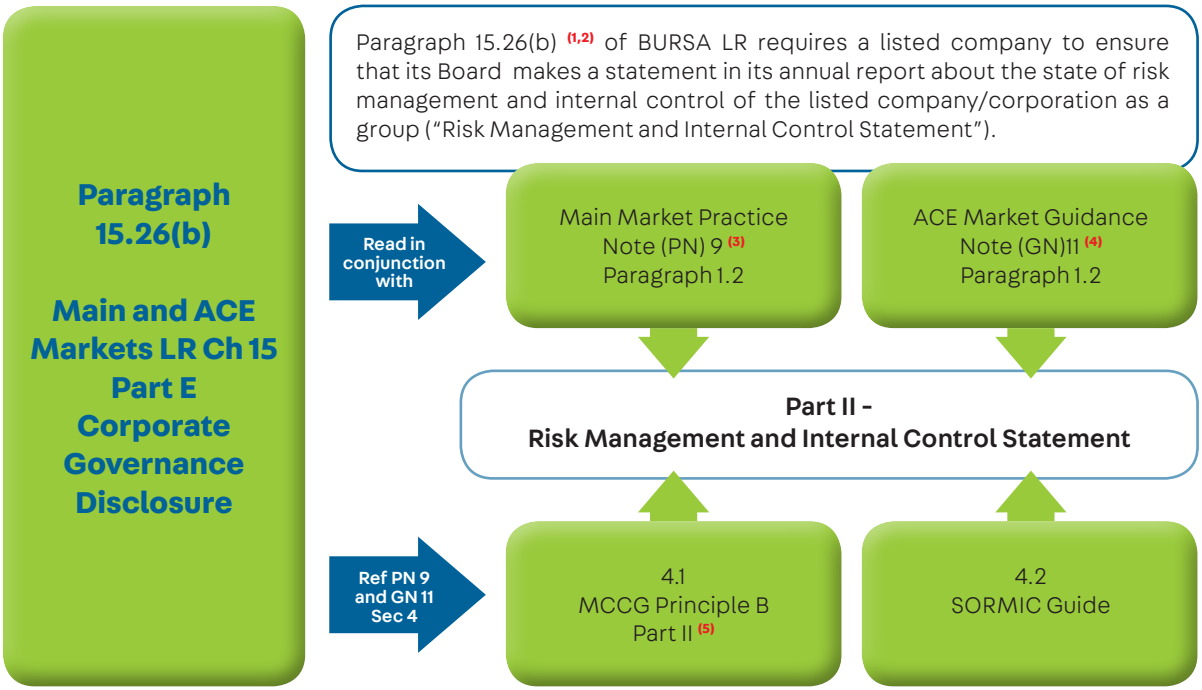
d) detail the process for evaluating the effectiveness of risk management and internal control system in place.

e) declare that the company's risk management and internal control systems are operating adequately and effectively, through assurances provided by the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) to the Board.

f) communicate the Board's oversight and approvals on the disclosures under (a) above.

2.3 Regulatory Context for Listed Companies

In making the Statement, the listed company is required to comply with the BURSA LR, summarised as follows:



2. ALIGNING THE STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL WITH PREVAILING REGULATORY REQUIREMENTS

2.4 Notes and Appendices

a) The following pages of explanatory notes on Risk Management and Internal Control provide the Board, risk management professionals and others involved, with the necessary knowledge, guidance and frameworks to formulate the Statement on Risk Management and Internal Control for a listed company.

b) References to relevant standards and authoritative bodies (with links) have been included in the respective sections for quick access and validation.

c) In the context of the SORMIC Guide 2025, Company and Group are defined as follows:

- **Company:** an individual listed company or corporation that is subject to corporate governance principles and practices as outlined in the MCCG. This includes listed companies on BURSA.

- **Group:** a listed company and its subsidiaries collectively. It encompasses the parent company (holding company) and all subsidiaries under its control, ensuring that corporate governance practices extend beyond just the listed entity to its broader business structure.

d) If material joint ventures and associate companies are excluded from the group for the purposes of these guidelines, these should be disclosed with an explanation.

e) The appendices to the SORMIC Guide 2025 contain questions that Boards should consider when applying the SORMIC Guide 2025 approach and recommendations.

3. DEFINING GOVERNANCE, RISK MANAGEMENT AND INTERNAL CONTROL

In making the Statement on Risk Management and Internal Control, **BURSA,** through Practice Note 9 of the Main Market LR and Guidance Note 11 of the ACE Market LR, requires listed companies to address Part II Risk Management and Internal Control Framework of MCCG's **Principle B** Effective Audit and Risk Management.

Principle B sets out the rationale for adopting a cohesive approach to integrating governance, risk management, and internal control within a company, as reflected in the following two intended outcomes:

3.1 Intended Outcome 10.0

Companies make informed decisions about the level of risk they want to take and implement necessary controls to pursue their objectives.

The Board is provided with reasonable assurance that adverse impact arising from a foreseeable future event or situation on the company's objectives is mitigated and managed.

Practice 10.1	The Board should establish an effective risk management and internal control framework.
Guidance G10.1	The Board should determine the company's level of risk tolerance and actively identify, assess and monitor key business risks to safeguard shareholders' investments and the company's assets. Internal controls are important for risk management and the Board should be committed to articulating, implementing and reviewing the company's internal control framework.
Practice 10.2	The Board should disclose the features in its risk management and internal control framework, and the adequacy and effectiveness of this framework.
Guidance G10.2	The Board should, in its disclosure, include a discussion on how key risk areas such as finance, operations, regulatory compliance, reputation, cyber security and sustainability were evaluated and the controls in place to mitigate or manage those risks. In addition, it should state if the risk management framework adopted by the company is based on an internationally recognised risk management framework. The Board should also disclose whether it has conducted an annual review and periodic testing of the company's internal control and risk management framework. This should include any insights it has gained from the review and any changes made to its internal control and risk management framework arising from the review. Where information is commercially sensitive and may give rise to competitive risk, disclosure in general terms is acceptable.
Practice 10.3	**Step-Up:** The Board establishes a Risk Management Committee, which comprises a majority of independent directors, to oversee the company's risk management framework and policies.

3. DEFINING GOVERNANCE, RISK MANAGEMENT AND INTERNAL CONTROL

3.2 Intended Outcome 11.0

Companies have an effective governance, risk management and internal control framework and stakeholders are able to assess the effectiveness of such a framework.

Practice 11.1	The Audit Committee should ensure that the internal audit function is effective and able to function independently.
Practice 11.2	The Board should disclose– • whether internal audit personnel are free from any relationships or conflicts of interest, which could impair their objectivity and independence. • the number of resources in the internal audit department. • name and qualification of the person responsible for internal audit, and • whether the internal audit function is carried out in accordance with a recognised framework.
Guidance G11.1	In developing the scope of the internal audit function, the Audit Committee should satisfy itself that– • the person responsible for internal audit has relevant experience, sufficient standing and authority to enable him to discharge his functions effectively. • internal audit has sufficient resources and is able to access information to enable it to carry out its role effectively, and • the personnel assigned to undertake internal audit have the necessary competency, experience and resources to carry out the function effectively. Internal auditors should continuously keep abreast with developments in the profession, relevant industry and regulations to ensure they are able to perform their role effectively including undertaking root-cause analysis to provide strategic advice and suggest meaningful business improvements.

4 MAPPING ELEMENTS OF A SOUND RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

4.1 Risk Management

A sound risk management framework integrates with the company's culture, processes, and structures. The framework should be adaptable to changes and clearly communicated across all levels. An adequate and effective control environment and Board oversight play an integral part in managing risk.

ISO 31000 is an internationally recognised standard for risk management that provides guidelines for identifying, assessing, and mitigating risks across various industries.

Incorporating ISO 31000 offers several benefits.

- **Consistency:** provides a standardised language and approach across departments and industries.
- **Accountability:** clarifies roles and responsibilities in risk management.
- **Strategic Alignment:** ties risk management directly to organisational objectives and decision-making.
- **Scalability:** applies to organisations of all types and sizes.

4.2 Key Elements of Risk Management

The following elements represent key components of a sound risk management system, in alignment with established frameworks such as ISO 31000 and COSO ERM.

a) Control Environment

- Written values, codes of conduct, policies, and procedures.
- Management's philosophy, risk attitude, and operating style aligned with Board-approved risk appetite.
- Documented roles and responsibilities for the Board, Committees, and Directors (via a set of charters), and/or terms of reference.
- Clear organisational structure and assignment of authority and responsibility.
- Commitment to competence: This includes ensuring that employees have the necessary knowledge, skills, and expertise to perform their duties, and that there is a process in place for recruiting, developing, and retaining competent staff. This is to align with COSO Principle 4, which emphasises the importance of attracting, developing, and retaining competent individuals. There should also exist a process for holding individuals accountable for their internal control responsibilities.

b) Board Oversight

The Board's ability to oversee a company's Management of risks starts with actively participating in the objective and strategy-setting process, ensuring that the risks inherent in each option are considered. The Board should subsequently receive sufficient and timely information concerning both performance and risk levels so that Management's performance in achieving strategies and objectives can be monitored and assessed.

- Actively participate in setting objectives and strategies, ensuring inherent risks are considered.
- Monitor performance and assess risks with timely and adequate information.
- Collaborate with Management to:
  - determine and communicate risk appetite and tolerance.
  - ensure adequacy of risk management practices.
  - review current risk levels relative to appetite and assess performance.
  - act promptly when risks exceed tolerable limits.

4 MAPPING ELEMENTS OF A SOUND RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

- To ensure a sound system of risk management and internal control, Boards and Management must periodically assess its adequacy and effectiveness. Boards and Management should ensure that Key Performance Indicators (KPIs) and other metrics are established and monitored to assess the adequacy and effectiveness of the risk management and internal control systems. These measures should reflect the company's risk appetite, regulatory obligations, and operational priorities, enabling timely identification of weaknesses and continuous improvement.

  These could include:
  - metrics for **risk mitigation effectiveness.**
  - indicators for **compliance with internal policies and regulatory requirements.**
  - metrics for Board-level oversight: e.g., the percentage (%) of key risks reviewed quarterly.
  - details of incident frequency/severity.
  - identifying risk exposure trends.
  - aligning of risk levels with the Board-approved risk appetite.

4.3 Internal Control

An internal control system comprises the policies, processes, and behaviours that collectively provide the required level of assurance for achieving operational, reporting, and compliance objectives.

a) *To enhance:* supports effective operations by addressing key business, operational, financial, compliance, and **other risks** to achieve company objectives.

b) *To ensure:* maintains proper records and processes to generate timely, relevant, and reliable internal and external information.

c) *To promote:* upholds adherence to laws, regulations, and internal policies governing business conduct.

4.4 Key components of Internal Control

The effectiveness of a company's internal control system is shaped by its control environment, which includes organisational structure, governance, human resource related policies and practices, and the code of conduct.

The most-widely recognised framework for internal control [6] is published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

The COSO Framework provides principles for designing, implementing, and evaluating internal control systems. It is widely used for ensuring compliance, operational efficiency, and financial reporting integrity.

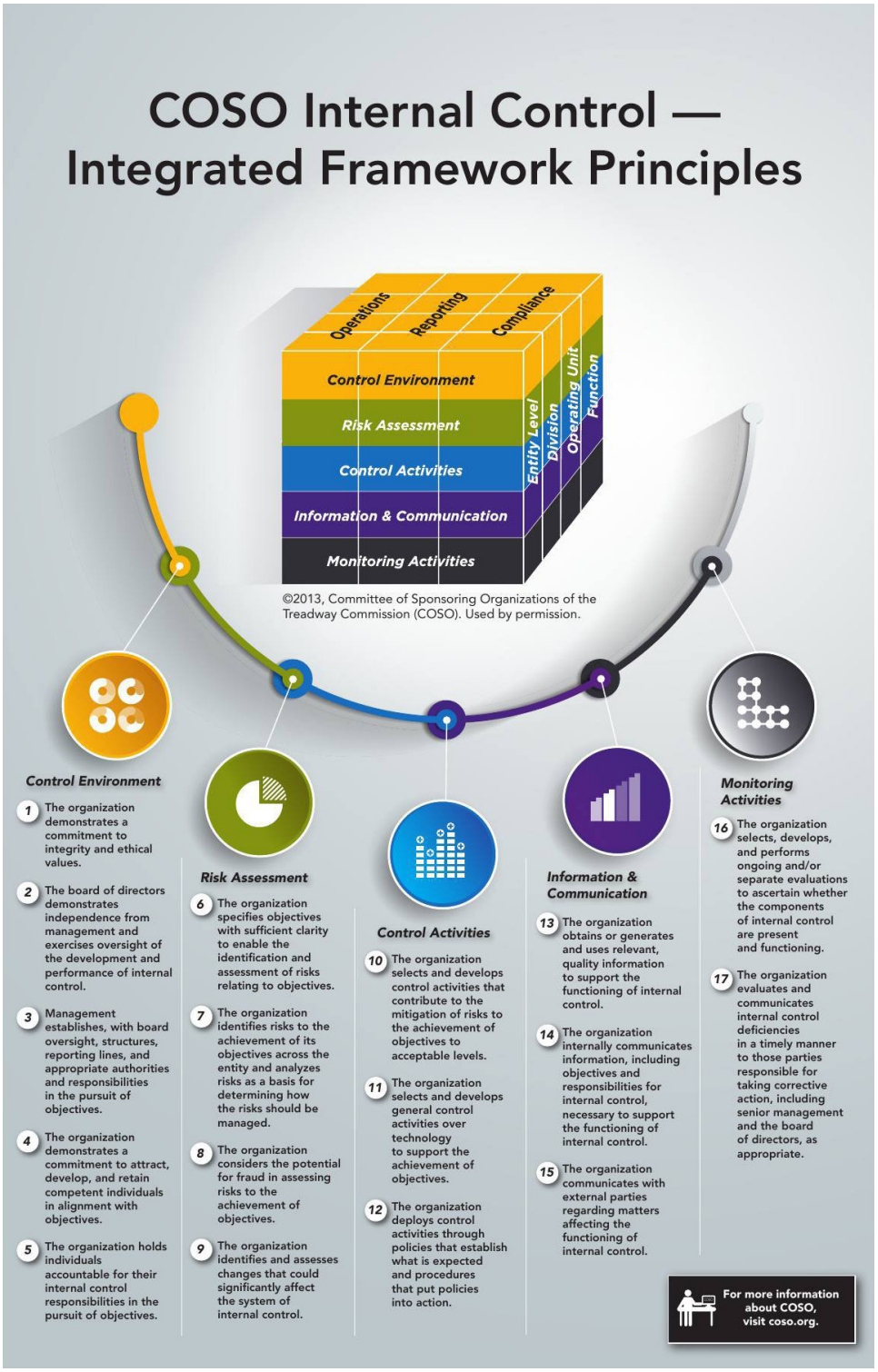
The holistic approach forms the basis for a dynamic relationship and is often illustrated using a cube (see diagram below), emphasising how each dimension influences and supports the others across all levels of the organisation.

a) The **three categories of objectives** to guide the purpose – operations, reporting, and compliance, represented by the columns.

b) The **five components,** the elements required to achieve those objectives, represented by the rows.

c) The entity's **organisational structure, defining the channels through which action occurs** (its operating units, legal entities, and governance arrangements), represented by the third dimension.

4 MAPPING ELEMENTS OF A SOUND RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM



4.5 Components and Principles

For purposes of the COSO framework, the term "organisation" is used to collectively capture the Board, Management, and other personnel, as reflected in the definition of internal control.

In the diagram above, the Framework sets out seventeen principles representing the fundamental enterprise Risk Management (ERM) processes. The COSO Internal Control – Integrated Framework Principles support listed companies in operationalising ESG and other sustainability risks integration.

4 MAPPING ELEMENTS OF A SOUND RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

4.6 Board Considerations

In evaluating a sound internal control system, the Board should assess:

a) the **nature** and **extent** of risks.

b) the **acceptable risk levels** and sources.

c) the likelihood and **impact of significant risks.**

d) the ability to **mitigate and manage** risk impacts effectively.

e) the **cost-benefit analysis** of controls.

f) the **effectiveness reviews** of the system from time to time, as is reasonably necessary to maintain oversight and assurance.

g) the **comparison** of current performance with **prior periods** or **benchmarks.**

h) the **insights** from audit findings, risk events, or near misses.

4.7 Limitations and Indicators

As governance practices evolve, it is important to recognise the limitations and indicators that have surfaced through the practical application of the SORMIC framework. While SORMIC has strengthened corporate governance practices, certain limitations remain that Boards and companies must acknowledge:

a) Inherent Limitations of Risk Management and Internal Control

Even the most robust systems cannot fully eliminate risks due to:

- human error or poor judgment, which may occur despite controls.
- intentional circumvention or Management override of established controls.
- unforeseeable events that fall outside the scope of anticipated risks.

b) Variability in Quality of Disclosures

- smaller companies often rely on boilerplate disclosures, reducing the effectiveness of the SORMIC Guide 2025 in driving meaningful transparency and accountability.

c) Gaps in Addressing Emerging Risks

- past applications of SORMIC have shown minimal focus on forward-looking or emerging risks, such as technological disruptions (e.g., AI) and climate-related risks, which are increasingly relevant.

d) Under-reporting of Internal Control Weaknesses

- despite clear recommendations, there is limited disclosure of internal control weaknesses, indicating a need for stronger Board engagement and assurance mechanisms.

e) Indicators of Control Ineffectiveness

These performance indicators are used to assess the effectiveness of internal controls and signal potential weaknesses:

- control Failure Rate – how frequently controls fail to operate as intended.
- deficiency Resolution Rate – the ratio of control deficiencies identified versus those resolved.
- timeliness of Remediation – the time taken to address and close control issues once identified.

4 MAPPING ELEMENTS OF A SOUND RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

4.8 Addressing Challenges Related to ESG and Other Sustainability Risks

Sustainability risks extend beyond ESG risks to include other sustainability risks that may materially affect a company's ability to achieve its objectives, maintain resilience, and meet stakeholder expectations. These risks can be interconnected, long-term in nature, and often cross traditional risk categories, requiring Boards to adopt an integrated, forward-looking approach.

The Board should ensure that ESG and other sustainability risks are embedded within the company's overall risk management and internal control framework, rather than addressed as stand-alone issues.

This involves:

a) Integration of ESG and Other Sustainability Risks

- Incorporating related risks – including climate, biodiversity, social, and other material sustainability factors – into existing risk identification, assessment, and monitoring processes.
- Mapping these risks to strategic objectives and operational plans, ensuring they are reflected in risk registers, control activities, and reporting mechanisms.
- Considering both direct impacts (e.g., carbon emissions, workforce diversity) and indirect impacts (e.g., supply chain practices, regulatory changes) that may influence the company's risk profile.
- Establishing clear accountability for ESG and other sustainability risk oversight at Board and Management levels, supported by relevant expertise and reporting structures.

b) Sustainability Control Guidance

- Incorporating practical measures from COSO's 2023 Supplemental Guidance: Achieving Effective Internal Control Over Sustainability Reporting (ICSR) [7] which applies the well-established COSO Internal Control–Integrated Framework to enhance controls over ESG and other sustainability-related risk reporting, including greenhouse gas (GHG) emissions [8].

c) Mapping of SORMIC Principles to ISSB Standards

The Statement on Risk Management and Internal Control (SORMIC) addresses ESG and other sustainability risks in alignment with the standards issued by the International Sustainability Standards Board (ISSB) and the National Sustainability Reporting Framework (NSRF) issued by the Securities Commission Malaysia, which operationalises these standards domestically.

The four-pillar structure of Governance, Strategy, Risk Management, and Metrics & Targets–originally forming the foundation of the Task Force on Climate-related Financial Disclosures (TCFD) [9] disclosure framework–together with the TCFD recommendations, has been fully subsumed into the ISSB's International Financial Reporting Standards (IFRS) S1 [10] and IFRS S2 [11].

4 MAPPING ELEMENTS OF A SOUND RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

The following table illustrates how certain IFRS S1 and S2 disclosure requirements and the TCFD pillars could be aligned and addressed in the SORMIC framework in Malaysia.

SORMIC FOCUS AREA	IFRS S1 / S2 REFERENCE
Board oversight of risk and internal control	S1 §9(a) – Governance processes for sustainability oversight
Identification and evaluation of material ESG risks	S1 §9(b); S2 §10(a) – Sustainability and climate risk identification
Integration of ESG risks into strategic planning	S2 §10(b)(i–iv) – Climate-related strategy and financial planning
Management accountability and implementation	S1 §9(d); S2 §10(c) – Risk response and resource allocation
Internal control system design and effectiveness	S1 §9(c) – Processes to monitor, review, and adjust controls
Metrics, KPIs, and control monitoring	S2 §10(e–f) – GHG metrics, targets, and progress disclosure
Disclosure of assurance and significant failings	S1 §9(e); S2 §10(g) – Internal and external assurance processes

Footnote:
The IFRS S1 and IFRS S2 Standards, issued by the ISSB in June 2023, incorporate the four-pillar disclosure framework of the Task Force on Climate-related Financial Disclosures (TCFD). The Financial Stability Board (FSB) announced the conclusion of the TCFD's work in October 2023, with responsibility for monitoring and supporting climate-related disclosure adoption formally transferred to the IFRS Foundation and ISSB. In Malaysia, the National Sustainability Reporting Framework (NSRF) provides the domestic reporting architecture to implement and align with these global standards.

d) Scenario Analysis and Forward-looking Risk

Embedding scenario planning and assessment of emerging risks, such as AI, cyber, and climate risks, into Board risk oversight processes.

See **Appendix I** which provides a comprehensive list of key risks, including business continuity, digital disruption, geopolitical and supply chain vulnerabilities, besides others.

e) Alignment with Global Standards

Building on existing sustainability and risk management practices, organisations are increasingly aligning with globally recognised frameworks to enhance comparability and transparency in disclosures, such as:

- EU CSRD [12] (Corporate Sustainability Reporting Directive).
- TNFD [13] (Task Force on Nature-related Financial Disclosures).

5 ASSIGNING ROLES AND RESPONSIBILITIES FOR EFFECTIVE RISK MANAGEMENT AND INTERNAL CONTROL

A robust and effective framework for risk management and internal control requires all stakeholders within the organisation to fulfil their respective roles effectively.

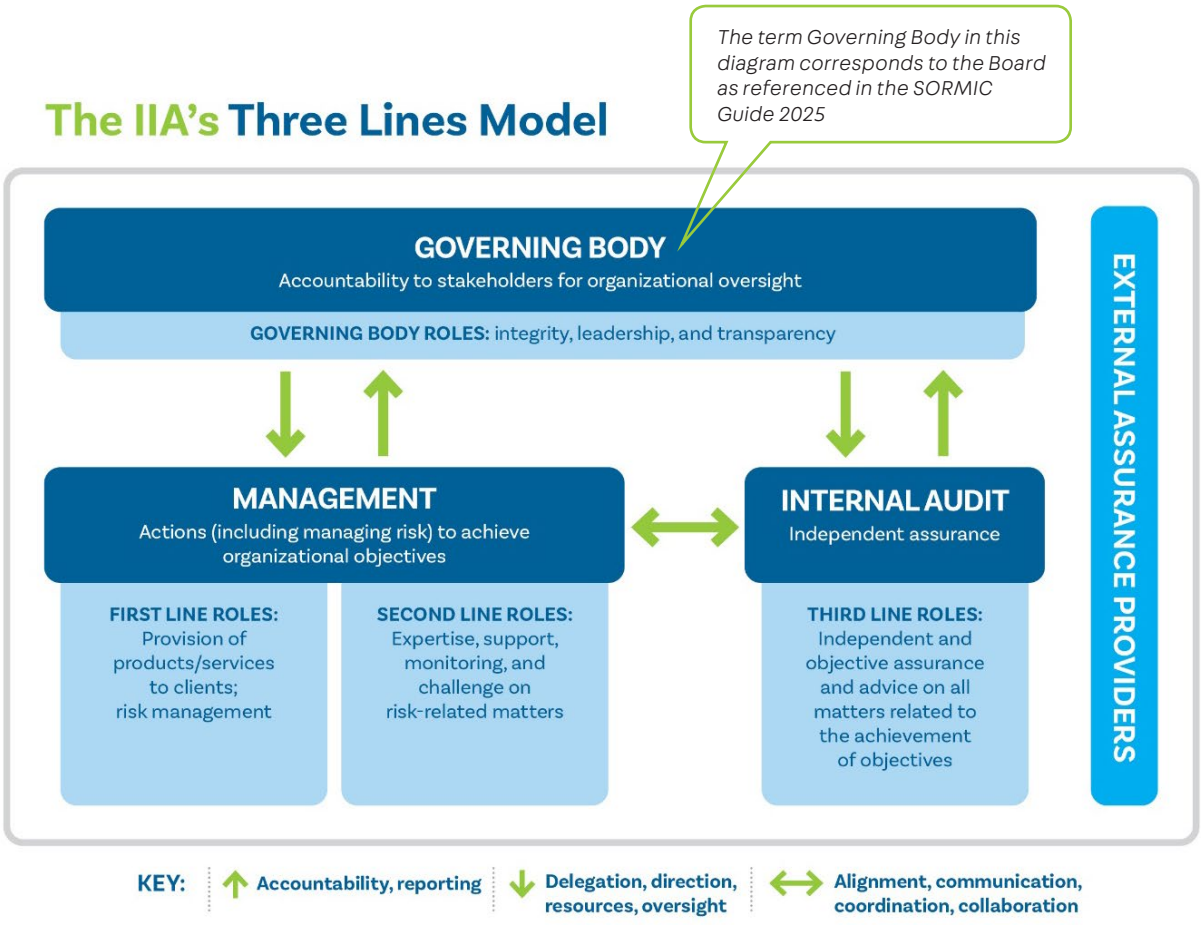
5.1 The IIA's Three Lines Model [14] is optimised by:

a) adopting a principle-based approach and adapting the model to suit organisational objectives and circumstances.

b) focussing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of "defence" and protecting value.

c) clearly understanding the roles and responsibilities represented by the model and the relationships among them.

d) implementing measures to ensure activities and objectives are aligned with the polarised interests of stakeholders.



5 ASSIGNING ROLES AND RESPONSIBILITIES FOR EFFECTIVE RISK MANAGEMENT AND INTERNAL CONTROL

5.2 Key Roles and Responsibilities in the Three Lines Model

Organisations differ considerably in their distribution of responsibilities. However, the following high-level roles serve to amplify the Principles of the Three Lines Model.

a) The Board

The Board's focus on effective risk oversight is critical to setting the tone and culture towards effective risk management and internal control. The responsibilities of the Board for the governance of risk and controls should include:

NO	RESPONSIBILITIES	DESCRIPTION OF GOVERNANCE
1	Accountability & Delegation	• Has clear terms of references for the Board Charter, Board Committees and delegation of authority limits to Management. • Ensures Management is responsible for implementation and execution. • Assigns oversight tasks while retaining final accountability for decisions within the Board's remit.
2	Governance & Strategic Oversight	• Ensures a risk-aware culture is embedded throughout the organisation. • Integrates risk considerations into corporate strategy and key decision-making. • Oversees transparency, ethical conduct, and regulatory compliance. • Evaluates and enhances the organisation's overall governance, risk Management, and internal control framework.
3	Monitoring & Engagement with Assurance Providers	• Oversees the adequacy and effectiveness of the risk Management and internal control system. • Evaluates whether key risks affecting the achievement of objectives are effectively identified, managed, and mitigated. • Ensures compliance with Paragraph 15.27(2) [15] of BURSA LR, including maintaining an internal audit function that is independent and reports directly to the Audit Committee. • Reviews consolidated risk and control information from Management, internal audit, and external audit at appropriate intervals. • Approves and periodically reviews the internal audit plan and assesses the performance and independence of the internal audit function. • Engages with internal and external assurance providers to validate the effectiveness of internal controls and identify areas for improvement. • Ensures the risk management framework provides reasonable assurance that material risks are appropriately addressed and escalated. • Uses internal audit as an independent function to provide assurance on internal controls and risk processes. • Uses external audit to obtain independent validation of financial risk controls. • Leverages assurance reports to support oversight of risk and control effectiveness.
4	Risk Appetite & Policy Setting	• Defines and approves acceptable risk appetite and tolerances for the organisation. • Reviews and endorses risk management policies and frameworks. • Ensures alignment between risk appetite, corporate objectives, and operational decisions.

5 ASSIGNING ROLES AND RESPONSIBILITIES FOR EFFECTIVE RISK MANAGEMENT AND INTERNAL CONTROL

b) Management – First-Line Roles (CEO and CFO)

- Lead and direct actions (including managing risk) and application of resources to achieve the objectives of the organisation.
- Establish and maintain appropriate structures and processes for the Management of operations and risk (including controls).
- Ensure compliance with legal, regulatory, and ethical expectations.
- Implement risk management policies and internal controls within the organisation.
- Facilitate alignment between strategy execution, risk management, and performance objectives.

While primarily first-line, the CEO and CFO have a dual-facing role.

- **To the Board** – they report on performance, risk exposure, and internal control effectiveness, providing assurance.
- **To assurance providers (e.g., internal audit)** – they cooperate and support assurance activities while not being independent themselves.
- **Signing off** on internal control statements or disclosures, where applicable, to reflect Management's accountability.

c) Management – Second-Line Roles

Provides complementary expertise, support, monitoring and challenge related to the management of risk, including:

- the development, implementation, and continuous improvement of risk management practices (including controls) at a process, systems, and entity level.
- the achievement of risk management objectives, such as compliance with BURSA LR regulations, and acceptable ethical behaviour, controls, information and technology security, sustainability, and quality assurance.
- the provision of analysis and reports on the adequacy and effectiveness of risk management (including controls).

d) Internal Audit Function - Third-Line Role

- Maintains primary accountability to the Board, and independence from the responsibilities of Management.
- Communicates independent and objective assurance and advice to Management and the governing body on the adequacy and effectiveness of governance and risk management (including controls) to support the achievement of organisational objectives and to promote and facilitate continuous improvement.
- Reports impairments to independence and objectivity to the governing body and implements safeguards as required.

e) External Assurance Providers

Provides an addendum to the three-lines model to obtain additional assurance to:

- satisfy legislative and regulatory expectations that serve to protect the interests of shareholders.
- satisfy requests by Management and the governing body to complement internal sources of assurance.

6 EVALUATING THE EFFECTIVENESS OF RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS

6.1 Board's Responsibility

Ongoing and Annual Assessments: The Board must establish clear processes for continuous and annual evaluations of the risk management and internal control system's effectiveness, including compliance with regulatory requirements (e.g., LR 15.26(b)).

6.2 Key Considerations for Assessment

a) Strategic Alignment:

- processes for setting long-term and short-term objectives, considering associated risks.
- determination and communication of the company's risk appetite.

b) Policies and Procedures:

- adequacy of risk management and internal control policies and procedures.

c) Risk Management Processes:

- identification, analysis, evaluation, and treatment of risks.
- communication of risk and control information across the business.

d) Monitoring and Adaptation:

- processes for monitoring and adjusting controls as business conditions or risks evolve.

e) Visibility of Risks:

- Management's reporting to ensure the Board has comprehensive insight into organisational risks.

6.3 Ongoing Assessment

a) Management Reporting: Periodic updates to the Board on:

- business risks affecting the company's objectives and strategies.
- effectiveness of the risk management and internal control system in addressing those risks.

b) Review of Management Reports

The Board should:

- identify and evaluate significant risks and how they are managed.
- assess the effectiveness of internal controls, addressing any significant failings or weaknesses reported.
- ensure prompt corrective actions are taken for significant failings or weaknesses.
- verify the presence and communication of early warning indicators for potential risk events.
- determine if findings necessitate more extensive monitoring of risk management and internal controls.
- evaluate emerging risks and ensure appropriate controls are in place.

6 EVALUATING THE EFFECTIVENESS OF RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS

6.4 Annual Assessment

The Board's annual assessment should:

a) Include the review of issues addressed in reports throughout the year, supplemented by additional information covering all significant risks and internal control aspects.

b) Focus on:
- changes in significant risks and the company's responsiveness to internal and external changes.
- effectiveness of risk management and internal control systems.
- contributions of internal audit, risk management, and other assurance providers.
- communication of monitoring results to the Board or its committees.
- significant control failings or weaknesses and their impact on company performance and/or condition.
- any events that impacted the achievement of objectives that were not anticipated by Management.
- overall adequacy and effectiveness of risk management and internal control policies.
- review and evaluate the credibility and sufficiency of assurances provided by the CEO and CFO on the design and operating effectiveness of the risk and control systems.

6.5 Assurances

The Board should assess whether Management processes provide reasonable assurance that significant risks are managed within acceptable levels aligned with the company's strategies and objectives.

Appendix II outlines key questions the Board needs to ask itself prior to making the Statement on Risk Management and Internal Control.

7 DRAFTING THE BOARD'S STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL

The disclosure requirements for the Statement must be made pursuant to Paragraph 15.26(b) of BURSA LR. The Statement should provide shareholders with sufficient and meaningful information to assess the main features and adequacy of the company's risk management and internal control system.

The Board's narrative statement should include the following aspects:

7.1 Key Features

Main aspects of the risk management and internal control system.

7.2 Risk Management Process

a) Ongoing processes for identifying, evaluating, and managing significant risks in achieving objectives and strategies.
b) Confirmation that these processes were in place for the year under review and up to the approval date of the statement.

7.3 Review and Actions

a) The process used (by the Board or via Board committees) to review the system and address any significant failings or weaknesses identified.
b) Assurance that actions have been or are being taken to remedy such issues.

7.4 Adequacy and Effectiveness

a) A review of the system's adequacy and effectiveness, along with commentary on its performance.
b) The approach to managing material internal control aspects of significant problems disclosed in the annual report and financial statements.

7.5 Joint Ventures and Associates

Disclosure if material joint ventures or associates are excluded from the group in applying these guidelines with explanations rendered.

7.6 CEO and CFO Assurances

The narrative statement should also indicate if the Board has received assurance from the CEO and CFO on whether the company's risk management and internal control system is operating adequately and effectively.

8 RISK APPETITE: KEY CONCEPTS AND CONSIDERATIONS

8.1 Definition and Characteristics of Risk Appetite

a) Risk Appetite: The level of risk a company is willing to accept in pursuing value and objectives.
b) Dynamic Nature: Risk appetite varies across different risks and over time.
c) Integration: It should be measurable and embedded in the company's control culture.

8.2 Factors influencing Risk Appetite

a) Capacity and Profile: Risk appetite must consider the company's capacity to take risks and its current risk profile, though not as a determinant.
b) Environmental Factors: Industry-specific dynamics, such as competitive changes or technological shifts, can influence risk appetite.
c) Strategy Interplay: Risk and strategy are interdependent, requiring alignment during both formulation and execution.

8.3 Board Considerations for Risk Appetite

a) Clarity on the significant risks the company is willing and unwilling to take in achieving strategic objectives.
b) Maturity of the company's risk management practices.
c) Robustness of the approach used to develop risk appetite.
d) Inclusion of external stakeholders' perspectives in shaping risk appetite.
e) Tailoring and proportionality of the risk appetite to the company's context.
f) Evidence of effective implementation of the defined risk appetite.

For more details, please refer to COSO ERM – Understanding and Communicating Risk Appetite [16].

See also Appendix III: Guiding Questions in respect of Risk Appetite.

9 MOVING FROM GUIDANCE TO PRACTICE

From a Strong Foundation to Future Resilience: Evolving with Purpose

Over more than a decade, the SORMIC framework has become a cornerstone of corporate governance in Malaysia, shaping how Boards approach risk oversight, transparency, and stakeholder trust.

As regulatory demands and market expectations continue to evolve, SORMIC remains a vital tool for Boards committed to governance excellence.

9.1 Institutional Impact

- Corporate Governance Monitor by Securities Commission Malaysia: Highlights progressive alignment with SORMIC in annual reports, particularly in disclosures on risk management, internal audit, and Board oversight.
- MCCG by Securities Commission Malaysia: Principle B reinforces Board and Board committees' accountability by strengthening focus on audit, risk management and the effectiveness of internal controls.
- Minority Shareholders Watch Group (MSWG) Assessments: Leverages SORMIC disclosures as benchmarks for Board accountability and transparency in corporate governance scorecards.

9.2 Evidence from Research

A study by Johari & Jaffar (2020) of 746 Bursa-listed companies (2015-2016) revealed that while full compliance with SORMIC requirements remains low, voluntary disclosures on risk appetite and internal control signal an increasing commitment to effective governance.

9.3 Market Adoption

- Institutional investors and ESG-focused funds consider SORMIC disclosures essential indicators of Board diligence and risk governance.
- Malaysia's leading listed companies, particularly the Top 100, increasingly align their Corporate Governance Overview Statements with SORMIC structures.

Building on this strong foundation, the SORMIC Guide 2025 delivers updated, practical guidance that reflects today's regulatory landscape and market realities. It transcends compliance - empowering Boards to lead with foresight, ensure resilient risk oversight, and drive long-term sustainable value.

10 STATING LIMITATIONS AND SIGNPOSTING CAUTION

Disclaimer and Advisory Note

The listed corporation should also be guided by the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers which is issued by the Taskforce on Internal Control with the support and endorsement of the Bursa.

The SORMIC Guide 2025 is intended to serve as supplementary guidance. While every effort has been made to ensure the accuracy, completeness, and reliability of the information provided, no express or implied representations or warranties are made regarding its content.

Users are advised to exercise discretion and due diligence when referencing the SORMIC Guide 2025. The responsibility lies with the Board and company officers to seek independent professional advice on matters requiring specific legal, regulatory, or governance interpretation. The SORMIC Guide 2025 should not be the sole basis for decision-making.

In the event of updates to any referenced laws or regulations after the publication of the SORMIC Guide 2025, the latest and prevailing versions of the BURSA LR and applicable regulatory frameworks shall take precedence.

The authors of the SORMIC Guide 2025 disclaim all liability for any loss or damages—whether direct, indirect, incidental, special, consequential, or punitive—including loss of profits or opportunities, arising from the use or reliance on this publication.

APPENDIX I

Emerging Global Risks for 2025 – Survey by IIA Foundation [17].

NO	RISK NAME	RISK DESCRIPTION
1	Business continuity	Business continuity, operational resilience, crisis management and disaster response
2	Climate change	Biodiversity and environmental sustainability
3	Communications/reputation	Communications, reputation, and stakeholder relationships
4	Cybersecurity	Cybersecurity, and data security
5	Digital disruption including AI	Digital disruption, new technology, and AI
6	Financial liquidity	Financial liquidity, and insolvency risks
7	Fraud	Fraud, bribery, and the criminal exploitation of disruption
8	Geopolitical uncertainty	Macroeconomic and geopolitical uncertainty
9	Governance/corporate reporting	Organisational governance and corporate reporting
10	Health/safety	Health, safety and security
11	Human capital	Human capital, diversity, and talent management and retention
12	Market changes/competition	Market changes/competition and customer behaviour
13	Mergers/acquisitions	Mergers and acquisitions
14	Organisational culture	Organisational culture
15	Regulatory change	Changes in laws and regulations
16	Supply chain (including third parties)	Supply chain, outsourcing, and 'nth' party risk

Strategic questions to consider:

10.1 What are the **top five** emerging global risks your organisation is currently exposed to?

10.2 What **five key** oversight and strategic actions has the Board taken to address these emerging risks?

APPENDIX II

Assessing the Effectiveness of the Company's Risk Management and Internal Control Processes

Diagnostic questions on Assessing the Risk Management and Internal Control Frameworks cover:

- evaluating Risk Management and Internal Control processes
- reviewing the Risk Management Framework
- assessing the control environment and control activities
- strengthening information communication
- enhancing monitoring activities

These questions are not exhaustive and should be tailored to the company's specific circumstances. This Appendix should be read in conjunction with the related sections set out in this document.

NO	QUESTION
	Aligning the Statement of Risk Management and Internal Control with Prevailing Regulatory Requirements
1	Has the company identified its legal and regulatory obligations with regard to risk disclosure?
2	How frequently does the company review its policies, procedures and frameworks relating to risk management and internal control, including its risk appetite?
	Defining Governance, Risk Management, and Internal Control
3	Does the Board of Directors and Senior Management perceive risk management as an integral part of objective setting and optimisation of performance?
4	Are ESG and other sustainability risks explicitly included in the Board's risk oversight responsibilities?
5	Does Senior Management demonstrate, through its actions as well as its policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company?
6	Do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and the risk management and internal control system?
7	Are succession planning activities in place and operating effectively?
8	Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations; service levels for both internal and outsourced activities; health, safety and environmental protection; security of tangible and intangible assets; business continuity issues; expenditure matters; accounting; financial and other reporting.
9	Are the decisions and actions of different parts of the company appropriately co-ordinated?
10	Are there established channels of communication for individuals to report suspected breaches of law or regulations or other improprieties?
11	Is the whistleblowing mechanism independent of Management and clearly communicated to all the stakeholders and employees?
	Mapping Elements of a Sound Risk Management and Internal Control System
12	Has the company established a risk management framework?
13	Has risk management ownership been clearly defined and accepted by the employees concerned?
14	Is it clear that the Management of risk is an integral part of business management, owned by every manager, with the support and facilitation of the risk management staff?

NO	QUESTION
15	Do people in the company (and in its providers of outsourced services) have the knowledge, skills and tools to support the achievement of the company's objectives and to effectively manage risks that may affect the achievement of these objectives?
16	Has the company's acceptable risk appetite (risk tolerance) or risk criteria been defined, by the Risk Management Committee (RMC), where appropriate, and disseminated?
17	Have the risk profiles for the company been established?
18	Has a system been established to identify significant risks affecting the preparation of the financial statements?
19	Does the company's scenario planning process consider climate-related risks (e.g., physical, transition) and nature-related risks such as biodiversity loss?
20	Are risks that exceed the acceptable limits or criteria defined by the company dealt with first?
21	Does the system for identifying and assessing risks have the following characteristics?
	• Systematic – formalised with sufficient level of appropriate detail
	• Comprehensive – encompassing all key areas of the company and reviewed on a regular basis.
	• Integrated – linked to the core business process (e.g. business/strategic planning, contracting, mergers and acquisitions) within the company.
	• Dynamic and iterative – repeated as necessary to ensure the assessment remains current in the midst of changing business conditions.
22	Do major risks give rise to specific actions?
23	Has the responsibility for such actions been defined?
24	Where appropriate, is implementation of these actions monitored?
25	Does the company have early warning key risk indicators (KRIs) in place to alert Management (and the Board as necessary) of significant changes in risk levels (e.g. political and economic upheavals, technological innovations resulting in the obsolescence of the company's products or services, system failure, project delays, fraud, new product from competitors, and emerging risks including AI impacts)?
26	How are processes/controls adjusted to reflect new or changing risks?
27	Is there a mechanism that makes it possible, when necessary in the light of changing business conditions and risks, for the company to make changes to the company's objectives and business strategies?
	Assigning Roles and Responsibilities for Effective Risk Management and Internal Control
28	Is there a Risk Management Committee (RMC) at Board level chaired by an Independent Director?
29	Is there a Management Committee on risk management, chaired by the CEO (or equivalent)?
30	Have risk management policies been approved by the RMC?
31	Are the Board and Senior Management aware of high-risk areas in the operations and strategies of the company and have these been properly documented and tracked?

NO	QUESTION
32	Is the Board meeting held periodically with Key Management to discuss the key risk profiles of the company, the changing risk levels, changes to risk processes and the adequacy of internal control?
33	Are discussions or deliberations at Board, Board Risk Committee or Risk Management Committee in relation to the company's risk management and internal control properly recorded/minuted?
34	Are authorities, responsibilities and accountabilities defined clearly so that decisions are made and actions taken by the appropriate people after due consideration of the risks involved and the approved risk appetite or criteria?
35	To what extent are the mandate and scope of multiple governance functions in the company aligned to avoid overlap and ensure that there are no coverage gaps?
36	Is there a designated function or individual accountable for monitoring these risks?
37	Do risk owners have an obligation and a process to provide assurance to the Board that they are adhering to the risk management and internal control framework?
38	Has a residual risk level been defined and reported to the Board?
	Evaluating the Effectiveness of Risk Management and Internal Control Systems
39	Have procedures for managing significant risks been defined, approved by Senior Management and implemented in the company?
40	Are the results of risk assessment activities shared across the company for appropriate actions to be taken?
41	Has appropriate risk information, including risk appetite or criteria and risk levels, been cascaded to all the operating units?
42	Are business continuity management processes in place?
43	Have these processes been periodically tested and communicated to relevant employees?
44	Do the Board and Management receive timely, relevant and reliable reports on progress against business objectives and the related risks to enable them to make appropriate decisions? This could include reports with key performance indicators (KPIs) and indicators of changes in key risk indicators (KRIs), together with qualitative information such as customer satisfaction, conversion rates etc.
45	Are periodic reporting procedures, including quarterly and annual reporting, effective in communicating a clear account of the company's performance and the achievement of company's objectives?
46	Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified?
47	Are ongoing processes embedded within the company's overall business operations to monitor the effective application of the policies, processes and activities related to risk management and internal control? (Such processes may include control self-assessment, confirmation by personnel of compliance with policies and codes of conduct, or internal audit or other management reviews).
48	Do these processes monitor the company's ability to re-evaluate risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment?

NO	QUESTION
49	Is there appropriate communication to the Board (or Board Committees such as RMC and AC) on the effectiveness of the ongoing monitoring processes on risk and control matters? This should include reporting any significant failings or weaknesses on a timely basis.
50	Are there specific arrangements for Management monitoring and reporting to the Board on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position.
	Drafting the Board's Statement on Risk Management and Internal Control
51	Does the CEO/CFO (or their equivalent) provide assurance that the risk management and internal control framework is in place and operating effectively?

APPENDIX III

Guiding Questions in respect of Risk Appetite

NO	QUESTION
1	Is the Board clear about the nature and extent of the significant risk it is willing to take in achieving its strategic objectives?
2	What are the significant risks the Board is willing to take and not willing to take?
3	Is the risk appetite aligned to the company's strategy, objective and capacity?
4	Has the company followed a robust approach in developing its risk appetite?
5	Who are the key external stakeholders and have their views been obtained when developing the risk appetite?
6	Is the risk appetite tailored and proportionate to the company?
7	What is the evidence that the company has implemented the risk appetite effectively?
8	Are risk management practices being consistently practised throughout the company for risk identification, assessment, mitigation, monitoring?
9	Have the mitigation factors been considered in an adequate manner?
10	Is the Board satisfied with the presentation of risks, including imminent or emerging risks by Management and the mitigation factors?
11	How often does the Board conduct risk assessment for the company (including reviewing the company's risk appetite)?

REFERENCES

1. BURSA Main Market LR Ch 15 Part E Corporate Governance Disclosure No 15.26(b) (1 July 2023) P1508
   https://tinyurl.com/BURSAMMch15

2. BURSA ACE Market LR Ch 15 Part E Corporate Governance Disclosure (1 July 2023) P1508
   https://tinyurl.com/BURSAAMch15

3. BURSA Main Market Practice Note 9 (31 December 2024) P1
   https://tinyurl.com/BURSAMMP9

4. BURSA ACE Market Guidance Note 11 (31 December 2024) (P1)
   https://tinyurl.com/BURSAAMgn11

5. Malaysian Code on Corporate Governance (MCCG 2021) Principle B Part II (28 April 2021) P50-52
   https://tinyurl.com/MCCGp4p11

6. COSO - The Internal Control – Integrated Framework (ICIF) (May 2013)
   https://tinyurl.com/COSOicf2013

7. Achieving Effective Internal Control Over Sustainability Reporting (ICSR) 2023
   https://tinyurl.com/Coso-ICSR

8. GHG - Green House Gases
   https://ghgprotocol.org/

9. TCFD - Task Force on Climate-related Financial Disclosures
   https://tinyurl.com/The-TCFD

10. IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information
    https://tinyurl.com/IFRS-S1

11. IFRS S2 Climate-related Disclosures
    https://tinyurl.com/IFRS-23

12. EU Corporate Sustainability Reporting Directive
    https://tinyurl.com/ECEUCSRD

13. TNFD Task Force on Nature-related Financial Disclosures
    https://tnfd.global/

14. IIA Three Lines Model (September 2024)
    https://tinyurl.com/IIA-3-Lines-Model

15. BURSA LR Chapter 15 Corporate Governance Part F - Internal Audit
    https://tinyurl.com/Bursa-LR-Ch-15-Part-F

16. COSO Enterprise Risk Management (November 2020)
    https://tinyurl.com/COSOerm20

17. IIA Foundation: Global Summary of Risk in Focus 2025 (2024)
    http://tinyurl.com/IIAFdngrs25

The Institute of
Internal Auditors
Malaysia

THE INSTITUTE OF INTERNAL AUDITORS MALAYSIA
1-17-07, Menara Bangkok Bank, Berjaya Central Park, 105 Jalan Ampang,
50450, Kuala Lumpur, Malaysia

Tel: +603 2181 8008 ext.220/223/204 Fax: +603 2181 1717

Email: technical@iiam.com.my

Like us on The Institute of Internal Auditors Malaysia mainpage
: @IIAMalaysia

www.iiam.com.my