

TITLE:

**STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL
Guidelines for Directors of Listed Companies
SORMIC GUIDE 2025**

SORMIC Guide Revision History



FOREWORD

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

The primary requirement for the SORMIC is set out in Paragraph 15.26(b) of Bursa Malaysia'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 purpose of this **SORMIC Guide** is to facilitate the boards of listed companies in preparing the Statement of Risk Management and Internal Control (**SORMIC**) for publication in the annual reports. The SORMIC is a **mandatory disclosure outlining** the state of risk management and internal control within the listed company and its group.

The SORMIC sets out the obligations of management and the board of directors with respect to risk management and internal control, and describes the processes that should be considered in reviewing its effectiveness. In making the statement, companies are required to explain their governance framework and policies, including any special circumstances which have led them to adopting a particular policy.

The SORMIC Guide provides an approach for listed companies to establish sound risk management and internal control systems, enhancing governance, transparency, and stakeholder confidence. The board of directors 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 also aligns with international best practices, as set by the Committee of Sponsoring Organisations of the Treadway Commission (COSO), International Organisation for Standardisation (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 of Internal Control in compliance with Bursa Malaysia's LR.

Over the years, Bursa Malaysia 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 of Risk Management and Internal Control (SORMIC): 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 Malaysia LR, Malaysian Code on Corporate Governance (MCCG) and related guidelines.

Building on previous versions, SORMIC Guide 2025 incorporates Bursa Malaysia's 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.

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

We are confident that the SORMIC Guide 2025 will provide company directors with the guidance and tools to meet Bursa Malaysia's disclosure requirements.

.....
Chairman of the Task Force
Date:

TASK FORCE MEMBERS**RTAC/IIAM**

Mohd Khaidzir Shahari <i>President</i> The Institute of Internal Auditors Malaysia (IIA Malaysia) CEO, Lembaga Zakat Selangor	Steven Kho Chai Huat <i>RTAC Chairman</i> Sarawak Energy Berhad
Ainon Mahat <i>RTAC Member</i> Malaysia Airports Holdings Berhad	Assoc. Prof. Dr Eddy Yap Tat Hiung <i>RTAC Member</i> CONDUCTIVITI Business Advisory Sdn Bhd
Jimmy Tium Beng Teck <i>RTAC Member</i> Securities Commission Malaysia	Datin Shamita Atputharaja <i>RTAC Member</i> Bursa Malaysia Berhad
Prof Dr Susela Devi <i>RTAC Member</i> Change Enablement Network Solutions Sdn.Bhd	

MEMBERS

Arivinth Raj <i>Director</i> Ernst & Young Consulting Sdn Bhd.	YBhg Dato Billy Goh Soo Wee <i>Vice President</i> Federation of Public Listed Companies Bhd
Chang Ming Chew <i>Director</i> ISACA Malaysia Chapter	Dipa Kaur <i>Deputy President</i> The Malaysian Institute of Chartered Secretaries and Administrators ("MAICSA")
Dominic Chegne How Kooi <i>Partner</i> PwC Malaysia	Faizatul Farhah Ghazali <i>Chairman</i> Malaysian Association of Risk and Insurance Management
Dr Ismet Al-Bakri bin Yusoff Al-Bakri <i>CEO</i> Minority Shareholders Watch Group ("MSWG")	Michele Kythe Lim Beng Sze <i>President & CEO</i> The Institute of Corporate Directors Malaysia ("ICDM")
Seline Goh Sek Lian <i>Director, Controls Assurance Practice</i> Deloitte Asia Pacific	Simon Tay Pit Eu <i>Executive Director, Professional Practices and Technical</i> Malaysian Institute of Accountants ("MIA")
Sujatha Sekhar Naik <i>Chairman</i> Malaysian Institute of Corporate Governance ("MICG")	Assoc. Prof. Dr Sherliza Puat Nelson <i>Research and Publication Committee</i> Malaysian Accounting Association ("MyAA")
Chan Chee Keong Partner KPMG	

SECRETARIAT

Geetha Kanny <i>Executive Director</i> The Institute of Internal Auditors Malaysia (IIA Malaysia)	Alyssa Hew Li Min <i>Head, Technical & Quality Assurance</i> The Institute of Internal Auditors Malaysia (IIA Malaysia)
Muhammad Aslam bin Ab Rahaman <i>Assistant Manager, Technical & Quality Assurance</i> The Institute of Internal Auditors Malaysia (IIA Malaysia)	

OBSERVERS

Jimmy Tium Beng Teck <i>Deputy Director, Internal Audit Department</i> Securities Commission Malaysia	Mohamad Azhar Mohamad Hamidi <i>EVP, Corporate Surveillance & Governance</i> Bursa Malaysia Berhad
---	--

TECHNICAL WRITERS

Devanesan Evanson <i>Technical Writer</i>	Vanajah Shanmugam <i>Assistant Technical Writer</i>
--	--

CONTENTS

- 1. GLOSSARY OF TERMS**
 - 2. ALIGNING the Statement of Risk Management and Internal Control with the prevailing regulatory requirements**
 - 3. DEFINING Governance, Risk Management and Internal Control**
 - 4. IDENTIFYING Elements of a Sound Risk Management and Internal Control System**
 - Risk Management
 - Internal Control
 - 5. DEFINING Roles and Responsibilities for Effective Risk Management and Internal Control**
 - Board's Role
 - Management's Role
 - Internal Audit's Role
 - 6. REVIEWING Effectiveness of the System of Risk Management and Internal Control**
 - Ongoing Assessment
 - Annual Assessment
 - 7. PREPARING The Board's Statement on Risk Management and Internal Control**
 - 8. APPENDIX I**
 - Risk Appetite
 - Considerations Affecting Risk Appetite
 - Questions
 - 9. APPENDIX II**
 - Assessing the effectiveness of the company's risk and internal control processes
 - Assessing the Risk Management Framework
 - Control Environment and Control Activities
 - Information and Communication
 - Monitoring
 - Questions
 - 10. APPENDIX III**
 - Emerging Global Risks for 2025
 - Questions
 - 11. WRAPPING-UP**
 - Evidence of Usefulness of SORMIC Guide
 - 12. DISCLAIMER**
 - Disclaimer statement.
-

1. GLOSSARY OF TERMS

Term	Definition
ACE Market	The ACE Market, formerly known as the MESDAQ Market, is a growth-oriented market within Bursa Malaysia (Malaysia's stock exchange) 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.
BOD	Board of directors (BoD), is the governing body of a corporation or organization, responsible for setting strategy, overseeing management, and protecting the interests of shareholders and other stakeholders.
Bursa Malaysia Berhad	Bursa Malaysia is the stock exchange in Malaysia, serving as the primary platform for trading securities and derivatives.
CDSB	Climate Disclosure Standards Board
COSO	Committee of Sponsoring Organisations of the Treadway Commission, 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 organizations to evaluate, design, and implement effective internal controls.
COSO ERM	COSO ERM refers to the Committee of Sponsoring Organisations (COSO) Enterprise Risk Management framework, a widely recognized model for managing risks across an entire organization. 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.
ESG	Environmental, Social and Governance
EU CSRD	The EU's Corporate Sustainability Reporting Directive (CSRD) is a framework that requires companies to disclose information about their environmental, social, and governance (ESG) performance.
GHG	Greenhouse gases (GHGs) are atmospheric gases that trap heat, contributing to the greenhouse effect and global warming
Governing Body / Board	The highest-level body charged with governance, termed "board" in the IIA Global Internal Audit Standards. In an organisation that has more than one governing body, board refers to the body/bodies authorised to provide the internal audit function with the appropriate authority, role, and responsibilities.
IFRS S1	General Requirements for Disclosures of Sustainability-related Financial Information
IFRS S2	Climate-related Disclosures
IIA	The Institute of Internal Auditors
IIAM	The Institute of Internal Auditors Malaysia

1. GLOSSARY OF TERMS (continued)

Term	Definition
ISO	International Organisation for Standardisation
ISSA	International Standard on Sustainability Assurance
ISSB	International Sustainability Standards Board
Listed Issuers	In this guide, termed as Listed Companies. Any company whose securities are listed and traded on Bursa Malaysia's Main Market and ACE Market
Listing Requirements	Collectively, the Main Market Listing Requirements and ACE Market Listing Requirements of Bursa Malaysia Securities Berhad
Limited Assurance	Primarily includes procedures such as inquiries and analytical procedures, and does not necessarily include consideration of whether internal controls have been effectively designed. The conclusion is usually provided in a negative form of expression (e.g. "nothing has come to our attention.....").
Main Market	Main Market is a prime market of Bursa Malaysia for established companies that have met the prescribed standards in terms of quality, size, and operations. Potential issuers for the Main Market must demonstrate that they have achieved either a minimum profit track record or size measured by market capitalisation (i.e. a minimum required market capitalisation of RM500 million upon listing).
MCCG	Malaysian Code of Corporate Governance
NSRF	National Sustainability Reporting Framework
MSWG	Minority Shareholders Watch Group
PLC	Public Listed Company
SORMIC	The Statement on Risk Management and Internal Control, a mandatory disclosure for companies listed on Bursa Malaysia.
Reasonable Assurance	Entails extensive procedures, which may include consideration of internal controls and tests of details. The conclusion is usually provided in a positive form of expression (e.g., "in our opinion, the subject matter information presents fairly").
TCFD	Task Force on Climate-related Financial Disclosures.
The IIA's Three Lines Model	The IIA's Three Lines Model helps organisations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management.
TNFD	The Taskforce on Nature-related Financial Disclosures (TNFD) has developed a set of disclosure recommendations and guidance that encourage and enable business and finance to assess, report and act on their nature-related dependencies, impacts, risks and opportunities.

2. ALIGNING THE STATEMENT OF RISK MANAGEMENT AND INTERNAL CONTROL WITH THE PREVAILING REGULATORY REQUIREMENTS – THE WHY

2.1 Objective of SORMIC:

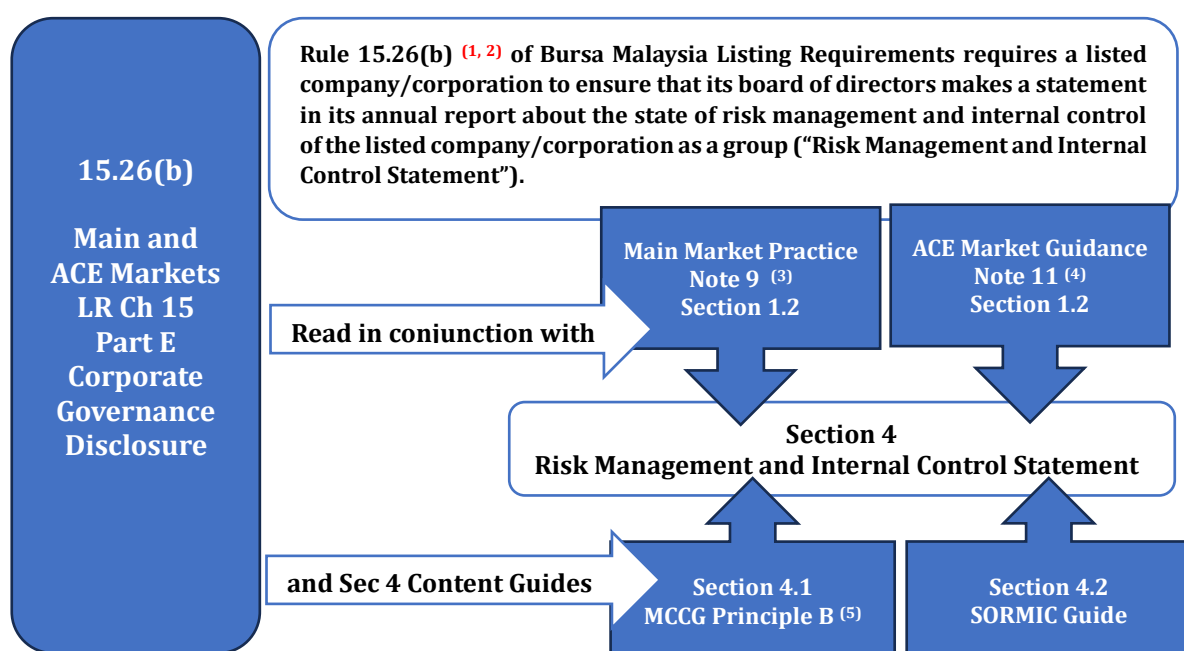
The primary objective of this SORMIC Guide is to assist the board of listed companies in making the Statement on Risk Management and Internal Control, as required by the Bursa Malaysia LR and Main Market Practice Note 9, and Ace Market Guidance Note 11.

2.2 This **SORMIC Guide**, in line with prevailing requirements for the Statement on Risk Management and Internal Control as outlined in the Bursa Malaysia 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 management and the board of directors 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 its effectiveness.
- 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 following Bursa Malaysia Listing Requirements (LR). *In a nutshell:*



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 of 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 MCGG context, the definitions of Company and Group are as follows:
 - **Company:** Refers to an individual listed company or corporation that is subject to corporate governance principles and practices as outlined in the MCGG. This includes public-listed companies (PLCs) on Bursa Malaysia.
 - **Group:** Refers to 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.
 - If material joint ventures and associate companies are excluded from the group for the purposes of these guidelines, this should be disclosed.
- d) The appendices to this Guide contain questions that boards should consider when applying the Guide's approach and recommendations.

References:

1. *Bursa Malaysia Main Market LR Ch 15 Part E Corporate Governance Disclosure No 15.26(b) (1 July 2023) P1508*
<https://tinyurl.com/BURSAMMch15>
 2. *Bursa Malaysia ACE Market LR Ch 15 Part E Corporate Governance Disclosure (1 July 2023) P1508*
<https://tinyurl.com/BURSAAMch15>
 3. *Bursa Malaysia Main Market Practice Note 9 (31 December 2024) P1*
<https://tinyurl.com/BURSAMP9>
 4. *Bursa Malaysia ACE Market Guidance Note 11 (31 December 2024) (P1)*
<https://tinyurl.com/BURSAAMgn11>
 5. *Malaysian Code on Corporate Governance (MCGG) Principle B Part II (28 April 2021) P50-52*
<https://tinyurl.com/MCCGp4p11>
-

3 PRINCIPLES AND PRACTICES OF GOVERNANCE, RISK MANAGEMENT AND INTERNAL CONTROL – THE WHAT

In making the Statement, Bursa Malaysia directs the listed company in Practice Note 9 and Guidance Note 11 Section 4 to address Principle B Effective Audit and Risk Management, Part II Risk Management and Internal Control Framework of the MCGG.

This Principle relates to the rationale of adopting a cohesive approach on integrating governance, risk management, and internal control by a company.

3.1 Intended Outcome 10.0 of the MCGG states that:

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.

3.2 Practice and Guidance of the MCGG Risk Management and Internal Control Framework

	Practice		Guidance
10.1	The board should establish an effective risk management and internal control framework.	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.
10.2	The board should disclose the features in its risk management and internal control framework, and the adequacy and effectiveness of this framework	G10.2	<p>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.</p> <p>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.</p>

4 IDENTIFYING ELEMENTS OF A SOUND RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM – THE WHICH

4.1 Risk Management

A sound risk management framework integrates with the company's culture, processes, and structures. The framework should adapt to changes and be clearly communicated across all levels. An adequate and effective Control Environment and Board Oversight plays 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.

4.2 Key Elements of Risk Management

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) Key Performance Indicators (KPIs) and Metrics

- Risk-specific KPIs linked to:
 - **Incident frequency/severity.**
 - **Risk exposure trends.**
 - Alignment of risk levels with the **board-approved risk appetite.**

c) 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.

- 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**.
- Board-level oversight metrics: e.g., % of key risks reviewed quarterly.

4.3 Internal Control

An internal control system comprises the policies, processes, tasks, behaviours, and other company elements that collectively:

- Enhance Operational Efficiency and Effectiveness*: Supports effective operations by addressing key business, operational, financial, and compliance and **other risks** to achieve company objectives.
- Ensure Reporting Quality*: Maintains proper records and processes to generate timely, relevant, and reliable internal and external information.
- Promote Compliance*: Upholds adherence to laws, regulations, and internal policies governing business conduct.
- KPIs help in evaluating*:
 - **Annual effectiveness reviews** of the system.
 - Comparison of current performance with **prior periods** or **benchmarks**.
 - Insights from **audit findings, risk events, or near misses**.

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.

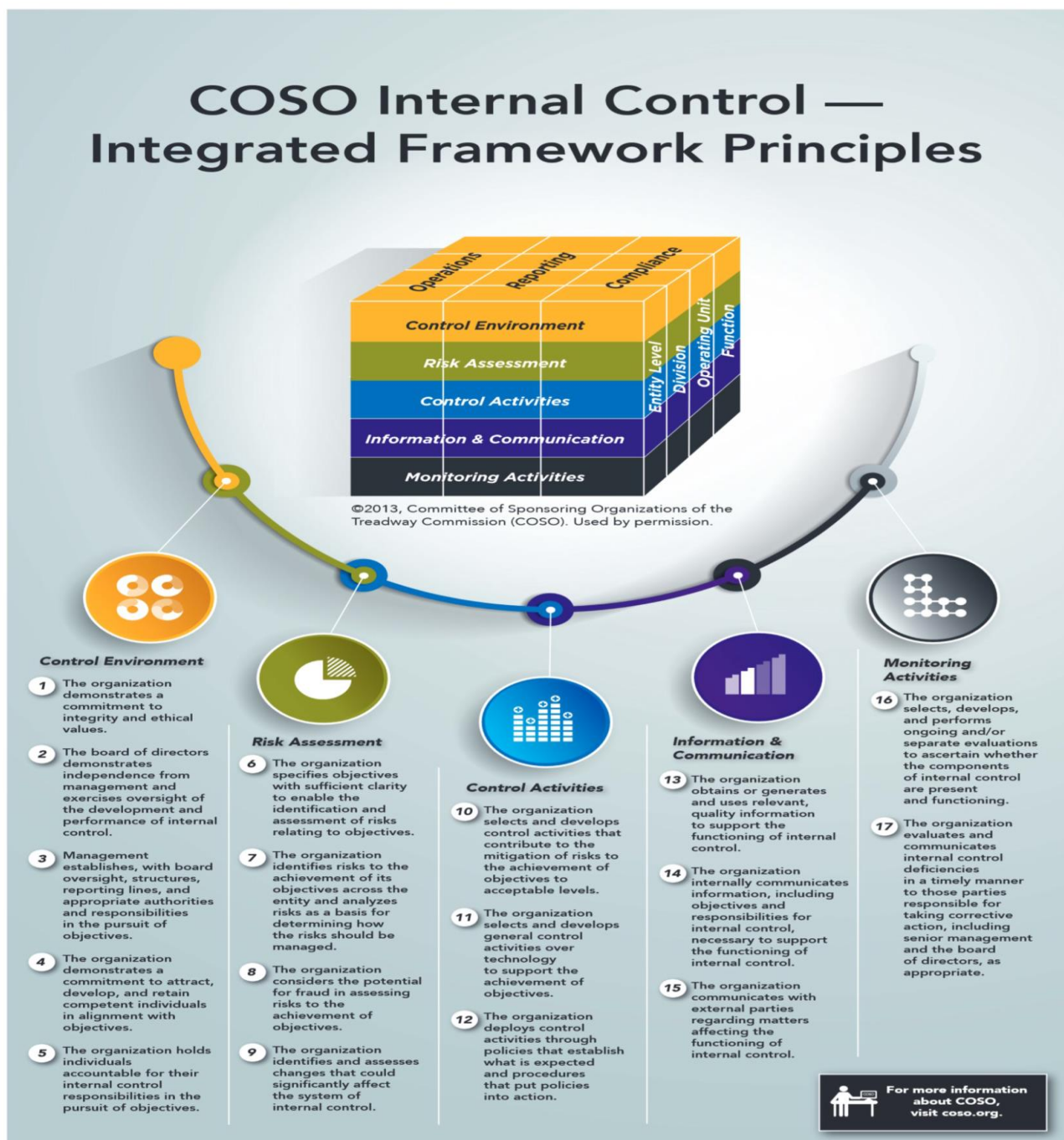
The most-widely recognised framework for internal control is published by the Committee of Sponsoring Organisations of the Treadway Commission (COSO) ⁽⁶⁾.

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.

- The **three categories of objectives** to guide the purpose – operations, reporting, and compliance, represented by the columns.
- The **five components**, the elements required to achieve those objectives, represented by the rows.

- b) 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.



Reference:

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

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 concepts associated with each component. Because these principles are drawn directly from the components, an entity can achieve effective internal control by applying all principles. All principles apply to operations, reporting, and compliance objectives.

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.

4.7 Challenges and Limitations

As governance practices evolve, it is important to recognise the challenges and limitations 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 Guide 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) Control performance indicators

Management should set **control performance indicators**, such as:

- Control failure rates.
- Number of control deficiencies identified vs. resolved.
- Timeliness of corrective actions.

4.8 Addressing Challenges:

To overcome existing limitations and align with global emerging risks, SORMIC Guide 2025 introduces several enhancements:

a) Integration of ESG and Sustainability Risks

- Incorporate ESG-related risks, including climate, biodiversity, and social factors, into risk management and internal control frameworks.

- b) **Sustainability Control Guidance**
 - Introduce practical guidance for controlling and reporting on sustainability metrics, including GHG ⁽⁷⁾ emissions and alignment with TCFD ⁽⁸⁾ recommendations.
- c) **IFRS S1/S2 Mapping for Integrated Reporting**
 - Provide a clear mapping between SORMIC principles and IFRS S1 ⁽⁹⁾ (General Sustainability Disclosures) and IFRS S2 ⁽¹⁰⁾ (Climate-related Disclosures) to support integrated reporting.
- d) **Scenario Analysis and Forward-looking Risk**
 - Embed scenario planning and assessment of emerging risks, such as AI, cyber, and climate risks, into board risk oversight processes.
- e) **Alignment with Global Standards**
 - Align with leading global frameworks, including:
 - i. **TNFD** ⁽¹¹⁾ (Task Force on Nature-related Financial Disclosures)
 - ii. **EU CSRD** ⁽¹²⁾ (Corporate Sustainability Reporting Directive)

References:

7. *GHG - Green House Gases*
<https://ghgprotocol.org/>
8. *TCFD - Task Force on Climate-related Financial Disclosures*
<https://assets.bbhub.io/company/sites/60/2020/10/FINAL-2017-TCFD-Report-11052018.pdf>
9. *IFRS S1 General Requirements for Disclosure of Sustainability-related Financial Information*
<https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s1-general-requirements/>
10. *IFRS S2 Climate-related Disclosures*
<https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s2-climate-related-disclosures/>
11. *TNFD Task Force on Nature-related Financial Disclosures*
<https://tnfd.global/>
12. *EU Corporate Sustainability Reporting Directive*
https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en

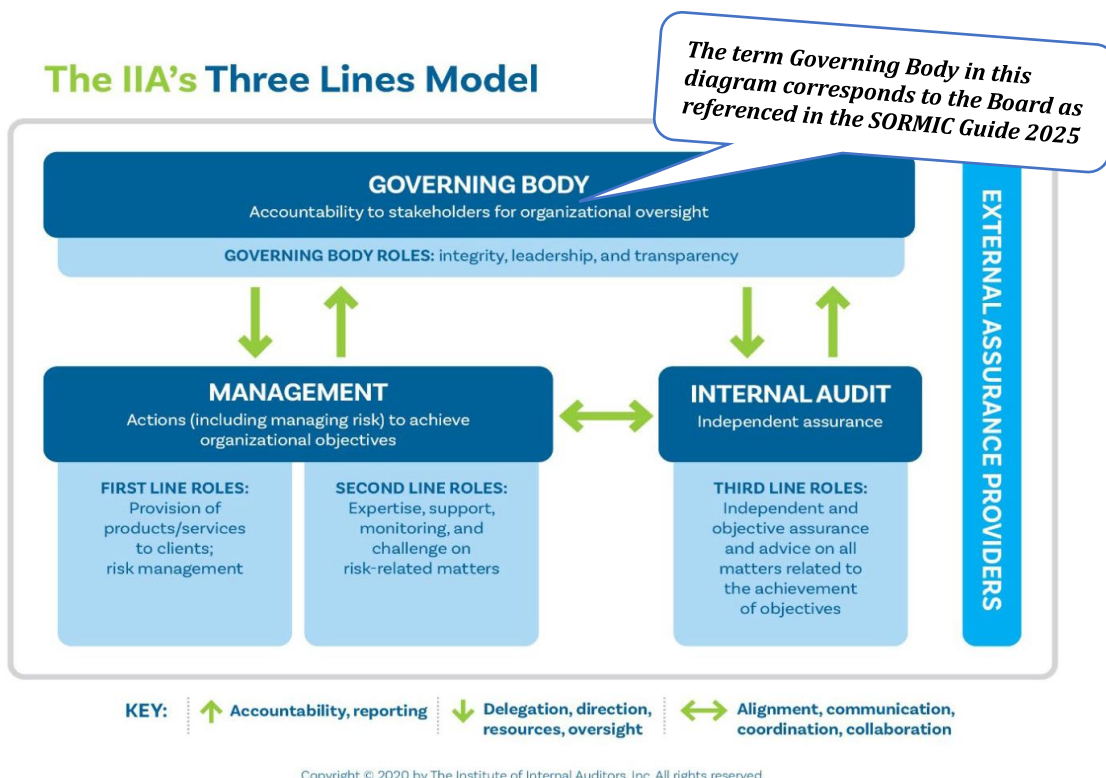
5 DEFINING ROLES AND RESPONSIBILITIES FOR EFFECTIVE RISK MANAGEMENT AND INTERNAL CONTROL - **THE WHO**

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 ⁽¹³⁾ 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.



Reference:

- 13. *IIA Three Lines Model (September 2024)*
<https://tinyurl.com/IIA-3-Lines-Model>

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	<ul style="list-style-type: none"> • Has clear terms of references for Board Charter, Board Committees and delegation of limits of authority to management • Ensuring management is responsible for implementation and execution. • Assigning detailed oversight tasks but ensuring the Board remains responsible for final decisions, within the Board’s remits of authority and responsibility.

2	Engagement with Assurance Provider	<ul style="list-style-type: none"> Using internal audit as an independent risk assurance function. Using external audit to gain independent validation on financial risks.
3	Governance & Strategic Oversight	<ul style="list-style-type: none"> Ensuring a risk-aware culture is embedded across the organisation. Integrating risk considerations into corporate strategy and decision-making. Ensuring transparency and regulatory compliance.
4	Monitoring & Assurance	<ul style="list-style-type: none"> Ensuring the risk management system provides reasonable assurance. Conducting formal reviews to assess system effectiveness. Using reports from management, internal audit, and external auditors to evaluate risk effectiveness.
5	Risk Appetite & Policy Setting	Defining and approving acceptable risk levels for the organisation.

b) Management – First-Line Roles

- Leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organisation.
- Maintains a continuous dialogue with the governing body, and reports on planned, actual, and expected outcomes linked to the objectives of the organisation, and risk.
- Establishes and maintains appropriate structures and processes for the management of operations and risk (including controls).
- Ensures compliance with legal, regulatory, and ethical expectations.

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 LR regulations, and acceptable ethical behaviour, controls, information and technology security, sustainability, and quality assurance.
- Provides 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 governing body 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.

Other functions include:

- Assessing whether risks affecting the company's objectives are effectively evaluated, managed, and controlled.
- Evaluating and enhancing the governance, risk management, and internal control framework.

- Ensuring compliance with regulatory requirements, such as Paragraph 15.27(2) (14), of the Listing Requirements which mandate an independent internal audit function reporting directly to the Audit Committee.

e) Internal Auditor's Qualifications and Competence Levels

The MCGG Principle B Part II Risk Management and Internal Control Framework highlights these recommendations:

Practice 11.2(15) requires that the board should disclose the name and qualification of the person responsible for internal audit.

Guidance 11.1(15) states "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.
- 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.

f) 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.

References:

14. *Bursa LR Chapter 15 Corporate Governance Part F - Internal Audit*
<https://tinyurl.com/Bursa-LR-Ch-15-Part-F>
 15. *MCGG Principle B Part 11 Risk Management and Internal Control Framework*
<https://tinyurl.com/MCGG-Principle-B-Part-11>
-

6 REVIEWING EFFECTIVENESS OF THE SYSTEM OF RISK MANAGEMENT AND INTERNAL CONTROL – THE WHEN

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., Listing Requirements 15.26(b)).

6.2 Key Considerations for Assessment

a) Strategic Alignment:

- Processes for setting long- 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.

6.4 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; and
- Overall adequacy and effectiveness of risk management and internal control policies.

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.

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

7 PREPARING THE BOARD'S STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL - **THE HOW**

The disclosure requirements for the Statement must be made pursuant to 15.26(b) of Bursa Malaysia 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:

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.

7.6 CEO and CFO Assurances:

In its narrative statement, the board should also include whether it 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 APPENDIX I***Risk Appetite: Key Concepts and Considerations*****8.1 Definition and Characteristics**

- 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 Influencing Factors

- 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).

Reference:

16. *COSO Enterprise Risk Management (November 2020)*

<https://tinyurl.com/COSOerm20>

QUESTIONS in respect of Risk Appetite:

No	Question	Yes	No	In-Progress	N/A
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	How mature is risk management in the company?				
4	Has the company followed a robust approach in developing its risk appetite? Who are the key external stakeholders and have their views been obtained when developing the 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	Have the mitigation factors been considered in an adequate manner?				
9	Is the Board satisfied with the presentation of risks, including imminent or emerging risks by Management and the mitigation factors?				

9 APPENDIX II***Assessing the Effectiveness of the Company's Risk and Internal Control Processes***

Some questions which the board may wish to consider and discuss with management when regularly reviewing reports on risk management and internal control and when carrying out its annual assessment are set out below. The questions are not intended to be exhaustive and will need to be tailored to the particular circumstances of the company.

This Appendix should be read in conjunction with the guidelines set out in this document.

QUESTIONS on Assessing the Risk Management Framework:

No	Question	Yes	No	In-Progress	N/A
1	Has the company established a risk management framework?				
2	Does the board of directors and senior management perceive risk management as an integral part of objective setting and optimisation of performance?				
3	Has risk management ownership been clearly defined and accepted by the employees concerned? 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?				
4	Is there a Risk Management Committee (RMC) at board level chaired by an independent director?				
5	Have risk management policies been approved by the RMC?				
6	Has the company's acceptable risk appetite (risk tolerance) or risk criteria been defined, by the RMC, where appropriate, and disseminated?				
7	Is there a Management Committee on risk management, chaired by the CEO (or equivalent)?				
8	Have procedures for managing significant risks been defined, approved by executive management and implemented in the company?				
9	Are the board and executive management aware of high-risk areas in the operations and strategies of the company and have these been properly documented and tracked?				
10	Have the risk profiles for the company been established?				
11	Has the company identified its legal and regulatory obligations with regard to risk disclosure?				
12	Has a system been established to identify significant risks affecting the preparation of the financial statements?				
13	Are risks that exceed the acceptable limits or criteria defined by the company dealt with first? Has a residual risk level been defined and reported to the board?				
14	Do major risks give rise to specific actions? Has the responsibility for such actions been defined? Where appropriate, is implementation of these actions monitored?				
15	Does the system for identifying and assessing risks have the following characteristics?				
	•Systematic – formalised with sufficient level of appropriate detail				

	<ul style="list-style-type: none"> •Comprehensive – encompassing all key areas of the company and reviewed on a regular basis. 				
	<ul style="list-style-type: none"> •Integrated – linked to the core business process (e.g. business/strategic planning, contracting, mergers and acquisitions) within the company. 				
	<ul style="list-style-type: none"> •Dynamic and iterative – repeated as necessary to ensure the assessment remains current in the midst of changing business conditions. 				
16	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?				
17	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)?				
18	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?				
19	Are the results of risk assessment activities shared across the company for appropriate actions to be taken?				
20	Has appropriate risk information, including risk appetite or criteria and risk levels, been cascaded to all the operating units?				
21	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?				
22	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?				
23	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?				
24	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?				
25	Are the decisions and actions of different parts of the company appropriately co-ordinated?				
26	How are processes/controls adjusted to reflect new or changing risks?				
27	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?				
28	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.				

29	Are business continuity management processes in place? Have these processes been periodically tested and communicated to relevant employees?				
30	Are succession planning activities in place and operating effectively?				
31	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 risk levels (KRIs), together with qualitative information such as customer satisfaction, conversion rates etc.				
32	Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified?				
33	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?				
34	Are there established channels of communication for individuals to report suspected breaches of law or regulations or other improprieties?				
35	Is the whistleblowing mechanism independent of management and clearly communicated to all the stakeholders and employees?				
36	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).				
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	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?				
39	Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to changes in risk and control assessments?				
40	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.				
41	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.				
42	Does the CEO/CFO (or their equivalent) provide assurance that the risk management and internal control framework is in place and operating effectively?				

10 APPENDIX III

Emerging Global Risks for 2025 – Survey by IIA Foundation (17).

Reference:

17. IIA Foundation: *Global Summary of Risk in Focus 2025 (2024)*

<https://tinyurl.com/IIAFdngrs25>

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 'n th ' party risk

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?

10.3 What are the **top five** areas where internal audit currently focuses its time, resources, and attention?

11 WRAPPING-UP

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.

11.1 Institutional Impact

- *Bursa Malaysia Corporate Governance Monitor (2019, 2020, 2023)*: Highlights progressive alignment with SORMIC in annual reports, particularly in disclosures on risk management, internal audit, and board oversight.
- *MCCG Revisions (2017, 2021)*: Embedded SORMIC principles in Principle B, reinforcing its institutional value.
- *Minority Shareholders Watch Group (MSWG) Assessments*: Leverages SORMIC disclosures as benchmarks for board accountability and transparency in corporate governance scorecards.

11.2 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.

11.3 Market Adoption

- Institutional investors and ESG-focused funds consider SORMIC disclosures essential indicators of board diligence and risk governance.
- Malaysia’s leading PLCs, 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.

12 DISCLAIMER AND ADVISORY NOTE

Bursa Malaysia's Listing Requirements – Main Market Practice Note 9 (Section 4) and ACE Market Guidance Note 11 (Section 4) encourage listed issuers to adopt the **Guide on the Statement of Risk Management and Internal Control (SORMIC)** in conjunction with all applicable laws, regulations, standards, and the prevailing provisions of the Bursa Malaysia Listing Requirements.

This Guide 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 this Guide. The responsibility lies with the board and company officers to seek independent professional advice on matters requiring specific legal, regulatory, or governance interpretation. This Guide should not be the sole basis for decision-making.

In the event of updates to any referenced laws or regulations subsequent to the publication of this Guide, the latest and prevailing versions of the Bursa Malaysia Listing Requirements and applicable regulatory frameworks shall take precedence.

The authors of this Guide 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.

THE END
