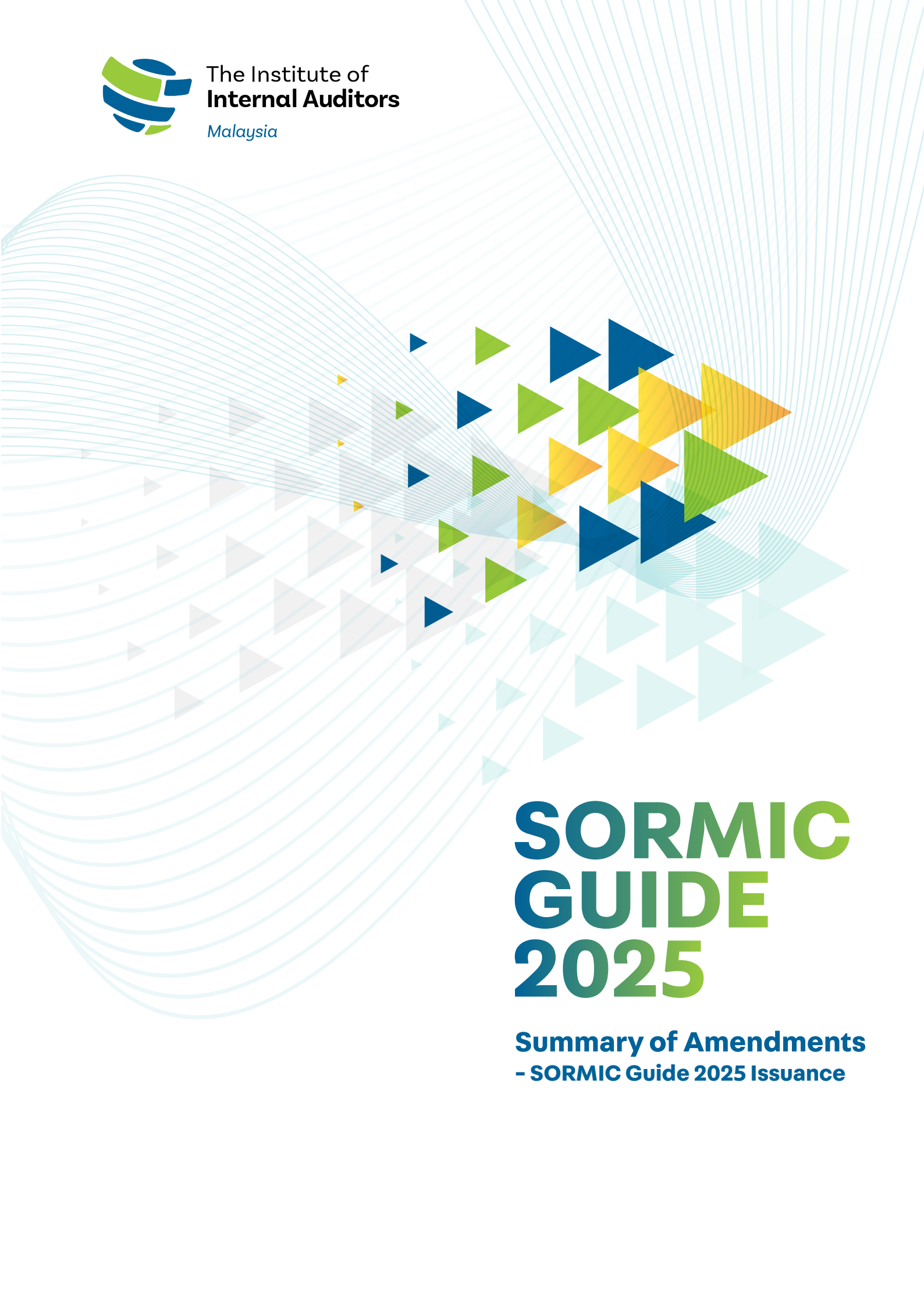
The Institute of
Internal Auditors
Malaysia



SORMIC GUIDE 2025

Summary of Amendments
- SORMIC Guide 2025 Issuance

Note: All elements in SORMIC 2012 continue to underpin the 2025 framework. The SORMIC Guide 2025 enhances and extends these foundational components by integrating contemporary standards, stakeholder expectations, and global developments in governance and risk management.

* Titles - shifting to active tone in titles signals clear ownership, immediacy, and a proactive mindset—traits especially important in regulatory, procedural, and guidance documents.

Also adding interrogative pronouns and adverbs (Ws' and H) to section titles in SORMIC 2025 transforms the document from a static compliance guide into a dynamic, inquiry-driven governance tool – promoting engagement, reflection, and action.

FOREWORD

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
FOREWORD: *Updated to emphasise regulatory cross-references, evolving governance context, and explicit link to Bursa LR 15.26(b) with GN/PN references.*		
Titled "Statement on Internal Control – Guidance for Directors of Public Listed Companies".	Renamed to "Statement on Risk Management and Internal Control (SORMIC)".	Scope expanded from internal control only to include risk management; acronym SORMIC introduced.
Purpose: guide directors in preparing statement in accordance with Bursa LR.	Purpose: facilitate boards in preparing SORMIC, enhance governance, transparency, and stakeholder confidence.	Broader, outcome-focused objectives stated.
References only Bursa LR.	References Bursa LR 15.26(b), Main Market PN9, ACE Market GN11.	Specific, detailed regulatory references added.
Focus on board and management obligations; review of effectiveness.	Clearer separation of roles: board oversight vs management implementation.	Strengthened governance role definition.
No reference to global standards.	Aligns with COSO, ISO, IIA best practices.	International alignment added for accountability and resilience.
Historical note: 2000 issuance; revised due to changing regulatory environment.	Expanded history: 2000 issuance, 2012 update and rename, post-2012 reforms.	More detailed evolution narrative.
General thanks to contributors.	Acknowledgements expanded to include regulators, industry experts, professional bodies.	Broader acknowledgement scope.
Ends with confidence it will assist compliance.	Ends with confidence it will provide tools to meet Bursa disclosure requirements.	More results-oriented closing.

SECTION 1

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 1 CLARIFYING KEY TERMS: *New section defining key governance, regulatory, sustainability, and market terms to aid reader understanding.*		
No glossary section in 2012.	New glossary section included, defining key regulatory, governance, sustainability, and market terms (e.g., Bursa, MCCG, COSO, ESG, ISSB, NSRF, TCFD, TNFD).	Added to clarify technical terms, support understanding of expanded subject matter, and align with global standards.

SECTION 2

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 2 ALIGNING THE STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL WITH PREVAILING REGULATORY REQUIREMENTS: *Expands scope to include ESG/sustainability risks, external dependencies, and broader stakeholder considerations.*		
Replaces 2000 Statement on Internal Control guidance; intended to help directors make disclosures on risk management and internal control per Bursa LR 15.26(b).	States primary objective of assisting boards in preparing the Statement on Risk Management and Internal Control per Bursa LR, PN9 (Main Market), GN11 (ACE Market).	Clearer framing of objective and alignment with specific LR provisions and guidance notes.
Outlines obligations of board and management; key elements of a sound system; process for reviewing effectiveness; CEO/CFO assurance requirement.	Provides structured approach covering public disclosures, board/management responsibilities, key elements, evaluation process, CEO/CFO assurances, and board approvals.	Expanded into a step-by-step structure with explicit inclusion of disclosure oversight by the board.
Refers to MCCG 2012 Principle 6 and Recommendation 6.1 with commentary on board duties, risk tolerance, monitoring, periodic testing, and disclosure.	Aligns with MCCG Principle B Part II, with links to PN9/GN11 content guides; integrates references to relevant standards and authoritative bodies.	Updates MCCG reference from 2012 Principle 6 to current Principle B, with emphasis on recognised frameworks and external standards.
Defines "company" and "group" in context of applying guidelines; mentions treatment of material JVs and associates.	Defines "company" and "group" similarly, but clarifies governance scope and disclosure expectations when excluding material JVs/associates.	Wording modernised, governance scope reinforced.
Appendix contains questions boards may consider when applying guidelines.	Appendices contain questions boards should consider when applying the Guide's approach and recommendations.	Language strengthened from optional to recommended board consideration.

SECTION 3

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 3 DEFINING GOVERNANCE, RISK MANAGEMENT AND INTERNAL CONTROL: *Clarifies board, committee, and management roles with stronger emphasis on accountability and alignment to governance frameworks.*		
Defines governance, risk management, and internal control broadly; emphasises embedding risk management within governance, focusing on business risks, and ensuring appropriate systems to identify, assess, and respond to risks.	Reframes as "Defining Governance, Risk Management and Internal Control – The What" and aligns directly with MCCG Principle B, Part II (Effective Audit and Risk Management) via BURSA PN9 (Main Market) and GN11 (ACE Market).	2025 ties definitions explicitly to Bursa LR and MCCG intended outcomes for stronger regulatory linkage.
States that internal control is about actions by board and management to manage risk, with reasonable assurance against adverse impacts, using preventive, detective, and corrective measures.	Breaks into MCCG "Intended Outcomes" and "Practices" covering board responsibilities, disclosure requirements, evaluation of key risks (including sustainability, cyber security), use of recognised frameworks, annual review/testing, and step-up requirement for a Risk Management Committee.	Moves from descriptive to prescriptive, embedding specific MCCG practices and detailed disclosure expectations.
Focus on overall contribution of risk management to achieving objectives and performance targets.	Adds governance integration, explicit board accountability for framework adequacy, and enhanced internal audit oversight (independence, resources, qualifications, compliance with recognised frameworks).	Expands scope to include internal audit governance and transparency on audit resources, independence, and competency.

SECTION 4

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 4 MAPPING ELEMENTS OF A SOUND RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM: *Moves from control-centric to integrated risk and control framework, embedding sustainability and strategic alignment.*		
Describes embedding risk management into culture, processes, and structures; outlines board/management roles in setting risk appetite, monitoring, and responding to risks.	Retains integration emphasis but adds alignment with ISO 31000 and COSO ERM, highlighting benefits such as consistency, accountability, strategic alignment, and scalability.	International standards explicitly incorporated, with clearer linkage to governance and decision-making.
Control environment includes values, codes of conduct, documented roles, structure, and assignment of responsibilities.	Expands control environment to include commitment to competence (aligning with COSO Principle 4) and accountability for internal control responsibilities.	Strengthens human capital and competency focus.
Internal control system defined as policies, processes, tasks, behaviours ensuring operational efficiency, reporting quality, and compliance; includes control activities, information flows, and monitoring.	Aligns internal control design and evaluation with COSO Internal Control–Integrated Framework, detailing components, principles, and purpose; links to ESG and sustainability risk integration.	Formal adoption of COSO as benchmark; embeds ESG and sustainability considerations.
Board considerations focus on nature/extent of risks, acceptable levels, likelihood, mitigation ability, and cost-benefit of controls.	Adds KPIs and metrics for oversight (e.g., risk mitigation effectiveness, compliance indicators, incident frequency, risk trend alignment with appetite).	More measurable and performance-driven oversight approach.
Acknowledges limitations (human error, override, unforeseeable events).	Expands limitations to include disclosure quality gaps, under-reporting of weaknesses, and lack of focus on emerging risks; adds indicators of control ineffectiveness.	Recognises practical governance challenges and need for forward-looking risk focus.
No specific sustainability/ESG framework references.	Embeds ESG and other sustainability risks into the RM/IC framework; integrates COSO ICSR 2023 guidance; aligns with ISSB IFRS S1/S2 and NSRF; includes mapping to TCFD pillars and other global standards (EU CSRD, TNFD).	Significant expansion to address sustainability risks, global reporting standards, and scenario analysis for emerging risks.

SECTION 5

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 5 ASSIGNING ROLES AND RESPONSIBILITIES FOR EFFECTIVE RISK MANAGEMENT AND INTERNAL CONTROL: *Retains core principles but aligns explicitly to global standards (COSO, ISO, ISSB) and integrates sustainability and emerging risks.*		
Defines roles of board, management, and internal audit in maintaining a sound risk management and internal control framework.	Adopts IIA's Three Lines Model, detailing responsibilities across board (governing body), management (first and second lines), internal audit (third line), and external assurance providers.	Broader framework integrating modern assurance model with multiple lines of defence.
Board responsibilities: embed risk management, approve risk appetite, review frameworks/processes, assess effectiveness annually, receive CEO/CFO assurance, seek internal/external audit feedback; may delegate to committees but retains accountability.	Board roles expanded into four governance pillars: accountability & delegation, governance & strategic oversight, monitoring & engagement with assurance providers, and risk appetite & policy setting; emphasis on independence of internal audit and engagement with multiple assurance sources.	More structured, principle-based governance duties; deeper focus on assurance integration.
Management responsibilities: implement risk processes, identify risks, align with strategy and risk appetite, report changes, provide annual CEO/CFO assurance to board.	Management roles split into first-line (CEO/CFO) with dual-facing accountability to board and assurance providers, and second-line (specialist functions) for risk oversight, compliance, sustainability, and quality assurance.	More nuanced role differentiation; explicit alignment with Bursa LR compliance and sustainability expectations.
Internal audit: independent assurance function reporting to Audit Committee; evaluates risk, control, and governance; must comply with professional standards.	Internal audit reaffirmed as third line, maintaining independence, providing strategic advice, reporting impairments, and promoting continuous improvement.	Reinforces independence, strategic advisory role, and continuous improvement culture.

SECTION 6

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 6 EVALUATING THE EFFECTIVENESS OF RISK MANAGEMENT AND INTERNAL CONTROL SYSTEMS: *Strengthens regulatory compliance focus, adds early warning monitoring, and validates CEO/CFO assurances.*		
Emphasises board responsibility for reviewing effectiveness through ongoing and annual assessments; considers strategic alignment, risk appetite, policies, processes, monitoring, and reporting.	Retains these elements but frames them as "The When" and explicitly links to regulatory compliance (LR 15.26(b)).	Strengthened regulatory emphasis and structured timing focus.
Ongoing assessment: management reports periodically on business risks and system effectiveness; board evaluates significant risks, control effectiveness, failings, early warnings, emerging risks.	Ongoing assessment includes same core activities but adds verification of early warning indicators, evaluation of need for extended monitoring, and emphasis on emerging risks with appropriate controls.	More explicit expectations for proactive monitoring and early risk detection.
Annual assessment: reviews changes in significant risks, effectiveness of systems, work of assurance providers, communication frequency, control failings, unanticipated events, and policy adequacy.	Annual assessment mirrors 2012 but adds credibility and sufficiency checks on CEO/CFO assurances regarding risk and control systems.	Stronger assurance validation requirement from executive sign-offs.
Recognises no absolute assurance, only reasonable assurance that risks are managed within board-approved levels.	Same principle retained; linked explicitly to alignment with company's strategies and objectives.	Reinforces strategic alignment of assurance outcomes.

SECTION 7

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 7 DRAFTING THE BOARD'S STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL: *Same disclosure requirements but restructured into clearer categories for ease of use.*		
Outlines disclosure content required under LR 15.26(b), including main features of RM/IC system, ongoing processes, review methods, adequacy/effectiveness commentary, treatment of significant problems, treatment of material JVs/associates, and CEO/CFO assurances.	Retains same core content but frames as "The How", grouping into clearer categories: Key Features, Risk Management Process, Review and Actions, Adequacy and Effectiveness, Joint Ventures/Associates, and CEO/CFO Assurances.	Same requirements, but 2025 version streamlines structure and categorises disclosures for clarity and ease of use.

SECTION 8

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 8 RISK APPETITE: KEY CONCEPTS AND CONSIDERATIONS: *Expands to include explicit board oversight, stakeholder perspectives, and evidence of implementation.*		
Defines risk appetite as the amount of risk a company is willing to seek or accept in pursuit of value; notes it varies by risk type and over time; should be measurable and embedded in control culture; influenced by capacity, current profile, environmental factors, and strategic alignment.	Retains core definition but reframes as "Key Concepts and Considerations", grouping into definition/characteristics, influencing factors, and board considerations (clarity on acceptable risks, RM maturity, robustness, stakeholder input, proportionality, implementation evidence).	Adds explicit board oversight responsibilities, emphasis on stakeholder perspectives, and demonstration of effective implementation.

SECTION 9

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 9 MOVING FROM GUIDANCE TO PRACTICE: *New section highlighting SORMIC's practical impact.*		
No equivalent section in 2012.	Introduces "Moving from Guidance to Practice" highlighting SORMIC's institutional impact, research evidence, and market adoption over a decade; emphasises its role in evolving governance and sustainable value creation.	New section providing context on SORMIC's practical influence, adoption trends, and relevance in current governance landscape.

SECTION 10

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
SECTION 10 STATING LIMITATIONS AND SIGNPOSTING CAUTION: *New section adding a legal disclaimer.*		
No equivalent section in 2012.	Adds "Stating Limitations and Signposting Caution" with a disclaimer and advisory note clarifying that SORMIC Guide 2025 is supplementary guidance, not a substitute for legal/ regulatory advice; stresses use alongside prevailing Bursa LR and applicable laws.	Adds formal limitation statement and legal disclaimer to manage user expectations and ensure alignment with current regulations.

APPENDIX I

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
APPENDIX I EMERGING GLOBAL RISKS: *New tool listing 16 emerging risks with strategic board oversight questions.*		
No equivalent appendix.	New appendix listing 16 emerging global risks from IIA Foundation 2025 survey (e.g., climate change, AI disruption, geopolitical uncertainty, regulatory change), plus strategic board questions on exposure and oversight actions.	Adds practical forward-looking tool for boards to identify, prioritise, and respond to emerging risks in strategic oversight.

APPENDIX II

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
APPENDIX II ASSESSING THE EFFECTIVENESS OF THE COMPANY'S RISK MANAGEMENT AND INTERNAL CONTROL PROCESSES: *Broader scope with regulatory alignment, emerging risks, and sustainability oversight.*		
Provides a set of diagnostic questions boards may consider when reviewing risk management and internal control, covering risk framework, control environment, information/communication, and monitoring.	Expands and restructures into five thematic areas: aligning with regulatory requirements, defining governance/RM/IC, mapping elements of RM/IC system, assigning roles and responsibilities, evaluating effectiveness; adds ESG/sustainability risks, scenario planning, AI impacts, and documentation of board deliberations.	Broader scope with explicit regulatory alignment, integration of emerging risks, sustainability considerations, and evidence-based oversight requirements.

APPENDIX III

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
APPENDIX III GUIDING QUESTIONS IN RESPECT OF RISK APPETITE: *Expanded from 7 to 11 questions with added focus on emerging risks and practice consistency.*		
Provides seven suggested board questions on risk appetite covering clarity on acceptable risks, RM maturity, robustness of approach, stakeholder input, proportionality, and evidence of implementation.	Expands to 11 questions, adding alignment of risk appetite to strategy/objectives/capacity, consistency of RM practices across company, adequacy of mitigation factors, satisfaction with management's presentation of risks (including emerging risks), and frequency of board risk assessments.	Broader and more granular oversight focus, incorporating emerging risk evaluation, practice consistency, and periodic reassessment of risk appetite.

REFERENCES

SORMIC GUIDE 2012	SORMIC GUIDE 2025	KEY CHANGES / NOTES
REFERENCES: *New formal list of authoritative sources for credibility and cross-checking.*		
No separate reference section.	Includes a dedicated reference list of authoritative sources: Bursa LR & guidance notes, MCCG, COSO frameworks, IIA materials, IFRS S1/S2, TCFD/TNFD, EU CSRD, GHG Protocol, and IIA Foundation risk survey.	Adds formal referencing to support credibility, facilitate cross-checking, and align with global/regional best practices.

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