



MALAYSIAN INSTITUTE
OF ACCOUNTANTS
ACCOUNTANTS: MANAGERS OF VALUE

AAPG 3
(Revised November 2022)
February 2018

Audit and Assurance Practice Guide 3

**Guidance for Auditors on Engagements to
Report on the Statement on Risk Management and
Internal Control included in the Annual Report**

This AAPG 3 is adapted from the previously issued RPG 5 (Revised 2015).

AUDIT AND ASSURANCE PRACTICE GUIDE 3

Guidance for Auditors on Engagements to Report on the Statement on Risk Management and Internal Control included in the Annual Report

Foreword

The Malaysian Institute of Accountants has approved the issue of this revised Audit and Assurance Practice Guide (AAPG) for issuance to members for guidance.

This AAPG is issued to provide guidance for auditors in applying Malaysian Approved Standard on Assurance Engagements, International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information* in the performance of a limited assurance engagement to report on the Statement on Risk Management and Internal Control included in the annual report.

This AAPG should be read in conjunction with the Preface to Malaysian Approved Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements, which sets out the application and authority of AAPGs.

AUDIT AND ASSURANCE PRACTICE GUIDE 3
GUIDANCE FOR AUDITORS ON ENGAGEMENTS TO REPORT ON THE
STATEMENT ON RISK MANAGEMENT AND INTERNAL CONTROL INCLUDED
IN THE ANNUAL REPORT

CONTENTS

		Paragraph
1.	Introduction	1-4
2.	Background to Malaysian Approved Standard on Assurance Engagements, ISAE 3000 (Revised), <i>Assurance Engagements Other than Audits or Reviews of Historical Financial Information</i>	5-8
3.	Scope of this Audit and Assurance Practice Guide (AAPG)	9-11
4.	Conduct of an Assurance Engagement in Accordance with ISAE 3000 (Revised)	12
5.	Ethical Requirements	13-14
6.	Quality Management	15
7.	Objectives	16
8.	Engagement Acceptance	17-23
9.	Professional Scepticism, Professional Judgement, and Assurance Skills and Techniques	24
10.	Planning and Performing the Engagement	25-32
11.	Obtaining Evidence	33-40
12.	Subsequent Events	41-43
13.	Forming the Assurance Conclusion	44
14.	Preparing the Limited Assurance Report	45
15.	Reporting by Exception	46-48
16.	Emphasis of Matter and Other Matter Paragraphs	49
17.	Modified Conclusions	50
18.	Other Communication Responsibilities	51-53
19.	Documentation	54-56
20.	Effective Date	57

Appendices

- 1 Guidance Notes in the Malaysian Code on Corporate Governance (as at 28 April 2021) (MCCG 2021): Extracted from Part II of Principle B of the MCCG 2021 dealing with Effective Risk Management and Internal Control Framework
- 2 Example of an Engagement Letter
- 3 Example of statements included in the SORMIC in accordance with the SRMICG and possible evidence to support these statements
- 4 Example of a Representation Letter
- 5 Example of Independent Limited Assurance Report
- 6 Extracts of Relevant Bursa Malaysia Securities Berhad Listing Requirements
- 7 Extracts of Statement on Risk Management and Internal Control: Guidance for Directors of Listed Issuers (SRMICG)

Introduction

1. Paragraph 15.26(b) of the Main Market and rule 15.26(b) of the ACE Market Listing Requirements of Bursa Malaysia Securities Berhad (Listing Requirements) require a listed issuer/corporation to include a statement about the state of risk management and internal control (SORMIC or Statement on Risk Management and Internal Control) in the annual report.
2. Paragraph 15.23 and rule 15.23 of the Listing Requirements require a listed issuer/corporation to ensure that the external auditor reviews the SORMIC made by the Board of Directors pursuant to paragraph 15.26(b) and rule 15.26(b) and reports the results of the review to the Board of Directors.
3. Practice Note 9, Risk Management and Internal Control, Corporate Governance and Sustainability Statement of the Main Market Listing Requirements and Guidance Note 11, Risk Management and Internal Control, Corporate Governance and Sustainability Statement of the ACE Market Listing Requirements of Bursa Malaysia Securities Berhad (Bursa Malaysia) requires a listed issuer/corporation to address the Principle, Intended Outcome and Practices read together with the Guidance in the Malaysian Code on Corporate Governance (as at 28 April 2021) (MCCG 2021) in the SORMIC, namely the following:

- (a) Part II of Principle B of the MCCG 2021 with the 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.

- (b) Part II of Principle B of the MCCG 2021 with the following Practices read together with the Guidance of the MCCG 2021 as follows will bring about the intended outcomes:

Practices

- 10.1 The board should establish an effective risk management and internal control framework.
- 10.2 The board should disclose the features of its risk management and internal control framework, and the adequacy and effectiveness of this framework.

- 10.3 The board establishes a Risk Management Committee, which comprises a majority of independent directors, to oversee the company's risk management framework and policies.¹

Guidances

The Guidance G10.1 and G10.2 are enclosed in Appendix 1. These are extracted from the MCCG 2021.

4. In preparing the SORMIC, a listed issuer/corporation should be guided by the "Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers" (SRMICG) which is issued by the Task Force on Internal Control in December 2012 with the support and endorsement of the Bursa Malaysia. The SRMICG is effective from financial year ended 31 December 2012.

The SRMICG sets out internal control and risk management practices in place in the Company which includes the following:

- Commentary on the adequacy and effectiveness of the risk management and internal control system;
- Affirmation that a review on the adequacy and effectiveness of the risk management and internal control system has been undertaken; and
- Assurance received from the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) whether the Company's risk management and internal control system is operating adequately and effectively in all material aspects based on the risk management and internal control system of the Company.

Background to Malaysian Approved Standard on Assurance Engagements, ISAE 3000 (Revised), Assurance Engagements Other than Audits or Reviews of Historical Financial Information

5. Malaysian Approved Standard on Assurance Engagements, ISAE 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information* (ISAE 3000 (Revised)) deals with assurance engagements other than audits or reviews of historical financial information.
6. The auditors shall comply with ISAE 3000 (Revised) when performing an assurance engagement to report on the SORMIC. ISAE 3000 (Revised) uses the terms "reasonable assurance engagement" and "limited assurance engagement". For the

¹ This is a Step-Up provision. Companies are strongly encouraged to adopt the Step-Up practices (in the Code) and when they do, to disclose the application of these practices to demonstrate their commitment to higher standards of corporate governance. The Step-Up practices encourage companies to go further in achieving corporate governance excellence. All listed companies, irrespective of size are encouraged to adopt these practices, in particular Large Companies.

purposes of applying this AAPG, the auditor shall apply the principles of a limited assurance engagement under ISAE 3000 (Revised).

7. The objective of a limited assurance engagement is a reduction in assurance engagement risk to a level that is acceptable in the circumstances of the engagement but where that risk is greater than for a reasonable assurance engagement as the basis for expressing a conclusion in a form that conveys whether, based on the procedures performed and evidence obtained, a matter(s) has come to the auditors' attention to cause the auditor to believe the subject matter is materially misstated. In limited assurance engagement, the auditor chooses a combination of assurance procedures, which can include: inspection; observation; confirmation; recalculation; reperformance; analytical procedures; and inquiry. Determining the assurance procedures to be performed on a particular engagement is a matter of professional judgement.
8. The level of assurance engagement risk is greater in a limited assurance engagement than in a reasonable assurance engagement because of the different nature, timing or extent of evidence-gathering procedures. However, in a limited assurance engagement, the combination of the nature, timing, and extent of evidence gathering procedures is at least sufficient for the practitioner (for the purpose of this AAPG referred to as "auditor") to obtain a meaningful level of assurance as the basis for a negative form of expression. To be meaningful, the level of assurance obtained is likely to enhance the intended users' confidence about the subject matter information to a degree that is clearly more than inconsequential.

Scope of this Audit and Assurance Practice Guide (AAPG)

9. This AAPG is issued to provide guidance to auditors in applying ISAE 3000 (Revised) in the performance of a limited assurance engagement to report on the SORMIC included in the annual report but is not intended to be a substitute for reading the standard itself.
10. The auditor is not required to consider whether the SORMIC covers all risks and controls, or to form an opinion on the adequacy and effectiveness of the Company's risk management and internal control system including the assessment and opinion by the Board of Directors and management thereon. The auditor is also not required to consider whether the processes described to deal with material internal control aspects of any significant problems disclosed in the annual report will, in fact, remedy the problems.
11. Malaysian Approved Standard on Auditing, ISA 701, *Communicating Key Audit Matters in the Independent Auditor's Report* prescribes the auditor's responsibility to communicate key audit matters in the auditors' report. The auditor also considers key audit matters reported by the auditor in the performance of a limited assurance engagement to report on the SORMIC in accordance with the guidance in this AAPG.

Conduct of an Assurance Engagement in Accordance with ISAE 3000 (Revised)

12. The auditor shall not represent compliance with ISAE 3000 (Revised) unless the auditor has complied with the requirements of ISAE 3000 (Revised) relevant to the performance of a limited assurance engagement to report on the SORMIC.

Ethical Requirements

13. The auditor shall comply with the By-Laws (On Professional Ethics, Conduct and Practice) of the Malaysian Institute of Accountants, issued by the Council of the Malaysian Institute of Accountants.
14. The By-Laws provides a framework of principles that members of assurance teams, firms and network firms use to identify threats to independence, evaluate the significance of those threats and, if the threats are other than clearly insignificant, identify and apply safeguards to eliminate the threats or reduce them to an acceptable level, such that independence of mind and independence in appearance are not compromised.

Quality Management

15. The auditor shall design, implement and operate a system of quality management (including policies and procedures to be put in place) as required by ISAE 3000 (Revised).²

Objectives

16. The objectives of the auditor are:
 - (a) To obtain limited assurance about whether the SORMIC to be included in the annual report has been prepared, in all material respects, on the basis of the reporting criteria as set out in paragraphs 41 and 42 of the SRMICG; and
 - (b) To report, in accordance with the auditor's findings, about whether anything has come to the auditor's attention that causes the auditor to believe, on the basis of the procedures performed and evidence obtained, that the SORMIC intended to be included in the annual report is not prepared, in all material respects, in accordance with the disclosures required by paragraphs 41 and 42 of the SRMICG to be set out, nor is factually inaccurate.

² ISAE 3000 (Revised), paragraphs 31-36 (including conforming and consequential amendments to ISAE 3000 (Revised) as a Result of the New and Revised Quality Management Standards)

Engagement Acceptance

17. The auditor shall accept an assurance engagement to report on the SORMIC only when the requirements of ISAE 3000 (Revised) with respect to engagement acceptance have been met.³
18. Before agreeing to accept a limited assurance engagement to report on the SORMIC, the auditor shall:
 - (a) Determine that those persons who are to perform the engagement collectively have the appropriate competence and capabilities, including having sufficient time to do so;
 - (b) Assess whether, on the basis of a preliminary knowledge of the engagement circumstances and discussion with the Board of Directors and management, nothing comes to the attention of the auditor to indicate that the requirements of the Institute's By-Laws, ISAE 3000 (Revised) or this AAPG will not be satisfied; and
 - (c) Determine the basis upon which the engagement is to be performed has been agreed with the Board of Directors.
19. In a limited assurance engagement under this AAPG, the intended users are the Board of Directors of the Company and the responsible party would be the party charged with the preparation of the SORMIC for the limited assurance engagement, such as the management of the Company or a delegated committee of the Board of Directors. The Board of Directors subsequently adopts the SORMIC reported upon by the auditor based on the limited assurance engagement, for inclusion in the annual report pursuant to paragraph 15.26(b) of the Listing Requirements.
20. When establishing whether the preconditions for an assurance engagement as required by ISAE 3000 (Revised) are present, the auditor shall determine the suitability of the criteria expected to be applied, including that they exhibit the characteristics set out in ISAE 3000 (Revised).⁴ The auditor shall apply paragraphs 41 and 42 of the SRMIG as the criteria to evaluate or measure the subject matter in performing this limited assurance engagement.
21. In applying the principles of ISAE 3000 (Revised)⁵, the auditor when engaged to report on the SORMIC shall agree the terms of engagement with the Board of Directors of the Company. The terms of engagement shall be recorded in writing.
22. The agreed terms of the engagement shall include:

³ ISAE 3000 (Revised), paragraphs 21-30 (including conforming and consequential amendments to ISAE 3000 (Revised) as a Result of the New and Revised Quality Management Standards)

⁴ ISAE 3000 (Revised), paragraph 24 (b)(ii)

⁵ ISAE 3000 (Revised), paragraph 27

- (a) The objectives and scope of the engagement;
- (b) The responsibilities of the auditor;
- (c) The responsibilities of the Board of Directors and management;
- (d) Identification of the reporting criteria for the preparation of the SORMIC;
- (e) Reference to the expected form and content of any report to be issued by the auditor and a statement that there may be circumstances in which a report may differ from its expected form and content.

23. An example of an engagement letter is included in Appendix 2 of this AAPG.

Professional Scepticism, Professional Judgement, and Assurance Skills and Techniques

24. The auditor shall apply professional scepticism, exercise professional judgement and apply assurance skills and techniques in planning and performing an assurance engagement on SORMIC as required by ISAE 3000 (Revised).⁶

Planning and Performing the Engagement

Planning

25. The auditor shall plan the engagement so that it will be performed in an effective manner as required by ISAE 3000 (Revised).⁷
26. In planning and performing the engagement, the auditor shall obtain an understanding of how the SORMIC has been prepared by considering, for example:
- (a) The approach in identifying disclosures to be included in the SORMIC;
 - (b) Competency of personnel preparing the SORMIC;
 - (c) Significant deficiencies in internal control identified during the audit of financial statements and through internal audit activities; and
 - (d) The nature and extent of oversight in the preparation of the SORMIC.
27. The auditor applies the knowledge and understanding of the operations of the Company obtained during the audit of financial statements of the Company, including

⁶ ISAE 3000 (Revised), paragraphs 37-39

⁷ ISAE 3000 (Revised), paragraph 40

knowledge of risk management and internal controls, in performing a limited assurance engagement to report on the SORMIC.

28. Malaysian Approved Standard on Auditing, ISA 265, *Communicating Deficiencies in Internal Control to Those Charged with Governance and Management* requires, among other things, that the auditor shall communicate in writing significant deficiencies in internal control identified during the audit to those charged with governance on a timely basis. The responsible party should consider such deficiencies reported by the auditor in the preparation of the SORMIC.

Materiality

29. When planning and performing the engagement, that auditor shall consider materiality with respect to evaluating whether the SORMIC has been prepared, in all material respects, on the basis of the reporting criteria, paragraphs 41 and 42 of the SRMICG.
30. The auditor considers materiality when determining the nature, timing and extent of evidence-gathering procedures, and when evaluating whether the subject matter information is free of material misstatement for the purposes of issuing the limited assurance report. Considering materiality requires the auditor to understand and assess what factors might influence the decisions of the intended users, i.e. the Board of Directors of the Company.
31. As paragraphs 41 and 42 of the SRMICG allow for variations in the presentation of the subject matter information, the auditor considers how the adopted presentation might influence the decisions of the intended users. Materiality is considered in the context of quantitative and qualitative factors, such as relative magnitude, the nature and extent of the effect of these factors on the evaluation of the SORMIC, and the interests of the intended users.
32. A misstatement in the context of an engagement performed under this AAPG is defined as the non-disclosure of one or more of the disclosures required by paragraphs 41 and 42 of the SRMICG to be set out, or a disclosure in the SORMIC that is factually inaccurate. For example, if the SORMIC does not disclose the process applied to deal with the material internal control aspects of any significant problems that are disclosed in the annual report this would constitute a misstatement.

Obtaining Evidence

33. The auditor shall perform procedures to obtain sufficient appropriate evidence to base the auditors' conclusion on the SORMIC.
34. If the auditor becomes aware of a matter(s) that causes that auditor to believe that the SORMIC may be materially misstated, the auditor shall design and perform additional procedures to obtain further evidence until the auditor is able to:
- (a) Conclude that the matter is not likely to cause the SORMIC to be materially misstated; or

- (b) Determine that the matter(s) causes the SORMIC to be materially misstated.⁸
35. Appendix 3 of this AAPG contains examples of statements included in the SORMIC in accordance with the SRMICG and examples of procedures to obtain sufficient appropriate evidence to support these statements.
36. The auditor shall also read the SORMIC as a whole to identify whether other information included in the SORMIC is consistent with the understanding of the auditor of the Company and is factually accurate. Other information in the SORMIC relates to disclosures other than those required by paragraphs 41 and 42 of the SRMICG.

Written Representation

37. In applying the principles of ISAE 3000 (Revised)⁹, the auditor shall obtain written representations from the responsible party.
38. These written representations are obtained as close as possible to or on the date of the limited assurance report, but not after the date, and cannot replace other evidence which the auditor can reasonably expect to be available.
39. The auditor shall evaluate written representations in accordance with ISAE 3000 (Revised).¹⁰
40. An example of a Representation Letter is included in Appendix 4 of this AAPG.

Subsequent Events

41. In accordance with paragraph 37 of the SRMICG, the annual assessment should consider issues dealt with in reports reviewed by the Board of Directors during the year together with any additional information necessary to ensure that it has taken into account all significant aspects of risks and internal control of the Company for the year under review and up to the date of approval of the SORMIC for inclusion in the annual report.
42. Therefore, in applying the principles of ISAE 3000 (Revised)¹¹, the auditor shall consider subsequent events up until the date of the limited assurance report, and shall respond appropriately to facts that become known to the auditor after the date of the assurance report, that, had they been known to the auditor at that date, may have caused the auditor to amend the assurance report, in accordance with paragraph 43 below.

⁸ ISAE 3000 (Revised), paragraph 49L

⁹ ISAE 3000 (Revised), paragraph 56

¹⁰ ISAE 3000 (Revised), paragraphs 58 - 60

¹¹ ISAE 3000 (Revised), paragraph 61

43. The extent of consideration of subsequent events depends on the potential for such events to affect the SORMIC and to affect the appropriateness of the auditor's conclusion. However, the auditor has no responsibility to perform any procedures regarding the SORMIC after the date of the assurance report.

Forming the Assurance Conclusion

44. The auditor shall evaluate the sufficiency and appropriateness of the evidence obtained in the context of the engagement and, if necessary, attempt to obtain further evidence. If the auditor is unable to obtain necessary further evidence, the auditor shall consider implications for the auditor's conclusion in accordance with ISAE 3000 (Revised).¹²

Preparing the Limited Assurance Report

45. The limited assurance report shall include the following basic elements:
- (a) A title that clearly indicates the report is an independent limited assurance report.
 - (b) The addressee of the assurance report: an addressee identifies the Board of Directors to whom the limited assurance report is directed.
 - (c) An identification and description of the limited assurance engagement:
 - The nature of the engagement;
 - The financial period to which the engagement relates; and
 - The name of the entity to which the subject matter relates.
 - (d) The responsibilities of the responsible party for the preparation of the SORMIC and of the Board for its ultimate issuance in the annual report.
 - (e) Identification of the applicable criteria: this informs the Board of Directors how the SORMIC was evaluated so as to enable the Board of Directors to understand the basis of the auditor's conclusion.
 - (f) Auditors' responsibilities: this informs the auditors' role is to independently express a conclusion about the SORMIC.
 - (g) A statement that the engagement was performed in accordance with Malaysian Approved Standard on Assurance Engagements, ISAE 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, and the guidance published in AAPG 3, *Guidance for Auditors on*

¹² ISAE 3000 (Revised), paragraph 64

Engagements to Report on the Statement on Risk Management and Internal Control Included in the Annual Report.

- (h) A statement that the firm applies Malaysian Approved Standard on Quality Management, ISQM 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*¹³.
- (i) A statement that the auditor has complied with the independence and other ethical responsibilities of the *By-Laws (on Professional Ethics, Conduct and Practice)* of the Malaysian Institute of Accountants.
- (j) An informative summary of the work performed as a basis for the auditor's conclusion: this informs the evidence-gathering procedures performed to understand the limited assurance conveyed by a conclusion expressed in the negative form.

Because in a limited assurance engagement an appreciation of the nature, timing, and extent of evidence-gathering procedures performed is essential to understanding the assurance conveyed by a conclusion expressed in the negative form, the summary of the work performed shall state that:

- (i) The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement; and
- (ii) Consequently, the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed;

The summary of work performed, shall also include:

- (i) The fact that the engagement is conducted to obtain limited assurance about whether the SORMIC has been prepared, in all material respects, on the basis of the reporting criteria as set out in paragraphs 41 and 42 of the SRMICG and is factually accurate.
- (ii) The fact that the auditors are not required to assess whether all risks and controls have been addressed by the Board of Directors or to form an opinion on the adequacy and effectiveness of the Company's risks and control procedures including the assessment and opinion by the Board of Directors and management thereon.
- (iii) The fact that the auditors are not required to assess whether the processes described to deal with material internal control aspects of

¹³ Effective on or after 15 December 2022

any significant problems disclosed in the annual report and financial statements will, in fact, remedy the problems.

- (iv) The fact that in a limited assurance engagement, the scope of evidence gathering procedures is less comprehensive than in a reasonable assurance engagement, and therefore less assurance is obtained than in a reasonable assurance engagement.
- (k) The auditors' conclusion: the conclusion shall be expressed in a form that conveys whether, based on the procedures performed and evidence obtained, a matter(s) has come to the auditor's attention to cause the auditor to believe that the SORMIC intended to be included in the annual report is not prepared, in all material respects, in accordance with the disclosures required by paragraphs 41 and 42 of the SRMICG to be set out, nor is the SORMIC factually inaccurate.
- (l) The restriction on distribution or use: the report should contain a statement restricting the use of the report to the Board of Directors in accordance with the listing requirements of Bursa Malaysia and for no other purposes.
- (m) The name of the firm.
- (n) The date of the limited assurance report.
- (o) The location in the jurisdiction where the auditor practices.

An example of Independent Limited Assurance Report is included in Appendix 5 of this AAPG.

Reporting by Exception

46. The auditors shall report the following circumstances to the responsible party and the Board of Directors with a view to seek revision of the SORMIC, if they conclude that there is:
- (a) A material misstatement in the disclosures in the SORMIC as required by paragraphs 41 and 42 of the SRMICG;
 - (b) A material misstatement or inconsistency in the other information contained in the SORMIC; or
 - (c) Insufficient appropriate evidence to support one or more disclosures made in the SORMIC pursuant to the requirements of paragraphs 41 and 42 of the SRMICG.
47. If revisions sought are not accepted, the auditors shall consider the guidance in paragraphs 51 to 53 of this AAPG if these revisions are deemed material.

48. If the effects of the uncorrected misstatements are not material, the auditor shall request that these uncorrected misstatements be included in the representation letter.

Emphasis of Matter and Other Matter Paragraphs

49. In applying the principles of ISAE 3000 (Revised),¹⁴ if the auditor considers it necessary to:
- (a) Draw the Board of Directors attention to a matter presented or disclosed in the SORMIC that, in the auditor's judgement, is of such importance that it is fundamental to the Board of Directors understanding of whether the SORMIC has been prepared, in all material respects, on the basis of the reporting criteria as set out in paragraphs 41 and 42 of the SRMIGG (an Emphasis of Matter paragraph); or
 - (b) Communicate a matter other than those that are presented or disclosed in the SORMIC that, in the auditor's judgement, is relevant to the Board of Directors understanding of the engagement, the auditor's responsibilities or the assurance report (an Other Matter paragraph);

the auditor shall do so in a paragraph in the assurance report, with an appropriate heading, that clearly indicates the auditor's conclusion is not modified in respect of the matter. In the case of an Emphasis of Matter paragraph, such a paragraph shall refer only to information presented or disclosed in the SORMIC.

Modified Conclusions

50. In applying the principles of ISAE 3000 (Revised)¹⁵, the auditor shall not express an unqualified conclusion when the following circumstances exist and, in the auditor's judgement, the effect of the matter is or may be material:
- (a) When, in the auditor's professional judgement, a scope limitation exists and the effect of the matter could be material. The auditor shall express a qualified conclusion or a disclaimer conclusion;
 - (b) There is a material non-disclosure of information required by paragraphs 41 and 42 in the SORMIC. The auditors shall express a qualified conclusion or an adverse conclusion.; or
 - (c) There is a material misstatement or inconsistency in the information contained in the SORMIC. The auditor shall express a qualified conclusion or an adverse conclusion.

¹⁴ ISAE 3000 (Revised), paragraph 73

¹⁵ ISAE 3000 (Revised), paragraphs 74-77

Other Communication Responsibilities

51. The auditor shall consider other communication responsibilities, including the appropriateness of communicating relevant matters of governance interest arising from this limited assurance engagement with the Board of Directors, as required by ISAE 3000 (Revised).¹⁶
52. If the auditor believes that the responsible party or the Board of Directors will not take appropriate action to avoid a modified conclusion, the auditor shall consider one or more of the following actions
 - (a) Withdrawing from the engagement;
 - (b) Consider impact on auditors' report in the audit of financial statements; or
 - (c) Reporting the qualified, adverse or disclaimer of opinion to Bursa Malaysia, provided the auditor has included a reference to such possibility in the terms of the engagement.
53. The auditor shall, if he chooses to do so, allow the Board of Directors to include in the annual report a statement that the SORMIC has been reviewed by the auditor and reported on pursuant to this AAPG. Where such a statement is set out, the auditor shall also require that the conclusions set out in the report issued should be suitably described.

Documentation

54. The auditor shall prepare documentation in accordance with ISAE 3000 (Revised)¹⁷.
55. The auditor shall document matters that are significant in providing evidence that supports the limited assurance report and that the limited assurance engagement was performed in accordance with ISAE 3000 (Revised) and the requirements of this AAPG.
56. In determining the extent of documentation to be prepared and retained the auditor may consider what is necessary to provide an understanding of the work performed on the basis of the principal decisions taken to another experienced auditor who has no experience with the engagement. This understanding is not expected to extend to the detailed aspects of the engagement without discussion with the auditor who prepared the documentation.

¹⁶ ISAE 3000 (Revised), paragraph 78

¹⁷ ISAE 3000 (Revised), paragraphs 79-83

Effective date

57. This AAPG is effective for limited assurance reports dated on or after 15 December 2022. Earlier adoption is permitted.

Appendix 1**Guidance in the Malaysian Code of Corporate Governance (As at 28 April 2021) (MCCG 2021): Extracted from Part II of Principle B of the MCCG 2021 Dealing with 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.

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 term is acceptable.

Appendix 2**Example of an Engagement Letter**

The following is an illustrative example of paragraphs that may be included in the auditor's engagement letter dealing with their responsibilities with respect to the Board of Directors' Statement on Risk Management and Internal Control as required by the Bursa Malaysia Securities Berhad Listing Requirements.

To the Board of Directors

We are writing to confirm the terms and conditions upon which we have been engaged to review and report on the statement on the state of risk management and internal control (Statement on Risk Management and Internal Control) intended to be included in the annual report for the financial [year/period] ended required to be provided by the Board of Directors pursuant to the [Bursa Malaysia Securities Berhad (Bursa Malaysia) Main Market Listing Requirements/ Bursa Malaysia Securities Berhad (Bursa Malaysia) ACE Market Listing Requirements].

Responsibilities of Board of Directors and Management

Management or a delegated committee of the Board of Directors or a specified party appointed by the Board of Directors are responsible for the preparation of Statement on Risk Management and Internal Control (SORMIC) in accordance with the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers (SRMICG) issued by Bursa Malaysia Securities Berhad.

The SORMIC should include sufficient and meaningful information needed by shareholders to make an informed assessment of the main features and adequacy of the Company's risk management and internal control system in accordance with paragraphs 41 and 42 of SRMICG.

Whilst the SORMIC is required to be in respect of the financial [year/period] covered by the financial statements included in the annual report and up to the date of approval of the SORMIC for inclusion in the annual report, if the Board of Directors become aware of events occurring between the date of approval of the SORMIC for inclusion in the annual report and the date of approval of the annual report, which materially affect the SORMIC, the Board of Directors should consider whether such events are properly addressed and adequately disclosed in the SORMIC.

Our responsibilities

Paragraph 15.23 of the Bursa Malaysia Listing Requirements states that the Company must ensure that the external auditors review the SORMIC and report the results thereof to the Board of Directors of the Company.

The objectives of our engagement are to obtain limited assurance about whether the SORMIC to be included in the annual report has been prepared, in all material respects, on the basis of

the reporting criteria as set out in paragraphs 41 and 42 of the SRMICG and to report, in accordance with the our findings, about whether anything has come to our attention that causes the us to believe, on the basis of the procedures performed and evidence obtained, that the SORMIC intended to be included in the annual report is not prepared, in all material respects, in accordance with the disclosures required by paragraphs 41 and 42 of the SRMICG to be set out, nor is the SORMIC factually inaccurate.

Accordingly, we will carry out the engagement in accordance with Malaysian Approved Standard on Assurance Engagements, ISAE 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information* and AAPG 3, *Guidance for Auditors on Engagements to Report on the Statement on Risk Management and Internal Control Included in the Annual Report*.

Scope of Engagement on Statement on Risk Management and Internal Control

We shall request sight of all documentation prepared by or for the Board of Directors in support of the SORMIC. The Board of Directors will provide us or cause the responsible party to provide us with such further information and explanations as we consider necessary. We may request you to provide written confirmation of oral representations which you make to us during the course of our engagement.

In accordance to paragraph 15.23 of the [*Bursa Malaysia Main Market Listing Requirements/ Bursa Malaysia ACE Market Listing Requirements*], our limited assurance procedures primarily comprised:

[Enumerate procedures as required]

As our work is not designed to consider whether the SORMIC covers all risks and controls, or to form an opinion on the adequacy and effectiveness of the Company's risk management and internal control system including the assessment and opinion by the Board of Directors thereon, our work performed will not be designed to enable us to express any assurance as to whether or not your risk management or internal control system is adequate and effective. In addition, our audit of the financial statements should not be relied upon to draw to your attention to matters that may be relevant to your consideration as to whether or not your risk management or internal control system is adequate and effective.

The SORMIC may include assertions on, or the Board of Directors may obtain representations from the management on, the adequacy and effectiveness of the risk management or internal control system of the Company. Our role does not include forming any opinion on the Board of Directors assessment or the management's representation on the adequacy and effectiveness of the Company's risk management and internal control system. Therefore, in no circumstances shall the contents of our report be read, construed or interpreted as any conclusion made or agreement by us with the Board of Directors assessment or management's representation.

If, after reviewing the SORMIC, we identify a material misstatement or inconsistency in the SORMIC and the circumstances are such that in our opinion, the matter has not been

adequately addressed in the SORMIC, we will consider taking further appropriate action, including modification of our limited assurance report.

Fees

Our fees, which will be billed as work progresses, are based on the time required by the individuals assigned to the engagement plus out-of-pocket expenses. Individual hourly rates vary according to the degree of responsibility involved and the experience and skill required. Our fees for this engagement are RM XXXXX (XXXXX only)

Agreement of terms

Please sign and return the attached copy of this letter to indicate that it is in accordance with your understanding of the terms of engagement.

We look forward to full cooperation with your staff and we trust that they will make available to us the relevant records, documentation and other information requested in connection with our engagement.

(Audit firm)

Acknowledged on behalf of
(name of the Company) by

(signed)

.....

Name and Title
Date

Appendix 3

Example of statements included in the SORMIC in accordance with the SRMICG and possible evidence to support these statements

Statement to disclose ‘the process Board applied to deal with material internal control aspects of any significant problems disclosed in the annual report and financial statements’

Procedures that may be performed with respect to this statement include:

- (a) Obtain an understanding of the processes applied by the Board of Directors to ensure that significant problems are disclosed in the annual report and financial statements.
- (b) Review documentation to support the processes described.
- (c) Review the adequacy of the information provided and assess if the disclosure appropriately reflects the processes the Board of Directors have adopted.

Statement to disclose ‘the process Board (or where applicable, its committees) has applied in reviewing the risk management and internal control system and confirming that necessary actions have been or are being taken to remedy any significant failings or weaknesses identified from that review’

Procedures that may be performed with respect to this statement include:

- (a) Obtain an understanding, through enquiring of the Board of Directors, of the process the Board (or where applicable, its committees) has applied in reviewing the risk management and internal control system and compare that understanding to the SORMIC intended to be included in the annual report.
- (b) Discuss with the Board of Directors, the actions that the Board has already taken, or being taken, with respect to identified significant failings or weaknesses.
- (c) Review documentation prepared for the Board of Directors to support the SORMIC and assess whether or not it provides sound support for the SORMIC.
- (d) Relate the SORMIC to the auditor’s knowledge of the Company obtained during the audit of financial statements.

Appendix 4

Example of a Representation Letter

Client's Letterhead

[To Auditor]

[Date]

Dear Sir,

This representation letter is provided in connection with your limited assurance engagement on the Statement on Risk Management and Internal Control (SORMIC) of [name of the Company¹⁸] intended to be included in the annual report for the financial [year/period] ended for the purposes of expressing a conclusion whether anything has come to your attention that causes you to believe that the SORMIC is not prepared, in all material respects, in accordance with the disclosures required by paragraphs 41 and 42 of the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers (SRMICG) to be set out, nor is the SORMIC factually inaccurate.

Accordingly, we make the following representations, which are true to the best of our knowledge and belief:

1. The SORMIC referred to above has been prepared and presented in compliance with the disclosures required by paragraphs 41 and 42 of the SRMICG.
2. [To describe the responsible party] are responsible for the preparation of the SORMIC.
3. The Board of Directors have acknowledged responsibility for the design and implementation of internal control to prevent and detect fraud and error.
4. The Board of Directors have during the [year/period] carried out reviews of the adequacy of the Group's system of internal controls, covering all controls including financial, operational and compliance controls, premised upon a risk based assessment of the Group.
5. There is no material joint venture or associate that has not been dealt with as part of the Group for the purposes of the SORMIC. [Alternative representation: The Group includes material joint ventures and associate companies/Material joint ventures or associates that were not dealt with as part of the Group for the purposes of the SORMIC are as follows: (to list those joint ventures or associates)]

¹⁸ Refers to Group/Company as appropriate

6.
 - (a) There exists an ongoing process within the Group for identifying, evaluating and managing the significant risks faced by the Group.;
 - (b) The ongoing process has been in place for the year under review and up to the date of the SORMIC for inclusion in the annual report.;
 - (c) The ongoing process has been regularly reviewed by the Board of Directors.;
 - (d) The ongoing process is in accordance with the SRMICG.
7. The summary of the processes the Board of Directors have applied in reviewing the adequacy and integrity of internal control disclosed in the SORMIC appropriately reflects those processes applied by the Board of Directors during the financial [year/period].
8. The [refer to the responsible party] have made available to you all the supporting documentation that have been prepared by or for the Board of Directors to support our statement made in connection with the matters described in (6) above and such documentation provides sound support for the assertions in (6) above.
9. The processes that the Board of Directors have applied to deal with material internal control aspects of any significant problems disclosed in the annual report appropriately reflect those processes.
10. The effects of uncorrected misstatements are immaterial, both individually and in the aggregate, to the SORMIC as a whole. A list of the uncorrected misstatements is attached to the representation letter in Appendix I. [Alternative representation: There are no uncorrected misstatements identified during the [year/period] under review for the SORMIC.]
11. There has been no known actual or possible non-compliance with laws and regulations that could have a material effect on the SORMIC in the event of non-compliance. [Alternative representation: The Board of Directors have disclosed to you all known actual or possible non-compliance with laws and regulations that could have a material effect on the SORMIC.]
12. The Board of Directors have disclosed to you all significant facts relating to any known frauds or suspected frauds that may have affected the Group. [Alternative representation: There has been no known instances of fraud or suspected fraud that may have affected the Group.]
13. The [refer to the responsible party] have disclosed to you the results of their assessment of the risk that the SORMIC may be materially misstated as a result of fraud or error. [This representation is only required if there are instances of material fraud or error during the reporting period.]

14. The SORMIC is in respect of the financial period covered by the financial statements and up to the date of approval of the SORMIC for inclusion in the annual report. The Board of Directors have represented that they are not aware of any events occurring between the date of the approval of the SORMIC and the date of approval of annual report, which would materially affect the SORMIC.

Yours faithfully,
(name of the Company)

Signature

Name :
(Position)

Signature

Name :
(Position)

Appendix 5

Example of Independent Limited Assurance Report**Independent Auditors' Limited Assurance Report to the Board of Directors of [Company's name] on the Statement on Risk Management and Internal Control**

We have been engaged to perform a limited assurance engagement on the accompanying Statement on Risk Management and Internal Control intended to be included in the annual report for the financial [year/period] ended as set out in the attachment which has been stamped by us for identification purposes.

[Describe the responsible party] Responsibility

[Refer to the responsible party] are responsible for the preparation of the Statement on Risk Management and Internal Control in accordance with the "Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers" as issued under the Bursa Malaysia listing requirements.

Our Quality Management and Independence

The firm applies Malaysian Approved Standard on Quality Management, ISQM 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* and accordingly, the firm is required to design, implement and operate a system of quality management including policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

We have complied with the independence and other ethical requirements of the *By-Laws (on Professional Ethics, Conduct and Practice)* of the Malaysian Institute of Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

Our Responsibilities

Our responsibility is to express a limited assurance conclusion on the Statement on Risk Management and Internal Control based on the procedures we have performed and the evidence we have obtained as to whether any matters have come to our attention that cause us to believe that the Statement on Risk Management and Internal Control has not been prepared, in all material respects, in accordance with the disclosures required by paragraphs 41 and 42 of the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers to be set out, nor is the SORMIC factually inaccurate.

We conducted our limited assurance engagement in accordance with Malaysian Approved Standard on Assurance Engagements, ISAE 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information* and AAPG 3, *Guidance for Auditors on Engagements to Report on the Statement on Risk Management and Internal Control Included in the Annual Report*.

Summary of Work Performed

Our engagement has been conducted to assess whether the Statement on Risk Management and Internal Control appropriately reflects the disclosures required by paragraphs 41 and 42 of the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers.

The procedures performed in a limited assurance engagement vary in nature and timing from, and are less in extent than for, a reasonable assurance engagement and consequently the level of assurance obtained in a limited assurance engagement is substantially lower than the assurance that would have been obtained had a reasonable assurance engagement been performed.

Our limited assurance procedures primarily comprised:

[Enumerate procedures as required]

We are not required to consider whether the Statement on Risk Management and Internal Control covers all risks and controls, or to form an opinion on the adequacy and effectiveness of the Company's risk management and internal control system including the assessment and opinion by the Board of Directors and management thereon. We are also not required to consider whether the processes described to deal with material internal control aspects of any significant problems disclosed in the annual report will, in fact, remedy the problems.

Conclusion

Based on the procedures performed and evidence obtained, nothing has come to our attention that causes us to believe that the Statement on Risk Management and Internal Control intended to be included in the annual report is not prepared, in all material respects, in accordance with the disclosures required by paragraphs 41 and 42 of the Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers to be set out, nor is the SORMIC factually inaccurate.

Restriction on distribution or use

This report is made solely to the Board of Directors in accordance with the listing requirements of Bursa Malaysia and for no other purposes. We do not assume responsibility to any other person for the content of this report. It should not be copied or disclosed to any third party or otherwise quoted or referred to, in whole or in part, without our prior written consent.

(Audit Firm)

(Date) [to be dated on or after the Board has approved the SORMIC]
Kuala Lumpur

Appendix 6**Extracts of Relevant Bursa Malaysia Securities Berhad Listing Requirements****Main Market Listing Requirements****Requirements of Auditors**

15.23 Review of statements

A listed issuer must ensure that the external auditors review a statement made by the board of directors of a listed issuer pursuant to subparagraph 15.26(b) below, with regard to the state of risk management and internal control of the listed issuer and report the results thereof to the board of directors of the listed issuer.

Statement on Directors 'Responsibilities on Audited Accounts and Internal Control

15.26 Additional statements by the board of directors

A listed issuer must ensure that its board of directors makes the following additional statements in its annual report:

- (a) A statement explaining the board of directors' responsibility for preparing the annual audited financial statements; and
- (b) A statement about the state of risk management and internal control of the listed issuer as a group.

[Cross reference: Practice Note 9]

Ace Market Listing Requirements**Requirements of Auditors**

15.23 Review of statements

A listed corporation must ensure that the external auditors review a statement made by the board of directors of a listed corporation pursuant to Rule 15.26(b) below, with regard to the state of risk management and internal control of the listed corporation and report the results to the board of directors of the listed corporation.

Statement on Directors 'Responsibilities on Audited Accounts and Internal Control

15.26 Additional statements by the board of directors

A listed corporation must ensure that its board of directors makes the following additional statements in its annual report:

- (a) A statement explaining the board of directors' responsibility for preparing the annual audited financial statements; and
- (b) A statement about the state of risk management and internal control of the listed corporation as a group.

[Cross reference: Guidance Note 11]

Appendix 7**Extracts of Statement on Risk Management and Internal Control: Guidelines for Directors of Listed Issuers (SRMICG)**

The Board's Statement on Risk Management and Internal Control

40. The statement pursuant to 15.26(b) of the LR should include sufficient and meaningful information needed by shareholders to make an informed assessment of the main features and adequacy of the Company's risk management and internal control system.
41. In its narrative statement, the board should disclose the following:
- The main features of the Company's risk management and internal control system;
 - The ongoing process for identifying, evaluating and managing the significant risks faced by the Company in its achievement of objectives and strategies;
 - That such process has been in place for the year under review and up to the date of approval of this statement for inclusion in the annual report;
 - The process it (or where applicable, through its committees) has applied in reviewing the risk management and internal control system and confirming that necessary actions have been or are being taken to remedy any significant failings or weaknesses identified from that review;
 - That a review on the adequacy and effectiveness of the risk management and internal control system has been undertaken;
 - Commentary on the adequacy and effectiveness of the risk management and internal control system;
 - The process it has applied to deal with material internal control aspects of any significant problems disclosed in the annual report and financial statements;
 - Where material joint ventures and associates have not been dealt with as part of the Group for the purposes of applying these guidelines, this should be disclosed; and
42. 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, in all material aspects, based on the risk management and internal control system of the Company.



MALAYSIAN INSTITUTE
OF ACCOUNTANTS

Dewan Akauntan, Unit 33-01, Level 33, Tower A, The Vertical, Avenue 3
Bangsar South City, No.8, Jalan Kerinchi, 59200 Kuala Lumpur, Malaysia

[phone] +603 2722 9000

[fax] +603 2722 9100

[web] www.mia.org.my

[email] technical@mia.org.my