

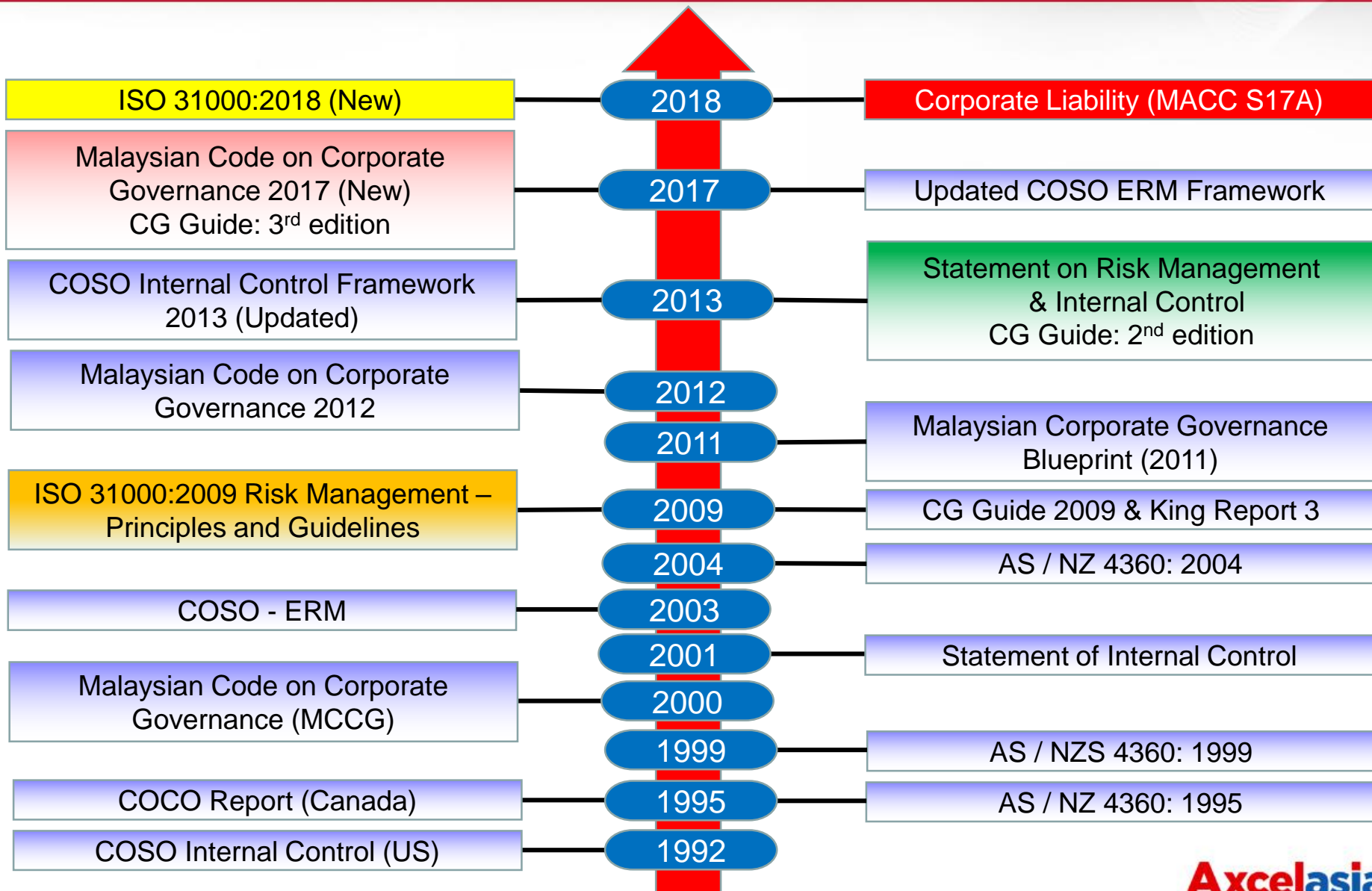


Statement on Risk Management and Internal Control

Its All About An Excellent SORMIC

26 September 2019

Governance, Risk and Controls Framework



MCCG 2017: Risk Management & Internal Control

- **MCCG Practice 9.1:** The board should establish an effective risk management and internal control framework.
- **MCCG Practice 9.2:** The board should disclose the features of its risk management and internal control framework, and the adequacy and effectiveness of this framework.
- ***Step Up: The board establishes a Risk Management Committee, which comprises a majority of independent directors, to oversee the company's risk management framework and policies.***
- *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.*

- **ISO 31000:2018** on principles and guidelines for risk management.
- **Revised COSO ERM 2017:** Integrating with Strategy and Performance.
- **CoCo Framework:** Other globally recognised internal control and risk management frameworks developed by professional organisations (e.g. Criteria of Control Framework developed by the Canadian Institute of Chartered Accountants)

ISO 31000:2018: Principles, Framework & Process

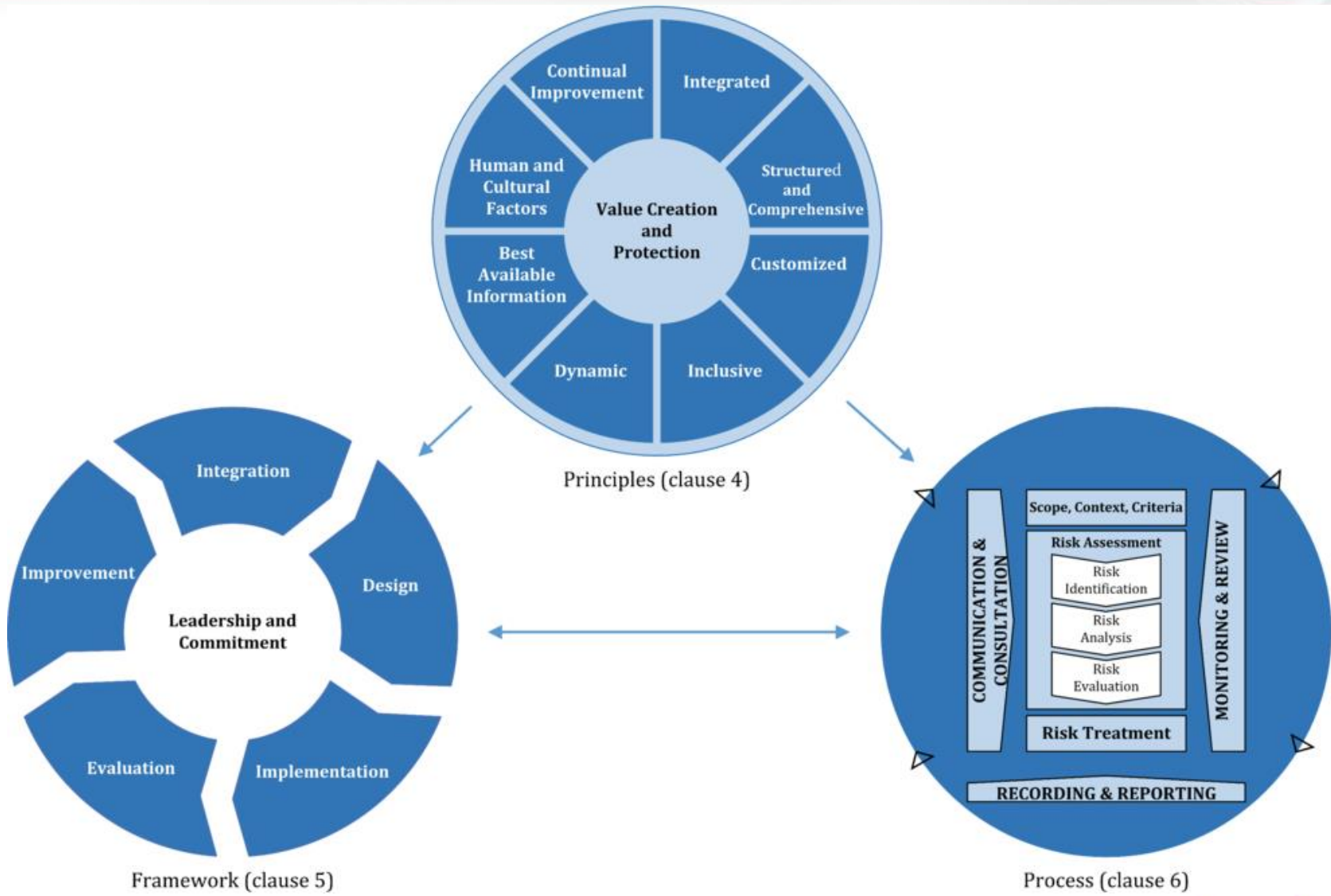


Figure 3—COSO Enterprise Risk Management, Components and Principles

ENTERPRISE RISK MANAGEMENT



Governance and Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy and Objective Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risk
13. Implements Risk Responses
14. Develops Portfolio View

Review and Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, and Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO, *Enterprise Risk Management: Integrating With Strategy and Performance*, USA, 2017. Reprinted with permission.

Bursa Regulations - Key Changes in Respect of Risk Disclosure

A statement containing the management discussion and analysis of the group's business, operations and performance (including financial performance) during the financial year which includes at least the following information:

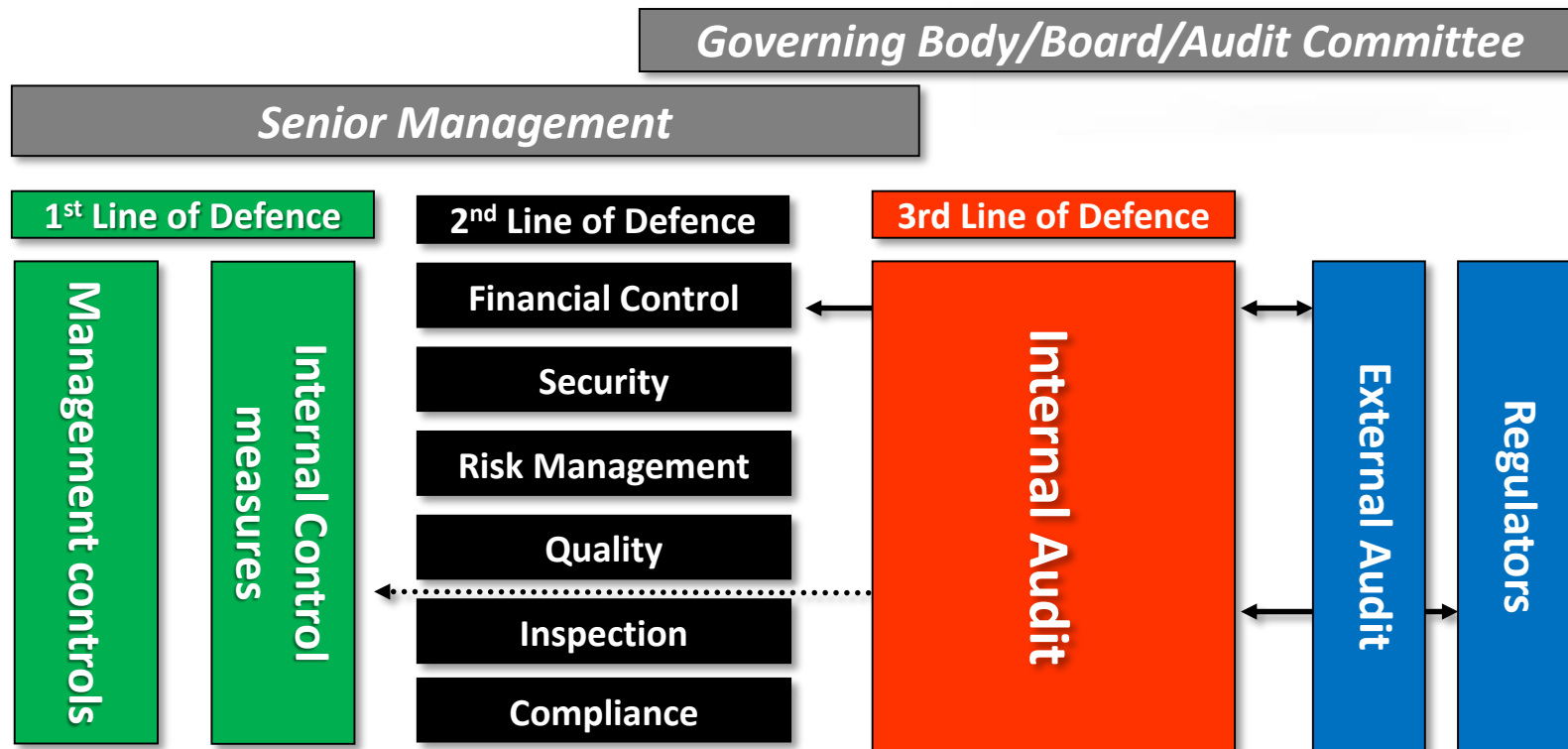
- discussion and analysis of the financial results and financial condition;
- **any identified anticipated or known risks that the group is exposed to which may have a material effect on the group's operations, performance, financial condition, and liquidity together with a discussion of the plans or strategies to mitigate such risks; and**
- forward-looking statement providing commentary on the -
 - group's possible trend, outlook and sustainability of each of its principal business segment;
 - prospects of new businesses or investments; and
 - dividend or distribution policy, if any, and factors contributing to the dividend or distribution for the financial year.

Listing Requirements

- Paragraph 15.25 of the Listing Requirements provides that a listed issuer must include in its annual report, a narrative statement of its corporate governance practices covering its Principles and Recommendations.
- Paragraph 15.26(b) of the Listing Requirements requires a listed issuer to ensure that its board of directors makes a statement in its annual report about the state of risk management and internal control of the listed issuer as a group.

(Reference is made to Practice Note 9 which then makes reference to SORMIC)

Who is Responsible: Three Lines of Defence



(Source: IIA position paper: *The Three Lines of defence in effective risk management and control*)

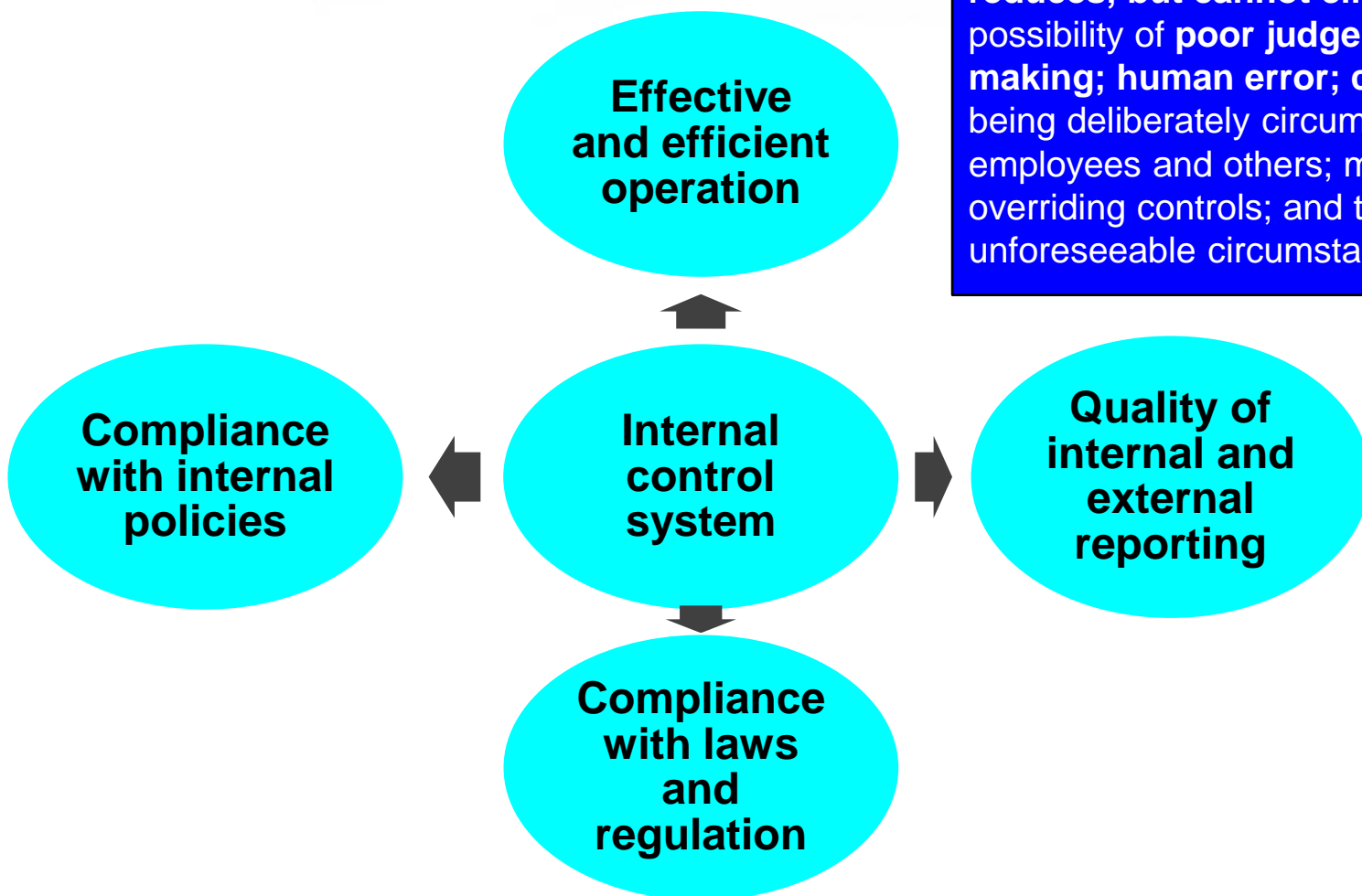
Element of a Sound Risk Management and Internal Control System

- Risk Management (“RM”):
 - RM and control framework is “**embedded**” into the culture, processes and structures of the Company;
 - It is **important** to provide a **control environment**; and
 - Board able to oversee both Company’s performance and risk levels so that management’s performance in achieving strategies and objectives can be monitored.

- Internal Control (“IC”)
 - IC system encompasses the policies, processes, tasks, behaviours and other aspects of a company, taken together;
 - Reflects the control environment which encompasses its organisational structure, governance activities, hiring and related policies & practices, and its code of conduct; and
 - Board’s Deliberation.

Element of a Sound Risk Management and Internal Control System (cont'd)

A sound system of internal control reduces, but cannot eliminate, the possibility of **poor judgement in decision-making; human error; control processes** being deliberately circumvented by employees and others; management overriding controls; and the occurrence of unforeseeable circumstances.



Internal Controls: Using RCSA Approach

A Management Tool for Reinforcing Process Owner Accountability



A Tool to Improve Business Efficiency

SRMIC: Disclosure

- The main features of the Group'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;

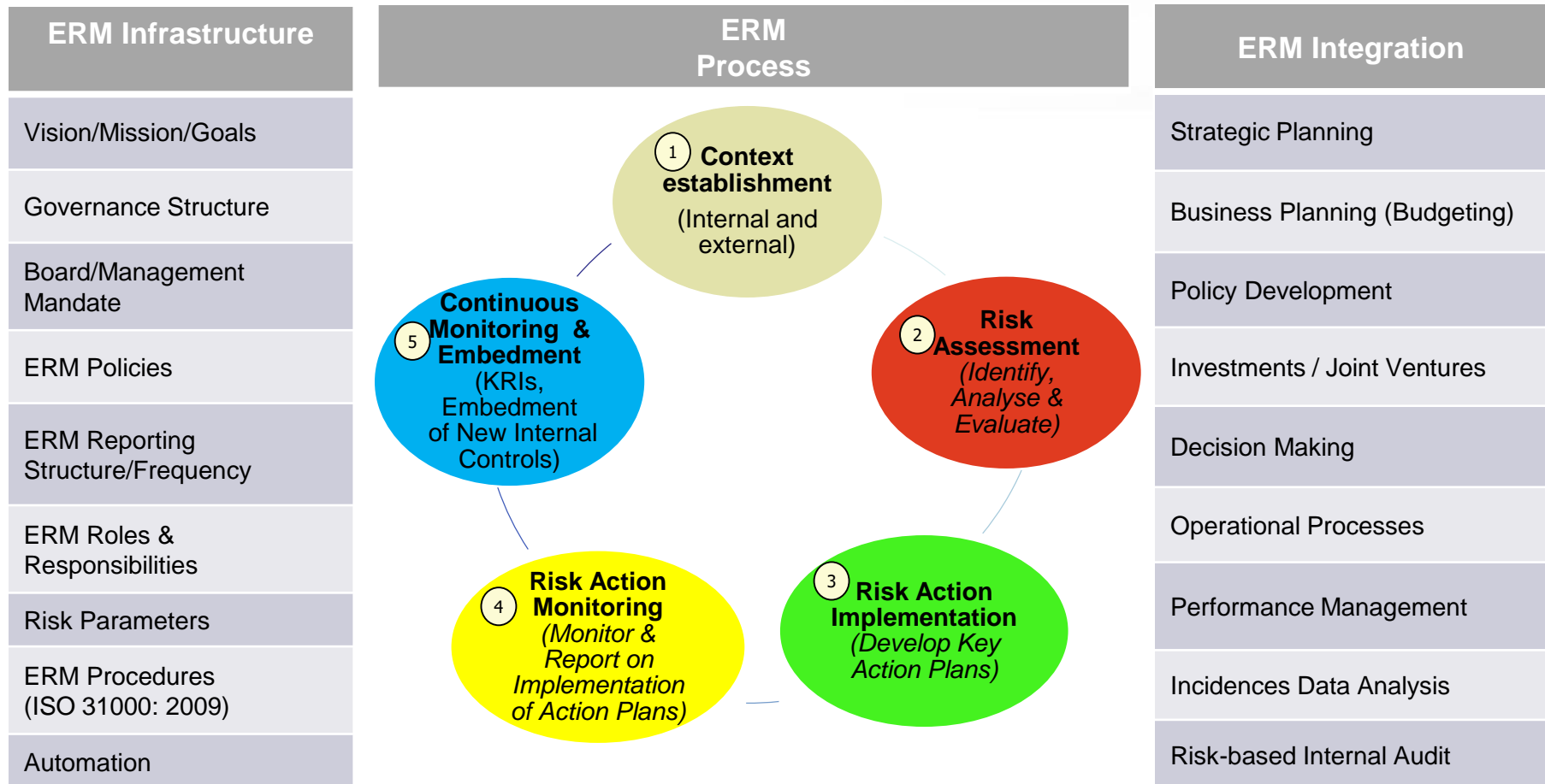
SRMIC: Disclosure

- 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; and
- 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.

In a 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.

ERM Framework

Enterprise Risk Management Framework



Communication

Awareness/Training

Continuous Improvement

Change Management

Confirming the Effectiveness of SORMIC

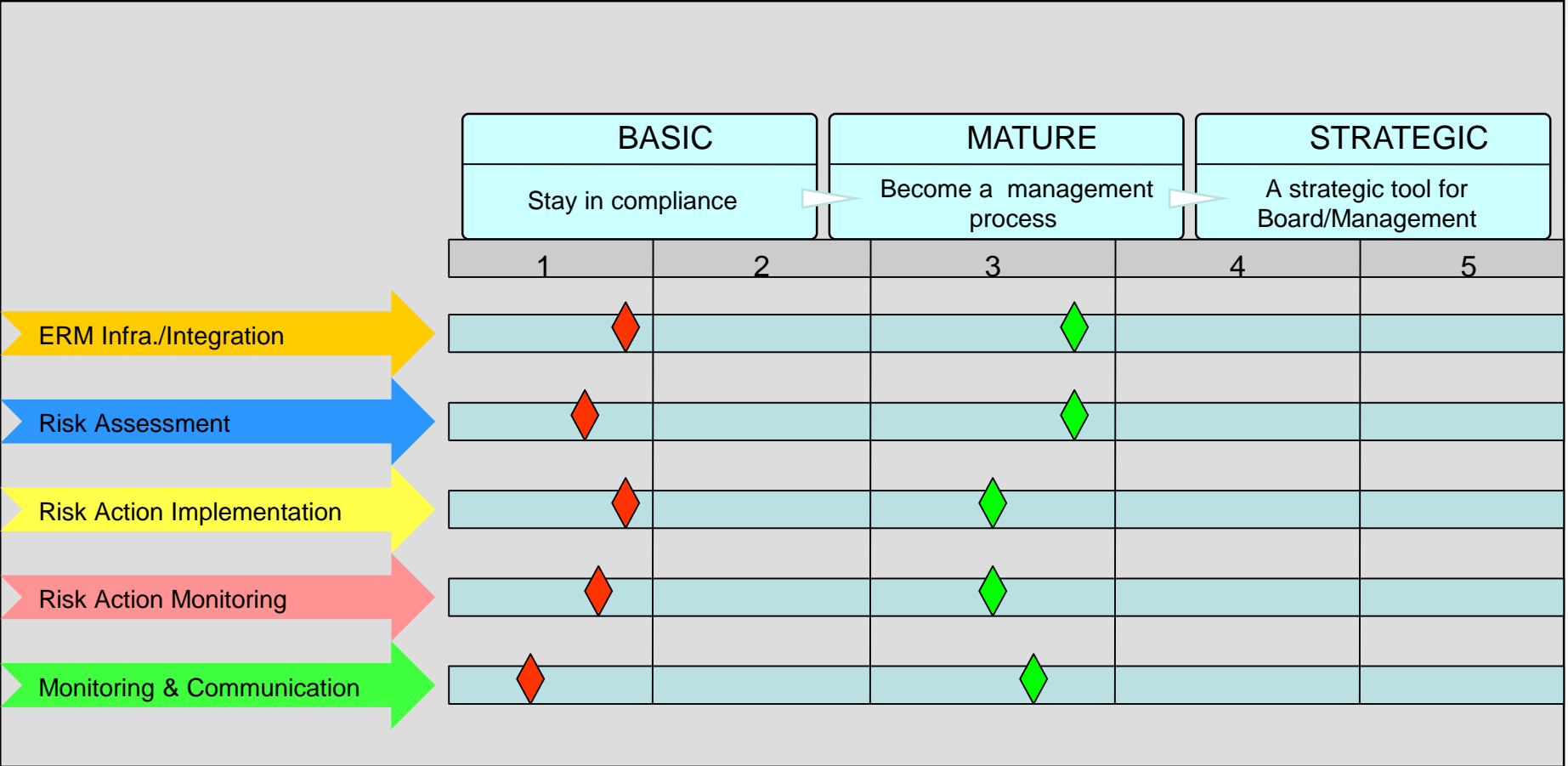
Board responsibility

Board should define the processes to be adopted (both for the ongoing assessment and annual assessment)

Ongoing assessment is required to be reported to the Board

Annual assessment should be performed by the Board

Risk Management Maturity Chart



◆ - Current status

◆ - Desired status in one year time

SRMIC: External Auditor Review

- Paragraph 15.23 of the Listing Requirements requires a listed issuer/corporation to ensure that the external auditor reviews the SORMIC made by the BOD pursuant to paragraph 15.26(b) and rule 15.26(b) and reports the results of the review to the BOD.
- “Negative” opinion is rendered under Audit and Assurance Practice Guide 3 (“AAPG 3 and formerly known as RPG 5”) of MIA.
- Review does NOT address adequacy & effectiveness of Company’s risk management and internal control system.
- Not required to consider whether the SRMIC covers all risks and controls.
- Auditors needs to apply ISAE 3000 in the performance of a limited assurance engagement to report on the SRMIC included in the annual report.

Group Discussion Exercise

- Who is responsible for preparing SRMIC?
- How to confirm that a review on the adequacy and effectiveness of the risk management and internal control system has been undertaken?
- How to provide assurance to the Board? Written or Verbal?
- What are the supporting documents to be retained!
- Group structure?



Contact Details

Axcelasia Columbus Sdn Bhd
1-23-7 Menara Bangkok Bank
Berjaya Central Park
105 Jalan Ampang
50450 Kuala Lumpur
T: +603 - 21818865
F: +603 - 21818867
www.axcelasia.com

Ranjit Singh
rs@axcelasia.com



Axcelasia Columbus Sdn Bhd is a subsidiary company of Axcelasia Inc., a company incorporated in Malaysia and listed on the Singapore Stock Exchange.

The use of this Document is solely for internal purpose by the recipient. This Document is not for general circulation or publication nor is it to be reproduced, either in part or in full, for any other purpose without our prior written consent.