Singapore Quick Guide to the COSO Enterprise Risk Management and Internal Control Frameworks
2016 Edition
The Protiviti-SAC COSO Academy

The Protiviti-SAC COSO Academy in Singapore was formed by global business consulting and internal audit firm Protiviti and the Singapore Accountancy Commission (SAC) in November 2014. Its mission is to advocate the adoption of the COSO Frameworks in Singapore as well as raise awareness on how the COSO Frameworks can help companies improve organizational performance through better corporate governance, stronger internal controls and achieve greater investor confidence. The Protiviti-SAC COSO Academy is supported by COSO.
Understanding the COSO Frameworks

The COSO Enterprise Risk Management-Integrated Framework and the COSO Internal Control-Integrated Framework (COSO Frameworks) are internationally recognised as the benchmark of good risk management and internal controls. They are widely used around the world by organizations to satisfy regulatory, governance and reporting requirements that are dictated by legislation, and rules and regulations that establish responsibility and accountability for reliable financial reporting.

The Singapore Quick Guide to the COSO Enterprise Risk Management and Internal Control Frameworks was put together for the purpose of building an understanding of the COSO Frameworks and its relevance to different stakeholders. The information presented is intended to be a guide and for reference, and is not exhaustive.

The quick guide draws on the expert views of the Protiviti-SAC COSO Academy’s founders – Singapore Accountancy Commission and Protiviti – and its strategic partners – The Institute of Internal Auditors Singapore, the Singapore Institute of Directors, the Singapore Management University’s School of Accountancy, and the Securities Investors Association (Singapore). Each strategic partner brings a group of stakeholders that is necessary to build a practical and sustainable enterprise risk management and internal control ecosystem for the Singapore business community.

We have provided information to introduce each of the stakeholder communities, namely the Boards, Senior Management, Practitioners and Retail Investors, to the benefits of the COSO Frameworks. We have also introduced to these stakeholders the questions they should ask to ensure organizations effectively manage their risks and design and execute control activities, and can successfully adapt to changes in business, operating, technological and regulatory environments.

For more information on the COSO Frameworks or the Protiviti-SAC COSO Academy, visit the respective websites www.coso.org and www.cosoacademy.com.
Contents

Message from COSO Chairman 6
What is COSO 7
Understanding the COSO Frameworks 8
The COSO Frameworks in Singapore 9
COSO Frameworks for Boards 10-11
COSO Frameworks for Management 12
COSO Frameworks for Internal Audit 13-15
COSO Frameworks for Retail Investors 16-17
Message from COSO Chairman

I am pleased to see the Singapore Accountancy Commission, Protiviti and its other supporting organizations continuing to take the lead in communicating the meaning and benefits of the COSO Frameworks through this guide. In essence, COSO’s materials are simply intended to help all organizations, regardless of size, industry or ownership improve their governance, risk management, operations, internal control and fraud deterrence.

And I am not surprised to see that professionals, management and board members in Singapore want to avail themselves of the COSO materials to improve and maintain sustainable, successful organizations for years to come.

I wish all readers and users of this material much success as they find ways to set appropriate objectives and meet them through effective risk management and internal control, including fraud deterrence.

Robert B. Hirth, Jr.
Chairman
Committee of Sponsoring Organizations of the Treadway Commission (COSO)
January 2016
What is COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five major professional associations: the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, The Institute of Internal Auditors and the Institute of Management Accountants. COSO is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

The COSO Cubes

COSO’s guidance on Enterprise Risk Management and Internal Control is presented in the form of two cubes to show the connection between organizational objectives (on the top), what is needed to achieve these objectives (on the front), as well as the organization’s operating units (on the side). The COSO cubes illustrate how each framework can be applied to the whole organization as well as to its parts.

The COSO Enterprise Risk Management (ERM) – Integrated Framework:

- Provides sound principles and guidance for ERM to help organizations deal with risk and achieve its objectives
- Provides a common language for ERM that is widely accepted by organizations and their stakeholders
- Clearly describes the key elements of a robust ERM process and how risks are managed within an organization’s risk appetite
- Demonstrates that ERM can add value to an organization by helping management achieve organizational performance and profitability targets and prevent loss of resources
- Enables management to better assess how much risk the organization accepts relative to stated objectives
- Provides clear and practical direction and guidance for the implementation of ERM

The COSO Internal Control (IC) – Integrated Framework provides:

- A means to apply internal control to any type of entity, regardless of industry, legal structure, at the levels of entity, operating unit, or function
- A principles-based approach that provides flexibility and allows for judgement in designing, implementing and evaluating internal control
- Requirements for an effective system of internal control by considering how components and principles are present and functioning, and how components operate together
- A means to identify and analyze risks, and to develop and manage appropriate responses to risks within acceptable levels and with a greater focus on anti-fraud measures
- An opportunity to expand the application of internal control beyond financial reporting to other forms
The COSO Frameworks comprise two sets of guidelines on the implementation and evaluation of the effectiveness of management and governance processes within organizations. The Enterprise Risk Management – Integrated Framework and the Internal Control – Integrated Framework incorporate the methodologies needed to ensure that controls and risk management processes are in place within organizations. It is applicable for use by businesses of all sizes, including government agencies and charities, and is widely adopted by publicly-traded companies in the United States, Japan and China.

Enterprise Risk Management is broader than Internal Control and focuses on risk. Internal Control is one of the important components of Enterprise Risk Management, whereas the latter forms part of the overall governance process. While the Enterprise Risk Management framework deals with strategic objectives and strategy-setting and alternative risk responses (risk avoidance, acceptance, sharing and reduction), the Internal Control framework deals primarily with risk reduction.

While either framework can be applied separately with positive results, the COSO Frameworks is the only fully integrated set of guidelines that facilitate and support the governance process when implemented effectively. It delivers the most structured and balanced approach to achieving business objectives and the protection of enterprise value.
COSO Frameworks in Singapore

Guidebook for Audit Committees in Singapore (Second Edition)

The latest edition of this guidebook recommends the COSO Frameworks – Section 3 on Risk Management and Internal Controls:

3.3.36 – Audit Committee members should ensure that the company has considered and established an internal control framework (as part of the ERM framework)

3.3.37 – The COSO Internal Control Framework is a leading framework that Audit Committees can consider

SGX Listing Rules 1207(10)

This SGX listing rule requires an issuer to disclose in its annual report, the opinion of the Board, with the concurrence of the audit committee, on the adequacy of the internal controls, addressing three areas: financial, operational and compliance risks.


The Singapore Code of Corporate Governance Principle 11 requires that the Board is responsible for the governance of risk. The Board should ensure that Management maintains a sound system of risk management and internal controls to safeguard shareholders’ interests and company assets, and should determine the nature and extent of the significant risks which the Board is willing to take in achieving its strategic objectives.

COSO Frameworks 2015 Singapore Survey

A survey was conducted by the Protiviti-SAC COSO Academy and The Institute of Internal Auditors Singapore of more than 80 internal audit professionals in organizations across industries. Its purpose was to ascertain levels of awareness and adoption of the COSO Frameworks among organizations in Singapore.

The survey showed that while 94% of respondents were aware of the COSO Frameworks, only 54% had implemented either one or both of the frameworks.

Limited manpower, lack of training and perceived low value of the COSO Frameworks, were among challenges cited for the less than ideal adoption rate.
COSO Frameworks for Boards

“The Board is responsible for the governance of risks and controls. It sets the tone and direction for the company in the way that risks are being managed and internal controls are implemented.”

Willie Cheng
Chairman, Singapore Institute of Directors

How COSO Frameworks Can Help Boards

A FULLY-INTEGRATED APPROACH
Implementing the Enterprise Risk Management Framework enables Boards to:

• Better understand the entity’s risk philosophy and concur with the entity’s risk appetite
• Ascertain the extent to which management has established effective enterprise risk management
• Review the entity's portfolio of risk and consider it against the entity’s risk appetite
• Be apprised of the most significant risks and determine whether management is responding appropriately

Implementing the Internal Controls Framework enables Boards to:

• Oversee more effectively the entity’s internal control systems
• Monitor risks to the achievement of the entity’s objectives
• Understand how internal control deficiencies are assessed and risks are mitigated

The Board Influences the “Tone at the Top” in Any Organization

The COSO Frameworks emphasizes the importance of the tone at the top and the Board’s responsibility in overseeing the development and performance of internal control. Directors exercise significant influence over the organization’s attitude toward risk, the aggressiveness of its policy choices and its commitment to responsible business behavior.

The Board Is Responsible for Oversight of the Control Environment

To illustrate the Board’s oversight of the control environment, the frameworks provide that Directors:

• Oversee the definition and standards of the organization’s conduct, establish expectations and evaluate CEO performance and integrity.
• Provide effective challenge to executive management by asking tough questions, regarding proposed plans, deals, and significant and unusual transactions.
• Seek input and support from independent risk management and compliance functions, internal auditors, external auditors and others.
The Board Needs to Pay Attention to the Risks of Management Override, Fraud and Illegal Acts

The Board is the last line of defense on matters involving Management overriding established controls for an illegitimate purpose, including personal gain or “cooking the books”.

The frameworks recommend that the Board (or a Board committee) oversees management’s assessment of the risk of override and challenges management as circumstances dictate.

Why the COSO Frameworks Are Important to Governance

The Board has a separate and distinct role from executive management in governing the organization. The Board approves strategic decisions, establishes boundaries, oversees execution and ensures accountability, fairness and transparency.

Executive management aligns strategy, processes, people, reporting and technology to accomplish the organization’s mission in accordance with its established values.

An important aspect of the delineation of responsibilities between the Board and Management is the setting of boundaries, as they reduce the risk of strategic drift leading to a lack of focus in managing the organization’s risk profile.

The internal environment of the COSO ERM Framework, the control environment of the COSO Internal Control Framework, and the information and communications component of both frameworks provide positive contributions to the governance process.

Why the COSO Frameworks Are Important to Adapting

Organizations must plan for disruption and build and refine their systems to measure and be alert for changes in key risk indicators (leading indicators) versus relying solely on key performance indicators (which are often lagging and retrospective in nature).

Looking forward will enable an organization’s culture to support an experimental and adaptable mindset.

With the emphasis on identifying and reacting to change, the event identification, risk assessment, information and communication, and monitoring components of the COSO ERM Framework contribute insights that can support an entity’s efforts to become adaptive. Likewise, the risk assessment, information and communication, and monitoring components of the COSO Internal Control Framework can support an entity’s efforts to become adaptive in disruptive times.
COSO Frameworks
For Management

“The COSO Frameworks is an international best practice and the only fully integrated risk management and internal controls framework. When applied effectively, the two frameworks contribute to improving organizational performance and corporate governance.”

Foo See Liang
Associate Professor, School of Accountancy, Singapore Management University

How COSO Frameworks Can Help Management

A FULLY-INTEGRATED APPROACH
Implementing the Enterprise Risk Management Framework enables Management to:
• Align risk appetite and strategy
• Enhance risk response decision-making
• Reduce operational surprises and losses
• Identify and manage multiple and cross-enterprise risks

Implementing the Internal Control Framework enables Management to:
• Better define and deploy effective internal controls
• Identify and analyze risks, and develop appropriate risk responses
• Evaluate the implementation of controls, and monitor and remediate internal controls deficiencies
• Establish anti-fraud programs to mitigate risk of fraudulent actions

Why the COSO Frameworks Are Important to Strategy Setting and Business Planning

Elements from the objective setting, event identification, risk assessment and risk response components of the COSO ERM Framework have a direct impact on strategy setting and business planning.

Given that Management cannot control external events, ERM focuses on strategic objectives while internal control provides an important risk response option in executing the strategy and business plan.

The control activities and information and communication components in either COSO Framework support the execution of the strategy and business plan to achieve organizational objectives.

Control activities can be categorized based on the nature of the organization’s objectives, e.g. operations, reporting and compliance, to enable a holistic view of the ability of the organization to mitigate unique risks.

Whether preventive or detective, automated or manual, or applied at the entity or organizational level, control activities contribute significant value to the organization if designed and operating effectively. They are vital to successful execution of the business model because they are intended to mitigate the risks of relevant objectives not being achieved.
COSO Frameworks
For Internal Audit

“COSO is an important framework that forms the basis for internal auditor’s assessment of the organization’s internal control and risk management processes. COSO emphasizes the need for Internal Audit to align its focus with organisational objectives and to assess the softer aspects of internal controls as it is effected by people, not just policy manuals and procedures.”

Tan Boon Yen
President, The Institute of Internal Auditors Singapore

The definition of Internal Auditing states the fundamental purpose, nature, and scope of internal auditing. Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The primary function of Internal Audit is to provide independent assurance to the Board that controls are adequate and operating effectively. To help organizations achieve their objectives, it is essential that Internal Audit professionals have a solid understanding of business strategies, thereby aligning the role of Internal Audit with that of the business. By proactively engaging stakeholders and taking the lead in addressing their needs, as well as identifying major issues, systemic risks and errors, Internal Audit is well placed to support Management in the achievement of strategic and business objectives. Internal Audit also plays the role of an advisor to the Board, Audit Committee and Management to fulfill their responsibilities respectively.

Why the COSO Frameworks Are Important to Internal Audit

Utilizing the COSO Frameworks enables Internal Audit to bring a systematic, and disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. It emphasizes the need for Internal Audit to align its focus with organizational objectives and to have a clear understanding of the relationship between organization’s objectives, risks and controls.

Internal Audit also needs to assess the softer aspects of internal controls as it is effected by people, not just policy manuals and procedures, which is provided by the Control Environment component of the COSO Internal Control Framework.

The Board and Management expect Internal Audit to evaluate fraud mitigation strategies. The COSO Internal Control Framework’s focus on fraud deterrence provides guidance for internal auditors.

Internal Audit professionals need to have a good understanding of the framework and its application in the Internal Audit role to provide independent assurance to the Board of Directors in reviewing the adequacy and effectiveness of the company’s risk management and internal control systems. This is especially relevant and important in supporting the Board in its oversight responsibility of the organization’s internal controls and risk management framework under the SGX Listing Rules 1207(10) and Principle 11 of the Singapore Code of Corporate Governance (Effective 1 November 2012).
Most frequently cited benefits from implementing COSO ERM Framework

- **87%** Better designed processes and controls
- **30%** Reduced chances of fraud
- **16%** Fewer audit findings

Most frequently cited benefits from implementing COSO IC Framework

- **93%** Better designed processes and controls
- **43%** Reduced chances of fraud
- **23%** Fewer audit findings

It is important to start with reviewing and understanding the organization's mission, vision, core values and its strategic objectives and operating plans. This is to ensure that the organization implements an effective ERM and internal control framework that is designed to improve organizational performance and governance and proactively manage strategic, business and operating risks.

Internal Audit needs to look beyond procedural compliance, transaction review and control activities. It is necessary for Internal Audit to clearly articulate the roles and responsibilities within the organization for effective management of risks and controls. The responsibilities of each group within the organization are (*):

1. **Own and manage** risk and control (front line operating management).
2. **Monitor** risk and control in support of management (risk, control, and compliance functions put in place by management).
3. **Provide independent assurance** to the Board and senior management concerning the effectiveness of management of risk and control (Internal Audit).

(*) Leveraging COSO Across The Three Lines Of Defense By The Institute of Internal Auditors, Committee of Sponsoring Organizations of the Treadway Commission. Available at [www.coso.org](http://www.coso.org)

In assessing the adequacy of internal controls, Internal Audit should assess all the 5 components and 17 principles of the COSO Internal Control Framework not only on an entity level basis, but also for business divisions, operating units and functions.
The following are some key aspects that Internal Audit professionals need to consider in assessing the 5 COSO components (the list below is not exhaustive):

1. **Control Environment**
   - Clearly articulated mission and vision statements
   - Strategic direction by the Board of Directors
   - Organization’s ethical climate to assess commitment to integrity and ethical values
   - Clearly defined responsibilities for strategic, operational, compliance and technology risks
   - Risk governance framework stating the risk appetite and risk tolerance limit
   - Clear structure and authority matrix
   - Program to continually maintain skilled and competent staff
   - Clear accountability and performance measures, rewards and incentives to ensure alignment with strategic and business objectives

2. **Risk Assessment**
   - Process to define the relevant strategic objectives that is aligned to its mission and vision and the risk appetite and risk tolerance limit as approved by the Board. The assessment should be based on the COSO ERM Framework
   - Process to identify, analyze and document and monitor risks on a continual basis
   - Fraud risk management framework to monitor and assess fraud risk
   - Process to identify and analyze significant changes that will increase the operational, financial and compliance risks, and the identification of risk mitigating measures to proactively manage new risks

3. **Control Activities**
   - Proactive approach to develop control activities that are aligned to the key risks identified
   - Effective control framework and well defined policies and procedures to govern the critical control activities

4. **Information and Communication**
   - Reporting framework to ensure critical information is communicated in a timely manner to relevant personnel
   - Reporting and monitoring key performance indicators
   - Process for timely, accurate and unbiased reporting of financial performance

5. **Monitoring**
   - Develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning
   - Process to communicate the deficiencies and a well defined work plan to deal with these deficiencies
COSO Frameworks
For Retail Investors

“Singapore investors should be aware of international standards in enterprise risk management and internal controls and how listed companies can apply the COSO Frameworks to boost internal governance structures. With this guide, I hope retail investors will gain the knowledge to ask the important questions at their meetings with Management and Board.”

David Gerald
President and CEO, Securities Investors Association (Singapore)

The Retail Investor’s Checklist

Questions to ask

• Does the organization have a policy for internal control to be an integral part of decision-making in the organization?

• Does the organization have proper guidance on risk taking in relation to the type and amount of risk that the organization is willing to accept?

• Has the organization committed sufficient and appropriate resources (e.g. financial and non-financial) in relation to internal controls and aligned with the expectations of the organization’s key stakeholders (e.g. shareholders, regulators and customers)?

• Does the organization properly assign ownership and accountability? Are roles and responsibilities on internal controls, including information flows, in the organization clearly stipulated?

• Does Management examine the effectiveness of internal controls?

• Is there transparent and timely reporting of risk profile and internal control effectiveness to key stakeholders?

• How competent are the employees who are responsible for internal control processes?

• Is internal control performance considered in each employees’ overall annual appraisal?

• Do existing internal controls address the causes and/or consequences of risks?

• Is there a competent party which is independent of Management (i.e. internal auditor) to ensure the design and operating effectiveness of internal controls?

• Do the Board and Management foster an organizational culture that motivates members of the organization to act in line with risk management strategy and policies on internal control set by the board to achieve the organization’s objectives?

• Does the organization base its risk management and internal control activities on any formal and internationally-recognized/ accepted framework?
What to look for

• There is a documented and well communicated policy on the internal control as an integral part of risk management and overall governance system.

• There is a relevant, well communicated and properly documented risk appetite statement stipulating the boundaries to risk taking.

• There is a periodic review to ensure that an adequate annual budget to support the organization’s internal controls infrastructure to improving internal controls at all levels of the organization are aligned with the organization’s risk profile and stakeholder expectations.

• There is a clearly written and well communicated policy on the assignment of internal control ownership to staff with the appropriate authority, and proper terms of reference are established for those involved in internal controls in the organization.

• There is a schedule for regular monitoring and evaluation by Management of the internal controls. There is a policy for the timely reporting of internal controls gaps and weaknesses to the appropriate level(s) and for ensuring that proper measures are taken.

• There is a policy on transparent and timely reporting of the organization’s risk profile by management and those charged with governance to key stakeholders. Compliance of the policy and the reporting process is subject to independent review by internal audit.

• The organization’s hiring policy includes the hiring of employees with the relevant internal control competencies, and their skill-sets are kept updated through regular internal control training and education.

• There is a well communicated policy which integrates each employee’s internal controls performance in his or her annual evaluation.

• Internal controls exist to effectively respond to risks. The measures should include a formal strategy, policy and processes for internal controls, as well as be designed, implemented and applied in a cost-effective manner to address the causes and/or consequences of the risks, and aligned with the organization’s risk appetite.

• There are regular independent reviews by internal audit. Internal controls gaps and weaknesses are reported to the appropriate level(s) and proper remedial measures are taken.

• There is a code of ethics to foster internal control awareness and compliance across the organization. There is regular communication to ensure that internal control principles are understood and applied correctly. Also, Management leads by example.

• The organization’s internal control framework is designed in accordance with the principles of well-established internal control models, such as the COSO Frameworks.
Sources

Used by permission:


6. 12 Questions on Internal Control for Investors, Foo See Liang, Associate Professor of Accounting (Practice), School of Accountancy, Singapore Management University.

7. Lessons Learned From the SOX Experience, SAC-Protiviti SOX Roundtable Report 2014. Available at www.cosoacademy.com

8. 2015 Singapore Survey on COSO Frameworks Results. Available at www.cosoacademy.com
