

The Road to Transition:

COSO's Internal Control 2013 –
Integrated Framework

kpmg.com



To review the
company's
internal control

Audit Committee's Roles

To monitor and
review the
effectiveness of the
company's
internal
audit function



Framework?

Reviewing the effectiveness of internal control and risk managing system is an essential part of board's responsibility. However, aspects of the review work are normally delegated to the audit committee.

COSO Frameworks

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of the five private sector organizations listed below and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.



COSO:

COSO Internal Control Integrated Framework
(1992)

New COSO Framework

Launching of the original
COSO's Internal Control–
Integrated Framework

1992



The updated COSO's Internal Control –
Integrated Framework will be in effect
(Dec 15th). The original framework will
then be superseded.

2014

TRANSITION PERIOD*

2013



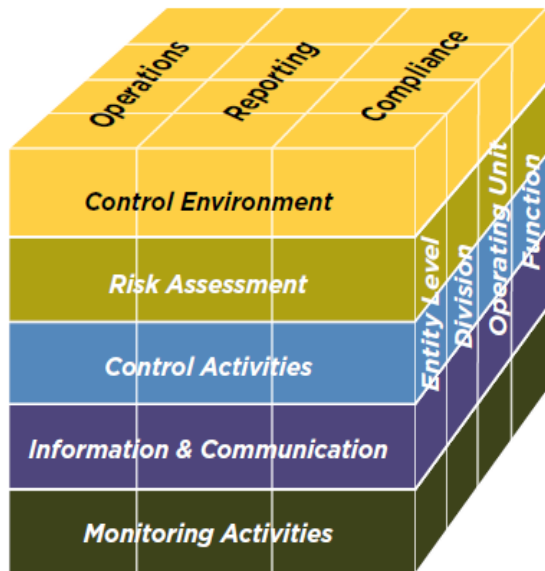
Launching of the updated
COSO's Internal Control–
Integrated Framework (May 14th).

*** Note:** During transition period, users are encouraged to use the updated Framework but is not required. In addition, external reporting should disclose whether the original or updated version of the Framework was used.

High-level Review of Internal Control

Old Assessment Form

New Assessment Form



(Translation)

Assessment Form of Sufficiency of Internal Control System

Dated _____

Part 1. Organizational Control and Environment Measures

Organizational Control and Environment Measures having a good structure of organizational control and environment measures which is the key base of the efficient

Part 2. Risk Management Measures

Risk management measures of the Company is clearly presented among the business

Part 3. Information and Communication Measures

Information and Communication Measures of the Company is clearly presented among the business

Part 4. Monitoring and Review Measures

Monitoring and Review Measures of the Company is clearly presented among the business

แบบประเมินความเพียงพอของระบบการควบคุมภายใน

วัตถุประสงค์ของการประเมิน

การประเมินความเพียงพอของระบบการควบคุมภายในมีความสำคัญอย่างยิ่งต่อการดำเนินงานของบริษัทและองค์กรที่มีประสิทธิภาพในการดำเนินงานของบริษัทที่ประสบความสำเร็จนั้นขึ้นอยู่กับประสิทธิภาพของระบบการควบคุมภายในของบริษัท ซึ่งการประเมินความเพียงพอของระบบการควบคุมภายในของบริษัทเป็นเครื่องมือที่สำคัญในการวัดประสิทธิภาพของระบบการควบคุมภายในของบริษัท และเพื่อที่จะสามารถระบุจุดอ่อนของระบบการควบคุมภายในของบริษัทได้อย่างทันท่วงที และสามารถนำจุดอ่อนเหล่านั้นมาปรับปรุงแก้ไขได้

การประเมินความเพียงพอของระบบการควบคุมภายใน (Assessment of Internal Control)

1. ข้อมูลพื้นฐานเกี่ยวกับบริษัท (Basic Information)

2. ข้อมูลเกี่ยวกับระบบการควบคุมภายใน (Internal Control System)

3. ข้อมูลเกี่ยวกับความเสี่ยง (Risk)

4. ข้อมูลเกี่ยวกับข้อมูลและการสื่อสาร (Information and Communication)

5. ข้อมูลเกี่ยวกับการตรวจสอบและทบทวน (Monitoring and Review)

6. ข้อมูลเกี่ยวกับความเพียงพอของระบบการควบคุมภายใน (Sufficiency of Internal Control)

COSO 2013 framework – Summary of changes

What is **NOT** changing...

- Core definition of internal control
- **3 categories** of objectives and **5 components** of internal control
- Each of the 5 components of internal control are required for effective internal control
- Important role of judgment in designing, implementing, and conducting internal control, and in assessing its effectiveness



What is changing...

- Updated for changes in business and operating environments
- Expanded operations and reporting objectives
- Implicit fundamental concepts underlying **5 components** codified as **17 principles**
- Updated for increased relevance and dependence on IT
- Addresses fraud risk assessment and response

Benefits of COSO 2013 Framework :



- ✓ Opportunity for re-evaluate existing control structure
- ✓ Improve the efficiency or effectiveness of internal controls
- ✓ Ensure to keep pace with the evolving business environment and emerging risks
- ✓ Enhancing governance
- ✓ Improving risk assessment and antifraud practices
- ✓ Enhancing adaptability to change and varied business/operating models

COSO components and principles

For effective internal control:

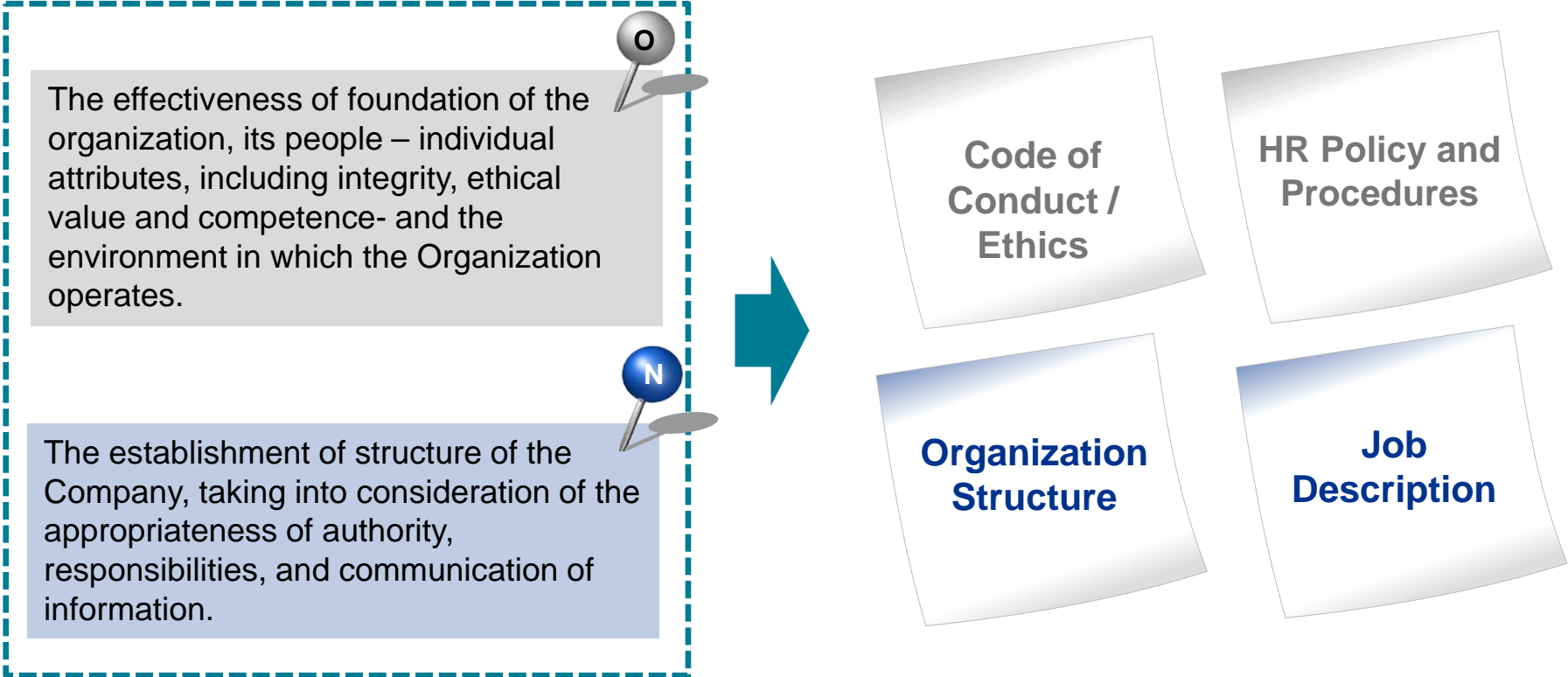
- Each of the five components and 17 principles must be present and functioning
- The five components must operate together in an integrated manner

Control Environment	<ol style="list-style-type: none">1. Demonstrates commitment to integrity and ethical values2. Exercises oversight responsibility3. Establishes structure, authority, and responsibility4. Demonstrates commitment to competence5. Enforces accountability
Risk Assessment	<ol style="list-style-type: none">6. Specifies suitable objectives7. Identifies and analyzes risk8. Assesses fraud risk9. Identifies and analyzes significant change
Control Activities	<ol style="list-style-type: none">10. Selects and develops control activities11. Selects and develops general controls over technology12. Deploys through policies and procedures
Information and Communication	<ol style="list-style-type: none">13. Uses relevant information14. Communicates internally15. Communicates externally
Monitoring Activities	<ol style="list-style-type: none">16. Conducts ongoing and/or separate evaluations17. Evaluates and communicates deficiencies

COSO components – Control Environment

Control Environment

The Management demonstrates commitment to integrity and ethical values as well as competence, exercise oversight responsibility, **establishes structure, authority, and responsibility**, and enforces accountability



The effectiveness of foundation of the organization, its people – individual attributes, including integrity, ethical value and competence- and the environment in which the Organization operates.

The establishment of structure of the Company, taking into consideration of the appropriateness of authority, responsibilities, and communication of information.

Code of Conduct / Ethics

HR Policy and Procedures

Organization Structure

Job Description

COSO components – Risk Assessment

Risk Assessment

The Organization sets objectives of the business and the mechanism to identify, analyze, and manage the related risks, including **fraud risks**.

The effectiveness of the current risk management activities.

The identification of fraud risks in current risk assessment activities

Risk Assessment Process

Risk Management Framework

Risk Tolerance

Specific assessment of fraud risk

COSO components – Control Activities

Control Activities

The Organization establishes and executes controls, **including controls over technology** to ensure that actions identified by management address risks for the achievement of the Company's objectives. Controls activities can be deployed through policies and procedures.

The effectiveness of the control activities of the Organization

The appropriateness of the selection and development of general controls over technology

Policies and Procedures

Segregation of Duties

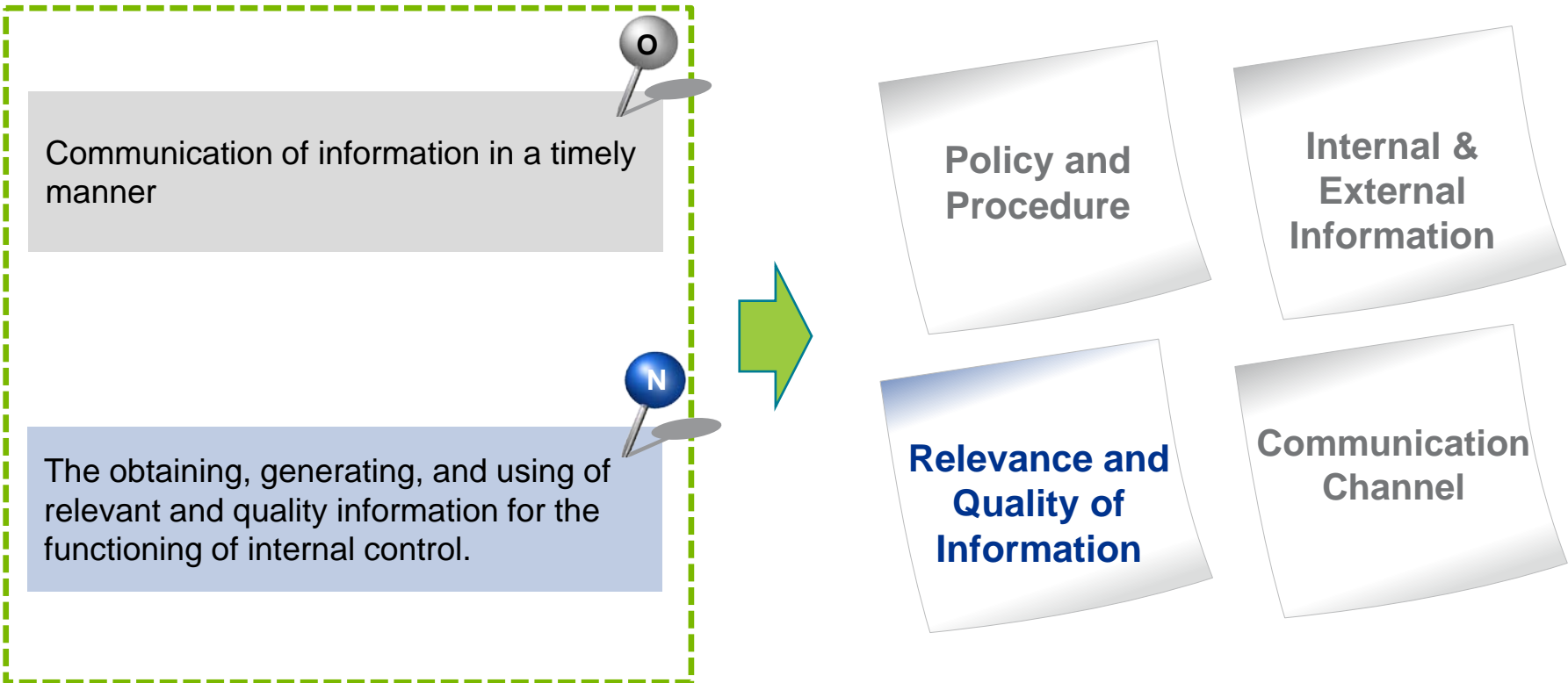
IT Structures

IT General Controls

COSO components – Information and Communication

Information and Communication

The Organization **uses relevant information** that have been communicated both internally and externally to support the functioning of internal control.



Communication of information in a timely manner

The obtaining, generating, and using of relevant and quality information for the functioning of internal control.

Policy and Procedure

Internal & External Information

Relevance and Quality of Information

Communication Channel

COSO components – Monitoring Activities

- 16. Conducts ongoing and/or separate evaluations
- 17. Evaluates and communicates deficiencies

Monitoring Activities

The entire process and controls must be monitored and modifications made as necessary through ongoing and/or separate evaluations as well as the evaluation and communication of deficiencies

The effectiveness of the monitoring of all activities

The selection, development, and performance of ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning

Report and Monitoring

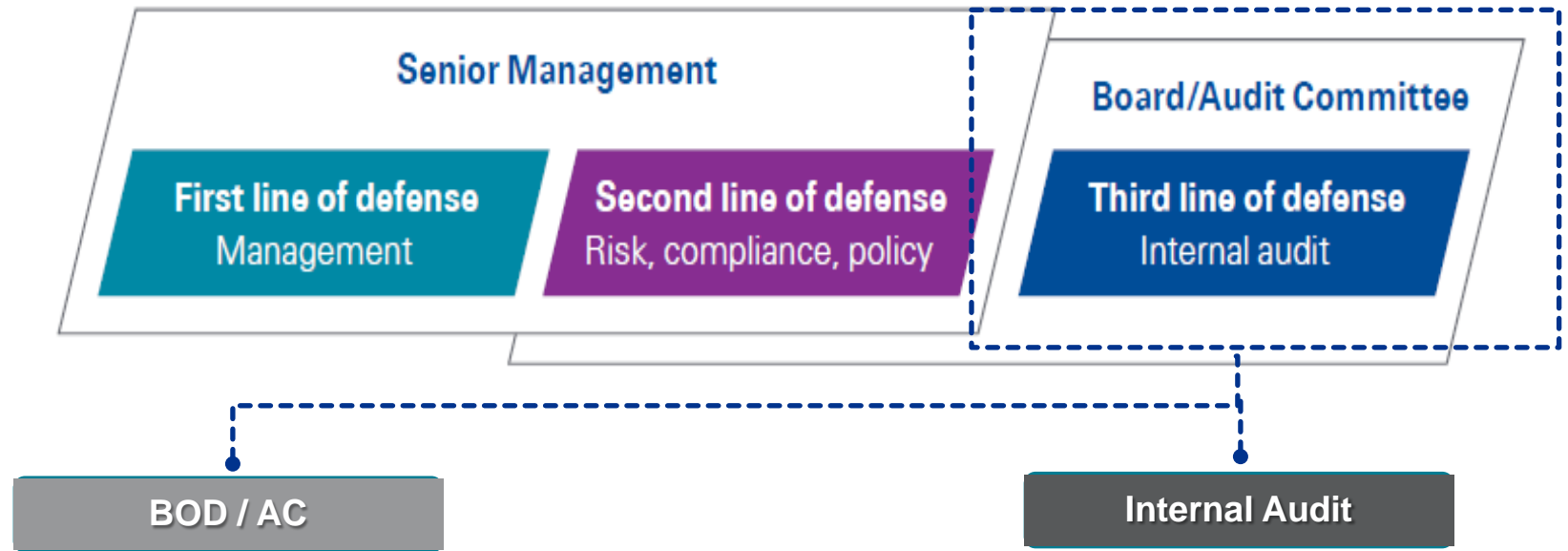
Control Self-Assessment

Internal Audit

Ongoing Evaluation

Preparing for the transition...

“3 lines of defense” — should fully comprehend the implications of the updated framework.



- **Understand how management is addressing the 2013 Framework** and the timing and implications of migrating from the 1992 Framework to the 2013 Framework
- **Engage in discussions with external audit firm** to review the organization's 2013 Framework transition plan and understand implications on the execution of the Audit
- Discuss with AC the impact of the 2013 Framework and **Internal Audit's operations and plans**
- Proactively work with first and second lines of defense to **create and manage the transition** process to the 2013 framework

Key questions to the Management

Have we identified the potential impacts of the 2013 Framework?

Has Management's plan fully addressed all aspects to the changes to the 2013 Framework?

Does Management's transition plan appropriately account for the people, process and technology resources that will be needed for the transition?

Has the documents system of internal control kept pace with significant changes in business organization, operations, technology and governance needs?

Can we use the 2013 framework to better integrate compliance needs to lower costs and create more transparent compliance process?



Appendices

1. Control Environment



Control Environment

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability



The control environment determines the background of the organization; influencing awareness of its people toward control; lays the foundation for all other components and influences risk assessment and response, business and control activities, information and communication, monitoring and response to IT. Stressing Internal Control may lead to positive working principle.

Hard Controls

- All staff shall comply with corporate policies and procedures.
- Business line unit managers and upper rank shall facilitate, perform and assess internal control including perform Control Self Assessment (CSA).
- According to the Company's policy, each unit shall implement procedures which are in accordance with the international accepted standards.
- Explicit approval consideration procedures for significant matters to the Company.
- Internal Audit Office shall audit administrations for various aspects of the Company.

Soft Controls

- Encourage honesty, transparency, virtue and ethics to prevent frauds or not following specified duties, rules and regulations.
- Specify policies and procedures for corporate governance, and business Code of Conduct to ensure that employees in every area strictly follow the stated policies and procedures.
- Specify the corporate value, SPIRIT, which is to implant integrity and ethics and having faithfulness and ethics become one of the Company's values.

Control Environment – 2013 Framework Changes

- Captures **7 factors** in 1992 Framework into **5 principles**
- Expands and clarifies guidance on:
 - **Governance roles in an organization**
 - Expectations of integrity and ethical values
 - **Risk oversight** and strengthening the linkages between risk and performance to help allocate resources to support internal control
 - The need to consider internal control across the expanded organization

2. Risk Assessment



Risk Assessment

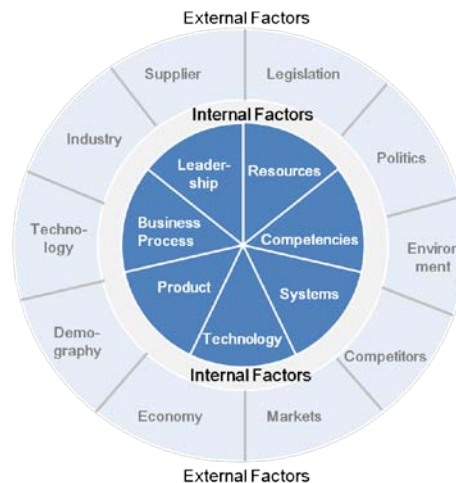
6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change



Risk Assessment is a process to identify and categorize potential risks, in order of its impact magnitude and the likelihood of occurrence. As the organization is confronted by unavoidable risks, both internally and externally, which impacts corporate achievement.

Risk Assessment – 2013 Framework Changes

- Clarifies that risk assessment includes **processes for risk identification, risk analysis, and risk response**
- Expands the discussion on:
 - **Risk tolerances** (acceptable risk levels)
 - The risk severity beyond impact and likelihood to include such velocity and persistence
 - The need to understand significant changes in internal and external factors and the impact on the system of internal control
- Includes **specific assessment of fraud risk**



3. Control activities



Control Activities

- 10. Selects and develops control activities
- 11. Selects and develops general controls over technology
- 12. Deploys through policies and procedures



Control activities are the policies and procedures established to ensure that the orders and instructions of management are followed in an appropriate manner.

Manual vs. IT

Manual Controls such as the signature approval of document and auditing of the transaction by the authority

IT-Dependent Manual Controls such as checking the odd transaction or process by calling data from the exception report

IT Application Controls such as the system the prevent the duplicate of the transactions

Preventive vs. Detective

Preventive such as revise the transaction before go on to the next process



Detective such as checking the transaction of the previous process that it has been done correctly



Control Activities – 2013 Framework Changes

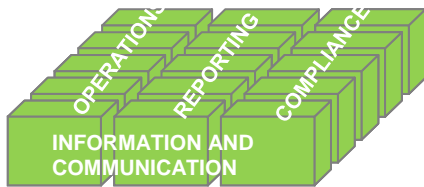
- **Updates the evolution in technology since 1992**
- **Addresses the linkage among business processes**, automated control activities, and GITCs
- Contrasts transaction-level controls from controls at other levels of the organization
- **Updates GITC applicability** across all technology platforms
- Clarifies that control activities are actions established by policies and procedures rather than being the policies and procedures themselves

4. Information and communication



Information & Communication

- 13. Uses relevant information
- 14. Communicates internally
- 15. Communicates externally



Information:

Everyone in the organization identify the information required in order to carry out their individual responsibilities in a timely and appropriate manner.

Communication:

Necessary information be conveyed to the appropriate personnel within organization in a timely manner. Also, Information must also be disseminated externally in a timely and appropriate manner, not just internally.



Characteristics of good information

Relevance/appropriateness

- relevant to the purpose for which it is required

Completeness

- contain all the details required by the user

Current

- provide the facts as close to the decision time as possible

Timely

- Information must be on time for the purpose for which it is required

Availability/accessibility

- easy to obtain or access and able to prevent non-relevant person to access

Good communication is

2 – way communication

which is to send and receive information to each other interactively. A good communication system must include both **internal** and **external** communication systems. In order to maximize value, the organization's communication systems should be evaluated regularly.



Information & Communication – 2013 Framework Changes

- Emphasizes importance of **quality of information**:
- Expands the discussion on:
 - The impact of **regulatory requirements** on reliability and protection of information
 - The volume and sources of information in light of increased complexity of business processes, greater interaction with external parties, and technology advances
- Reflects **the impact of technology** and other communication mechanisms on the speed, means, and quality of the flow of information



5. Monitoring Activities



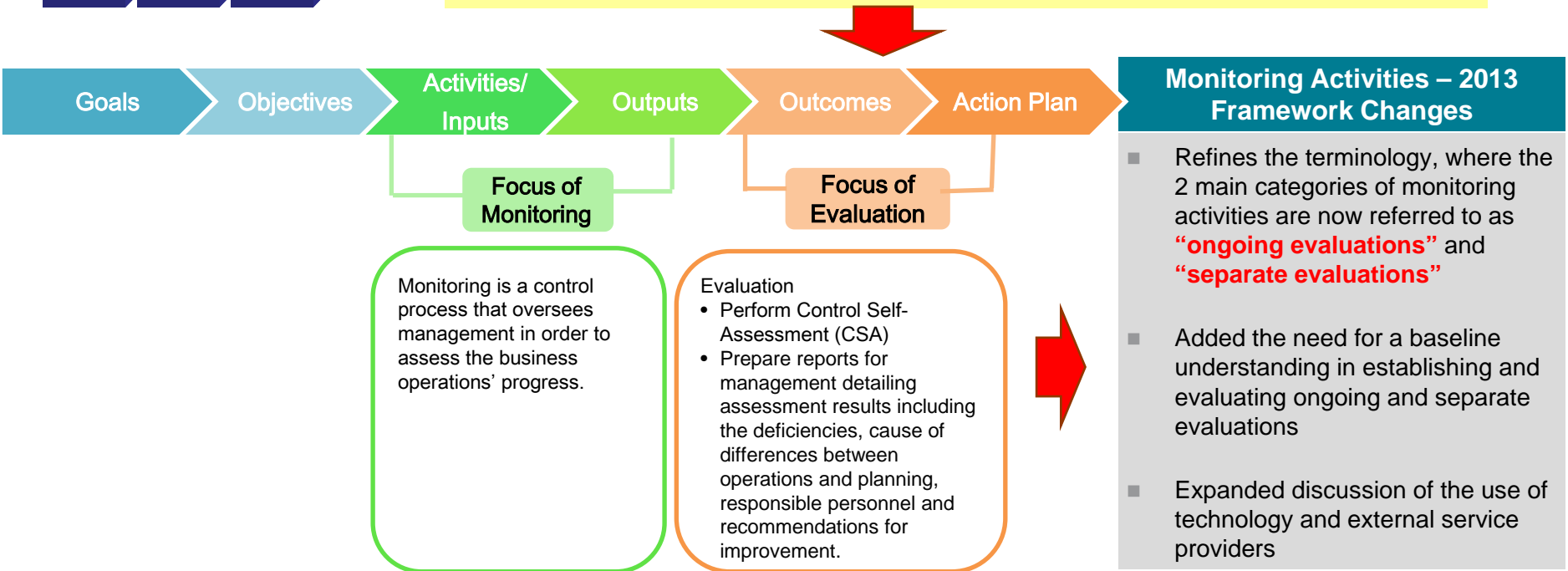
Monitoring Activities

16. Conducts ongoing and/or separate evaluations

17. Evaluates and communicates deficiencies



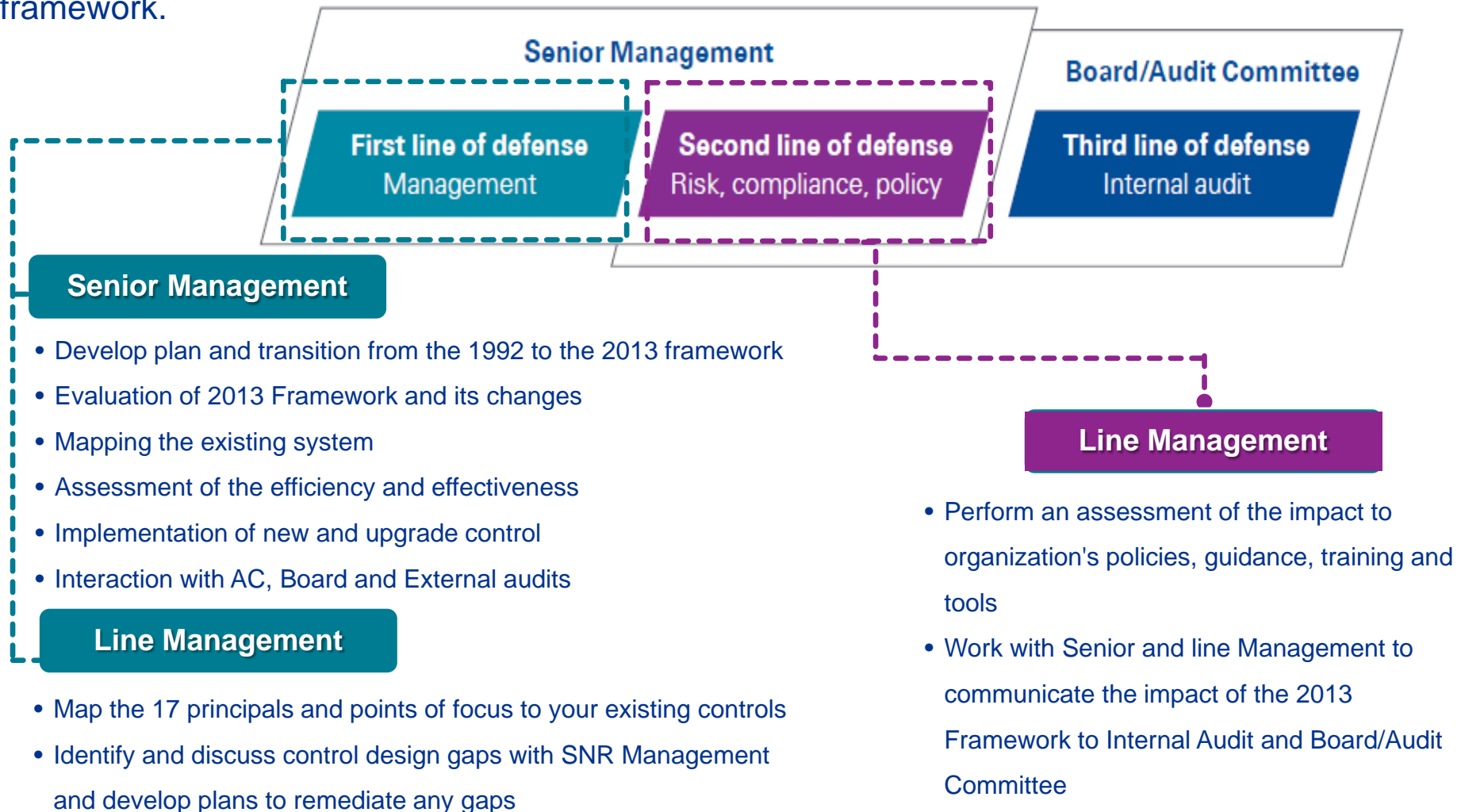
In due time, circumstances affecting both internal and external factors in internal control may arise and deteriorate its effectiveness. Monitoring is the process used to assess the quality of internal control performance over time. Monitoring provides a means of continually observing, assessing and correcting internal controls.



Preparing for the transition...

First line and Second line of defense

“3 lines of defense” — should fully comprehend the implications of the updated framework.





cutting through complexity

KPMG Phoomchai Audit Ltd.

Empire Tower, 50th – 51st Floor
195 South Sathorn Road
Bangkok 10120, Thailand

Tel : 02-677 2000

Fax : 02-677 2222



Winid Silamongkol

Partner

Office: 02-677 2144

winid@kpmg.co.th

Term Techasarin

Partner

Office: 02-677 24703

term@kpmg.co.th

Natthaphong Tantichattanont

Associate Principal

Office: 02-677 2354

natthaphong@kpmg.co.th

This presentation was produced for the AC Forum at KPMG.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation