



Deloitte.



เอกสารประกอบการสัมมนาทางวิชาการ (ไม่เสียค่าใช้จ่าย)

โครงการสัมมนา เสริมความคิด ตัดปีกวิชาชีพ กับคณะพาณิชยศาสตร์

โดยการสนับสนุนเงินทุนจาก มูลนิธิบุญชู โรจนเสถียร

บริษัท ดีลอยท์ ทูช ไร้มัทส์ ไชยยศ สอบบัญชี จำกัด

บริษัทสำนักงาน อี วาย จำกัด

บริษัท ไฟร์ชวอเตอร์เฮาส์คูเปอร์ส เอพีเอเอส จำกัด และคณะ

เรื่อง กรอบการบริหารความเสี่ยง 2017

(Enterprise Risk Management Integrating with Strategy
and Performance: 2017)

วันพฤหัสบดีที่ 30 พฤศจิกายน 256

เวลา 09.00 – 12.15 น.

ณ ห้อง F-310 อาคารเอนกประสงค์ 2 ชั้น 3

มหาวิทยาลัยธรรมศาสตร์ ท่าพระจันทร์

วิทยากร :

คุณศิวัชร รักษ์ พิณจารมณ

ประธานกรรมการตรวจสอบ

บริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย

Risk Base Internal Controls & Audit:

What's New under COSO-ERM 2017 Framework?

Sivaraks Phinicharomna

California CPA, Internal Revenue Services EA, CIA & CFE

1

Internal Control - Integrated Framework



มิติที่1: วัตถุประสงค์ขององค์กร

ปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผล

มีรายงานที่ถูกต้องครบถ้วน

ปฏิบัติตามกฎหมาย กฎเกณฑ์และระเบียบต่างๆ

มิติที่2: องค์ประกอบของการควบคุมเพื่อบรรลุวัตถุประสงค์

สภาพแวดล้อมในการควบคุม

ประเมินความเสี่ยงที่จะทำให้การควบคุมไม่บรรลุวัตถุประสงค์

สร้างหรือปรับปรุงกิจกรรมการควบคุม

สร้างหรือพัฒนาระบบข้อมูลและการสื่อสาร

ทบทวนและสอบทานองค์ประกอบเพื่อการแก้ไขปรับปรุง

มิติที่3: บุคลากรผู้รับผิดชอบ

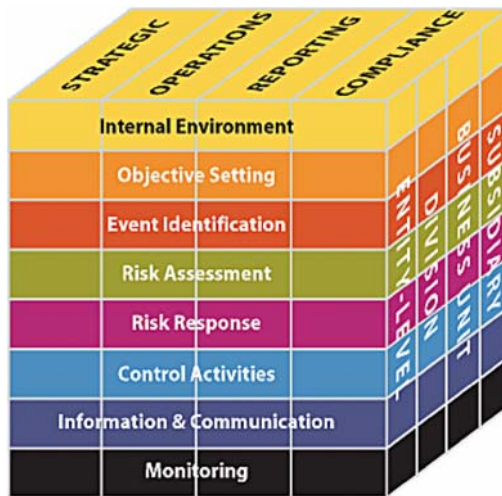
หน่วยงาน

ฝ่าย

ส่วนงาน

บริษัท

Enterprise Risk Management - Integrated Framework



มิติที่ 1: วัตถุประสงค์ขององค์กร

สร้างกลยุทธ์ที่เหมาะสม

ปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผล

มีรายงานที่ถูกต้องครบถ้วน

ปฏิบัติตามกฎหมาย กฎเกณฑ์และระเบียบต่างๆ

มิติที่ 2: องค์ประกอบของการบริหารความเสี่ยงเพื่อบรรลุวัตถุประสงค์

สภาพแวดล้อมภายใน

จัดตั้งวัตถุประสงค์ให้ชัดเจน

ระบุเหตุการณ์ที่อาจเกี่ยวข้องกับจุดประสงค์

ประเมินความเสี่ยงของเหตุการณ์

พิจารณาตอบสนองความเสี่ยง

สร้างหรือปรับปรุงกิจกรรมการควบคุม

สร้างหรือพัฒนาระบบข้อมูลและการสื่อสาร

ทบทวนและสอบทานเพื่อแก้ไขปรับปรุง

มิติที่ 3: ผู้รับผิดชอบ

บริษัทย่อย

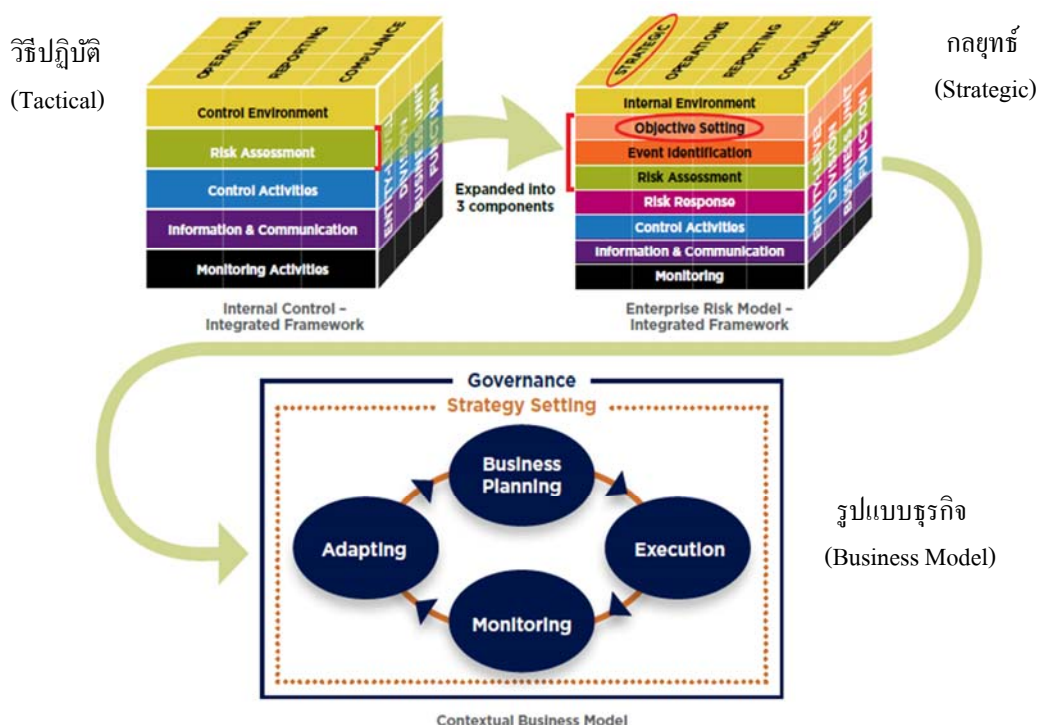
ส่วนงาน

สาขางาน

บริษัทใหญ่

3

How Frameworks can Improve Org. Governance & Performance



4

New COSO-ERM 2017

Enterprise Risk Management Integrating with Strategy and Performance



5

Clearing up a Few Misconceptions

- ❖ ERM is not a function or department
It is the culture, capabilities & practice to manage risks in creating, preserving, and realizing value.
- ❖ ERM is more than a risk listing
It includes practices that management put in place to actively manage risk
- ❖ ERM address more than internal control
It also address other topics such as strategy-setting, governance, stakeholder communicating and measuring performance
- ❖ ERM is not a checklist
It is a set of principles on which process can be built or integrated for a particular organization.
- ❖ ERM can be used by organizations of any size
It can and should be used by all kinds of organizations from small business, social enterprises, government agencies and fortune 500 companies.

6

Look into the COSO-ERM 2017

- ❖ World Economic increasing volatility, complexity & ambiguity
- ❖ Stakeholder seeking transparency & accountability
- ❖ The need to understand impact of risk on performance
- ❖ New COSO-ERM is comprehensive & sophisticate tool
- ❖ It provides insight of ERM when setting and carrying out strategy
- ❖ It deals extensively with management process
- ❖ It confuses when reading even with examples
- ❖ It is not too practical method for ERM implementation
- ❖ It is not too clear for integration between COSO-IC & COSO-ERM
- ❖ It has good example of inherent risk, target and residual Risk
- ❖ It accommodates evolving of technology and data analytics
- ❖ It demonstrates in term of systematic and disciplinary
- ❖ It could be a criteria for maturity measurement by regulators as COSO-IC 2013

7

The Role of Risk in Strategy Selection



8

A Focus Framework



9



Governance & 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
- ❖ กรรมการบริษัทกำกับดูแลความเสี่ยง
 - ❖ จัดโครงสร้างสายการบังคับบัญชา
 - ❖ พิจารณาวัฒนธรรมที่ต้องการ
 - ❖ แสดงความมุ่งมั่นในค่านิยม
 - ❖ จูงใจ พัฒนาและรักษาไว้ซึ่งบุคลากรที่มีความสามารถ

10

(Sample POF) Principle 1: Exercises Board Risk Oversight

The board of directors provides oversight of the strategy and carries out risk governance responsibilities to support management in achieving strategy and business objectives.

คณะกรรมการบริษัทกำกับดูแลกลยุทธ์ และรับผิดชอบในการดูแลความเสี่ยงเพื่อสนับสนุนฝ่ายบริหารให้บรรลุความสำเร็จในเรื่องกลยุทธ์และวัตถุประสงค์ทางธุรกิจโดยมี**จุดเน้น**คือ

- ❖ Accountability & Responsibility
- ❖ Skills, Experience, and Business Knowledge
- ❖ Independence
- ❖ Suitability of Enterprise Risk Management
- ❖ Organizational Bias

11



Strategy and Objective Setting

6. Analyzes Business Context

- ❖ วิเคราะห์โครงสร้างของธุรกิจ

7. Defines Risk Appetite

- ❖ กำหนดความต้องการที่จะเสี่ยง

8. Evaluates Alternative Strategies

- ❖ ประเมินกลยุทธ์ในรูปแบบต่างๆ

- ❖ กำหนดวัตถุประสงค์ทางธุรกิจ

9. Formulates Business Objectives

12

(Sample POF) Principle 6: Analyzes Business Context

The organization considers potential effects of business context on risk profile.

องค์กรพิจารณาจะเป็นความเสี่ยงถึงผลที่จะเกิดขึ้นต่อธุรกิจโดยมี**จุดเน้น**คือ

- ❖ Understanding Business Context
- ❖ Considering External Environment and Stakeholders
- ❖ Considering Internal Environment and Stakeholders
- ❖ How Business Context Affects Risk Profile

13



Performance

- 10. Identifies Risk
- 11. Assesses Severity of Risk
 - ❖ ระบุความเสี่ยง
 - ❖ ประเมินความรุนแรงของความเสี่ยง
- 12. Prioritizes Risks
 - ❖ จัดลำดับความเสี่ยง
- 13. Implements Risk Responses
 - ❖ ดำเนินการตอบสนองความเสี่ยง
 - ❖ พัฒนาภาพรวมความเสี่ยงขององค์กร
- 14. Develops Portfolio View

14

(Sample POF) Principle 10: Identifies Risk

The organization identifies risk in execution that impacts the achievement of business objectives.

องค์กรระบุความเสี่ยงที่เกิดขึ้นว่ากระทบ ความสำเร็จของวัตถุประสงค์ทางธุรกิจโดย มี
จุดเน้นคือ

- ❖ Identifying Risk
- ❖ The Scope of Identification
- ❖ Identifying Potential Opportunities
- ❖ Risk Universe

15



Review & Revision

15. Assesses Substantial
Change

16. Reviews Risk and
Performance

17. Pursues Improvement
in Enterprise Risk
Management

- ❖ ประเมินการเปลี่ยนแปลงที่มีสาระสำคัญ
- ❖ สอบทานความเสี่ยงและผลการจัดการ
- ❖ หาทางปรับปรุงการบริหารความเสี่ยงของ
องค์กร

16

(Sample POF) Principle 15: Assesses Substantial Change

The organization identifies and assesses internal and external changes that may substantially impact strategy and business objectives.

องค์กรระบุและประเมินการเปลี่ยนแปลงทั้งภายในและภายนอกที่อาจมีผลกระทบต่อกลยุทธ์และวัตถุประสงค์ทางธุรกิจอย่างเป็นสาระสำคัญ โดยมี**จุดเน้น**คือ

- ❖ Integrating Reviewing & Revision into Business Processes
 - Internal Environment
 - External Environment
 - Culture

17



Information, Communication & Reporting

18. Leverages Information and Technology

19. Communicates Risk Information

20. Reports on Risk, Culture, and Performance

- ❖ ผลักดันในเรื่องข้อมูลและเทคโนโลยี
- ❖ สื่อสารข้อมูลความเสี่ยง
- ❖ รายงานความเสี่ยง วัฒนธรรมและผลประกอบการ

18

(Sample POF) Principle 18: Leverages Information & Technology

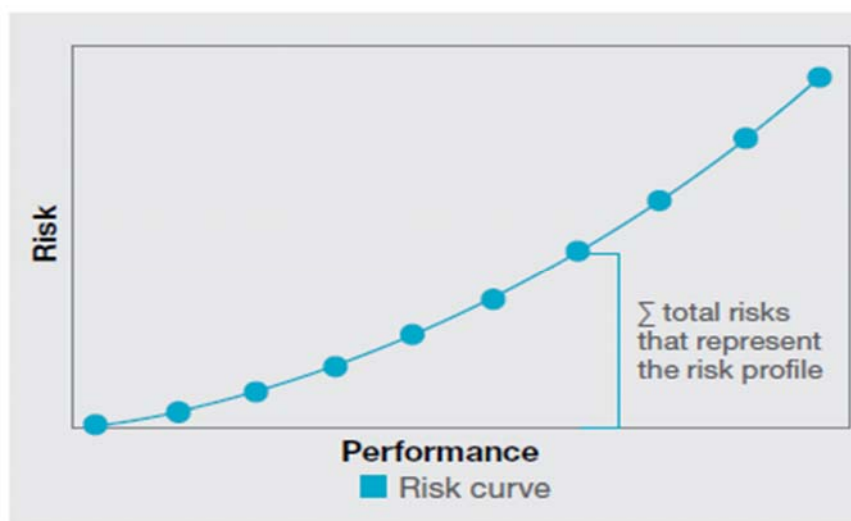
The organization leverages the entity's information systems and technology to support enterprise risk management.

องค์กรผลักดันให้มีระบบข้อมูลและเทคโนโลยีที่สนับสนุนการบริหารความเสี่ยงทั้งองค์กรโดยมี**จุดเน้น**คือ

- ❖ Using Information Systems
- ❖ Using Enterprise Risk Management Taxonomies
- ❖ Sustaining Enterprise Risk Management
- ❖ Changing Information System Requirements

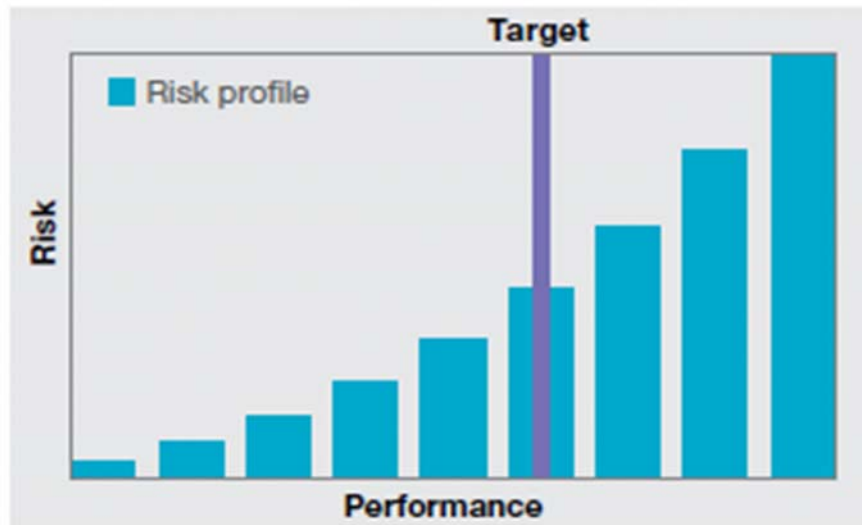
19

Develop Risk Profile



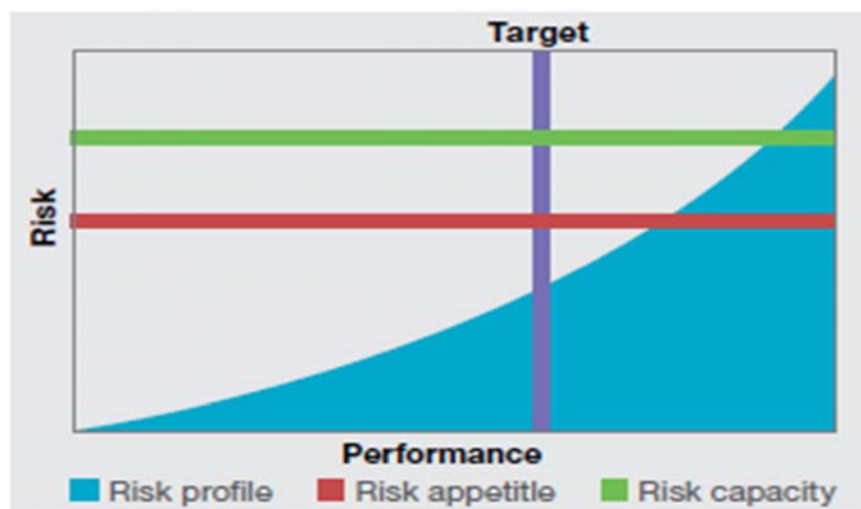
20

Risk Profile & Target



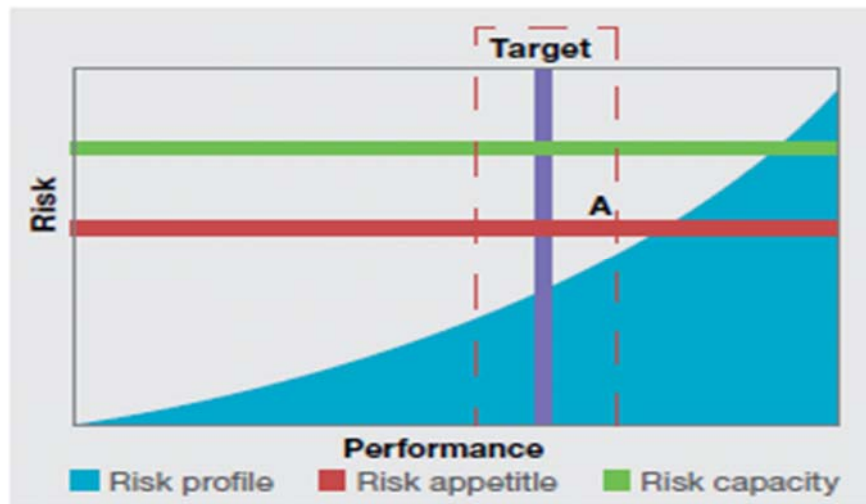
21

Risk Appetite & Risk Capacity



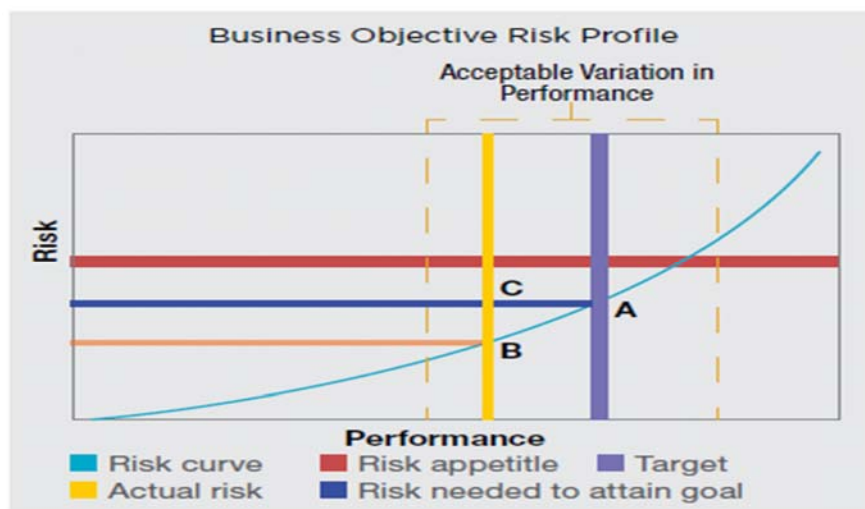
22

Acceptable Variation in Performance



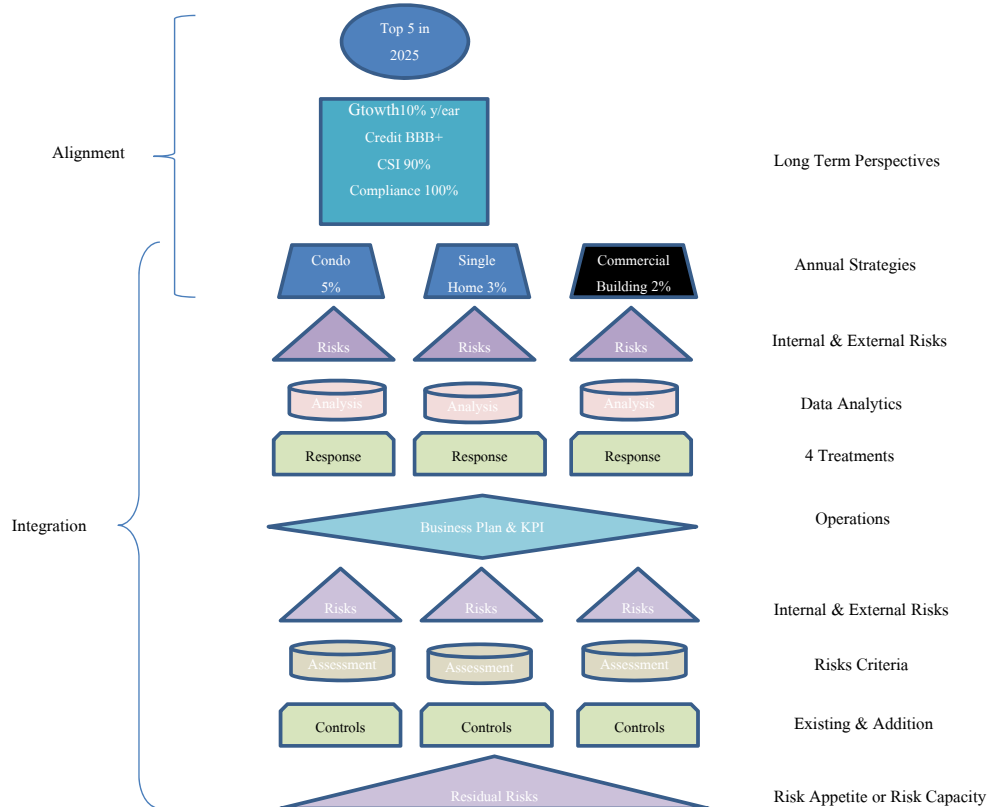
23

Monitoring ERM Performance



24

Case Study



25

Management Roles

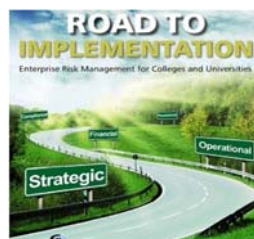
Large Public/Private Entity	Small Business Entity	Governmental Entity
• Chief executive officer and president • Chief administrative officer • Chief audit executive • Chief compliance officer • Chief data officer • Chief financial officer • Chief human resources officer • Chief information officer • Chief innovation officer • Chief legal officer/general counsel • Chief marketing officer • Chief operating officer • Chief strategy officer	• President • Chief financial officer/vice president (VP) of finance/finance director/head of finance/controller • Director of risk management/head of risk management • Chief operating officer • General manager/VP of operations • VP marketing/marketing manager • VP human resources/human resources director • VP of technology/IT manager	• Secretary • Assistant secretary/deputy director/undersecretary • Chief financial officer • Chief information officer • Chief of human resources • Chief of staff • Deputy assistant secretary/directorate • General counsel • Inspector general

26

Head of Risk Management

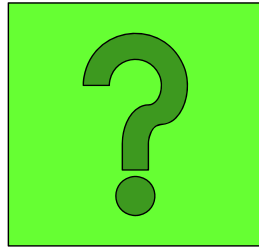
- ❖ Report to CEO & Assist Board Oversight on ERM
- ❖ Establishing Ongoing ERM Practices
- ❖ Overseeing ERM as Second Line of Accountability
- ❖ Review ERM in Each Operating Unit
- ❖ Communicating with Management through a Forum
- ❖ Integrating ERM into Business Plan & Reporting
- ❖ Evolving Organization to ERM Maturity & Suitability
- ❖ Escalating Risk Exposures to Executive and Board

27



Assessing ERM Maturity

28



Tel: (089) 919-7000

Email:

sphinicharomna@yahoo.com

leeandphinicharomna@gmail.com