

The New, COSO 2017 ERM Framework



ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

กรรมการผู้จัดการ บริษัท เลาบราเคอร์สอินเตอร์เนชั่นแนล จำกัด

อาจารย์พิเศษ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

14 พฤษภาคม 2017

Topics



- The Old, COSO 2004 ERM (Enterprise Risk Management) Framework
 - Obstacles and misconceptions
- The New, COSO 2017 ERM Framework
 - Comparison with COSO 2004

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

2



The Old, COSO 2004 ERM Framework

OBSTACLES AND MISCONCEPTIONS

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

3



What is Risk?

- Need to understand the difference between the risk management concepts of **expected outcome (loss)** and **unexpected outcome** (Loss/Gain) or uncertainty
 - Many people think that expected loss or any undesirable outcome is "risk".*

พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. ๒๕๕๔

เสี่ยง ๒

ก. ลองเผชิญดู, ลองทำดูในสิ่งที่อาจให้ผลได้ ๒ ทาง คือ ดีหรือไม่ดี แต่หวังว่าจะได้ผลทางดี เช่น งานนี้ไม่แน่ใจว่าจะสำเร็จหรือไม่ ต้องเสี่ยงทำดู.

เสี่ยง ๓

ก. มีโอกาสจะได้รับทุกข์หรืออันตรายเป็นต้น เช่น พูดอย่างนี้เสี่ยงคุกเสี่ยงตะราง.

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

4

Risk Management



- Risk management becomes *not the process of controlling and reducing expected losses* (which is essentially a budgeting, pricing, and business efficiency concern), but the process of understanding, costing, and efficiently **managing unexpected levels of variability in the outcomes** for a business.

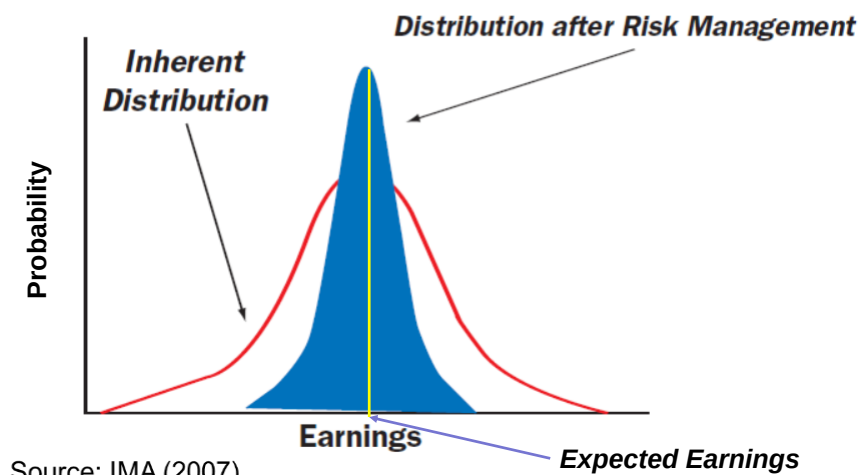
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

5

Goals of Risk Management



EXHIBIT 12. GOALS OF RISK MANAGEMENT



ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

6

COSO



- Committee of Sponsoring Organizations of the Treadway Commission (COSO) was organized in 1985.
- COSO is a joint initiative of five private sector organizations and it's goal is to provide thought leadership dealing with three interrelated subjects:
 - enterprise risk management (ERM),
 - internal control, and
 - fraud deterrence.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

7

ERM-COSO



- Enterprise risk management is a **process**,
- effected by an entity's **board of directors, management and other personnel**,
- applied in **strategy** setting and **across** the enterprise,
- designed to **identify potential events** that may affect the entity,
- and manage risk to be within its **risk appetite**,
- to provide reasonable assurance regarding the achievement of **entity objectives**.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

8

The ERM Framework-COSO



- ERM framework is geared to achieving an entity's objectives, set forth in four categories:
 - *Strategic* – high-level goals, aligned with and supporting its mission
 - *Operations* – effective and efficient use of its resources
 - *Reporting* – reliability of reporting
 - *Compliance* – compliance with applicable laws and regulations
- A particular objective can fall into more than one category.
 - *ERM does not say that there are 4 types of risk category.*



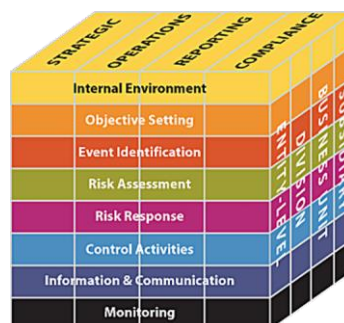
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

9

The ERM Framework-COSO



- ERM considers activities **at all levels** of the organization:
 - Enterprise-level
 - Division or subsidiary
 - Business unit processes
 - *The integration process is not easy.*
- ERM requires an entity to take a **portfolio** view of risk.
 - Management considers how individual risks interrelate.
 - *This can be viewed as consistent with Basel III concept.*



ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

10

ERM Creates Values

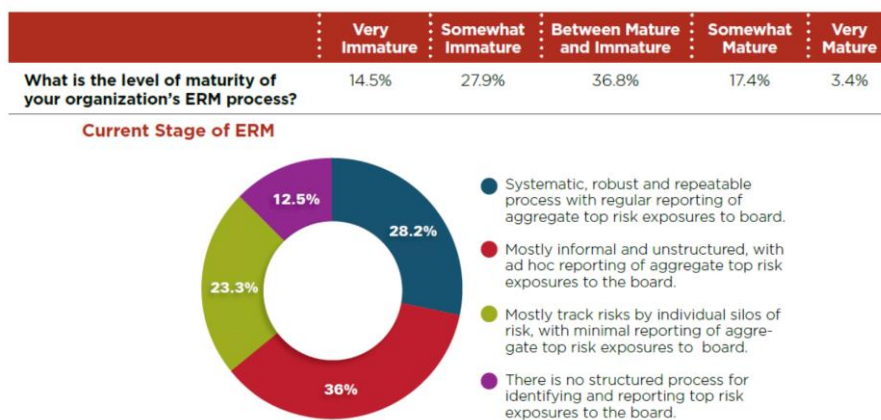


- From Carroll (2015), ERM can deliver value by driving positive change. A survey of business executives showed the following improvements:
 - 72% made better risk-adjusted decision making
 - 60% enhanced board risk oversight
 - 59% improved performance management
 - 58% improved capital efficiency
 - 55% experienced organizational and process optimization
 - 54% achieved higher quality strategic planning
 - 53% improved regulatory compliance
 - 50% improved brand reputation

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

11

ERM: Full Integration is Hard



Source: Beasley et. al. (2010)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

12

ERM: Full Integration is Hard



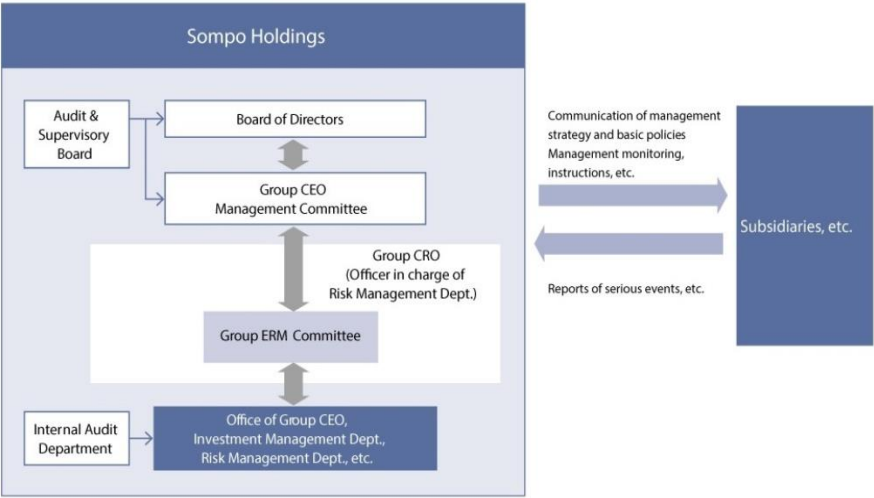
Figure 1: Changes in Mindset towards Risk Management (Percentage Distribution)

	North America	Europe	Revenues Under \$1 Billion	Revenues At Least \$1 Billion	Publicly Traded	Privately Owned
Continue to see risk as a threat to the organization and actively manage it, but not in an integrated manner	38%	40%	39%	34%	35%	38%
Now see risk as part of business and we actively manage both the opportunities and threats, but not in an integrated manner	28	38	23	38	33	24
Recently decided to approach risk in integrated manner across functions, business lines and risk classes	26	8	24	19	26	19
Continue to see risk as a threat to the organization, but we still do not manage it actively	6	11	14	6	2	19
Other	2	3	1	3	4	0

Source: 2013 gtnews Treasury Risk Survey

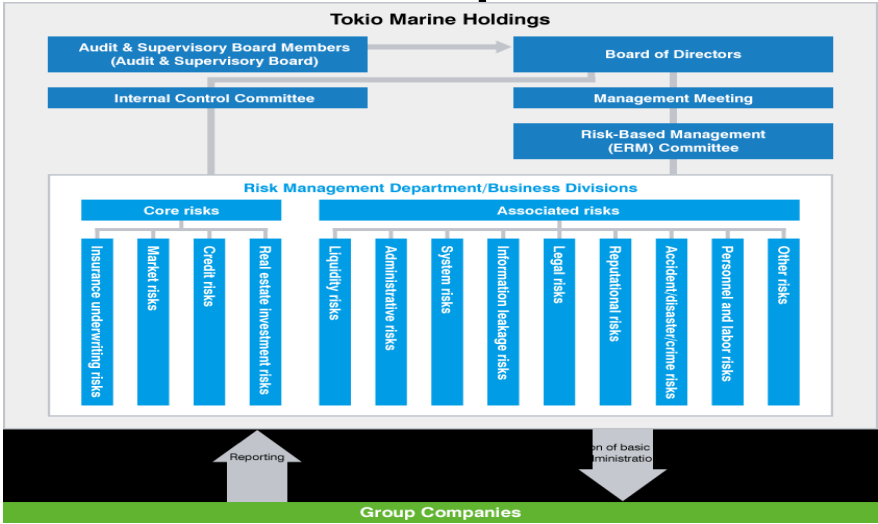
Source: Essaiades (2013) ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ 13

ERM for Holding Companies is Complex



ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ 14

ERM for Holding Companies is Complex



ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

15

Practical Direction?



Perceptions about COSO's ERM Framework Positive Statements	Percentages		
	"Not at All or Minimal"	"Moderate"	"Significant or A Great Deal"
Provides theoretically sound principles and guidance for ERM	8.4%	25.0%	66.6%
Provides a common language for ERM that is widely accepted by organizations and their stakeholders	20.2%	33.4%	46.4%
Clearly describes the key elements of a robust ERM process	17.8%	36.4%	45.8%
Demonstrates that ERM can add value to an organization	29.5%	32.5%	38.0%
Enables management to better assess how much risk the organization accepts relative to stated objectives	26.8%	37.0%	36.2%
Provides clear and practical direction and guidance for the implementation of ERM	35.8%	39.5%	24.7%

Source: Beasley et. al. (2010)

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

16

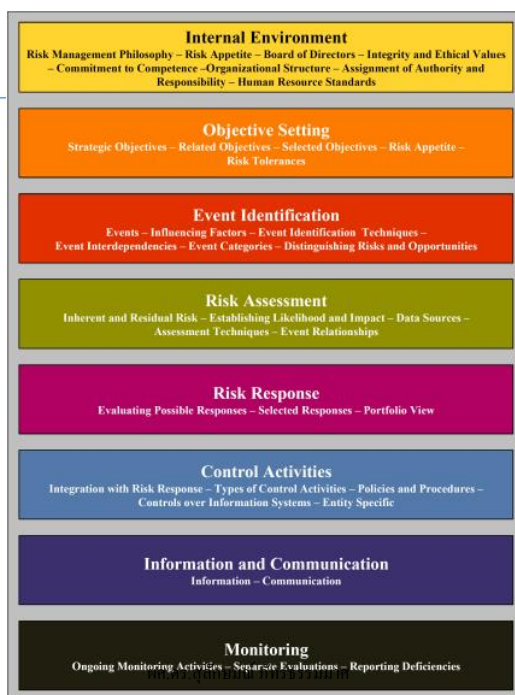
Clearing of Misconceptions



- From COSO (2017)
- Enterprise risk management is not a function or department.
- Enterprise risk management is more than a risk listing.
- Enterprise risk management addresses more than internal control.
- Enterprise risk management is not a checklist.
- Enterprise risk management can be used by organizations of any size.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

17



Source:
COSO
(2004b)

18

1. Internal Environment



- The 2 most difficult tasks are:
 - *Established Risk Appetite*
 - *Establishes the entity's risk culture*

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

19

Risk Appetite



- Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of value.
- It reflects the entity's risk management philosophy, and in turn influences the entity's culture and operating style.
 - *What is the unit of such risk appetite?*
 - *Numerical or Statement?*
 - *Low risk/High risk could mean different level of risks to different people.*

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

20

Examples of Risk Appetite Statements



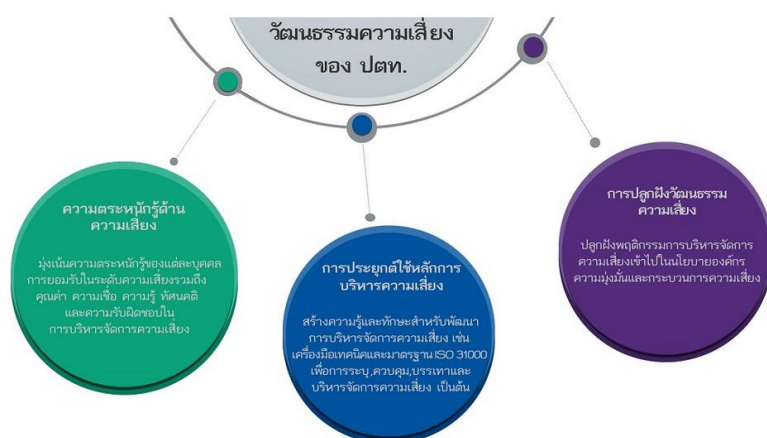
- The Organization operates *within a low overall risk range*. The Organization's lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite towards its strategic, reporting, and operations objectives. This means that reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment, and meeting our legal obligations will take priority over other business objectives.

Source: Office of the Comptroller of the Currency (2016)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

21

Risk Culture: Implementation?



ด้วยตระหนักว่าการบริหารจัดการความเสี่ยงและการบริหารความต่อเนื่องทางธุรกิจอย่างมีประสิทธิภาพจำเป็นต้องได้รับความร่วมมือจากทุกคนในองค์กร ปตท. จึงได้บรรจุเรื่องการบริหารจัดการความเสี่ยงและการบริหารความต่อเนื่องทางธุรกิจเป็นส่วนหนึ่งของคำบรรยายลักษณะงาน (Job Description) สร้างความตระหนักรู้และปลูกฝังวัฒนธรรมให้กับพนักงานทุกระดับตามบทบาทและหน้าที่ และให้ผู้ที่เกี่ยวข้องทุกฝ่ายมีส่วนร่วมในแผนการบริหารจัดการฯ อีกทั้งยังกำหนดตัววัดของผลการดำเนินงานสำหรับผู้บริหารเพื่อการวัดประสิทธิภาพและประสิทธิผลการดำเนินงานอย่างต่อเนื่อง

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

22

2. Objective Setting



- Is applied when management considers risks strategy in the setting of objectives.
- Risk tolerance, the acceptable level of variation around objectives, is aligned with risk appetite.
 - No standard guidelines
 - Tend to define risk tolerance for each risk factor not at objective level.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

23

Risk Appetite & Risk Tolerance



- Source: <https://www.izenbridge.com/blog/what-is-the-difference-between-risk-appetite-risk-tolerance-and-risk-threshold/>

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

24

3. Event Identification



- Differentiates **risks and opportunities**.
- Events that may have a negative impact represent risks.
 - *Most organization tends to focus more on this part.*
- Events that may have a positive impact represent natural offsets (opportunities), which management channels back to strategy setting.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

25

Inherent and Residual Risk



- **Inherent Risk**: The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls)
- **Residual Risk**: The risk that remains after controls are taken into account (the net risk or risk after controls).
- *Most of the time we tend to focus on and identify residual risk.*
 - Low residual risk could mean that the inherent risk is large but the existing risk management is very effective.

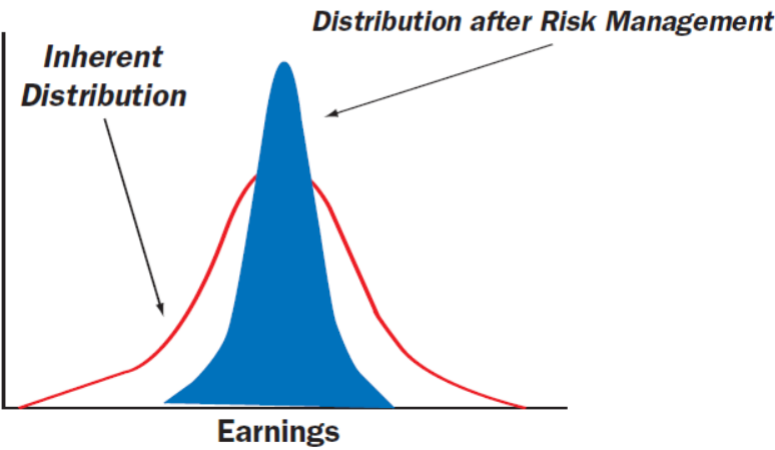
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

26

Inherent and Residual Risk



EXHIBIT 12. GOALS OF RISK MANAGEMENT



Source: IMA (2007)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

27

Risk List & Domains- Examples



Strategic / External	Operational	Human Capital	Financial	Legal & Compliance	Technology	Hazard
• Competition • Affiliation, Mergers & Acquisitions • Variability in Patient-Related Volume • Research Grant / Funding Availability • New Models for Care Delivery • Diminished Market • Regulatory Change / Healthcare Reform • Conflict of Interest • Decreased Capital Spending • Hospital / Physician Relationship • Availability of Public Data (HAI/HAC)	• Business Management Discipline / Cost Management • Equipment Maintenance • Failure to Identify & Follow EBM • Facility Maintenance • Timely Access to Care • Failure to Refer • Failure to Diagnose • Clinical Continuity • Insufficient Discharge Planning • Inconsistent Clinical Competency	• Hiring & Retention • Organizational Structure, Alignment & Direction • Succession Planning • Unionization • Turnover • Recruitment • Aging Workforce • Disruptive Behavior • Flex Staffing • Workers' Compensation • Physician Shortage	• Credit / Collections • Financial Performance • Billing Accuracy / Compliance • Payer Mix / Reimbursements • Pension / Retirement Obligations • Philanthropy / Fundraising / Capital Campaign • Failure to Meet Margin • Uncompensated Care • Access to Capital • Contract Management • Revenue Enhancement	• Conflicts of Interest • Fraud, Theft and Embezzlement • Governance, Compliance and Oversight • ACO • HIPAA Privacy & Security • Health Reform • Employment Practices	• Multiple Vendors • Social Networking • Information Breach • Bar Coding • Hybrid EMR • IT Infrastructure & Security • Paucity of IT Professionals • Failure to Act in a Timely Manner • Incompatible Programs	• Natural Disaster • Failure to Plan • Failure to Act Timely • Inability to Manage a Crisis • No Backup Systems or Appropriate Duplicate systems

Overlapping Issue

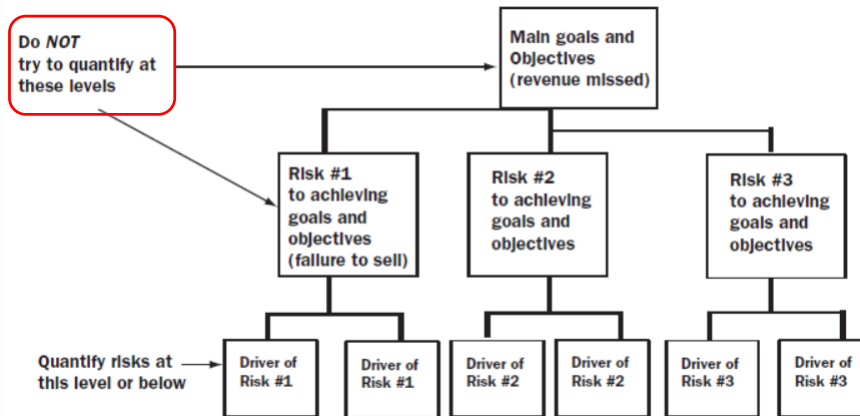
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

28

Risk Identification



EXHIBIT 5. QUANTIFYING RISK: DETERMINE THE DRIVERS



Source: IMA (2007)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

29

4.การประเมินความเสี่ยง (Risk Assessment)



- Allows an entity to understand the extent to which potential events might impact objectives.
- Assesses risks from two perspectives:
 - Likelihood
 - Impact
- Is used to assess risks and is normally also used to measure the related objectives.
- Employs a combination of both qualitative and quantitative risk assessment methodologies.
- Assesses risk on both an inherent and a residual basis.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

30

Assess Risk Process Flow



Exhibit 2: Assess Risks Process Flow Diagram



Source: Curtis and Carey (2012)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

31

Develop Assessment Criteria



- Developing Assessment Scales
- Some form of measurement of risk is necessary.
 - Without a **standard** of comparison, it's simply not possible to **compare and aggregate risks across the organization**.
 - Most organizations define scales for rating risks in terms of impact, likelihood, and other dimensions.
 - These scales comprise rating levels and definitions that foster consistent interpretation and application by different constituencies.
 - A Likert scale ranking of one (1) to five (5) is most often used.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

32

Illustrative Impact Scale

Rating	Descriptor	Definition
5	Extreme	- Financial loss of \$X million or more¹ - International long-term negative media coverage; game-changing loss of market share - Significant prosecution and fines, litigation including class actions, incarceration of leadership - Significant injuries or fatalities to employees or third parties, such as customers or vendors - Multiple senior leaders leave
4	Major	- Financial loss of \$X million up to \$X million - National long-term negative media coverage; significant loss of market share - Report to regulator requiring major project for corrective action - Limited in-patient care required for employees or third parties, such as customers or vendors - Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3	Moderate	- Financial loss of \$X million up to \$X million - National short-term negative media coverage - Report of breach to regulator with immediate correction to be implemented - Out-patient medical treatment required for employees or third parties, such as customers or vendors - Widespread staff morale problems and high turnover
2	Minor	- Financial loss of \$X million up to \$X million - Local reputational damage - Reportable incident to regulator, no follow up - No or minor injuries to employees or third parties, such as customers or vendors - General staff morale problems and increase in turnover
1	Incidental	- Financial loss up to \$X million - Local media attention quickly remedied - Not reportable to regulator - No injuries to employees or third parties, such as customers or vendors - Isolated staff dissatisfaction

Source: Curtis and Carey (2012) ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

33



Important Issues

- Different definitions are often used due to different nature of risk.
- Can different definitions really have the same level of impact?
 - Basel III define categories of risk and provide options on how to calculate risk.
- Are the definitions of scale 1 to 5 clearly defined?
- Can all business units/levels use the same scale?
 - How can we sum up the severity of risk from lower levels to upper levels?

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

34



แผนบริหารความเสี่ยง มหาวิทยาลัยธรรมศาสตร์



ปีงบประมาณ 2559

1.1) ความล่าช้าของโครงการที่ใช้เงินลงทุนสูง

ผลกระทบต่อ มธ.	ความเสียหาย	ระดับคะแนน
สูงมาก	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 180 วัน	5

1.2) ความล่าช้าของโครงการสำคัญ เช่น โครงการตามยุทธศาสตร์มหาวิทยาลัย

โครงการตามนโยบายมหาวิทยาลัย โครงการหลักสูตรใหม่

ผลกระทบต่อ มธ.	ความเสียหาย	ระดับคะแนน
สูงมาก	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 360 วัน	5

1.3) ความล่าช้าในการปฏิบัติงานตามปกติ

ผลกระทบต่อ มธ.	ความเสียหาย	ระดับคะแนน
สูงมาก	ทำให้เกิดความล่าช้าในการปฏิบัติงานมากกว่า 24 วัน	5

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

35

แผนบริหารความเสี่ยง มหาวิทยาลัยธรรมศาสตร์



ปีงบประมาณ 2559

2) ความเสียหายด้านการเงิน หมายถึง การที่มหาวิทยาลัยต้องสูญเสียเงิน อันเนื่องมาจากการทุจริตภายใน การถูกปรับ การชดเชยให้คู่กรณี การซ่อมแซมครุภัณฑ์/อาคาร ที่เกิดการปฏิบัติงานที่บกพร่อง ผิดพลาด ส่วนต่างอันเนื่องมาจากการลงทุนที่ผิดพลาด หนี้สูญ การฟื้นฟูความเสียหายจากภัยพิบัติ

ผลกระทบต่อ มธ.	ความเสียหาย	ระดับคะแนน
สูงมาก	สูญเสียเงินมากกว่า 10% ของเงินสะสม	5

3) ความเสียหายด้านชื่อเสียง หมายถึง การเผยแพร่ข่าวทางลบผ่านสื่อต่าง ๆ ยกเว้นทาง

Internet

ผลกระทบต่อ มธ.	ความเสียหาย	ระดับคะแนน
สูงมาก	เป็นข่าวทางลบในหนังสือพิมพ์หน้า 1 มากกว่า 5 ฉบับ	5

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

36

แผนบริหารความเสี่ยง มหาวิทยาลัยธรรมศาสตร์



ปีงบประมาณ 2559

4.1 การประเมินในลักษณะนามธรรม ดังนี้

ผลกระทบต่อ มธ.	ความเสี่ยง	ระดับคะแนน
สูงมาก	เสียทรัพยากร (เงิน เวลา บุคลากร) โดยไม่เกิดประโยชน์ และก่อให้เกิดความเสียหาย	5

4.2 การประเมินในลักษณะรูปธรรม โดยพิจารณาจากอันดับของมหาวิทยาลัย

ธรรมศาสตร์ในภูมิภาคเอเชีย จำแนกตามกลุ่มสาขาวิชา โดย Quacquarelli Symonds Ltd., หรือ QS University Rankings ต่ำกว่าเป้าหมายที่มหาวิทยาลัยธรรมศาสตร์ต้องการ

ผลกระทบต่อ มธ.	ความเสี่ยงที่พิจารณาจากผลการจัดลำดับโดย QS	ระดับคะแนน
สูงมาก	มี 5 กลุ่มสาขาวิชา ที่ไม่อยู่ใน 100 ลำดับแรก	5

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

37

แผนบริหารความเสี่ยง มหาวิทยาลัยธรรมศาสตร์



ปีงบประมาณ 2559

5) ความเสียหาย ด้านคุณค่า และความดีงาม หมายถึงพฤติกรรมและการแสดงออกของ

นักศึกษา บุคลากร ที่ส่งผลกระทบต่อมหาวิทยาลัยในลักษณะต่าง ๆ ดังนี้

ผลกระทบต่อ มธ.	ความเสี่ยง	ระดับคะแนน
สูงมาก	สูญเสียอัตลักษณ์และความเป็นตัวตน	5
สูง	มธ. ได้รับการสนับสนุนน้อยลงจากสังคม	4
ปานกลาง	จำนวน นศ. สมัครเข้า มธ. ลดลง	3
ต่ำ	ประชาคม มธ. อยู่อย่างไม่เกื้อกูลกัน	2
ต่ำมาก	จำนวนกิจกรรมที่ดีและสำเร็จลดลง	1

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

38

แผนบริหารความเสี่ยง มหาวิทยาลัยธรรมศาสตร์



ปีงบประมาณ 2559

5. ปัจจัยเสี่ยง : กระบวนการพิจารณาตำแหน่งทางวิชาการใช้เวลามากเกินไป

2) ประเมินความเสียหาย ปัจจัยเสี่ยงนี้จะทำให้เกิดความเสียหาย ในลักษณะที่หลากหลาย ดังนี้

ลักษณะความเสียหาย	การแปลค่า	แปลงเป็นคะแนน
สัดส่วนตำแหน่งทางวิชาการต่ำกว่ามหาวิทยาลัยอื่นที่มีขนาดใกล้เคียงกัน	สูงมาก	5
บรรยากาศวิชาการในมหาวิทยาลัยไม่คึกคัก	สูง	4
ระยะเวลาในการบรรจุนโยบายอธิการบดี (อ.ประจักษ์) ตำแหน่งทางวิชาการมากกว่า 55% ภายในปี 2560) มากเกินความเป็นจริง	ปานกลาง	3
อาจารย์ที่ยื่นขอตำแหน่งแล้วขาดขวัญและกำลังใจ	ต่ำ	2
อาจารย์ขาดแรงจูงใจในการเข้าสู่ตำแหน่งวิชาการ	ต่ำมาก	1

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

39

Likelihood



- Likelihood represents the possibility that a given event will occur. Likelihood can be expressed using qualitative terms (frequent, likely, possible, unlikely, rare), as a percent probability, or as a frequency.
- When using numerical values, whether a percentage or frequency, the relevant time period should be specified such as annual frequency or the more relative probability over the life of the project or asset.
- *Tend to be less problematic.*

ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

40



Likelihood Scale

Illustrative Likelihood Scale				
Rating	Annual Frequency		Probability	
	Descriptor	Definition	Descriptor	Definition
5	Frequent	Up to once in 2 years or more	Almost certain	90% or greater chance of occurrence over life of asset or project
4	Likely	Once in 2 years up to once in 25 years	Likely	65% up to 90% chance of occurrence over life of asset or project
3	Possible	Once in 25 years up to once in 50 years	Possible	35% up to 65% chance of occurrence over life of asset or project
2	Unlikely	Once in 50 years up to once in 100 years	Unlikely	10% up to 35% chance of occurrence over life of asset or project
1	Rare	Once in 100 years or less	Rare	<10% chance of occurrence over life of asset or project

Source: Curtis and Carey (2012)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

41



แผนบริหารความเสี่ยง มหาวิทยาลัยธรรมศาสตร์ ปีงบประมาณ 2559

โอกาสที่จะเกิดขึ้น (เฉลี่ย)	การแปลค่าโอกาสที่จะเกิด	ระดับคะแนน
1 ครั้งในรอบ 1 เดือน	สูงมาก	5

2) การประเมินโอกาสที่จะเกิดความเสี่ยงในระดับส่วนงานย่อย (หรือหน่วยงานภายในมหาวิทยาลัยธรรมศาสตร์)

จำนวนหน่วยงานที่มีความเสี่ยง	การแปลค่าจำนวนหน่วยงาน	ระดับคะแนน
มากกว่า ร้อยละ 80	สูงมาก	5

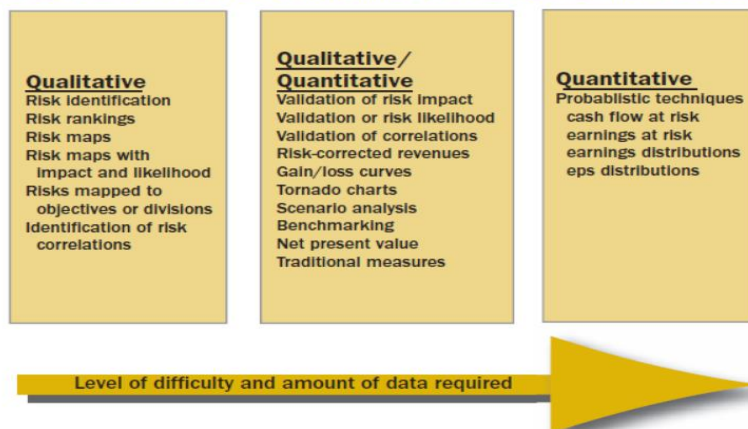
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

42

การประเมินความเสี่ยง (Risk Assessment)



EXHIBIT 6. QUALITATIVE AND QUANTITATIVE APPROACHES TO RISK ASSESSMENT



Source: IMA (2007)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

43

Risk Scores



- To determine the ranking the likelihood score is multiplied by the impact score to determine the risk score.
- Likelihood x Impact = Risk Score**
 - If likelihood and impact criteria is not comparable for all risk factors, the risk scores cannot be comparable.
- If impacts are not comparable, using risk score for comparison and allocating resources would be problematic.*

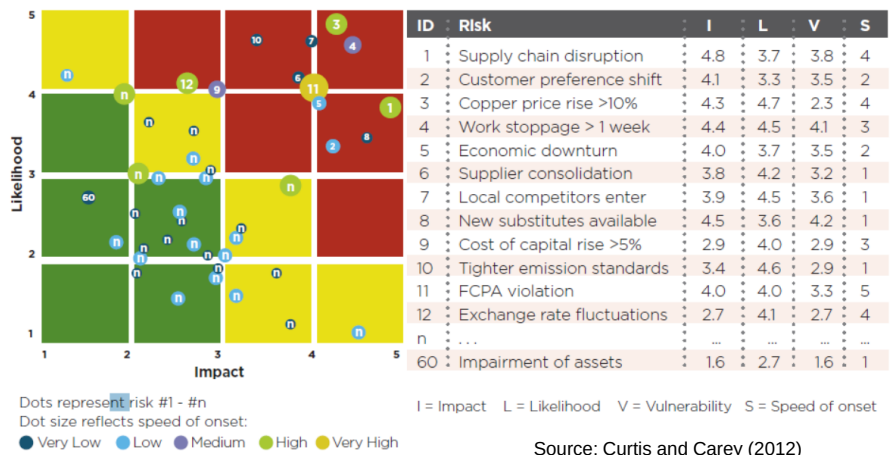
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

44

Risk Mapping/Heat Map



Exhibit 7: Illustrative Heat Map



ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

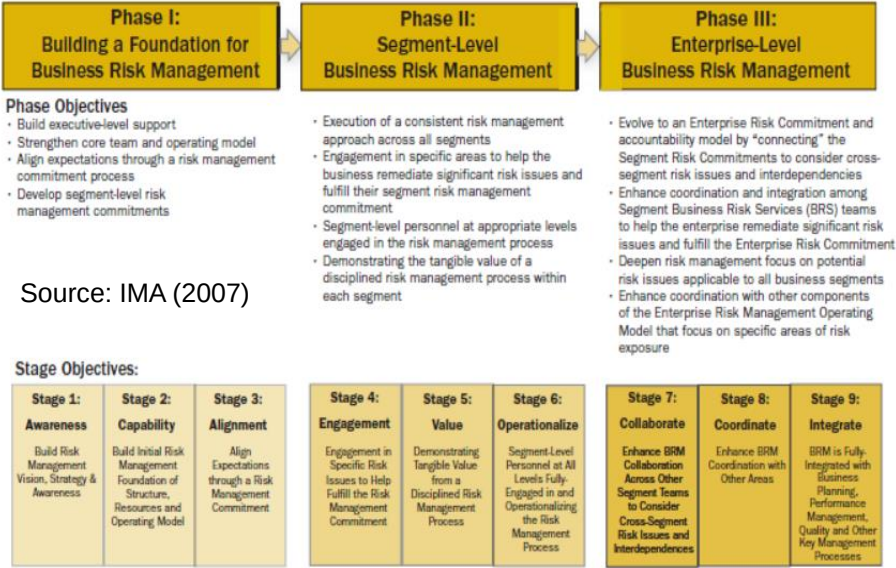
แผนบริหารความเสี่ยง มหาวิทยาลัยธรรมศาสตร์ ปีงบประมาณ 2559



ผลกระทบ	5	H	H	VH	VH	VH
	4	M	H	H	VH	VH
	3	M	M	H	H	VH
	2	L	M	M	H	H
	1	L	L	M	M	H
		1	2	3	4	5
โอกาสที่จะเกิด						

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

EXHIBIT 17. ERM MATURITY MODEL



ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส



The New, COSO 2017 ERM Framework

COMPARISON WITH COSO 2004

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

Definition of Risk



- The **possibility** that events will occur and affect the achievement of strategy and business objectives.
 - *If business objectives are set unreasonably high, the risk would be high.*

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

49

Definition of ERM



- The culture, capabilities, and practices, **integrated** with strategy-setting and **performance**, that organizations rely on to manage risk in creating, preserving, and realizing **value**.
- From COSO (2004), ERM is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

50

Role of Risk in Strategy Selection



Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

51

8 vs 5 Components



ERM 2004

- Internal Environment
- Objective Setting
- Event Identification
- Risk Assessment
- Risk Response
- Control Activities
- Information and Communication
- Monitoring

ERM 2017

- Governance and Culture
- Strategy & Objective-Setting
- Performance
- Review & Revision
- Information, Communication & Reporting

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

52

ERM Components



Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

53

Sets of Principles



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



Strategy & Objective-Setting

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



Performance

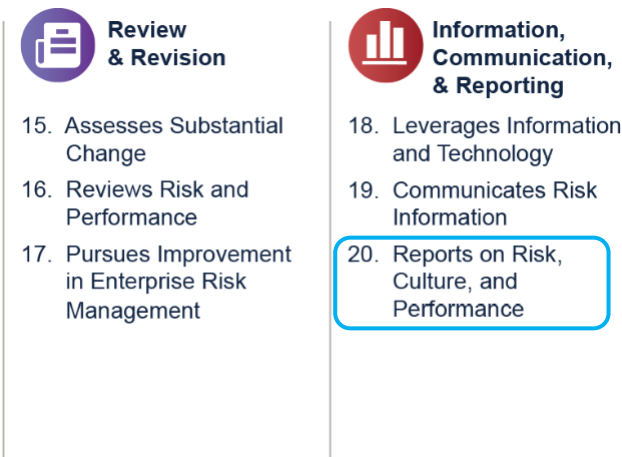
10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

54

Sets of Principles



Source: COSO (2017)

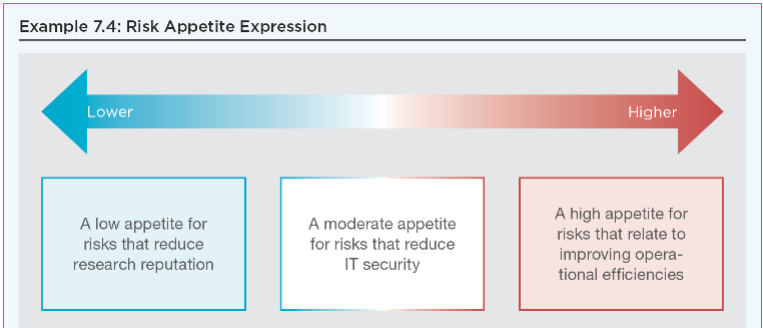
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

55

P7. Defines Risk Appetite



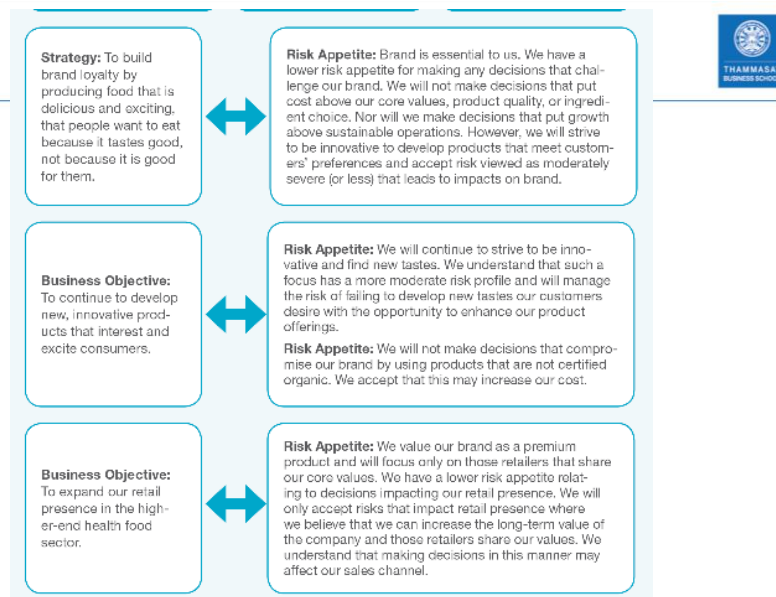
- There is no standard or “right” risk appetite that applies to all entities.



Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

56



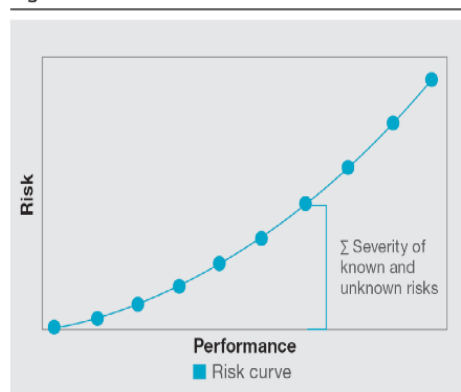
Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

57

Developing Risk Profile

Figure D.1: Risk Profile



- Each data point is plotted by considering the perceived amount of risk that corresponds to the achievement of a business objective or strategy.
- How could we do this in practice?

Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

58

Risk to Implementing the Strategy and Business Objectives



- From COSO (2017) p.51:
- Wherever possible, the organization should use **similar units** for measuring risk for each objective.
- Doing so will help to align the severity of the risk with established performance measures.

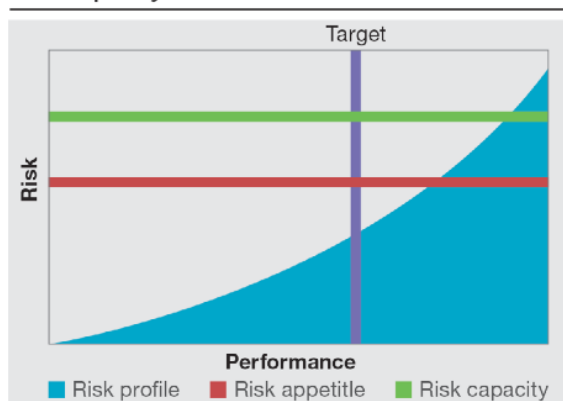
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

59

Risk Profile



Figure 7.3 Risk Profile Showing Risk Appetite and Risk Capacity



Risk appetite can be in qualitative or quantitative terms.

Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

60

P9. Formulates Business Objectives



Example 7.9: Sample Business Objectives by Level

Business objectives	Business Objective	Performance Measure and Target
Business objectives (entity)	- Continue to develop innovative products that interest and excite consumers - Expand retail presence in the health food sector	8 products in R&D at all times 5% growth year over year
Business objectives for North America (division)	- Increase shelf space in leading stores that share our core values - Continue to source products in local markets	7% increase in shelf space 92% local source rate
Business objectives for Confectionary (operating unit)	Develop high-quality and safe snack products that exceed consumer expectations	4.8 out of 5 in customer satisfaction survey
Business objectives for Human Resources (function)	- Maintain favorable annual turnover of employees - Recruit and train product sales managers in the coming year	- Turnover less than 10% - Recruit 50 sales managers 95% training rate for sales staff

Source: COSO (2017) ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

61

Risk Tolerance



Example 7.11: Tolerance Statements

Business Objective	Target	Tolerance
Return on investment (ROI) for an asset manager	Target 5% annual return on its portfolio	3% to 7% annual return
On-line home delivery orders for a restaurant	Target delivery within 40 minutes	30- to 50-minute delivery time
Minimize missed calls from a call center	Target 2% of overall calls	1% to 5% of overall calls

- Tolerance focuses on objectives and performance, not specific risks.*

Source: COSO (2017)

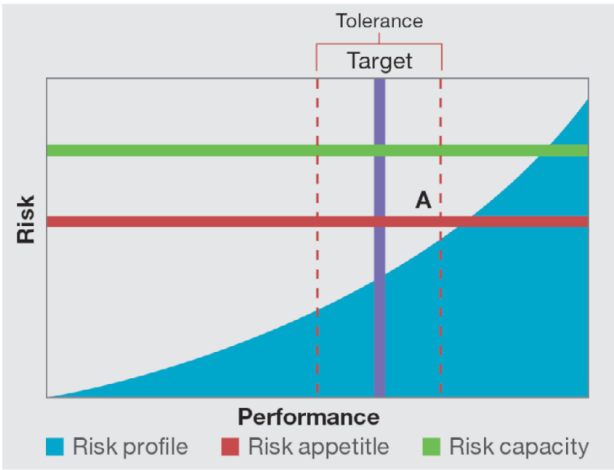
ผศ.ดร.สุลักษณ์ ภักธรธรรมมาศ

62



Risk Profile

Figure 7.5 Risk Profile Showing Tolerance



Source: COSO (2017)

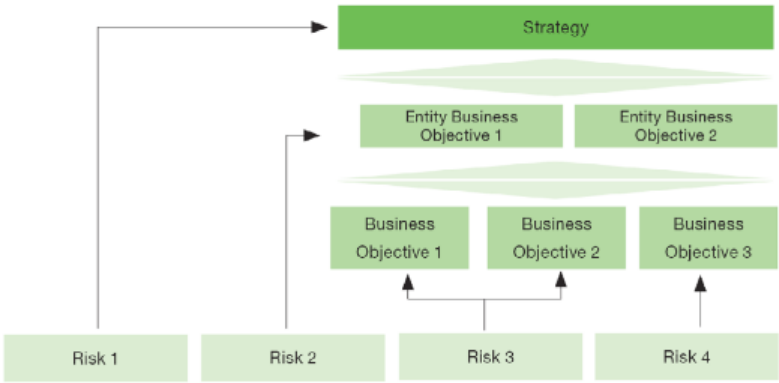
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

63



P10. Identifies Risk

Figure 8.2: Risk Impacts at Differing Levels



Source: COSO (2017)

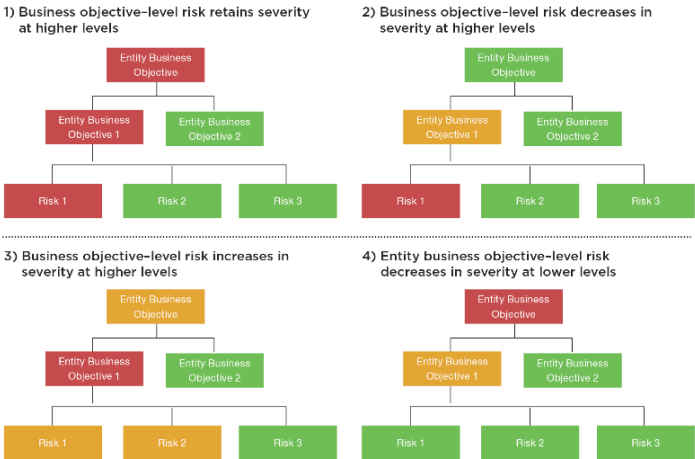
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

64

P11. Assesses Severity of Risk



Figure 8.6: Assessing Severity at Different Levels



Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

Depicting Assessment Results



Figure 8.8: Business Objective Heat Map



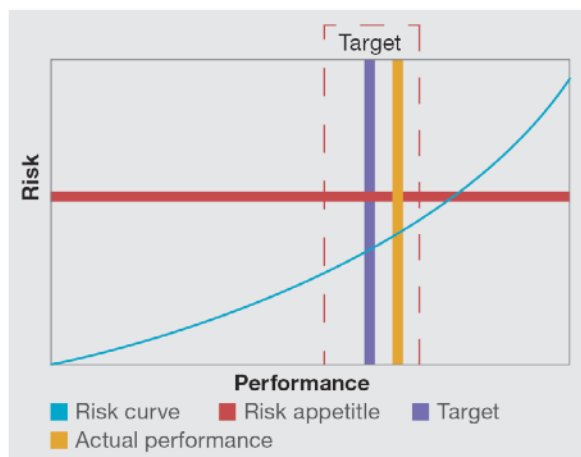
Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

Risk Profile



Figure 8.9: Business Objective Risk Profile



- Does better actual performance mean that risk is under control?
- Does lower actual performance mean lower risk?

Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

67

P12. Prioritize Risks



- Prioritization takes into account the **severity** of the risk compared to **risk appetite**.
 - Risks with **similar assessments of severity** may be **prioritized differently**.
 - *Puzzle!!*
 - *Using severity measure plus ????*
- Priorities are determined by applying **agreed-upon criteria**.
 - This would mean organization would have to design these criteria and how to measure them.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

68

Prioritize Risks



- Examples of these criteria include:
 - **Adaptability**: The capacity of an entity to adapt and respond to risks.
 - **Complexity**
 - **Velocity**: The speed at which a risk impacts an entity.
 - **Persistence**
 - **Recovery**: The capacity of an entity to return to tolerance.

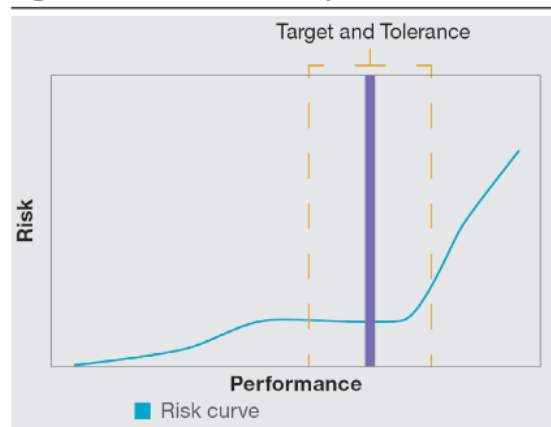
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

69

P13. Implements Risk Responses



Figure D.8 Effect of Risk Response



Source: COSO (2017)

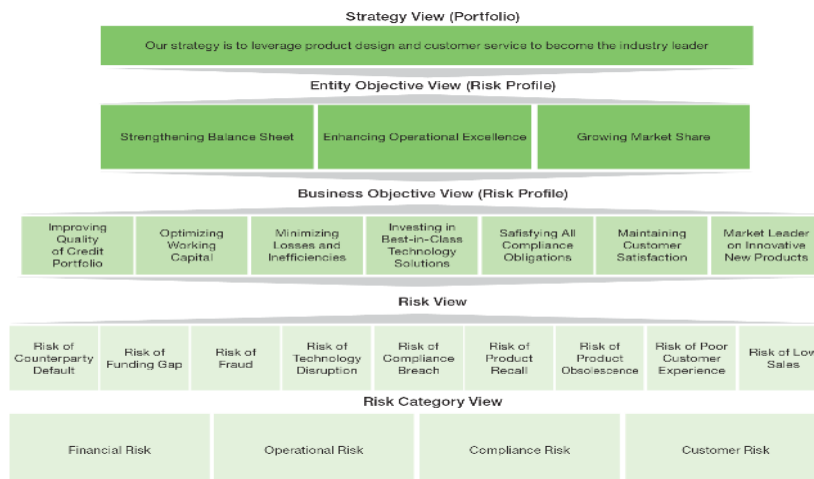
ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

70

P14. Develops Portfolio View



Figure 8.10 Portfolio View of Risk



Source: COSO (2017)

ผศ.ดร.สุลักษณ์ ภักตร์ธรรมมาศ

71

Analyzing Portfolio View



- To evaluate the portfolio view of risk, the organization will want to use both qualitative and quantitative techniques.
 - *Could all risk owners at all levels of entity do this?*
- Quantitative techniques** include regression modeling and other means of statistical analysis to understand the sensitivity of the portfolio to changes and shocks.
- Qualitative techniques** include scenario analysis and benchmarking.

ผศ.ดร.สุลักษณ์ ภักตร์ธรรมมาศ

72

Analyzing Portfolio View



- Undertaking **stress testing**, scenario analysis, or other analytical exercises helps an organization to avoid or better respond to big surprises and losses.
 - *Choosing how to do the stress testing has always been a challenging task.*
- By analyzing the effect of hypothetical changes on the portfolio view, the organization **identifies potential new, emerging, or changing risks** and evaluates the adequacy of existing risk responses.
 - *Does this mean that the risk identification was incomplete at the early stage?*

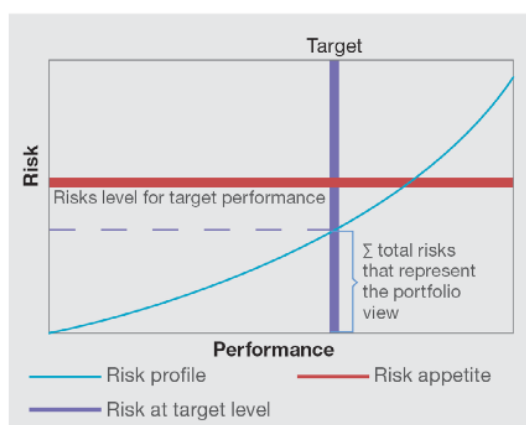
ผศ.ดร.สุลักษณ์ กัทรธรรมมาศ

73

Risk Profile with Portfolio View



Figure 8.11: Risk Profile Showing Risk as a Portfolio View



How to calculate these total risks?

Source: COSO (2017)

ผศ.ดร.สุลักษณ์ กัทรธรรมมาศ

74

References



- Beasley, M. S., B. C. Branson, B.V. Hancock, 2010, COSO's 2010 Report on ERM.
- Branson, B., 2015, Reporting Key Risk Information to the Board of Directors.
- Carroll, R., 2015, ASHRM Enterprise Risk Management Playbook (1st ed., Vol. 1), Chicago: ASHRM.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004a, Enterprise Risk Management – Integrated Framework.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004b, Applying COSO's Enterprise Risk Management – Integrated Framework.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2012, Understanding and Communicating Risk Appetite.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017, Enterprise Risk Management—Integrating with Strategy and Performance
- Curtis, P. and M.Carey, 2012, Risk Assessment in Practice

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

75

References



- Essaides, N., 2013, CTC guide to Enterprise Risk Management Beyond Theory: Practitioner Perspectives on ERM.
- IMA, 2007, Enterprise Risk Management: Tools and Techniques for effective Implementation.
- Narvez, K., 2013, Risk Appetite and Risk Tolerance: Critical Components of an Effective ERM Program.
- Office of the Comptroller of the Currency, 2016, Enterprise Risk Appetite Statement.
- Rittenberg, L. and F. Martens, 2012, Enterprise Risk Management — Understanding and Communicating Risk Appetite.
- สุลักษณ์ ภัทรธรรมมาส, บทที่ 10 “การบริหารความเสี่ยง,” ในการกำกับดูแลเพื่อสร้างมูลค่ากิจการ, อัญญา ชันชวิทย์ ศิลปพร ศรีจันทะพร และ เดือนเพ็ญ จันทศิริศรี บรรณาธิการ, พิมพ์ครั้งที่ 1 กรุงเทพมหานคร: อมรินทร์พริ้นติ้งแอนด์พับลิชชิ่ง, 2009, 281-312.

ผศ.ดร.สุลักษณ์ ภัทรธรรมมาส

76