หลักการและแนวปฏิบัติ

Board Risk Oversight

Roles and Responsibility

ศาสตราจารย์ ดร.อัญญา ขันธวิทย์

คณะพาณิชยศาสตร์และการบัญชี

มหาวิทยาลัยธรรมศาสตร์

หลักการและเหตุผล เพื่อ Value Creation

- บริษัทต้องบริหารจัดการเพื่อสร้างมูลค่าให้สูงที่สุด (Value Maximization)
- กลไก: ความเสี่ยงและการสร้างมูลค่าเพิ่ม (Market Value Added หรือ MVA) ของบริษัทจดทะเบียน

$$\text{MVA} = \frac{\text{EEP}_{(\text{Performance,Risk}),1}}{\left(1 + \text{ReqRet}_{(\text{Risk})}\right)^{\text{t=1}}} + \frac{\text{EEP}_{(\text{Performance,Risk}),2}}{\left(1 + \text{ReqRet}_{(\text{Risk})}\right)^{\text{t=2}}} + \cdots$$

- Expected Economic Profit (EEP) และ Required Rate of Return (ReqRet) ขึ้นกับ Performance and Risk ของบริษัท
- การบริหารจัดการ (Management) เป็น Key Driver ของ Performance and Risk
- Value Creation ย่อมหมายถึง **RISK-MANAGED Value Creation**

บทบาท หน้าที่ และความรับผิดชอบของกรรมการ

THAMMASAT BUSINESS SCHOOL

หลักการ

คณะกรรมการมีบทบาทสำคัญในการกำกับดูแลกิจการเพื่อประโยชน์สูงสุดของบริษัท คณะกรรมการมีความรับผิดชอบต่อผลการปฏิบัติหน้าที่ต่อผู้ถือหุ้นและเป็นอิสระจากฝ่ายจัดการ

แนวปฏิบัติที่ดี

3. บทบาท หน้าที่ และความรับผิดชอบของคณะกรรมการ

3.1 เรื่องที่ควรกำหนดให้เป็นหน้าที่ ความรับผิดชอบของคณะกรรมการให้ครอบคลุมในเรื่องดังต่อไปนี้

(1) การพิจารณาและให้ความเห็นชอบในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของบริษัท เช่น วิสัยทัศน์ และภารกิจ กลยุทธ์ เป้าหมายทางการเงิน ความเสี่ยง แผนงาน และงบประมาณ เป็นต้น

(2) การติดตามและดูแลให้ฝ่ายจัดการดำเนินงานตามนโยบายและแผนที่กำหนดไว้อย่างมีประสิทธิภาพและประสิทธิผล

(3) การควบคุมภายในและการบริหารความเสี่ยง รวมทั้งกลไกในการรับเรื่องร้องเรียนและการดำเนินการกรณีมีการชี้เบาะแส

(4) การดูแลให้การดำเนินธุรกิจต่อเนื่องในระยะยาว รวมทั้งแผนการพัฒนาพนักงาน ความต่อเนื่องของผู้บริหาร (Succession Plan)

นี่คือ Risk Oversight ไม่ใช่ Risk Management

บทบาท หน้าที่ และความรับผิดชอบของกรรมการ (ต่อ)

Risk Management
โดยฝ่ายจัดการ

หลักการ

คณะกรรมการมีบทบาทสำคัญในการกำกับดูแลกิจการเพื่อประโยชน์สูงสุดของบริษัท คณะกรรมการมีความรับผิดชอบต่อผลการปฏิบัติหน้าที่ต่อผู้ถือหุ้นและเป็นอิสระจากฝ่ายจัดการ

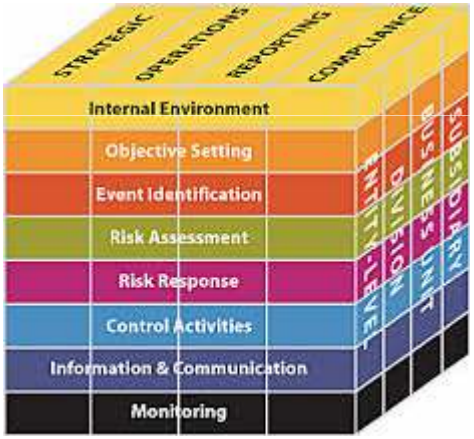
แนวปฏิบัติที่ดี

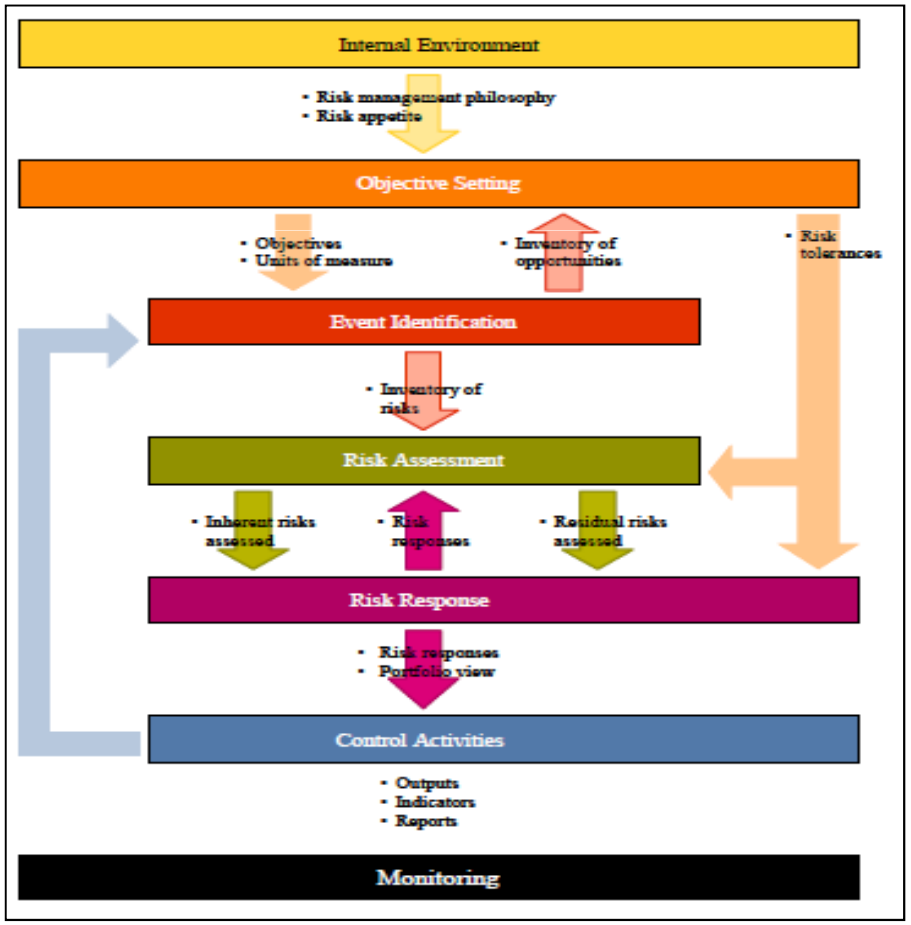
3.6 คณะกรรมการควรกำหนดนโยบายด้านการบริหารความเสี่ยง (Risk Management Policy) ให้ครอบคลุมทั้งองค์กร โดยให้ฝ่ายจัดการเป็นผู้ปฏิบัติตามนโยบายและรายงานให้คณะกรรมการทราบเป็นประจำ และควรมีการทบทวนระบบหรือประเมินประสิทธิผลของการจัดการความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และให้เปิดเผยไว้ในรายงานประจำปี และในทุกๆ ระยะเวลาที่พบว่า ระดับความเสี่ยงมีการเปลี่ยนแปลง ซึ่งรวมถึงการให้ความสำคัญกับสัญญาณเตือนภัยล่วงหน้าและรายการผิดปกติทั้งหลาย

3.7 คณะกรรมการ หรือคณะกรรมการตรวจสอบควรให้ความเห็นถึงความเพียงพอของระบบการควบคุมภายในและการบริหารความเสี่ยงไว้ในรายงานประจำปี

การบริหารความเสี่ยง ERM ตาม COSO ซึ่ง ตลท. ยอมรับ

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.

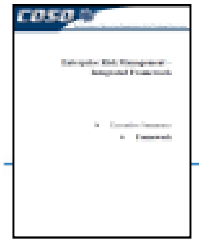




อ้างอิง:

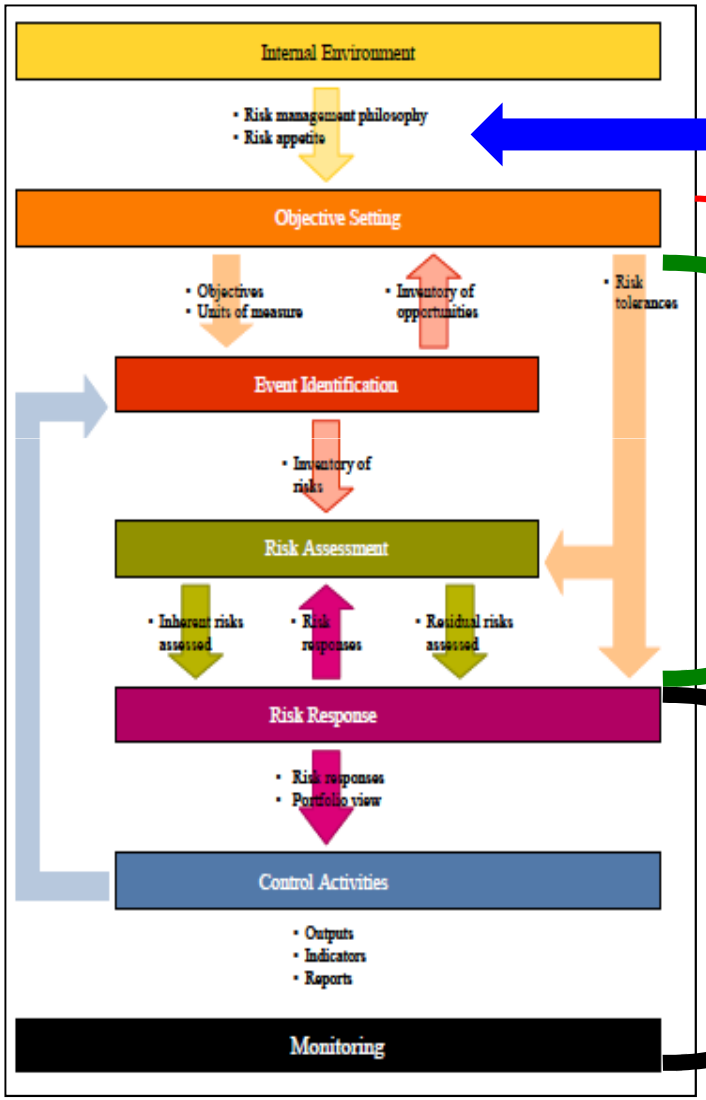
Risk Management vs. Risk Oversight

จาก https://www.youtube.com/watch?v=oeVo3cdOtTM



Recap:

COSO ERM



COSO's FOUR Highlighted Areas of Board Risk Oversight

THAMMASAT BUSINESS SCHOOL

- *Understand the entity's risk philosophy and concur with the entity's risk appetite.* Risk appetite is the amount of risk, on a broad level, an organization is willing to accept in pursuit of stakeholder value. Because boards represent the views and desires of the organization's key stakeholders, management should have an active discussion with the board to establish a mutual understanding of the organization's overall appetite for risks.

- *Review the entity's portfolio of risk and consider it against the entity's risk appetite.* Effective board oversight of risks is contingent on the ability of the board to understand and assess an organization's strategies with risk exposures. Board agenda time and information packets that integrate strategy and operational initiatives with enterprise-wide risk exposures strengthen the ability of boards to ensure risk exposures are consistent with overall appetite for risk.

- *Know the extent to which management has established effective enterprise risk management of the organization.* Boards should inquire of management about existing risk management processes and challenge management to demonstrate the effectiveness of those processes in identifying, assessing, and managing the organization's most significant enterprise-wide risk exposures.

- *Be apprised of the most significant risks and whether management is responding appropriately.* Risks are constantly evolving and the need for robust information is of high demand. Regular updating by management to boards of key risk indicators is critical to effective board oversight of key risk exposures for preservation and enhancement of stakeholder value.

ความหมาย

Area 1: Risk Philosophy, Risk Appetite and Communication

ก. Risk Philosophy (ความเชื่อที่ถูกต้อง)

ก.1 Risk-Managed Value Creation

ก.2 ความเสี่ยงสามารถบริหารจัดการได้

ข. Risk Appetite (ระดับความเสี่ยงเป้าหมาย เพื่อสร้างผลตอบแทนเป้าหมาย) และ Risk Tolerance (ระดับความเสี่ยงที่ “ทนได้ รับไหว” หากพลาดเป้า)

ข.1 Corporate ในภาพรวมของบริษัท (การสื่อสารอาจตั้งต้นที่ ROE ที่เท่ากับค่าเฉลี่ยอุตสาหกรรม อาจพิจารณาว่าเป็น ระดับปานกลาง)

ข.2 Strategic Objectives สื่อสารผ่าน KPIs และ Targets

ค. Communication ผ่าน Objective Settings ซึ่งมี Strategies and Plans “ที่ดี” ระดับ Sound Strategies and Disciplined Planning

ความหมาย

Area 2: Portfolio Risks

ก. ตั้งต้นที่แผนงานซึ่งกำหนดกิจกรรม KPIs และ Targets

ความเสี่ยงคือความเสี่ยงที่ดำเนินการตามแผนงาน แล้วได้ผลลัพธ์คลาดเคลื่อนจากเป้าหมายในทางลบ เกิดความเสียหายเกิน Risk Tolerance

ข. ฝ่ายจัดการประเมินระดับความเสี่ยงตาม (Impact x Likelihood) เทียบกับ Heat Map หากอยู่ใน Rejection Zone ระบุเป็น Key Risks ที่ กรรมการต้องอนุมัติ เพื่อให้ฝ่ายจัดการทำ Mitigation

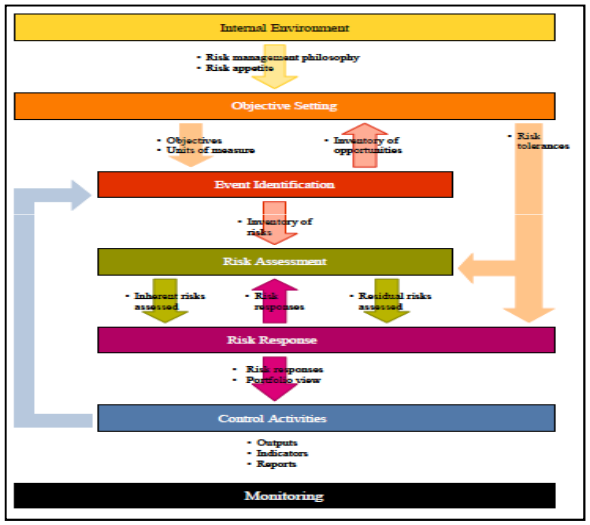
ค. กรรมการพิจารณาแล้ว “เชื่อหรือไม่เชื่อ” ว่าครอบคลุม ครบถ้วน และเป็น Key จริง

“เชื่อหรือไม่เชื่อ” = Comfortable

ความหมาย

Area 3: Established Effective Enterprise Risk Management

ก. Established? มีขั้นตอนครบถ้วน ตามสาระ จริง ซึ่งอาจมีรูปแบบชัดเจน หรือโดยนัย



ข. Effective? เป็นผล เกิดประโยชน์จริง

ข.1 **RISKs** นำไปสู่การบริหารจัดการได้ทัน ผลงานเป็นไปตามหรือเหนือกว่าเป้าหมาย

ข.2 **OPPORTUNITIEs** เห็นโอกาสเพิ่มเติมจากยุทธศาสตร์หรือแผนเดิม ปรับเป้าหมาย ขยายโอกาสและเพิ่มมูลค่าให้สูงยิ่งขึ้น (เริ่มต้นอาจเน้น ข.1 ก่อน)

ความหมาย

Area 4: Appropriate Risk Response (and Monitoring)

หลังจาก BOD เห็นชอบ Key Risks ฝ่ายจัดการจัดการ Key Risks โดยใช้ Risk Mitigation ตาม Risk Mitigation Plans

การเช็คสอบ Appropriate Response >>> "เชื่อหรือไม่เชื่อ" ว่าทำตาม Risk Mitigation Plans แล้ว Key Risks จะลดลงมาเหลืออยู่ภายใต้ Risk Tolerance

แนวทาง

1. เช็คสอบ Root Cause Analysis >> ให้ไปให้สุดทาง (5 Why's)

2. ทำ Cost-Benefit Analyses และเป็น Net Positive Value

3. ระวังภาพลวงตา อาทิ ความเสี่ยงค่าเงินอาจแก้ได้อย่างตรงไปตรงมาโดยใช้ Forward Hedging แต่ บริษัทอาจใช้ Natural Hedge ก่อน แล้วค่อยทำเพิ่มเฉพาะ Residual

"เชื่อหรือไม่เชื่อ"

ความหมาย

Area 4: Appropriate Risk Response (and Monitoring) (ต่อ)

ข้อสังเกต

Risk Mitigation Plan คือแผนงาน จะเกิดผลได้ต้องทำ และคาดหวังว่าจะเป็นไปตามเป้าหมาย คือความเสี่ยงลดลง และผลงานได้ตามเป้าหมาย

เพื่อให้เกิดความมั่นใจและแก้ไขปรับปรุงทัน ต้อง **Monitor**

ก. ตาม **Milestones** ของ

ก.1 **Outputs >>** ดำเนินกิจกรรมแล้วเสร็จตามแผนงาน

ก.2 **Outcome >>** ผลงานตาม **KPIs** และ **Targets** ของ **Key Risks**

ข. **Key Risk Indicators (KRIs)**

ข.1 การตรวจตราสภาพแวดล้อม และ **Assumptions**

ข.2 ออกแบบและติดตาม **KRIs** อย่างน้อยต้องมี

ข.2.1 **Escalation Triggers >>** ง่ายมาก เพราะคือการทำ **Performance Monitoring**

ข.2.2 **Loss Events >>** อาจต้องเริ่มเก็บ ตั้งต้นที่ฝ่ายตรวจสอบภายใน ถ้ายังไม่มี **OpRisk Unit**

COSO's 2010 Board Risk Oversight Survey

การสำรวจความเห็นของ **Board Members** กว่า **200** คนในประเทศสหรัฐอเมริกาและที่อื่น

What are the top obstacles that inhibit the risk oversight process? (multiple responses permitted)

Response	Percentage
There are more pressing needs, e.g., executing strategy and/or making sure the organization survives	40%
Lack of understanding/acceptance of enterprise risk management by board members	31%
Lack of perceived value of pursuing an ERM approach to risk management	31%
Organizational culture, e.g., risk management is viewed as a compliance activity, treated as an appendage to performance management, etc.	29%
Lack of clarity around/inability to agree on the entity's risk philosophy	28%
Availability of dedicated resources	26%
Disparate systems/processes make an enterprisewide view of risks difficult	19%
Inadequate risk management reporting, methodologies, systems and data	19%
Decentralized organization with highly autonomous business units	17%
Lack of understanding/acceptance of enterprise risk management by management	15%
Difficulty in getting on the same page with management with respect to the entity's risk appetite	14%
Other	8%

TBS-SET 2015 Board Risk Oversight "Quick" Survey

		1 = เห็นด้วย			4 = เห็นด้วย

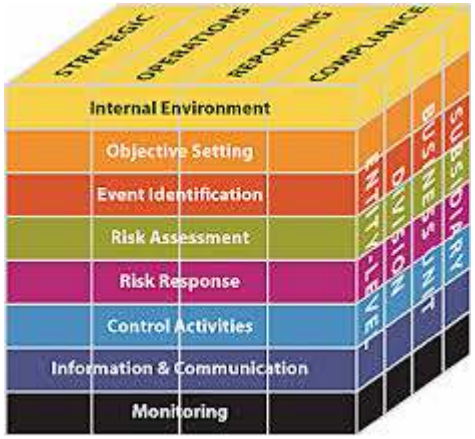
5. โปรดเลือกคำตอบที่ตรงกับ Risk Management and Oversight ของบริษัท (1 = เห็นด้วยน้อยที่สุด ถึง 4 = เห็นด้วยมากที่สุด)

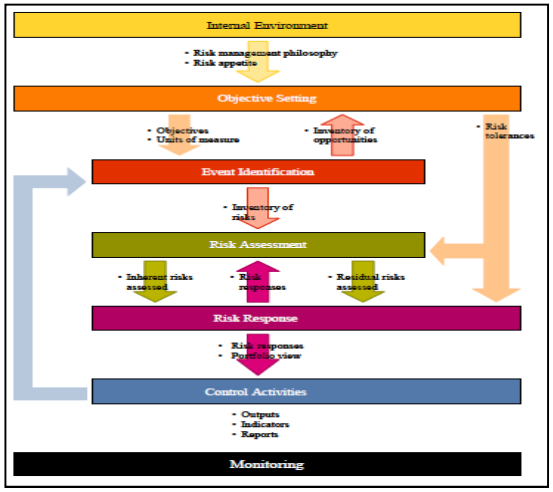
	1	2	3	4	Response Total	Response Average
1. กรรมการ ให้ ความสำคัญ แก่ การบริหารความเสี่ยง จริงจัง และ มี ความรู้เข้าใจ เกี่ยวกับ กระบวนการ ถ่องแท้	1% (2)	9% (18)	39% (77)	51% (101)	198	3.4
2. ผู้บริหารระดับสูง มี ความรู้ เข้าใจ เกี่ยวกับกระบวนการบริหาร ความเสี่ยง ถ่องแท้ และ บริหาร ความเสี่ยง จริงจัง	1% (2)	8% (16)	48% (95)	43% (84)	197	3.3
3. บริษัทมี ระบบและทรัพยากร เพียงพอเพื่อ สนับสนุน การบริหาร ความเสี่ยงให้ดำเนินการได้จริง	1% (2)	10% (21)	48% (95)	41% (82)	200	3.3
				Total Respondents		200

คำแนะนำ

ข้อ	ประเด็น	คำแนะนำ
1	More Pressing Needs to Execute Strategies and to Make sure the Firm Survives.	การบริหารจัดการและการบริหารความเสี่ยงเป็นเรื่องเดียวกัน Value Creation คือ Risk-Manage Value Creation
2	Lack of Understanding/Acceptance of ERM by Board Members	2.1 การทำหน้าที่ของคณะกรรมการสรรหา 2.2 การพัฒนาตนเองอย่างสม่ำเสมอของบุคคล
3	Lack of Perceived Value of ERM by Board Members and/or Management	ดู 2.1 และ 2.2
4	Infrastructure เพื่อรองรับ ERM	4.1 ต้องพัฒนา ใช้เวลา ต้องเชื่อมั่นและอดทน 4.2 Board Members (บางคน) อาจต้องเชี่ยวชาญมากถึงขนาดช่วย Guide ฝ่ายจัดการเพื่อผลักดันให้เกิดระบบและกระบวนการ 4.3 Infrastructure ขั้นต้น ก. Risk Charter และ Manual เพื่อ Communication ข. Strategies and Plans ที่สมบูรณ์ เพราะ Risk คือ Possible Deviations from Targets ค. กิจกรรมและปฏิทินกิจกรรม ง. KPIs, Targets and KRIs เพื่อ Monitoring

สรุป





- บริษัทสร้างมูลค่าโดย **Risk-Managed Value Creation**
- **Risk Management** โดย**ฝ่ายจัดการ** **vs. Risk Oversight** โดย **Board of Directors**
- **COSO เน้น 4 ข้อ**
  - เข้าใจ **Risk Philosophy and Appetite**
  - สอบทานและอนุมัติ **Portfolio Risks**
  - มั่นใจว่ามี **Established Effective Risk Management**
  - มีการจัดการความเสี่ยง **Risk Response** ที่เหมาะสม (รวม **Monitoring**)
- **เงื่อนไขบังคับก่อน**
  - **Board Members** ต้องมี**ความรู้ ความเข้าใจ ERM** และเชื่อมั่นว่าสร้างมูลค่าเพิ่มได้
  - **Management ต้องทำ ERM เป็น** และต้องไม่คิดว่าเป็นงานเพิ่ม แต่เป็นเรื่องเดียวกันกับ **Performance Management**
  - **Tone at the Top** สำคัญสำหรับการจัดให้มี **Infrastructure** และการนำไปปฏิบัติ