เอกสารประกอบการสัมมนาทางวิชาการ **(ไม่เสียค่าใช้จ่าย)**

โครงการสัมมนา เสริมความคิด ติดปีกวิชาชีพ กับคณะพาณิชย์ฯ ธรรมศาสตร์

โดยการสนับสนุนเงินทุนจาก มูลนิธิบุญชู โรจนเสถียร

บริษัท ดีลอยท์ ทู้ช โธมัทสุ ไชยยศ สอบบัญชี จำกัด

บริษัทสำนักงาน อี วาย จำกัด

บริษัท ไพร้ซวอเตอร์เฮาส์คูเปอร์ส เอบีเอเอส จำกัด และคณะฯ

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

วันที่ 6 ธันวาคม 2560

เวลา 09.00 – 12.15 น.

ณ ห้อง F-310 อาคารเอนกประสงค์ 2 ชั้น 3

มหาวิทยาลัยธรรมศาสตร์ ท่าพระจันทร์

วิทยากร :

ผู้ช่วยศาสตราจารย์ ดร.ศิลปพร ศรีจั่นเพชร

อาจารย์ประจำภาควิชาการบัญชี คณะพาณิชยศาสตร์และการบัญชี มธ.

ผู้สอบบัญชีรับอนุญาต

กรรมการมาตรฐานการสอบบัญชี อนุกรรมการกลั่นกรองมาตรฐานการบัญชี

สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์

What's New under COSO-ERM 2017 Framework?

Sillapaporn Srijunpetch, Ph.D, CPA

New COSO-ERM 2017

Today's organizations are concerned about:

- Risk Management
- Governance
- Control
- Assurance **(and** Consulting**)**

Please note Governance **has been dropped to ranking** number two.

- กรอบแนวคิดเดิม
- COSO ERM 2004

- COSO: The Committee of Sponsoring Organization of Treadway Commission

ERM Defined:

"… 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 risks to be within its risk appetite,

to provide reasonable assurance regarding the achievement of entity objectives."

Source: ***COSO Enterprise Risk Management – Integrated Framework. 2004, COSO.***

ความหมายของการบริหารความเสี่ยง

ความเสี่ยง คือ โอกาสที่ผลลัพธ์ที่เกิดขึ้นจริงแตกต่างไปจากผลลัพธ์ที่คาดการณ์ไว้ มีโอกาสเกิดได้ใน 2 ลักษณะ คือ

- **ผลกระทบในเชิงลบ (Negative Effect)** ทำให้องค์กรไม่บรรลุวัตถุประสงค์ และสร้างความเสียหายให้กับองค์กร หรือ **ความเสี่ยง** (Risk)
- **ผลกระทบในเชิงบวก (Positive Effect)** ทำให้มูลค่าขององค์กรมีระดับเพิ่มมากขึ้น การเกิดเป็นประโยชน์ต่อองค์กร ซึ่งเรียกว่า **โอกาส** (Opportunity)

Why ERM Is Important

[Exec Summary page 1]

Underlying principles:

- **Every entity, whether for-profit or not, exists to** realize value for its stakeholders**.**
- **Value is** created, preserved**, or** eroded **by management decisions in all activities,** from **setting strategy** to **operating the enterprise day-to-day.**

Why ERM Is Important

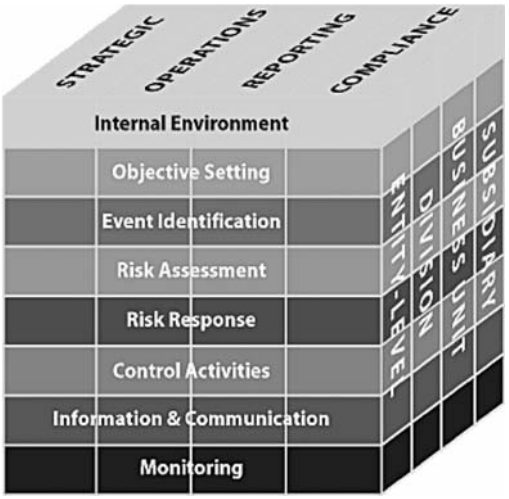
ERM supports value creation by enabling management to: [Exec Summary: page 1]

- Deal effectively **with potential future events that create uncertainty.**
- Respond **in a manner that** reduces **the likelihood of downside outcomes and** increases **the upside.**

ERM- Integrated Framework

This COSO ERM framework
- defines essential components,
- suggests a common language, and
- provides clear direction and guidance for enterprise risk management.

Enterprise Risk Management - Integrated Framework



มิติที่ 1: วัตถุประสงค์ขององค์กร

สร้างกลยุทธ์ที่เหมาะสม

ปฏิบัติงานได้อย่างมีประสิทธิผลและประสิทธิภาพ

มีรายงานที่ถูกต้องครบถ้วน

ปฏิบัติตามกฎหมาย กฎเกณฑ์และระเบียบต่างๆ

มิติที่ 2: องค์ประกอบของการบริหารความเสี่ยงเพื่อบรรลุวัตถุประสงค์

สภาพแวดล้อมภายใน

จัดตั้งวัตถุประสงค์ให้ชัดเจน

ระบุเหตุการณ์ที่อาจเกี่ยวข้องกับจุดประสงค์

ประเมินความเสี่ยงของเหตุการณ์

พิจารณาตอบสนองความเสี่ยง

สร้างหรือปรับปรุงกิจกรรมการควบคุม

สร้างหรือพัฒนาระบบข้อมูลและการสื่อสาร

ทบทวนและสอบทานเพื่อแก้ไขปรับปรุง

มิติที่ 3: ผู้รับผิดชอบ

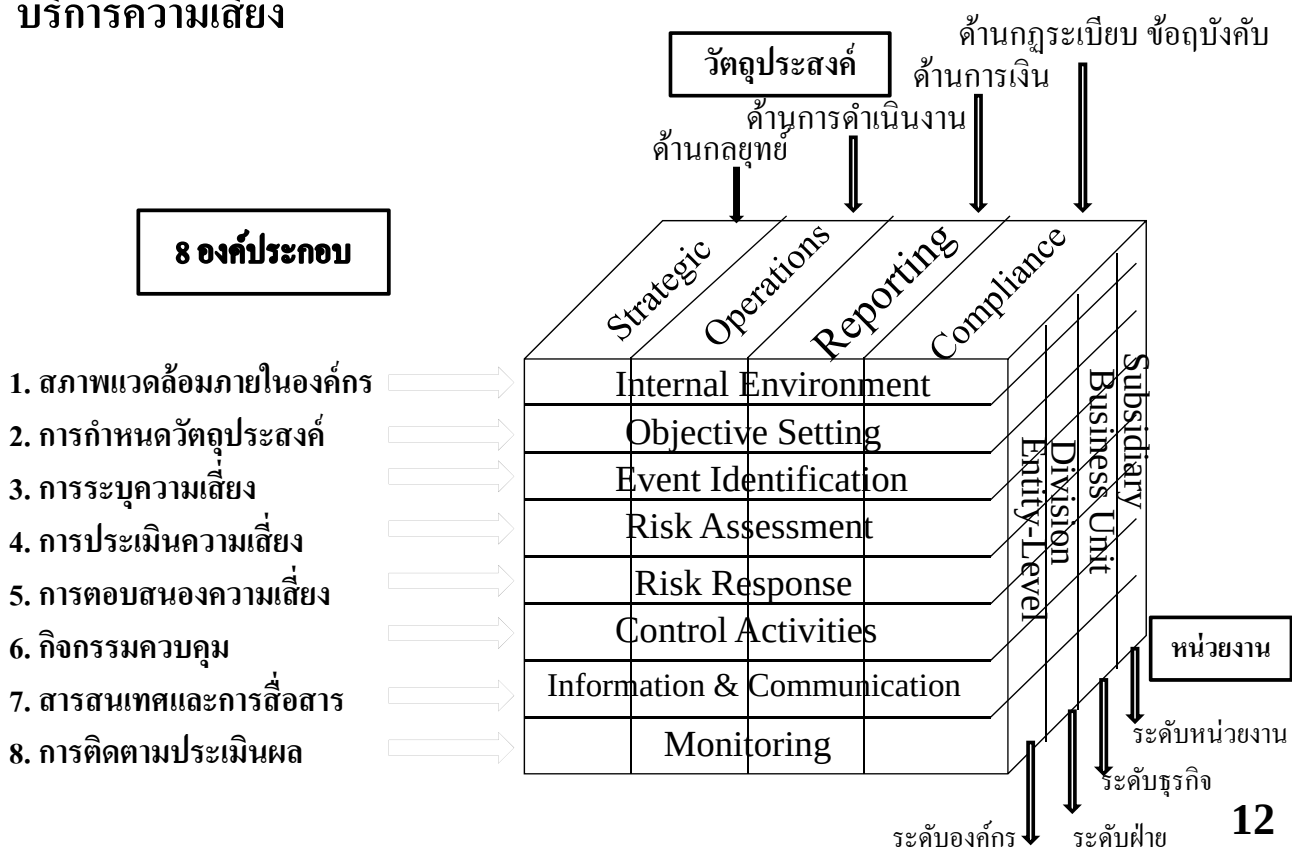
บริษัทย่อย

ส่วนงาน

สายงาน

บริษัทใหญ่

ความสัมพันธ์ระหว่างวัตถุประสงค์ ระดับหน่วยงานและองค์ประกอบของการบริการความเสี่ยง



Internal Environment

- **Establishes a** philosophy **regarding risk management. It recognizes that** unexpected **as well as** expected **events may occur.**

- **Establishes the entity's** risk culture**.**

- **Considers** all other aspects **of how the organization's actions may affect its risk culture.**

Objective Setting

- **Is applied when management considers** risks strategy **in the setting of objectives.**

- **Forms the** risk appetite **of the entity - a high-level view of** how much **risk management and the board** are willing to accept**.**

Event Identification

- Differentiates **risks** and **opportunities**.
- Events that may have a **negative impact** represent **risks**.
- Events that may have a **positive impact** represent natural offsets (**opportunities**), which management channels back to strategy setting.

Event Identification

- Involves **identifying those incidents**, occurring internally or externally, that could **affect strategy** and **achievement of objectives**.
- Addresses how internal and external factors **combine** and **interact** to influence the risk profile.

Risk Assessment

- Allows an entity to **understand** the extent to which potential events might **impact objectives**.
- Assesses risks from **two** perspectives:
  - Likelihood
  - Impact

Risk Assessment

- Employs a combination of both **qualitative** and **quantitative** risk assessment methodologies.

Risk Response

- **Identifies** and **evaluates** possible responses to risk.
- Evaluates **options** in relation to entity's risk appetite, cost vs. benefit of potential risk responses, and degree to which a response will reduce impact and/or likelihood.

Control Activities

- **Policies** and **procedures** that help ensure that the risk responses, as well as other entity directives, are carried out.
- Occur **throughout** the organization, at **all levels** and in **all functions**.
- Include **application** and **general** information technology **controls**.

Information & Communication

- **Management** identifies, captures, **and** communicates **pertinent information in a** form **and** timeframe **that enables people to carry out their responsibilities.**

- **Communication occurs in a** broader **sense, flowing** down, across, **and** up **the organization.**

Monitoring

Effectiveness of the other ERM components is monitored through:

- **Ongoing monitoring activities.**
- **Separate evaluations.**
- **A combination of the two.**

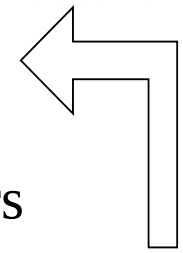
Internal Control

A strong system of internal control is essential to effective enterprise risk management.

This ERM Framework does not replace **the earlier Framework on Internal control, but** encompasses **it.**

ERM Roles & Responsibilities

- Management
- The board of directors
- Risk officers
- Internal auditors



There is now a CRO **Chief Risk Officer, in addition to CEO, COO, CFO & CIO.**

Example: Risk Model

Environmental Risks

- Capital Availability
- Regulatory, Political, and Legal
- Financial Markets and Shareholder Relations

Process Risks

- Operations Risk
- Empowerment Risk
- Information Processing / Technology Risk
- Integrity Risk
- Financial Risk

Information for Decision Making

- Operational Risk
- Financial Risk
- Strategic Risk

DETERMINE RISK APPETITE

Key questions:

- **What risks will the organization** not accept**?**
  (e.g. environmental or quality compromises)
- **What risks will the organization** take **on new initiatives?**
  (e.g. new product lines)
- **What risks will the organization** accept **for competing objectives?**
  (e.g. gross profit vs. market share?)

IDENTIFY RISK RESPONSES

- Quantification **of risk exposure**
- Options **available:**

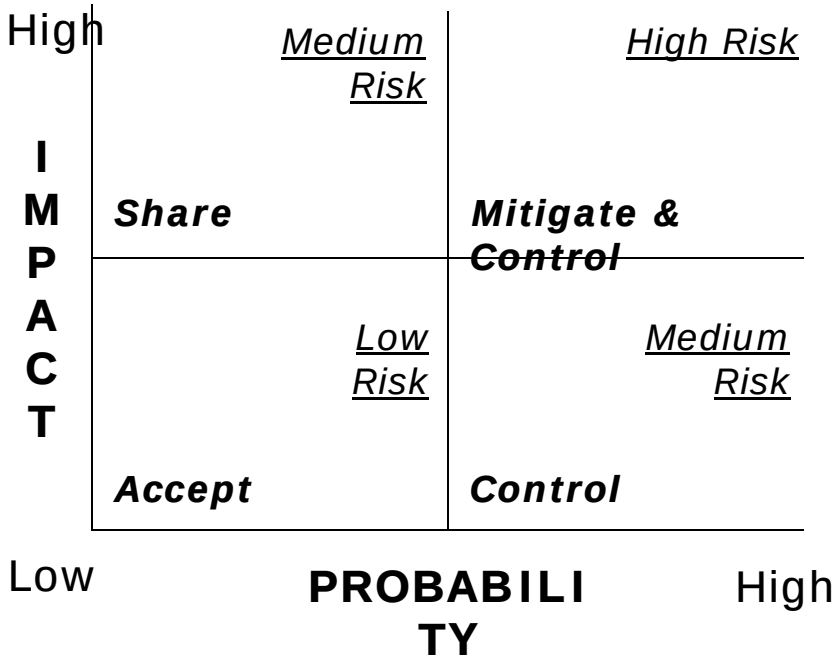
  - Accept = monitor

  - Avoid = eliminate ***(get out of situation)***

  - Reduce = institute controls

  - Share = partner with someone ***(e.g. insurance)***

Impact vs. Probability



COSO ERM 2017

- Enterprise Risk Management Integrating with Strategy and Performance

New COSO-ERM 2017

Questions

- Why update the 2004 ERM-Integrated Framework?
- Enterprise Risk Management – Integrating with Strategy and Performance
- Update Approach

What are key changes?

- Adopt a structure of components and principles
- Simplify the definition of ERM

Key Changes

- Is the adoption of the Framework mandatory?

- How does the Updated Framework relate to COSO's 2013 Internal Control-Integrated Framework?

Key changes

- Emphasizes the relationship between risk and value

- Focus on the integration of ERM

Key Changes

- Examine the role of culture

- Elevate discussion of strategy

Key Changes

- Enhance the alignment between performance and ERM

- ERM and Internal Control

ERM 2004

1. Internal Environment
2. Objective Setting
3. Event Identification
4. Risk Assessment
5. Risk Response
6. Control Activities
7. Information and
8. Communication
   Monitoring

ERM 2017

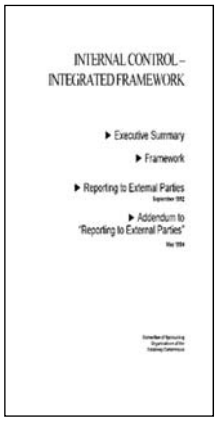
1. Governance and Culture
2. Strategy & Objective-Setting
3. Performance
4. Review & Revision
5. Information, Communication & Reporting

- COSO ERM 2017 แตกต่างจาก COSO Internal Control Framework 2013 อย่างไร

COSO 2013

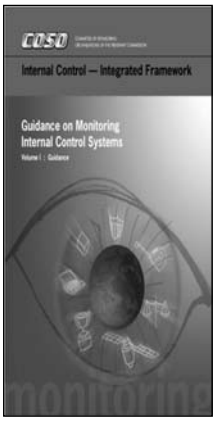
กรอบโครงสร้างการควบคุมภายใน

COSO Overview – Internal control publications



1992

2006



2009

2013

Internal Control - Integrated Framework

มิติที่1: วัตถุประสงค์ขององค์กร

ปฏิบัติงานได้อย่างมีประสิทธิภาพและประสิทธิผล

มีรายงานที่ถูกต้องครบถ้วน

ปฏิบัติตามกฎหมาย กฎเกณฑ์และระเบียบต่างๆ

มิติที่2: องค์ประกอบของการควบคุมเพื่อบรรลุวัตถุประสงค์

สภาพแวดล้อมในการควบคุม

ประเมินความเสี่ยงที่จะทำให้การควบคุมไม่บรรลุจุดประสงค์

สร้างหรือปรับปรุงกิจกรรมการควบคุม

สร้างหรือพัฒนาระบบข้อมูลและการสื่อสาร

ทบทวนและสอบทานองค์ประกอบเพื่อการแก้ไขปรับปรุง

มิติที่3: บุคลากรผู้รับผิดชอบ

หน่วยงาน

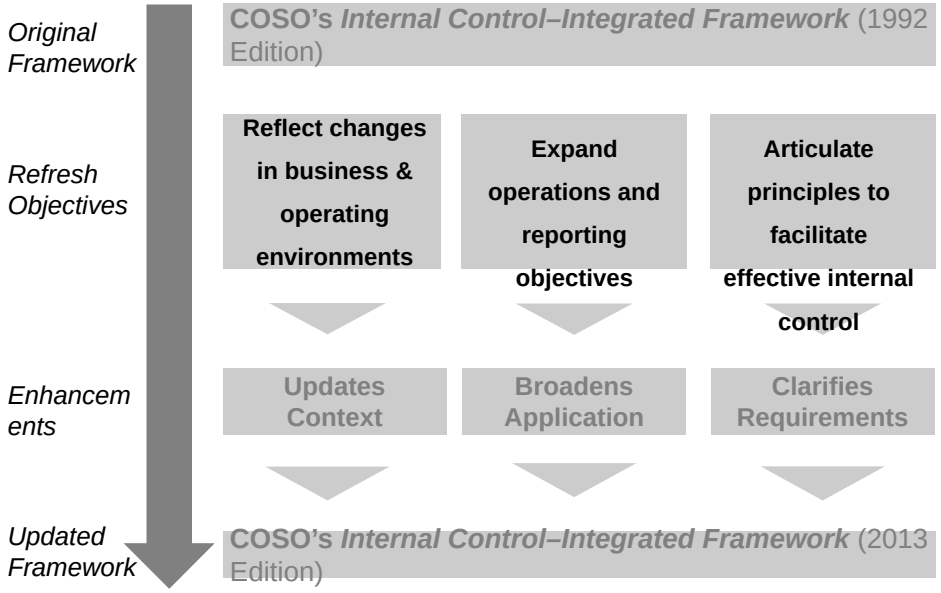
ฝ่าย

ส่วนงาน

บริษัท

* COSO: The Committee of Sponsoring Organization of Treadway Commission

Why update what works – The Framework has become the most widely adopted control framework worldwide.



Update articulates principles of effective internal control

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
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

องค์ประกอบของควบคุมภายใน

1. การควบคุมภายในองค์กร (Control Environment
2. การประเมินความเสี่ยง (Risk Ass
3. กิจกรรมการควบคุม (Control Activites)
4. ระบบสารสนเทศและการสื่อสารข้อมูล (Information & Communication)
5. ระบบการติดตาม (Monitoring Activities)

หลักการที่อยู่ภายใต้การควบคุมภายในองค์กร

1. องค์กรแสดงถึงความยึดมั่นในคุณค่าของความซื่อตรงและจริยธรรม
2. คณะกรรมการมีความเป็นอิสระจากฝ่ายบริหารและทำหน้าที่กำกับดูแลและพัฒนาการดำเนินการด้านการควบคุมภายใน

3. ฝ่ายบริหารได้จัดให้มีโครงสร้างสายการรายงาน การกำหนดอำนาจในการสั่งการและความรับผิดชอบที่เหมาะสมเพื่อให้องค์กรบรรลุวัตถุประสงค์ภายใต้การกำกับดูแลของคณะกรรมการ

4. องค์กรแสดงถึงความมุ่งมั่นในการจูงใจ พัฒนาและรักษาบุคคลากรที่มีความรู้ความสามารถ
5. องค์กรกำหนดให้บุคคลากรมีหน้าที่และความรับผิดชอบในการควบคุมภายในเพื่อให้บรรลุวัตถุประสงค์ขององค์กร

หลักการที่อยู่ภายใต้การประเมินความเสี่ยง

6. องค์กรกำหนดวัตถุประสงค์ไว้อย่างชัดเจนเพียงพอ เพื่อให้สามารถระบุและประเมินความเสี่ยงต่างๆที่เกี่ยวข้องกับวัตถุประสงค์ขององค์กร

7. องค์กรระบุและวิเคราะห์ความเสี่ยงทุกประเภทที่อาจกระทบต่อการบรรลุวัตถุประสงค์ไว้อย่างครอบคลุมทั่วทั้งองค์กร

8. องค์กรได้พิจารณาถึงโอกาสที่จะเกิดการทุจริต ในการประเมินความเสี่ยงที่จะบรรลุวัตถุประสงค์ขององค์กร

9. องค์กรสามารถระบุและประเมินความเปลี่ยนแปลงที่อาจมีผลกระทบต่อระบบการควบคุมภายใน

หลักการที่อยู่ภายใต้การควบคุมการปฏิบัติงาน

10. องค์กรมีมาตรการควบคุมที่ช่วยลดความเสี่ยงที่จะไม่บรรลุวัตถุประสงค์ขององค์กร ให้อยู่ในระดับที่ยอมรับได้

11. องค์กรเลือกและพัฒนากิจกรรมการควบคุมทั่วไปด้วยระบบเทคโนโลยี เพื่อช่วยสนับสนุน การบรรลุวัตถุประสงค์

12. องค์กรจัดให้มีกิจกรรมการควบคุมผ่านทางนโยบาย ซึ่งได้กำหนดสิ่งที่คาดหวังและขั้นตอน การปฏิบัติ เพื่อให้นโยบายที่กำหนดไว้นั้นสามารถนำไปสู่การปฏิบัติได้

หลักการที่อยู่ภายใต้ระบบสารสนเทศและการสื่อสารข้อมูล

13. องค์กรมีข้อมูลที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้การควบคุมภายในสามารถดำเนินไปได้ตามที่กำหนดไว้

14. องค์กรสื่อสารข้อมูลภายในองค์กร ซึ่งรวมถึงวัตถุประสงค์และความรับผิดชอบต่อการควบคุมภายในที่จำเป็นต่อการสนับสนุนให้การควบคุมภายในสามารถดำเนินไปได้ตามที่วางไว้

15. องค์กรได้สื่อสารกับหน่วยงานภายนอก เกี่ยวกับประเด็นที่อาจมีผลกระทบต่อการควบคุมภายใน

Points of Focus

- Principle 1: The organization demonstrates a commitment to integrity and ethical values.

- ***Point of focus***
- Sets the tone at the Top
- Establishes Standards of Conduct
- Evaluates Adherence to Standards of Conduct
- Addresses Deviations in a Timely Manner

หนังสือการควบคุมภายใน SET

บทที่ 1 แนวคิดทั่วไปของการควบคุมภายใน

บทที่ 2 สภาพแวดล้อมของการควบคุม

บทที่ 3 การประเมินความเสี่ยง

บทที่ 4 กิจกรรมการควบคุม

บทที่ 5 ข้อมูลสารสนเทศและการสื่อสาร

บทที่ 6 กิจกรรมควบคุมด้านสารสนเทศ

บทที่ 7 การติดตามประเมินผลการควบคุมภายใน

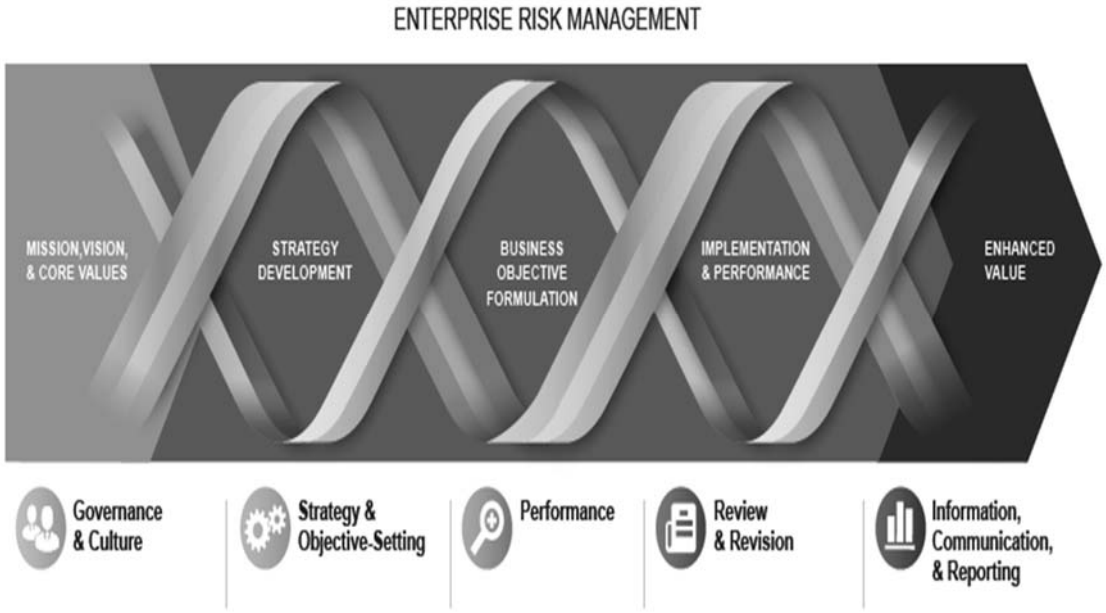
บทที่ 8 การทุจริต

COSO ERM 2017

- **Enterprise Risk Management** Integrating with Strategy and Performance

New COSO-ERM 2017

A Focus Framework



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

Strategy and Objective Setting

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

- วิเคราะห์โครงสร้างของธุรกิจ
- กำหนดความต้องการที่จะเสี่ยง
- ประเมินกลยุทธ์ในรูปแบบต่างๆ
- กำหนดวัตถุประสงค์ทางธุรกิจ

Performance

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

- ระบุความเสี่ยง
- ประเมินความรุนแรงของความเสี่ยง
- จัดลำดับความเสี่ยง
- ดำเนินการตอบสนองความเสี่ยง
- พัฒนาภาพรวมความเสี่ยงขององค์กร

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

- ประเมินการเปลี่ยนแปลงที่มีสาระสำคัญ
- สอบทานความเสี่ยงและผลการจัดการ
- หาทางปรับปรุงการบริหารความเสี่ยงขององค์กร

Information, Communication & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

- ผลักดันในเรื่องข้อมูลและเทคโนโลยี
- สื่อสารข้อมูลความเสี่ยง
- รายงานความเสี่ยง วัฒนธรรมและผลประกอบการ