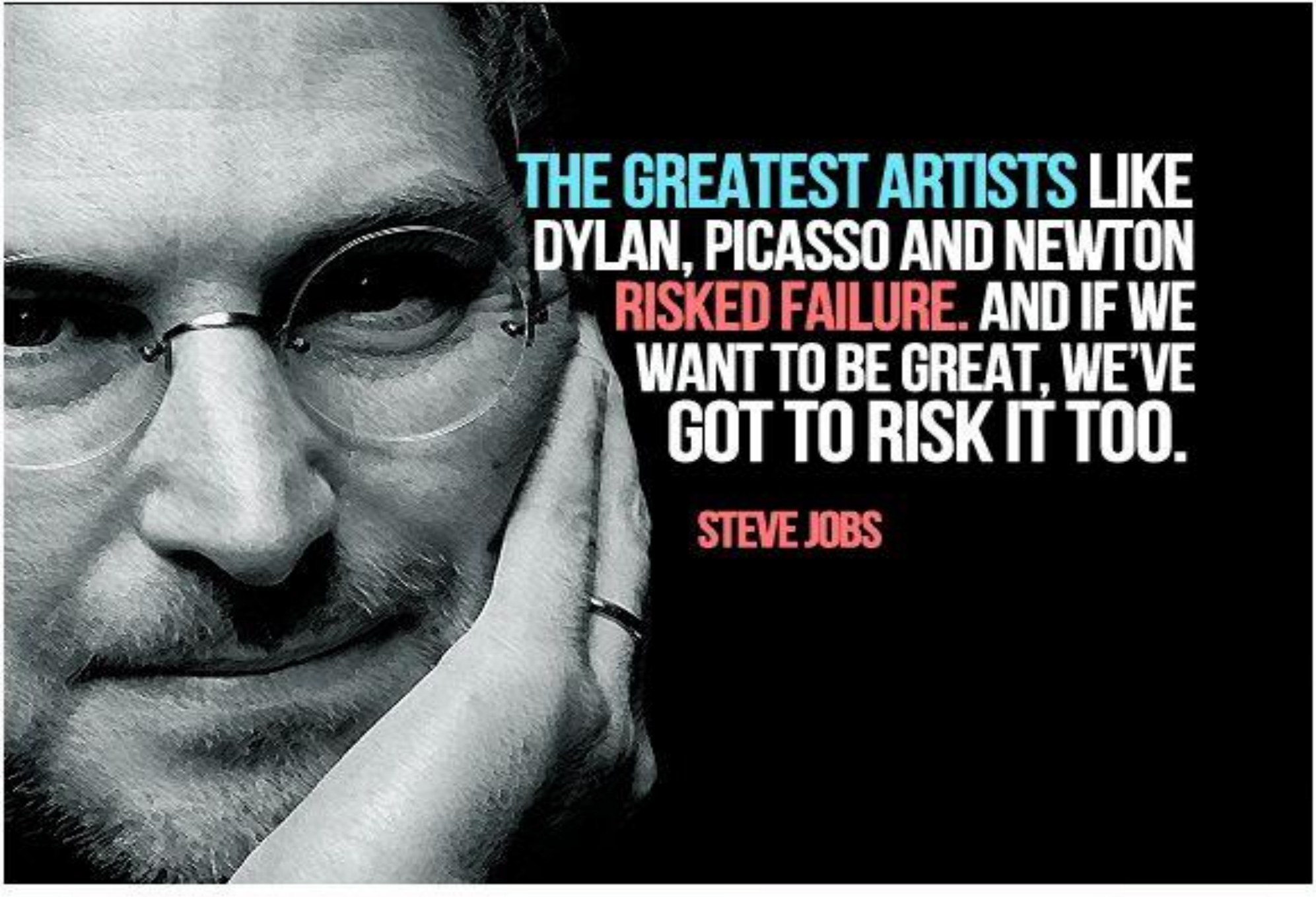
25th ANNIVERSARY
COLLEGE OF MUSIC
MAHIDOL UNIVERSITY
1994-2019

Risk Management Concept

Risk Management Concept in Music Business

You got to take risk!



Risk Management Concept – The Beginning

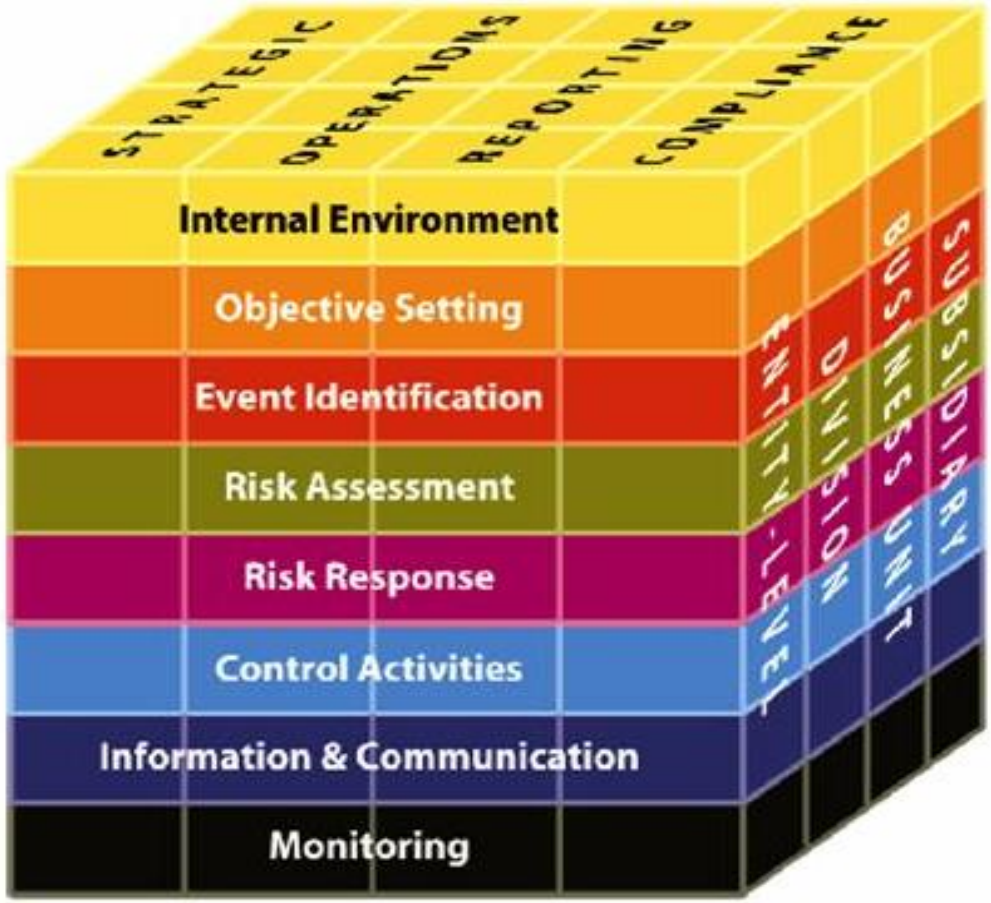
การจัดการความเสี่ยงจริงๆมีมานานแล้ว แต่ได้เริ่มมีมาตรฐานกันอย่างจริงจังเมื่อประมาณปี ค.ศ. 2004 หลังจากเกิดเหตุการณ์การโกงทางการเงินขึ้น จึงทำให้องค์กรที่เกี่ยวข้องกับการกำกับดูแลทางด้านมาตรฐานทางการเงินและบัญชีได้ร่วมกันจ้างบริษัทที่ปรึกษาเข้ามาจัดทำมาตรฐานการควบคุมภายในและมาตรฐานการจัดการความเสี่ยง เพื่อใช้เป็นมาตรฐานให้องค์กรชั้นนำได้นำไปปรับใช้ อันจะนำไปสู่การพัฒนาองค์กรได้อย่างยั่งยืนต่อไป โดยเรียกมาตรฐานการจัดการความเสี่ยง COSO ERM – Enterprise Risk Management Integrated Framework (COSO ERM 2007)

COSO หรือ The Committee of Sponsoring Organization of the Treadway Commission ได้จัดตั้งขึ้นมาในปี ค.ศ. 1985 ในประเทศสหรัฐอเมริกา เพื่อจัดทำมาตรฐานด้านการควบคุมภายใน (Internal Control – Integrated Framework) ซึ่งในเวลาต่อมาได้มีการผสมผสานแนวคิดเรื่องการจัดการความเสี่ยงเข้าไป จนทำให้พัฒนาขึ้นมาเป็นแนวคิดที่เรียกว่า Enterprise Risk Management – Integrated Framework โดยมีกระบวนการจัดการความเสี่ยงตามแนวทางของ COSO ที่เรียกว่า COSO ERM 2004

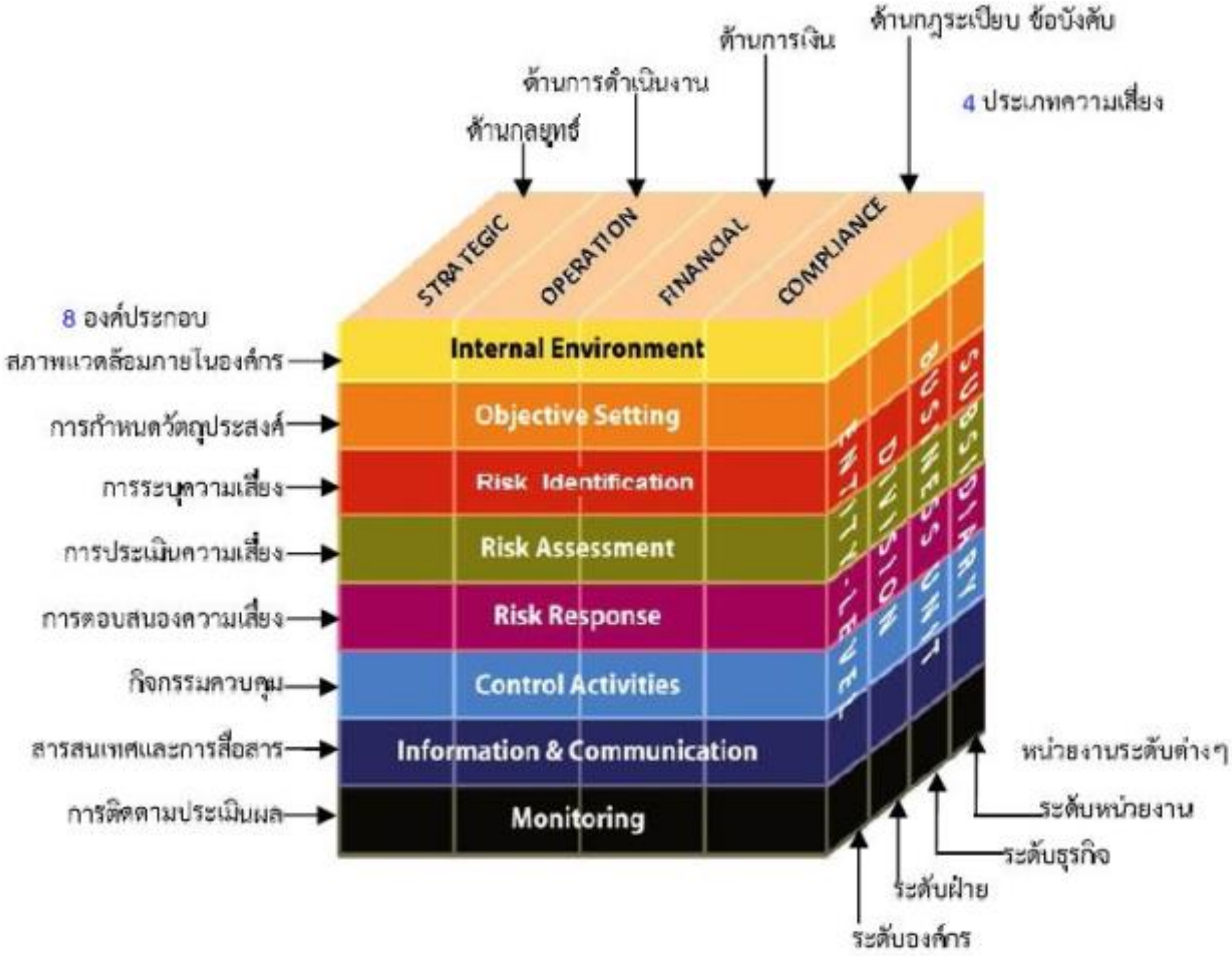
Relationship between COSO 1 and COSO 2

ERM is fully aligned with the COSO Internal Control- Integrated Framework

COSO 1 "Internal Control – Integrated Framework"



COSO 2 "Enterprise Risk Management – Integrated Framework"


ด้านกฎระเบียบ ข้อบังคับ
ด้านการเงิน
ด้านการดำเนินงาน
ด้านกลยุทธ์
4 ประเภทความเสี่ยง
STRATEGIC
OPERATION
FINANCIAL
COMPLIANCE
8 องค์ประกอบ
สภาพแวดล้อมภายในองค์กร
การกำหนดวัตถุประสงค์
การระบุความเสี่ยง
การประเมินความเสี่ยง
การตอบสนองความเสี่ยง
กิจกรรมควบคุม
สารสนเทศและการสื่อสาร
การติดตามประเมินผล
Internal Environment
Objective Setting
Risk Identification
Risk Assessment
Risk Response
Control Activities
Information & Communication
Monitoring
หน่วยงานระดับต่างๆ
ระดับหน่วยงาน
ระดับธุรกิจ
ระดับฝ่าย
ระดับองค์กร

COSO ERM 2004 – Integrated Framework

การพัฒนาสภาพแวดล้อมภายในขององค์กรให้เอื้อ

การกำหนดวัตถุประสงค์ของการบริหารความเสี่ยง

การระบุถึงความเสี่ยงต่อเป้าหมายขององค์กร

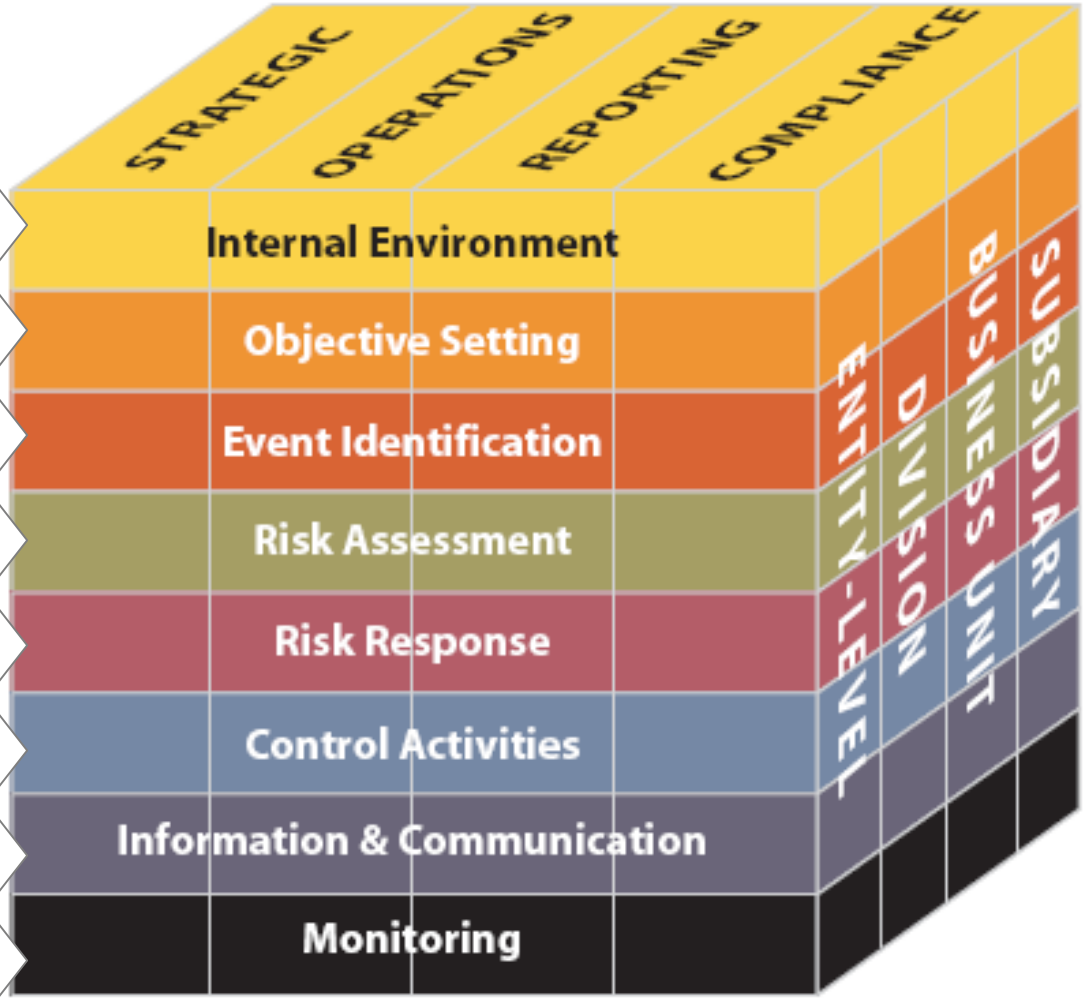
การวิเคราะห์ความเสี่ยง (โอกาส / ผลกระทบ)

การกำหนดแนวทางในการจัดการความเสี่ยง

การกำหนดกิจกรรมควบคุมความเสี่ยง

การจัดการสารสนเทศและการสื่อสาร

การติดตามร่องรอยความเสี่ยง



การจัดการความเสี่ยงทั้ง 8 ขั้นตอนนี้เป็นกระบวนการที่สามารถประยุกต์ใช้ได้ทุกระดับขององค์กร ซึ่งถ้าองค์กรได้ดำเนินการตาม 8 ขั้นตอนนี้อย่างละเอียดรอบคอบก็สามารถที่จะป้องกันผลกระทบเชิงลบที่อาจจะเกิดขึ้นจากความเสี่ยงได้ รวมทั้งองค์กรยังสามารถมั่นใจได้ว่าการจัดการความเสี่ยงนั้นอยู่ในวิสัยที่สามารถควบคุมได้ด้วยความมั่นใจ

“ความเสี่ยง” หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด ทั้งนี้ COSO ได้กำหนดความเสี่ยงไว้ 4 ประเภท

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)
2. ความเสี่ยงด้านการดำเนินงาน (Operational Risk)
3. ความเสี่ยงด้านการเงิน (Financial Risk)
4. ความเสี่ยงด้านกฎหมาย (Legal Risk)

แต่ก็มีความเสี่ยงที่อยู่นอกเหนือจาก 4 ประเภทแรกด้วย เช่น ความเสี่ยงด้านภัยพิบัติ ความเสี่ยงด้านเทคโนโลยี เป็นต้น

การแบ่งประเภทความเสี่ยง ได้จัดแบ่งตามแนวทางที่กระทรวงการคลังกำหนดไว้ โดย
จัดแบ่งเป็น 4 ประเภทดังนี้

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk : S) หมายถึง ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์และการปฏิบัติตามแผนกลยุทธ์อย่างไม่เหมาะสม รวมถึงความไม่สอดคล้องกันระหว่างนโยบาย, เป้าหมายกลยุทธ์, โครงสร้างองค์กร, ภาวการณ์แข่งขัน, ทรัพยากรและสภาพแวดล้อม อันส่งผลกระทบต่อวัตถุประสงค์หรือเป้าหมายองค์กร

2. ความเสี่ยงด้านการดำเนินงาน (Operational Risk : O) หมายถึง ความเสี่ยงที่เกิดจากการปฏิบัติงานทุกๆ ขั้นตอน อันเนื่องมาจากขาดการกำกับดูแลที่ดีหรือขาดการควบคุมภายในที่ดี โดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ / อุปกรณ์ / เทคโนโลยีสารสนเทศ / บุคลากรในการปฏิบัติงานและความปลอดภัยของทรัพย์สิน

3. ความเสี่ยงด้านการเงิน (Financial Risk) หมายถึง ความเสี่ยงเกี่ยวกับสภาพคล่องทางการเงิน ความสามารถในการทำกำไรและ การรายงานทางการเงิน

4. ความเสี่ยงด้านกฎระเบียบต่างๆ (Compliance Risk : C) หมายถึง ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับ

ในปีค.ศ. 2017 COSO ได้ออกแนวทางการจัดการความเสี่ยงตัวใหม่ออกมา เรียกว่า COSO Enterprise Risk Management – Integrating with Strategy and Performance 2017 (หรือ COSO 2017) ซึ่งเป็นการบูรณาการการจัดการความเสี่ยงเข้ากับกลยุทธ์ขององค์กร (Organization Strategy) และเชื่อมโยงไปถึงการประเมินผลการดำเนินงาน (Organization Performance) ด้วย

กรอบแนวคิดการจัดการความเสี่ยง COSO ERM 2017

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

Review & Revision

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

Information, Communication, & Reporting

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

COSO 2017 ประกอบด้วย 5 องค์ประกอบหลัก (Component) และ 20 หลักการ (Principle)

การประยุกต์ใช้หลักการจัดการความเสี่ยงทั่วทั้งองค์กรตามแนวทางของ COSO 2017 นี้คาดว่าจะช่วยให้องค์กรได้ประโยชน์ดังต่อไปนี้

1. เพิ่มโอกาสทางธุรกิจ
2. ลดผลกระทบเชิงลบที่อาจจะเกิดขึ้น และในขณะเดียวกันก็เพิ่มผลกระทบเชิงบวก
3. ทำให้เกิดความมั่นใจว่าได้มีการจัดการความเสี่ยงโดยรวมไม่ใช่เน้นความเสี่ยงเพียงด้านใดด้านหนึ่ง
4. ลดความผันผวนของการดำเนินงาน
5. ทำให้การจัดสรรทรัพยากรได้อย่างเหมาะสมตามลำดับความสำคัญมากขึ้น

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

องค์ประกอบแรกของ COSO 2017 ได้ระบุแนวทางไว้ว่าคณะกรรมการขององค์กรจะต้องมีส่วนร่วมอย่างใกล้ชิดในการกำกับดูแลองค์กรที่ดีและจะต้องควบคุมให้เกิดการจัดการความเสี่ยงด้วย นอกจากนั้นจะต้องมีการจัดโครงสร้างองค์กรให้รองรับการการจัดการความเสี่ยง รวมทั้งควรจะต้องมีการกำหนดวัฒนธรรมอันพึงประสงค์ควบคู่ไปกับการแสดงให้เห็นถึงความมุ่งมั่นในคุณค่าหลักขององค์กร และยังต้องดึงดูด พัฒนา และเพิ่มศักยภาพให้แก่บุคลากรที่มีความสามารถให้คงอยู่ในองค์กรให้ได้

Strategy & Objective-Setting

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

องค์ประกอบที่สองของ COSO 2017 ได้ระบุแนวทางไว้ว่าจะต้องมีการวิเคราะห์บริบทของธุรกิจอย่างเหมาะสม โดยพิจารณาถึงบทบาทของผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร จุดสำคัญคือผู้บริหารจะต้องพิจารณาความเสี่ยงจากการเปลี่ยนแปลงในบริบทของธุรกิจ และกำหนดความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อที่จะประเมินทางเลือกเชิงกลยุทธ์ของธุรกิจ อันจะนำไปสู่การกำหนดวัตถุประสงค์ของธุรกิจที่เหมาะสมต่อไป

Performance

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

องค์ประกอบที่สามของ COSO 2017 ได้ระบุแนวทางไว้ว่า องค์กรจะต้องมีการระบุความเสี่ยงที่อาจจะเกิดขึ้นมาจากการเปลี่ยนแปลงในบริบทของธุรกิจ (Change in Business Context) และจะต้องมีการประเมินความรุนแรงของความเสี่ยง เพื่อนำมาจัดอับดับความสำคัญของความเสี่ยง แล้วจะเข้าสู่กระบวนการตอบสนองความเสี่ยงที่ประเมินแล้ว (Risk response – Accept, Avoid, Exploit, Reduce และ Share risks) หลังจากนั้นจึงเป็นการจัดทำเป็นภาพรวมความเสี่ยงองค์กร

จากกรอบแนวคิดเรื่องการจัดการความเสี่ยงทั่วทั้งองค์กร องค์ประกอบที่สำคัญมากๆ คือองค์ประกอบด้าน Performance ซึ่งมีขั้นตอนหลักๆของการจัดการความเสี่ยงอยู่ 3 ขั้นตอน ประกอบด้วย

1. การระบุความเสี่ยง
2. การประเมินและจัดลำดับความเสี่ยง
3. การตอบสนองอย่างเสี่ยง

ในการระบุความเสี่ยงนั้นจะต้องร่วมกันระบุความเสี่ยงที่จะส่งผลต่อยุทธศาสตร์ขององค์กร ซึ่งเป็นความเสี่ยงที่อาจจะทำให้ไม่สามารถบรรลุตามภารกิจและเป้าหมายที่ตั้งไว้ องค์กรจะต้องทำความเข้าใจและระบุให้ได้ถึงปัจจัยที่เป็นสาเหตุของความเสี่ยง และองค์กรจะต้องวิเคราะห์ถึงโอกาสและผลกระทบของความเสี่ยงที่มีต่อองค์กร เพื่อองค์กรจะได้กำหนดวิธีการจัดการความเสี่ยงโดยจะต้องคำนึงถึงความเหมาะสมและความคุ้มค่าด้วยจึงจะสามารถจัดการความเสี่ยงได้อย่างเหมาะสมต่อไป

เมื่อวิเคราะห์โอกาสและผลกระทบของความเสี่ยงอย่างรอบคอบแล้ว หน่วยรับตรวจต้องพิจารณาถึงระดับของความเสี่ยงว่ามีความเสี่ยงสูงหรือต่ำโดยพิจารณาจากแผนภูมิความเสี่ยง (Risk Map)

ผลกระทบ

5					
4				สูง	มาก
3			สูง		
2		ปาน	กลาง		
1	ต่ำ				
	1	2	3	4	5

โอกาสที่จะเกิด

Review & Revision

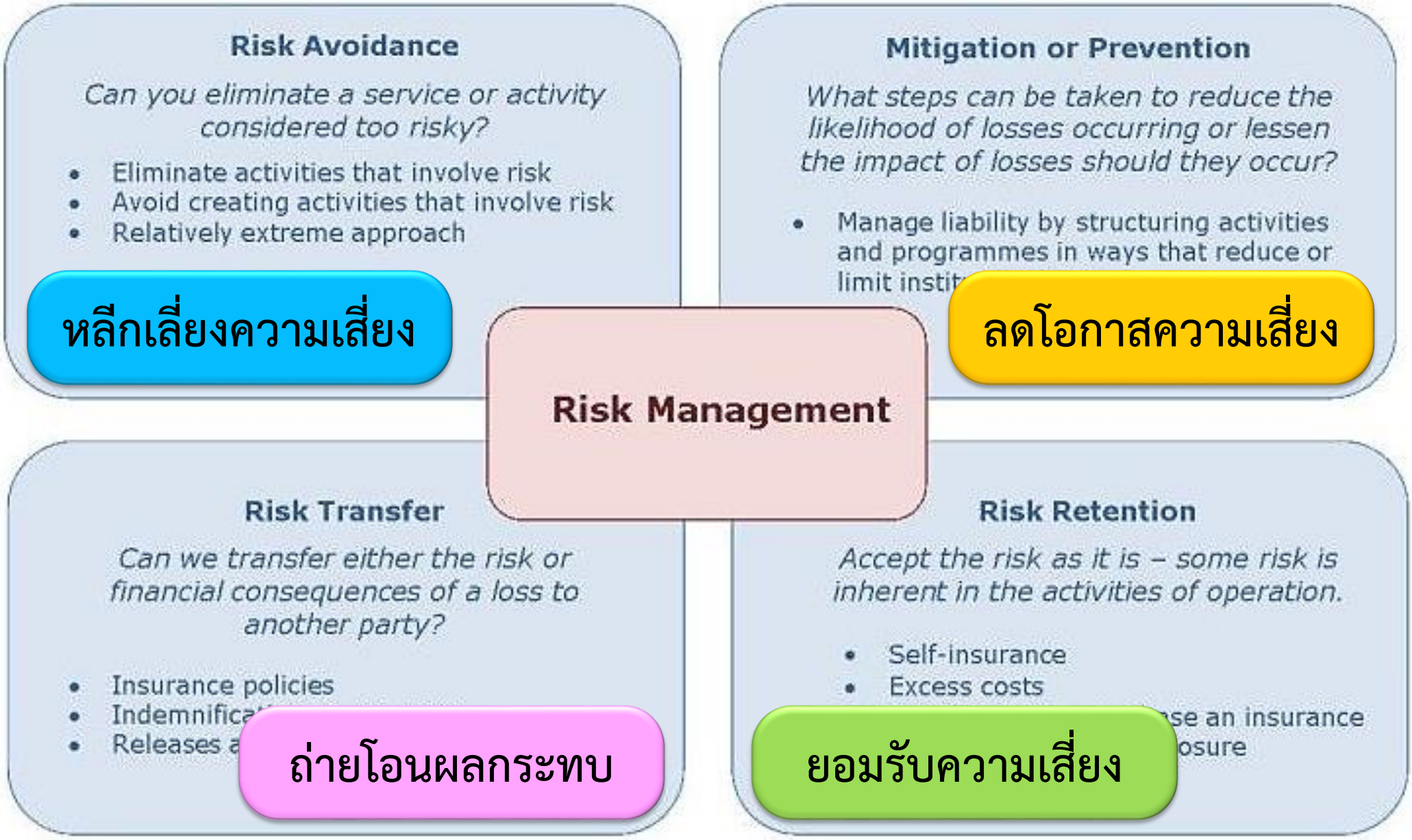
15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

องค์ประกอบที่สี่ของ COSO 2017 ได้ระบุแนวทางไว้ว่า องค์กรควรจะมีการประเมินการเปลี่ยนแปลงที่เป็นสาระสำคัญ และจัดให้มีการทบทวนความเสี่ยงและผลการดำเนินการตอบสนองความเสี่ยงว่าเป็นไปตามความตั้งใจหรือไม่ ซึ่งจะนำไปสู่การปรับปรุงการจัดการความเสี่ยงทั่วทั้งองค์กรอย่างต่อเนื่องต่อไป

Information, Communication, & Reporting

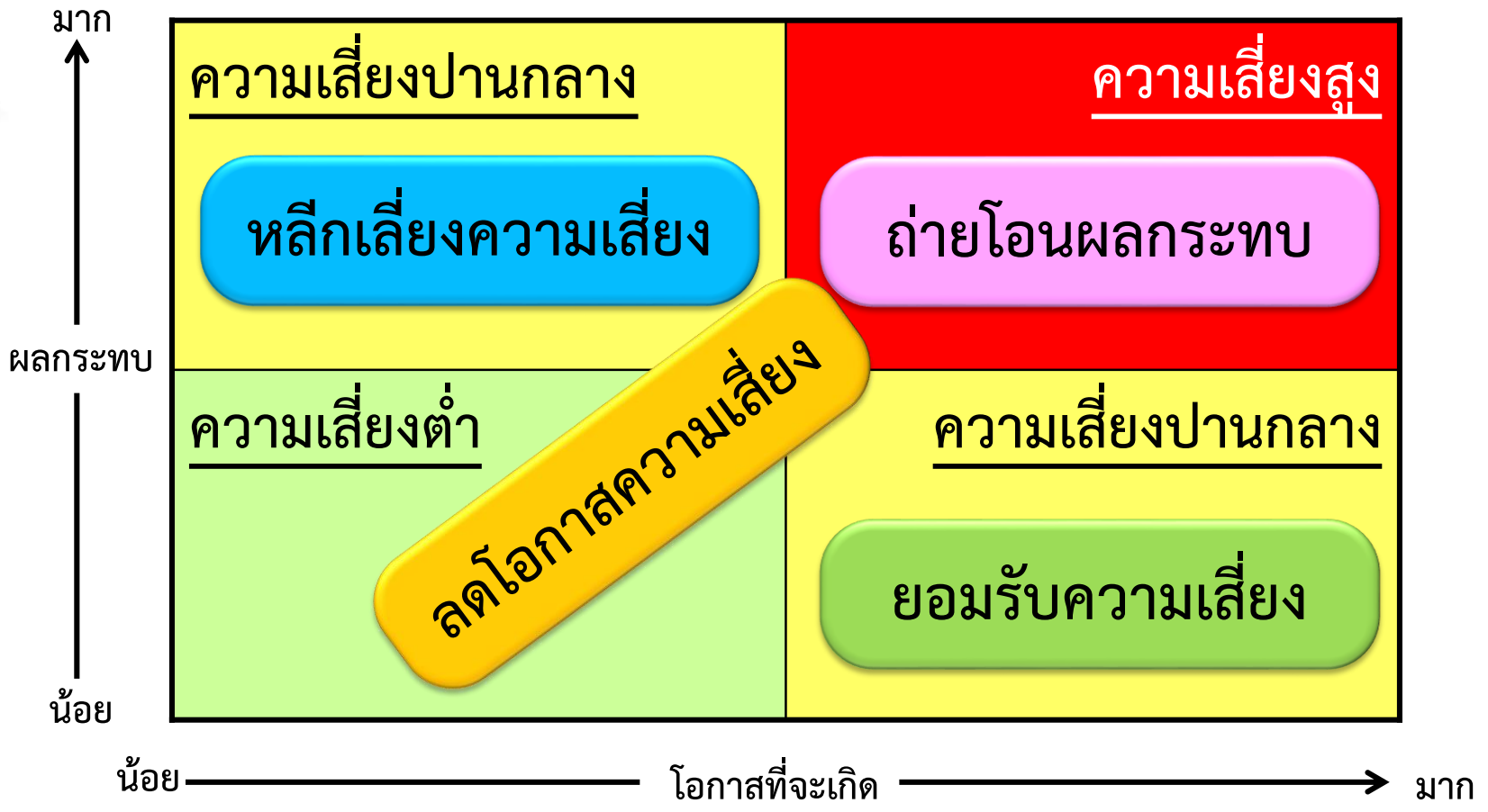
18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

องค์ประกอบที่ห้าของ COSO 2017 ได้ระบุแนวทางไว้ว่าองค์กรควรพิจารณาการนำเอาสารสนเทศและเทคโนโลยีสารสนเทศ มาสนับสนุนการจัดการความเสี่ยงทั่วทั้งองค์กร ตลอดจนต้องมีการสื่อสารเรื่องราวของความเสี่ยงให้บุคลากรในองค์กรทุกระดับและผู้มีส่วนได้ส่วนเสียได้รับทราบอย่างทั่วถึง และท้ายสุดองค์กรจะต้องมีการจัดทำรายงานเกี่ยวกับความเสี่ยง วัฒนธรรม และผลการดำเนินงาน



เนื่องจากความเสี่ยงมีหลากหลายรูปแบบและแต่ละองค์กรก็มีความเสี่ยงที่ยอมรับได้ไม่เหมือนกัน ดังนั้น กลยุทธ์การจัดการความเสี่ยงจึงมีหลายลักษณะให้องค์กรได้เลือกใช้อย่างเหมาะสม

กลยุทธ์ในการจัดการความเสี่ยง



การเลือกกลยุทธ์การจัดการความเสี่ยงอาจจะพิจารณาจากระดับของความเสี่ยงด้วย ซึ่งถ้าความเสี่ยงสูงอาจจะใช้กลยุทธ์การถ่ายโอนความเสี่ยงเพื่อที่จะไม่ต้องรับความเสี่ยงเอง หรืออาจจะใช้กลยุทธ์การลดความเสี่ยง (ลดโอกาส) ในขณะที่ความเสี่ยงที่มีผลกระทบสูงแต่โอกาสที่เกิดมีน้อยก็อาจจะเลือกที่จะหลีกเลี่ยงความเสี่ยง แต่ถ้าความเสี่ยงนั้นมีผลกระทบน้อยมากแม้ว่าโอกาสที่เกิดจะสูงก็อาจจะใช้กลยุทธ์การยอมรับความเสี่ยงได้