RISK MANAGEMENT SPECIALIST (RMS)
นักบริหารความเสี่ยงมืออาชีพ

TRISACADEMY of Management

สุรเดช จองวรรณศิริ
suradej@tris.co.th

22 May 2014

Outline (9.00-12.00)

- Enterprise Risk Management
  การบริหารความเสี่ยงองค์กร
- COSO-ERM Integrated Framework
  กรอบแนวคิดการบริหารความเสี่ยงเชิงบูรณาการที่องค์กรทั่วโลกใช้อ้างอิง
- ERM & IC for Risk Management
  การบริหารความเสี่ยงองค์กรและการบริหารความเสี่ยงหน่วยงานย่อยหรือการควบคุมภายใน เพื่อการบริหารความเสี่ยงบูรณาการทั้งระบบ
- Initiative for ERM
  แนวทางและกระบวนการในการริเริ่ม พัฒนา ระบบบริหารความเสี่ยงขึ้นในองค์กร
- Embedding risk management
  การดำเนินการต่อเนื่องสู่การสร้างวัฒนธรรมการจัดการความเสี่ยงทั่วทั้งองค์กร

TRISACADEMY of Management

WORLD ECONOMIC FORUM

Global Risks Report 2014

ประเภทของความเสี่ยง

Economic	Fiscal crises in key economies
	Failure of a major financial mechanism or institution
	Liquidity crises
	Structurally high unemployment/underemployment
	Oil-price shock to the global economy
	Failure/shortfall of critical infrastructure
	Decline of importance of the US dollar as a major currency
Environmental	Greater incidence of extreme weather events (e.g. floods, storms, fires)
	Greater incidence of natural catastrophes (e.g. earthquakes, tsunamis, volcanic eruptions, geomagnetic storms)
	Greater incidence of man-made environmental catastrophes (e.g. oil spills, nuclear accidents)
	Major biodiversity loss and ecosystem collapse (land and ocean)
	Water crises
	Failure of climate change mitigation and adaptation
Geopolitical	Global governance failure
	Political collapse of a nation of geopolitical importance
	Increasing corruption
	Major escalation in organized crime and illicit trade
	Large-scale terrorist attacks
	Deployment of weapons of mass destruction
	Violent inter-state conflict with regional consequences
	Escalation of economic and resource nationalization
Societal	Food crises
	Pandemic outbreak
	Unmanageable burden of chronic disease
	Severe income disparity
	Antibiotic-resistant bacteria
	Mismanaged urbanization (e.g. planning failures, inadequate infrastructure and supply chains)
	Profound political and social instability
Technological	Breakdown of critical information infrastructure and networks
	Escalation in large-scale cyber attacks
	Massive incident of data fraud/theft

TRISACADEMY of Management

WORLD ECONOMIC FORUM

Ten Global Risks of Highest Concern in 2014

ความเสี่ยงในปี 2557 ที่มีความกังวลสูงสุด 10 อันดับ จากการสำรวจ CEO

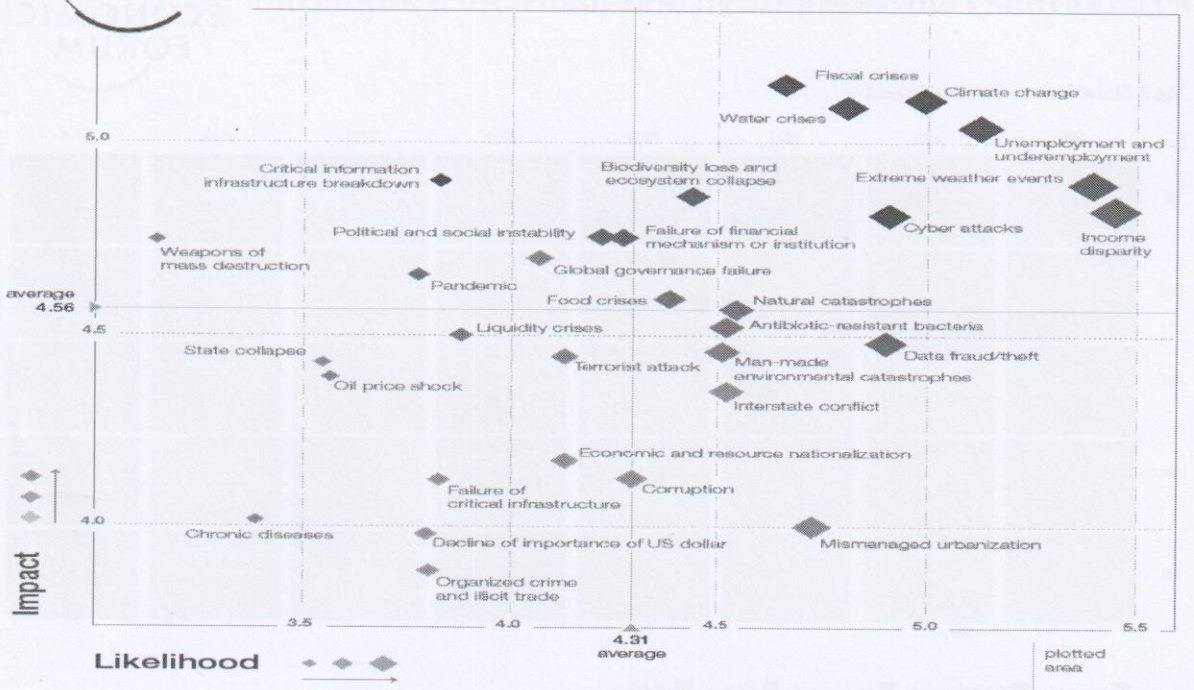
No.	Global Risk
1	Fiscal crises in key economies
2	Structurally high unemployment/underemployment
3	Water crises
4	Severe income disparity
5	Failure of climate change mitigation and adaptation
6	Greater incidence of extreme weather events (e.g. floods, storms, fires)
7	Global governance failure
8	Food crises
9	Failure of a major financial mechanism/institution
10	Profound political and social instability

Source: Global Risks Perception Survey 2013-2014.
Note: From a list of 31 risks, survey respondents were asked to identify the five they are most concerned about.

TRISACADEMY of Management

WORLD ECONOMIC FORUM

แผนผังความเสี่ยง แสดงผลกระทบ โอกาสที่จะเกิด และประเภทความเสี่ยง



TRISACADEMY of Management

เป็นการให้มุมมองที่หลากหลายและแปลกใหม่ด้วยตนเอง

Global Risks Report 2014

ความเสี่ยงที่มีความกังวลสูงสุดในโอกาสที่จะเกิดขึ้น 5 อันดับแรก

WORLD ECONOMIC FORUM

Top 5 Global Risks in Terms of Likelihood

เกิด

	2007	2008	2009	2010	2011	2012	2013	2014
1st	Breakdown of critical information infrastructure	Asset price collapse	Asset price collapse	Asset price collapse	Storms and cyclones	Severe income disparity	Severe income disparity	Income disparity
2nd	Chronic disease in developed countries	Middle East instability	Slowing Chinese economy (<6%)	Slowing Chinese economy (<6%)	Flooding	Chronic fiscal imbalances	Chronic fiscal imbalances	Extreme weather events
3rd	Oil price shock	Failed and failing states	Chronic disease	Chronic disease	Corruption	Rising greenhouse gas emissions	Rising greenhouse gas emissions	Unemployment and underemployment
4th	China economic hard landing	Oil and gas price spike	Global governance gaps	Fiscal crises	Biodiversity loss	Cyber attacks	Water supply crises	Climate change
5th	Asset price collapse	Chronic disease, developed world	Retrenchment from globalization (emerging)	Global governance gaps	Climate change	Water supply crises	Mismanagement of population ageing	Cyber attacks

Economic Environmental Geopolitical Societal Technological

TRISACADEMY of Management

Global Risks Report 2014

ความเสี่ยงที่มีความกังวลสูงสุดในขนาดของผลกระทบ 5 อันดับแรก

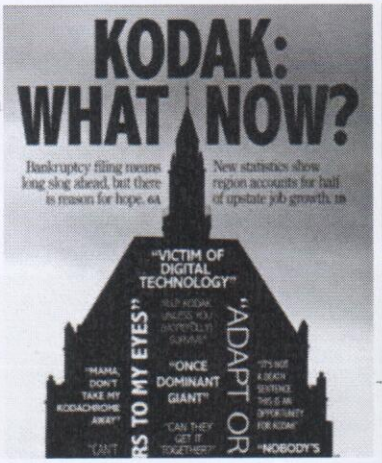
WORLD ECONOMIC FORUM

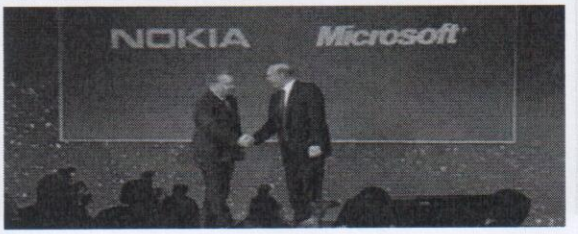
Top 5 Global Risks in Terms of Impact

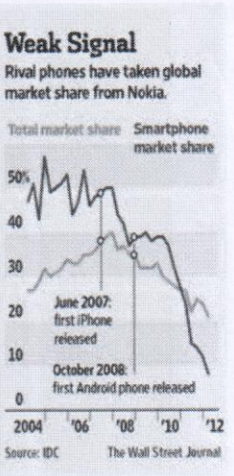
	2007	2008	2009	2010	2011	2012	2013	2014
1st	Asset price collapse	Asset price collapse	Asset price collapse	Asset price collapse	Fiscal crises	Major systemic financial failure	Major systemic financial failure	Fiscal crises
2nd	Retrenchment from globalization	Retrenchment from globalization (developed)	Retrenchment from globalization (developed)	Retrenchment from globalization (developed)	Climate change	Water supply crises	Water supply crises	Climate change
3rd	Interstate and civil wars	Slowing Chinese economy (<6%)	Oil and gas price spike	Oil price spikes	Geopolitical conflict	Food shortage crises	Chronic fiscal imbalances	Water crises
4th	Pandemics	Oil and gas price spike	Chronic disease	Chronic disease	Asset price collapse	Chronic fiscal imbalances	Diffusion of weapons of mass destruction	Unemployment and underemployment
5th	Oil price shock	Pandemics	Fiscal crises	Fiscal crises	Extreme energy price volatility	Extreme volatility in energy and agriculture prices	Failure of climate change adaptation	Critical information infrastructure breakdown

Economic Environmental Geopolitical Societal Technological

TRISACADEMY of Management





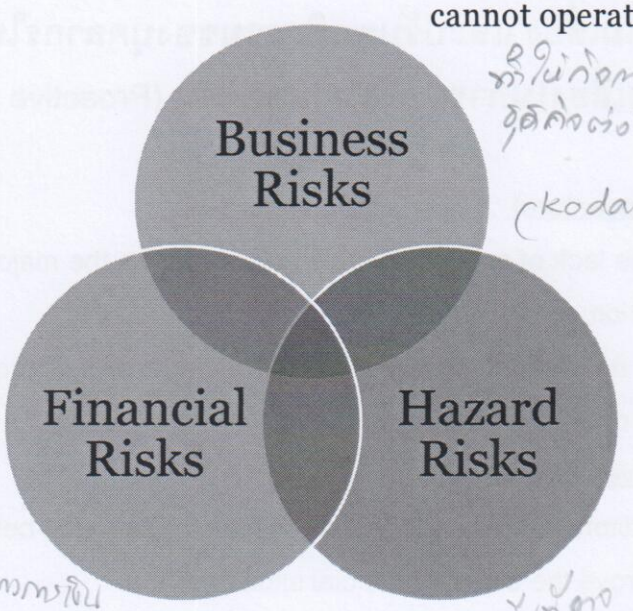


TRISACADEMY of Management

Enterprise Risk

ลักษณะความเสี่ยงระดับองค์กร

The Business risk is the possibility that an organization cannot operate successfully.



The financial risk is the possibility that a company will fail to meet financial obligations.

The hazard risk is defined as exposures that can cause loss without the possibility of gain.

TRISACADEMY of Management

Enterprise Risk Management

การบริหารความเสี่ยงองค์กร

Defined by COSO as,

"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."

ERM ENTERPRISE RISK MANAGEMENT

Everyone is a Risk Manager

TRISACADEMY of Management

Enterprise Risk Management

การบริหารความเสี่ยงองค์กร

เป้าหมายของ ERM คือ เพิ่มการมีส่วนร่วมและความรับผิดชอบของบุคลากรในการบริหารความเสี่ยง และปรับพฤติกรรมของบุคลากรในองค์กรให้มีความตระหนักต่อความเสี่ยงในการปฏิบัติงานของตน (Proactive behaviors)

Executive survey (Accenture)

- 82% considered the lack of enterprise-wide risk culture as the major cause of managerial dysfunction
- 85% said that they needed to improve their risk management approach in reaction to the current financial crisis

Internal auditors survey (IIA)

- 40% of internal auditors in the financial services sector said that better risk management practices could improve the current financial situation

TRISACADEMY of Management

Traditional Risk Management VS ERM

ความแตกต่างระหว่างการบริหารความเสี่ยงแบบดั้งเดิมกับ ERM

Traditional risk management	**ERM**
Risk as individual hazards	Risk viewed in context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Risks with no owners	Defined risk responsibilities
Haphazard risk quantification	Monitoring and measurement of risks

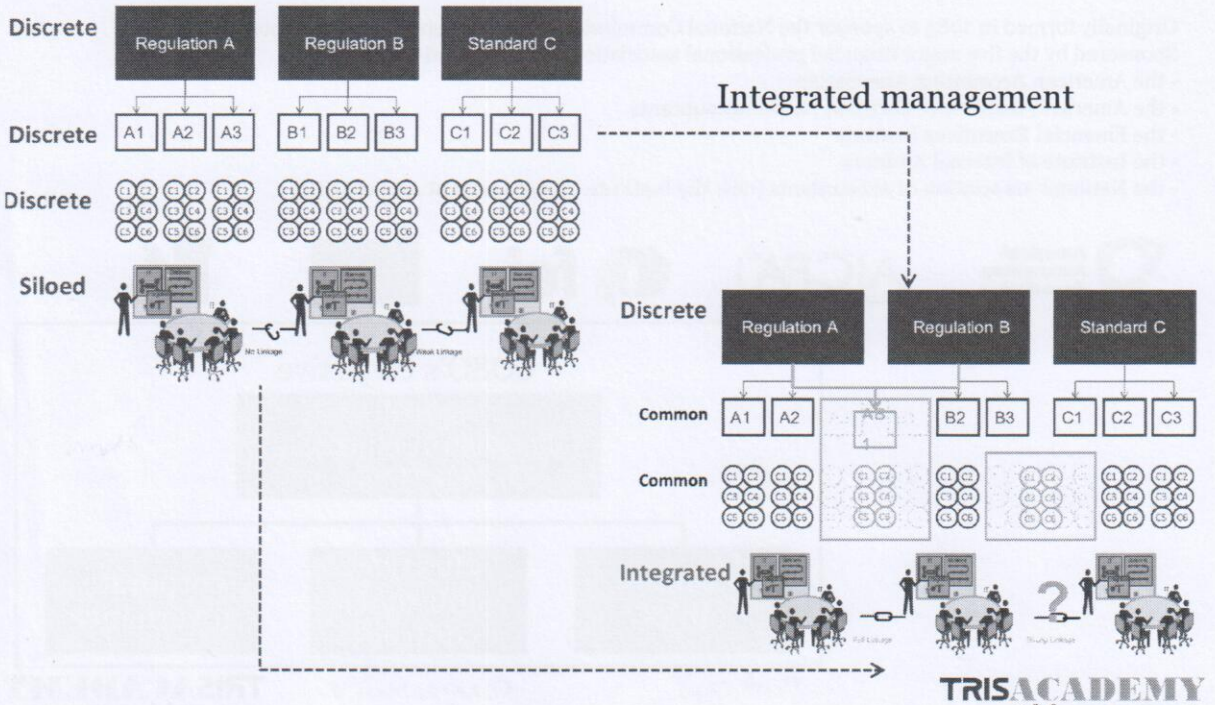
"Risk is not my responsibility"

"Risk is everyone's responsibility"

TRISACADEMY of Management

Traditional Risk Management VS ERM

ความแตกต่างระหว่างการบริหารความเสี่ยงแบบดั้งเดิมกับ ERM

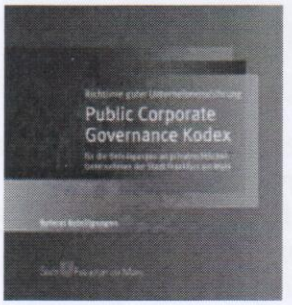


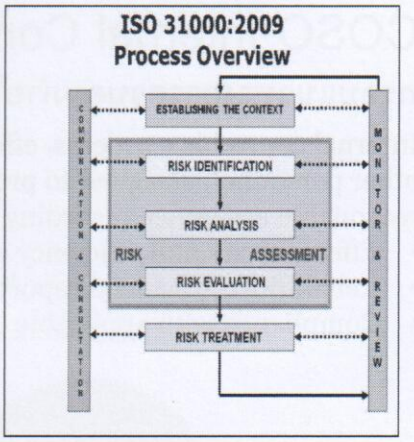
TRISACADEMY of Management

ERM Framework

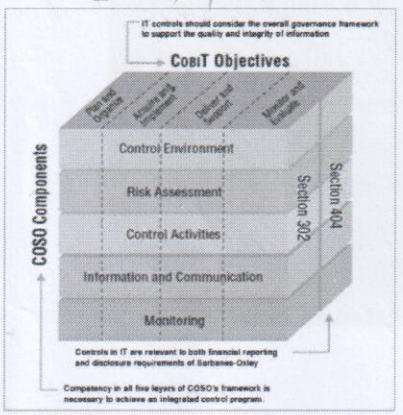
กรอบการบริหารความเสี่ยงองค์กร

- ISO 31000
- Sarbanes Oxley Act
- Corporate Governance Kodex
- COSO
- COBIT





COSO



Sarbanes-Oxley

Financial and Accounting Disclosure Information

Areas of Emphasis	Management Reporting	Board Governance	Management & Board Conduct	Enforcement & Penalties	Auditor Independence
Key Sections	* Management Certifications (Section 302)	Audit Committee Standards	Accelerated reporting of insider trading	Public Company Oversight Board (PCAOB)	Audit Committee pre-approval all auditor services
	* Management Report on Internal Controls (Section 404)	Prohibition of loans to Directors & Officers	Disclose Code of Conduct for finance officers	* Criminal penalties for knowingly untrue certifications (Section 906)	Prohibits auditor from certain services
			Protection of Whistleblowers		Lead audit partner limited to 5 year rotation

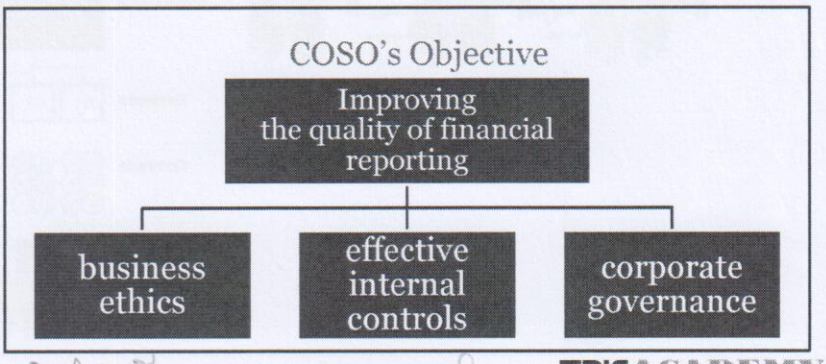
* Sections 302 & 404 address improving Corporate Governance through effective internal controls. Section 906 addresses criminal penalties.

TRISACADEMY of Management

COSO

COSO, the Committee of Sponsoring Organizations of the treadway Commission

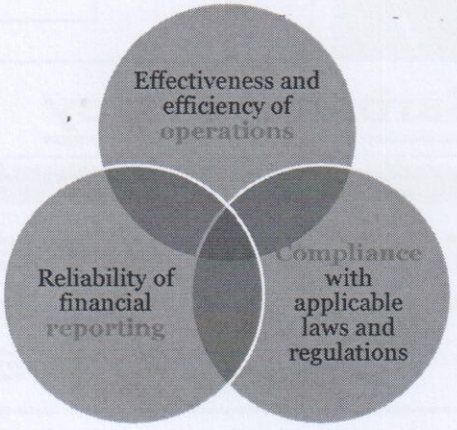
Originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting.
Sponsored by the five major financial professional associations in the United States
- the American Accounting Association
- the American Institute of Certified Public Accountants
- the Financial Executives Institute
- the Institute of Internal Auditors
- the National Association of Accountants (now the Institute of Management Accountants)

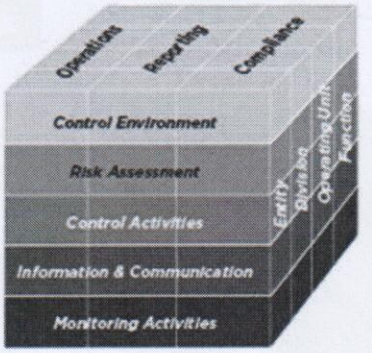


COSO-Internal Control

กรอบแนวทางการควบคุมภายในของ COSO

Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide
reasonable assurance regarding the achievement of objectives in
- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

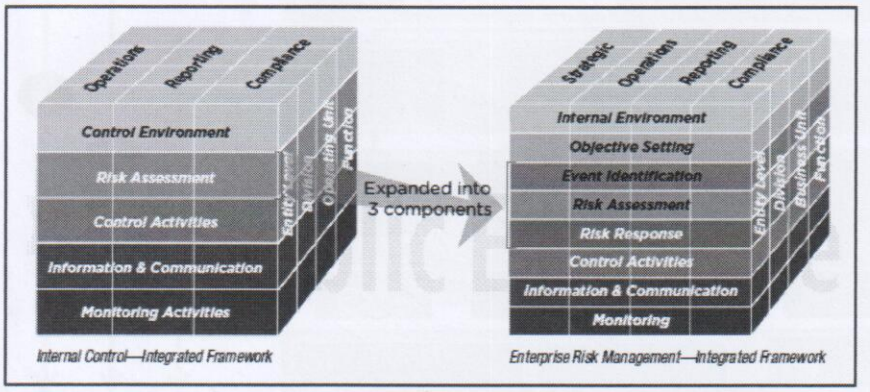




COSO-ERM Integrated Framework

กรอบแนวทางการบริหารความเสี่ยงองค์กรของ COSO

- Enterprise risk management is broader than internal control, elaborating on internal control and focusing more directly on risk.
- Internal control is an integral part of enterprise risk management, while enterprise risk management is part of the overall governance process.



Ref: Exposure Draft: Internal Control-Integrated Framework • September 2012 (COSO)

TRISACADEMY of Management

COSO-ERM Integrated Framework

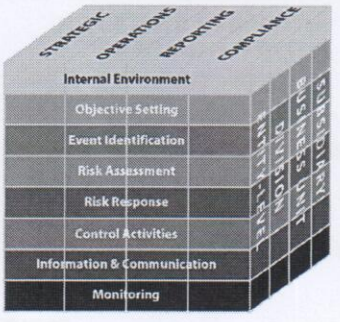
กลุ่มประเภทตามแนวทางของ COSO

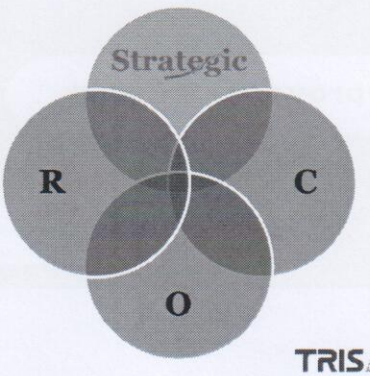
Strategic – relating to high-level goals, aligned with and supporting the entity's mission/vision.

Operations – relating to effectiveness and efficiency of the entity's operations, including performance and profitability goals. They vary based on management's choices about structure and performance.

Reporting – relating to the effectiveness of the entity's reporting. They include internal and external reporting and may involve financial or non-financial information.

Compliance – relating to the entity's compliance with applicable laws and regulations.

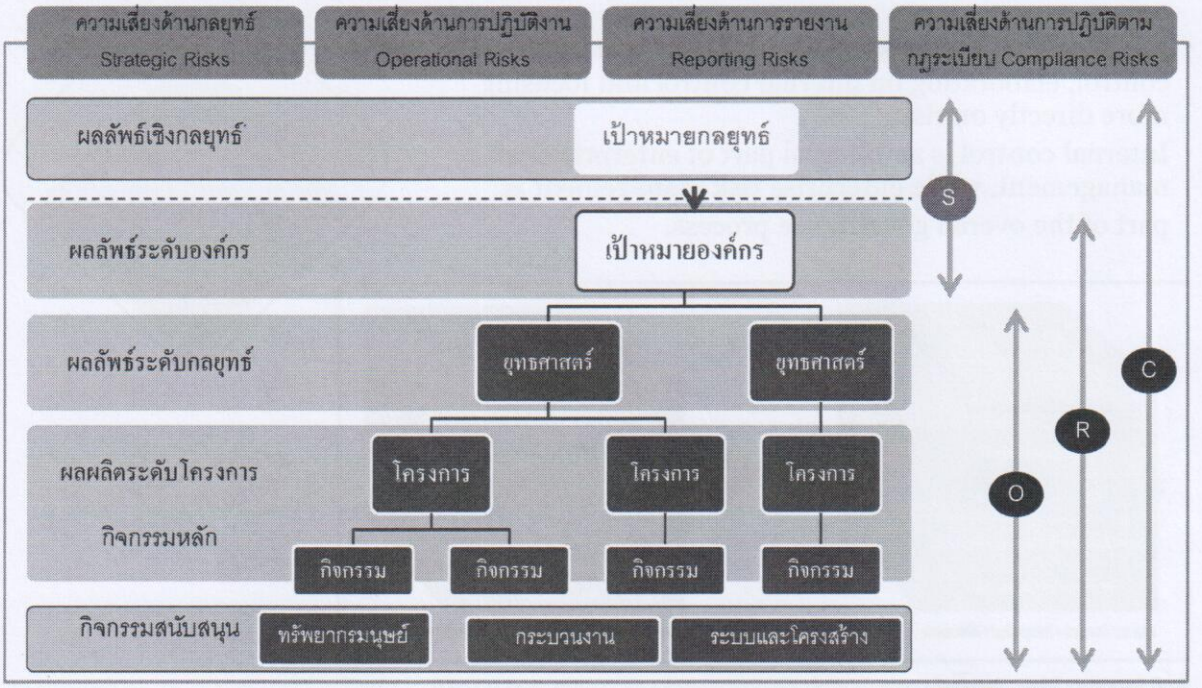




TRISACADEMY of Management

COSO-ERM Integrated Framework

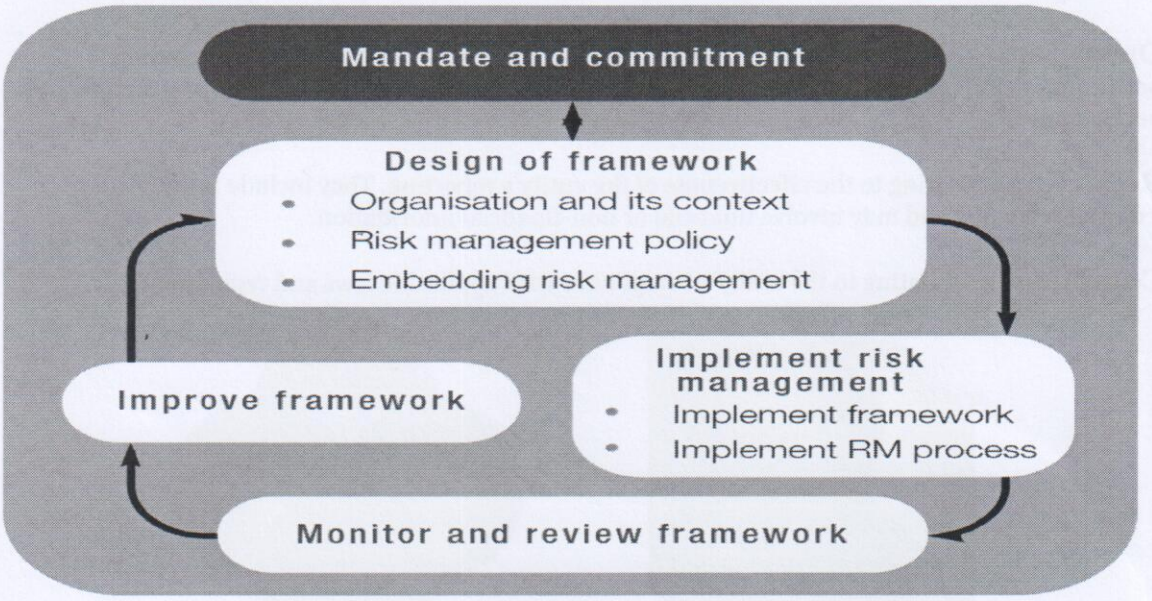
ภาพรวมการบริหารความเสี่ยงเชิงบูรณาการตามแนวทางของ COSO



TRISACADEMY of Management

ERM Process

กระบวนการของ ERM



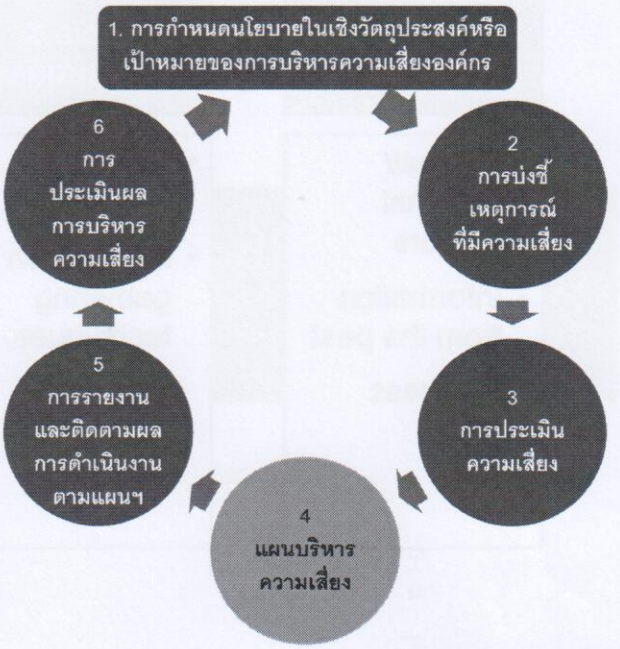
TRISACADEMY of Management

ERM Process

กระบวนการของ ERM

กระบวนการบริหารความเสี่ยงองค์กร โดยทั่วไป ประกอบด้วย

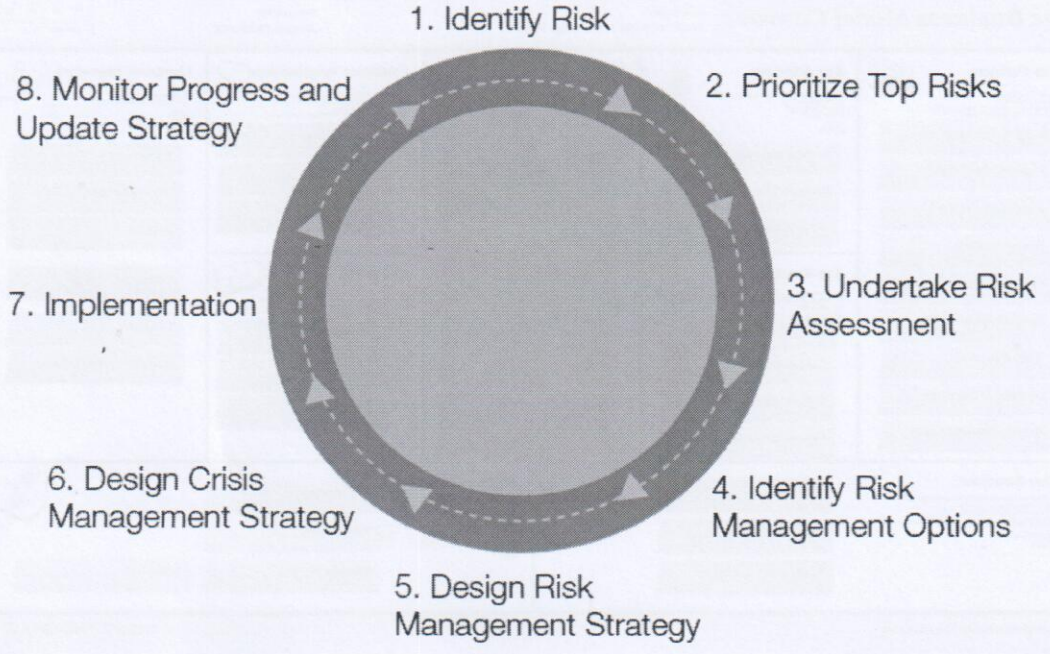
1. การกำหนดนโยบายในเชิงวัตถุประสงค์หรือเป้าหมายของการบริหารความเสี่ยงองค์กร
2. การบ่งชี้เหตุการณ์ที่มีความเสี่ยง
3. การประเมินความเสี่ยง
4. แผนบริหารความเสี่ยง
   - 4.1 กลยุทธ์การจัดการความเสี่ยง
   - 4.2 การจัดทำแผนบริหารความเสี่ยงองค์กร
5. การรายงานและติดตามผลการดำเนินงานตามแผนบริหารความเสี่ยง
6. การประเมินผลการบริหารความเสี่ยง



TRISACADEMY of Management

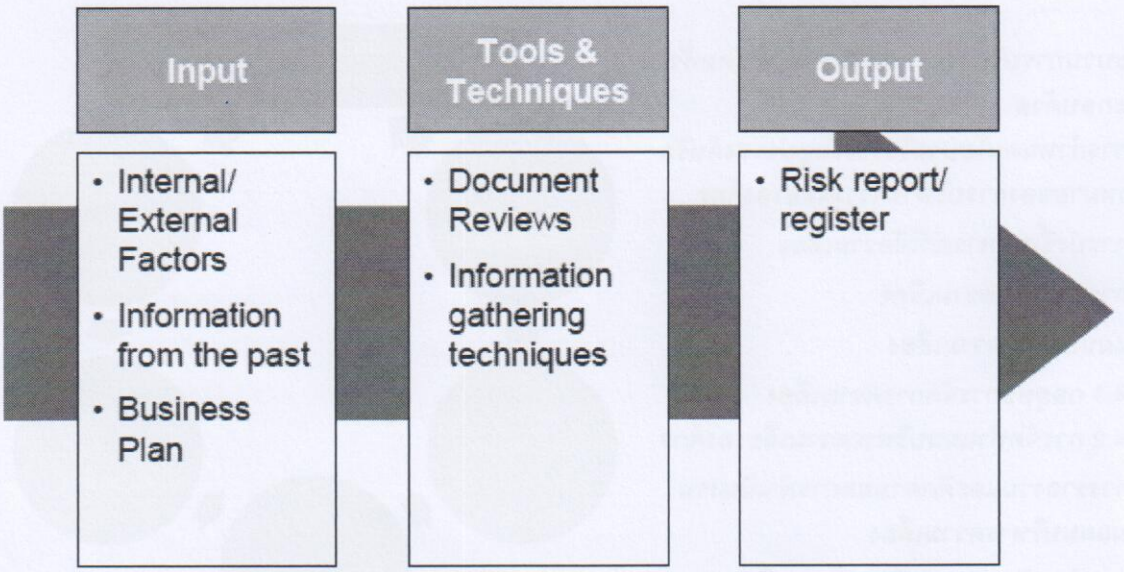
Risk Management Process

กระบวนการโดยทั่วไปของการบริหารความเสี่ยง



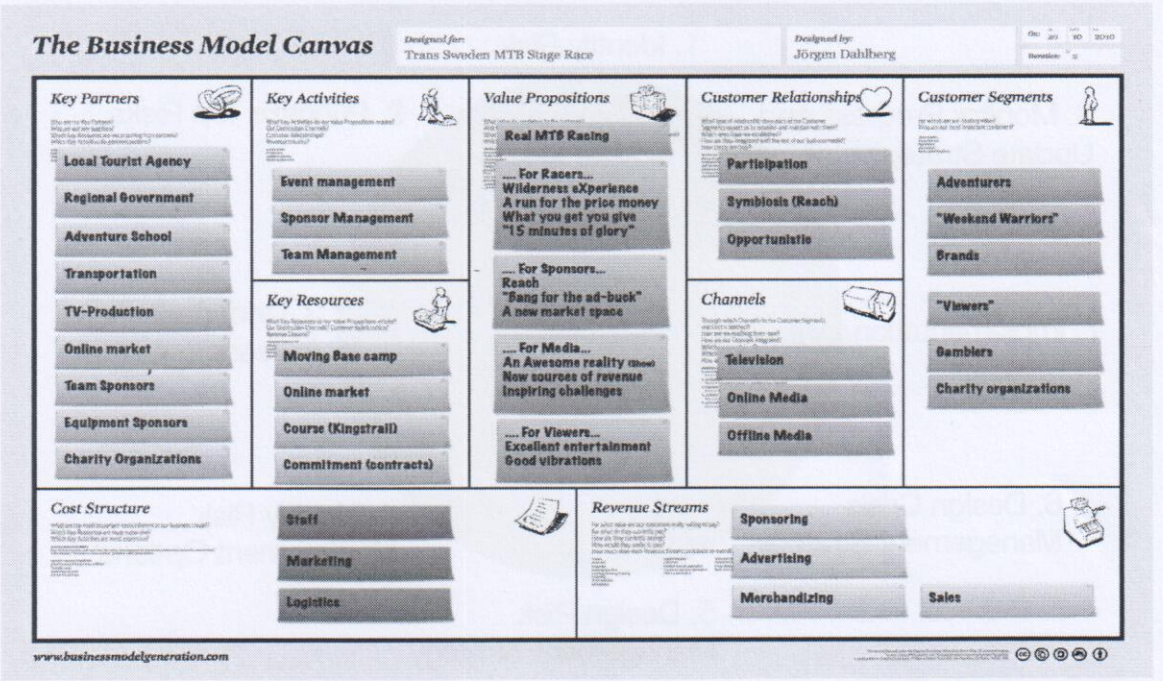
TRISACADEMY of Management

Risk Identification
การระบุความเสี่ยง



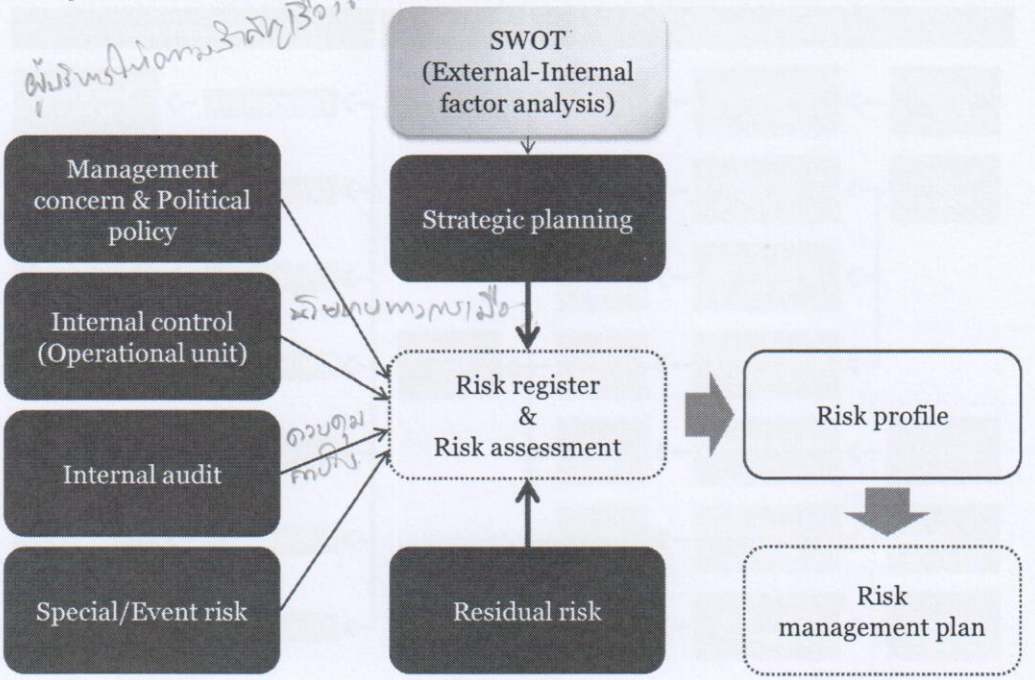
TRISACADEMY of Management

Risk Identification
การระบุความเสี่ยง

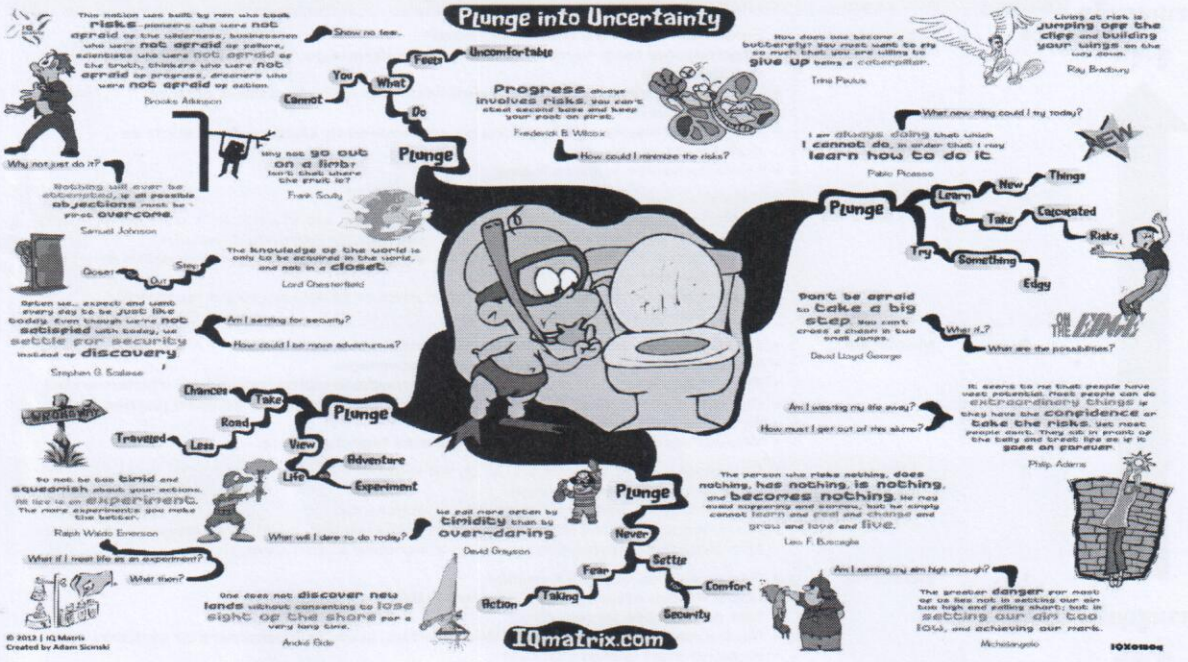


TRISACADEMY of Management

Risk Identification
การระบุความเสี่ยง

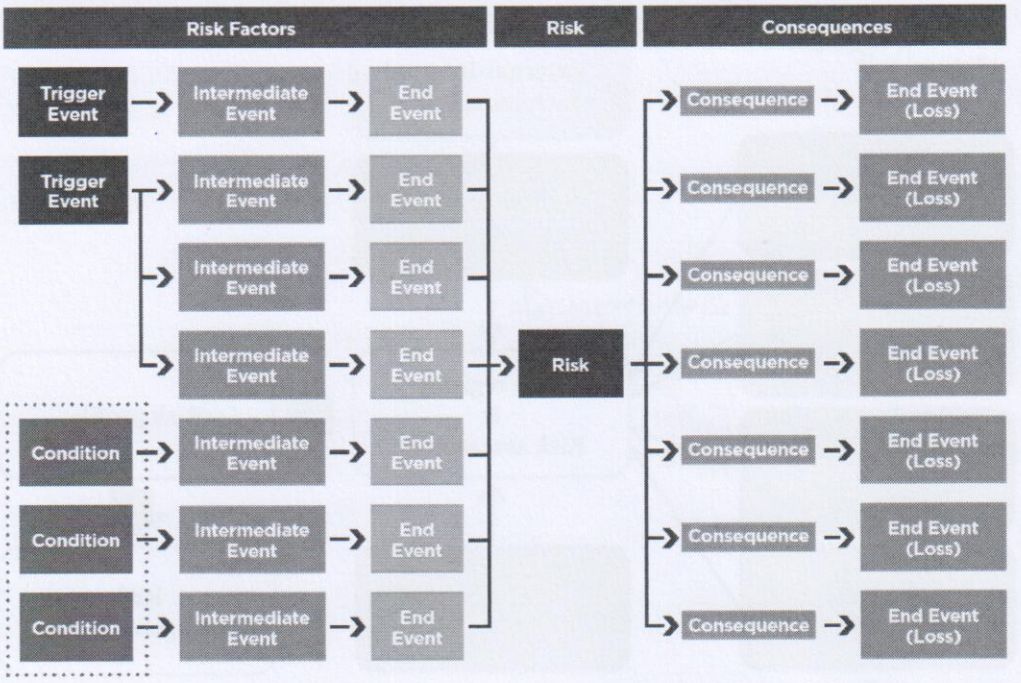


Risk Identification
การระบุความเสี่ยง



Risk Identification

การระบุความเสี่ยง



TRISACADEMY of Management

Risk Analysis

การวิเคราะห์ความเสี่ยง

ความสูญเสียสูงสุด

Rating	Descriptor	Definition
5	Extreme	• Financial loss of $X million or more[3] • 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

ความสูญเสียต่ำสุด

TRISACADEMY of Management

Risk Analysis
การวิเคราะห์ความเสี่ยง

โอกาสเกิดขึ้นสูงสุด

โอกาสเกิดขึ้นต่ำสุด

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

TRISACADEMY of Management

Risk Analysis
การวิเคราะห์ความเสี่ยง

ตัวอย่างมิติในการพิจารณากำหนดผลกระทบหรือความสูญเสีย

Impact	1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Cost	Insignificant cost increase	< 10% cost increase	10-20% cost increase	20-40% cost increase	> 40% cost increase
Time	Insignificant time increase	< 5% time increase	5-10% time increase	10-20% time increase	> 20% time increase
Scope	Scope decrease barely noticeable	Minor areas of scope affected	Major areas of scope affected	Scope reduction unacceptable to sponsor	Project end item is effectively useless
Quality	Quality degradation barely noticeable	Only very demanding applications are affected	Quality reduction requires sponsor approval	Quality reduction unacceptable	Project end item is effectively useless

TRISACADEMY of Management

Risk Analysis
การวิเคราะห์ความเสี่ยง

การจัดทำผังความเสี่ยง (Risk Matrix หรือ Risk Profile)

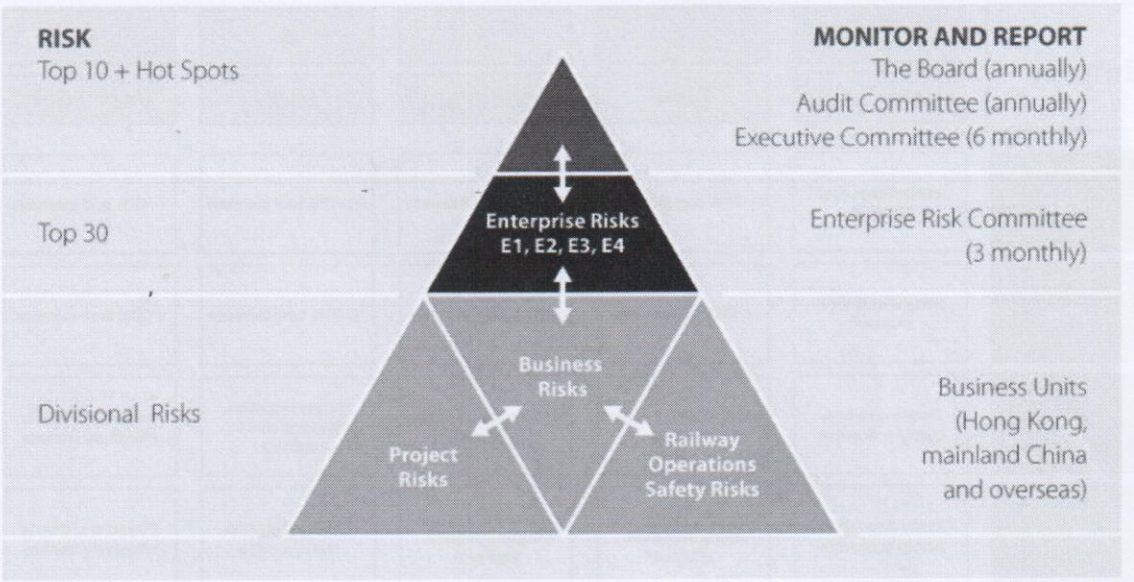
Risk = Impact x Likelihood

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Moderate	High	High	Extreme	Extreme
Likely	Moderate	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Moderate	Moderate	Moderate	High
Rare	Low	Low	Moderate	Moderate	High

TRISACADEMY of Management

Risk Analysis
การวิเคราะห์ความเสี่ยง

ตัวอย่างกรอบแนวทางการบริหารความเสี่ยงองค์กร

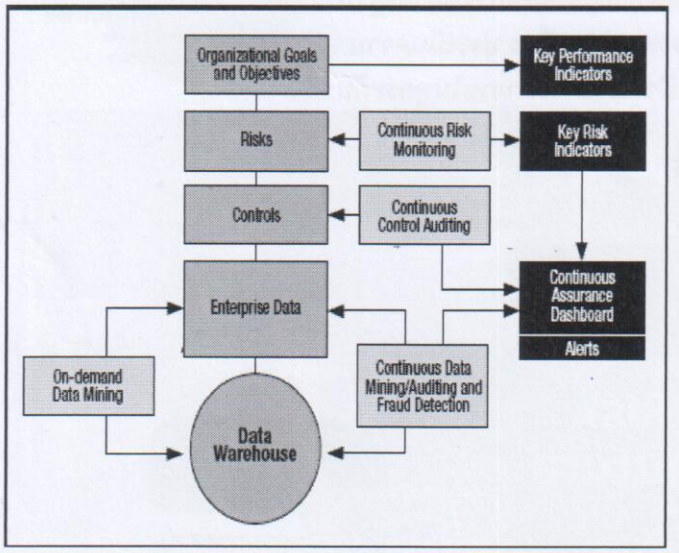


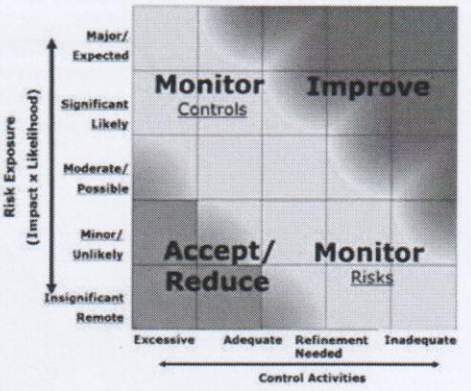
TRISACADEMY of Management

Risk Response
การตอบสนองต่อความเสี่ยง

TRISACADEMY of Management

Risk Control
การควบคุมความเสี่ยง





TRISACADEMY of Management

Risk Control

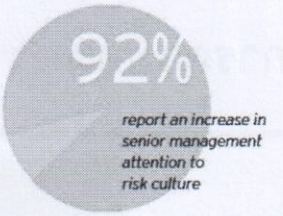
การควบคุมความเสี่ยง

ระดับความเสี่ยง	แนวทางการปฏิบัติและเงื่อนไขเวลา
เล็กน้อย	ไม่ต้องดำเนินการใดๆ เพิ่มเติม
ยอมรับได้	ไม่ต้องมีการควบคุมเพิ่มเติม การกำหนดมาตรการควบคุมเพิ่มเติมอาจทำเมื่อเห็นว่าสามารถลดความสูญเสียให้กับองค์กรได้ การติดตามตรวจสอบยังคงต้องทำเพื่อให้แน่ใจว่าการควบคุมยังคงมีอยู่และใช้ได้ผล
ปานกลาง	จะต้องใช้ความพยายามที่จะลดความเสี่ยงลง การดำเนินการจัดหามาตรการเพื่อลดความเสี่ยงลงจะต้องอยู่ภายในระยะเวลาที่กำหนดไว้ เมื่อความเสี่ยงระดับปานกลางมีความสัมพันธ์กับอันตรายร้ายแรง ควรทำการประเมินเพิ่มเติมด้วยเทคนิคที่เหมาะสม เพื่อหาความเป็นไปได้ที่จะเกิดอันตรายที่แม่นยำขึ้นเพื่อการตัดสินความจำเป็นในการปรับปรุงแก้ไขมาตรการควบคุมต่อไป
สูง	ต้องลดความเสี่ยงลงก่อนจึงเริ่มทำงานได้ ต้องจัดสรรทรัพยากรให้เหมาะสมและเพียงพอเพื่อลดความเสี่ยงนั้น โดยถ้าความเสี่ยงเกิดขึ้นในกระบวนการผลิตหรือระหว่างการปฏิบัติงานจะต้องมีการแก้ไขอย่างเร่งด่วน
ที่ยอมรับไม่ได้	งานจะเริ่มหรือทำต่อไปไม่ได้จนกว่าจะลดความเสี่ยงลง ถ้าไม่สามารถลดความเสี่ยงลงได้ ถึงแม้จะใช้ทรัพยากรอย่างไม่จำกัดหรืออย่างเต็มที่แล้วก็ตาม ต้องห้ามทำงานต่อไปอย่างเด็ดขาด

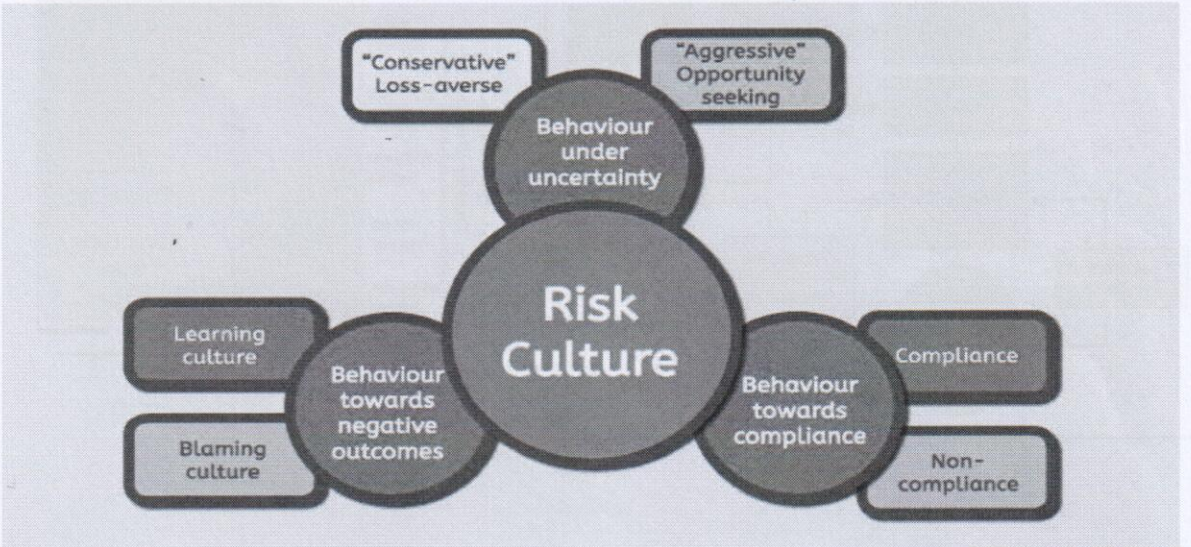
TRISACADEMY of Management

Risk Culture

วัฒนธรรมการตระหนักต่อความเสี่ยง



องค์กรที่มี Strong Risk Culture จะเป็นองค์กรที่มีความมุ่งมั่นต่อการมีมาตรฐานการปฏิบัติงานที่จะผนวกในกระบวนการของการระบุความเสี่ยง ประเมินความเสี่ยง และจัดการความเสี่ยงอย่างเป็นระบบ ต่อเป้าหมายการทำงานในทุกระดับ



TRISACADEMY of Management

Value of ERM

คุณค่าจากการพัฒนาระบบบริหารความเสี่ยงองค์กร

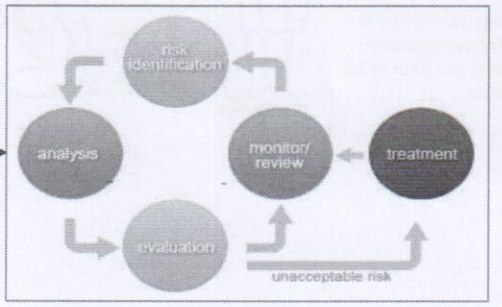
" High Risk, High Return "

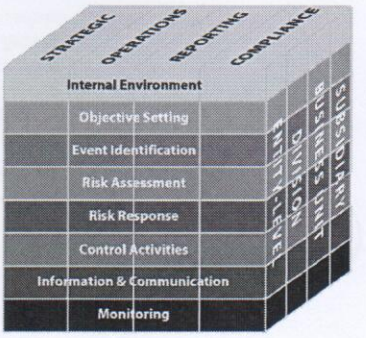
	Impact									
	Opportunities					Risks				
Likelihood	Extreme	Major	Moderate	Minor	Incidental	Incidental	Minor	Moderate	Major	Extreme
Frequent										
Likely										
Possible										
Unlikely										
Rare										

TRISACADEMY of Management

RISK – RISK Management – ERM

Risk Management Process





Enterprise-wide Risk Management

Probable impact			
Significant	Average	High	High
Average	Low	Average	High
Insignificant	Low	Low	Average
	Improbable	Possible	Probable
	Likelihood of risk occurring		

Risk = Impact x Likelihood

TRISACADEMY of Management

Performance Management & Risk Management

TRISACADEMY of Management

Q & A

"What really makes ERM successful is what I call — having everybody in the organization thinking about risk whenever they have to make a decision."
—Paul Sobel

Another way to say this is to bake risk management thinking into the DNA of an organization.

Thank You

สถาบันวิทยาการจัดการ
TRIS Academy of Management
บริษัท ทริส คอร์ปอเรชั่น จำกัด
อาคารสีลมคอมเพล็กซ์ ชั้น 24
เลขที่ 191 ถนนสีลม แขวงสีลม เขตบางรัก กรุงเทพฯ 10150
โทรศัพท์ 0 2231 3011 ต่อ318 โทรสาร 0 2231 3680
e-Mail : trisacademy@tris.co.th
www.trisacademy.com